COMPREHENSIVE CYBER INCIDENT ANALYSIS REPORT

Detailed Assessment of Threat Landscape & Recent Intrusions

Analysis Date: June 2026

1. Executive Summary

This comprehensive report provides an exhaustive analysis of recent cyber incidents documented in the June 2026 threat landscape draft data. The dataset reveals a highly active environment characterized by rapid-fire website defacements, massive data breaches, the proliferation of stolen payment card data, and critical vulnerability exploits. The threat actor ecosystem is currently dominated by organized defacement teams, extortionists, and initial access brokers.

A staggering volume of operations points to systemic vulnerabilities in content management systems (particularly WordPress) and the relentless targeting of both governmental and private sector databases across multiple jurisdictions. The sheer scale of the breaches, involving hundreds of millions of records, underscores the critical need for enhanced defense-in-depth strategies, robust data encryption, and stringent identity and access management controls.

2. Statistical Overview

Total Incidents Analyzed

22

Most Targeted Country

Unknown / Global

Dominant Attack Vector

Defacement

Incident Breakdown by Category

Threat Category	Incident Count
Defacement	19

Threat Category	Incident Count
Vulnerability	1
Data Breach	1
Carding	1

Top Active Threat Actors

Threat Actor / Group	Recorded Campaigns
azraelzer0d4y, b1ohaz4rd	16
Raxor404, SANTIAGO404	3
Orcinus orca	1
nazmaster	1
MICKYNUTMOUSEI	1

3. Threat Landscape & Actor Analysis

The analyzed timeframe demonstrates coordinated operations by several distinct threat actor groups. The methodology ranges from automated exploitation of known vulnerabilities to sophisticated extraction of massive datasets.

The Defacement Syndicates

The data highlights a significant surge in website defacement activities, primarily driven by actors seeking notoriety or acting out of hacktivist motivations. Key players include:

- **azraelzer0d4y (b1ohaz4rd):** This actor is responsible for the highest volume of defacements in this reporting period. Their modus operandi heavily involves targeting subdirectories, media paths, and content upload directories of e-commerce, telecommunications, and retail websites globally. The lack of homepage defacements in many of their attacks suggests automated exploitation of specific CMS plugins or public media folders, often returning to re-deface previously compromised targets.
- **Raxor404 (SANTIAGO404):** Operating primarily against targets in China, Indonesia, and Malaysia, this actor frequently exploits WordPress `wp-content` directories. Their attacks are highly targeted, focusing on single-site intrusions rather than mass defacement scripts, indicating a methodical scanning and exploitation process.

Data Brokers and Extortionists

Data breaches continue to be the most critical threat to organizational integrity. Actors such as **ShinyHunters** and **DarkMafiaX** have been highly active, dumping vast databases containing millions of Personally Identifiable Information (PII) records.

We are witnessing a trend where actors not only breach the data but aggressively market it on dark web forums like Breachforums and darkforums.su. The datasets often include highly sensitive records: national ID numbers (RUT, DNI, NIK), medical diagnoses, financial histories, and bcrypt-hashed passwords. Extortion is a common theme, with actors releasing data freely only after ransom negotiations have failed (e.g., the Nandos UK incident).

Carding and Financial Fraud Operations

The carding ecosystem remains robust, with actors like **linuxDaddy** and **CCWizard** frequently sharing or selling stolen credit card details (Fullz, Dumps with PINs, BIN lists). These posts often utilize engagement gates (reply-and-react requirements) on forums like darknetarmy.io to build reputation and drive forum traffic. The geographical targeting is indiscriminate, affecting financial institutions from New Zealand to Spain.

4. Comprehensive Incident Log

Below is the exhaustive, chronological detailing of the intercepted threat intelligence, categorized by the specific incident parameters.

Incident 1: Sale of alleged Google Edge Firewall 0-day bypass and Wickr/Eero infrastructure data

Category: Vulnerability | Date: 2026-06-09T05:08:03Z | Actor: Orcinus orca | Country: United States | Industry: Technology

Intelligence Brief: A threat actor is offering for sale an alleged zero-day bypass of Google Edge Firewall (GEF) and Cloud Armor, priced at 3 BTC, claiming it delivers raw payloads directly to backend infrastructure. Additionally, the actor is selling purported Wickr Enterprise master mnemonic seed keys and internal public keys — claimed to enable E2EE decryption and identity takeover — alongside an active Shopify Storefront Access Token linked to Eero infrastructure, priced at 1.2 BTC. The claims are unverified an…

Incident 2: Website Defacement of Baligrosir by Raxor404 (SANTIAGO404)

Category: Defacement | Date: 2026-06-09T04:50:08Z | Actor: Raxor404, SANTIAGO404 | Country: Indonesia | Industry: E-Commerce / Wholesale Retail

Intelligence Brief: On June 9, 2026, threat actor Raxor404, operating under the team SANTIAGO404, defaced the login page of www.baligrosir.com, an Indonesian wholesale e-commerce platform. The attack targeted a specific login endpoint rather than the homepage, suggesting a targeted intrusion. The incident was recorded and mirrored by zone-xsec.com with mirror ID 931952.

Incident 3: Website Defacement of Cronus by Raxor404 of SANTIAGO404

Category: Defacement | Date: 2026-06-09T04:27:21Z | Actor: Raxor404, SANTIAGO404 | Country: Malaysia | Industry: Unknown

Intelligence Brief: On June 9, 2026, the website cronus.com.my was defaced by threat actor Raxor404, operating under the group SANTIAGO404. The attack targeted a specific page path (/master) and was neither a mass defacement nor a redefacement, suggesting a targeted intrusion against this Malaysian organization.

Incident 4: Website Redefacement of Handicrafts Zone by azraelzer0d4y (b1ohaz4rd)

Category: Defacement | Date: 2026-06-09T04:21:08Z | Actor: azraelzer0d4y, b1ohaz4rd | Country: Unknown | Industry: Retail / Handicrafts & Arts

Intelligence Brief: The website handicraftszone.com was defaced by threat actor azraelzer0d4y, a member of the group b1ohaz4rd, on June 9, 2026. This incident is classified as a redefacement, indicating the site had been previously compromised by the same or a different attacker. The defacement targeted a subdirectory of the media folder rather than the homepage, and a mirror of the defaced page has been archived at zone-xsec.com.

Incident 5: Website defacement of Pivotel by azraelzer0d4y (b1ohaz4rd)

Category: Defacement | Date: 2026-06-09T04:19:53Z | Actor: azraelzer0d4y, b1ohaz4rd | Country: Australia | Industry: Telecommunications

Intelligence Brief: On June 9, 2026, threat actor azraelzer0d4y, affiliated with the group b1ohaz4rd, defaced a page on the Australian telecommunications company Pivotels website. The attack targeted a sub-path within the public media directory and was not classified as a mass or home page defacement. A mirror of the defacement was archived via zone-xsec.com.

Incident 6: Website Defacement of cpct-copycat.com by azraelzer0d4y (b1ohaz4rd)

Category: Defacement | Date: 2026-06-09T04:18:28Z | Actor: azraelzer0d4y, b1ohaz4rd | Country: Unknown | Industry: Unknown

Intelligence Brief: On June 9, 2026, threat actor azraelzer0d4y, affiliated with the group b1ohaz4rd, defaced a subdirectory of www.cpct-copycat.com. The attack targeted a specific media path rather than the homepage, suggesting a targeted subdirectory defacement. No specific motive or additional technical details were disclosed.

Incident 7: Website Defacement of Ainmane by Threat Actor azraelzer0d4y (b1ohaz4rd Team)

Category: Defacement | Date: 2026-06-09T04:17:23Z | Actor: azraelzer0d4y, b1ohaz4rd | Country: Unknown | Industry: E-Commerce

Intelligence Brief: Threat actor azraelzer0d4y, operating under the team b1ohaz4rd, defaced a subdirectory of the website ainmane.com on June 9, 2026. The defacement targeted a specific media path within the site rather than the homepage, indicating a targeted intrusion into the web servers public media directory. The incident was recorded and mirrored by zone-xsec.com under mirror ID 931950.

Incident 8: Website Redefacement of Classic Motorcycle Spares by azraelzer0d4y (b1ohaz4rd)

Category: Defacement | Date: 2026-06-09T04:16:18Z | Actor: azraelzer0d4y, b1ohaz4rd | Country: Unknown | Industry: Retail - Automotive Parts

Intelligence Brief: On June 9, 2026, threat actor azraelzer0d4y, affiliated with the group b1ohaz4rd, carried out a redefacement of the Classic Motorcycle Spares website. This incident marks at least a second defacement of the same target, indicating persistent targeting by the attacker. No specific motive or technical details were disclosed in the available intelligence.

Incident 9: Website Redefacement of OMS Electric by azraelzer0d4y (b1ohaz4rd)

Category: Defacement | Date: 2026-06-09T04:15:02Z | Actor: azraelzer0d4y, b1ohaz4rd | Country: Singapore | Industry: Electrical Services / Energy

Intelligence Brief: The website omselectric.com.sg, belonging to OMS Electric in Singapore, was defaced by threat actor azraelzer0d4y operating under the team b1ohaz4rd on June 9, 2026. This incident is recorded as a redefacement, indicating the site had been previously compromised by the same or another attacker. The attack targeted a subdirectory path rather than the homepage, suggesting exploitation of a vulnerable web application component.

Incident 10: Alleged data breach of Cyprus Airways

Category: Data Breach | Date: 2026-06-09T04:08:55Z | Actor: nazmaster

Country: Cyprus | Industry: Transportation

Intelligence Brief: A threat actor is offering what they claim to be the full dataset of Cyprus Airways for sale, requiring a middleman for the transaction. The data was previously listed for sale by another actor identified as rip_real_world, suggesting the dataset may have changed hands or is being resold.

Incident 11: Website Defacement of melhorescolha.net by azraelzer0d4y (b1ohaz4rd)

Category: Defacement | Date: 2026-06-09T04:03:23Z | Actor: azraelzer0d4y, b1ohaz4rd

Country: Brazil | Industry: Unknown

Intelligence Brief: On June 9, 2026, a threat actor known as azraelzer0d4y, operating under the team b1ohaz4rd, defaced a subdirectory of melhorescolha.net. The attack was a targeted single-page defacement, not classified as a mass or home page defacement. No specific motivation or server details were disclosed in connection with the incident.

Incident 12: Website Defacement of Sophie Collection by azraelzer0d4y (b1ohaz4rd)

Category: Defacement | Date: 2026-06-09T04:02:12Z | Actor: azraelzer0d4y, b1ohaz4rd

Country: Australia | Industry: Retail / E-Commerce

Intelligence Brief: On June 9, 2026, the Australian retail website sophiecollection.com.au was defaced by threat actor azraelzer0d4y, operating under the team b1ohaz4rd. The attack was a targeted single-page defacement, with no indication of mass or repeated defacement activity. The incident was archived via zone-xsec.com mirror.

Incident 13: Website Defacement of BS Computers by azraelzer0d4y (b1ohaz4rd)

Category: Defacement | Date: 2026-06-09T04:01:04Z | Actor: azraelzer0d4y, b1ohaz4rd

Country: Australia | Industry: Technology / Computer Services

Intelligence Brief: On June 9, 2026, threat actor azraelzer0d4y, affiliated with the group b1ohaz4rd, defaced a subdirectory of bscomputers.com.au, an Australian computer services company. The attack was a targeted single-site defacement, not classified as mass or home page defacement. No specific motive or server details were disclosed.

Incident 14: Website Redefacement of Conecticplus by azraelzer0d4y (b1ohaz4rd)

Category: Defacement | Date: 2026-06-09T04:00:03Z | Actor: azraelzer0d4y, b1ohaz4rd | Country: Unknown | Industry: Technology/Connectivity Services

Intelligence Brief: The website conecticplus.com was redefaced by threat actor azraelzer0d4y, affiliated with the group b1ohaz4rd, on June 9, 2026. This incident is marked as a redefacement, indicating the site had been previously compromised by the same or a related actor. The attack targeted a subdirectory within the sites media path, suggesting exploitation of a publicly accessible web directory.

Incident 15: Website defacement of DBS by azraelzer0d4y of b1ohaz4rd

Category: Defacement | Date: 2026-06-09T03:58:53Z | Actor: azraelzer0d4y, b1ohaz4rd | Country: Norway | Industry: Financial Services

Intelligence Brief: On June 9, 2026, threat actor azraelzer0d4y, operating under the team b1ohaz4rd, defaced a page on the Norwegian domain www.dbs.no, targeting a media or customer address directory path. The incident was a single targeted defacement, not classified as mass or home page defacement. No additional technical details such as server software or IP address were disclosed.

Incident 16: Website Redefacement of Wahlmans Klader by azraelzer0d4y (b1ohaz4rd)

Category: Defacement | Date: 2026-06-09T03:57:48Z | Actor: azraelzer0d4y, b1ohaz4rd | Country: Sweden | Industry: Retail / Fashion

Intelligence Brief: The Swedish clothing retailer Wahlmans Klader had a subdirectory of its website defaced by threat actor azraelzer0d4y, operating under the team b1ohaz4rd, on June 9, 2026. This incident is recorded as a redefacement, indicating the site had been previously compromised by the same or another actor. The defacement targeted a non-homepage path and was not part of a mass defacement campaign.

Incident 17: Website Redefacement of Gaddis New York by azraelzer0d4y of b1ohaz4rd

Category: Defacement | Date: 2026-06-09T03:56:44Z | Actor: azraelzer0d4y, b1ohaz4rd | Country: United States | Industry: Retail / E-commerce

Intelligence Brief: The website gaddisny.com was redefaced by threat actor azraelzer0d4y, a member of the group b1ohaz4rd, on June 9, 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 within the sites media path, suggesting possible exploitation of a content management system vulnerability.

Incident 18: Website Redefacement of Aeras Medical by azraelzer0d4y (b1ohaz4rd)

Category: Defacement | Date: 2026-06-09T03:54:08Z | Actor: azraelzer0d4y, b1ohaz4rd | Country: Unknown | Industry: Healthcare / Medical

Intelligence Brief: The threat actor azraelzer0d4y, operating under the team b1ohaz4rd, conducted a redefacement of the Aeras Medical website on June 9, 2026, targeting a subdirectory path within the media section of the site. This is a confirmed redefacement, indicating the attacker had previously compromised the same target. The incident was archived via zone-xsec mirror ID 931931.

Incident 19: Website Defacement of Aaralia Technologies by Raxor404 (SANTIAGO404)

Category: Defacement | Date: 2026-06-09T03:36:56Z | Actor: Raxor404, SANTIAGO404 | Country: Unknown | Industry: Technology

Intelligence Brief: On June 9, 2026, threat actor Raxor404, operating under the team SANTIAGO404, successfully defaced the homepage of Aaralia Technologies at www.aaraliastechnologies.com. The attack was a targeted single-site homepage defacement and does not appear to be part of a mass defacement campaign. No specific motive or proof-of-concept details were disclosed, and server infrastructure details remain unknown.

Incident 20: Sale of stolen payment cards and financial transfer services

Category: Carding | Date: 2026-06-09T03:14:51Z | Actor: MICKYNUTMOUSEI

Country: Unknown | Industry: Unknown

Intelligence Brief: A forum user is advertising the sale of stolen payment card data including credit/debit cards, dumps with PINs, EBT cards with PINs, and track 1&2 data. The seller also offers fraudulent financial transfers via Cashapp, Apple Pay, PayPal, and bank transfers for US and UK targets. Contact is solicited via Telegram and Discord.

Incident 21: Website defacement of Proteus Sensor by azraelzer0d4y (b1ohaz4rd team)

Category: Defacement | Date: 2026-06-09T02:51:38Z | Actor: azraelzer0d4y, b1ohaz4rd

Country: Unknown | Industry: Technology / Sensor Manufacturing

Intelligence Brief: On June 9, 2026, the website proteussensor.com was defaced by threat actor azraelzer0d4y, operating under the team b1ohaz4rd. The defacement targeted a subdirectory of the site rather than the homepage, indicating a targeted partial defacement. No specific motive or exploited vulnerability details were disclosed.

Incident 22: Website Defacement of Maqna.de by azraelzer0d4y (b1ohaz4rd)

Category: Defacement | Date: 2026-06-09T02:50:16Z | Actor: azraelzer0d4y, b1ohaz4rd

Country: Germany | Industry: E-commerce / Retail

Intelligence Brief: On June 9, 2026, threat actor azraelzer0d4y, affiliated with the group b1ohaz4rd, defaced a sub-path of the German website maqna.de, targeting a media/custom directory likely associated with a web store or CMS platform. The defacement was a targeted single-site attack with no indication of mass or repeated defacement activity. A mirror of the defacement was archived via zone-xsec.com.

5. Strategic Recommendations

Based on the overwhelming volume of web application compromises and data exfiltrations identified in this report, organizations are strongly advised to implement the following countermeasures:

- **CMS Security & Patch Management:** A significant portion of the defacements target WordPress installations and their media/upload directories. Organizations must enforce strict directory permissions, disable PHP execution in upload folders, and maintain aggressive patching schedules for core files and plugins.
- **Data Encryption & Tokenization:** The theft of databases containing plaintext PII and weakly hashed passwords (e.g., MD5) is prevalent. Organizations must adopt modern hashing algorithms (Argon2, bcrypt with high work factors) and encrypt sensitive data at rest.
- **Threat Intelligence Integration:** Organizations should actively monitor dark web forums and Telegram channels for brand mentions, leaked credentials, and API keys to preemptively rotate compromised assets.
- **Endpoint and Cloud Telemetry:** To combat advanced threats like the reported Hyper-V injection frameworks and info-stealers, organizations must deploy robust XDR (Extended Detection and Response) solutions that can detect anomalous behavior at the kernel and hypervisor levels.