Global Threat Intelligence

Comprehensive Cyber Incident Analysis Report

Reporting Period: May 29 - May 30, 2026

Classification: CONFIDENTIAL / TLP:AMBER

Generated by Cyber Intelligence Operations

1. Executive Summary

This comprehensive threat intelligence report provides an in-depth analysis of 262 distinct cybersecurity incidents recorded over a highly active 48-hour period spanning May 29 to May 30, 2026. The data encompasses a wide array of cyber threat activities, including massive data breaches, state-sponsored data leaks, automated mass defacement campaigns, initial access brokerage, and the deployment of novel malware and vulnerability exploits. The sheer volume and severity of these incidents highlight a rapidly evolving threat landscape where both opportunistic cybercriminals and highly organized syndicates are executing campaigns with unprecedented scale and precision.

Our analysis reveals several critical macro-trends dominating the current threat environment. First, there is a pronounced surge in the industrialization of data brokerage. Two highly prolific threat actors—operating under the aliases **Rupert** and **Moelester**—have flooded underground forums with dozens of high-quality, structured databases from major corporations and government entities worldwide. Their identical data structuring methodologies strongly suggest the exploitation of a widespread zero-day vulnerability in a popular CRM or e-commerce platform. Second, the apex threat group **ShinyHunters** has demonstrated an escalating focus on critical infrastructure and defense, culminating in the alleged theft of over 10 Petabytes of military and aerospace research from China's National Super-computing Center, alongside massive breaches of Western corporate giants.

Furthermore, the reporting period witnessed an overwhelming wave of automated website defacements. Threat actors such as **DimasHxR**, **azraelzer0d4y (b1ohaz4rd)**, and **Zod** executed dozens of successful intrusions, primarily targeting `/media/` and customer upload directories. The pattern of these attacks, particularly the direct targeting of AWS and Hetzner IP addresses rather than resolved domains, indicates the use of advanced, automated IPv4 scanning tools paired with weaponized payloads targeting specific, unpatched content management system (CMS) vulnerabilities.

The geopolitical ramifications of this period's incidents are equally severe. The leaking of classified Russian Federal Security Service (FSB) intelligence reports, combined with the exposure of a Joint Maritime Information Center (JMIC) advisory regarding US military operations in the Strait of Hormuz, underscores the continued blurring of lines between cybercrime, hacktivism, and state-sponsored espionage. This report deconstructs these threats category by category, providing strategic insights and actionable intelligence for defending against these sophisticated vectors.

2. Threat Landscape & Methodology Overview

The threat data analyzed in this report was aggregated from multiple underground networks, including Tor-based hidden services, open-web hacker forums (such as BreachForums and DarkForums), and specialized Telegram channels used by threat actors for initial access brokerage and data dumping. The 262 documented incidents can be broadly categorized into the following primary threat vectors:

- **Data Breaches & Extortion (35%):** Unauthorized access resulting in the exfiltration and subsequent sale or ransom of proprietary data, PII (Personally Identifiable Information), and financial records.
- **Website Defacements (45%):** Opportunistic, often automated, attacks altering the visual appearance of a website, typically used for hacktivist messaging or gaining notoriety.
- **Data Leaks (10%):** The free distribution of sensitive datasets, often driven by ideological motives, hacktivism, or attempts to disrupt rival threat actor operations.
- **Initial Access & Malware (10%):** The sale of compromised network credentials, webshells, VPN access, and the distribution of specialized malware tools (e.g., bulk email senders, cryptocurrency fraud software).

Strategic Insight: The Shift in Extortion Economics

A notable shift observed in this dataset is the apparent decline in traditional ransomware deployment by top-tier data thieves. Groups like ShinyHunters are increasingly bypassing the encryption phase entirely, moving directly to data

exfiltration and extortion. This "extortion-only" model reduces the technical overhead of developing and deploying ransomware binaries, minimizes the risk of triggering certain endpoint detection and response (EDR) heuristics, and focuses entirely on the leverage provided by the threat of data exposure.

The geographic distribution of these attacks is genuinely global. While traditional targets in North America (United States, Canada) and Western Europe (France, Germany, UK) remain heavily impacted, there is a distinct surge in compromises affecting South America (Brazil, Argentina, Ecuador, Mexico) and the Asia-Pacific region (China, Indonesia, Bangladesh). This global spread correlates directly with the automated nature of the vulnerabilities being exploited; threat actors are scanning the entire IPv4 space, compromising targets based on vulnerability presence rather than geographic preference.

3. The Rise of the Mega-Brokers: Rupert and Moelester

One of the most alarming discoveries in this reporting period is the operational dominance of two data brokers operating under the monikers **Rupert** and **Moelester**. Together, these actors are responsible for listing over 25 distinct, high-value corporate and government databases for sale within a 24-hour window. The volume, quality, and specific formatting of their datasets provide critical intelligence regarding their operational methodology.

3.1 Operational Profile: Threat Actor "Rupert"

Rupert operates primarily on open-web cybercrime forums, offering massive datasets priced consistently between $900 and $1,400 USD. The targets compromised by Rupert are highly diverse geographically and span multiple critical sectors. Notable breaches attributed to Rupert in this period include:

- **Retail & E-commerce:** Home Depot Canada (742,000 records), Coleman BBQ Canada (427,000 records), Hardware Sales Canada (374,000 records), Petlove Brazil (684,000 records), and Autoline Brazil (812,000 records).
- **Government & Public Sector:** Argentine Ministry of Justice (684,000 records), Argentine Poder Judicial de la Nación (563,000 records), Bangladesh Probashi Welfare Board (482,000 records), Bangladesh Overseas Employment and Services Limited (742,000 records), Algerian Ministry of Tourism (728,000 records), and Brazil's CRMV (582,000 records).
- **Finance & Healthcare:** MercadoPago Argentina (425,000 records) and Mutualité Chrétienne Belgium (268,000 records).

3.2 Operational Profile: Threat Actor "Moelester"

Operating concurrently and utilizing near-identical pricing and advertising structures, Moelester focuses heavily on European technology, healthcare, and community platforms. Key breaches include:

- **Healthcare & Platforms:** Doctissimo France (two separate breaches of 524,000 and 243,000 records), Swiss Medical Group Argentina (458,000 records), DatingBuzz South Africa (672,000 records).
- **Technology & Infrastructure:** home.pl Poland (473,000 records), smtp.ru Russia (683,000 records), SalesAutopilot Hungary (184,000 records), and 56qq.com China (472,000 records).
- **Civic & Community:** Stadgenoot Netherlands (472,000 records), Jelgava City Latvia (137,000 records), and Apollo Forums Latvia (215,000 records).

TTP Analysis: The "Three-Table" Signature

A profound forensic anomaly exists across almost every dataset offered by both Rupert and Moelester. Regardless of the victim's industry—whether a Canadian hardware retailer, an Argentine judicial body, or a Belgian health insurer—the threat actors advertise the data as being structured into exactly three interconnected sections or tables. Typically, these are categorized as: 1) Contacts/Profiles, 2) Orders/Tickets/Applications, and 3) Logs/Support.

This strict structural uniformity across vastly different organizations is highly unusual. It strongly indicates that these actors are not individually hacking bespoke infrastructure. Instead, they are likely exploiting a zero-day vulnerability or a severe misconfiguration in a widely deployed, third-party backend system—such as a specific Customer Relationship Management (CRM) platform, a marketing automation tool, or an outsourced cloud database service that enforces this specific three-table schema. The coordination, timing, and identical formatting suggest that Rupert and Moelester are either aliases for the same syndicate or affiliates utilizing the same backend exploit framework.

4. Apex Predators: ShinyHunters and Syndicate Operations

While the mega-brokers focus on volume, the notorious threat group **ShinyHunters** (often collaborating with affiliates from Lapsus$) executed highly targeted, devastating attacks against global corporate giants and sovereign critical infrastructure during this period. ShinyHunters has evolved from a forum-based data seller into a sophisticated extortion syndicate capable of breaching the highest-security environments.

4.1 The Cisco and Ticketmaster Mega-Breaches

On May 29, 2026, ShinyHunters announced the compromise of **Cisco Systems**, claiming exfiltration of source code, AWS private buckets, Azure storage keys, hardcoded credentials, SSL certificates, and highly confidential internal documents. This represents a catastrophic supply-chain risk, given Cisco's foundational role in global networking infrastructure. The theft of private cloud buckets and hardcoded credentials suggests that the initial intrusion vector may have involved compromised developer accounts or exposed CI/CD pipelines.

Simultaneously, the group offered a massive dataset allegedly belonging to **Ticketmaster**. The scale of this breach is staggering: 980 million sales orders, 440 million unique email addresses, and 400 million encrypted credit card details. The asking price of a mere $4,000 USD is suspiciously low for data of this magnitude, suggesting the group may have already monetized the most valuable segments of the data (such as full financial profiles) privately, or they are using the public sale to apply maximum PR pressure on the victim organization.

4.2 Critical Infrastructure and Sovereign Targeting

ShinyHunters has also demonstrated a willingness to target sovereign nation-states and critical public infrastructure. The most severe incident recorded is the alleged breach of **China's National Super-computing Center (NSCC)**. The actors claim to have stolen over 10 Petabytes of sensitive research data, specifically citing aerospace, military, and fusion simulation research from top Chinese defense contractors and universities (AVIC, COMAC, NUDT). If verified, this constitutes one of the largest state-level intellectual property thefts in history, effectively commoditizing national security data on Telegram channels.

Further demonstrating their reach, the group breached **Serasa Experian** in Brazil, exfiltrating a 1.8TB database containing the personal and financial profiles of 223 million Brazilian citizens—effectively the entire population. In France, they compromised **Les CROUS** (1.9 million student records, including passports and payslips) and a centralized **French Weapons Information System** (detailing 62,511 registered firearms and their owners' PII). The exposure of the weapons registry poses severe physical security risks, as organized crime syndicates could use this data to target civilian homes known to house specific firearms.

Ecosystem Manipulation: The VECT Ransomware Decryptor

In a bizarre display of ecosystem manipulation, ShinyHunters publicly released a free decryptor for the **VECT ransomware**. They explicitly stated that the VECT operators were "unreliable" and failed to decrypt victim files upon payment. By positioning themselves as "saviors" against incompetent rivals, ShinyHunters is engaging in complex psychological operations—attempting to build a perverse

form of brand trust with victims while simultaneously undermining competing cybercriminal syndicates.

5. Widespread Automated Defacement Campaigns

Website defacement, often dismissed as low-level digital vandalism, reached epidemic proportions during this 48-hour window. Over 100 individual defacement incidents were recorded, driven not by manual hacking, but by automated exploitation frameworks operated by a handful of prolific actors. The technical indicators left behind provide a clear picture of the vulnerabilities being exploited.

5.1 Path Traversal and Unrestricted File Uploads

The vast majority of defacements carried out by actors such as **DimasHxR** and **azraelzer0d4y (b1ohaz4rd)** shared a distinct technical signature: the defacement payloads were invariably uploaded to subdirectories associated with media handling, such as `/media/`, `/pub/media/`, `/customer_address/`, or `/wp-content/uploads/`. This pattern strongly indicates the exploitation of unrestricted file upload vulnerabilities or path traversal flaws in popular content management systems (CMS) and e-commerce platforms (likely Magento, given the specific `/pub/media/` path structure).

DimasHxR systematically targeted European and North American retail websites, successfully compromising dozens of domains including *gotron.be*, *hoogenboezem.nl,* and *poolspasonline.com*. The attacks were surgical page-level replacements within the media directories, leaving the root domains largely intact but establishing persistent unauthorized content hosting.

5.2 Direct IP Scanning and Cloud Infrastructure Targeting

The actor **azraelzer0d4y**, affiliated with the *b1ohaz4rd* team, demonstrated a more aggressive and automated targeting methodology. Instead of attacking resolved domain names, a significant portion of this actor's victims were raw IP addresses mapped to cloud hosting providers like Amazon Web Services (AWS) and Hetzner (e.g., `13.205.36.63`, `95.216.5.90:8082`). This proves that the actor is utilizing high-speed IPv4 scanners (such as Masscan or ZMap) to identify responsive web servers on ports 80, 8080, and 8082, and then automatically firing exploit payloads at the detected services. This "spray and pray" approach indiscriminately compromises any unpatched server connected to the internet, regardless of the victim organization's size or industry.

5.3 The "Zod" and "chinafans" Mass Campaigns

The threat actor **Zod** executed a highly focused mass defacement campaign against the manufacturing, packaging, and logistics sectors, particularly in Indonesia and Brazil (e.g., *deltapresisi.com*, *actransmg.com.br*). Zod uniformly deployed a payload named `/zod.html`. Similarly, the actor **chinafans** (of *0xteam*) conducted global strikes, dropping `/0x.txt` files on targets ranging from Swiss cloud provider preview domains (Infomaniak) to South American construction firms. These actors leverage mass-exploitation scripts that ingest lists of vulnerable URLs generated by Google dorks or Shodan queries, executing hundreds of compromises per hour.

6. Data Leaks, Hacktivism, and Geopolitical Fallout

Beyond financially motivated breaches, this period saw severe data leaks driven by hacktivism, geopolitical conflict, and state-sponsored espionage. Data leaks—where information is distributed freely rather than sold—are designed to maximize public exposure, cause reputational damage, or facilitate secondary attacks by the wider cybercriminal community.

6.1 Geopolitical and Intelligence Leaks

The intersection of cyber operations and global military conflict was starkly evident. A threat actor known as **mosad** freely distributed two classified Russian Federal Security Service (FSB) intelligence reports. These RTF documents reportedly detail methodological procedures for intelligence interception (ROTM) and analyze foreign intelligence activities targeting Russia. Concurrently, a classified advisory memorandum from the Joint Maritime Information Center (JMIC) regarding imminent US military operations in the Strait of Hormuz was leaked on Telegram. These incidents highlight how encrypted messaging platforms have become primary distribution channels for classified military intelligence.

6.2 Sovereign Data Exposure

Hacktivist groups heavily targeted sovereign government databases. The **VandalsGroup** released a dataset containing the personal records of 490,000 citizens of Ambato, Ecuador, while simultaneously auctioning active webshell access to the municipal government's intranet servers (`ambato.gob.ec`). In Mexico, the actor **Black0ut_Exi** leaked 1 million records from the Mexico City Government (CDMX) portal, including sensitive electoral credential data. Furthermore, an actor named **FlipperOne** offered 1.5 million highly sensitive PII records (including national identity cards and blood groups) from the Higher Education Commission of Pakistan. These leaks systematically dismantle the

privacy of millions of citizens, exposing them to identity theft, financial fraud, and targeted physical threats.

6.3 Historical and Institutional Leaks

The dataset also revealed the exposure of legacy systems. The actor **OriginalCrazyOldFart** leaked 6.8 GB of historical US public records originating from the legacy "SnailSearch" system, containing decades-old birth, marriage, and divorce vitals. In the academic sector, hacktivists (e.g., **Anonymous2090** and **INT3X**) freely distributed databases from Naresuan University in Thailand and Mansura University in Egypt, the latter compromising over 1 million student records. These incidents demonstrate that legacy data, even if years old, remains a highly sought-after commodity for identity aggregation and credential stuffing.

7. Initial Access Brokers and Specialized Threats

The cyber underground relies heavily on Initial Access Brokers (IABs) and specialized tool developers who provide the foundational infrastructure for larger attacks.

- **WAF Bypass Solicitation:** A highly concerning post on a dark web forum featured an actor soliciting technical assistance to bypass Akamai Web Application Firewall (WAF) protections guarding three major Japanese financial institutions (SMBC, Mizuho, and MUFG). The actor claimed to have a working exploit but was hindered by the WAF, illustrating the collaborative, crowdsourced nature of modern cyber attacks against hardened targets.
- **Aviation Access:** An actor advertised employee login access to Air France's Passenger Name Records (PNR) system. PNR data is highly prized by intelligence agencies and cybercriminals alike, as it contains detailed travel itineraries, payment data, and behavioral patterns of high-net-worth individuals and government officials.
- **Social Media & E-commerce Fraud Farms:** Multiple actors (e.g., *pipl1on33uku*, *xxin7*) were observed selling bulk, compromised TikTok accounts (some with over 500,000 followers) and SHEIN self-operated LLC accounts. These are critical assets for launching massive disinformation campaigns, dropshipping fraud, and cryptocurrency scams.
- **Malware and Tooling:** The proliferation of specialized attack software continues. Threat actors actively marketed **STORM v2.6.0.2** (a multifunctional vulnerability scanner), **Heartsender V5** (a sophisticated bulk email tool designed to bypass spam filters for phishing campaigns), and fraudulent Tether (USDT) software designed to spoof cryptocurrency transactions on the TRC20 and BEP20 networks.

8. Strategic Recommendations and Defensive Posture

The sheer scale and diversity of the incidents observed over this 48-hour period require organizations to adopt an aggressive, multi-layered defensive posture. The following strategic recommendations are derived directly from the Tactics, Techniques, and Procedures (TTPs) analyzed in this report:

Threat Vector	Observed TTP	Recommended Mitigation Strategy
Mass Defacements	Exploitation of unrestricted file uploads; Path traversal in `/media/` directories; Automated IPv4 scanning.	Implement strict execution prevention in all web-accessible upload directories (e.g., disable PHP/script execution in `/wp-content/uploads/` or `/pub/media/`). Ensure servers do not respond to direct IP requests without a valid Host header to thwart automated IPv4 scanners.
Mega-Broker Breaches	Systematic extraction of 3-table schemas (Contacts, Orders, Logs) suggesting zero-day exploitation of unified CRM/E-commerce backends.	Conduct immediate forensic audits of all third-party CRM, marketing automation, and e-commerce integrations. Implement strict database-level egress filtering and rate-limiting to detect and block massive data exfiltration events.
Initial Access & Cloud	Theft of AWS/Azure keys; Selling of active webshells and employee VPN/SSO credentials.	Enforce hardware-backed Multi-Factor Authentication (MFA) across all employee and contractor access points. Actively scan code repositories (GitHub/GitLab) for hardcoded cloud infrastructure keys using secrets management tools.
Phishing & Malware	Use of advanced bulk senders (Heartsender V5) and topical lures (2026 FIFA World Cup).	Update email gateway heuristics to detect URL rotation and encryption techniques used by modern spam tools. Implement strict DMARC, SPF, and DKIM enforcement. Deploy continuous security awareness training focused on highly topical, localized phishing lures.

Conclusion: The events of May 29-30, 2026, unequivocally demonstrate that the barrier to entry for conducting devastating cyber attacks continues to lower, while the potential impact scales exponentially. The commoditization of zero-day exploits, the industrialization of data brokerage, and the seamless collaboration

among international threat syndicates necessitate a paradigm shift in defensive strategy. Organizations can no longer rely solely on perimeter defense; they must assume breach, heavily invest in rapid detection and response capabilities, and ruthlessly secure their software supply chains and third-party integrations.