Monthly Crimeware activity report – October 2025

Report Id: CW-20251101
Version: 1.0 (13.November.2025)

We start our monthly report with a quick overview of things that have made the headlines, research from other vendors that has caught our eye and some of the more important aspects of research that we've reported in the past month. We also provide summaries of the private reports that we have published this month.

Mandiant and Google Threat Intelligence uncovered UNC5142, a financially motivated threat cluster that abuses BNB Smart Chain (BSC) smart contracts in a novel "EtherHiding" campaign[1] to distribute infostealers like VIDAR, LUMMAC.V2, RADTHIEF, and ATOMIC. Active since late 2023, UNC5142 compromises thousands of WordPress sites and injects CLEARSHORT JavaScript downloaders that fetch malicious stages from blockchain-stored payloads instead of typical web servers, enhancing evasion and resiliency. The group's architecture evolved from a single smart contract to a three-layer "proxy-pattern" system – routing victim traffic, fingerprinting users, and dynamically pulling AES-encrypted payloads hosted on Cloudflare Pages. Infection lures mimic browser updates, Cloudflare "Unusual Traffic" errors, and anti-bot checks, tricking users into executing ClickFix-style commands to run PowerShell or .hta scripts that decrypt and launch final payloads in memory. On-chain analysis shows two parallel infrastructures funded via OKX-linked wallets, suggesting professionalized, scalable operations. Though quiet since July 2025, UNC5142's blend of blockchain-based command-and-control (C2) agility, Web3 abuse, and cross-platform targeting (Windows/macOS) marks a major step in malware distribution innovation leveraging immutable ledgers for persistence and control.

Researchers uncovered a large-scale extortion[2] campaign exploiting a zero-day vulnerability (CVE-2025-61882) in Oracle E-Business Suite (EBS), attributed to actors using the CL0P extortion brand, potentially linked to FIN11. Beginning in July 2025, threat actors exploited Oracle EBS components like UiServlet and SyncServlet to gain remote code execution and deploy a multi-stage Java implant framework involving GOLDVEIN.JAVA and the SAGE malware family (SAGEGIFT, SAGELEAF, SAGEWAVE). These implants were stored directly in Oracle EBS databases via malicious XSL templates, enabling in-memory execution and data exfiltration. By September 29, 2025, the attackers launched widespread extortion emails – sent from compromised third-party accounts – to executives of numerous organizations, claiming data theft from Oracle EBS environments. The campaign's tactics mirror prior CL0P/FIN11 mass exploitation events against managed file transfer systems, combining zero-day exploitation, data theft, and delayed extortion attempts.

Cisco Talos discovered that ransomware operators, assessed with moderate confidence to be linked to Storm-2603, are abusing Velociraptor[3], a legitimate open-source digital forensics and incident response (DFIR) tool, to maintain persistence during Warlock, LockBit, and Babuk ransomware attacks. In the August 2025 incident, attackers deployed an outdated Velociraptor version (0.73.4.0) vulnerable to CVE-2025-6264, potentially enabling privilege escalation and remote command execution. The actors leveraged the tool for stealthy access while targeting VMware ESXi and Windows servers, executing scripts to disable Microsoft Defender protections, modify Group Policy Objects, and use Smbexec and PowerShell for lateral movement, encryption, and data exfiltration. The campaign aligns with Storm-2603's prior activity exploiting ToolShell vulnerabilities in on-premises SharePoint and deploying multiple ransomware variants simultaneously – a rare and notable tactic.

[1] New Group on the Block: UNC5142 Leverages EtherHiding to Distribute Malware
[2] Oracle E-Business Suite Zero-Day Exploited in Widespread Extortion Campaign
[3] Velociraptor leveraged in ransomware attacks

NVISO Labs uncovered an attack chain employed by Lunar Spider – a cybercriminal group developing and operating IcedID (BokBot) and its successor Latrodectus – leveraging[4] FakeCaptcha (a.k.a. "TeleCaptcha") pages to deliver malware through compromised websites exploiting CORS vulnerabilities. The attackers inject malicious JavaScript ("iFrameOverload") into European sites to overlay fake CAPTCHA pages that trick users into copying and executing PowerShell commands, which download an MSI installer that deploys Latrodectus V2 via DLL sideloading of a malicious `wtsapi32.dll` through Intel's legitimate `igfxSDK.exe`. Acting as a loader, Latrodectus communicates with C2 servers to run reconnaissance commands , establishes persistence, and provides access for ransomware affiliates like ALPHV/BlackCat. The fake CAPTCHA additionally monitors victims in real time via a Telegram bot, exfiltrating browser, OS, and interaction data to the attackers.

Elastic Security Labs revisited the WARMCOOKIE[5] backdoor one year after its discovery, revealing that it remains actively developed and deployed in phishing, spam, and malvertising campaigns – now even distributed by the CASTLEBOT Malware-as-a-Service loader. The latest variants introduce new execution handlers for PE, DLL, and PowerShell scripts, a campaign ID field for tracking infections, and a string bank of legitimate company names used for scheduled task names and folder paths to improve defense evasion. Additional updates include dual mutexes for synchronization, cleaner code, and the shift from hardcoded paths to dynamically generated ones. Researchers also identified a default SSL certificate reused across WARMCOOKIE command-and-control infrastructure, despite its expiration, allowing tracking of ongoing operations. The campaign IDs and RC4 encryption keys suggest distinct operator clusters with different capabilities – some variants executing PowerShell, others only DLL/EXE payloads. Despite takedowns during Europol's Operation Endgame (May 2025), new WARMCOOKIE infrastructure continues to appear, signaling that the malware's developers remain active and that it will likely persist as a stealthy and adaptable threat in the MaaS ecosystem.

Check Point Research analyzed Rhadamanthys stealer v0.9.2, a multi-modular infostealer active worldwide, which continues to evolve with new features and deeper anti-analysis capabilities[6]. Initially released in 2022 and now linked to ClickFix-related campaigns, Rhadamanthys is maintained as a professionalized "Rhad Security / Mythical Origin Labs" service with paid tiers and a Telegram-based customer infrastructure. Version 0.9.x introduces key technical changes: new mutex generation and configuration logic, extended process-injection options, updated custom XS1/XS2 executable formats, and new RC4-based string encryption. Its evasion module performs extensive sandbox detection using wallpaper hashes, fake files, usernames, MAC and hardware ID blocklists, and even collects browser fingerprints via a new JavaScript module (fingerprint.js). The malware now downloads Stage 3 payloads disguised as PNG images instead of WAV/JPG files and supports configurable injection targets for better flexibility. Rhadamanthys also expands its Lua-based stealers to include the Ledger Live crypto wallet, adding to an already vast set of targets spanning browsers, mail clients, messengers, VPNs, and wallets.

Researchers exposed[7] the YouTube Ghost Network, a large-scale malware distribution ecosystem abusing over 3,000 compromised YouTube accounts and videos to spread infostealers like Lumma and Rhadamanthys. Active since 2021 and tripling in volume in 2025, the network uses fake "game hacks" and "software crack" tutorials with positive AI-generated comments to create false legitimacy. Videos share links to phishing sites or cloud storage (Dropbox, Google Drive, MediaFire) hosting password-protected malware archives. After Lumma's takedown, actors shifted to Rhadamanthys v0.9.2, rotating C2 servers and payloads every few days to evade detection. This platform-based Ghost Network model leverages real engagement, compromised channels, and redundant hosting, representing an evolved, highly scalable malware delivery infrastructure targeting users worldwide.

[4] Lunar Spider Expands their Web via FakeCaptcha
[5] WARMCOOKIE One Year Later: New Features and Fresh Insights
[6] Rhadamanthys 0.9.x – walk through the updates
[7] Dissecting YouTube's Malware Distribution Network

AhnLab researchers discovered that Rhadamanthys is being distributed through fake Ren'Py-based games hosted on file-sharing sites[8]. Ren'Py, a Python framework for creating visual novels, was exploited by embedding a malicious script inside the game's `script.rpy` file, which loads additional malware during execution. When users launch the trojanized game, it executes a malicious loader that decrypts hidden files and injects Rhadamanthys into a .NET process while displaying a fake loading screen to mask activity.

Trellix researchers analyzed XWorm V6.0, a resurgent modular RAT that resurfaced in mid-2025 after being abandoned in 2024, now actively used in global phishing campaigns[9]. First observed in 2022 and originally authored by XCoder, XWorm returned under the alias XCoderTools through new Telegram, Signal, and YouTube channels. The malware follows a multi-stage infection chain (malicious JavaScript → PowerShell loader → DLL injector → XWorm client) connecting to its C2, and introduces over 35 plugins enabling data theft, remote control, surveillance, and ransomware. It also delivers other payloads such as DarkCloud Stealer, Hworm, Remcos RAT, Snake Keylogger, and coin miners. Persistence relies on registry Run keys, logon scripts, and ResetConfig.xml abuse – previously seen in Pulsar RAT. Researchers also uncovered rootkit and reset-survival modules, along with cracked and trojanized builder versions circulating among cybercriminals – some already infected by XWorm itself – and found that its ransomware component reuses code from the .NET NoCry Ransomware.

Zscaler ThreatLabz researchers uncovered a global SEO-poisoning campaign distributing a trojanized Ivanti Pulse Secure VPN installer via look-alike download pages; the signed installer drops malicious DLLs that harvest VPN connection data and exfiltrate credentials to attacker-controlled infrastructure[10]. The pages use referrer-based content switching to hide the malicious payload from analysts (serving benign content when visited directly but delivering the trojanized installer via search redirects). This credential-harvesting activity is linked to initial-access operations that can lead to ransomware deployments.

WithSecure researchers exposed TamperedChef[11], a malvertising-driven credential theft campaign targeting European organizations. The operation masqueraded as a legitimate "AppSuite PDF Editor" app promoted through paid ads and distributed via MSI installers. The decoy worked normally for nearly two months before activating its payload, stealing browser-stored credentials through an obfuscated JavaScript module and a native NodeJS DLL. The malware persisted via autorun registry entries and communicated with attacker-controlled infrastructure under the guise of a functional Electron-based PDF tool. After discovery, the attackers released "clean" updates to disguise their activity and later pivoted to a new decoy project called S3-Forge, still under development.

CYFIRMA researchers analyzed Yurei[12] Ransomware, a new Go-based threat targeting Windows systems worldwide, designed for fast encryption, lateral movement, and forensic evasion. Yurei appends a ".Yurei" extension to files, uses per-file ChaCha20 encryption keys wrapped with ECIES, and deletes shadow copies, backups, and event logs to prevent recovery. It propagates through SMB shares, USB drives, and credential-based remote execution using PsExec-style techniques, while wiping memory and logs to conceal traces. Each victim receives a Tor-based ransom note with unique ticket IDs and negotiation tokens, supporting double extortion. CYFIRMA linked Yurei's codebase to the open-source Prince Ransomware, sharing its cryptographic structure, header format, and behavioral quirks but with enhanced concurrency and anti-forensics.

[8] Distribution of Rhadamanthys Malware Disguised as a Game Developed with Ren'Py
[9] XWorm V6: Exploring Pivotal Plugins
[10] Search, Click, Steal: The Hidden Threat of Spoofed Ivanti VPN Client Sites
[11] TamperedChef: Malvertising to Credential Theft
[12] YUREI RANSOMWARE : THE DIGITAL GHOST

Trend Micro researchers uncovered Water Saci, a self-propagating malware campaign targeting Brazilian users and organizations through WhatsApp[13] and phishing emails. The malware, named SORVEPOTEL, spreads via malicious ZIP attachments disguised as invoices or documents, urging victims to open them on desktop systems – an indication that enterprises are the main target. Once executed, it establishes persistence, hijacks active WhatsApp Web sessions, and automatically sends the same infected file to all contacts and groups to propagate further. The payload, a multi-stage .NET infostealer, monitors banking activity and targets major Brazilian financial institutions and cryptocurrency platforms such as Bradesco, Itaú, Caixa, and Binance. It employs overlay phishing tactics to mimic legitimate banking interfaces, steal credentials, and control user input.

A new phase of the Water Saci campaign[14] employs script-based infection chains, multi-vector persistence, and an email-driven command-and-control system. The malware, written in VBS and PowerShell, hijacks WhatsApp Web sessions, harvests contacts, and automatically distributes malicious ZIP files while maintaining remote synchronization through an IMAP-based C2 hosted on Brazilian email services. Attackers can pause, resume, and coordinate infections in real time, turning compromised endpoints into a botnet under centralized control. This evolution reflects a broader shift from compiled banking Trojans toward fileless, automation-driven attacks that exploit social messaging platforms.

Rapid7 researchers uncovered a new cloud-focused[15] threat group dubbed "Crimson Collective", observed targeting AWS environments worldwide for data exfiltration and extortion. The group exploits leaked long-term AWS access keys found using tools like TruffleHog to gain initial access, create new IAM users, and escalate privileges by attaching AdministratorAccess policies. Once established, the attackers perform extensive reconnaissance – enumerating EC2 instances, RDS databases, S3 buckets, and IAM roles – before exfiltrating data via AWS snapshots and S3 exports. In confirmed incidents, the group used Amazon SES to send extortion emails from victims' own infrastructure after stealing sensitive databases and project repositories.

Aryaka[16] Threat Research Labs exposed a new campaign by the Vietnamese threat actor "BatShade", which is targeting job seekers and digital marketing professionals worldwide through fake recruiter outreach on professional platforms. The campaign delivers a Go-based malware dubbed "Vampire Bot", disguised as legitimate job-related files inside ZIP archives. Once executed, it launches a hidden PowerShell script, displays a decoy PDF, and installs the actual malware in the background. Vampire Bot collects system information, maintains persistence using mutexes, hides within system folders, and continuously captures screenshots sent via encrypted channels to its C2 servers. The campaign demonstrates BatShade's evolution from using commodity malware to developing custom, stealth-focused tools capable of long-term surveillance and data theft, marking a clear shift toward more sophisticated, targeted cyber-espionage operations.

Cofense researchers uncovered a career-themed phishing campaign impersonating major brands – Tesla, Google, Ferrari, and Red Bull – to lure[17] job seekers worldwide, especially those in marketing and social media roles. The emails spoof legitimate recruitment outreach using trusted domains like Xero's messaging service to bypass filters and increase credibility. Victims are led through multi-stage phishing paths that mimic Glassdoor, Facebook, or X login portals, stealing both corporate and personal credentials. A new twist includes prompting users to upload resumes, allowing attackers to harvest additional PII for follow-up social-engineering attacks. The realistic branding, CAPTCHA screens, and job-application flow make the scam highly convincing.

[13] Self-Propagating Malware Spreading Via WhatsApp, Targets Brazilian Users
[14] Active Water Saci Campaign Spreading Via WhatsApp Features Multi-Vector Persistence and Sophisticated C&C
[15] Crimson Collective: A New Threat Group Observed Operating in the Cloud
[16] Vietnamese Threat Actor Expands Operations
[17] Phishing from Home – The Hidden Danger in Remote Jobs Lurking in Tesla, Google, Ferrari, and Glassdoor

Expel analyzed a new phishing campaign leveraging a technique[18] called “cache smuggling”, marking an evolution of the ClickFix-style social engineering attack. The lure impersonates Fortinet’s VPN Compliance Checker and targets corporate users, particularly those with remote-access privileges. Victims are tricked into pasting a command that appears benign but actually runs a hidden PowerShell script designed to reconstruct and execute a ZIP payload hidden inside the browser’s cached “image” files. Instead of downloading malware, the attack abuses the browser’s caching mechanism to store a disguised ZIP archive labeled as a JPG image, which later gets extracted and executed locally – allowing it to bypass traditional download-based security detections. This novel “cache smuggling” method lets attackers deploy malicious payloads without network indicators or direct file transfers.

Malwarebytes researchers uncovered a social engineering campaign targeting gamers with fake itch.io-style pages[19] that spread malware loaders disguised as indie games. Attackers pose as friends or developers on Discord, asking users to “test their game”. The links lead to convincing imitation pages hosted on Blogspot or cloud services, sometimes even fronted by fake Discord login screens to steal credentials. The downloaded “Setup Game.exe” silently runs PowerShell commands encoded in Base64, launches hidden scripts, and installs Node.js components into user cache directories while forcibly closing browsers to prevent suspicion. These loaders act as stagers for later payloads such as backdoors, keyloggers, or miners, activating only after confirming they’re on real machines.

Unit 42 researchers analyzed the IUAM ClickFix[20] Generator, a phishing-as-a-service toolkit that mass-produces ClickFix-style social engineering pages designed to trick users into manually executing malware commands. Mimicking browser verification pages like Cloudflare’s “Just a moment…” screens, the kit automates clipboard injection, OS detection, and obfuscation to deliver commands that download and install infostealers such as DeerStealer and Odyssey across Windows and macOS. The phishing pages lure victims into copying and running PowerShell or Terminal commands disguised as verification checks, enabling attackers to deploy multi-stage payloads without direct downloads. Researchers observed multiple active campaigns generated by this kit – some Windows-only variants dropping DeerStealer, and others multi-platform builds delivering Odyssey to macOS users – revealing a shared codebase, indicating an expanding underground ecosystem.

Researchers uncovered Jingle Thief[21], a Morocco-based cloud-centric fraud campaign targeting global retail and consumer services enterprises to conduct gift card theft at scale. The actors, tracked as CL-CRI-1032 (overlapping with Atlas Lion/STORM-0539), infiltrate Microsoft 365 environments through phishing and smishing, harvesting credentials to access SharePoint, OneDrive, and Exchange. They perform cloud reconnaissance, send internal phishing emails, create malicious inbox rules for covert monitoring, and register rogue devices in Entra ID for MFA-resistant persistence. Operating stealthily for months, often during holiday periods, they exploit internal gift-card issuance systems to generate and resell high-value cards. Unit 42 attributes this campaign to financially motivated Moroccan operators active since 2021, representing a sophisticated example of identity-based cloud abuse and long-term credential persistence rather than traditional endpoint malware.

Researchers uncovered global phishing campaigns deploying the PhantomVAI[22] Loader, an evolved .NET-based malware loader that delivers multiple infostealers including Katz Stealer, AsyncRAT, XWorm, FormBook, and DCRat. The attacks use multi-stage chains beginning with phishing emails containing obfuscated JavaScript or VBS scripts, followed by PowerShell loaders employing steganography to conceal DLL payloads within GIF images. Once executed, PhantomVAI performs VM detection, sets up persistence through scheduled tasks or Run keys,

[18] Cache smuggling: When a picture isn’t a thousand words
[19] “Can you test my game?” Fake itch.io pages spread hidden malware to gamers
[20] The ClickFix Factory: First Exposure of IUAM ClickFix Generator
[21] Jingle Thief: Inside a Cloud-Based Gift Card Fraud Campaign
[22] PhantomVAI Loader Delivers a Range of Infostealers

and uses process hollowing (typically into `MSBuild.exe`) to inject final payloads. Originally linked to the MaaS-based Katz Stealer, gathering credentials, crypto wallets, Telegram data, and system information while avoiding execution on CIS-region systems.

Fortinet's FortiGuard Labs analyzed a new Chaos[23] ransomware variant dubbed Chaos-C++, the family's first major rewrite from .NET to C++, marking a sharp evolution toward speed, destruction, and stealth. Masquerading as a fake System Optimizer utility, the downloader installs the ransomware silently, encrypting small files with AES-256-CFB or fallback XOR, skipping medium-sized files, and deleting large ones over 1.3 GB. The variant also introduces clipboard hijacking, replacing any copied Bitcoin address with the attacker's wallet to divert ransom or crypto transfers, while disabling recovery features via vssadmin, wmic, and bcdedit commands before dropping ransom notes across directories. Compared to earlier Chaos variants like Lucky_Gh0$t and BlackSnake, Chaos-C++ reflects a strategic shift from traditional encryption to data-wiping behavior, blurring the line between ransomware and wipers and signaling a more aggressive, destructive threat evolution.

Researchers discovered a new Stealit[24] malware campaign that leverages Node.js' experimental Single Executable Application (SEA) feature to distribute standalone, obfuscated binaries that can execute on systems without Node.js installed. The campaign, which continues to masquerade as fake game or VPN installers hosted on platforms like MediaFire and Discord, marks an evolution from earlier Stealit variants built with Electron. Once executed, the malware unpacks multiple layers of encoded scripts, performs extensive anti-analysis and sandbox checks, and downloads additional components from its C2 infrastructure. These modules steal credentials, cryptocurrency wallets, and data from browsers, messengers, and game clients, while enabling full remote access functions such as screen capture, webcam streaming, file theft, and ransomware deployment. The operators market Stealit as a paid "data extraction" service, complete with a web dashboard and Telegram promotions.

Trend Micro researchers uncovered a large-scale RondoDox[25] botnet campaign exploiting more than 50 vulnerabilities across 30+ vendors, including flaws first demonstrated at Pwn2Own contests. Initially identified in mid-2025, RondoDox targets routers, DVRs, NVRs, CCTV systems, and other internet-facing network devices using a "shotgun exploitation" approach – launching multiple command-injection and path traversal exploits to compromise anything exposed. The campaign notably abuses vulnerabilities like CVE-2023-1389 (TP-Link AX21), CVE-2024-3721 (TBK DVR), and CVE-2024-12856 (Four-Faith routers), several of which are now listed in CISA's KEV catalog. Evolving from single-device compromises to a multiarchitecture loader-as-a-service operation, RondoDox has been observed distributing Mirai/Morte payloads and maintaining persistent footholds for data theft and network disruption.

eSentire's researchers uncovered a new Rust-based backdoor named ChaosBot[26], which abuses Discord as its C2 platform to manage infected systems. First observed in late September 2025 within a financial services network, ChaosBot spreads via compromised VPN credentials, malicious Windows shortcut files, or phishing lures themed around the State Bank of Vietnam. Once executed – often through DLL sideloading with legitimate Microsoft Edge components – the malware establishes communication with a Discord server, creates channels named after infected hosts, and executes commands like PowerShell shell execution, file upload/download, and screenshot capture, sending all results back through Discord messages. It also deploys Fast Reverse Proxy (FRP) for persistent remote access and experiments with Visual Studio Code tunnels as secondary backdoors. Written entirely in Rust, ChaosBot employs ETW patching and anti-VM checks for evasion. Two identified Discord accounts – chaos_00019 and lovebb0024 – operate the C2 network, suggesting a small but active threat cluster targeting mainly Vietnamese-speaking users.

[23] The Evolution of Chaos Ransomware: Faster, Smarter, and More Dangerous
[24] New Stealit Campaign Abuses Node.js Single Executable Application
[25] RondoDox: From Targeting Pwn2Own Vulnerabilities to Shotgunning Exploits
[26] New Rust Malware "ChaosBot" Uses Discord for Command and Control

Socket's Threat Research Team uncovered a large-scale phishing operation named Beamglea, which abused 175 malicious npm[27] packages (26,000+ downloads) to host redirect scripts on legitimate infrastructure such as npm's public registry and the `unpkg.com` CDN. Rather than deploying malware, the packages turned the open-source supply chain into phishing infrastructure, redirecting victims to credential-harvesting portals themed as business or Microsoft login pages. The attackers automated their workflow through Python scripts that generated randomized package names, injected victim-specific details, and published them to npm, with unpkg.com automatically serving each package as a trusted HTTPS resource. HTML lures disguised as purchase orders, project specs, and technical documents loaded these scripts directly from `unpkg.com`, allowing the campaign to scale quickly without hosting costs or SSL management.

Zimperium zLabs identified ClayRat[28], a fast-evolving Android spyware campaign primarily targeting Russian users through Telegram channels and phishing sites impersonating popular apps like WhatsApp, YouTube, and Google Photos. Once installed, ClayRat can exfiltrate SMS messages, call logs, notifications, and device info, take photos, and even send SMS or make calls directly from the victim's device. Its most dangerous feature is the abuse of Android's default SMS handler role, which grants broad messaging access and allows it to spread autonomously by sending malicious links ("Узнай первым! <link>") to every contact in the victim's phone book – turning each infected device into a distribution hub. Over 600 samples and 50 droppers have been detected in just three months, with variants adding new obfuscation, encryption (AES-GCM), and session-based installers that mimic Google Play updates to bypass Android 13 restrictions. ClayRat communicates with its C2 servers via HTTP and supports commands for surveillance, propagation, and device control.

CYJAX researchers uncovered a search engine[29] poisoning campaign that impersonates 14 global airlines – including KLM, Delta, Lufthansa, Emirates, and Singapore Airlines – using over 150 fake "support" webpages hosted on Cloudflare's `pages.dev` platform. These sites display fraudulent customer service numbers, tricking travelers into calling scammers posing as airline agents. Each fake page is packed with airline-related keywords ("support", "contact list", "helpdesk") to boost SEO visibility and manipulate both traditional and AI-enhanced search results. In one case, a fake phone number appeared directly in Google's AI-generated answer box, confirming that poisoned content is influencing AI-driven search summaries. The pages contain no phishing forms or downloads but instead rely on data poisoning, using structured FAQ markup and keyword repetition to rank high in results and appear in rich snippets.

McAfee Labs uncovered a new Astaroth[30] banking trojan campaign that abuses GitHub repositories to host its malware configurations, ensuring resilience even after takedowns of traditional C2 servers. Delivered via phishing emails with malicious ZIP archives containing Windows shortcut (.LNK) files, the infection chain executes obfuscated JavaScript through `mshta.exe`, downloads AutoIt-based loaders, and injects the Astaroth payload into memory. Written in Delphi, the malware employs anti-analysis techniques, keylogs credentials when users access banking or cryptocurrency websites, and exfiltrates data via Ngrok reverse proxies. Its configuration updates every two hours by downloading image files hosted on GitHub, which conceal C2 details through steganography – allowing dynamic reconfiguration without exposing raw indicators.

Koi Security researchers uncovered a major TigerJack[31] malware campaign infiltrating developer ecosystems through malicious Visual Studio Code extensions, impacting over 17,000 developers. Operating under aliases ab-498, 498, and 498-00, the threat actor published at least 11 extensions that appeared to provide legitimate functionality – such as real-time C++ compilation and HTTP formatting – while secretly exfiltrating source code,

[27] 175 Malicious npm Packages Host Phishing Infrastructure Targeting 135+ Organizations
[28] ClayRat: A New Android Spyware Targeting Russia
[29] Engine Fault: Search engine poisoning targets airline support numbers
[30] Astaroth: Banking Trojan Abusing GitHub for Resilience
[31] TigerJack's Extensions Continue to Rob Developers Blind Across Different Marketplaces

mining cryptocurrency, and deploying remote execution backdoors. The "C++ Playground" extension uploads developers' source code to multiple endpoints, including a subdomain `ab498.pythonanywhere[.]com`, which is not part of the legitimate PythonAnywhere service but rather a user-controlled workspace on that trusted platform abused for data collection, allowing the attacker to leverage a whitelisted domain to evade detection. Meanwhile, the "HTTP Format" extension covertly runs CoinIMP miners, draining CPU resources, while other variants poll attacker infrastructure every 20 minutes for new payloads using JavaScript `eval()` calls – granting full remote control of infected systems. Although Microsoft eventually removed several of these extensions, they remain active on OpenVSX, used by IDEs such as Cursor and Windsurf, which lack robust malware scanning. Koi researchers note that TigerJack's use of legitimate cloud platforms like PythonAnywhere for staging and C2 operations, combined with cross-marketplace republishing under new names.

Cyble Research and Intelligence Labs uncovered a resurgence of GhostBat[32] RAT, an Android malware posing as India's RTO/mParivahan app to steal banking data, mine cryptocurrency, and harvest OTPs via Telegram bot registration. Distributed through WhatsApp, SMS smishing links, GitHub-hosted APKs, and compromised websites, the campaign uses multi-stage droppers, ZIP header manipulation, and native (.so) packers to evade detection. Once installed, the fake app requests SMS permissions, loads phishing pages mimicking UPI payments, and exfiltrates banking keywords and PINs to Firebase and C2 servers. Some variants embed cryptominers while registering infected devices via the Telegram bot `GhostBatRat_bot`. The campaign, active since mid-2025, primarily targets Indian Android users.

Koi Security researchers uncovered GlassWorm[33], the first known self-propagating worm targeting VS Code extensions in the OpenVSX marketplace. The campaign compromises legitimate developer extensions and hides its payload inside invisible Unicode characters, making the malicious code literally undetectable in editors or Git diffs. Once executed, GlassWorm connects to an immutable Solana blockchain C2, reading commands and payload links from transaction memos – a takedown-proof control channel – and uses Google Calendar as a fallback C2. Its payload, dubbed ZOMBI, turns infected developer machines into RAT-controlled proxy nodes that steal GitHub, npm, and crypto wallet credentials, install hidden VNC access, deploy SOCKS proxies, and spread automatically using stolen tokens. Within 24 hours, at least 35,000 downloads of infected extensions were recorded, with multiple variants still active across OpenVSX and VS Code.

Arctic Wolf Labs uncovered Caminho[34], a Brazilian Loader-as-a-Service (LaaS) that hides .NET payloads inside image files using LSB steganography and executes them filelessly to deliver malware such as REMCOS RAT, XWorm, and Katz Stealer. Active since early 2025, the operation spreads via phishing emails with JavaScript or VBS archives, which download PowerShell scripts retrieving steganographic images from `archive.org`. The concealed Caminho loader extracts and injects the payload into `calc.exe`, establishing persistence through scheduled tasks.

Researchers analyzed Vidar[35] Stealer 2.0, a major rewrite of the long-running infostealer, now fully implemented in C with a multithreaded architecture for faster data theft and enhanced evasion. The new version improves browser credential extraction, bypassing Chrome's AppBound encryption by injecting code into running browser processes and stealing keys directly from memory. Vidar 2.0 also introduces an automatic polymorphic builder to generate unique samples and uses control-flow flattening for anti-analysis. Its broad theft scope includes credentials from browsers, cloud services, crypto wallets, gaming, and communication apps like Telegram and

[32] GhostBat RAT: Inside the Resurgence of RTO-Themed Android Malware
[33] GlassWorm: First Self-Propagating Worm Using Invisible Code Hits OpenVSX Marketplace
[34] Brazilian Caminho Loader Employs LSB Steganography and Fileless Execution to Deliver Multiple Malware Families Across South America, Africa, and Eastern Europe
[35] Fast, Broad, and Elusive: How Vidar Stealer 2.0 Upgrades Infostealer Capabilities

Discord. Following Lumma Stealer's decline, Vidar 2.0 is rapidly gaining adoption across underground markets, signaling its rise as the next dominant infostealer in global cybercrime campaigns.

Trend Micro uncovered Operation Zero Disco[36], a campaign exploiting the Cisco SNMP vulnerability (CVE-2025-20352) to deploy Linux-based rootkits on Cisco 9400, 9300, and legacy 3750G switches. Attackers achieved remote code execution, installed hooks in the IOSd memory, and set a universal "disco" password for persistent access. The implants could hide configurations, disable logs, bypass AAA and VTY ACLs, and manipulate timestamps to erase traces. In some cases, a modified Telnet exploit enabled direct memory read/write, while ARP spoofing allowed lateral movement across VLANs. The rootkit's UDP controller managed authentication bypass and covert command control.

CYFIRMA uncovered GhostGrab[37], a sophisticated Android malware that merges cryptocurrency mining with large-scale banking credential theft, representing a new hybrid threat in mobile cybercrime. Distributed through fake update apps, GhostGrab abuses broad Android permissions to intercept SMS messages, harvest financial and personal data, and secretly mine cryptocurrency in the background. It impersonates legitimate banking and KYC portals using in-app WebViews to deceive users into entering sensitive details such as debit card numbers, CVVs, PINs, and internet banking credentials. The malware hides its icon, maintains persistence through foreground services and auto-restart mechanisms, and exfiltrates stolen data via encrypted cloud channels.

IBM X-Force uncovered a phishing campaign in Latin America, primarily targeting Colombian users, that impersonates the Attorney General's Office of Colombia to distribute HijackLoader, which ultimately deploys the PureHVNC remote access trojan[38]. Victims receive judicial-themed emails containing SVG files hosted on Google Drive, which trigger the download of a password-protected ZIP carrying a renamed legitimate Java executable used for DLL side-loading. The chain executes multiple payload stages, culminating in HijackLoader modules responsible for DLL hollowing, privilege escalation, persistence via LNK or scheduled tasks, and injection of PureHVNC. The malware employs anti-VM, unhooking, and indirect API-calling techniques to evade detection and verify execution environments before activating. IBM notes that this marks one of the first observed uses of PureHVNC in Spanish-language campaigns, indicating an expansion of dark-web tooling into LATAM-focused attacks that leverage judicial-themed phishing lures and modular loaders for stealthy remote control and credential theft.

Bitsight researchers analyzed a persistent Brazilian spam campaign delivering the Lampion[39] stealer, which has evolved with multi-stage Visual Basic scripts, ClickFix lures, and new persistence mechanisms. Active for over a year, the campaign uses compromised corporate email accounts to distribute ZIP attachments disguised as payment receipts, replacing earlier link-based delivery. The infection chain involves multiple obfuscated VBS scripts that download and execute payloads in stages, culminating in a large Delphi-based DLL acting as the stealer. This final payload collects system, user, and antivirus information, terminates browsers to capture data, and uses file bloating and advanced obfuscation to evade detection. Lampion's operators employ cloud infrastructure with IP filtering, automation to generate numerous unique samples, and modular persistence through scheduled tasks and startup scripts.

Researchers at ReversingLabs identified and tracked an evolving[40] family of Discord-based remote access trojans (RATs) operated by a threat actor calling itself STD Group. The campaign comprises four related C++ RATs – UwUdisRAT, STD RAT, Minecraft RAT, and Propionanilide RAT – all using Discord bot tokens and server IDs for

[36] Operation Zero Disco: Attackers Exploit Cisco SNMP Vulnerability to Deploy Rootkits
[37] GHOSTGRAB ANDROID MALWARE
[38] X-Force Threat Analysis Report: LATAM baited into the delivery of PureHVNC
[39] From Brazil with Love: New Tactics from Lampion
[40] Tracking an evolving Discord-based RAT family

command-and-control communication. Early variants stored credentials in plaintext, while later ones used a ROT23 cipher and stack-string obfuscation to conceal tokens. The newest variant, Propionanilide RAT, introduced a custom packer dubbed Proplock / STD Crypter, combining XZ + LZMA2 compression and rolling XOR encryption. The malware family shares mutex strings ("std"), embedded decoy tokens, and links to older .NET samples labeled "AnyDesks," suggesting ongoing code reuse by STD Group.

Koi Security uncovered a large-scale supply-chain campaign named PhantomRaven[41], involving 126 malicious npm packages that collectively amassed over 86,000 downloads. The operation covertly stole npm tokens, GitHub credentials, and CI/CD secrets by exploiting a novel method called Remote Dynamic Dependencies (RDD) – fetching hidden malicious code from `packages.storeartifact.com` during installation, invisible to dependency scanners. The malware used preinstall scripts to auto-execute payloads, exfiltrating system, network, and developer data via HTTP and WebSocket channels to `jpd.php` on the same server. Attackers registered packages mimicking legitimate libraries and exploited AI-generated "hallucinated" package names, a tactic dubbed slopsquatting, to trick developers relying on coding assistants.

For more information, please contact: crimewareintel@kaspersky.com.

[41] PhantomRaven: NPM Malware Hidden in Invisible Dependencies

The monthly brief – summary of Kaspersky's private reports for October 2025

Researcher Notes – Campaigns Impersonating Mexican Tax Entity to Deliver Malicious Browser Extensions

During our monitoring of campaigns attacking Mexican users, we regularly look for websites seeking to impersonate entities such as the Tax Administration Service (Servicio de Administración Tributaria, SAT), the National Population Registry in Mexico (Registro Nacional de Población, RENAPO), and official personal documentation such as the Unique Population Registry Code (CURP), passports, or birth certificates. This monitoring is the result of previous research[42] into campaigns targeting Mexico.

We initially identified and reported[43] locally about websites seeking to steal personal and banking information from Mexicans by impersonating the service to schedule an appointment to obtain their passports. In this line of scams seeking to impersonate the appointment scheduling service of Mexican official entities, we identified some websites that impersonate the appointment service in the SAT to distribute malicious browser extensions.

This report describes an update in the infection chain of this campaign and the analysis of each of the artifacts involved, including the functioning of the malicious extension.

Tsundere: an emerging NodeJS-based botnet

We have identified a new and evolving threat, which we named the Tsundere botnet. This NodeJS-based malware has been spreading through various means, including MSI installers disguised as fake game installers or documents, as well as PowerShell scripts. The Tsundere bot has been observed using WebSockets for command and control (C2) communication and has implemented a unique mechanism for hosting its C2 addresses, utilizing Web3 contracts, also known as smart contracts, on the Ethereum blockchain. This approach allows the threat actor to maintain a level of anonymity, making it more challenging for security researchers to disrupt the botnet's operations. The botnet's infrastructure includes a panel for monitoring and managing infected devices, as well as a marketplace where users can promote and sell access to compromised machines. At the time of our research, the panel had approximately 100 active bots connected to the C2 server at any given time.

Maverick: A Banking Trojan Utilizing WhatsApp for Propagation in a Multi-Stage Infection Chain

A recent malware campaign targeting Brazil has been detected, involving the distribution of a malicious LNK file via WhatsApp. The campaign primarily targets Brazilian users and utilizes Portuguese-named URLs. To evade detection, the command-and-control (C2) server verifies each download to ensure it originates from the malware itself. The infection chain is complex and entirely fileless, ultimately delivering a new banking trojan known as Maverick. Notably, Maverick shares significant code similarities with the Coyote trojan[44]. This report will provide a detailed analysis of the infection chain, encryption algorithm, and trojan's targets, as well as discuss the similarities with known threats.

Pro-Ukrainian threat actors collaboration and their unique tools

This report examines a series of coordinated cyberattacks carried out by multiple hacktivist groups, with a focus on the activities of pro-Ukrainian actors. A notable aspect of these incidents is the simultaneous involvement of two to three distinct groups targeting a single victim. This overlapping activity significantly complicates attribution, as distinguishing the tactics, techniques, and procedures (TTPs) of each group becomes challenging.

[42] LambadaRanchera Threat Cluster Targeting Banking Users in Mexico
[43] Advierte Kaspersky por ciberfraude en trámites de pasaporte en México
[44] Coyote: A multi-stage banking Trojan abusing the Squirrel installer | Securelist

Analysis of digital artifacts revealed strong evidence of the use of specific tools and malware, including 4BID ransomware, BO TEAM backdoors, and other unique components. These indicators suggest the attacks were collaborative, with multiple groups operating in parallel or in a coordinated manner to achieve shared objectives.

Researcher Notes – NTLM vulnerabilities, ongoing exploitation in 2025

Microsoft has long announced its intention to retire NTLM; however, as time passes, the protocol remains present for legacy compatibility. This continued presence leaves an open door for attackers, who persist in leveraging well-known NTLM attack vectors while also discovering new vulnerabilities to exploit the protocol.

In this report, we examine the numerous NTLM-related vulnerabilities identified over the past year, along with the cybercriminal campaigns that have actively weaponized them across various regions of the world.