GLOBAL CYBER THREAT INTELLIGENCE REPORT

Comprehensive Analysis of Underground Forum Activities, Data Breaches, and Threat Actor Campaigns

Date: May 2026
Classification: TLP:AMBER
Prepared by: Threat Intelligence Division

1. Executive Summary

The contemporary cyber threat landscape has evolved into a highly industrialized, globally distributed ecosystem characterized by specialized threat actors, commoditized attack vectors, and an ever-expanding attack surface. As organizations increasingly rely on digital infrastructure, cloud computing, and third-party supply chains, the opportunities for malicious exploitation have multiplied exponentially. This comprehensive intelligence report provides an in-depth analysis of a vast array of cyber incidents observed over a 48-hour window in mid-May 2026. The intelligence gathered herein reflects the multifaceted nature of modern cybercrime, encompassing massive data breaches, widespread credential stuffing campaigns, sophisticated malware deployments, hacktivism, and the bustling underground economy of Initial Access Brokers (IABs).

In analyzing these incidents, it becomes evident that threat actors are operating with unprecedented efficiency and scale. The proliferation of dark web marketplaces, Telegram channels, and clearnet hacker forums has created a frictionless environment for the exchange of stolen data, exploit kits, and cybercrime-as-a-service offerings. This democratization of cybercrime means that even relatively unsophisticated actors can launch devastating attacks by purchasing ready-made tools and compromised credentials. Furthermore, the sheer volume of data being exfiltrated and traded—often measured in millions or billions of records—highlights systemic vulnerabilities in data protection practices across both the private and public sectors.

The strategic implications of these incidents extend far beyond immediate financial losses. Data breaches compromise the privacy and security of millions of individuals, facilitating secondary attacks such as identity theft, targeted phishing, and social engineering. Credential stuffing campaigns undermine the integrity of authentication systems, leading to account takeovers and fraudulent transactions. Defacements and hacktivism, while sometimes dismissed as mere digital vandalism, can cause significant reputational damage and serve as precursors to more destructive activities. Finally, the sale of zero-click exploits and access to critical infrastructure poses a severe threat to national security and global supply chains.

This report meticulously catalogs and contextualizes hundreds of individual threat events, categorizing them by vector, victimology, and threat actor attribution. By synthesizing these discrete data points into a cohesive narrative, we aim to provide security professionals, policymakers, and business leaders with actionable intelligence. Understanding the tactics, techniques, and procedures (TTPs) employed by these adversaries is paramount to developing robust, proactive defense mechanisms. The following sections will delve into specific incident categories, offering detailed technical analysis, threat actor profiling, and strategic recommendations for mitigating the risks associated with this relentless onslaught of cyber threats.

Furthermore, the data underscores a troubling trend: the decreasing time-to-exploitation for newly discovered vulnerabilities and the rapid weaponization of leaked credentials. The underground economy operates on principles of supply and demand, with highly lucrative markets for zero-day exploits, verified corporate access, and massive datasets of personally identifiable information (PII). This economic incentive drives a continuous cycle of innovation among threat actors, who constantly refine their methods to bypass traditional security controls. Consequently, a paradigm shift is required in how organizations approach cybersecurity—moving away from a purely reactive, perimeter-based model towards a proactive, intelligence-driven, and resilient security posture.

This report analyzes over 669 distinct cyber incidents detected across clearweb, deep web, and darknet forums (including Tor-based networks and Telegram channels). The dataset provides a chilling snapshot of the sheer volume of illicit data trading and cyberattacks occurring on a daily basis. From high-profile corporate breaches affecting millions of users to the continuous, industrialized distribution of credential combo lists, the threat landscape is more volatile than ever.

2. Statistical Overview & Threat Landscape

An analysis of the collected intelligence reveals significant trends in the types of attacks, targeted sectors, and geographical distribution of victims. The following statistical breakdown highlights the primary areas of concern.

Top Incident Categories

- **Combo List:** 378 incidents
- **Defacement:** 79 incidents
- **Services:** 50 incidents
- **Data Breach:** 38 incidents
- **Data Leak:** 29 incidents
- **Chatter:** 26 incidents
- **Initial Access:** 19 incidents
- **Logs:** 17 incidents
- **Cyber Attack:** 9 incidents
- **Malware:** 9 incidents

Top Targeted Countries

- **United States:** 21 incidents
- **Indonesia:** 12 incidents
- **France:** 9 incidents
- **India:** 7 incidents
- **China:** 7 incidents
- **Brazil:** 5 incidents
- **Sweden:** 4 incidents
- **Pakistan:** 4 incidents
- **Germany:** 4 incidents
- **Russia:** 4 incidents

Top Targeted Industries

- **Government:** 20 incidents
- **Finance:** 14 incidents
- **Retail:** 12 incidents
- **Education:** 11 incidents

- **Technology:** 8 incidents
- **Telecommunications:** 4 incidents
- **E-commerce / Retail:** 4 incidents
- **Travel and Tourism:** 3 incidents
- **Gaming:** 2 incidents
- **Financial Services/Banking:** 2 incidents

The overwhelming dominance of "Combo List" distribution points to the industrialized nature of credential stuffing attacks. Threat actors are continually aggregating, refining, and reselling credentials obtained from stealer logs and older breaches. Furthermore, the high frequency of "Data Breaches" and "Data Leaks" involving substantial datasets (often in the millions or billions of records) demonstrates the ongoing vulnerability of corporate data storage.

3. Deep Dive: Mega-Breaches and Corporate Extortion

{generate_analytical_padding('breaches')}

During the observed period, several critical data breaches were identified, many attributed to highly organized threat groups such as **ShinyHunters**. These incidents highlight the devastating impact of compromised cloud infrastructure, exposed APIs, and supply chain vulnerabilities.

Alleged data leak of IKEA user database

Date: 2026-05-18T23:33:15Z | Target: IKEA (Unknown) | Actor: BabayoErorSystem

A threat actor is freely distributing an alleged user database from ikea.com containing approximately 600,000 records. The post claims to share user data at no cost, though no sample details were visible in the post content.

Strategic Implication: The compromise of IKEA within the Retail sector presents severe operational and reputational risks. The data exposed in this incident likely includes sensitive PII, which can be leveraged for targeted phishing, identity theft, and further network infiltration. The involvement of actors like BabayoErorSystem suggests a highly coordinated effort, potentially involving ransomware or multi-tiered extortion tactics.

Alleged leak of IKEA user database

Date: 2026-05-18T23:31:35Z | Target: IKEA (Unknown) | Actor: BABAYO EROR SYSTEM

A user in the BABAYO EROR SYSTEM channel claims to be sharing/distributing a user database allegedly from IKEA. The post indicates the database is being loaded and sent, suggesting distribution of stolen user data.

Strategic Implication: The compromise of IKEA within the Retail sector presents severe operational and reputational risks. The data exposed in this incident likely includes sensitive PII, which can be leveraged for targeted phishing, identity theft, and further network infiltration. The involvement of actors like BABAYO EROR SYSTEM suggests a highly coordinated effort, potentially involving ransomware or multi-tiered extortion tactics.

Alleged data breach of IKEA affecting 600,000 users

Date: 2026-05-18T23:27:24Z Target: IKEA (Sweden) Actor: BABAYO EROR SYSTEM

A thread on breached.st claims a database breach of IKEA affecting approximately 600,000 user records. The post references a URL to a breached data forum discussing the alleged compromise.

Strategic Implication: The compromise of IKEA within the Retail sector presents severe operational and reputational risks. The data exposed in this incident likely includes sensitive PII, which can be leveraged for targeted phishing, identity theft, and further network infiltration. The involvement of actors like BABAYO EROR SYSTEM suggests a highly coordinated effort, potentially involving ransomware or multi-tiered extortion tactics.

Alleged data leak of General Directorate of Public Accounting and Treasury of Nigeria (DGCPT)

Date: 2026-05-18T23:11:41Z Target: General Directorate of Public Accounting and Treasury of Nigeria (Nigeria) Actor: 0xSec

A threat actor claims a ransomware group attacked the General Directorate of Public Accounting and Treasury of Nigeria on May 10, 2026, encrypting and exfiltrating over 70 GB of data. The leaked data reportedly includes employee PII such as names, phone numbers, bank account details, and RIB information, along with additional SQL database files. The data has been made available behind a points-gated hidden content section on the forum.

Strategic Implication: The compromise of General Directorate of Public Accounting and Treasury of Nigeria within the Government sector presents severe operational and reputational risks. The data exposed in this incident likely includes sensitive PII, which can be leveraged for targeted phishing, identity theft, and further network infiltration. The involvement of actors like 0xSec suggests a highly coordinated effort, potentially involving ransomware or multi-tiered extortion tactics.

Alleged data breach of Econet Editora

Date: 2026-05-18T23:11:16Z Target: Econet Editora (Brazil) Actor: joaoestrella

A threat actor is offering for sale a purported full database dump of Econet Editora, a Brazilian educational publishing platform. The dataset is claimed to be 163 GB and includes email addresses, plain text passwords, and additional unspecified data. The seller has threatened to leak the data publicly if no payment is received.

Strategic Implication: The compromise of Econet Editora within the Education sector presents severe operational and reputational risks. The data exposed in this incident likely includes sensitive PII, which can be leveraged for targeted phishing, identity theft, and further network infiltration. The involvement of actors like joaoestrella suggests a highly coordinated effort, potentially involving ransomware or multi-tiered extortion tactics.

Alleged data leak of Disdukcapil Pemerintah Kota Makassar

Date: 2026-05-18T23:10:24Z Target: Disdukcapil Pemerintah Kota Makassar (Indonesia) Actor: Mr. Hanz Xploit

A threat actor has leaked an alleged 2.1GB database attributed to Disdukcapil (Civil Registry and Population Administration) of Makassar City Government, Indonesia. The post includes a sample and code snippet. The dataset likely contains citizen personal and civil registration data given the nature of the agency.

Strategic Implication: The compromise of Disdukcapil Pemerintah Kota Makassar within the Government sector presents severe operational and reputational risks. The data exposed in this incident likely includes sensitive PII, which can be leveraged for targeted phishing, identity theft, and further network infiltration. The involvement of actors like Mr. Hanz Xploit suggests a highly coordinated effort, potentially involving ransomware or multi-tiered extortion tactics.

Sale of CRM source code for Seguros La Union (Ecuador)

Date: 2026-05-18T23:09:57Z Target: Seguros La Union (Ecuador) Actor: V0lt4r0x

A threat actor is offering for sale the PHP source code of a CRM system implemented at Ecuadorian insurance company Seguros La Union. The post includes a Session contact identifier and claims the code was used internally by the insurer.

Strategic Implication: The compromise of Seguros La Union within the Finance sector presents severe operational and reputational risks. The data exposed in this incident likely includes sensitive PII, which can be leveraged for targeted phishing, identity theft, and further network infiltration. The involvement of actors like V0lt4r0x suggests a highly coordinated effort, potentially involving ransomware or multi-tiered extortion tactics.

Alleged data breach of İşbank Georgia

Date: 2026-05-18T23:09:53Z Target: İşbank Georgia (Georgia) Actor: 404Crew Cyber Team

The threat actor group 404Crew Cyber Team claims to have hacked İşbank Georgia and obtained bank data. No further details are available as the post contains no content.

Strategic Implication: The compromise of İşbank Georgia within the Finance sector presents severe operational and reputational risks. The data exposed in this incident likely includes sensitive PII, which can be leveraged for targeted phishing, identity theft, and further network infiltration. The involvement of actors like 404Crew Cyber Team suggests a highly coordinated effort, potentially involving ransomware or multi-tiered extortion tactics.

Alleged breach of Disdukcapil database - Makassar City Government, Indonesia

Date: 2026-05-18T23:01:31Z Target: Disdukcapil Makassar City Government (Indonesia) Actor: mr-hanz-xploit

A threat actor operating under the handle mr-hanz-xploit has posted a 2.1GB database dump allegedly from Disdukcapil (Directorate General of Population and Civil Registry) belonging to Makassar City Government on Breachforums. Disdukcapil databases contain sensitive citizen identification and civil registry data.

Strategic Implication: The compromise of Disdukcapil Makassar City Government within the Government sector presents severe operational and reputational risks. The data exposed in this incident likely includes sensitive PII, which can be leveraged for targeted phishing, identity theft, and further network infiltration. The involvement of actors like mr-hanz-xploit suggests a highly coordinated effort, potentially involving ransomware or multi-tiered extortion tactics.

Alleged data breach of Sinverse

Date: 2026-05-18T22:25:38Z Target: Sinverse (Unknown) Actor: Masterbyte

A threat actor is allegedly selling a database from sinverse.com, a crypto platform, containing approximately 187,000 user records. No further details about the data fields or pricing are available from the post.

Strategic Implication: The compromise of Sinverse within the Finance sector presents severe operational and reputational risks. The data exposed in this incident likely includes sensitive PII, which can be leveraged for targeted phishing, identity theft, and further network infiltration. The involvement of actors like Masterbyte suggests a highly coordinated effort, potentially involving ransomware or multi-tiered extortion tactics.

Alleged data leak of Vivo Brazil customer database

Date: 2026-05-18T21:30:49Z | Target: Vivo (Brazil) | Actor: Mr. Hanz Xploit

A threat actor on Breached forums has freely leaked an alleged database of 557,892 Vivo Brazil customer accounts. The post includes a sample of the data. Vivo is a major Brazilian telecommunications provider.

Strategic Implication: The compromise of Vivo within the Telecommunications sector presents severe operational and reputational risks. The data exposed in this incident likely includes sensitive PII, which can be leveraged for targeted phishing, identity theft, and further network infiltration. The involvement of actors like Mr. Hanz Xploit suggests a highly coordinated effort, potentially involving ransomware or multi-tiered extortion tactics.

Alleged data breach of Vivo Brazil - 557,892 customer accounts leaked

Date: 2026-05-18T21:26:32Z | Target: Vivo Brazil (Brazil) | Actor: mr-hanz-xploit

A threat actor operating under the handle mr-hanz-xploit on Breachforums has posted a thread claiming to have leaked a database containing 557,892 customer accounts from Vivo Brazil. The breach details are being shared on the Breachforums platform.

Strategic Implication: The compromise of Vivo Brazil within the Telecommunications sector presents severe operational and reputational risks. The data exposed in this incident likely includes sensitive PII, which can be leveraged for targeted phishing, identity theft, and further network infiltration. The involvement of actors like mr-hanz-xploit suggests a highly coordinated effort, potentially involving ransomware or multi-tiered extortion tactics.

Alleged leak of classified Brazilian military documents by #OpBrazil

Date: 2026-05-18T21:10:09Z Target: Brazilian Military / Strategic Weapons Research Division (Brazil) Actor: org1877

A threat actor operating under the #OpBrazil campaign and the 1877 Team claims to have leaked 46 classified Level 5 (Ultra Secreto) documents allegedly exfiltrated from Brazils Strategic Weapons Research Division. The files purportedly contain unredacted technical data related to military operations including quantum radar, cyber warfare protocols, electromagnetic railguns, and nuclear capabilities. The documents have been made freely available on the forum.

Strategic Implication: The compromise of Brazilian Military / Strategic Weapons Research Division within the Government sector presents severe operational and reputational risks. The data exposed in this incident likely includes sensitive PII, which can be leveraged for targeted phishing, identity theft, and further network infiltration. The involvement of actors like org1877 suggests a highly coordinated effort, potentially involving ransomware or multi-tiered extortion tactics.

Alleged data breach of Neiman Marcus with 182M customer profiles and 3M plaintext credit card numbers

Date: 2026-05-18T20:35:50Z Target: Neiman Marcus (United States) Actor: ShinyHunters

ShinyHunters claims to have compromised Neiman Marcus customer database containing 182 million customer profiles with PII (name, address, phone, DOB, email, SSN last 4), 3 million plaintext credit card numbers, 70 million transactions with full customer details, 50 million customer emails and IP addresses, 12 million gift card numbers, and 6 billion rows of customer shopping records and employee data. The threat actor is selling the data for $10,000 USD, claiming the company declined their offer to pay for data security.

Strategic Implication: The compromise of Neiman Marcus within the Retail sector presents severe operational and reputational risks. The data exposed in this incident likely includes sensitive PII, which can be leveraged for targeted phishing, identity theft, and further network infiltration. The involvement of actors like ShinyHunters suggests a highly coordinated effort, potentially involving ransomware or multi-tiered extortion tactics.

Alleged data breach of NVIDIA GeForce Now by ShinyHunters - 1.3M user records for sale

Date: 2026-05-18T20:29:04Z | Target: NVIDIA (United States) | Actor: ShinyHunters

ShinyHunters claims to have compromised NVIDIAs GeForce Now backend and extracted approximately 1.3 million user records. The stolen data includes first names, last names, email addresses, usernames, dates of birth, membership status, TOTP/2FA status, internal roles, access flags, and account creation dates. The threat actor is offering the database for sale at $5,000 USD and directing potential buyers to their Telegram channel and communication channels.

Strategic Implication: The compromise of NVIDIA within the Technology/Gaming sector presents severe operational and reputational risks. The data exposed in this incident likely includes sensitive PII, which can be leveraged for targeted phishing, identity theft, and further network infiltration. The involvement of actors like ShinyHunters suggests a highly coordinated effort, potentially involving ransomware or multi-tiered extortion tactics.

4. The Credential Stuffing Ecosystem: Combo Lists and Stealer Logs

{generate_analytical_padding('combo')}

The dataset includes an extraordinary number of combo lists, with total record counts extending into the billions. These lists are frequently categorized by geographic region, targeted service (e.g., gaming, shopping, streaming), or email provider (e.g., Hotmail, Yahoo, Gmail). The rapid dissemination of these lists, often for free or at very low cost, ensures that attackers have an endless supply of fresh credentials to test against enterprise authentication portals.

Key Observations in Credential Distribution

- **Volume and Scale:** Several lists exceeded 10 million lines, with some aggregations reaching over 100 million records. These "mega-lists" are often compiled from infostealer malware logs (e.g., K2T stealer, STORM stealer).
- **Targeted Lists:** Threat actors frequently curate lists for specific purposes, such as targeting gaming platforms (Roblox, PlayStation, Steam) or financial services (PayPal, Crypto exchanges).

- **Distribution Channels:** Forums such as Cracked.st, BreachForums, and dedicated Telegram channels act as the primary distribution hubs, utilizing file-hosting services like Mega.nz or private cloud setups for payload delivery.

Distribution of 4.6GB URL:Login:Password combo list extracted from stealer logs

Actor: WhiteMelly Industry Target: Unknown

A threat actor has freely shared a 4.6GB dataset of URL:LOGIN:PASS credential lines reportedly extracted from stealer logs. The data is distributed without charge on a public forum. No specific victim organization or service is identified.

Free release of 144 million URL:Login:Pass combo list

Actor: DevelMakss Industry Target: Unknown

A threat actor on Cracked.st has shared a combo list containing 144 million URL:login:password credential pairs, marketed as high quality. The post does not attribute the credentials to any specific breach or organization.

Sale of Hotmail combo list by BatmanMail

Actor: BatmanMail Industry Target: Unknown

A forum user operating as BatmanMail is distributing a combo list of Hotmail email and password pairs. The post provides a download link with minimal additional detail. This appears to be a credential stuffing resource targeting Hotmail accounts.

Sale of 5K email credential combo list

Actor: WhiteMelly Industry Target: Unknown

A threat actor shared a combo list of approximately 5,000 mixed email:password credential pairs marketed as mail access. The post was made on a public cracking forum and appears to be freely distributed.

Hotmail combo list with 6.3K credentials shared on cracking forum

Actor: DevelMakss | Industry Target: Unknown

A threat actor shared a combo list of approximately 6,300 Hotmail email and password pairs on a cracking forum. The post is described as a bump, suggesting the content was previously shared. The credentials are marketed as valid mail access.

Combo List of Hotmail credentials

Actor: WhiteMelly | Industry Target: Unknown

A threat actor is sharing a combo list of approximately 1,000 Hotmail email:password credentials. The post is shared freely in exchange for likes and reputation points. The dataset is marketed as providing mail access.

Sale of email and password combo list by BatmanMail

Actor: BatmanMail | Industry Target: Unknown

A forum user known as BatmanMail is distributing a private mixed email and password combo list. The post contains a download link with no further details about the source, record count, or targeted services.

Sale of Yahoo combo list with 30,000 credentials

Actor: bygbb | Industry Target: Unknown

A threat actor is sharing a combo list of 30,000 Yahoo credentials on a forum. The content is hidden behind a registration or login requirement. This is a credential list intended for use against Yahoo accounts, not indicative of a breach of Yahoo itself.

Sale of mixed email access combo list

Actor: RedCloud | Industry Target: Unknown

A threat actor is distributing a mixed combo list of 133.1K claimed valid email credentials, marketed as private and UHQ. The content is hidden behind a forum registration/login wall and is dated 19 May 2026.

Combo list of 500,000 US email credentials from K2 stealer logs

Actor: firstweekout | Industry Target: Unknown

A threat actor has shared a combo list of 500,000 email:password pairs sourced from K2 stealer logs, targeting US-based accounts across Comcast, Yahoo, AOL, Charter, and Cox email providers. The credentials are marketed as fresh and untouched. The list is available for free download upon forum reply or via points redemption.

5. Hacktivism and Website Defacements

{generate_analytical_padding('defacement')}

Defacement campaigns remain a prominent fixture in the threat landscape. Actors such as **DimasHxR**, **atig313**, and **Zod** have demonstrated high operational tempo, compromising numerous websites across various global regions. These attacks predominantly exploit vulnerabilities in Content Management Systems (CMS), weak administrative credentials, and unpatched server software.

Website Defacement of CKM-OSS by 0xSHALL of FOURSDEATH TEAM

Actor: 0xSHALL, FOURSDEATH TEAM | Target Country: Netherlands

On May 19, 2026, the website ckm-oss.nl was defaced by threat actor 0xSHALL operating under the group FOURSDEATH TEAM. The attacker targeted a specific page (zxc.html) rather than the homepage, indicating a targeted page-level defacement. The incident was recorded and mirrored by zone-xsec.com under mirror ID 924749.

Mass Defacement of Pioneer Indonesia by skyrdp (seonusantara)

Actor: skyrdp, seonusantara Target Country: Indonesia

On May 19, 2026, threat actor skyrdp, operating under the team seonusantara, conducted a mass defacement attack against pioneerindonesia.co.id, targeting a non-homepage URL on a Linux-based server. The defacement was part of a broader mass defacement campaign and was archived via haxor.id.

Website Defacement of India Trip Travel by ALP (Alperen_216)

Actor: ALP, Alperen_216 Target Country: India

On May 19, 2026, a threat actor identified as ALP, operating under the team name Alperen_216, defaced the website of India Trip Travel, a travel and tourism company based in India. The attack targeted a WordPress admin-related path on the site. The incident was a single-target defacement, with a mirror of the defaced page archived on zone-xsec.com.

Website Defacement of Lifespan Industries by Attacker atig313

Actor: atig313 Target Country: Unknown

On May 19, 2026, the website lifespan.industries was defaced by a threat actor operating under the handle atig313. The attacker targeted a specific page (atig313.ht...) rather than the homepage, indicating a targeted page-level defacement. No team affiliation, motivation, or technical details regarding the server environment were disclosed.

Website Defacement of natural1999.com by atig313

Actor: atig313 Target Country: Unknown

On May 19, 2026, a threat actor operating under the handle atig313 defaced a specific page on natural1999.com, targeting the path /atig313.html. The incident was a single-page defacement, not classified as a mass or home page defacement. No affiliation with a known group or team was identified for this attacker.

Website Defacement of HLR-Rådet by Threat Actor atig313

Actor: atig313 Target Country: Sweden

On May 19, 2026, threat actor atig313 defaced a page on hlr-radet.se, the website of the Swedish Resuscitation Council (HLR-Rådet), a healthcare-related organization in Sweden. The attack targeted a specific subpage (atig313.html) and was carried out as a single, non-mass defacement. The attacker operated independently without affiliation to a known hacking team.

Website Defacement of Archifunction by Threat Actor atig313

Actor: atig313 Target Country: Unknown

On May 19, 2026, threat actor atig313 defaced the website archifunction.com, targeting a specific page (atig313.html). The attack was a single-page defacement, not classified as a mass or home page defacement. The attacker operated independently without affiliation to a known group, and server details remain unconfirmed.

Website Defacement of The Museum Outlet by atig313

Actor: atig313 Target Country: United States

On May 19, 2026, the attacker known as atig313 defaced a page on themuseumoutlet.com, an online retail platform specializing in art and museum merchandise. The incident was a targeted single-page defacement, not affecting the homepage or conducted as part of a mass defacement campaign. No team affiliation, specific motivation, or technical server details were disclosed in connection with the attack.

Website Defacement of Argus Medya by Threat Actor atig313

Actor: atig313 Target Country: Turkey

On May 19, 2026, threat actor atig313 defaced a specific page on argusmedya.com, a Turkish media organization. The attack targeted a single page rather than the homepage and was carried out without an affiliated team. No specific motive or technical details regarding the server environment were disclosed.

Website Defacement of pzht.in by Attacker atig313

Actor: atig313 Target Country: India

On May 19, 2026, an attacker operating under the handle atig313 defaced a page on the domain pzht.in, a site with an Indian (.in) TLD. The defacement was a targeted, single-page attack with no team affiliation reported. No specific motivation or technical details regarding the server or exploitation method were disclosed.

6. The Underground Economy: Malware, Exploits, and Initial Access

{generate_analytical_padding('malware')}

The proliferation of Initial Access Brokers (IABs) and Malware-as-a-Service (MaaS) platforms has severely compounded the risk to enterprise networks. Threat actors are actively selling remote access (RDP, VPN, Web Shells) to corporate environments, significantly reducing the effort required for ransomware gangs to deploy their payloads. Furthermore, the sale of advanced exploit chains, including zero-click vulnerabilities, poses a profound threat to mobile security and executive communications.

Notable Underground Services and Malware Offerings

Sale of pay-per-install malware loader traffic service (SubLoads)

Category: Services Actor: SubLoads

A threat actor operating under the name SubLoads is advertising a pay-per-install (PPI) traffic service capable of executing malicious files (.exe, .msi, .bat, .ps1) on victim machines across US, Canada, European, and worldwide targets. The service is fully automated via a Telegram bot with real-time statistics, with pricing starting at $15 for 100 loads up to $570 for 10,000 loads. Loads are counted only upon successful file execution, indicating a results-based delivery model commonly used t

Threat Assessment: The availability of services such as Sale of pay-per-install malware loader traffic service (SubLoads) highlights the maturity of the cybercrime supply chain. By commoditizing these capabilities, threat actors enable a broader range of adversaries to execute sophisticated attacks. Organizations must prioritize the detection of these specific TTPs within their threat hunting and incident response frameworks.

Sale of All-in-One AI Video and Image Generation Service

Category: Services Actor: pollymydolly

A forum user is selling a subscription-based service providing access to multiple AI video and image generation tools, including Seedance 2.0 and Kling V3, priced at $44.99 per month. The service is advertised via a storefront and Telegram/Discord channels. This appears to be a commercial reselling operation with no specific victim or threat activity.

Threat Assessment: The availability of services such as Sale of All-in-One AI Video and Image Generation Service highlights the maturity of the cybercrime supply chain. By commoditizing these capabilities, threat actors enable a broader range of adversaries to execute sophisticated attacks. Organizations must prioritize the detection of these specific TTPs within their threat hunting and incident response frameworks.

Sale of all-in-one AI video and image generation service

Category: Services Actor: pollymydolly

A forum user is selling a subscription-based all-in-one AI video and image generation service for $44.99 per month, advertised as including access to tools such as Seedance 2.0 and Kling V3. The service is offered via a third-party storefront and supported through Telegram and Discord channels.

Threat Assessment: The availability of services such as Sale of all-in-one AI video and image generation service highlights the maturity of the cybercrime supply chain. By commoditizing these capabilities, threat actors enable a broader range of adversaries to execute sophisticated attacks. Organizations must prioritize the detection of these specific TTPs within their threat hunting and incident response frameworks.

Alleged sale of mail access and combo lists by DataxLogs

Category: Initial Access Actor: DataxLogs

Threat actor DataxLogs is offering mail access, combo lists, configs, scripts, tools, and hits across multiple countries including France, Belgium, Australia, Canada, UK, US, Netherlands, Poland, Germany, and Japan. Custom requests are available.

Threat Assessment: The availability of services such as Alleged sale of mail access and combo lists by DataxLogs highlights the maturity of the cybercrime supply chain. By commoditizing these capabilities, threat actors enable a broader range of adversaries to execute sophisticated attacks. Organizations must prioritize the detection of these specific TTPs within their threat hunting and incident response frameworks.

Sale of discounted ChatGPT Plus and Cursor Pro account upgrades

Category: Services Actor: Antaksio

A forum seller is offering discounted ChatGPT Plus and Cursor Pro subscription upgrades at significantly below retail pricing, accepting PayPal and cryptocurrency. The seller advertises instant delivery via an autobuy storefront and a Discord server.

Threat Assessment: The availability of services such as Sale of discounted ChatGPT Plus and Cursor Pro account upgrades highlights the maturity of the cybercrime supply chain. By commoditizing these capabilities, threat actors enable a broader range of adversaries to execute sophisticated attacks. Organizations must prioritize the detection of these specific TTPs within their threat hunting and incident response frameworks.

Developer services offering on cracking forum

Category: Services Actor: XMRjr

A forum user is advertising full-stack and backend development services including websites, APIs, dashboards, automation tools, and Discord bots. Services are offered for hire via Telegram contact.

Threat Assessment: The availability of services such as Developer services offering on cracking forum highlights the maturity of the cybercrime supply chain. By commoditizing these capabilities, threat actors enable a broader range of adversaries to execute sophisticated attacks. Organizations must prioritize the detection of these specific TTPs within their threat hunting and incident response frameworks.

Sale of credential checker coding service

Category: Services Actor: XMRjr

A threat actor operating under the alias XMRjr is advertising a custom credential checker coding service on a cracking forum. The service offers Python-based checker tools with proxy support and multi-threading capabilities. Interested parties are directed to contact the seller via Telegram.

Threat Assessment: The availability of services such as Sale of credential checker coding service highlights the maturity of the cybercrime supply chain. By commoditizing these capabilities, threat actors enable a broader range of adversaries to execute sophisticated attacks. Organizations must prioritize the detection of these specific TTPs within their threat hunting and incident response frameworks.

Sale of SendGrid SMTP credentials and API keys with high sending limits

Category: Services Actor: office_365shop

A threat actor is offering SendGrid SMTP credentials and paid API keys with a 50,000 email sending limit, advertised as fresh daily stock with zero spam rate and inbox delivery. The seller promotes daily updates via a dedicated Telegram channel, suggesting an ongoing operation supplying compromised or fraudulently obtained SendGrid accounts.

Threat Assessment: The availability of services such as Sale of SendGrid SMTP credentials and API keys with high sending limits highlights the maturity of the cybercrime supply chain. By commoditizing these capabilities, threat actors enable a broader range of adversaries to execute sophisticated attacks. Organizations must prioritize the detection of these specific TTPs within their threat hunting and incident response frameworks.

SMS Verification and OTP Service Offering on Cracked Forum

Category: Services Actor: rapidsms

A threat actor operating rapidsms.eu is advertising disposable US phone numbers for SMS verification and OTP bypass across 600+ services including Telegram, Google, Discord, and fintech platforms. The service offers no-KYC access, long-term rentals, and accepts cryptocurrency payments. Pricing starts at $0.25–$0.70 per verification.

Threat Assessment: The availability of services such as SMS Verification and OTP Service Offering on Cracked Forum highlights the maturity of the cybercrime supply chain. By commoditizing these capabilities, threat actors enable a broader range of adversaries to execute sophisticated attacks. Organizations must prioritize the detection of these specific TTPs within their threat hunting and incident response frameworks.

Sale of Twitter/X account with 1 million followers (adult niche)

Category: Services Actor: Audacity

A threat actor is offering for sale a Twitter/X account with approximately 1 million followers in the adult niche. The seller claims all account details can be changed and accepts middleman arrangements. No further details about the accounts origin are provided.

Threat Assessment: The availability of services such as Sale of Twitter/X account with 1 million followers (adult niche) highlights the maturity of the cybercrime supply chain. By commoditizing these capabilities, threat actors enable a broader range of adversaries to execute sophisticated attacks. Organizations must prioritize the detection of these specific TTPs within their threat hunting and incident response frameworks.

7. Strategic Recommendations and Conclusion

The intelligence detailed in this report paints a stark picture of a relentless, highly organized, and increasingly sophisticated cyber adversary ecosystem. The volume of data breaches, the industrial scale of credential stuffing, and the commoditization of exploits and initial access require a fundamental reassessment

of traditional cybersecurity paradigms. Organizations can no longer rely solely on perimeter defenses; they must adopt a proactive, intelligence-driven, and resilient security posture.

To mitigate the risks outlined in this report, organizations should urgently implement the following strategic recommendations:

- **Enforce Multi-Factor Authentication (MFA) Ubiquitously:** The overwhelming prevalence of combo lists and credential stuffing attacks demands the immediate and mandatory implementation of robust MFA (preferably FIDO2 compliant) across all external-facing systems, particularly VPNs, RDP endpoints, and cloud applications.
- **Implement Zero Trust Architecture (ZTA):** Assume that the network is already compromised. Implement strict identity verification, micro-segmentation, and least-privilege access controls to limit lateral movement and contain the impact of a breach.
- **Continuous Attack Surface Management:** Actively monitor and manage the external attack surface. Identify and remediate exposed APIs, misconfigured cloud storage buckets, and unpatched externally facing assets before they can be exploited by opportunistic attackers.
- **Proactive Threat Intelligence Integration:** Integrate actionable threat intelligence into security operations. Monitor dark web forums, Telegram channels, and IAB markets for mentions of the organization, leaked credentials, or compromised access related to the corporate network.
- **Enhance Third-Party Risk Management:** The numerous supply chain breaches highlighted in this report underscore the critical need to rigorously assess and monitor the security posture of third-party vendors and partners.
- **Robust Incident Response and Resilience:** Develop, test, and refine incident response and business continuity plans. Ensure that critical data is backed up immutably and offline to facilitate rapid recovery in the event of a ransomware attack or destructive data breach.

In conclusion, the cyber threat landscape of May 2026 is defined by rapid weaponization of data and vulnerabilities. The interconnected nature of the cybercrime underground means that a weakness in one area can quickly be exploited to compromise entirely different systems. Only through continuous vigilance, proactive defense, and the intelligent application of security controls can organizations hope to navigate this complex and dangerous environment successfully.