
Weekly Cybersecurity Briefing (25 May – 31 May 2026)

CyberSecBrief Team

CyberSecBrief provides clear, concise cybersecurity briefings that summarise the most relevant developments of the week. The report highlights notable incidents, key themes, and significant activity across the threat landscape, supported by daily updates sourced from trusted feeds and advisories. Its purpose is to offer a practical, time-efficient overview for readers who need a reliable snapshot of current cybersecurity events.

For more briefings, visit CYBERSECBRIEF.COM.



June 1, 2026

Overview of the Week

A week of large-scale infrastructure takedowns, high-impact data breaches and novel AI agent exploits.

- **Dutch authorities arrested two individuals and seized over 800 servers** linked to MIRhosting and WorkTitans, companies providing infrastructure to EU-sanctioned Russian entities connected to Stark Industries and attacks on Danish government organisations.
- **A separate Dutch operation dismantled a 17-million-device botnet**, seizing over 200 servers linked to proxy service Asocks and used in distributed denial-of-service and traffic proxying activity.
- **ShinyHunters was linked to two major breaches**: a Canvas LMS compromise exposing accounts tied to approximately 275 million users, and a Carnival Corporation breach affecting nearly six million individuals following a social engineering attack on an employee account.
- **CrowdStrike coordinated the takedown of the Glassworm botnet**, which targeted software developers through trojanised VSCode extensions, poisoned npm and Python packages, and compromised GitHub repositories using blockchain and peer-to-peer command-and-control.
- **The Lazarus Group deployed the RemotePE memory-only RAT** against financial and cryptocurrency organisations, using DPAPI encryption, ETW suppression and in-memory execution to evade forensic detection.
- **Adversa AI disclosed SymJack**, a symlink-based attack technique achieving remote code execution against Claude Code, Gemini CLI, Cursor, GitHub Copilot CLI, Grok Build and OpenAI Codex CLI through malicious repository configurations.

Key developments:

- Glassworm botnet takedown
- ShinyHunters breaches
- RemotePE RAT (Lazarus)
- SymJack AI agent RCE
- Dutch infrastructure seizures
- Tycoon 2FA AiTM phishing
- Gentlemen ransomware
- Canvas LMS breach
- Chrome 148 patches

- DPRK supply-chain activity

Highlights of the Week

Dutch Police Seize Servers Linked to Russian Cyber Operations

Dutch financial crime investigators arrested two men and seized more than 800 servers during raids targeting MIRhosting and WorkTitans, companies accused of providing infrastructure to EU-sanctioned Russian entities. Authorities said the firms operated network infrastructure linked to Stark Industries, a hosting provider associated with distributed denial-of-service attacks and cyber operations attributed to Russian intelligence groups. De Volkskrant reported that WorkTitans and MIRhosting networks were heavily used in pro-Russian attacks against Danish government organisations during Denmark's municipal elections in November 2025.

Sources:

- [KrebsOnSecurity](#)

ShinyHunters Supply Chain Attack Hits Canvas LMS Platform

ShinyHunters accessed Canvas LMS operated by Instructure, exposing accounts and data tied to approximately 275 million users across education institutions globally. The platform was shut down during incident response, and Instructure disabled Free-For-Teacher accounts after attackers exploited an unspecified vulnerability in the system. Instructure announced on May 12 an agreement to pay ShinyHunters to prevent public disclosure of stolen data, while services were gradually restored.

Sources:

- [ReversingLabs](#)

CrowdStrike Disrupts Glassworm Developer Supply Chain Botnet

CrowdStrike executed a coordinated takedown of the Glassworm botnet on 26 May 2026, targeting developers through supply chain compromises across open-source ecosystems. Operators distributed trojanised VSCode extensions, poisoned npm and Python packages, and compromised GitHub repositories while using Solana blockchain, BitTorrent DHT and Google Calendar for command-and-control. In collaboration with Google and Shadowserver Foundation, CrowdStrike simultaneously disrupted four command-and-control channels, severing Glassworm operators' access and halting further payload delivery capabilities.

Sources:

- [CrowdStrike Counter Adversary Operations](#)

SymJack Attack Hijacks AI Coding Agents Through Symlinked Repositories

Adversa AI disclosed SymJack, a symlink-based attack technique that achieved remote code execution against Claude Code, Gemini CLI, Cursor Agent CLI, GitHub Copilot CLI, Grok Build and OpenAI Codex CLI by overwriting agent configuration files through disguised shell copy operations. The attack used malicious repositories containing symlinked media files and hidden instruction files to trick agents into writing attacker-controlled MCP server configurations, which then executed arbitrary commands on the next restart with the user's privileges. Adversa AI said the technique also affected CI runners configured to auto-trust workspaces, potentially exposing deploy keys, cloud credentials and registry tokens through a single malicious pull request.

Sources:

- [Adversa AI](#)

Dutch Authorities Dismantle Malware Botnet Infecting 17 Million Devices

Dutch authorities took offline a malware botnet involving 17 million infected devices and seized over 200 servers in the Netherlands. Police and the National Cyber Security Centre said the infrastructure controlled computers, tablets and smartphones used in cyberattacks and was linked to proxy service Asocks. Authorities confirmed the seized servers supported distributed denial-of-service, traffic proxying and other illicit activity across the botnet network.

Sources:

- [BleepingComputer](#)

Threats

Lazarus Deploys Memory-Only RemotePE Malware Chain

Fox-IT analysed a Lazarus-linked malware chain comprising DPAPILoader, RemotePELoader and RemotePE, targeting financial and cryptocurrency organisations using DPAPI encryption, reflective PE loading and fully memory-resident execution. RemotePELoader retrieves AES-GCM encrypted payloads from HTTP-based command-and-control servers, disables ETW logging, remaps clean ntdll.dll sections through HellsGate syscalls and polls operators for manually delivered malware stages. The final-stage RemotePE RAT supports file operations, process execution, plugin loading and secure file deletion, while using Microsoft-themed cookie fields and JSON keys to disguise command-and-control traffic on Namecheap-hosted infrastructure.

Sources:

- [Fox-IT](#)

ShinyHunters Breach Exposes Six Million Carnival Records

Carnival confirmed a breach linked to ShinyHunters involving an April 14 social engineering attack on an employee affecting six million individuals. Exposed data included names, addresses, emails, phone numbers, birth dates and state ID numbers, with the company filing with the Maine attorney general recording just under six million affected individuals. ShinyHunters claimed attackers breached a Salesforce environment, stole more than 600,000 records and published a 9.4GB archive after ransom demands were rejected.

Sources:

- [The Register](#)

North Korean Group Targets macOS Financial Sector in Multi-Stage Campaign

Sapphire Sleet, a North Korean group tracked as BlueNoroff and UNC1069, ran a macOS intrusion campaign targeting financial and cryptocurrency organisations using a fake Zoom SDK update. Initial access used social engineering delivering an AppleScript executed through Script Editor, osascript and curl, with a fake macOS password prompt used for credential harvesting and Finder abused for TCC[.]db manipulation under Full Disk Access permissions. Persistence was established via a LaunchDaemons service enabling data theft from compromised systems.

Sources:

- [LevelBlue](#)

JINX-0164 Targets Crypto Developers via macOS Malware and CI/CD Intrusions

Wiz identified JINX-0164, a financially motivated threat actor active since mid-2025, conducting social engineering campaigns against cryptocurrency developers using LinkedIn impersonation and fake recruitment lures to deliver macOS malware. The AUDIOFIX Python-based RAT deployed via malicious domains stole macOS Keychain data, browser credentials, SSH keys, cloud API tokens and cryptocurrency wallet extension data, while also exfiltrating secrets from GitHub Actions pipelines. The actor laterally moved into CI/CD systems, modified repositories through commit impersonation and in one case trojanised the npm package [@velora-dex/sdk](#) to distribute the MINIRAT Go backdoor.

Sources:

- [Wiz Research](#)

Kimsuky Deploys JSONPing and New HttpSpy Malware Chain

ENKI WhiteHat researchers identified Kimsuky campaigns targeting South Korean military and corporate organisations through fake security software pages and spoofed Webex meeting sites

that delivered a redesigned HttpSpy remote access trojan. The campaigns introduced a JSONPing technique that uses JSONP requests to localhost services to verify infection status in real time and prompt installation when execution has not occurred. Analysis linked the activity to Kimsuky through shared RC4 keys, infrastructure overlaps and code patterns, with the latest HttpSpy variant supporting command execution, file transfer, screenshot capture and DLL injection.

Sources:

- [ENKI WhiteHat](#)

Lithuania Investigates Foreign Role in National Data Register Leak

Lithuanian authorities are investigating a breach involving more than 600,000 entries from national real estate and legal entity registers accessed using credentials belonging to authorised institutions. Prosecutors said additional cybersecurity restrictions were introduced after the leak, including blocking suspected user accounts and forcing credential updates, while officials suspect involvement by a foreign state actor. The breach prompted the resignation of State Enterprise Centre of Registers head Adrijus Jusas.

Sources:

- [SecurityWeek](#)

Infrastructure & Exploits

KnowledgeDeliver Flaw Enables Remote Code Execution Attacks

Mandiant disclosed CVE-2026-5426, a critical unauthenticated remote code execution flaw in the KnowledgeDeliver learning management system caused by identical ASP.NET machine keys shared across customer deployments. Attackers exploited malicious ViewState deserialisation through the `__VIEWSTATE` parameter, deployed the BLUEBEAM in-memory web shell inside IIS worker processes and modified JavaScript files to load remote malicious scripts. Mandiant observed the compromised sites delivering fake security plugin installers that infected users with Cobalt Strike BEACON payloads encrypted using organisation-specific keys.

Sources:

- [Google Threat Intelligence Group](#)

Gitea Flaw Exposes Private Container Images Without Authentication

Orca Security disclosed CVE-2026-27771, a critical access control vulnerability in Gitea's built-in container registry allowing unauthenticated attackers to pull private OCI images without credentials or tokens. The flaw affects all Gitea versions before 1.26.2 and also impacts Forgejo,

with researchers estimating roughly 31,750 internet-facing instances across more than 30 countries potentially exposed. Orca said attackers could retrieve application source code, API keys, database credentials and infrastructure configurations embedded within private images, with the vulnerability reportedly undetected for approximately four years.

Sources:

- [Orca Security](#)

Unpatched Gogs Flaw Enables Authenticated Server Takeover

Rapid7 disclosed a critical CVSS 9.4 argument injection vulnerability in Gogs that allows any authenticated user to achieve remote code execution through the “Rebase before merging” feature. The flaw abuses malicious branch names to inject the Git `--exec` flag during `git rebase`, enabling command execution as the Gogs service account without administrator privileges or user interaction. Rapid7 confirmed the issue in Gogs 0.14.2 and 0.15.0+dev across Linux, macOS and Windows deployments, with no vendor patch available at disclosure.

Sources:

- [Rapid7](#)

CIFSwitch Flaw Grants Root Access on Linux Systems

Researcher Asim Manizada disclosed CIFSwitch, a local privilege escalation vulnerability affecting Linux systems using vulnerable CIFS kernel code and certain cifs-utils versions. The flaw allows unprivileged users to create forged cifs.spnego key requests that launch the root-privileged cifs.upcall helper, which trusts attacker-controlled fields including pid and upcall_target. Exploitation abuses namespace switching and NSS module loading to execute attacker-controlled code as root, with confirmed impact on multiple Ubuntu, Debian, Rocky Linux, CentOS Stream, Kali Linux and SUSE configurations.

Sources:

- [Asim Viladi Oglu Manizada](#)

FortiClient EMS Exploited to Deploy EKZ Infostealer via CVE-2026-35616

Arctic Wolf observed exploitation of CVE-2026-35616 affecting FortiClient Endpoint Management Server, allowing unauthenticated attackers to bypass API authentication and modify EMS configurations to distribute malicious updates. The campaign leveraged FortiClient EMS to push PowerShell commands via Remote Access Profile settings, which executed on managed endpoints through fortitray.exe and deployed a credential stealer named EKZ Infostealer. The malware extracted credentials from Chromium- and Firefox-based browsers, staging results locally before exfiltration over HTTP to attacker-controlled infrastructure.

Sources:

- [Arctic Wolf Labs](#)

AI Agent Uses LLM to Drive Rapid Cloud Intrusion via CVE

Sysdig reported an intrusion where an LLM agent exploited CVE-2026-39987 in a marimo notebook to gain initial remote code execution access. The attacker pivoted using harvested AWS credentials, retrieved secrets from Secrets Manager, and used Cloudflare Workers and SSH bastion to exfiltrate an internal PostgreSQL database. Sysdig stated the end-to-end compromise from initial access to database dump occurred in under one hour, with the bastion exfiltration completing in under two minutes.

Sources:

- [Sysdig](#)

Chrome 148 Fixes 151 Security Flaws

Google released Chrome 148 to address 151 vulnerabilities, including 22 critical flaws such as CVE-2026-9872, an out-of-bounds write in GPU, and CVE-2026-9873, a use-after-free issue in Network. Additional critical vulnerabilities include CVE-2026-9874 in Dawn, CVE-2026-9875 in WebGL and CVE-2026-9876 in WebGL, with use-after-free defects accounting for most critical findings. The update also fixes 123 high-severity and six medium-severity vulnerabilities across components including ANGLE, Skia, V8, WebRTC and PDFium, with more than \$130,000 awarded for externally reported bugs.

Sources:

- [SecurityWeek](#)
- [Google Chrome Releases](#)

Flowise Chatflow Import Triggers One-Click Server Compromise

Obsidian Security disclosed CVE-2026-40933, a one-click remote code execution vulnerability in self-hosted Flowise deployments where Custom MCP tools can launch user-supplied stdio MCP commands as server-side child processes. A crafted chatflow JSON can embed a malicious MCP configuration, and importing the workflow automatically triggers command execution when Flowise enumerates available MCP actions during canvas rendering. Researchers found current validation controls can be bypassed, enabling access to server environments, stored credentials, API keys and connected cloud or SaaS services, while Flowise Cloud is unaffected because stdio MCP is disabled.

Sources:

- [Obsidian Security](#)

Tools & Techniques

Kali365 Steals Microsoft 365 Tokens Through Device Code Phishing

The FBI warned that the Kali365 phishing-as-a-service platform, first observed in April 2026 and distributed through Telegram, enables attackers to steal Microsoft 365 OAuth tokens and bypass multi-factor authentication. Kali365 campaigns send phishing emails containing device codes that direct victims to legitimate Microsoft verification pages, where entered codes authorise attacker-controlled devices to access accounts. The stolen access and refresh tokens provide persistent access to Microsoft 365 services including Outlook, Teams and OneDrive without requiring passwords or additional MFA prompts, while the platform also offers AI-generated phishing lures and real-time tracking dashboards.

Sources:

- [Federal Bureau of Investigation](#)

Chinese Phishing Platforms Target Digital Wallets Worldwide

Google Threat Intelligence Group analysed multiple Chinese-language phishing-as-a-service platforms that use Telegram, RCS and iMessage to deliver phishing campaigns targeting payment cards, digital wallets and account credentials across international markets. The services provide real-time interception panels that capture one-time passcodes, enabling attackers to provision stolen payment cards into attacker-controlled digital wallets for contactless payments and ATM withdrawals. Google linked the Darcula platform to UNC5814 and reported that operators increasingly use AI-generated phishing pages and browser automation tools impersonating brands including Apple, Amazon, PayPay, Nintendo and Japanese financial institutions.

Sources:

- [Google Threat Intelligence Group](#)

Tycoon 2FA AiTM Phishing Bypasses MFA Across Entra ID

Elastic analysed Tycoon 2FA AiTM phishing-as-a-service targeting Microsoft Entra ID and Google Workspace, using reverse-proxy credential theft and session token interception to bypass multi-factor authentication. Campaign variants include WebSocket-based relays and OAuth device-code abuse, with infrastructure using cloud VPS ASNs and real-time token forwarding to capture session cookies and refresh tokens. Detection engineering identified Graph API reconnaissance bursts, device registration persistence via primaryRefreshToken, and cross-ASN sign-ins enabling automated compromise across enterprise identity systems.

Sources:

- [Elastic Security Labs](#)

Cryptojacking Campaign Uses AI Chatbots and Fake Utility Downloads

Microsoft identified a cryptojacking campaign using SEO poisoning and AI chatbot responses to direct users to fake downloads impersonating CrystalDiskInfo, HWMonitor, FurMark and other Windows utilities favoured by GPU owners. The malware chain used DLL sideloading, abused ConnectWise ScreenConnect for persistent remote access, deployed a SimpleRunPE-based loader, and hollowed Microsoft-signed .NET binaries including InstallUtil.exe and MSBuild.exe to run GPU miners such as lolMiner and SRBMiner-MULTI.

Sources:

- [Microsoft](#)

Microsoft Details Self-Propagating Gentlemen Ransomware Go Variant

Microsoft documented the Gentlemen ransomware operated by Storm-2697 as a Go-based RaaS encryptor targeting Windows systems with self-propagating capabilities and double extortion. It uses Curve25519 and XChaCha20 per-file encryption and a self-propagation module that abuses multiple Windows lateral movement techniques including PsExec, WMI and scheduled tasks. The malware disables Microsoft Defender, deletes shadow copies and event logs, and terminates security, backup and database services during network-wide compromise across enterprise environments.

Sources:

- [Microsoft Threat Intelligence](#)

DriveSurge Hijacks Thousands of Sites for Malware Delivery

Silent Push identified a threat actor named DriveSurge that uses the zTDS traffic distribution system to compromise thousands of legitimate websites and redirect visitors to ClickFix and FakeUpdates malware campaigns. The operation serves fake browser updates impersonating Chrome, Firefox, Edge and Safari, with observed downloads including malicious ZIP archives and executables. Researchers also analysed an obfuscated macOS infection chain that hijacks clipboard contents, delivers payloads from attacker-controlled servers and connects to command-and-control infrastructure at 147.45.42.205:8133.

Sources:

- [Silent Push](#)

Malicious Packagist Branch Delivers DPRK-Linked Malware Loader

Socket discovered malicious JavaScript hidden in the Packagist development release of the legitimate PHP package [roberts/leads](#), with the payload appended to a Tailwind configuration file in an exposed development branch. The loader contacts TRON, Aptos and BNB Smart Chain infrastructure to retrieve encrypted payloads, decrypts them with embedded XOR keys, executes them via `eval()` and can launch detached Node.js child processes. Researchers linked the infrastructure and techniques to Famous Chollima activity, noting similarities to Contagious Interview campaigns and previous delivery of BeaverTail, DEV#POPPER RAT and OmniStealer malware.

Sources:

- [Socket](#)

Malicious npm Packages Impersonate OpenSearch Libraries and Steal Credentials

A single npm maintainer published 14 malicious packages in four hours impersonating OpenSearch and Elasticsearch libraries using typosquatting and lookalike names, Microsoft reported. Packages used install-time hooks to run stagers collecting host and CI/CD environment data, exfiltrating it to command-and-control servers and delivering second-stage payloads. All 14 packages were removed after discovery, with payloads persisting across module re-imports and optionally using the Bun runtime for additional credential theft.

Sources:

- [The Register](#)

Malicious Codex UI Package Exfiltrates AI Authentication Tokens

Aikido Security identified `codexui-android` as a compromised remote web UI for OpenAI Codex that exfiltrates authentication data from users' local environments. The npm package executes a preloaded module at startup that reads `~/ .codex/auth.json` and sends access, refresh and ID tokens to an attacker-controlled endpoint via HTTPS. The same tooling is distributed through an Android application that installs a Node.js runtime and executes the package inside a PRoot sandbox, enabling repeated token theft during normal use.

Sources:

- [Aikido Security](#)

Policy & Legal

California Sues 23andMe Over 2023 Data Breach

California Attorney General Rob Bonta sued 23andMe, now operating as Chrome Holding Co., alleging the company failed to protect sensitive genetic and personal data exposed in a 2023 credential-stuffing attack. The breach compromised roughly 14,000 accounts and enabled access to data belonging to nearly 7 million customers, including genetic information, health reports, DNA matching details and relatives' location data. The lawsuit alleges attackers remained undetected for more than five months while warning signs including unusual login activity and reports of stolen data surfaced before the company disclosed the incident.

Sources:

- [SecurityWeek](#)

FBI Warns of FIFA Website Spoofing Ahead of 2026 World Cup

The FBI issued a PSA warning that cyber actors are spoofing FIFA websites ahead of the 2026 World Cup using typosquatting, with spoofed sites mimicking fifa.com with minor spelling changes and alternative domains. Campaigns harvest names, addresses and banking details, and sell fake tickets and hospitality products through fraudulent portals. The FBI listed multiple example domains including fifa[.]cab, fifa[.]pink, fifa[.]help and fifa-2026[.]xyz identified for fraud monitoring and reporting via IC3.

Sources:

- [Federal Bureau of Investigation \(IC3\)](#)

Silent Ransom Group Uses IT Impersonation for Data Theft at US Law Firms

The FBI reported that the Silent Ransom Group, also known as Luna Moth and Chatty Spider, has conducted social engineering campaigns targeting US law firms through impersonation of IT support personnel since spring 2026. Actors use phone calls and phishing emails to trick victims into granting remote access, after which legitimate tools such as WinSCP, Rclone and cloud storage services are used to exfiltrate data without deploying ransomware encryption. In some cases, attackers escalate to physical access by visiting victim premises and using removable media to extract data, followed by extortion threats and publication on a dedicated leak site.

Sources:

- [FBI IC3](#)

Microsoft Condemns Uncoordinated Windows Zero-Day Releases

Microsoft criticised a campaign by researcher Nightmare Eclipse that publicly released six Windows zero-day vulnerabilities with proof-of-concept code on GitHub and Blogger without coordi-

nated disclosure. Three flaws disclosed in April — BlueHammer, UnDefend and RedSun — have been exploited in attacks and are listed in CISA's Known Exploited Vulnerabilities catalogue, while YellowKey, GreenPlasma and MiniPlasma remain unpatched. Microsoft stated that disclosures providing exploit code for unpatched vulnerabilities are "never justifiable" and said its Digital Crimes Unit pursues threat actors and those enabling criminal activity.

Sources:

- [Recorded Future News](#)

Weekly Topic Distribution



Copyright and Legal Notice

© CyberSecBrief. All rights reserved.

Reproduction, redistribution, or modification of this document or its contents without explicit written permission is strictly prohibited.

Disclaimer & Terms of Use

CyberSecBrief is a personal, non-commercial project operated from Germany and is not affiliated with any company or organisation. The information provided is intended solely for general informational and educational purposes and does not constitute professional cybersecurity, legal, or financial advice. Security-related information changes rapidly; although accuracy and timeliness are sought, no guarantee is given regarding completeness, correctness, or applicability. Users must verify details with official sources or qualified professionals before making decisions.

The owner disclaims liability for any indirect, incidental, or consequential damages arising from reliance on this material. External links and third-party feeds are offered for convenience; their content, accuracy, availability, and privacy practices are outside our control and are not endorsed. Sponsored or promoted material may appear, yet inclusion does not imply endorsement.

Original content is protected by copyright. Where external material is used, appropriate attribution is provided. Reproduction of original content without prior written consent is prohibited. Content may be updated, modified, or removed at any time without notice.

This disclaimer and the Terms of Use are governed by the laws of Germany and applicable European Union regulations. Should any provision be deemed invalid, the remaining provisions shall continue in full force and effect.

Credits and Sources

CVE entries are sourced from the [CVE® Program](#), operated by [The MITRE Corporation](#), and from the [National Vulnerability Database \(NVD\)](#), maintained by the National Institute of Standards and Technology (NIST). The NVD is provided “as is” without warranty of any kind.

Definitions for APT groups are derived from the [MITRE ATT&CK® knowledge base](#), reproduced and distributed with the permission of The MITRE Corporation. © 2025 The MITRE Corporation.

All feeds and advisories are properly acknowledged and linked to their original sources where referenced, including within briefings.

Logo icon created by Ida Desi Mariana — [Flaticon](#).

Powered by [CyberFeedBites](#).

Source

This briefing is published by *CyberSecBrief* –
<https://www.cybersecbrief.com/>