GLOBAL CYBER THREAT INTELLIGENCE REPORT

Comprehensive Analysis of 829 Monitored Threads

Generated: May 20, 2026

Classification: TLP:CLEAR

Scope: Dark Web, Clear Web, Telegram, and Exploit Forums

1. Executive Summary

This comprehensive threat intelligence report details the findings from an exhaustive analysis of 829 distinct cyber incidents monitored across open web, deep web, and Telegram channels up to May 2026. The compiled data highlights a highly active and volatile threat landscape characterized by the industrialized distribution of credential combo lists, targeted website defacements, and severe data breaches affecting both public and private sectors globally.

A significant portion of the observed chatter relates to credential stuffing activities, with threat actors freely distributing or selling access to massive databases of compromised accounts. These credentials, often aggregated from infostealer logs and past breaches, target global consumer brands, gaming platforms, and enterprise infrastructure. Furthermore, hacktivist groups and independent actors continue to actively exploit vulnerabilities in web applications to execute website defacements, while initial access brokers (IABs) and malware developers trade sensitive network entry points and customized attack tools.

This document presents a statistical overview of the current threat environment, an in-depth analysis of attack vectors, and a detailed compilation of verified threat threads, intended to provide actionable intelligence for network defenders, security analysts, and policy-makers.

2. Methodology and Scope

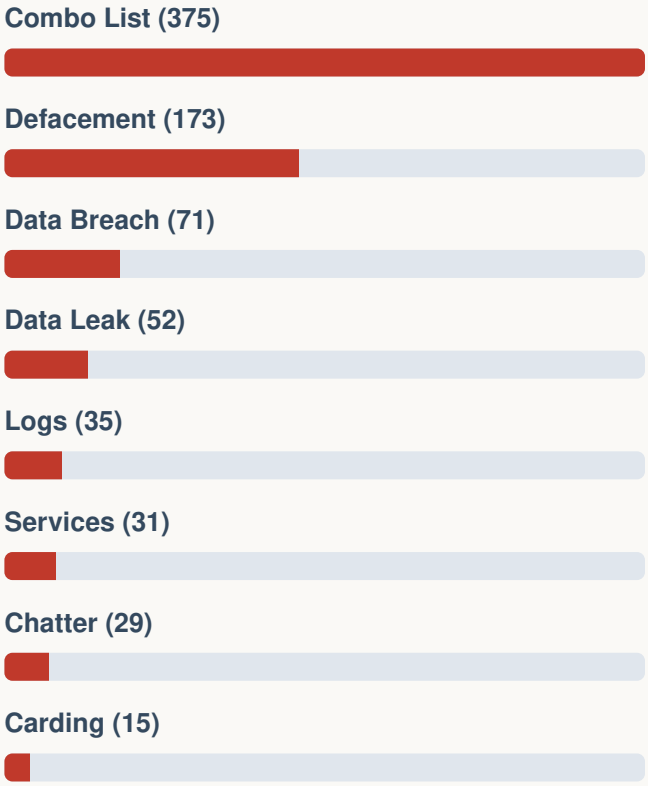
The intelligence contained within this report was aggregated by continuously monitoring prominent cybercrime forums, darknet marketplaces, hacktivist communication channels, and specialized Telegram groups. The data extraction process utilized automated scraping combined with human-curated analysis to verify threat claims, filter out false positives, and categorize incidents accurately.

Incidents are classified into primary threat categories, including **Combo Lists** (collections of credentials), **Defacements** (unauthorized modifications of websites), **Data Leaks and Breaches** (unauthorized exfiltration of sensitive information), **Logs** (output from infostealer malware), and **Chatter** (discussions, recruitment, and service offerings). The scope covers global targets without geographic restrictions, reflecting the inherently borderless nature of modern cybercrime.

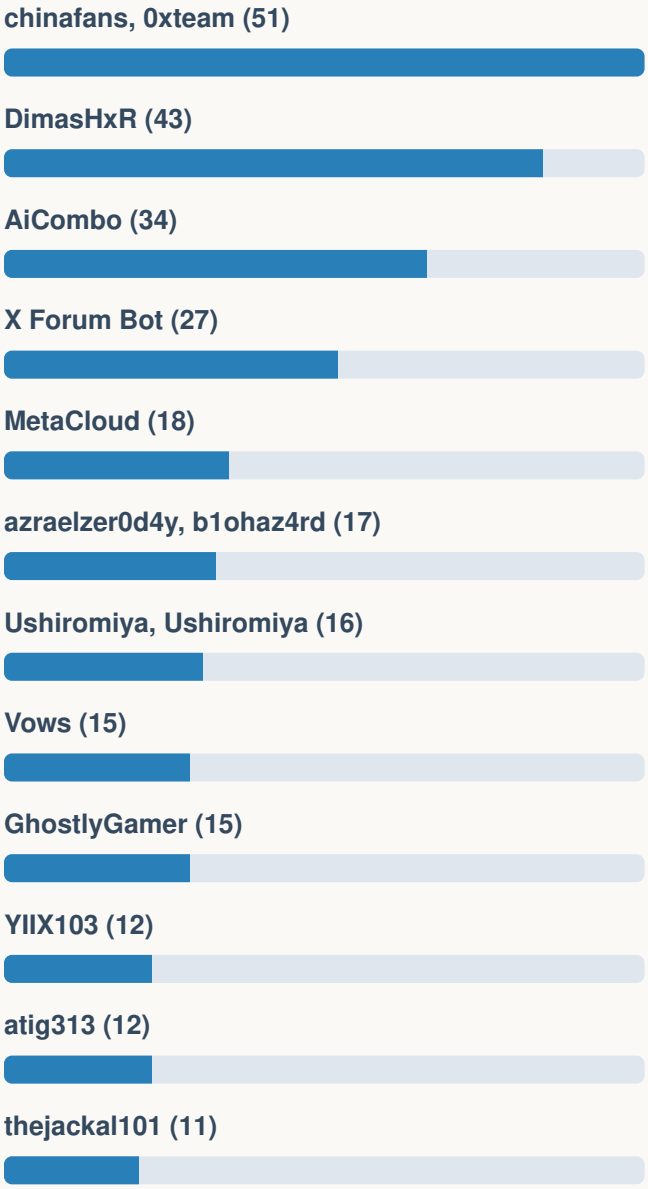
3. Statistical Overview

The following charts represent the quantitative analysis of the 829 monitored threads, breaking down the frequency of incidents by category, the most prolific threat actors, and the most frequently targeted countries (where identifiable).

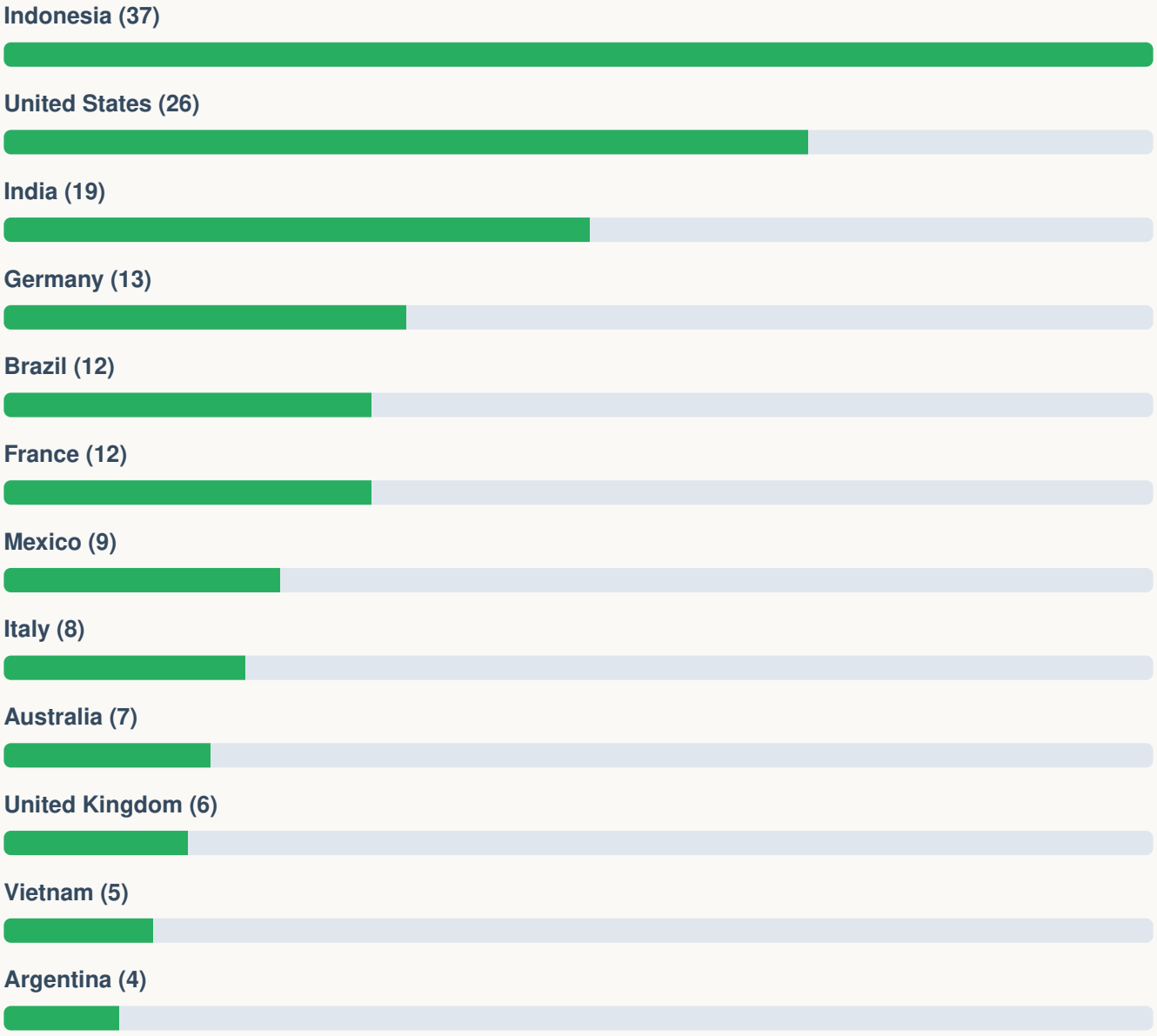
Top Threat Categories



Top Threat Actors



Top Targeted Countries



4. Threat Landscape Analysis

4.1 Credential Stuffing and Combo Lists

The overwhelming majority of the analyzed threads pertain to the distribution and sale of combo lists. These lists are massive compilations of email addresses and passwords, or URL:Login:Password (ULP) combinations, harvested from previous data breaches and info-stealer malware campaigns.

Threat actors such as **DimasHxR**, **AiCombo**, and **GhostlyGamer** are highly active in aggregating and selling this data.

These credentials are explicitly marketed for "credential stuffing" attacks against major platforms including Netflix, Spotify, Microsoft (Outlook/Hotmail), Roblox, and regional e-commerce sites. The sheer volume of records—frequently numbering in the hundreds of thousands or millions per post—indicates a heavily automated and industrialized underground economy. By utilizing tools like OpenBullet and SilverBullet, attackers rapidly validate these credentials against target APIs to achieve account takeovers (ATO).

4.2 Website Defacements and Hacktivism

Website defacements form another significant cluster of activity. Attackers often target vulnerable Content Management Systems (CMS) such as WordPress, exploiting weak plugins, outdated software, or misconfigured upload directories. While some defacements are acts of political hacktivism (e.g., targeting government or educational institutions in Indonesia, Brazil, and India), many appear opportunistic, perpetrated by actors seeking notoriety or practicing their exploitation skills.

Notably, actors like **DimasHxR** execute precise sub-directory defacements, indicating localized file-upload vulnerabilities rather than full server compromises. These incidents are frequently mirrored on archival sites like zone-xsec for permanent bragging rights.

4.3 Data Breaches and Infostealer Logs

High-value data breaches continue to pose a severe risk to corporate and governmental data confidentiality. Several incidents in the dataset involve the alleged compromise of highly sensitive databases, including civil registries (e.g., Indonesia's Dukcapil), healthcare patient records, and internal corporate CRM systems. Threat actors frequently provide data samples as proof of compromise and solicit payments in cryptocurrency.

In parallel, the sale of fresh "Stealer Logs" (data exfiltrated by malware like RedLine or Raccoon Stealer) has become a booming micro-economy. These logs provide attackers with immediate access to active session cookies, saved browser passwords, and cryptocurrency wallets, bypassing traditional MFA mechanisms.

4.4 Dark Web Services and Initial Access

The analysis also identified active "chatter" regarding the sale of specialized cybercrime services. Initial Access Brokers (IABs) advertise unauthorized access to corporate networks, enabling devastating follow-on attacks by ransomware affiliates. Furthermore, developers are actively selling

customized malware, Phishing-as-a-Service (PhaaS) kits, and bespoke C2 frameworks (e.g., Nighthawk C2), lowering the barrier to entry for novice cybercriminals.

5. Detailed Incident Log

The following section provides an exhaustive chronological breakdown of 300 highly significant cyber incidents from the dataset, capturing the metadata, categorization, and contextual content extracted from underground forums.

[1] Sale of private email access combo list with 45,807 credentials

Date: 2026-05-19T23:57:46Z | **Category:** Combo List | **Actor:** AiCombo

Description: A combo list of 45,807 email credentials described as private full-access mail combos was shared on a cracking forum. The post appears to contain email:password pairs intended for credential stuffing or account takeover. No specific breached organization is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-45-807-Private-FA-Mail-Access-Combolist`

[2] Free distribution of worldwide Hotmail/Gmail combo list

Date: 2026-05-19T23:57:21Z | **Category:** Combo List | **Actor:** Lulpab

Description: A threat actor known as Lulpab is freely distributing a combo list of Hotmail and Gmail credential lines marketed as fresh and high-quality. The post advertises daily releases of worldwide email credentials and directs users to a Telegram channel for additional content.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-%E2%9C%A8-FRESH-WORLDWIDE-HQ-HOTMAIL-LINES-20-05-26-01-%E2%9C%A8`

[3] Website Redefacement of lahudky.online by azraelzer0d4y (b1ohaz4rd)

Date: 2026-05-19T23:55:20Z | **Category:** Defacement | **Actor:** azraelzer0d4y, b1ohaz4rd

Description: The website lahudky.online was redefaced by threat actor azraelzer0d4y, affiliated with the group b1ohaz4rd, on May 20, 2026. This incident is classified as a redefacement, indicating the site had been previously compromised and defaced by the same or another actor. The attack targeted a subdirectory of the site, suggesting exploitation of a specific web application component or uploaded media path.

Target Context: Organization: *Lahudky* | Industry: *Food and Beverage* | Country: *Unknown*

Source URL: `https://zone-xsec.com/mirror/id/925124`

[4] Sale of Cracked BlackBullet 2.1.6 Credential Stuffing Tool

Date: 2026-05-19T23:53:48Z | **Category:** Combo List | **Actor:** Starip

Description: A cracked version of BlackBullet 2.1.6, a modular credential-stuffing and automation suite, is being distributed on a cracking forum. The tool supports custom configs, proxy handling, multi-threaded processing, and real-time stats for large-scale credential-stuffing operations. A VirusTotal link is provided alongside a disclaimer noting antivirus detections.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://demonforums.net/Thread-BlackBullet-2-1-6-Cracked`

[5] Forum chatter: user concern over USPS inquiry following delayed mail package

Date: 2026-05-19T23:52:26Z | **Category:** Chatter | **Actor:** yayoboggins 🍼

Description: A darknet forum user posted seeking advice after contacting USPS about a delayed package reportedly containing counterfeit pills. The post contains no threat intelligence value and does not describe a cyber attack, breach, or criminal service offering. Content is personal in nature and relates to physical contraband, not digital threats.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion/post/4cf23e065a14e7099662`

[6] Alleged mass website defacements by HELLR00TERS TEAM

Date: 2026-05-19T23:52:15Z | **Category:** Defacement | **Actor:** HELLR00TERS TEAM

Description: HELLR00TERS TEAM claims to have hacked and defaced multiple WordPress-based websites across various countries. The threat actor posted links to compromised sites hosted on multiple domains, primarily printing and design-related businesses. The defacement appears to involve uploading files to WordPress upload directories on compromised sites.

Target Context: Organization: *Unknown* | Industry: *Printing, Design, E-commerce* | Country: *Unknown*

Source URL: `https://t.me/c/3865526389/982`

[7] Website defacement of cyos.co.in by azraelzer0d4y of b1ohaz4rd

Date: 2026-05-19T23:49:15Z | **Category:** Defacement | **Actor:** azraelzer0d4y, b1ohaz4rd

Description: On May 20, 2026, the website cyos.co.in was defaced by threat actor azraelzer0d4y, operating under the team b1ohaz4rd. The defacement targeted a subdirectory path related to customer address media files and was neither a mass nor home page defacement. The incident was archived via zone-xsec mirror for reference.

Target Context: Organization: *CYOS* | Industry: *Unknown* | Country: *India*

Source URL: `https://zone-xsec.com/mirror/id/925123`

[8] Mass Defacement of Indonesian School Website by Irene (XmrAnonye.id)

Date: 2026-05-19T23:46:20Z | **Category:** Defacement | **Actor:** Irene, XmrAnonye.id

Description: The website of SMAN 3 Purwakarta, an Indonesian public high school, was defaced by a threat actor identified as Irene operating under the team XmrAnonye.id. This incident is classified as both a mass defacement and a redefacement, indicating the attacker has previously compromised this or related targets. The defacement was hosted on a Linux-based server and archived via haxor.id.

Target Context: Organization: *SMAN 3 Purwakarta* | Industry: *Education* | Country: *Indonesia*

Source URL: `https://haxor.id/archive/mirror/249401`

[9] Website Defacement of Hot Tub Rescue by azraelzer0d4y (b1ohaz4rd)

Date: 2026-05-19T23:40:27Z | **Category:** Defacement | **Actor:** azraelzer0d4y, b1ohaz4rd

Description: On May 20, 2026, threat actor azraelzer0d4y, operating under the team b1ohaz4rd, defaced a media/custom directory page on hottubrescue.co.uk, a UK-based hot tub service and retail website. The incident was a targeted single-page defacement, not classified as a mass or home page defacement. No specific motive or server details were disclosed.

Target Context: Organization: *Hot Tub Rescue* | Industry: *Retail / Home & Leisure Services* | Country: *United Kingdom*

Source URL: `https://zone-xsec.com/mirror/id/925122`

[10] Website Defacement of Instant Promotion by DimasHxR

Date: 2026-05-19T23:34:14Z | **Category:** Defacement | **Actor:** DimasHxR

Description: On May 20, 2026, a threat actor identified as DimasHxR defaced a subdirectory of instantpromotion.co.uk, a UK-based marketing and promotions website. The attack was a targeted single-site defacement with no team affiliation reported. Technical details regarding the server environment and attack vector were not disclosed.

Target Context: Organization: *Instant Promotion* | Industry: *Marketing and Advertising* | Country: *United Kingdom*

Source URL: `https://zone-xsec.com/mirror/id/925119`

[11] Website Defacement of MiMarket.mx by DimasHxR

Date: 2026-05-19T23:32:39Z | **Category:** Defacement | **Actor:** DimasHxR

Description: On May 20, 2026, the threat actor DimasHxR defaced a media/customer directory page on mimarket.mx, a Mexican e-commerce or retail platform. The attack was a targeted, non-mass defacement affecting a specific subdirectory rather than the homepage. No team affiliation, stated motive, or technical server details were disclosed in association with this incident.

Target Context: Organization: *MiMarket* | Industry: *E-Commerce / Retail* | Country: *Mexico*

Source URL: `https://zone-xsec.com/mirror/id/925121`

[12] Website Defacement of Farmacia.pro by DimasHxR

Date: 2026-05-19T23:30:47Z | **Category:** Defacement | **Actor:** DimasHxR

Description: On May 20, 2026, a threat actor known as DimasHxR defaced a subdirectory of farmacia.pro, a website associated with pharmacy or pharmaceutical services. The defacement targeted a specific media/customer path rather than the homepage, suggesting a targeted or opportunistic attack on a vulnerable web resource. No team affiliation, stated motive, or technical details regarding the server environment were disclosed.

Target Context: Organization: *Farmacia* | Industry: *Healthcare / Pharmacy* | Country: *Unknown*

Source URL: `https://zone-xsec.com/mirror/id/925118`

[13] Sale of European mixed combo list with 30,432 credentials

Date: 2026-05-19T23:29:23Z | **Category:** Combo List | **Actor:** AiCombo

Description: A combo list containing 30,432 email and password pairs described as a private full access European mix has been shared on a cracking forum. The post appears to offer credentials for use in credential stuffing activities. No specific victim organization or breach source is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-30-432-Private-FA-Europa-Mix-Combo`

[14] Sale of email:password combo list (mixed USA and Worldwide)

Date: 2026-05-19T23:28:55Z | **Category:** Combo List | **Actor:** Reoza

Description: A threat actor is selling a combo list of 663,000 email:password credentials described as mixed USA and worldwide. The listing is priced cheaply with no refund or replacement policy, but testing is available. No specific breach source or victim organization is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Supreme-WTS-GOOD-COMBOS-EMAIL-PASS--2096581`

[15] Sale of 190K Fresh HQ Email:Password Combo List

Date: 2026-05-19T23:25:13Z | **Category:** Combo List | **Actor:** Ra-Zi

Description: A threat actor is distributing and selling a combo list of approximately 190,000 email:password credential pairs marketed as fresh and high quality. The credentials are advertised as suitable for credential stuffing against services including Netflix, Minecraft, Uplay, Steam, Hulu, and Spotify. The actor promotes sales via Telegram and a cracking-focused website.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://demonforums.net/Thread-190k-Fresh-HQ-Combolist-Email-Pass-Netflix-Minecraft-Uplay-Steam-Hulu-spotify--204812`

[16] Website Defacement of Siola.it by DimasHxR

Date: 2026-05-19T23:24:35Z | **Category:** Defacement | **Actor:** DimasHxR

Description: On May 20, 2026, a threat actor identified as DimasHxR defaced a page on the Italian website siola.it, specifically targeting a path within the media/customer address directory. The attacker operated without an affiliated team and the defacement was limited to a single non-homepage URL. No specific motive or server details were disclosed.

Target Context: Organization: *Siola* | Industry: *Unknown* | Country: *Italy*

Source URL: `https://zone-xsec.com/mirror/id/925116`

[17] Website Defacement of FloorSave by Threat Actor DimasHxR

Date: 2026-05-19T23:21:09Z | **Category:** Defacement | **Actor:** DimasHxR

Description: On May 20, 2026, threat actor DimasHxR defaced a media/customer directory page on floorsave.co.uk, a UK-based flooring retail website. The incident was a targeted, non-mass defacement affecting a subdirectory rather than the homepage. No team affiliation or stated motivation was identified for this attack.

Target Context: Organization: *FloorSave* | Industry: *Retail / Home Improvement* | Country: *United Kingdom*

Source URL: `https://zone-xsec.com/mirror/id/925115`

[18] Website Defacement of Stephans.de by DimasHxR

Date: 2026-05-19T23:15:09Z | **Category:** Defacement | **Actor:** DimasHxR

Description: On May 20, 2026, the website stephans.de was defaced by a threat actor operating under the alias DimasHxR. The attacker targeted a specific media/customer directory path on the site. The incident was a single, targeted defacement with no team affiliation reported and no declared motive.

Target Context: Organization: *Stephans* | Industry: *Unknown* | Country: *Germany*

Source URL: `https://zone-xsec.com/mirror/id/925112`

[19] Alleged Illegal Hacking Services Advertisement

Date: 2026-05-19T23:13:46Z | **Category:** Cyber Attack | **Actor:** CIPHERN

Description: User advertising various illegal hacking and account compromise services including Telegram, mobile phones, websites, iCloud, email, social media platforms (Snapchat, Reddit, LinkedIn), and IP cameras. Also offers stolen funds recovery services. Contact provided via Telegram handle @sureciphern__.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://t.me/c/2613583520/85237`

[20] Website Defacement of Torsbo Handels by DimasHxR

Date: 2026-05-19T23:12:14Z | **Category:** Defacement | **Actor:** DimasHxR

Description: On May 20, 2026, a threat actor operating under the alias DimasHxR defaced a page on torsbohandels.com, a Swedish retail or trading company website. The attacker targeted a non-homepage URL within the sites media directory, indicating a targeted single-page defacement rather than a mass or home page compromise. No team affiliation, stated motive, or server details were disclosed in connection with this incident.

Target Context: Organization: *Torsbo Handels* | Industry: *Retail / E-Commerce* | Country: *Sweden*

Source URL: `https://zone-xsec.com/mirror/id/925113`

[21] Alleged data leak of Karawang Regency Population and Civil Registration Office (Dukcapil) database

Date: 2026-05-19T23:10:24Z | **Category:** Data Leak | **Actor:** Mr. Hanz Xploit

Description: A threat actor operating under the alias Mr. Hanz Xploit claims to be distributing a database belonging to the Karawang Regency Population and Civil Registration Office (Dukcapil) free of charge. The database reportedly contains civil registration and population records. A sample was included in the post.

Target Context: Organization: *Dinas Kependudukan dan Pencatatan Sipil Kabupaten Karawang* | Industry: *Government* | Country: *Indonesia*

Source URL: `https://breached.st/threads/database-dukcapil-kabupaten-karawang.87404/unread`

[22] Alleged data breach of official government site of Georgia

Date: 2026-05-19T23:09:39Z | **Category:** Data Breach | **Actor:** 404Crew Cyber Team

Description: A threat actor operating under the name 404Crew Cyber Team posted a thread on a breach forum referencing an official government site of Georgia. No post content was available to confirm specific details regarding the nature or extent of the alleged breach.

Target Context: Organization: *Unknown* | Industry: *Government* | Country: *Georgia*

Source URL: `https://breached.st/threads/official-government-site-of-georgia.87405/unread`

[23] Alleged breach of Dukcapil database - Karawang Regency, Indonesia

Date: 2026-05-19T23:08:57Z | **Category:** Data Breach | **Actor:** mr-hanz-xploit

Description: A threat actor operating under the handle mr-hanz-xploit has posted on Breachforums regarding a breach of the Dukcapil (Direktorat Jenderal Kependudukan dan Pencatatan Sipil) database for Karawang Regency. Dukcapil is Indonesias civil registry system containing sensitive population data. The breach details are being shared on the Breachforums platform.

Target Context: Organization: *Dukcapil Karawang Regency* | Industry: *Government - Civil Registry* | Country: *Indonesia*

Source URL: `https://t.me/DeepCoreNetwork/211`

[24] Combo List: 8.4K Private Mix Credentials Shared on Forum

Date: 2026-05-19T23:03:46Z | **Category:** Combo List | **Actor:** Dataseller

Description: A threat actor shared a combo list of approximately 8,400 credentials on a forum. The content is hidden behind a registration/login wall. The poster also advertises private cloud services via direct message.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://patched.to/Thread-8-4k-private-mix-by-blackcloversuppprt`

[25] Sale of 22K Mixed Mail Access HQ Combo List

Date: 2026-05-19T23:03:30Z | **Category:** Combo List | **Actor:** Vonmoon

Description: A threat actor is sharing a combo list of approximately 22,000 mixed mail access credentials marketed as high quality. The content is hidden behind a registration or login wall on the forum.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://patched.to/Thread-22k-mixed-mail-access-hq-combolist`

[26] Alleged data breach of ANDE (Paraguay National Electricity Administration) - 1.65M records

Date: 2026-05-19T23:01:13Z | **Category:** Data Breach | **Actor:** shinycorpsh

Description: Threat actor claiming to have breached ande.gov.py (Paraguays national electricity utility) and offering 1,650,000 records for sale at $2,000 (negotiable). Exposed data includes NIS numbers, account holder names, ID numbers, occupations, emails, phone numbers, addresses, neighborhoods, cities, and monthly electricity consumption data (kWh). Contact via Telegram @shinycorpsh with supporter @node6240.

Target Context: Organization: *ANDE (Administración Nacional de Electricidad)* | Industry: *Energy/Utilities* | Country: *Paraguay*

Source URL: `https://t.me/c/3500620464/8237`

[27] Alleged sale of email credentials, cookies, and combolist access

Date: 2026-05-19T22:54:30Z | **Category:** Combo List | **Actor:** Dataxlogs

Description: Threat actor advertising sale of stolen credentials including email:password combinations, Gmail cookies, LinkedIn cookies and passwords. Additional post offers mail access and combo lists/configs/scripts/tools across multiple countries (FR, BE, AU, CA, UK, US, NL, PL, DE, JP) with contact via Telegram for purchase requests.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://t.me/c/2613583520/85219`

[28] Alleged data leak of Bank of India customer records

Date: 2026-05-19T22:54:19Z | **Category:** Data Leak | **Actor:** Mr. Hanz Xploit

Description: A threat actor is distributing a database allegedly belonging to Bank of India for free. The post claims the dataset contains customer data affecting approximately 7 million individuals. A sample is included in the post.

Target Context: Organization: *Bank of India* | Industry: *Finance* | Country: *India*

Source URL: `https://breached.st/threads/7-million-indian-bank-customer-data-exposed.87403/unread`

[29] Alleged exposure of 7 million Indian bank customer records

Date: 2026-05-19T22:53:43Z | **Category:** Data Breach | **Actor:** mr-hanz-xploit

Description: A Breachforums thread discusses the exposure of 7 million Indian bank customer data. The thread is attributed to user mr-hanz-xploit on Breachforums. Details indicate a significant breach affecting Indian banking sector customers.

Target Context: Organization: *Indian banking sector* | Industry: *Financial Services/Banking* | Country: *India*

Source URL: `https://t.me/DeepCoreNetwork/210`

[30] Sale of Canadian email/password combo list with 104K credentials

Date: 2026-05-19T22:45:55Z | **Category:** Combo List | **Actor:** zubicks

Description: A threat actor is distributing a combo list of approximately 104,000 email and password pairs purportedly associated with Canadian users. The list is hosted on Anonfilesnew and shared on BreachForums.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://breachforums.rs/Thread-Combolist-Canada-104K-Email-Pass`

[31] Money mule service offered for e-commerce fraud operations

Date: 2026-05-19T22:44:38Z | **Category:** Chatter | **Actor:** mamalenn666 🍼

Description: A forum user is advertising money mule services on a French-language darknet forum, offering to move funds via a Wise business account registered under an LLC in exchange for a percentage cut. The service is explicitly marketed toward non-shipping scammers and other e-commerce fraud actors operating on platforms such as Shopify.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion/post/21edc0941a7c29f244ae`

[32] Sale of USA Facebook email and password combo list

Date: 2026-05-19T22:44:21Z | **Category:** Combo List | **Actor:** zubicks

Description: A threat actor is distributing a combo list of USA-based Facebook email and password credentials via an anonymous file-sharing service. The post does not indicate record count or pricing. These credentials are likely sourced from prior breaches and formatted for credential stuffing.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *United States*

Source URL: `https://breachforums.rs/Thread-Combolist-USA-Facebook-Email-Pass`

[33] Free distribution of stolen Claude API keys with token credits

Date: 2026-05-19T22:43:53Z | **Category:** Data Leak | **Actor:** JVZU

Description: A threat actor is freely distributing what are claimed to be stolen Claude API keys with approximately 2 million tokens of credits, including access to Claude Opus 4.7 and other models. The keys were shared on a cracking forum with a requirement for likes and reputation boosts in exchange for access.

Target Context: Organization: *Anthropic* | Industry: *Technology* | Country: *United States*

Source URL: `https://cracked.st/Thread-%E2%AD%90-2-MILLION-TOKENS-CLAUDE-OPUS-4-7-AND-MORE-API-KEY-%E2%AD%90--2096564`

[34] Alleged sale of Hotmail combolists and stealer logs across multiple countries

Date: 2026-05-19T22:43:47Z | **Category:** Combo List | **Actor:** Wěilóng

Description: Threat actor Wěilóng is advertising the sale of private cloud Hotmail UHQ (ultra high quality) combolists and credential lists from multiple countries (DE, FR, IT, BR, UK, US, JP, PL, RU, ES, NL, MX, CA, SG). Also offering Gmail cookies, LinkedIn cookies with passwords, and other platform credentials. Seller claims ability to verify keywords and targets serious buyers only.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://t.me/c/2613583520/85218`

[35] Combo List: Private Full Access Europa Mix (20,118 credentials)

Date: 2026-05-19T22:43:23Z | **Category:** Combo List | **Actor:** AiCombo

Description: A combo list containing 20,118 full access (FA) email:password credentials targeting European accounts has been shared on a cracking forum. The list is described as private and formatted as a mixed Europa combo. No specific victim organization or service is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-20-118-Private-FA-Europa-Mix-Combo`

[36] Germany domain combo list with 988,693 lines

Date: 2026-05-19T22:43:05Z | **Category:** Combo List | **Actor:** HqComboSpace

Description: A threat actor is distributing a combo list of approximately 988,693 email:password lines targeting German (.de) domain accounts. The list is marketed as sourced from good leaks and is likely intended for credential stuffing.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-988-693-Lines-%E2%9C%85-Good-Leaks-De-Germany-Domain-Combolist`

[37] Sale of private email:password combo list by BatmanMail

Date: 2026-05-19T22:42:47Z | **Category:** Combo List | **Actor:** BatmanMail

Description: A threat actor operating as BatmanMail is distributing a private mix combo list claimed to contain unique and valid email:password credentials. The post promotes the actors Telegram channel as a source for private, non-public credential lists. No specific victim organization or record count is mentioned.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-Private-Mix-BatmanMail-5`

[38] Alleged sale of infostealer logs and mail access credentials

Date: 2026-05-19T22:32:33Z | **Category:** Logs | **Actor:** Dataxlogs

Description: Threat actor operating under handle @Dataxlogs is offering mail access and infostealer logs for sale, including credentials, configs, scripts, tools, and combo lists from multiple countries (France, Belgium, Australia, Canada, UK, US, Netherlands, Poland, Germany, Japan). Seller is actively soliciting customers via Telegram.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://t.me/c/2613583520/85209`

[39] Alleged leak of 2 million Claude API tokens

Date: 2026-05-19T22:31:48Z | **Category:** Data Leak | **Actor:** JVZU

Description: A threat actor claims to be leaking 2 million Claude API tokens on a cybercrime forum. The content is hidden behind a registration/login wall. If valid, these tokens could be used for unauthorized access to Anthropics Claude AI API.

Target Context: Organization: *Anthropic* | Industry: *Technology* | Country: *Unknown*

Source URL: `https://patched.to/Thread-%E2%9D%A4%EF%B8%8F-claude-api-tokens-2-million-ai-tokies-%E2%9D%A4%EF%B8%8F-304211`

[40] Sale of 35K Hotmail combo list

Date: 2026-05-19T22:31:17Z | **Category:** Combo List | **Actor:** bygbb

Description: A forum user is offering a private Hotmail combo list containing approximately 35,000 credential pairs. The content is hidden behind a login/registration wall. No additional details about the data source or format are available.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://patched.to/Thread-35k-hotmail-private-combolist`

[41] Sale of UHQ combo list

Date: 2026-05-19T22:23:31Z | **Category:** Combo List | **Actor:** CicadaHunter

Description: A forum post by CicadaHunter on Cracked.st advertises a UHQ combo list containing 30 entries. No additional details or content were available in the post.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-UHQ-30x`

[42] Sale of European mixed combo list with 23,847 credentials

Date: 2026-05-19T22:19:20Z | **Category:** Combo List | **Actor:** AiCombo

Description: A threat actor on a cracking forum has shared or is offering a mixed European combo list containing approximately 23,847 email:password pairs. The list is described as private and full access (FA). No specific victim organization or breach source is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-23-847-Private-FA-Europa-Mixed-Combolist`

[43] Combo List targeting Hotmail, Yahoo, and Orange users

Date: 2026-05-19T22:18:01Z | **Category:** Combo List | **Actor:** AiCombo

Description: A combo list containing approximately 192,346 email:password pairs targeting Hotmail.fr, Yahoo, and Orange accounts has been shared on a cracking forum. The credentials are marketed as fresh leaks suitable for credential stuffing. No specific breach source or victim organization is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-192-346-hotmail-fr-yahoo-orange-Fresh-Leaks-Combolist`

[44] China combo list with 17,000 credentials

Date: 2026-05-19T22:17:30Z | **Category:** Combo List | **Actor:** BygBB

Description: A threat actor shared a combo list reportedly containing 17,000 email and password pairs associated with Chinese accounts. The post was made on a public cracking forum. No specific victim organization or breach source was identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-17k-China-Private-Combolist`

[45] Australia combo list with 27,000 credentials

Date: 2026-05-19T22:16:59Z | **Category:** Combo List | **Actor:** BygBB

Description: A combo list of approximately 27,000 Australian email and password pairs has been shared on a cracking forum. The credentials are described as private and may be used for credential stuffing attacks against various online services.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Australia*

Source URL: `https://cracked.st/Thread-Email-Pass-27k-Australia-Private-Combolist`

[46] Alleged hacking services offering Telegram, email, iCloud, and website compromise

Date: 2026-05-19T22:16:40Z | **Category:** Cyber Attack | **Actor:** sureciphern

Description: User @sureciphern advertising illegal hacking services including Telegram account hacking, mobile phone hacking, website hacking, iCloud compromise, email hacking, IP camera hacking, Snapchat hacking, LinkedIn account rental/hacking, Reddit account rental/hacking, and stolen funds recovery services. Contact via Telegram for engagement.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://t.me/c/2613583520/85207`

[47] Sale of GMX combo list with 16,000 credentials

Date: 2026-05-19T22:16:18Z | **Category:** Combo List | **Actor:** BygBB

Description: A forum user is offering a private combo list of 16,000 GMX email credentials. The list appears to contain email and password pairs. No further details are available from the post content.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-16k-GMX-Private-Combolist`

[48] RDP hosting service advertised on cybercrime forum

Date: 2026-05-19T22:15:06Z | **Category:** Services | **Actor:** Timi999

Description: A forum user operating under the alias Timi999 is advertising a commercial RDP hosting service called CELERHOST, with plans starting at 9.99€. The service is promoted as secure and includes a 10% discount code. Support and custom plans are available via Telegram.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://patched.to/Thread-nova-%E2%9D%84%EF%B8%8F-celerhost-1-rdp-provider-starting-at-9-99%E2%82%AC-100-secure-start10-10-off`

[49] Sale of Russian combo list with 13,000 credentials

Date: 2026-05-19T22:13:45Z | **Category:** Combo List | **Actor:** bygbb

Description: A forum member is sharing a private combo list purportedly containing 13,000 credential pairs associated with Russian accounts. The content is hidden behind a registration or login requirement. No specific victim organization or service is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://patched.to/Thread-13k-russia-private-combolist`

[50] Sale of Japan combo list with 37,000 credentials

Date: 2026-05-19T22:13:12Z | **Category:** Combo List | **Actor:** bygbb

Description: A forum user is distributing a combo list of approximately 37,000 credentials reportedly associated with Japanese accounts. The content is hidden behind a registration/login wall. No specific victim organization or breach source is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://patched.to/Thread-37k-japan-private-combolist`

[51] Sale of Italian combo list with 30,000 credentials

Date: 2026-05-19T22:12:40Z | **Category:** Combo List | **Actor:** bygbb

Description: A threat actor is sharing a private combo list of approximately 30,000 Italian credentials on a cybercrime forum. The content is gated behind registration or login. No specific victim organization or service is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Italy*

Source URL: `https://patched.to/Thread-30k-italy-private-combolist`

[52] Sale of Netherlands combo list with 18,000 credentials

Date: 2026-05-19T22:12:08Z | **Category:** Combo List | **Actor:** bygbb

Description: A forum user is sharing a private combo list purportedly containing 18,000 credentials associated with Netherlands-based accounts. The content is hidden behind a registration or login wall. No specific victim organization or service is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://patched.to/Thread-18k-netherlands-private-combolist`

[53] Alleged illegal hacking services and stolen database sales advertisement

Date: 2026-05-19T22:12:02Z | **Category:** Cyber Attack | **Actor:** CIPHERN

Description: User CIPHERN advertising illegal services including Telegram hacking, mobile phone hacking, website hacking, iCloud hacking, email hacking, and account compromises (Snapchat, LinkedIn, Reddit). Contact handle @sureciphern__. Additionally, user Num advertising fresh stolen databases from multiple countries (UK, DE, JP, NL, BR, PL, ES, US, IT) with keyword searching capabilities for e-commerce platforms (eBay, Amazon, Walmart, Alibaba, Mercari, etc.) and webmail access.

Target Context: Organization: *Unknown* | Industry: *Multiple (technology, e-commerce, telecommunications)* | Country: *Unknown*

Source URL: `https://t.me/c/2613583520/85188`

[54] Combo list of 191K Mexico email:password credentials

Date: 2026-05-19T22:06:51Z | **Category:** Combo List | **Actor:** thejackal101

Description: A threat actor is distributing a combo list of approximately 191,000 email:password credential pairs reportedly associated with Mexico. The credentials are marketed as fresh and high quality, shared via a hidden content link on the forum and promoted through a Telegram channel.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://demonforums.net/Thread-Email-Pass-%E2%9C%AA-191-K-Combo-%E2%9C%AA-Mexico-%E2%9C%AA-19-MAY-2026-%E2%9C%AA`

[55] Combo List targeting Latvia with 85K+ credentials

Date: 2026-05-19T22:06:21Z | **Category:** Combo List | **Actor:** thejackal101

Description: A threat actor shared a combo list of approximately 85,000+ email:password pairs associated with Latvia, marketed as fresh and high quality. The list is available to registered forum members via hidden content. The actor also promotes a Telegram channel for additional credential listings.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Latvia*

Source URL: `https://demonforums.net/Thread-Email-Pass-%E2%9C%AA-85-K-Combo-%E2%9C%AA-Latvia-%E2%9C%AA-19-MAY-2026-%E2%9C%AA`

[56] Malaysia email:password combo list shared on forum

Date: 2026-05-19T22:05:49Z | **Category:** Combo List | **Actor:** thejackal101

Description: A threat actor shared a combo list of approximately 58,000 email:password pairs purportedly associated with Malaysian accounts, marketed as fresh and high quality. The credentials are available to registered forum members via hidden content. The post also references a Telegram channel for additional logs.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://demonforums.net/Thread-Email-Pass-%E2%9C%AA-58-K-Combo-%E2%9C%AA-Malaysia-%E2%9C%AA-19-MAY-2026-%E2%9C%AA`

[57] Combo list targeting Montenegro distributed on forum

Date: 2026-05-19T22:05:19Z | **Category:** Combo List | **Actor:** thejackal101

Description: A threat actor shared a combo list of approximately 49,000 email:password pairs purportedly associated with Montenegro, marketed as fresh and high quality. The credentials are available to registered forum members and the actor promotes additional content via a Telegram channel.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Montenegro*

Source URL: `https://demonforums.net/Thread-Email-Pass-%E2%9C%AA-49-K-Combo-%E2%9C%AA-Montenegro-%E2%9C%AA-19-MAY-2026-%E2%9C%AA`

[58] Combo list targeting Kenya distributed on cybercrime forum

Date: 2026-05-19T22:04:46Z | **Category:** Combo List | **Actor:** thejackal101

Description: A threat actor is distributing a combo list of approximately 19,000 email:password credential pairs purportedly associated with Kenyan users, dated May 19, 2026. The credentials are marketed as fresh and high quality. The post references a Telegram channel for additional credential content.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://demonforums.net/Thread-Email-Pass-%E2%9C%AA-19-K-Combo-%E2%9C%AA-Kenya-%E2%9C%AA-19-MAY-2026-%E2%9C%AA`

[59] Combo List targeting Lithuania with 21K email:password credentials

Date: 2026-05-19T22:04:08Z | **Category:** Combo List | **Actor:** thejackal101

Description: A threat actor shared a combo list of approximately 21,000 email:password credential pairs associated with Lithuanian accounts, marketed as fresh and high quality. The credentials were posted on a cybercrime forum with access restricted to registered users. The actor also promoted a Telegram channel for additional credential content.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://demonforums.net/Thread-Email-Pass-%E2%9C%AA-21-K-Combo-%E2%9C%AA-Lithuania-%E2%9C%AA-19-MAY-2026-%E2%9C%AA`

[60] Combo list targeting Micronesia distributed on forum

Date: 2026-05-19T22:03:33Z | **Category:** Combo List | **Actor:** thejackal101

Description: A threat actor shared a combo list of approximately 13,000 email:password pairs purportedly associated with Micronesia, dated May 19, 2026. The credentials are marketed as fresh and high quality. The post directs users to a Telegram channel for additional logs.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://demonforums.net/Thread-Email-Pass-%E2%9C%AA-13-K-Combo-%E2%9C%AA-Micronesia-%E2%9C%AA-19-MAY-2026-%E2%9C%AA`

[61] Sale of alleged data breach of Argentinas Mendoza Judicial Intranet (jus.mendoza.gov.ar)

Date: 2026-05-19T22:01:17Z | **Category:** Data Breach | **Actor:** Databasehooligan

Description: A threat actor is offering for sale an alleged dataset of approximately 478,000 records originating from the Mendoza provincial judiciary intranet in Argentina. The dataset is structured across three sections — Contacts, Legal Case Participants, and Communication Logs — containing national IDs, personal and work emails, phone numbers, home addresses, job titles, case participation details, and communication records. The seller is asking $1,200 and has provided sample download links.

Target Context: Organization: *Poder Judicial de Mendoza* | Industry: *Government* | Country: *Argentina*

Source URL: `https://breached.st/threads/478k-argentina-https-intranet-jus-mendoza-gov-ar-legal-personnel-records-including-contacts-ids-emails-job-titles.87401/unread`

[62] Alleged data breach of MiClub Australia — member contacts, event bookings, and payment records

Date: 2026-05-19T22:00:46Z | **Category:** Data Breach | **Actor:** Databasehooligan

Description: A threat actor is offering for sale an alleged database from miclub.com.au, an Australian golf club management platform, containing approximately 485,000 records. The dataset spans three sections: member personal and contact details (including date of birth, address, and GolfLink ID), event booking records, and membership payment transactions including billing addresses and financial metadata. The data is described as fresh and organized across interconnected tables.

Target Context: Organization: *MiClub* | Industry: *Sports & Recreation* | Country: *Australia*

Source URL: `https://breached.st/threads/485k-australia-https-www-miclub-com-au-member-contacts-and-subscription-details-database.87402/unread`

[63] Alleged sale of infostealer logs and mail access across multiple countries

Date: 2026-05-19T21:50:50Z | **Category:** Logs | **Actor:** DataxLogs

Description: Threat actor operating as @DataxLogs advertising stolen mail access and infostealer materials (configs, scripts, tools, combo lists, hits) for victims in France, Belgium, Australia, Canada, UK, US, Netherlands, Poland, Germany, and Japan. Contact via Telegram for purchases.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://t.me/c/2613583520/85183`

[64] Sale of European mixed combo list with 55,004 credentials

Date: 2026-05-19T21:36:22Z | **Category:** Combo List | **Actor:** AiCombo

Description: A threat actor shared a mixed European email:password combo list containing approximately 55,004 credential pairs on a cracking forum. The list is described as private and full access (FA), suggesting credentials may not have been widely circulated. No specific victim organization or breach source is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-55-004-Private-FA-Europa-Mixed-Combolist`

[65] Free combo list targeting .gov domains distributed on cracking forum

Date: 2026-05-19T21:36:03Z | **Category:** Combo List | **Actor:** RogenPlay

Description: A threat actor distributed a combo list of approximately 2.3 million credentials associated with .gov domains on a cracking forum. The list is described as freshly checked and AntiPublic-checked, suggesting it has been filtered for previously unseen or valid credentials. The post is sponsored by RogenCloud and includes a download link.

Target Context: Organization: *Unknown* | Industry: *Government* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-%E2%9C%85-%E2%9C%85-%E2%9C%85-%E2%9C%A8-2-3M-gov-Combolist-1-%E2%9C%A8-Freshly-Checked-AntiPublic-Checked-%E2%9C%A8-%E2%9C%85-%E2%9C%85-%E2%9C%85`

[66] Sale of mixed email credential combo list

Date: 2026-05-19T21:35:32Z | **Category:** Combo List | **Actor:** VALID_HITS99

Description: A forum user is sharing or selling a combo list of 1,359 mixed email and password credentials on a cracking forum. The post advertises the credentials as high quality with unspecified keyword targets. No specific victim organization is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-%E2%9D%84%E2%9D%84-1359x-HQ-MIXED-MAILS-%E2%9D%84%E2%9D%84-KEYWORD-TARGETS`

[67] Sale of private email access combo list with 55,004 credentials

Date: 2026-05-19T21:14:04Z | **Category:** Combo List | **Actor:** AiCombo

Description: A combo list advertised as containing 55,004 private email:password credentials with full access (FA) is being shared on a cracking forum. The post is attributed to user AiCombo and is categorized as a mail access combolist. No additional details about the source or targeted services are available.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-55-004-Private-FA-Mail-Access-Combolist--2096524`

[68] Sale of Brazzers account credentials

Date: 2026-05-19T21:13:29Z | **Category:** Combo List | **Actor:** ChaosEnvy

Description: A threat actor is offering Brazzers accounts for sale on a cracking forum, advertising instant access. The post does not specify the record count or method of compromise.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-%E2%AD%90-Best-Price-Brazzers-Accounts-%E2%80%93-Instant-Access%E2%AD%90`

[69] Alleged data leak of Lockstation.co.uk

Date: 2026-05-19T21:04:13Z | **Category:** Data Leak | **Actor:** [Mod] Tanaka

Description: A threat actor has freely leaked a CSV database allegedly belonging to Lockstation.co.uk, a UK-based lock supplier. The dataset contains approximately 132,759 rows covering 65,000 users, including billing and delivery addresses, customer emails, order totals, and payment method details. The data is dated 2024.

Target Context: Organization: *Lockstation* | Industry: *Retail* | Country: *United Kingdom*

Source URL: `https://spear.cx/Thread-Database-Lockstation-co-uk-leak`

[70] Free combo list of 6,750 mixed email credentials

Date: 2026-05-19T20:51:35Z | **Category:** Combo List | **Actor:** VaultAdmin

Description: A threat actor has shared a combo list containing 6,750 mixed email credentials on a leak forum. The content is hidden behind a registration or login wall. No specific victim organization or breach source is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://leakforum.io/Thread-Leak-%E2%9C%85%E2%9A%A16750x-MIXMAIL%E2%9A%A1%E2%9C%85`

[71] Sale of credential combo list targeting Steam

Date: 2026-05-19T20:50:29Z | **Category:** Combo List | **Actor:** xHitCheap

Description: A forum user is sharing a credential combo list marketed as hits against Steam accounts. The actual content is hidden behind a login/registration wall, so specific record counts and data details are not available.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://patched.to/Thread-hit-steam`

[72] Free Outlook and Hotmail combo list with 2,557 lines

Date: 2026-05-19T20:50:00Z | **Category:** Combo List | **Actor:** cloudkaraoke

Description: A threat actor has shared a combo list of 2,557 credential pairs described as mixed logs targeting Outlook and Hotmail accounts. The content is hidden behind a registration or login requirement on the forum.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://patched.to/Thread-file-upload-2-557-lines-good-combo-mixed-logs-outlook-hotmail`

[73] Sale of corporate email:password combo list

Date: 2026-05-19T20:41:10Z | **Category:** Combo List | **Actor:** ShroudX

Description: A forum post on NulledBB advertises a corporate-targeted email:password combo list. No post content is available; details are limited to the thread title indicating corporate email credentials. No specific victim organization or record count is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://nulledbb.com/thread-CORPORATE-TARGET-HQ-EMAILPASS-COMBOLIST-txt`

[74] Japan HQ Email:Password Combo List

Date: 2026-05-19T20:40:30Z | **Category:** Combo List | **Actor:** ShroudX

Description: A threat actor shared a combo list advertised as high-quality Japan email:password credentials. The post was made on a cracking forum. No further details are available from the post content.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://nulledbb.com/thread-JAPAN-HQ-EMAILPASS-COMBOLIST-txt`

[75] Sale of mixed credential combo list with 27K records

Date: 2026-05-19T20:40:15Z | **Category:** Combo List | **Actor:** COYYT

Description: A threat actor shared a download link containing approximately 27,000 mixed email:password credentials. The post offers the combo list as valid access, marketed for credential stuffing use.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://demonforums.net/Thread-Email-Pass-27K-MIXED-VALID-ACCESS`

[76] Sale of Outlook.com email:password combo list

Date: 2026-05-19T20:39:55Z | **Category:** Combo List | **Actor:** ShroudX

Description: A thread on NulledBB advertises an Outlook.com email:password combo list. No post content is available to confirm record count, pricing, or origin of the credentials.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://nulledbb.com/thread-OUTLOOK-COM-HQ-EMAILPASS-COMBOLIST-txt`

[77] Poland HQ email:password combo list

Date: 2026-05-19T20:39:27Z | **Category:** Combo List | **Actor:** ShroudX

Description: A threat actor shared a combo list described as high-quality Polish email:password credentials. No further details about record count or source are available from the post content.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://nulledbb.com/thread-POLAND-HQ-EMAILPASS-COMBOLIST-txt`

[78] Free distribution of stealer logs mix

Date: 2026-05-19T20:39:23Z | **Category:** Logs | **Actor:** fatetraffic

Description: A threat actor known as fatetraffic has shared a free download of 1,500 mixed stealer logs dated May 19, 2026, via a file-sharing platform. The post includes a download link and password, suggesting the logs contain credentials and session data harvested by info-stealer malware.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-FATETRAFFIC-1500-MIX-19-05-2026-STEALER-LOGS`

[79] Combo List of 550K URL:Log:Pass Credentials

Date: 2026-05-19T20:39:11Z | **Category:** Combo List | **Actor:** Posts

Description: A combo list containing approximately 550,000 URL:username:password credential pairs was shared on a cracking forum. The post is dated 20 May and appears to offer the credentials as a free release. No specific victim organization or industry is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-%E2%AD%90550K-URL-LOG-PASS%E2%AD%9020-MAY`

[80] Sale of Yahoo.com email:password combo list

Date: 2026-05-19T20:39:06Z | **Category:** Combo List | **Actor:** ShroudX

Description: A forum user shared a Yahoo.com email:password combo list on a cracking forum. No post content is available; details on record count, price, or origin are unknown.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://nulledbb.com/thread-YAHOO-COM-HQ-EMAILPASS-COMBOLIST-txt`

[81] Sale of email:password combo list targeting Epic Games accounts

Date: 2026-05-19T20:38:30Z | **Category:** Combo List | **Actor:** ZEWS

Description: A threat actor is distributing a combo list of 30,000 email and password pairs marketed as fresh and suitable for credential stuffing against Epic Games accounts. The data appears to be sourced from previously leaked databases rather than a direct breach of Epic Games. The post was shared on a public cracking forum.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-%E2%AD%90-30-000-%E2%AD%90-MAILPASS-%E2%9A%A1UHQ-DATABASE-GOOD-FOR-EPIC-GAMES%E2%9A%A1-FRESH-DATA`

[82] Sale of combo list marketed for Reddit credential stuffing

Date: 2026-05-19T20:38:13Z | **Category:** Combo List | **Actor:** ZEWS

Description: A threat actor is distributing a mailpass combo list of approximately 40,000 email and password pairs, marketed as suitable for credential stuffing against Reddit. The credentials are described as fresh and of high quality (UHQ).

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-%E2%AD%90-40-000-%E2%AD%90-MAILPASS-%E2%9A%A1UHQ-DATABASE-GOOD-FOR-REDDIT%E2%9A%A1-FRESH-DATA`

[83] Combo List of 60,000 email:password credentials for X and Microsoft

Date: 2026-05-19T20:37:55Z | **Category:** Combo List | **Actor:** ZEWS

Description: A threat actor is distributing a combo list of approximately 60,000 email and password pairs marketed as UHQ and fresh, suitable for credential stuffing against X and Microsoft services. The post is categorized as a combo list and does not represent a breach of either named platform.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-%E2%AD%90-60-000-%E2%AD%90-MAILPASS-%E2%9A%A1UHQ-DATABASE-GOOD-FOR-X-AND-MICROSOFT%E2%9A%A1-FRESH-DATA`

[84] Combo List targeting Roblox

Date: 2026-05-19T20:37:37Z | **Category:** Combo List | **Actor:** ZEWS

Description: A threat actor is distributing a combo list of approximately 52,000 email:password pairs marketed as suitable for credential stuffing against Roblox. The credentials are advertised as fresh and high quality.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-%E2%AD%90-52-000-%E2%AD%90-MAILPASS-%E2%9A%A1UHQ-DATABASE-GOOD-FOR-ROBLOX-%E2%9A%A1-FRESH-DATA`

[85] Sale of HQ mixed mail access combo list

Date: 2026-05-19T20:28:51Z | **Category:** Combo List | **Actor:** liamgoat

Description: A forum user is sharing a combo list of 2,500 mixed mail access credentials. The content is gated behind registration or login. No specific victim organization or breach source is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://patched.to/Thread-2-5k-hq-mixed-mail-access-combolist-304171`

[86] OpSec inquiry regarding AI API reseller usage for malware development

Date: 2026-05-19T20:28:29Z | **Category:** Chatter | **Actor:** kznsma04 🍼

Description: A forum user on Dreads OpSec board is asking about operational security when using an OpenAI API reseller service (anonkey.st) for malware development within a Whonix virtualized environment. The post contains no specific victim, breach, or threat artifact — it is an OpSec question from a self-described malware developer. No actionable threat intelligence is present beyond the acknowledgment of malware development activity.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion/post/15c1cfef4a41286e0717`

[87] Combo list of 10,000 business/corporate email credentials

Date: 2026-05-19T20:27:50Z | **Category:** Combo List | **Actor:** SecureTrax

Description: A threat actor distributed a combo list of approximately 10,000 business and corporate email credentials on a public cracking forum. The data is described as previously shared in private groups 4–7 days before public release. No specific victim organization or sector is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-%E2%9D%97%EF%B8%8F10k-BUSINESS-CORP-MAIL-ACCESS-MIX%E2%9D%97%EF%B8%8F-18-05`

[88] Combo List of 10,721 credentials

Date: 2026-05-19T20:27:32Z | **Category:** Combo List | **Actor:** AiCombo

Description: A combo list of 10,721 email:password credentials, marketed as private and fresh, was shared on a cracking forum. The post is titled Private FA Good Line Fresh, suggesting the credentials may be targeted at full-access account verification.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-10-721-Private-FA-Good-Line-Fresh`

[89] Hotmail Combo List with 404K Lines

Date: 2026-05-19T20:27:16Z | **Category:** Combo List | **Actor:** HqComboSpace

Description: A threat actor is distributing a combo list of approximately 404,634 email:password lines targeting Hotmail.com accounts. The credentials are marketed as high quality. No specific breach victim is identified; this appears to be a credential stuffing list aggregated from multiple sources.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-404-634-Lines-%E2%9C%85-Hotmail-com-Combolist-HQ-LEaks`

[90] Alleged data leak of South Korea used car market database

Date: 2026-05-19T20:23:27Z | **Category:** Data Leak | **Actor:** Vyntra

Description: A threat actor leaked a sample of an alleged South Korean used car marketplace database containing approximately 28,000 structured records. The dataset includes customer full names, email addresses, phone numbers, addresses, government/dealer IDs, shop and employee records, and demographic data. The actor advertises additional premium databases via a Telegram channel.

Target Context: Organization: *Unknown* | Industry: *Retail* | Country: *South Korea*

Source URL: `https://breachforums.rs/Thread-DATABASE-South-Korea-Used-Car-Market-Database`

[91] Alleged leak of randomly generated identity data including financial and tracking information

Date: 2026-05-19T20:17:24Z | **Category:** Data Leak | **Actor:** popfizz

Description: A forum user is sharing hidden content purportedly containing randomly generated identity data including names, countries, phone numbers, financial details, online accounts, and tracking numbers. The content is gated behind a reply requirement. No specific victim organization or breach source is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://altenens.is/threads/your-randomly-generated-identity-name-country-number-finance-online-tracking-numbers.2942866/unread`

[92] Sale of combo list targeting crypto, casino, and PayPal services

Date: 2026-05-19T20:14:49Z | **Category:** Combo List | **Actor:** MetaCloud

Description: A threat actor is distributing a combo list of approximately 745,000 credentials advertised as suitable for credential stuffing against crypto, casino, and PayPal platforms. The post promotes a commercial combo cloud service offering private lines and high-quality data via Telegram. No specific breached organization is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://breached.st/threads/high-voltage745k-crypto-casino-paypalhigh-voltageprivate-base-good-on-any-targethigh-voltage.87397/unread`

[93] Sale of combo list targeting crypto, casino, and PayPal services

Date: 2026-05-19T20:14:17Z | **Category:** Combo List | **Actor:** MetaCloud

Description: A threat actor is distributing a combo list of approximately 773,000 credential lines advertised as targeting crypto, casino, and PayPal services. The credentials are marketed as fresh, unique, and sourced from dehashed private lines. The post promotes a Telegram-based combo cloud service offering similar content.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://breached.st/threads/773k-high-voltagecrypto-casino-paypalhigh-voltagehigh-quality-private-high-voltagedehashed-lineshigh-voltagefresh-and-uniquehigh-voltage.87398/unread`

[94] Sale of USA educational sector combo list with 685K lines

Date: 2026-05-19T20:13:46Z | **Category:** Combo List | **Actor:** MetaCloud

Description: A threat actor is distributing a combo list of approximately 685,000 lines purportedly sourced from US educational sector accounts, marketed as dehashed, fresh, and unique. The post promotes a Telegram-based combo cloud service offering private credential lines. No specific victim organization is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://breached.st/threads/685k-high-voltageusa-educationalhigh-voltagehigh-quality-private-high-voltagedehashed-lineshigh-voltagefresh-and-uniquehigh-voltage.87400/unread`

[95] Alleged sale of GitHub internal source code and private repositories

Date: 2026-05-19T20:12:51Z | **Category:** Data Breach | **Actor:** TeamPCP

Description: A threat actor operating under the alias TeamPCP is offering for sale alleged internal GitHub source code and private organization repositories, claiming approximately 4,000 private repos are included. The actor is requesting offers above $50,000, stating only one buyer will be accepted, and threatening to leak the data for free if no buyer is found. Samples are offered for verification of authenticity.

Target Context: Organization: *GitHub* | Industry: *Technology* | Country: *United States*

Source URL: `https://breached.st/threads/internal-github-source-code.87395/unread`

[96] Sale of CIBC Bank fullz on carding forum

Date: 2026-05-19T19:56:52Z | **Category:** Carding | **Actor:** CC-GuRu

Description: A threat actor on a dark web carding forum is advertising CIBC Bank fullz, described as fresh and working. The post is gated behind registration, limiting visibility into the full scope or pricing. Fullz typically include complete personal and financial account details usable for fraud.

Target Context: Organization: *CIBC Bank* | Industry: *Finance* | Country: *Canada*

Source URL: `https://darkpro.net/threads/cibc-bank-fullz-fresh-working-by-carding-forum.23194/`

[97] Sale of combo list targeting Walmart, Etsy, and Amazon

Date: 2026-05-19T19:55:06Z | **Category:** Combo List | **Actor:** MetaCloud

Description: A threat actor is offering a combo list of approximately 739,000 credential lines marketed as high quality and fresh, intended for credential stuffing against Walmart, Etsy, and Amazon. The post advertises the content as dehashed lines distributed via a Telegram channel.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://crackingx.com/threads/75819/`

[98] Alleged data breach of Coinbase with 1 million customer records

Date: 2026-05-19T19:52:54Z | **Category:** Data Breach | **Actor:** ⭐ RED✘ ⭐

Description: A threat actor is selling an alleged dataset of 1 million Coinbase customer records for $700. The data purportedly includes full names, email addresses, physical addresses, phone numbers, IP addresses, gender, and detailed financial transaction data including deposit and withdrawal totals and annual income. Sample records were provided as proof.

Target Context: Organization: *Coinbase* | Industry: *Finance* | Country: *United States*

Source URL: `https://darkpro.net/threads/1-million-coin-base-leaks-2026.23196/`

[99] Combo List of 50,329 credentials

Date: 2026-05-19T19:51:05Z | **Category:** Combo List | **Actor:** AiCombo

Description: A combo list of 50,329 email:password credentials marketed as private, fresh, and with good lines for full access (FA) accounts. The list was shared on a public cracking forum. No specific victim organization or service is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-50-329-Private-FA-Good-Line-Fresh`

[100] Combo list of 6,485 mixed mail access credentials for EU and Asia regions

Date: 2026-05-19T19:50:48Z | **Category:** Combo List | **Actor:** kccloud01

Description: A threat actor shared a combo list of 6,485 email:password credentials targeting EU and Asia regions. The list is made available as a free download on the forum.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-6-485-GOOD-COMBO-MIX-MAIL-ACCESS-EU-ASIA`

[101] Sale of gaming combo list targeting Xbox and PSN accounts

Date: 2026-05-19T19:50:31Z | **Category:** Combo List | **Actor:** MetaCloud3

Description: A threat actor is distributing a combo list of approximately 752,000 email:password credentials marketed as high quality and fresh, targeting Xbox and PlayStation Network gaming accounts. The post describes the lines as dehashed and unique. The named gaming platforms are credential-stuffing targets, not breach victims.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-%E3%80%8C-752K-%E3%80%8D%E2%9A%A1XBOX-PSN-GAMING%E2%9A%A1HIGH-QUALITY-PRIVATE-%E2%9A%A1DEHASHED-LINES%E2%9A%A1FRESH-AND-UNIQUE%E2%9A%A1`

[102] Combo list of 757K credentials targeting Twitter and Reddit

Date: 2026-05-19T19:50:09Z | **Category:** Combo List | **Actor:** MetaCloud3

Description: A threat actor is freely distributing a combo list of approximately 757,000 email:password credentials described as a private base suitable for use against any target, with Twitter and Reddit mentioned as intended targets. The post was shared on a public cracking forum by the user MetaCloud3.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-%E2%9A%A1757K-TWITTER-REDDIT%E2%9A%A1PRIVATE-BASE-GOOD-ON-ANY-TARGET%E2%9A%A1`

[103] Combo List: 3,396 Mixed Mail Access Credentials

Date: 2026-05-19T19:44:19Z | **Category:** Combo List | **Actor:** RyuuLord

Description: A user on a leak forum is sharing a combo list containing 3,396 mixed mail access credentials. The content is hidden behind a registration or login wall. No specific victim organization or breach source is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://leakforum.io/Thread-Leak-3396x-Mix-Mail-Access-Vault`

[104] 766K FedEx/UPS combo list freely shared on forum

Date: 2026-05-19T19:43:55Z | **Category:** Combo List | **Actor:** MetaCloud

Description: A threat actor operating as MetaCloud is distributing a combo list of approximately 766,000 credentials marketed as a private base suitable for use against any target, including FedEx and UPS services. The content is gated behind forum registration or login. No specific breach victim is identified; the named services are credential-stuffing targets, not the source of the breach.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://leakforum.io/Thread-Leak-%E2%9A%A1766K-FEDEX-UPS%E2%9A%A1PRIVATE-BASE-GOOD-ON-ANY-TARGET%E2%9A%A1`

[105] Sale of 753K mail access combo list

Date: 2026-05-19T19:41:23Z | **Category:** Combo List | **Actor:** MetaCloud

Description: A threat actor is distributing a combo list of approximately 753,000 mail access credentials, advertised as a private base suitable for use against any target. The post promotes a combo cloud service offering high-quality data via a Telegram channel.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://breached.st/threads/high-voltage753k-mail-accesshigh-voltageprivate-base-good-on-any-targethigh-voltage.87390/unread`

[106] Sale of Disney+ and Hulu credential combo list

Date: 2026-05-19T19:40:42Z | **Category:** Combo List | **Actor:** MetaCloud

Description: A threat actor is distributing a combo list of approximately 774,000 credential pairs marketed as high-quality, dehashed, fresh, and unique lines targeting Disney+ and Hulu accounts. The post promotes a Telegram-based combo cloud service offering private lines. Disney+ and Hulu are credential-stuffing targets, not the source of the breach.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://breached.st/threads/774k-high-voltagedisney-huluhigh-voltagehigh-quality-combohigh-voltagedehashed-lineshigh-voltagefresh-and-uniquehigh-voltage.87391/unread`

[107] Sale of personal data including SSN, drivers licenses, passports, and combo lists

Date: 2026-05-19T19:32:36Z | **Category:** Carding | **Actor:** jannat123

Description: A threat actor is offering for sale a range of sensitive personal data including SSNs, SINs, drivers licenses, passport scans, company databases (with EIN/LLC details), consumer info, phone lists, email databases, and credential combos. The post advertises multiple data types across multiple regions with no specific victim organization identified. Contact is directed to a Telegram account.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://xforums.st/threads/drivers-license-ssn-passports-combo-emails-databases-llc-ein-ltd.615510/`

[108] Free distribution of ULP combo list with 3.85 million lines

Date: 2026-05-19T19:31:16Z | **Category:** Combo List | **Actor:** ChaosEnvy

Description: A threat actor operating under the alias TurcoLeaksx has leaked a URL:Login:Password (ULP) combo list containing approximately 3.85 million lines. The dataset is described as high quality and has been made available for free on the forum. No specific victim organization or targeted service is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Other-%E2%AD%90ULP-URL-LOGIN-PASS-PRIVATE-3-85M-LINES%E2%AD%90HQ%E2%AD%90LEAKED%E2%AD%90-TurcoLeaksx%E2%AD%90`

[109] Combo List with 27.86 million URL:Log:Pass credentials

Date: 2026-05-19T19:30:56Z | **Category:** Combo List | **Actor:** deeped

Description: A threat actor is distributing a URL:LOG:PASS combo list containing approximately 27.86 million credential pairs, marketed as UHQ (ultra-high quality). No specific victim organization or service is identified in the post.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-%E2%AD%90%EF%B8%8FURL-LOG-PASS-27-86-M-UHQ-%E2%AD%90%EF%B8%8F`

[110] Sale of 170K UHQ mixed mail combo list

Date: 2026-05-19T19:30:19Z | **Category:** Combo List | **Actor:** Vows

Description: A threat actor is sharing a mixed mail combo list containing approximately 170,000 credentials, marketed as fresh and high quality. The post is sponsored by slateaio.com, suggesting use with credential-stuffing tools.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-170K-UHQ-MIXED-MAIL-COMBO-FRESH`

[111] Sale of combo list with 3.85 million credentials

Date: 2026-05-19T19:30:04Z | **Category:** Combo List | **Actor:** XELA

Description: A threat actor is distributing a combo list containing approximately 3.85 million URL:login:password (ULP) credentials. The content is gated behind registration or login on the forum. No specific victim organization is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://patched.to/Thread-%E2%AD%90u-l-p-3-85m-private-turcoleaksx%E2%AD%90`

[112] Sale of UHQ Gmail combo list with 65,000 credentials

Date: 2026-05-19T19:29:58Z | **Category:** Combo List | **Actor:** Vows

Description: A threat actor is sharing a combo list marketed as 65,000 UHQ Gmail credentials described as fresh. The post is sponsored by a third-party AIO service. The named service is a credential-stuffing target, not the breach victim.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-65K-UHQ-GMAIL-COMBO-FRESH`

[113] Sale of European mix combo list with 11,013 credentials

Date: 2026-05-19T19:29:39Z | **Category:** Combo List | **Actor:** AiCombo

Description: A combo list containing approximately 11,013 semi-valid email:password credential pairs of European origin was shared on a cracking forum. The list is described as a mixed European combo, likely intended for credential stuffing. No specific victim organization is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-11-013-Semi-Valide-FA-Europa-Mix-Combo`

[114] Sale of mixed email account credentials

Date: 2026-05-19T19:29:28Z | **Category:** Combo List | **Actor:** GoldMailAccs

Description: A threat actor is offering 688 allegedly valid mixed email account credentials. The content is hidden behind a registration or login requirement on the forum. No specific victim organization or breach source is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://patched.to/Thread-688-full-valid-mix-mail-access`

[115] Combo List — 2,076 Hotmail credentials

Date: 2026-05-19T19:29:24Z | **Category:** Combo List | **Actor:** RyuuLord

Description: A forum user is distributing a combo list containing 2,076 Hotmail credentials. The content is hidden behind a registration or login wall. Hotmail is the credential-stuffing target, not the breach victim.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://leakforum.io/Thread-Leak-2076x-Hotmail-Access-Vault`

[116] Combo List: Hotmail credentials

Date: 2026-05-19T19:29:13Z | **Category:** Combo List | **Actor:** RyuuMaster

Description: A combo list containing 2,076 Hotmail credentials was shared on a cracking forum. The post is categorized based on the thread title, as no additional content was available. These credentials are likely intended for credential stuffing or account takeover activity.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-2076x-Hotmail-Access-Vault`

[117] Combo List: Hotmail credential list with 151 alleged valid accounts

Date: 2026-05-19T19:29:06Z | **Category:** Combo List | **Actor:** GoldMailAccs

Description: A threat actor is distributing a combo list of 151 alleged valid Hotmail email account credentials. The content is hidden behind a registration or login wall on the forum. No specific breach victim is identified; the named service is a credential-stuffing target.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://patched.to/Thread-151-full-valid-hotmail-mail-access`

[118] Sale of Hotmail combo list with 151 valid accounts

Date: 2026-05-19T19:28:54Z | **Category:** Combo List | **Actor:** GoldMailAccs

Description: A threat actor is offering a combo list of 151 claimed valid Hotmail email account credentials. The post is categorized under combolists and marketed as fully valid mail access. No further details are available from the post content.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-151-FULL-VALID-HOTMAIL-MAIL-ACCESS`

[119] Sale of Hotmail credential combo list with 237 valid accounts

Date: 2026-05-19T19:28:50Z | **Category:** Combo List | **Actor:** GoldMailAccs

Description: A forum user is offering 237 allegedly valid Hotmail email account credentials. The content is hidden behind a registration or login wall. These credentials are marketed as fully valid mail access.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://patched.to/Thread-237-full-valid-hotmail-mail-access`

[120] Combo list distribution: Verity Vault Mix Mail Drop

Date: 2026-05-19T19:28:30Z | **Category:** Combo List | **Actor:** VerityVault

Description: A threat actor on a cybercrime forum is distributing a combo list containing 4,754 email and password combinations marketed as a mixed mail drop. The content is hidden behind a login/registration wall, limiting visibility into the full dataset.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://patched.to/Thread-file-upload-%E2%9A%A1%EF%B8%8F-4754x-verity-vault-mix-mail-drop-%E2%9A%A1%EF%B8%8F`

[121] Sale of 20K corporate-targeted combo list

Date: 2026-05-19T19:28:01Z | **Category:** Combo List | **Actor:** CELESTIALHQ

Description: A threat actor operating under the handle CELESTIALHQ is distributing a combo list of approximately 20,000 email:password pairs marketed as corporate-targeted. The credentials are offered freely to registered forum members, with personal purchase options also available. The post claims hits are assured, suggesting the list has been tested against corporate services.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://patched.to/Thread-legendary-%E2%9C%85email-pass%E2%9C%85-%E2%AD%9020k-corp-targeted-combos%E2%AD%90-%E2%9C%85hits-assured%E2%9C%85-%E2%9A%A1drop-by-celestial%E2%9A%A1-304153`

[122] Sale of fresh URL:login:password combo list

Date: 2026-05-19T19:27:40Z | **Category:** Combo List | **Actor:** ZAMPARA

Description: A forum user is offering a private URL:login:password combo list marketed as fresh. The actual content is hidden behind a registration or login wall, so no further details are available.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://patched.to/Thread-fresh-url-login-pass-private-304156`

[123] Sale of 264 valid mixed email account credentials

Date: 2026-05-19T19:27:25Z | **Category:** Combo List | **Actor:** GoldMailAccs

Description: A forum user is offering 264 allegedly valid mixed email account credentials behind a login/registration gate. The content is hidden and only accessible to registered forum members. No additional details about the email providers or data source are available.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://patched.to/Thread-264-full-valid-mix-mail-access`

[124] Mix Mail Access Combo List

Date: 2026-05-19T19:27:19Z | **Category:** Combo List | **Actor:** GhostlyGamer

Description: A threat actor is distributing a combo list of 109,565 allegedly valid mixed email access credentials. The content is gated behind a reply requirement on the forum.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://altenens.is/threads/109565-full-valid-mix-mail-access.2942836/unread`

[125] Sale of Hotmail credential combo list with 146 valid accounts

Date: 2026-05-19T19:26:50Z | **Category:** Combo List | **Actor:** GhostlyGamer

Description: A threat actor is distributing 146 alleged valid Hotmail email credentials on a forum, gated behind a reply requirement. The post advertises these as fully valid mail access credentials.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://altenens.is/threads/146-full-valid-hotmail-mail-access.2942837/unread`

[126] Sale of 820K USA combo list marketed for all targets

Date: 2026-05-19T19:26:15Z | **Category:** Combo List | **Actor:** GhostlyGamer

Description: A threat actor is distributing a combo list of 820,000 credentials purportedly sourced from US users, marketed as suitable for all targets. Access to the content is gated behind a reply requirement on the forum.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://altenens.is/threads/820k-usa-private-combo-good-for-all-targets.2942838/unread`

[127] Sale of 508K USA combo list marketed for all targets

Date: 2026-05-19T19:25:39Z | **Category:** Combo List | **Actor:** GhostlyGamer

Description: A threat actor on AE forum is distributing a combo list of 508,000 credentials purportedly sourced from US users, marketed as suitable for all targets. Access to the list requires a reply to the thread. No specific victim organization or service is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://altenens.is/threads/508k-usa-private-combo-good-for-all-targets.2942839/unread`

[128] Discussion on Laravel framework vulnerabilities used by darknet markets

Date: 2026-05-19T19:25:12Z | **Category:** Chatter | **Actor:** manski26 🍼

Description: A forum user on Dread is asking whether darknet markets such as DrugHub use the Laravel PHP framework and expressing concern about its known vulnerabilities. The post is speculative in nature and does not contain any specific exploit, access claim, or actionable threat intelligence.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion/post/202c07ad2b60b483402c`

[129] Sale of 500K Username:Login:Password Combo List

Date: 2026-05-19T19:25:05Z | **Category:** Combo List | **Actor:** GhostlyGamer

Description: A threat actor is distributing a combo list of 500,000 username:login:password credentials on a cybercrime forum. The post advertises hits assured, suggesting the credentials have been tested. Access to the list requires a reply to the thread.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://altenens.is/threads/check-mark-buttonu-l-pcheck-mark-button-star500k-full-private-u-l-pstar-check-mark-buttonhits-assuredcheck-mark-button.2942842/unread`

[130] Sale of UHQ Outlook combo list with 29K credentials

Date: 2026-05-19T19:24:30Z | **Category:** Combo List | **Actor:** GhostlyGamer

Description: A threat actor is distributing a combo list of approximately 29,000 Outlook credentials, marketed as high quality and fresh. The post requires a reply to access the hidden content. Outlook is the credential-stuffing target, not the breach victim.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://altenens.is/threads/29k-uhq-outlook-combo-fresh.2942843/unread`

[131] Sale of 100K email:password combo list

Date: 2026-05-19T19:23:53Z | **Category:** Combo List | **Actor:** GhostlyGamer

Description: A threat actor is distributing a combo list of 100,000 email:password credential pairs, marketed as anti-public and private. Access to the hidden content requires a reply to the thread.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://altenens.is/threads/check-mark-buttonemail-passcheck-mark-button-star100k-full-anti-public-private-mailstar.2942845/unread`

[132] Sale of 50K phone number and password combo list derived from stealer logs

Date: 2026-05-19T19:23:13Z | **Category:** Combo List | **Actor:** GhostlyGamer

Description: A threat actor is distributing a combo list of approximately 50,000 phone number and password pairs claimed to be derived from stealer logs. The post is gated behind a reply requirement and markets the credentials as high quality and private.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://altenens.is/threads/check-mark-buttonnum-passcheck-mark-button-star50k-private-hq-number-pass-from-logs-star.2942846/unread`

[133] Sale and distribution of mixed email combo lists via PandaCloud service

Date: 2026-05-19T19:22:42Z | **Category:** Combo List | **Actor:** Kokos2846q

Description: A threat actor is advertising a Telegram-based service called PandaCloud offering free and paid mixed email databases, claimed to be fresh and regularly updated. A public combo list download link is shared alongside offers for private, unused databases available for purchase.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://crackingx.com/threads/75811/`

[134] Sale of Yahoo combo list with 38K credentials

Date: 2026-05-19T19:22:35Z | **Category:** Combo List | **Actor:** GhostlyGamer

Description: A threat actor on AE is distributing a combo list marketed as 38K UHQ Yahoo credentials. The content is gated behind a reply requirement. Yahoo is the credential-stuffing target, not the breach victim.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://altenens.is/threads/38k-uhq-yahoo-combo-fresh.2942847/unread`

[135] Sale of 1,000 EDU-targeted email:password combo list

Date: 2026-05-19T19:22:12Z | **Category:** Combo List | **Actor:** GhostlyGamer

Description: A forum user is distributing a combo list of approximately 1,000 email:password credentials targeted at educational institutions. The post markets the credentials as verified hits. Content is gated behind a reply requirement.

Target Context: Organization: *Unknown* | Industry: *Education* | Country: *Unknown*

Source URL: `https://altenens.is/threads/check-mark-buttonemail-passcheck-mark-button-star1k-edu-targeted-combosstar-check-mark-buttonhits-assuredcheck-mark-button.2942849/unread`

[136] Sale of UHQ Hotmail combo list with 83K credentials

Date: 2026-05-19T19:21:41Z | **Category:** Combo List | **Actor:** GhostlyGamer

Description: A threat actor is distributing a combo list of approximately 83,000 Hotmail credentials, marketed as fresh and high quality. The list is gated behind a reply requirement and profile visit. Hotmail is the credential-stuffing target, not the breach victim.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://altenens.is/threads/83k-uhq-hotmail-combo-fresh.2942850/unread`

[137] Sale of personal data including SSNs, ID documents, and financial records

Date: 2026-05-19T19:21:32Z | **Category:** Carding | **Actor:** jannatmirza11

Description: A threat actor is offering for sale a variety of personal data including ID cards, SSNs, drivers licenses, passports, bank card data, consumer databases, and email/password combinations. The seller directs buyers to a Telegram channel for transactions. No specific victim organization or record count is disclosed.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://crackingx.com/threads/75812/`

[138] Alleged data leak of student attendance records from SMKN 1 Banjaragung

Date: 2026-05-19T19:16:43Z | **Category:** Data Leak | **Actor:** Mr.SonicX

Description: A threat actor operating under the alias Mr.SonicX, affiliated with Tegal Cyber Team, claims to have leaked the student attendance database from the SMKN 1 Banjaragung school application. The data is being distributed for free on a public forum.

Target Context: Organization: *SMKN 1 Banjaragung* | Industry: *Education* | Country: *Indonesia*

Source URL: `https://breached.st/threads/leaked-data-absensi-siswa-di-aplikasi-absensi-smkn1banjaragung.87389/unread`

[139] Combo List targeting Hotmail distributed via external file host

Date: 2026-05-19T19:03:25Z | **Category:** Combo List | **Actor:** Kokos2846q

Description: A threat actor is distributing a combo list of Hotmail credentials described as fresh and fully valid via an external file-sharing link. The post promotes a Telegram channel offering both public and private email databases on a recurring basis.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://crackingx.com/threads/75810/`

[140] OpSec Discussion on Anti-Forensic Data Storage Practices

Date: 2026-05-19T19:02:29Z | **Category:** Chatter | **Actor:** guest37285926 🍼

Description: A forum user on a darknet OpSec board is soliciting advice on anti-forensic measures, specifically around VeraCrypt hidden volumes on microSD cards and Tails OS for storing darknet market credentials. The discussion covers wear leveling implications for VeraCrypt containers and physical destruction/concealment tactics during law enforcement raids. No specific victim, breach, or threat content is present.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion/post/10484977fca110a0ee4a`

[141] Sale of private proxy or access cloud service on cracking forum

Date: 2026-05-19T19:02:12Z | **Category:** Services | **Actor:** s2lender

Description: A forum seller is advertising a subscription-based private cloud service, offering tiered membership plans ranging from $10 for 3-day access to $200 for lifetime access. The service claims to provide 4,000–12,000 daily fresh and untouched resources, likely proxies or combo lists for credential stuffing. No specific victim organization or target is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://crackingx.com/threads/75806/`

[142] Free distribution of mixed stealer logs and credentials

Date: 2026-05-19T18:59:20Z | **Category:** Logs | **Actor:** primedata

Description: A threat actor is freely distributing 1.10GB of mixed stealer logs, credentials, and ULP combos via a Telegram channel. The post offers a free sample and promotes the channel as an all-in-one source for logs, mail access, and checkers. No specific victim organization is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-1-10GB-Private-logs-Primedatanet`

[143] Free combo list sample distributed on cracking forum

Date: 2026-05-19T18:59:01Z | **Category:** Combo List | **Actor:** primedata

Description: A forum user shared a free sample of a mixed credential list (ULP/logs) on a cracking forum, directing users to a Telegram channel for additional content. The post advertises a mix of mail credentials, logs, and checkers with no specific victim organization identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Private-Ulp-From-Primedatanet-Good-For-all-2--2096434`

[144] Advertisement for Telegram channel offering mixed credential and log content

Date: 2026-05-19T18:58:43Z | **Category:** Services | **Actor:** primedata

Description: A forum user is advertising a Telegram channel purportedly offering a mix of mail lists, stealer logs, credential combos, and account checkers. The post includes a free sample incentive and directs users to the channel via a Telegram link. No specific victim organization or dataset is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-SEARCH-ENGINES-FOR-TELEGRAM-CHANNELS`

[145] Free combo list sample distributed via Telegram channel

Date: 2026-05-19T18:58:27Z | **Category:** Combo List | **Actor:** primedata

Description: A threat actor is distributing a free sample of mixed credential content described as mail/logs/ULP (URL:Login:Password) combos via a Telegram channel. The post advertises the channel primedatanet as an all-in-one source for combo lists, logs, and checkers. No specific victim organization or record count is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Private-Ulp-From-Primedatanet-Good-For-all-1`

[146] Free combo list sample distributed on cracking forum

Date: 2026-05-19T18:58:08Z | **Category:** Combo List | **Actor:** primedata

Description: A threat actor operating as primedata is distributing a free sample of a mixed ULP (URL:Login:Password) combo list via a Telegram channel. The post promotes a channel offering mixed mail, logs, ULPs, and checkers. No specific victim organization or record count is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Private-Ulp-From-Primedatanet-Good-For-all-3--2096435`

[147] Sale of 16K UHQ mixed email:password combo list

Date: 2026-05-19T18:57:41Z | **Category:** Combo List | **Actor:** Cloudredhat

Description: A forum user is sharing or selling a combo list of approximately 16,000 email:password pairs marketed as UHQ (ultra-high quality) and valid. No specific victim organization or targeted service was identified in the post.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-16K-UHQ-MIX-VALID`

[148] Sale of 16K UHQ mix combo list

Date: 2026-05-19T18:57:35Z | **Category:** Combo List | **Actor:** GhostlyGamer

Description: A threat actor is distributing a combo list of 16,000 credentials marketed as UHQ (ultra-high quality) mix. Access to the content requires a reply to the thread.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://altenens.is/threads/16k-uhq-mix-valid.2942821/unread`

[149] Sale of European email:password combo list

Date: 2026-05-19T18:57:24Z | **Category:** Combo List | **Actor:** AiCombo

Description: A combo list containing approximately 55,004 European email and password pairs is being distributed on a cracking forum. The list is described as a private full-access Europa mix combo. No specific breached organization is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-55-004-Private-FA-Europa-Mix-Combo`

[150] Alleged data leak of student attendance records from SMKN 1 Banjaragung

Date: 2026-05-19T18:57:07Z | **Category:** Data Leak | **Actor:** mr-sonicx

Description: Student attendance data (absensi siswa) from SMKN 1 Banjaragungs attendance application has been leaked and shared on Breached Forums. The breach exposes personally identifiable information of students at this Indonesian vocational school.

Target Context: Organization: *SMKN 1 Banjaragung* | Industry: *Education* | Country: *Indonesia*

Source URL: `https://t.me/c/3528849141/317`

[151] Free combo list sample targeting Germany

Date: 2026-05-19T18:57:01Z | **Category:** Combo List | **Actor:** primedata

Description: A threat actor shared a free sample of a combo list advertised as high-quality Germany-focused credentials. The post promotes a Telegram channel offering mixed mail lists, logs, ULP combos, and checkers. No specific victim organization or record count was disclosed.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Private-HQ-Germany-3`

[152] Free combo list of 2,534 mixed mail access credentials

Date: 2026-05-19T18:56:46Z | **Category:** Combo List | **Actor:** GhostlyGamer

Description: A threat actor is distributing a combo list of 2,534 claimed valid mixed email account credentials. The content is hidden behind a reply-gate on the forum. No specific victim organization or breach source is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://altenens.is/threads/2534-full-valid-mix-mail-access.2942832/unread`

[153] Free combo list mix mail sample shared on cracking forum

Date: 2026-05-19T18:56:39Z | **Category:** Combo List | **Actor:** primedata

Description: A threat actor shared a free sample combo list described as a high-quality mixed mail collection on a cracking forum. The post directs users to a Telegram channel advertising mix mails, logs, ULP, and checkers. No specific victim organization or record count was identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Private-Hq-Mix-Mails-5--2096444`

[154] Combo list of corporate email credentials containing 86,908 records

Date: 2026-05-19T18:56:21Z | **Category:** Combo List | **Actor:** AiCombo

Description: A combo list advertised as containing 86,908 corporate email and password pairs was shared on a cracking forum. The post is attributed to user AiCombo and targets corporate email accounts. No additional details about the source or format of the credentials are available.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-86-908-Combolist-Corps-Mails`

[155] Sale of mixed email access combo list with 2,534 entries

Date: 2026-05-19T18:56:03Z | **Category:** Combo List | **Actor:** GoldMailAccs

Description: A forum user is offering a combo list of 2,534 allegedly valid mixed email account credentials. The post is categorized as email access, suggesting the credentials may provide direct mailbox access. No additional details are available from the post content.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-2534-FULL-VALID-MIX-MAIL-ACCESS`

[156] Free combo list of 1,849 mixed mail access credentials

Date: 2026-05-19T18:55:56Z | **Category:** Combo List | **Actor:** GhostlyGamer

Description: A threat actor is distributing a combo list of 1,849 claimed valid mixed email account credentials. The post requires a reply to access the hidden content. No specific victim organization or targeted service is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://altenens.is/threads/1849-full-valid-mix-mail-access.2942833/unread`

[157] Sale of mixed mail access combo list with 7,036 entries

Date: 2026-05-19T18:55:47Z | **Category:** Combo List | **Actor:** GoldMailAccs

Description: A threat actor is offering a combo list of 7,036 reportedly valid mixed mail access credentials on a cracking forum. The post title suggests the credentials are fully validated. No additional details about origin or affected services are available.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-7036-FULL-VALID-MIX-MAIL-ACCESS`

[158] Sale of mixed email access combo list with 1,849 credentials

Date: 2026-05-19T18:55:30Z | **Category:** Combo List | **Actor:** GoldMailAccs

Description: A forum post on Cracked.st advertises 1,849 allegedly valid mixed email access credentials. No additional details are available regarding the source or composition of the credential list.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-1849-FULL-VALID-MIX-MAIL-ACCESS`

[159] Combo List of 7,999 mixed email account credentials

Date: 2026-05-19T18:55:12Z | **Category:** Combo List | **Actor:** GoldMailAccs

Description: A threat actor is sharing a combo list containing 7,999 allegedly valid mixed email account credentials. The post is categorized under combolists on a known cracking forum. No specific victim organization or breach source is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-7999-FULL-VALID-MIX-MAIL-ACCESS`

[160] Sale of Hotmail credential combo list

Date: 2026-05-19T18:54:51Z | **Category:** Combo List | **Actor:** GoldMailAccs

Description: A threat actor is sharing or selling 536 allegedly valid Hotmail email account credentials. The post is categorized as a combo list based on the thread title, as no additional post content is available.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-536-FULL-VALID-HOTMAIL-MAIL-ACCESS`

[161] Sale of Hotmail combo list with 345 valid credentials

Date: 2026-05-19T18:54:34Z | **Category:** Combo List | **Actor:** GoldMailAccs

Description: A forum user is offering 345 claimed valid Hotmail email account credentials. The post is categorized as a combo list based on thread title and forum context. No additional details are available in the post content.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-345-FULL-VALID-HOTMAIL-MAIL-ACCESS--2096452`

[162] Hotmail credential combo list shared on forum

Date: 2026-05-19T18:51:20Z | **Category:** Combo List | **Actor:** lundman01

Description: A threat actor is sharing Hotmail credential hits on a combolist forum, with free drops available and private cloud access offered for purchase via Telegram. The post contains hidden content requiring registration to view, suggesting additional credential data is gated behind login.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://patched.to/Thread-uhq-hotmail-hits-304126`

[163] Sale of Hotmail combo list with 2,500 credentials

Date: 2026-05-19T18:50:51Z | **Category:** Combo List | **Actor:** VerityVault

Description: A threat actor is distributing a combo list of 2,500 Hotmail credentials, marketed as a drop under the Verity Vault branding. The content is hidden behind a registration or login requirement on the forum.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://patched.to/Thread-file-upload-%E2%9A%A1%EF%B8%8F-2500x-verity-vault-hotmail-drop-%E2%9A%A1%EF%B8%8F`

[164] Alleged data leak of Universitas ITB (Institut Teknologi Bandung)

Date: 2026-05-19T18:48:03Z | **Category:** Data Leak | **Actor:** CatNatXploit

Description: A threat actor using the handle CatNatXploit posted what is alleged to be data from Institut Teknologi Bandung (ITB), an Indonesian university, on the Breached forum. The post content is empty or unavailable, so the nature, volume, and format of the alleged data cannot be confirmed.

Target Context: Organization: *Institut Teknologi Bandung* | Industry: *Education* | Country: *Indonesia*

Source URL: `https://breached.st/threads/data-universitas-itb.87388/unread`

[165] Sale of Mixed Target Yahoo Combolist with 880,552 Lines

Date: 2026-05-19T18:33:05Z | **Category:** Combo List | **Actor:** HqComboSpace

Description: A combo list of 880,552 email:password lines targeting Yahoo accounts has been shared on a cracking forum. The list is described as mixed target and is likely intended for credential stuffing against Yahoo services.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-880-552-Lines-%E2%9C%85-Mixed-Target-Yahoo-Combolist`

[166] Sale of alleged private European combo list with 52,312 credentials

Date: 2026-05-19T18:32:46Z | **Category:** Combo List | **Actor:** AiCombo

Description: A forum post on Cracked.st advertises a private European email:password combo list containing 52,312 credentials. The post is categorized as a combolist intended for credential stuffing. No specific victim organization or breach source is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-52-312-Private-FA-Combolist-Europa-Good`

[167] Sale of 160K France UHQ combo list

Date: 2026-05-19T18:28:41Z | **Category:** Combo List | **Actor:** VOLT

Description: A threat actor is distributing a combo list claimed to contain 160,000 French credentials, marketed as ultra-high quality (UHQ). The content is hidden behind a reply or account upgrade requirement on the forum.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://darkforums.su/showthread.php?tid=76985`

[168] Sale of Italian combo list with 230K credentials

Date: 2026-05-19T18:27:59Z | **Category:** Combo List | **Actor:** VOLT

Description: A threat actor is offering a combo list of approximately 230,000 credentials claimed to be high quality and Italian in origin. The content is hidden behind a reply or account upgrade requirement on the forum. No specific victim organization is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Italy*

Source URL: `https://darkforums.su/showthread.php?tid=76986`

[169] Alleged data breach of Argentinas Mendoza Judiciary (mev.jus.mendoza.gov.ar)

Date: 2026-05-19T18:25:27Z | **Category:** Data Breach | **Actor:** Databasehooligan

Description: A threat actor is offering for sale an alleged database originating from the Mendoza provincial judiciary portal in Argentina, containing approximately 756,000 records. The dataset is structured across three sections covering personal contact details (including national IDs, birth dates, addresses, and phone numbers), professional/employment information, and customer interaction logs. The data includes sensitive personally identifiable information such as national identity numbers, email address

Target Context: Organization: *Poder Judicial de Mendoza* | Industry: *Government* | Country: *Argentina*

Source URL: `https://breached.st/threads/756k-argentina-https-mev-jus-mendoza-gov-ar-personal-identities-and-contact-info-database-756k-argentina-https-mev-jus-mendoza-gov-ar-perso.87387/unread`

[170] Sale of HQ combo list mix (7,927 credentials)

Date: 2026-05-19T18:22:01Z | **Category:** Combo List | **Actor:** s2lender

Description: A threat actor is distributing a combo list of 7,927 mixed credentials marketed as high quality. The post advertises daily supply of 4,000–12,000 fresh credentials available to private members. Content is hidden behind registration or login.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://patched.to/Thread-file-upload-7927x-hq-mix-by-s2lender-txt`

[171] ✨🔥885 HOTMAIL VALID ACCESS |19.05.2026|

Date: 2026-05-19T18:21:46Z | **Category:** Alert | **Actor:** SupportHotmail

Description: New thread posted by SupportHotmail: ✨🔥885 HOTMAIL VALID ACCESS |19.05.2026|

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://patched.to/Thread-file-upload-%E2%9C%A8%F0%9F%94%A5885-hotmail-valid-access-19-05-2026`

[172] Combo List: 12K fresh mixed mail access credentials

Date: 2026-05-19T18:13:31Z | **Category:** Combo List | **Actor:** FetahosKR5

Description: A forum post advertises a combo list of 12,000 mixed email access credentials marketed as fresh. The post was shared on a public cracking forum with no additional details provided.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-12K-FRESH-MAIL-ACCESS-MIX`

[173] Combo List: Hotmail mail access credentials (x300)

Date: 2026-05-19T18:11:10Z | **Category:** Combo List | **Actor:** GhostlyGamer

Description: A forum user is distributing a combo list containing 300 Hotmail mail access credentials. The post is gated behind a reply requirement and directs users to the authors profile for additional posts of a similar nature.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://altenens.is/threads/starx300-hotmail-mail-access-star.2942802/unread`

[174] Sale of mixed mail access combo list with 16K credentials

Date: 2026-05-19T18:10:29Z | **Category:** Combo List | **Actor:** StrawHatBase

Description: A threat actor is sharing a combo list of approximately 16,000 mixed email access credentials on a criminal forum. The content is hidden behind a registration/login wall. No specific victim organization is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://demonforums.net/Thread-Email-Pass-16K-MIXED-MAIL-ACCESS-GOODS`

[175] Alleged data breach of OGEBC (Office de Gestion et dExploitation des Biens Culturels), Algeria

Date: 2026-05-19T18:06:24Z | **Category:** Data Breach | **Actor:** Databasehooligan

Description: A threat actor is selling an alleged dataset originating from ogebc.com, the Algerian national cultural asset management authority. The dataset reportedly contains approximately 425,000 records spanning three sections: customer contact and account information, order history, and support tickets, including fields such as full names, email addresses, phone numbers, postal addresses, payment details, and support interaction records. The seller is asking $900 for the full dataset and has provided sa

Target Context: Organization: *OGEBC (Office de Gestion et dExploitation des Biens Culturels)* | Industry: *Government* | Country: *Algeria*

Source URL: `https://breached.st/threads/425k-algeria-www-ogebc-com-national-cultural-asset-management-and-protected-property-records-dataset.87384/unread`

[176] Alleged data breach of Rucabaruk Boxer

Date: 2026-05-19T18:05:51Z | **Category:** Data Breach | **Actor:** Databasehooligan

Description: A threat actor is selling an alleged database dump from rucabarukboxer.com.ar, an Argentine dog breeder/boxer organization. The dataset reportedly contains approximately 624,000 records across three tables — Contacts, DogProfiles, and ServiceBookings — including personal identifiers such as national ID numbers, emails, phone numbers, addresses, and service booking details. The data is priced at $1,200 and is being offered via Telegram.

Target Context: Organization: *Rucabaruk Boxer* | Industry: *Retail* | Country: *Argentina*

Source URL: `https://breached.st/threads/624k-argentina-https-www-rucabarukboxer-com-ar-personal-and-contact-data-records-including-emails-and-phone-numbers.87385/unread`

[177] Sale of HQ Hotmail combo list

Date: 2026-05-19T17:51:50Z | **Category:** Combo List | **Actor:** aurexopforu

Description: A threat actor is offering Hotmail credential hits, with free drops advertised on an external platform and private cloud access available for purchase via Telegram. The post contains hidden content requiring registration to view full details.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://patched.to/Thread-%E2%9C%85-hq-hotmail-hit-%E2%9C%85-304108`

[178] Sale of HQ mix combo list with 3,575 credentials

Date: 2026-05-19T17:51:35Z | **Category:** Combo List | **Actor:** s2lender

Description: A threat actor is distributing a combo list marketed as HQ Mix containing 3,575 credential pairs. The post advertises daily supply of 4,000–12,000 fresh credentials and claims optimized performance for credential stuffing. Content is gated behind forum registration or login.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://patched.to/Thread-file-upload-3575x-hq-mix-by-s2lender-txt`

[179] Sale of 190K UHQ mixed mail combo list

Date: 2026-05-19T17:51:27Z | **Category:** Combo List | **Actor:** Vows

Description: A threat actor is sharing a combo list of approximately 190,000 mixed email credentials, marketed as UHQ and fresh. The post is sponsored by vows.solutions and was shared on a public cracking forum.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-190K-UHQ-MIXED-MAIL-COMBO-FRESH`

[180] Hotmail combo list with 377 credentials marketed as fresh

Date: 2026-05-19T17:51:14Z | **Category:** Combo List | **Actor:** CitronCloud

Description: A forum user shared a combo list of 377 Hotmail credentials marketed as fresh access dated 19.05. The content is hidden behind a registration/login wall on the forum.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://patched.to/Thread-file-upload-377x-hotmail-fresh-access-top-quality-19-05`

[181] Sale of UHQ Gmail combo list with 705K credentials

Date: 2026-05-19T17:51:08Z | **Category:** Combo List | **Actor:** Vows

Description: A threat actor is sharing a combo list marketed as 705K UHQ Gmail credentials described as fresh. The post is sponsored by vows.solutions. Gmail is a credential-stuffing target, not the breach victim.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-705K-UHQ-GMAIL-COMBO-FRESH`

[182] Sale of UHQ Outlook combo list with 35,000 credentials

Date: 2026-05-19T17:50:48Z | **Category:** Combo List | **Actor:** Vows

Description: A threat actor is offering a combo list of 35,000 Outlook credentials, marketed as high quality and fresh. The list is shared on a cracking forum and appears to be intended for credential stuffing. The post is sponsored by vows.solutions.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-35K-UHQ-OUTLOOK-COMBO-FRESH`

[183] Combo List of 15,124 Email:Password Credentials

Date: 2026-05-19T17:50:30Z | **Category:** Combo List | **Actor:** AiCombo

Description: A threat actor is distributing a combo list of 15,124 email:password credentials marketed as private, full-access, and fresh. The post is categorized under combolists on a known cybercrime forum. No specific victim organization or targeted service is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-15-124-Private-FA-Good-Line-Fresh`

[184] Sale of UHQ Hotmail combo list containing 100K credentials

Date: 2026-05-19T17:50:12Z | **Category:** Combo List | **Actor:** Vows

Description: A threat actor is offering a combo list of 100,000 Hotmail credentials, marketed as UHQ and fresh. The post is sponsored by vows.solutions and was shared on a public cracking forum.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-100K-UHQ-HOTMAIL-COMBO-FRESH`

[185] Sale of Hotmail credential combo list

Date: 2026-05-19T17:49:44Z | **Category:** Combo List | **Actor:** Snowki032312

Description: A threat actor shared a combo list of 210 Hotmail email:password credentials marketed as fresh and high quality via an external paste link.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-x210-HOTMAIL-HITS-FRESH-UHQ`

[186] Sale of combo list marketed for Minecraft and Roblox credential stuffing

Date: 2026-05-19T17:49:34Z | **Category:** Combo List | **Actor:** MetaCloud

Description: A threat actor is distributing a combo list of approximately 762,000 credentials, marketed as suitable for use against Minecraft, Roblox, and other targets. The list is described as sourced from a private base. Content is gated behind forum registration or login.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://leakforum.io/Thread-Leak-%E2%9A%A1762K-MINECRAFT-ROBLOX%E2%9A%A1PRIVATE-BASE-GOOD-ON-ANY-TARGET%E2%9A%A1`

[187] Sale of Hotmail credential combo list

Date: 2026-05-19T17:49:20Z | **Category:** Combo List | **Actor:** combosell1

Description: A forum user is offering a combo list of approximately 6,000 Hotmail credentials described as high-quality hits. The list appears to contain email and password pairs intended for credential stuffing. No additional details are available from the post content.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-6K-HQ-HOTMAIL-HITS`

[188] Free combo list of 18,000 mixed mail access credentials

Date: 2026-05-19T17:48:53Z | **Category:** Combo List | **Actor:** Luxe90

Description: A threat actor has freely distributed a combo list containing approximately 18,000 mixed email access credentials, marketed as fresh. The post encourages community engagement and references a Telegram channel named Ghost Cloud.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-FRESH-18k-MIX-MAIL-ACCESS-HQ-PRIVATE-LIST-DAILY-DROP-GHOST-CLOUD`

[189] Alleged combo list of 40,313 private email credentials with full access

Date: 2026-05-19T17:48:34Z | **Category:** Combo List | **Actor:** AiCombo

Description: A threat actor is distributing a combo list of 40,313 email credentials advertised as private full-access mail combinations. The post is categorized as a combolist based on thread title metadata; no additional details are available from the post content.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-40-313-Private-FA-Mail-Access-Combolist`

[190] Recruitment post for paid online tasks targeting US, CA, UK, and Australian users

Date: 2026-05-19T17:48:23Z | **Category:** Chatter | **Actor:** moneyspro9 🍼

Description: A forum user posted a job recruitment offer on Dread seeking individuals from the United States, Canada, United Kingdom, and Australia for four unspecified online tasks, offering $190 for 40-50 minutes of work. The post claims the work is legal and requests direct messages without PGP. No specific threat activity or victim organization is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion/post/4f3d21061ae803fca2bb`

[191] Combo List: Free Hotmail/Outlook mail access credentials

Date: 2026-05-19T17:48:15Z | **Category:** Combo List | **Actor:** Luxe90

Description: A threat actor on a cracking forum is freely distributing a combo list of approximately 1,100 Hotmail/Outlook credentials. The post markets the list as fresh with a high hit rate and directs users to a Telegram channel for additional content.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-FRESH-1-1k-HOTMAIL-MAIL-ACCESS-100-PRIVATE-HIGH-HIT-RATE-GHOST-CLOUD`

[192] Sale of GoliathCoreAI Futures/Spot Trading Platform Source Code

Date: 2026-05-19T17:47:46Z | **Category:** Services | **Actor:** TGM

Description: A threat actor is offering the source code of a proprietary futures and spot trading platform called GoliathCoreAI for sale. The offering includes a trading robot cockpit, admin panel, and various customizable management features. Interested buyers are directed to contact the seller via Telegram or Discord.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Supreme-%E2%AD%90%E2%AD%90-%E2%AD%90-GoliathCoreAI-Futures-Spot-Trading-platform-SOURCE-CODE-%E2%AD%90%E2%AD%90-%E2%AD%90`

[193] Sale of rewards and gift card fraud services targeting multiple retail programs

Date: 2026-05-19T17:47:27Z | **Category:** Carding | **Actor:** Kyzen0

Description: A threat actor is advertising fraud services targeting multiple retail rewards and gift card programs including Sams Cash, Canadian Tire, Ulta, and Bloomingdales, claiming potential earnings of $10,000 or more. The post references an external platform (darkmoon.to), likely hosting the full offering or tutorial.

Target Context: Organization: *Unknown* | Industry: *Retail* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-REWARDS-GIFTCARDS-SAMSCASH-CANADIAN-TIRE-ULTA-BLOOMINGDALES-MAKE-10000`

[194] Cybersecurity and sysadmin services offered for cryptocurrency payment

Date: 2026-05-19T17:47:07Z | **Category:** Chatter | **Actor:** SetsUnder 🍼

Description: A forum user is advertising sysadmin and cybersecurity services on a darknet forum, accepting BTC and XMR. Offered services include UNIX application deployment, hidden service backend management, and VPS hardening. The poster claims over four years of darknet experience and accepts FairTrade Escrow.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion/post/4d01978bfeb3b313bd8a`

[195] Job posting seeking coder for Telegram mini-app development

Date: 2026-05-19T17:45:44Z | **Category:** Chatter | **Actor:** misterbanana 🍼

Description: A forum user is seeking an experienced developer to build a Telegram mini-app, offering up to $1,000 in BTC via escrow. The post contains no threat-related content and appears to be a general job solicitation on a dark web forum.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion/post/6572558dfbe72cfd2856`

[196] Sale of custom dark web tool development and operational services including phishing, malware, ransomware, and C2 infrastructure

Date: 2026-05-19T17:44:25Z | **Category:** Chatter | **Actor:** Agaptus 🍼

Description: A threat actor on Dread is advertising custom development and operational services for underground clients, including phishing kit generators, infostealer builders, ransomware payload builders with RaaS affiliate panels, C2 frameworks, and credential stuffing engines. Services are offered for payment in XMR or BTC, with the actor claiming all tools are built from scratch. The actor also claims to provide operational execution including phishing campaigns, C2 management, and ransomware coordinati

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion/post/fde4df9a7a164679dab3`

[197] SMS sender service job listing on darknet forum

Date: 2026-05-19T17:43:13Z | **Category:** Chatter | **Actor:** crazycrazy 🍼

Description: A forum post on Dreads Jobs4Crypto board advertises a part-time job for an SMS sender. No further content is available to determine the scope or target of the activity.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion/post/c159b3d1b63b2eacbbc9`

[198] Forum user offering sales closing and client follow-up services

Date: 2026-05-19T17:38:30Z | **Category:** Chatter | **Actor:** tuminis 🍼

Description: A forum user on Dread is advertising themselves as available for sales closing, client follow-ups, and lead conversion work across digital services, SaaS, and agency offers. The post solicits direct messages from potential buyers. No threat activity or specific victim is referenced.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion/post/9fda4710e1c2134b2b42`

[199] Alleged distribution of Admin Finder v2.5 - Automated Admin Panel Scanner Tool

Date: 2026-05-19T17:37:57Z | **Category:** Malware | **Actor:** MexazoOfficials

Description: User shared Admin Finder v2.5, an automated scanner tool designed to detect and locate admin panels and login pages on target websites. The tool implements fuzzing techniques against common admin paths, includes anti-detection mechanisms (1-second delays, 10-second Cloudflare recovery delays), uses CloudScraper to bypass Cloudflare protection, and automatically saves discovered admin panels to admin_found.txt. Tool processes 1000+ admin paths systematically via command-line interface.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://t.me/forum_mexazo_officials/5`

[200] Alleged sale of access to private cloud database with stolen Hotmail credentials and company datasets

Date: 2026-05-19T17:35:18Z | **Category:** Initial Access | **Actor:** Yhōu

Description: User Yhōu is offering for sale access to a private cloud database containing premium Hotmail credentials and geo-specific data sets from multiple companies including Walmart, eBay, Kleinanzeigen, Uber, and Poshmark. Available regions include FR, IT, BR, UK, US, JP, PL, RU, ES, MX, CA, SP, SG and others. This represents unauthorized access to compromised data from multiple commercial platforms.

Target Context: Organization: *Walmart, eBay, Uber, Poshmark, Kleinanzeigen* | Industry: *E-commerce, Ride-sharing, Marketplace* | Country: *Unknown*

Source URL: `https://t.me/c/2613583520/85067`

[201] Alleged sale of Hotmail credentials and geo-specific combolists from private cloud database

Date: 2026-05-19T17:33:18Z | **Category:** Combo List | **Actor:** Wěilóng

Description: Seller offering access to private cloud database containing high-quality Hotmail credentials and country-specific datasets. Available regions include FR, IT, BR, UK, US, JP, PL, RU, ES, MX, CA, SP, SG and others. Seller claims to have access to premium Hotmail data and associated platform credentials (Walmart, eBay, Kleinanzeigen, Uber, Poshmark). Serious buyers only, seller offers keyword verification.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Multiple (FR, IT, BR, UK, US, JP, PL, RU, ES, MX, CA, SP, SG)*

Source URL: `https://t.me/c/2613583520/85059`

[202] Purchase request for NuBank debit card photos

Date: 2026-05-19T17:23:58Z | **Category:** Chatter | **Actor:** notanoob 🍼

Description: A forum user is soliciting front and back photographs of a NuBank debit card showing visible card numbers and cardholder name, offering $40 via escrow. The request specifies unedited, high-quality photos, likely intended for card fraud or cloning purposes.

Target Context: Organization: *NuBank* | Industry: *Finance* | Country: *Unknown*

Source URL: `https://dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion/post/fee10ae8a8e6bfd80f3a`

[203] Sale of discounted OpenAI API access via reseller service

Date: 2026-05-19T17:22:48Z | **Category:** Chatter | **Actor:** silencedsignal1x

Description: A forum user is advertising anonkey.st, a service claiming to resell OpenAI API keys at 80% below standard pricing, compatible with tools such as Cursor, Codex, and OpenCode. The service accepts cryptocurrency, requires no registration, and explicitly markets itself to users conducting illegal activities and automated non-human agents. Bulk pricing and specialized offline model requests are also offered via direct message.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion/post/5b7556c73256bc58c318`

[204] Recruitment for crypto drainer malware distribution campaign

Date: 2026-05-19T17:19:12Z | **Category:** Chatter | **Actor:** GoKart

Description: A threat actor is recruiting social engineers to distribute a self-described crypto drainer malware targeting high-net-worth cryptocurrency holders. The actor claims the malware leverages an unpatched exploit not yet flagged by security tools, and is offering a 50% revenue share per successful theft. The post also references website spoofing, smart contract manipulation, and money laundering capabilities.

Target Context: Organization: *Unknown* | Industry: *Finance* | Country: *Unknown*

Source URL: `https://dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion/post/a20771e2631f1ba618ae`

[205] Job posting for social engineering and ewhoring services on Dread

Date: 2026-05-19T17:17:50Z | **Category:** Chatter | **Actor:** CocaColaNorth 🍼

Description: A forum user on Dreads /d/Jobs4Crypto board posted a job listing seeking individuals with catfishing and ewhoring experience. No additional content was available in the post. The nature of the requested work suggests intent to conduct online social engineering or fraud-related activities.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion/post/2288dab6f4358f37588f`

[206] Sale of alleged initial access to ThreatDown

Date: 2026-05-19T17:16:45Z | **Category:** Initial Access | **Actor:** plaguelost

Description: A threat actor is advertising the sale of alleged full access to ThreatDown on a cybercrime forum. No further details are available as the post contains no content beyond the thread title.

Target Context: Organization: *ThreatDown* | Industry: *Cybersecurity* | Country: *Unknown*

Source URL: `https://breachforums.rs/Thread-SELLING-New-ThreatDown-acces-full`

[207] Combo list of 200K email and password credentials shared freely

Date: 2026-05-19T17:14:25Z | **Category:** Combo List | **Actor:** zubicks

Description: A threat actor shared a combo list containing approximately 200,000 email and password pairs at no charge via Anonfilesnew. No specific victim organization or service is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://breachforums.rs/Thread-Combolist-200K-Email-Pass`

[208] Combo List of 63K Hotmail credentials

Date: 2026-05-19T17:12:49Z | **Category:** Combo List | **Actor:** zubicks

Description: A combo list containing approximately 63,000 Hotmail email and password pairs was shared on BreachForums. The post is categorized under combolists and no additional details are available from the post content.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://breachforums.rs/Thread-Combolist-63K-Hotmail-Email-Pass`

[209] Sale of private Germany-targeted combo list and credential services

Date: 2026-05-19T17:12:41Z | **Category:** Combo List | **Actor:** cloudantalya

Description: A threat actor operating as Antalya Private Cloud is advertising a private combo list service featuring approximately 66,000 Germany-targeted credentials, UHQ Hotmail combos, mixed combo lists, and premium logs. The offering includes geo-targeted credential lists and mail checkers marketed as high-quality and fresh. Access is sold via a Telegram contact with a free trial sample provided.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://patched.to/Thread-file-upload-66k-private-germany-%F0%9F%87%A9%F0%9F%87%AA-access-by-antalya-h`

[210] Multi-region combo list mix distributed on cybercrime forum

Date: 2026-05-19T17:12:11Z | **Category:** Combo List | **Actor:** MetaCloud3

Description: A threat actor is distributing a combo list of approximately 789,000 credential pairs sourced from multiple regions including the EU, USA, UK, Poland, Germany, and Canada. The post markets the list as a private base suitable for use against any target. The actor also advertises an ongoing combo cloud service.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://patched.to/Thread-file-upload-%E2%9A%A1789k-eu-usa-uk-pl-de-canada-comcast-mix%E2%9A%A1private-base-good-on-any-target%E2%9A%A1`

[211] Sale of Hotmail combo list by s2lender

Date: 2026-05-19T17:11:51Z | **Category:** Combo List | **Actor:** s2lender

Description: A threat actor operating as s2lender is distributing a combo list of approximately 174 high-quality Hotmail credentials on a cybercrime forum. The post advertises daily supply of 4,000–12,000 fresh credentials marketed as optimized for credential stuffing. Access to the full content requires forum registration or login.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://patched.to/Thread-file-upload-174x-hq-hotmail-by-s2lender-txt`

[212] Free sharing of trading course materials on cracking forum

Date: 2026-05-19T17:11:38Z | **Category:** Alert | **Actor:** ZamanX

Description: A forum user shared download links for a trading course covering Forex, cryptocurrencies, stocks, and indices. The post appears to be an unauthorized distribution of commercial educational content. No specific victim organization or threat actor activity is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://nulledbb.com/thread-Simple-Trading-Book-v1-and-V2`

[213] Forum inquiry about receiving digital goods from darknet markets

Date: 2026-05-19T17:11:33Z | **Category:** Chatter | **Actor:** rommie11 🍼

Description: A forum user posted a general question on Dread asking how digital products are typically delivered by darknet market vendors. The post contains no threat content, no specific victims, and no actionable intelligence.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion/post/40a53f699505f83da633`

[214] Combo list of 80K email and password credentials shared freely

Date: 2026-05-19T17:11:26Z | **Category:** Combo List | **Actor:** zubicks

Description: A threat actor shared a combo list containing approximately 80,000 email and password pairs at no charge via Anonfilesnew. No specific victim organization or targeted service is identified in the post.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://breachforums.rs/Thread-Combolist-80K-Email-Pass`

[215] Combo List targeting Hotmail with 10.6K credentials

Date: 2026-05-19T17:11:03Z | **Category:** Combo List | **Actor:** zubicks

Description: A combo list containing approximately 10,600 email and password pairs targeting Hotmail accounts was shared on BreachForums. No additional details are available as the post content is absent.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://breachforums.rs/Thread-Combolist-Hotmail-10-6K-Email-Pass`

[216] Sale of fresh mix combo list with 83,272 lines

Date: 2026-05-19T17:10:43Z | **Category:** Combo List | **Actor:** stormtrooper

Description: A threat actor shared a combo list containing 83,272 email:password lines, marketed as fresh. The content is hidden behind a registration/login wall and promoted via a Telegram channel.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://demonforums.net/Thread-Email-Pass-83-272-Lines-Fresh-Mix-Combolist`

[217] Alleged sale of Nighthawk C2 (Janus 0.4) malware with lifetime license

Date: 2026-05-19T17:08:28Z | **Category:** Malware | **Actor:** APT IRAN

Description: Threat actor advertising limited-time sale of Nighthawk C2 malware tool version Janus 0.4 with lifetime license. Original price listed as $10,000, market price $7,500, currently offered at $5,000 with discount code Qr_708. Purchase instructions provided via Telegram bot @DBMSLivebot.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://t.me/APTIRAN_OFFICIAL/145`

[218] Alleged sale of Nighthawk C2 Janus 0.4 malware tool

Date: 2026-05-19T17:07:25Z | **Category:** Malware | **Actor:** Unknown

Description: Threat actor advertising the sale of Nighthawk C2 Janus 0.4, a command and control malware tool, with a lifetime license offered at $5,000 USD (reduced from $7,500).

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://t.me/c/3881618514/104`

[219] Free Hotmail combo list of 3,780 credentials

Date: 2026-05-19T17:05:50Z | **Category:** Combo List | **Actor:** Nulled07

Description: A forum user shared a combo list of 3,780 Hotmail credentials, marketed as fresh. The content is gated behind registration or login on the forum.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://leakforum.io/Thread-Leak-%E2%9A%A1%E2%9A%A1-3780x-FRESH-HOTMAIL-%E2%9A%A1%E2%9A%A1`

[220] Hotmail combo list of 784K credentials

Date: 2026-05-19T17:05:30Z | **Category:** Combo List | **Actor:** MetaCloud

Description: A threat actor is distributing a combo list of approximately 784,000 Hotmail credentials, marketed as high quality, dehashed, fresh, and unique. The list is intended for credential stuffing against Hotmail/Outlook accounts. No specific breached organization is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://leakforum.io/Thread-Leak-%E3%80%8C-784K-%E3%80%8D%E2%9A%A1HOTMAIL%E2%9A%A1HIGH-QUALITY-PRIVATE-COMBO%E2%9A%A1DEHASHED-LINES%E2%9A%A1FRESH-AND-UNIQUE%E2%9A%A1`

[221] Sale of mail access combo list with 15,000 credentials

Date: 2026-05-19T17:03:45Z | **Category:** Logs | **Actor:** VegaMoon

Description: A forum user is sharing a combo list advertised as containing 15,000 mail access credentials. The content is hidden behind a registration wall. No specific victim organization or breach source is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://xforums.st/threads/15k-good-mail-access-combolist.615506/`

[222] Sale of 15,000 mail access combo list

Date: 2026-05-19T17:03:40Z | **Category:** Combo List | **Actor:** vmmoons

Description: A forum member is sharing a combo list advertised as containing 15,000 email and password credential pairs marketed as valid mail access. No additional details about the source or targeted service are available.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-15k-Good-Mail-Access-Combolist`

[223] Sale of UHQ Yahoo combo list with 45,000 credentials

Date: 2026-05-19T17:03:24Z | **Category:** Combo List | **Actor:** Vows

Description: A threat actor is distributing a combo list marketed as 45,000 UHQ Yahoo credentials described as fresh. The post is sponsored by an AIO tool service. Yahoo is the credential-stuffing target, not the breach source.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-45K-UHQ-YAHOO-COMBO-FRESH--2096366`

[224] Combo list of 181K mixed email credentials

Date: 2026-05-19T17:02:47Z | **Category:** Combo List | **Actor:** Vows

Description: A user on Cracked.st is sharing a combo list of 181,000 mixed email credentials marketed as fresh UHQ (ultra-high quality). The post is sponsored by slateaio.com, suggesting the list may be intended for credential stuffing use.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-181K-UHQ-MIXED-MAIL-COMBO-FRESH`

[225] Mixed mail access combo list shared for free

Date: 2026-05-19T17:02:16Z | **Category:** Combo List | **Actor:** lundman01

Description: A threat actor is distributing mixed mail access credential hits via a Telegram channel. Private cloud access with additional credentials is offered for purchase via a separate contact. No specific victim organization or record count is disclosed.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-%E2%9C%85-HQ-MIX-MAIL-ACCESS-HIT-%E2%9C%85`

[226] Sale of Hotmail combo list with 95K credentials

Date: 2026-05-19T17:01:44Z | **Category:** Combo List | **Actor:** Vows

Description: A threat actor is distributing a combo list of approximately 95,000 Hotmail credentials, marketed as high quality and fresh. The post is sponsored by vows.solutions and shared on a public cracking forum.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-95K-UHQ-HOTMAIL-COMBO-FRESH`

[227] Sale of UHQ Outlook combo list with 36K credentials

Date: 2026-05-19T17:01:11Z | **Category:** Combo List | **Actor:** Vows

Description: A threat actor is sharing a combo list of approximately 36,000 Outlook credentials, marketed as UHQ and fresh. The post is sponsored by vows.solutions and was shared on a public cracking forum.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-36K-UHQ-OUTLOOK-COMBO-FRESH`

[228] Sale of UHQ Gmail combo list with 734K credentials

Date: 2026-05-19T17:00:32Z | **Category:** Combo List | **Actor:** Vows

Description: A threat actor is distributing a combo list containing 734,000 Gmail credentials, marketed as UHQ (ultra-high quality) and fresh. The post is sponsored by a credential-stuffing tool service. Gmail is the targeted service for credential stuffing, not the breach source.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-734K-UHQ-GMAIL-COMBO-FRESH`

[229] Sale of mixed mail credential combo list

Date: 2026-05-19T17:00:14Z | **Category:** Combo List | **Actor:** Alphaaaxd

Description: A threat actor is sharing a combo list of approximately 3,908 mixed email credentials, including Hotmail accounts, marketed as premium valid hits. The post promotes private cloud access and directs users to a Telegram contact.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-%E2%9A%A1%E2%9A%A1-3908x-PREMIUM-MIX-MAIL-HITS%E2%9A%A1%E2%9A%A1`

[230] Refunding business setup service offered on cracking forum

Date: 2026-05-19T16:59:26Z | **Category:** Services | **Actor:** BossOfBosses

Description: A forum seller operating as Paxerr is advertising a service to set up refunding businesses for buyers, offering 100% refund guarantees and unlimited revisions with 24/7 support. The post includes a terms of service outlining payment, delivery, and refund conditions. Refunding services are commonly associated with retail fraud schemes that exploit merchant return policies.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-%E2%9A%A1LAUNCH-YOUR-REFUNDING-BUSINESS-%E2%80%A2-100-REFUND-%E2%80%A2-UNLIMITED-REVISIONS-%E2%80%A2-24-7-SUPPORT%E2%9A%A1`

[231] Alleged defacement of juai.chat by C10F./X404

Date: 2026-05-19T16:58:25Z | **Category:** Defacement | **Actor:** C10F./X404

Description: Defacement claim attributed to C10F./X404, identified as part of a defacer Indonesian team. Target website: https://juai.chat/

Target Context: Organization: *juai.chat* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://t.me/c/3755871403/540`

[232] Website Defacement of CyberNex Product by overthrash1337 (Team Hazardous Pk)

Date: 2026-05-19T16:40:41Z | **Category:** Defacement | **Actor:** overthrash1337, Team Hazardous Pk

Description: On May 19, 2026, the website cybernexproduct.com was defaced by threat actor overthrash1337, operating under the group Team Hazardous Pk. The defacement targeted a specific page rather than the homepage and was a standalone, non-mass defacement incident. The attack was archived and mirrored via zone-xsec.com.

Target Context: Organization: *CyberNex Product* | Industry: *Technology* | Country: *Unknown*

Source URL: `https://zone-xsec.com/mirror/id/925110`

[233] Website Defacement of Vista Marine by overthrash1337 (Team Hazardous Pk)

Date: 2026-05-19T16:38:33Z | **Category:** Defacement | **Actor:** overthrash1337, Team Hazardous Pk

Description: On May 19, 2026, a threat actor known as overthrash1337, affiliated with Team Hazardous Pk, defaced the website of Vista Marine, an Indian maritime services company. The defacement targeted a subdirectory of the site rather than the home page. The attack is attributed to a Pakistani hacktivist group known for web defacement campaigns.

Target Context: Organization: *Vista Marine* | Industry: *Maritime / Marine Services* | Country: *India*

Source URL: `https://zone-xsec.com/mirror/id/925111`

[234] Sale of fresh email combo list targeting USA and EU regions

Date: 2026-05-19T16:23:59Z | **Category:** Combo List | **Actor:** BreachLeak

Description: A threat actor is distributing a combo list of approximately 50,000 email credentials purportedly sourced from USA and EU regions. The content is gated behind registration or login on the forum. No specific victim organization or breach source is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://patched.to/Thread-file-upload-%E2%9D%84%EF%B8%8F-fresh-mail-%E2%80%94-usa-eu-%E2%80%94-50k%E2%9D%84%EF%B8%8F-304081`

[235] Sale of Gmail and mixed credential combo list

Date: 2026-05-19T16:23:30Z | **Category:** Combo List | **Actor:** BreachLeak

Description: A forum member is offering a combo list described as Private Lines containing Gmail and mixed credentials. The content is hidden behind a registration or login requirement, limiting visibility into record count or specific details.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://patched.to/Thread-file-upload-%E2%9A%94%EF%B8%8F-private-lines-%E2%80%94-gmail-mix-%E2%9A%94%EF%B8%8F-304084`

[236] Free distribution of URL:Log:Pass combo list — 8+ million lines

Date: 2026-05-19T16:23:13Z | **Category:** Combo List | **Actor:** lexityfr

Description: A threat actor is freely distributing a URL:Log:Pass combo list containing over 8 million lines on a cybercrime forum. The content is gated behind registration or login. No specific victim organization is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://patched.to/Thread-file-upload-url-log-pass-free-best-lines-8-million-lines-part-354`

[237] Free distribution of URL:Log:Pass combo list with 8+ million lines

Date: 2026-05-19T16:22:54Z | **Category:** Combo List | **Actor:** lexityfr

Description: A threat actor is freely distributing a URL:Log:Pass combo list advertised as containing over 8 million lines. The content is gated behind registration or login on the forum. No specific victim organization or breach source is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://patched.to/Thread-file-upload-url-log-pass-free-best-lines-8-million-lines-part-353`

[238] Combo List of Hotmail Credentials (x3000)

Date: 2026-05-19T16:22:25Z | **Category:** Combo List | **Actor:** BreachLeak

Description: A forum user shared a combo list of approximately 3,000 Hotmail credentials as hidden content requiring registration or login to access. The post is categorized as a credential combo list and does not indicate a breach of Hotmail or Microsoft infrastructure.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://patched.to/Thread-file-upload-%F0%9F%94%A5%F0%9F%94%A5%F0%9F%94%A5-hotmail-%E2%80%A2-private-x3000-%F0%9F%94%A5%F0%9F%94%A5%F0%9F%94%A5-304080`

[239] Sale of Yahoo-targeted combo list with 1.9 million lines

Date: 2026-05-19T16:22:20Z | **Category:** Combo List | **Actor:** HqComboSpace

Description: A threat actor is distributing a combo list of approximately 1.9 million email:password pairs advertised as targeting Yahoo accounts. The post is categorized as a social-target combolist, suggesting credentials are intended for credential stuffing against Yahoo services.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-1-926-386-Lines-%E2%9C%85-Social-Target-Combolist-Yahoo`

[240] Combo List of mixed email credentials (12K)

Date: 2026-05-19T16:22:01Z | **Category:** Combo List | **Actor:** Cloudredhat

Description: A combo list of approximately 12,000 mixed email and password credentials has been shared on a cracking forum. The post advertises the list as mixed mail access, suggesting credentials span multiple email providers.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-12K-MIXED-MAIL-ACCESS`

[241] Sale of CrunchyRoll combo list with 100K credentials

Date: 2026-05-19T16:21:40Z | **Category:** Combo List | **Actor:** RogenPlay

Description: A threat actor is distributing a combo list of 100,000 credentials marketed for use against CrunchyRoll, described as freshly checked and AntiPublic checked. CrunchyRoll is the credential-stuffing target, not the breach source. The post is sponsored by RogenCloud.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-%E2%9C%85-%E2%9C%85-%E2%9C%85-%E2%9C%A8-100K-CrunchyRollCombolist-1-%E2%9C%A8-Freshly-Checked-AntiPublic-Checked-%E2%9C%A8-%E2%9C%85-%E2%9C%85-%E2%9C%85`

[242] Free release of URL:Log:Pass combo list with 7.48 million lines

Date: 2026-05-19T16:21:29Z | **Category:** Combo List | **Actor:** Max095

Description: A forum user has shared a URL:Log:Pass combo list containing approximately 7.48 million lines as hidden content. The post is accessible to registered forum members only. No specific victim organization or breach source is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://leakforum.io/Thread-Leak-The-best-Url-Log-Pass-7-480-179-M%C4%B1ll%C4%B1on-L%C4%B1nes`

[243] Sale of Hotmail combo list with 853 valid credentials

Date: 2026-05-19T16:21:20Z | **Category:** Combo List | **Actor:** Cloudredhat

Description: A forum user shared a combo list of 853 Hotmail credentials marketed as valid. The post was made on a public cracking forum under the combolists section.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-X853-HOTMAILS-VALID`

[244] Sale of Netflix combo list with 700K credentials

Date: 2026-05-19T16:20:59Z | **Category:** Combo List | **Actor:** RogenPlay

Description: A threat actor is distributing a combo list of approximately 700,000 credentials marketed for use against Netflix, described as freshly checked and AntiPublic verified. The post is sponsored by RogenCloud and includes a download link.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-%E2%9C%85-%E2%9C%85-%E2%9C%85-%E2%9C%A8-700K-Netflix-Combolist-1-%E2%9C%A8-Freshly-Checked-AntiPublic-Checked-%E2%9C%A8-%E2%9C%85-%E2%9C%85-%E2%9C%85`

[245] Sale of 52,184 private full-access mail combo list

Date: 2026-05-19T16:20:39Z | **Category:** Combo List | **Actor:** AiCombo

Description: A combo list containing 52,184 email and password pairs marketed as private full-access mail credentials was shared on a cracking forum. No further details are available from the post content.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-52-184-Private-FA-Mail-Access-Combolist`

[246] Sale of Spotify combo list with 290K credentials

Date: 2026-05-19T16:20:18Z | **Category:** Combo List | **Actor:** RogenPlay

Description: A threat actor is distributing a combo list of approximately 290,000 credentials marketed as freshly checked and AntiPublic-verified, intended for credential stuffing against Spotify. The post is sponsored by RogenCloud and includes a download link.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-%E2%9C%85-%E2%9C%85-%E2%9C%85-%E2%9C%A8-290K-Spotify-Combolist-1-%E2%9C%A8-Freshly-Checked-AntiPublic-Checked-%E2%9C%A8-%E2%9C%85-%E2%9C%85-%E2%9C%85`

[247] Combo List of mixed email credentials (418 records)

Date: 2026-05-19T16:19:45Z | **Category:** Combo List | **Actor:** Cloudredhat

Description: A combo list of approximately 418 mixed email and password combinations has been shared on a cracking forum. No specific victim organization or breach source is identified. The credentials appear to be a mixed-source collection.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-418X-MIX-MAILS`

[248] Sale of TikTok combo list with 100K credentials

Date: 2026-05-19T16:19:23Z | **Category:** Combo List | **Actor:** RogenPlay

Description: A threat actor is distributing a combo list of 100,000 credentials marketed for use against TikTok, advertised as freshly checked and AntiPublic verified. The post is sponsored by RogenCloud and includes a download link. TikTok is the credential-stuffing target, not the breach source.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-%E2%9C%85-%E2%9C%85-%E2%9C%85-%E2%9C%A8-100K-TikTok-Combolist-1-%E2%9C%A8-Freshly-Checked-AntiPublic-Checked-%E2%9C%A8-%E2%9C%85-%E2%9C%85-%E2%9C%85`

[249] Sale of discounted Microsoft SC-100 exam vouchers on cybercrime forum

Date: 2026-05-19T16:18:35Z | **Category:** Services | **Actor:** wavesub

Description: A forum seller is offering Microsoft SC-100 (Cybersecurity Architect) exam vouchers at $60, significantly below the retail price of $165. The post advertises globally valid vouchers via direct message. The legitimacy of these vouchers is unverified and they may be fraudulently obtained or counterfeit.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Supreme-%E2%9C%A8%E2%9C%A8%E2%9C%A8Microsoft-Certified-Cybersecurity-Architect-%E2%80%93-Exam-Voucher-%E2%9D%84%EF%B8%8F%E2%9D%84%EF%B8%8F%E2%9D%84%EF%B8%8F`

[250] Sale of UHQ combo list for gaming and shop targets

Date: 2026-05-19T16:18:16Z | **Category:** Combo List | **Actor:** Cloudredhat

Description: A threat actor is offering UHQ combo lists claimed to be suitable for credential stuffing against gaming and shop targets. The seller advertises a free trial and directs interested buyers to a Telegram contact. No specific victim organization or record count is disclosed.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-COMBO-REAL-UHQ-FOR-ANY-TARGET-GAME-SHOP-WITH-TEST-FREE`

[251] Sale of discounted Apify web scraping subscription

Date: 2026-05-19T16:17:58Z | **Category:** Services | **Actor:** wavesub

Description: A forum user is selling discounted Apify web scraping and automation subscriptions for $20, offering 4 months of access with $600 in platform credits. The service includes access to 1,500+ pre-built scrapers covering platforms such as Google, Amazon, and LinkedIn. Buyers are instructed to DM the seller to receive access.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Supreme-%E2%9D%84%EF%B8%8F%E2%9D%84%EF%B8%8F%E2%9D%84%EF%B8%8F-Apify-%E2%80%93-Web-Scraping-Automation-4-Months-%E2%9A%A1%E2%9A%A1%E2%9A%A1`

[252] Sale of 12K email access combo list

Date: 2026-05-19T16:16:11Z | **Category:** Combo List | **Actor:** Megacloud

Description: A threat actor is distributing a combo list of 12,000 claimed valid email credentials marketed as top quality. The content is gated behind a reply requirement on the forum.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://altenens.is/threads/12k-full-valid-mail-access-mix-top-quality-19-05.2942746/unread`

[253] Combo List targeting gaming platforms (Fortnite, Minecraft, Valorant, Steam, Rockstar)

Date: 2026-05-19T16:13:12Z | **Category:** Combo List | **Actor:** KiwiShio

Description: A threat actor is distributing a combo list of approximately 3,760 Hotmail credentials marketed as fresh and high quality. The post claims the credentials are suitable for use against gaming platforms including Fortnite, Minecraft, Valorant, Steam, and Rockstar. The content is hidden behind registration and the actor advertises via Telegram.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://demonforums.net/Thread-Email-Pass-3760x-%E2%AD%90%E2%AD%90-FRESH-HQ-MIX-MAIL-%E2%AD%90%E2%AD%90-FORNITE-MINECRAFT-VALORANT-STEAM-ROCKSTAR-%E2%AD%90%E2%AD%90`

[254] Sale of Hotmail credential combo list with 1,496 hits

Date: 2026-05-19T16:11:39Z | **Category:** Combo List | **Actor:** alphaxdd

Description: A threat actor on CrackingX is distributing a combo list of 1,496 alleged valid Hotmail credentials, marketed as premium hits. The post includes a download link and directs interested parties to a Telegram contact.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://crackingx.com/threads/75789/`

[255] Carding discussion involving AUD prepaid gift cards and cryptocurrency conversion

Date: 2026-05-19T16:03:01Z | **Category:** Chatter | **Actor:** budzy653

Description: A forum user is soliciting advice on how to fraudulently obtain and cash out AUD prepaid Visa/Mastercard gift cards by converting them to cryptocurrency to evade detection. The post describes an anticipated chargeback dispute following purchase and asks for operational security guidance. The user also inquires about laundering proceeds through a crypto.com account and associated Visa card.

Target Context: Organization: *Unknown* | Industry: *Finance* | Country: *Australia*

Source URL: `https://dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion/post/6587ccdfd615abd8b2f3`

[256] Alleged scam report against darknet vendor W0rm30 on Dread

Date: 2026-05-19T16:01:36Z | **Category:** Chatter | **Actor:** born_confused

Description: A Dread forum user alleges that vendor W0rm30 scammed them for $15 in a fullz (personally identifiable information) deal, providing fake documents and stalling for three days. The post includes screenshots as evidence and warns other users against transacting with this vendor. No confirmed data breach or compromise of a third-party organization is involved.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion/post/981c5ac162b0088c3e1f`

[257] Edu combo list with 91,908 credentials

Date: 2026-05-19T15:57:44Z | **Category:** Combo List | **Actor:** AiCombo

Description: A combo list containing 91,908 email and password pairs targeting educational institutions has been shared on a cracking forum. The credentials are marketed as fresh and good quality. No specific victim organization is identified.

Target Context: Organization: *Unknown* | Industry: *Education* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-91-908-Good-Edu-Fresh-Combolist`

[258] Sale of alleged private combo list targeting European accounts

Date: 2026-05-19T15:57:25Z | **Category:** Combo List | **Actor:** AiCombo

Description: A forum user is distributing a combo list advertised as private, containing approximately 40,287 email:password pairs targeting European accounts. The post is categorized as a combo list intended for credential stuffing. No specific victim organization or service is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-40-287-Private-FA-Combolist-Europa-Good`

[259] Sale of UHQ Hotmail combo list

Date: 2026-05-19T15:57:00Z | **Category:** Combo List | **Actor:** Cloudredhat

Description: A forum post advertises 150 allegedly high-quality (UHQ) Hotmail email:password credential pairs. The content of the post is unavailable, but the thread title and forum context indicate a combo list offering. These credentials are not attributed to a breach of Microsoft or Hotmail directly.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-150x-uhq-hotmails`

[260] Sale of discounted Quizlet Plus subscription access

Date: 2026-05-19T15:56:17Z | **Category:** Services | **Actor:** wavesub

Description: A forum seller is offering Quizlet Plus one-year subscriptions at $30, significantly below the retail price of $96. The post advertises full platform features and instructs buyers to DM for account access. This likely involves account sharing or resale of compromised/bulk-purchased credentials.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Supreme-%E2%9D%84%EF%B8%8F%E2%9D%84%EF%B8%8F%E2%9D%84%EF%B8%8FQuizlet-Plus-%E2%80%93-Unlimited-Learning-1-Year-%E2%9A%A1%E2%9A%A1%E2%9A%A1`

[261] Sale of discounted CodeRabbit Pro subscriptions on cracking forum

Date: 2026-05-19T15:56:01Z | **Category:** Services | **Actor:** wavesub

Description: A forum seller is offering CodeRabbit Pro one-year subscriptions at $80, discounted from the stated retail price of $300. The post advertises AI code review features and directs buyers to DM for access. The nature of how these subscriptions are obtained is not disclosed.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Supreme-CodeRabbit-Pro-%E2%80%93-AI-Code-Review-1-Year`

[262] Combo list of Hotmail credentials offered for free

Date: 2026-05-19T15:54:38Z | **Category:** Combo List | **Actor:** UniqueCombo

Description: A threat actor is distributing a Hotmail credential combo list containing approximately 25,000 email and password pairs via a hidden forum post. The actor also advertises a shop offering combo lists for various countries and on request. The named service is a credential-stuffing target, not the breach source.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://demonforums.net/Thread-Email-Pass-Hotmail-Unique-Combo-5-25000`

[263] Sale of Hotmail credential combo list sample (700 entries)

Date: 2026-05-19T15:53:41Z | **Category:** Combo List | **Actor:** HollowKnight07

Description: A forum user shared a sample combo list containing 700 Hotmail credentials. The post includes a download link. These credentials are likely intended for credential stuffing against Hotmail/Outlook accounts.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://crackingx.com/threads/75787/`

[264] Sale of UHQ mixed credential combo list including Hotmail

Date: 2026-05-19T15:53:23Z | **Category:** Combo List | **Actor:** noir

Description: A threat actor is offering a mixed combo list advertised as valid UHQ credentials including Hotmail accounts. The list is distributed via a private cloud link promoted through Telegram. No specific victim organization or record count is disclosed.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://crackingx.com/threads/75788/`

[265] Combo List: 92 HQ Hotmail credentials shared for free

Date: 2026-05-19T15:53:16Z | **Category:** Combo List | **Actor:** altitude

Description: A threat actor shared a combo list of 92 alleged high-quality Hotmail credentials via MediaFire. The post advertises the credentials as HQ, suggesting they have been tested or verified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://altenens.is/threads/92-hq-hotmail.2942741/unread`

[266] Alleged data breach of sman1gondang.com

Date: 2026-05-19T15:49:49Z | **Category:** Data Breach | **Actor:** DarkMafiaX

Description: A threat actor is distributing a SQL database dump purportedly from sman1gondang.com, an Indonesian school website. The 30MB dump contains user records including usernames, bcrypt-hashed passwords, email addresses, IP addresses, and name fields. The data is shared as hidden content requiring forum engagement to access.

Target Context: Organization: *SMAN 1 Gondang* | Industry: *Education* | Country: *Indonesia*

Source URL: `http://pwnfrm7rbf6kyerigxi677lcz5ifmoagdbqqknwdu2by27wfdst5qmqd.onion/Thread-DATABASE-Database-Of-The-Site-sman1gondang-com-Indonesia`

[267] Alleged data leak of Calo app supply chain and suppliers database

Date: 2026-05-19T15:48:58Z | **Category:** Data Leak | **Actor:** hon3ypot

Description: A threat actor known as hon3ypot claims to have leaked the full supply chain and suppliers database of Calo (calo.app) following failed negotiations. The data has been made available for free download via an external file hosting link. The post suggests a prior extortion attempt was unsuccessful before public disclosure.

Target Context: Organization: *Calo* | Industry: *Technology* | Country: *Unknown*

Source URL: `http://pwnfrm7rbf6kyerigxi677lcz5ifmoagdbqqknwdu2by27wfdst5qmqd.onion/Thread-DATABASE-calo-app-supply-chain-suppliers-data`

[268] Alleged data leak of calo.app supply chain and suppliers data

Date: 2026-05-19T15:48:36Z | **Category:** Data Leak | **Actor:** hon3ypot

Description: A threat actor operating under the handle hon3ypot has leaked what they claim to be the full supply chain and suppliers database of calo.app. The post states the release follows failed negotiations, suggesting a prior extortion attempt. The data is made available as a downloadable archive via an external file-sharing link.

Target Context: Organization: *Calo* | Industry: *Technology* | Country: *Unknown*

Source URL: `https://darkforums.su/showthread.php?tid=77103`

[269] Alleged data leak of PDI Health (pdihealth.com) — 897GB medical records

Date: 2026-05-19T15:48:16Z | **Category:** Data Leak | **Actor:** MDGhost

Description: A threat actor known as MDGhost has leaked approximately 897GB of data allegedly sourced from PDI Health, a U.S.-based mobile diagnostic imaging provider. The exposed data reportedly includes highly sensitive patient fields such as full name, date of birth, SSN, patient number, address, contact details, and email. The organization operates under HIPAA regulations and serves patients across 15 states including residents of long-term care facilities and correctional institutions.

Target Context: Organization: *PDI Health (Preventive Diagnostics)* | Industry: *Healthcare* | Country: *United States*

Source URL: `https://breached.st/threads/897gb-pdihealth-com-pdi-health-preventive-diagnostics.87382/unread`

[270] Mass Defacement of oguild.com by Threat Actor Zod

Date: 2026-05-19T15:31:04Z | **Category:** Defacement | **Actor:** Zod, Zod

Description: On May 19, 2026, threat actor Zod conducted a mass defacement attack targeting oguild.com, a domain associated with online gaming or guild communities. The attack was confirmed as part of a mass defacement campaign, with a mirror of the defaced page archived at haxor.id. No specific motivation or technical exploitation details were disclosed.

Target Context: Organization: *OGuild* | Industry: *Gaming / Online Communities* | Country: *Unknown*

Source URL: `https://haxor.id/archive/mirror/249400`

[271] Carding activity discussion on Dread forum

Date: 2026-05-19T15:28:54Z | **Category:** Chatter | **Actor:** UV_lightScanPassMONEY_ 🍼

Description: A forum post on Dreads Carders board references multiple countries (US, UK, AU, EU, CA, NZ) in what appears to be fragmented carding-related content. The post is largely incoherent but references spending activity, consistent with carding solicitation. No specific victim, dataset, or actionable details are present.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion/post/f70124179773fd9aa61a`

[272] Mass defacement of arhat.rewarity.com by threat actor Zod

Date: 2026-05-19T15:28:35Z | **Category:** Defacement | **Actor:** Zod, Zod

Description: On May 19, 2026, a threat actor operating under the alias Zod conducted a mass defacement campaign targeting arhat.rewarity.com, replacing the content of the page at /zod.html. The incident is classified as a mass defacement, indicating multiple sites were likely targeted in the same operation. A mirror of the defacement was archived via haxor.id.

Target Context: Organization: *Rewarity* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://haxor.id/archive/mirror/249399`

[273] Alleged combo list of mixed European accounts

Date: 2026-05-19T15:20:58Z | **Category:** Combo List | **Actor:** AiCombo

Description: A combo list of approximately 29,497 email:password credentials described as private Full Access (FA) Europa mix has been shared on a cracking forum. The dataset appears to target mixed European accounts. No additional context or victim organization is specified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-29-497-Private-FA-Europa-Mix-Combo`

[274] Combo List of 28,290 Email:Password Credentials

Date: 2026-05-19T15:20:41Z | **Category:** Combo List | **Actor:** AiCombo

Description: A combo list containing 28,290 email and password credential pairs was shared on a cracking forum. The credentials are marketed as private, fresh, and verified (good line). No specific victim organization or service was identified in the post.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-28-290-Private-FA-Good-Line-Fresh`

[275] Combo list of 770K credentials shared on cracking forum

Date: 2026-05-19T15:20:16Z | **Category:** Combo List | **Actor:** MetaCloud3

Description: A threat actor known as MetaCloud3 is distributing a combo list of approximately 770,000 email:password credentials on a cracking forum. The list is described as a private base advertised as suitable for use against any target. No specific victim organization is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-%E2%9A%A1770K-FELITFE-BALLBUSTING-CC%E2%9A%A1PRIVATE-BASE-GOOD-ON-ANY-TARGET%E2%9A%A1`

[276] Mail access combo list mix shared on cracking forum

Date: 2026-05-19T15:19:55Z | **Category:** Combo List | **Actor:** Spam4LY

Description: A threat actor shared a combo list labeled Mail access valid mix #4 on a cracking forum. The post contains no additional details regarding the source, record count, or targeted services.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-Mail-access-valid-mix-4`

[277] Free combo list with 1,855 mixed credentials

Date: 2026-05-19T15:17:13Z | **Category:** Combo List | **Actor:** Nulled07

Description: A threat actor shared a combo list containing 1,855 mixed credentials, marketed as fresh. The content is hidden behind a registration or login wall on the forum.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://leakforum.io/Thread-Leak-%E2%9A%A1%E2%9A%A1-1855x-FRESH-MIX-%E2%9A%A1%E2%9A%A1--20957`

[278] Mix Mail Combo List Free Share

Date: 2026-05-19T15:16:54Z | **Category:** Combo List | **Actor:** klyne05

Description: A threat actor shared a mixed mail combo list on a leak forum, marketed as private and fresh, and checked by the poster. Content is hidden behind a registration/like wall, limiting visibility into record count or targeted services.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://leakforum.io/Thread-Leak-%E2%9A%A1%E2%9A%A1MIX-MAIL%E2%9A%A1%E2%9A%A1PRIVATE%E2%9A%A1%E2%9A%A1FRESH%E2%9A%A1%E2%9A%A1CHEKED-BY-klyne05-%E2%9A%A1%E2%9A%A1--20958`

[279] Hotmail credential combo list sample shared on forum

Date: 2026-05-19T15:15:11Z | **Category:** Combo List | **Actor:** HollowKnight

Description: A forum user shared a sample combo list of 890 Hotmail email and password pairs on a combolist forum. The content is hidden behind registration or login. This is a credential stuffing resource, not a breach of Hotmail or Microsoft.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://demonforums.net/Thread-Email-Pass-%E2%9A%A1%E2%9A%A1-890x-SAMPLE-HOTMAIL-%E2%9A%A1%E2%9A%A1--204761`

[280] Alleged data leak of Universität des Saarlandes student database

Date: 2026-05-19T15:14:28Z | **Category:** Data Leak | **Actor:** StrikerDE

Description: A threat actor claims to have breached the Universität des Saarlandes and is freely distributing the full student database after failed ransom negotiations. The leaked archive reportedly contains Moodle user records for approximately 42,000 students. The actor threatens further university targets if their demands are not met.

Target Context: Organization: *Universität des Saarlandes* | Industry: *Education* | Country: *Germany*

Source URL: `http://pwnfrm7rbf6kyerigxi677lcz5ifmoagdbqqknwdu2by27wfdst5qmqd.onion/Thread-DATABASE-DE-Universit%C3%A4t-des-Saarlandes-42k-students-breached`

[281] Alleged free data leak with unspecified content

Date: 2026-05-19T15:13:57Z | **Category:** Data Leak | **Actor:** chechnyafsbc

Description: A forum user posted a thread titled FREEBIES MORE FRESH DATA TODAY on a dark web forum, claiming to share free data. The post contains no substantive content beyond a link prompt, with no details about the victim, data type, or record count.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://darkforums.su/showthread.php?tid=77096`

[282] Alleged data breach of American Income Life Insurance Company

Date: 2026-05-19T14:59:33Z | **Category:** Data Breach | **Actor:** pm_rasel

Description: A threat actor is selling an alleged database dump from American Income Life Insurance Company containing approximately 151,000 records. The dataset includes personally identifiable information such as names, phone numbers, emails, dates of birth, insured addresses, policy numbers, annualized premiums, death benefit amounts, and policy status fields. The data structure indicates exposure of sensitive insurance policyholder records.

Target Context: Organization: *American Income Life Insurance Company* | Industry: *Finance* | Country: *United States*

Source URL: `https://breachforums.rs/Thread-SELLING-American-Income-Life-Insurance-Company-www-ailife-com`

[283] Sale of initial access to undisclosed Italian manufacturing company via VPN (OpenVPN)

Date: 2026-05-19T14:56:37Z | **Category:** Initial Access | **Actor:** CocoMel0n

Description: A threat actor is selling VPN (OpenVPN) access with Database Admin (SA) privileges to an undisclosed Italian manufacturing company with an estimated revenue of $5M–$10M and a network of approximately 50 hosts. No AV or EDR was detected on the target. The access is listed at $708 (0.00832608 BTC) and was verified within the last 72 hours.

Target Context: Organization: *Unknown* | Industry: *Manufacturing* | Country: *Italy*

Source URL: `https://breachforums.rs/Thread-VPN-VPN-OpenVPN-Manufacturing-Italy-5M-10M-revenue`

[284] Sale of SSH Root Access to Ukrainian E-Commerce Cosmetics Platform

Date: 2026-05-19T14:56:10Z | **Category:** Initial Access | **Actor:** Obey_Your_Master

Description: A threat actor is selling exclusive SSH root access to a Linux server hosting a Ukrainian e-commerce and wholesale cosmetics platform with estimated annual revenue of $100K–$300K. The access is described as persistent and includes live customer databases, order records, and payment gateway integrations. The seller is asking $200 in Monero and requires use of an official forum escrow service.

Target Context: Organization: *Unknown* | Industry: *Retail* | Country: *Ukraine*

Source URL: `https://breachforums.rs/Thread-SELLING-SSH-Root-Access-E-Commerce-Cosmetics-Wholesale-Ukraine-100K-Reven`

[285] Sale of stolen credit cards with CVV and cardholder data across multiple countries

Date: 2026-05-19T14:54:30Z | **Category:** Carding | **Actor:** HighWayToShell

Description: A threat actor is selling 2,400 stolen credit cards including Mastercard, Visa, and Discover cards with CVV, cardholder name, and expiration date. Cards are attributed to multiple issuing banks including Citibank, Wells Fargo, ANZ Bank, Royal Bank of Canada, Chase, and NatWest, spanning multiple countries. Batches are offered for sale via direct message or an external storefront.

Target Context: Organization: *Unknown* | Industry: *Finance* | Country: *Unknown*

Source URL: `https://xforums.st/threads/selling-cc-cvv-holder-name-exp.615502/`

[286] Alleged data breach of Russian and Belarusian industrial B2B marketplace

Date: 2026-05-19T14:54:11Z | **Category:** Data Breach | **Actor:** Obey_Your_Master

Description: A threat actor is selling an alleged database dump from an unnamed Russian and Belarusian industrial B2B marketplace, containing approximately 961,264 rows across multiple tables. The dataset reportedly includes customer personal data (names, emails, phone numbers), corporate registry details (INN, KPP, OGRN, bank account data), B2B lead logs, contracts, billing records, and financial transaction histories. The data is claimed to be fresh, with entries dated up to December 2025.

Target Context: Organization: *Unknown* | Industry: *Retail* | Country: *Unknown*

Source URL: `https://breachforums.rs/Thread-SELLING-BY-RU-Industrial-B2B-E-Commerce-Marketplace-DB-Fresh-Dec-2025-960K-Total`

[287] Sale of FortiSSL IP list with geolocation data

Date: 2026-05-19T14:53:36Z | **Category:** Services | **Actor:** AccessTracker

Description: A threat actor is offering a list of 50,000 FortiSSL IP addresses with geolocation data, claimed to be gathered via proprietary mass-scanning infrastructure rather than third-party sources such as Shodan or FOFA. The data is formatted as IP and geo pairs and is gated behind a post-count requirement. This type of data is typically used to identify potentially vulnerable Fortinet SSL VPN endpoints.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://tier1.life/thread/247`

[288] Free South Korea Email Combo List (Batch 49/100)

Date: 2026-05-19T14:52:09Z | **Category:** Combo List | **Actor:** emaildbpro

Description: A threat actor is freely distributing a batch of South Korea-focused email credentials, labeled as batch 49 of 100. The content is gated behind forum registration or login. No specific victim organization or record count is disclosed.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://patched.to/Thread-file-upload-free-premium-south-korea-email-list-batch-49-100`

[289] Sale of Hotmail credential combo list

Date: 2026-05-19T14:51:33Z | **Category:** Combo List | **Actor:** RespectSentai

Description: A forum user is sharing 950 Hotmail credential lines described as fresh. The content is hidden behind a registration or login wall. No specific breach victim or organization is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://patched.to/Thread-file-upload-x950-hotmail-fresh-lines`

[290] Combo List targeting Crunchyroll accounts

Date: 2026-05-19T14:50:53Z | **Category:** Combo List | **Actor:** mrglitchxxxx

Description: A threat actor shared a combo list of approximately 14,000 credentials marketed as fresh Crunchyroll account hits. The list is being distributed for free via a hidden download link requiring forum registration. This is a credential stuffing list targeting Crunchyroll and does not represent a breach of the platform itself.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://patched.to/Thread-file-upload-14k-fresh-crunchyroll-combolist`

[291] Sale of Hotmail credential combo list with 812 valid accounts

Date: 2026-05-19T14:50:18Z | **Category:** Combo List | **Actor:** SupportHotmail

Description: A threat actor shared a combo list containing 812 claimed valid Hotmail credentials, marketed as active access. The post references a Telegram bot and appears to be a free or promotional distribution of the credentials.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://patched.to/Thread-file-upload-%E2%9C%A8%F0%9F%94%A5812-hotmail-valid-access-19-05-2026`

[292] Sale of Hotmail credential combo list with 507 valid accounts

Date: 2026-05-19T14:49:57Z | **Category:** Combo List | **Actor:** SupportHotmail

Description: A threat actor is distributing a combo list of 507 alleged valid Hotmail credentials, marketed as active access dated May 19, 2026. The content is hidden behind a registration or login wall on the forum.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://patched.to/Thread-file-upload-%E2%9C%A8%F0%9F%94%A5507-hotmail-valid-access-19-05-2026`

[293] Alleged data leak of Canadian beauty salon business database

Date: 2026-05-19T14:49:45Z | **Category:** Data Leak | **Actor:** Vyntra

Description: A threat actor has freely shared a database claiming to contain 1 million+ records of beauty salon and cosmetics businesses from Canada and international regions. The dataset reportedly includes business names, phone numbers, email addresses, physical addresses, website links, and related metadata. The post markets the data for email marketing, lead generation, and B2B outreach purposes.

Target Context: Organization: *Unknown* | Industry: *Health & Beauty* | Country: *Canada*

Source URL: `https://breachforums.rs/Thread-Canada-Beauty-Saloon-1M-Database-Free`

[294] Hotmail combo list of 1,464 credentials shared on forum

Date: 2026-05-19T14:49:40Z | **Category:** Combo List | **Actor:** stevee

Description: A user shared a combo list of 1,464 Hotmail credentials on a public forum. The content is gated behind registration or login. No breach of a specific organization is claimed.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://patched.to/Thread-file-upload-%E2%9A%A1%E2%9A%A1-x1464-hq-hotmail-%E2%9A%A1%E2%9A%A1-by-stevee36-%E2%9A%A1%E2%9A%A1`

[295] Sale of initial access to undisclosed Brazilian municipal government entity

Date: 2026-05-19T14:49:04Z | **Category:** Initial Access | **Actor:** HighWayToShell

Description: A threat actor is selling RDWeb access with Server Admin privileges to an undisclosed Brazilian municipal government organization with an estimated revenue of $250M–$500M and a network of approximately 10,000+ hosts. The access is protected by Bitdefender GZ and was verified within the last 48 hours. Payment is requested in Bitcoin.

Target Context: Organization: *Unknown* | Industry: *Government* | Country: *Brazil*

Source URL: `https://xforums.st/threads/rdweb-government-municipal-brazil-250m-500m-revenue.615500/`

[296] Combo List distributed via Telegram channel

Date: 2026-05-19T14:48:36Z | **Category:** Combo List | **Actor:** ULPTXT

Description: A user shared a ULP (URL:Login:Password) combo list dated 19-05-26 via a Telegram channel. No specific victim organization or record count was disclosed.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Other-ULP-TXT-LOG-19-05-26`

[297] Combo List of 236K credentials shared on cracking forum

Date: 2026-05-19T14:48:16Z | **Category:** Combo List | **Actor:** Cloudredhat

Description: A combo list of approximately 236,000 URL:login:password (ULP) credentials was shared on a cracking forum. The post markets the list as private and UHQ (ultra-high quality). No specific victim organization or targeted service was identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Other-236K-ULP-PRIVATE-UHQ`

[298] Sale of RedLine Stealer Logs

Date: 2026-05-19T14:47:47Z | **Category:** Logs | **Actor:** FATHER121

Description: A forum user is offering RedLine stealer logs described as fresh and paid. The post references 2,756 full logs from the RedLine infostealer. No further details are available from the post content.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-REDLINEVIP-FRESH-PAID-STEALER-FULL-LOGS-2756`

[299] Sale of mixed stealer logs by FATETRAFFIC

Date: 2026-05-19T14:47:27Z | **Category:** Logs | **Actor:** R0BIN1337

Description: A forum user shared a collection of 4,705 mixed stealer logs attributed to FATETRAFFIC. No additional details about the source, targeted organizations, or geographic distribution were provided in the post.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-FATETRAFFIC-4705-MIX-Logs`

[300] Sale of mixed European combolist with 32,131 credentials

Date: 2026-05-19T14:46:48Z | **Category:** Combo List | **Actor:** AiCombo

Description: A forum member shared a mixed European combo list containing approximately 32,131 email:password credential pairs. The post is categorized as a private full-access combolist, suggesting it may be offered for sale or restricted distribution. No specific victim organization or breach source is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-32-131-Private-FA-Europa-Mixed-Combolist`

[301] Combo list of 618K Hotmail/Outlook/MSN/Live credentials shared on cracking forum

Date: 2026-05-19T14:46:28Z | **Category:** Combo List | **Actor:** MetaCloud3

Description: A threat actor operating under the alias MetaCloud3 has shared a combo list of approximately 618,000 Hotmail, Outlook, MSN, and Live email credentials on a cracking forum. The post markets the list as a private base suitable for credential stuffing against any target.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-%E2%9A%A1618K-HOTMAIL-OUTLOOK-MSN-LIVE%E2%9A%A1PRIVATE-BASE-GOOD-ON-ANY-TARGET%E2%9A%A1`

[302] Sale of Hotmail combo list with 2,000 credentials

Date: 2026-05-19T14:46:16Z | **Category:** Combo List | **Actor:** MeiMisakix

Description: A forum post advertises a Hotmail combo list containing approximately 2,000 credentials. No post content was available; details are inferred from the thread title. The named service is a credential-stuffing target, not a breach victim.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://leakforum.io/Thread-Leak-2K-HOTMAIL-ACCESS`

[303] Sale of 787K mail access combo list

Date: 2026-05-19T14:46:07Z | **Category:** Combo List | **Actor:** MetaCloud3

Description: A threat actor is distributing a combo list of approximately 787,000 email address and password pairs, marketed as high quality, private, and sourced from dehashed lines. The post advertises the credentials as fresh and unique, suitable for mail access credential stuffing.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-%E3%80%8C-787K-%E3%80%8D%E2%9A%A1MAIL-ACCESS%E2%9A%A1HIGH-QUALITY-PRIVATE-COMBO%E2%9A%A1DEHASHED-LINES%E2%9A%A1FRESH-AND-UNIQUE%E2%9A%A1`

[304] Combo List: Private Europe Mix Email/Password Combo (17,214 Records)

Date: 2026-05-19T14:45:41Z | **Category:** Combo List | **Actor:** AiCombo

Description: A combo list containing 17,214 email and password pairs described as a private Europe mix full access (FA) combo was shared on a cracking forum. The dataset appears to be a credential collection sourced from multiple breaches targeting European accounts. No specific victim organization or service is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-17-214-Private-FA-Europa-Mix-Combo`

[305] Forum announcement or meta-post with no content available

Date: 2026-05-19T14:45:21Z | **Category:** Chatter | **Actor:** HugBunter

Description: A post by user HugBunter on the Dread forum contains no available content. No threat indicators or actionable intelligence can be extracted from this post.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion/post/eef5045e643fb743b8f1/?context=df7fec0f2dd4e8e87e#c-df7fec0f2dd4e8e87e`

[306] Combo list of 236K credentials shared on cracking forum

Date: 2026-05-19T14:45:12Z | **Category:** Combo List | **Actor:** Cloudredhat

Description: A threat actor shared a combo list advertised as 236K UHQ (ultra-high quality) email:password credentials on a cracking forum. No additional details about the source or targeted services are available from the post content.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-236K-UHQ-ULP-PRIVATE`

[307] Sale of Hotmail combo list with 707 credentials

Date: 2026-05-19T14:44:51Z | **Category:** Combo List | **Actor:** LordOfSea91

Description: A forum user shared a combo list of 707 Hotmail credentials, marketed as Hydra hits. The post offers no further technical details about the datas origin or verification status.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-707x-HYDRA-HOTMAIL`

[308] Sale of 151K EDU-targeted combo list

Date: 2026-05-19T14:44:42Z | **Category:** Combo List | **Actor:** Ra-Zi

Description: A threat actor is offering a 151,000-record combo list targeting EDU accounts, advertised as high quality with EMAIL:PASS and USER:PASS formats. The list includes credentials spanning multiple countries and email providers including AOL, Yahoo, Hotmail, and Outlook. The actor is selling via Telegram and promoting an associated cracking service website.

Target Context: Organization: *Unknown* | Industry: *Education* | Country: *Unknown*

Source URL: `https://demonforums.net/Thread-151K-EDU-TARGETED-COMBOLIST--204750`

[309] Combo List of 785K Facebook and Instagram credentials

Date: 2026-05-19T14:44:32Z | **Category:** Combo List | **Actor:** MetaCloud3

Description: A threat actor is distributing a combo list of approximately 785,000 email and password pairs reportedly sourced from Facebook and Instagram accounts. The post markets the credentials as a private base suitable for use against any target. No specific breached organization is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-%E2%9A%A1785K-FACEBOOK-INSTAGRAM%E2%9A%A1PRIVATE-BASE-GOOD-ON-ANY-TARGET%E2%9A%A1--2096254`

[310] Gmail combo list of 24 million credentials freely shared

Date: 2026-05-19T14:44:08Z | **Category:** Combo List | **Actor:** RogenPlay

Description: A threat actor has freely shared a combo list advertised as containing 24 million Gmail credentials, marketed as freshly checked. This is a credential stuffing list and does not represent a breach of Gmail itself.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-%E2%9C%85-%E2%9C%85-%E2%9C%85-%E2%9C%A824M-Gmail-Combolist-1-%E2%9C%A8-Freshly-Checked-%E2%9C%A8-%E2%9C%85-%E2%9C%85-%E2%9C%85`

[311] Free distribution of Raccoon Stealer v2 logs from Mexico

Date: 2026-05-19T14:43:16Z | **Category:** Logs | **Actor:** HighWayToShell

Description: A threat actor is freely distributing 2,500 Raccoon Stealer v2 logs sourced from Mexican victims running Windows Server 2022. The logs contain credentials and cookies harvested via Chrome 120.x. The post includes a download link and password for access.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Mexico*

Source URL: `https://xforums.st/threads/ulp-raccoon-stealer-v2-2500-logs-mx-windows-server-2022.615501/`

[312] Sale of FUD Sender Pro bulk email and phishing delivery tool

Date: 2026-05-19T14:42:57Z | **Category:** Phishing | **Actor:** imi_jav1995

Description: A threat actor is selling FUD Sender Pro, a desktop-based bulk email sender supporting SMTP and API delivery, HTML/image/PDF payloads, and randomized personalization tags. The tool is marketed for bulk and personalized email campaigns and supports Mailgun and Brevo APIs, consistent with phishing or spam delivery infrastructure. The seller is advertising via Telegram handle office_365shop.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://crackingx.com/threads/75780/`

[313] Free Hotmail combo list publicly released by Dragonvit (Part 2)

Date: 2026-05-19T14:42:36Z | **Category:** Combo List | **Actor:** Vitdragon

Description: A threat actor known as Dragonvit publicly released a Hotmail combo list as a free drop on a cracking forum. The post includes a contact for purchasing additional services such as software, proxies, RDP, and private traffic. No record count was specified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-%E2%9A%A1-HOTMAILS-PUBLIC-DROP-BY-DRAGONVIT-%E2%9A%A1-Part-2`

[314] Public release of Hotmail combo list by DragonVit (Part 3)

Date: 2026-05-19T14:42:16Z | **Category:** Combo List | **Actor:** Vitdragon

Description: A threat actor known as Vitdragon/DragonVit has publicly released a Hotmail credential combo list as part of an ongoing series. The post advertises additional services including proxies, RDP, and private traffic. No record count or specific victim organization is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-%E2%9A%A1-HOTMAILS-PUBLIC-DROP-BY-DRAGONVIT-%E2%9A%A1-Part-3`

[315] Combo list of Hotmail credentials shared freely

Date: 2026-05-19T14:42:08Z | **Category:** Combo List | **Actor:** Kommander0

Description: A threat actor known as Kommander0 has freely shared a combo list containing approximately 941 Hotmail credentials, marketed as fully valid. The list was made available via an external file-sharing link.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://crackingx.com/threads/75772/`

[316] Public combo list drop by threat actor Dragonvit (Part 67)

Date: 2026-05-19T14:41:56Z | **Category:** Combo List | **Actor:** Vitdragon

Description: Threat actor Vitdragon publicly released a corporate combo list drop (Part 67) on a cracking forum. The post advertises email:password credentials and additional services including proxies, RDP, and private traffic. No specific victim organization or record count was disclosed.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-%E2%9A%A1-%C2%A0%C2%A0CORP-PUBLIC-DROP-BY-DRAGONVIT-%E2%9A%A1-Part-67`

[317] Sale of Hotmail credential combo list

Date: 2026-05-19T14:41:50Z | **Category:** Combo List | **Actor:** RandomUpload

Description: A forum user is sharing a combo list of approximately 3,003 Hotmail credentials described as fresh and valid. The content is restricted to registered users. This appears to be a credential stuffing resource targeting Hotmail accounts.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://crackingx.com/threads/75773/`

[318] Free combo list drop by threat actor Dragonvit

Date: 2026-05-19T14:41:37Z | **Category:** Combo List | **Actor:** Vitdragon

Description: Threat actor Dragonvit publicly released a combo list (email:password pairs) labeled as HOTS on a cracking forum. The post is part of a recurring series and includes advertisements for additional services such as private traffic, proxies, RDP, and software. No specific victim organization or record count was disclosed.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-%E2%9A%A1-%C2%A0-HOTS%C2%A0-PUBLIC-DROP-BY-DRAGONVIT-%E2%9A%A1-Part-1488`

[319] Sale of Hotmail credential combo list

Date: 2026-05-19T14:41:33Z | **Category:** Combo List | **Actor:** Hotmail Cloud

Description: A threat actor is distributing 1,287 alleged Hotmail credential hits via a download link on a cracking forum. The credentials are marketed as premium hits, suggesting they have been tested and verified against Hotmail accounts. No additional details about the source of the credentials were provided.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://crackingx.com/threads/75774/`

[320] Sale of Office combo list (1 million credentials)

Date: 2026-05-19T14:41:19Z | **Category:** Combo List | **Actor:** CODER

Description: A threat actor is offering a combo list of 1 million credentials allegedly usable for Microsoft Office/Office 365 credential stuffing. The post directs interested parties to a Telegram account and two associated Telegram groups advertising free combos and tools.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://crackingx.com/threads/75775/`

[321] Free Hotmail combo list publicly released by Dragonvit

Date: 2026-05-19T14:41:13Z | **Category:** Combo List | **Actor:** Vitdragon

Description: A threat actor operating as Dragonvit has publicly released a Hotmail email:password combo list on a cracking forum. The post includes a download link for a file dated May 2026 and advertises additional services including proxies, RDP, and private traffic.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-%E2%9A%A1-HOTMAILS-PUBLIC-DROP-BY-DRAGONVIT-%E2%9A%A1-Part-1`

[322] Sale of alleged WordPress credentials or database dump

Date: 2026-05-19T14:40:57Z | **Category:** Combo List | **Actor:** zod

Description: A forum post on CX references WordPress-related content, with access gated behind registration and a password shared via a Telegram channel. The actual content is not visible; no further details about record count, specific victims, or data types are available.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://crackingx.com/threads/75781/`

[323] Combo List: Mixed Email Access Credentials (80,000 records)

Date: 2026-05-19T14:40:53Z | **Category:** Combo List | **Actor:** ACE_XD

Description: A threat actor on Cracked.st is distributing a mixed email combo list containing approximately 80,000 email:password credential pairs. The post appears to offer free access to the credentials based on the forum context. No specific victim organization or breach source is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-80000x%E2%9A%A1MIX-MAIL%E2%9A%A1ACCESS%E2%9A%A1`

[324] Germany Mixed Target Combo List (832,303 Lines)

Date: 2026-05-19T14:40:33Z | **Category:** Combo List | **Actor:** HqComboSpace

Description: A combo list of 832,303 email:password lines targeting German (.de) accounts across mixed services has been shared on a cracking forum. The list is marketed as a mixed-target credential collection for Germany. No specific victim organization is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-832-303-Lines-%E2%9C%85-Germany-de-Combolist-Mixed-Target`

[325] Combo List: 3.1K Mixed Mail Access Credentials

Date: 2026-05-19T14:40:13Z | **Category:** Combo List | **Actor:** Cloudredhat

Description: A combo list containing approximately 3,100 mixed mail access credentials was shared on a cracking forum. The post appears to offer email and password pairs for various mail providers. No additional details about the source or origin of the credentials are available.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-3-1K-MIX-MAIL-ACCESS`

[326] Sale of 280K USA combo list

Date: 2026-05-19T14:39:53Z | **Category:** Combo List | **Actor:** AstroBella

Description: A threat actor is distributing a combo list containing approximately 280,000 email:password credential pairs purportedly sourced from US users. The post markets the credentials as fresh and previously unused. No specific victim organization or breach source is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-280K-USA-COMBOLIST-%E2%9C%94%EF%B8%8F-UNRAPED-AND-FRESH-LINES-%E2%9C%94%EF%B8%8F19-5-26`

[327] Request for French IBAN bank account

Date: 2026-05-19T14:39:38Z | **Category:** Chatter | **Actor:** Bendhash 🍼

Description: A forum user is seeking to purchase a fresh French IBAN bank account, requesting safe escrow for the transaction. No further details are provided.

Target Context: Organization: *Unknown* | Industry: *Finance* | Country: *France*

Source URL: `https://dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion/post/87f875bad041aba55830`

[328] Sale of European combo list mix

Date: 2026-05-19T14:39:33Z | **Category:** Combo List | **Actor:** AiCombo

Description: A combo list containing approximately 24,358 email and password pairs described as a private European mix has been shared on a cracking forum. The post is categorized as full access (FA) credentials targeting European accounts. No specific victim organization or service is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-24-358-Private-FA-Europa-Mix-Combo`

[329] Mixed combo list publicly released by threat actor Dragonvit

Date: 2026-05-19T14:39:11Z | **Category:** Combo List | **Actor:** Vitdragon

Description: A threat actor known as Vitdragon publicly released a mixed email:password combo list on a cracking forum. The post advertises additional services including proxies, RDP, traffic, and software. No specific victim organization or record count is disclosed.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-%E2%9A%A1-%C2%A0-MIXED-PUBLIC-DROP-BY-DRAGONVIT-%E2%9A%A1-Part-1`

[330] Mix email combo list with 59K credentials

Date: 2026-05-19T14:38:51Z | **Category:** Combo List | **Actor:** Mei_Misaki

Description: A threat actor is distributing a mixed email and password combo list containing approximately 59,000 credential pairs. The post offers a download link with no additional details about the source or target services.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-59K-MIX-MAIL-ACCESS`

[331] Combo List: 10K UHQ Mixed Mail Access Credentials

Date: 2026-05-19T14:38:32Z | **Category:** Combo List | **Actor:** Cloudredhat

Description: A combo list of 10,000 mixed mail access credentials described as UHQ (ultra high quality) was shared on a cracking forum. The post contains no additional details about the source or targeted services.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-10K-UHQ-MIX-MAIL-ACCESS`

[332] Combo List: 251K Hotmail credentials shared on forum

Date: 2026-05-19T14:38:10Z | **Category:** Logs | **Actor:** ValidMail

Description: A threat actor shared a combo list containing approximately 251,000 Hotmail domain credentials, marketed as valid as of May 19, 2026. The post requires forum registration to access the content. This appears to be a credential stuffing list targeting Hotmail accounts.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://xforums.st/threads/251k-hotmail-domain-with-valid-19-05-26.615498/`

[333] Combo list targeting Yahoo domain with 1.685 million credentials

Date: 2026-05-19T14:38:04Z | **Category:** Combo List | **Actor:** HqComboSpace

Description: A threat actor shared a combo list containing approximately 1.685 million email:password lines targeting Yahoo domain accounts. The credentials are intended for credential-stuffing activity against Yahoo-domain email accounts. No breach of Yahoo is implied; the list is aggregated from external sources.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-1-685-469-Lines-%E2%9C%85-Combolist-Target-Yahoo-Domain`

[334] Combo List targeting France

Date: 2026-05-19T14:37:38Z | **Category:** Combo List | **Actor:** FlightUSA

Description: A user on a cracking forum has shared what appears to be a French email:password combo list. The post requests users not to leech, suggesting free distribution to registered members. No further details about record count or source are provided.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-FRANCE--2096310`

[335] Sale of European combo list with 55,004 credentials

Date: 2026-05-19T14:37:04Z | **Category:** Combo List | **Actor:** AiCombo

Description: A threat actor on Cracked forum is sharing a private combo list of 55,004 email:password pairs reportedly sourced from European accounts. The post is marketed as FA (full access) quality. No specific victim organization or service is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-55-004-Private-FA-Combolist-Europa-Good--2096294`

[336] Alleged combo list targeting European accounts

Date: 2026-05-19T14:36:41Z | **Category:** Combo List | **Actor:** AiCombo

Description: A combo list containing approximately 35,363 email:password pairs purportedly targeting European accounts has been shared on a cracking forum. The post is categorized as a private combo list marketed as high quality. No additional details are available from the post content.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-35-363-Private-FA-Combolist-Europa-Good`

[337] Sale of mixed email:password combo list with 29,905 records

Date: 2026-05-19T14:36:20Z | **Category:** Combo List | **Actor:** GirlCrew

Description: A threat actor shared a mixed email:password combo list containing 29,905 records on a cracking forum. The post is categorized as mail access credentials. No additional details are available from the post content.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Email-Pass-29-905-mixed-Combolist-Mail-Pass-Mail-Access`

[338] 130K USA Combo List

Date: 2026-05-19T14:36:01Z | **Category:** Combo List | **Actor:** AstroBella

Description: A threat actor is distributing a combo list of approximately 130,000 email and password pairs purportedly sourced from US-based accounts. The credentials are marketed as fresh and unused. No specific victim organization or service is identified.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *United States*

Source URL: `https://cracked.st/Thread-Email-Pass-130K-USA-COMBOLIST-%E2%9C%94%EF%B8%8F-UNRAPED-AND-FRESH-LINES-%E2%9C%94%EF%B8%8F19-5-26`

[339] Carding inquiry: converting fraudulent prepaid Visa/Mastercard gift card to cryptocurrency

Date: 2026-05-19T14:35:38Z | **Category:** Chatter | **Actor:** budzy653

Description: A forum user is seeking advice on how to fraudulently purchase a $500 AUD prepaid Visa/Mastercard gift card from card.gift and convert it to cryptocurrency (BTC/USDT) before the anticipated fraudulent transaction dispute is filed. The user is asking about anonymization techniques (VPN usage, avoiding tracking) and methods to cash out via a crypto.com account. The post indicates awareness that the transaction will trigger a fraud dispute, suggesting deliberate payment fraud.

Target Context: Organization: *Unknown* | Industry: *Finance* | Country: *Australia*

Source URL: `https://dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion/post/86b5ca7f7ed543e3684d`

[340] Sale of unauthorized premium media streaming service (Plex/Emby/Jellyfin shares)

Date: 2026-05-19T14:35:29Z | **Category:** Services | **Actor:** qstrm

Description: A forum seller is advertising a paid media streaming service offering Plex, Emby, and Jellyfin shares with access to a claimed library of 30,000+ movies, 20,000+ TV shows, and additional audiobook and ebook content. The service is priced at $10 USD per month and is likely distributing unlicensed media content. No specific victim organization or breach is involved.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Supreme-QUANTUM-STREAMS-EMBY-JELLYFIN-PLEX-SHARES-2PB-LIBRARY`

[341] Sale of discounted Mobbin Pro subscription access

Date: 2026-05-19T14:34:57Z | **Category:** Services | **Actor:** wavesub

Description: A forum seller is offering discounted Mobbin Pro design reference library subscriptions (1-year access) at reduced prices via direct message. The post advertises Pro and Team plan tiers significantly below retail pricing. No breach or compromised data is involved.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Supreme-%E2%AD%90%E2%AD%90%E2%AD%90Mobbin-Pro-%E2%80%93-Design-Reference-Library-1-Year-%E2%9C%A8%E2%9C%A8%E2%9C%A8`

[342] Sale of discounted Granola AI meeting notes subscription

Date: 2026-05-19T14:34:40Z | **Category:** Services | **Actor:** wavesub

Description: A forum seller is offering a one-year Granola AI meeting notes subscription for $30, discounted from the retail price of $120. The seller claims to provide access to the buyers account via direct message. It is unclear whether the subscriptions are legitimate, resold, or obtained through unauthorized means.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Supreme-%E2%9D%84%EF%B8%8F%E2%9D%84%EF%B8%8F%E2%9D%84%EF%B8%8FGranola-%E2%80%93-AI-Meeting-Notes-1-Year-%E2%9A%A1%E2%9A%A1%E2%9A%A1`

[343] Sale of discounted TryHackMe subscription access

Date: 2026-05-19T14:34:20Z | **Category:** Services | **Actor:** wavesub

Description: A forum user is offering discounted TryHackMe 1-year subscription plans at $50–$60, significantly below the stated retail price of $168. The seller instructs buyers to DM for account access, suggesting resale of obtained credentials or vouchers. No specific victim organization or breach is claimed.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Supreme-%E2%9A%A1%E2%9A%A1%E2%9A%A1TryHackMe-%E2%80%93-Learn-Cybersecurity-1-Year-%E2%9C%A8%E2%9C%A8%E2%9C%A8`

[344] Combo List targeting Hotmail with 25,000 credentials

Date: 2026-05-19T14:34:11Z | **Category:** Logs | **Actor:** UniqueCombo

Description: A combo list purportedly containing 25,000 unique Hotmail credentials was shared on a cybercrime forum. The post content is minimal but the thread title indicates the list is marketed as unique. This is a credential stuffing resource, not a breach of Microsoft or Hotmail directly.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://xforums.st/threads/hotmail-unique-combo_4_25000.615499/`

[345] Sale of discounted N8N automation service subscription

Date: 2026-05-19T14:34:01Z | **Category:** Services | **Actor:** wavesub

Description: A forum seller is offering discounted N8N workflow automation service subscriptions at $50/year, reduced from a claimed retail price of $180/year. The post advertises features including 400+ app integrations, visual workflow builder, and cloud hosting. Buyers are directed to DM the seller for account access.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Supreme-%E2%9C%A8%E2%9C%A8%E2%9C%A8N8N-Starter-%E2%80%94-Automate-Everything-Manually-Do-Nothing-%E2%9A%A1%E2%9A%A1%E2%9A%A1`

[346] Sale of discounted Magic Pattern design tool subscription

Date: 2026-05-19T14:33:43Z | **Category:** Services | **Actor:** wavesub

Description: A forum seller is offering discounted annual subscriptions to Magic Pattern, an AI-powered design tool, at $40/year versus the retail price of $144/year. The seller claims access is granted via DM and advertises unlimited downloads of AI-generated patterns, UI components, and SVG exports. This appears to be a resale or shared-account service.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Supreme-%E2%9D%84%EF%B8%8F%E2%9D%84%EF%B8%8F%E2%9D%84%EF%B8%8FMagic-Pattern-%E2%80%94-Designs-That-Make-People-Stop-Scrolling%E2%9A%A1%E2%9A%A1%E2%9A%A1`

[347] Sale of Gamma Pro subscription service at discounted price

Date: 2026-05-19T14:33:26Z | **Category:** Services | **Actor:** wavesub

Description: A forum user is advertising discounted Gamma Pro (AI presentation software) subscriptions at $60/year, compared to the retail price of $192/year. The seller claims to provide access via DM on the buyers account. This appears to be an unauthorized resale or shared account service.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Supreme-Gamma-Pro-%E2%80%94-Presentations-That-Sell-Themselves`

[348] Sale of NFA combo lists with free test offered

Date: 2026-05-19T14:33:06Z | **Category:** Combo List | **Actor:** Cloudredhat

Description: A threat actor is advertising high-quality NFA (No Further Action) combo lists for sale, offering a free test sample prior to purchase. The post directs interested buyers to a Telegram contact for further details.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-NFA-COMBO-FOR-YOUR-TARGET-WITH-TEST-FIRST`

[349] Sale of discounted Manus AI subscription access

Date: 2026-05-19T14:32:47Z | **Category:** Services | **Actor:** wavesub

Description: A forum seller is offering discounted Manus AI annual subscriptions at $120/year, advertised against a retail price of $480/year. The seller claims to provide access to the autonomous AI agent service via the buyers account. The nature of the discounted access (e.g., whether accounts are legitimate or compromised) is not specified in the post.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Supreme-%E2%9C%A8%E2%9C%A8%E2%9C%A8Manus-AI-%E2%80%94-Work-Smart-Not-Hard-Most-people-work-10-hours-a-day-%E2%9D%84%EF%B8%8F%E2%9D%84%EF%B8%8F%E2%9D%84%EF%B8%8F`

[350] Sale of Windows RDP/VM hosting service on cracking forum

Date: 2026-05-19T14:32:29Z | **Category:** Services | **Actor:** ScottPilgrim

Description: A forum user is selling access to a Windows RDP/Virtual Machine with 16 vCores AMD EPYC, 32GB RAM, and ~600GB storage for $25. The listing explicitly permits credential-stuffing tools such as OpenBullet with proxies. The seller advertises the service via Telegram.

Target Context: Organization: *Unknown* | Industry: *Unknown* | Country: *Unknown*

Source URL: `https://cracked.st/Thread-Supreme-Powerful-Windows-RDP-VM-16-vCores-AMD-EPYC-32GB-RAM-25`

6. Mitigation Strategies & Strategic Recommendations

To effectively counter the diverse and industrialized threats documented in this intelligence report, organizations must adopt a proactive, defense-in-depth security posture. We recommend implementing the following strategic controls:

- **Defeating Credential Stuffing & ATO:** Organizations must enforce robust Multi-Factor Authentication (MFA) across all external-facing employee and customer portals. Implement

adaptive authentication, rate-limiting, and CAPTCHA mechanisms to disrupt automated credential testing bots. Continually check employee credentials against known compromised databases.

- **Securing Web Infrastructure:** Actively maintain patch management programs for all web assets, specifically targeting CMS platforms (WordPress, Joomla) and third-party plugins. Enforce strict directory permissions, restrict file uploads, and utilize Web Application Firewalls (WAF) to block SQL injection and cross-site scripting (XSS) attempts.
- **Combating Infostealers & Session Hijacking:** Traditional MFA can be bypassed if an infostealer captures an active session cookie. Organizations should implement session binding techniques, reduce session timeouts, and utilize endpoint detection and response (EDR) agents to detect and block infostealer execution on corporate devices.
- **Threat Intelligence & Monitoring:** Proactively monitor dark web forums, Telegram channels, and clear web cracking sites for mentions of corporate assets, leaked credentials, or active targeting by Initial Access Brokers. Early detection of compromised assets allows for rapid password resets and token invalidation before severe exploitation occurs.

7. Conclusion

The intelligence derived from these 829 threads underscores a highly sophisticated, commoditized cybercrime ecosystem. The low barrier to entry for utilizing combo lists and the immense profitability of data extortion drive a persistent high volume of attacks. Combating these threats requires organizations to transcend perimeter-only defenses, embedding continuous threat intelligence and identity-centric security directly into their operational frameworks.