
Weekly Cybersecurity Briefing (11 May – 17 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](https://cybersecbrief.com).



May 18, 2026

Overview of the Week

Supply chain attacks, ransomware incidents, and critical infrastructure vulnerabilities defined a turbulent week across the cybersecurity landscape.

- **TeamPCP's expanding supply chain campaign** compromised over 80 TanStack npm packages, Bitwarden CLI, and PyPI libraries including OpenSearch and Mistral AI, using GitHub Actions OIDC token theft to publish malicious versions.
- **ShinyHunters breached Instructure's Canvas Free-For-Teacher** platform on 25 April 2026, exfiltrating 3.65 TB of data covering 275 million records from nearly 9,000 educational institutions, before shifting to school-by-school extortion.
- **Microsoft's May Patch Tuesday** resolved 120 vulnerabilities, including a critical zero-click remote code execution flaw in Outlook and Word (CVE-2026-40361) exploitable via the Preview Pane, and no zero-days were disclosed.
- **Foxconn confirmed a Nitrogen ransomware attack** affecting North American factories, with attackers claiming theft of 8 TB of data including schematics linked to Apple, Nvidia, Google, Dell and Intel.
- **Cisco Catalyst SD-WAN CVE-2026-20182** was added to CISA's Known Exploited Vulnerabilities catalog, with active exploitation enabling authentication bypass and webshell deployment by threat actor UAT-8616.
- **The Gentlemen ransomware-as-a-service operation** suffered an internal data leak, exposing affiliate coordination, infrastructure details, ransom negotiations and roughly 332 published victims during 2026.

Key developments:

- TeamPCP supply chain campaign
- TanStack npm compromise
- ShinyHunters Canvas breach
- Nitrogen ransomware / Foxconn
- Cisco SD-WAN CVE-2026-20182
- Microsoft Patch Tuesday
- Fragnesia Linux LPE
- Kazuar P2P botnet
- cPanel CVE-2026-41940
- The Gentlemen ransomware leak

Highlights of the Week

TeamPCP Supply Chain Worm Hits TanStack, Bitwarden and PyPI Ecosystems

Socket and Wiz researchers identified malicious code across 84 compromised npm packages under the TanStack namespace, including @tanstack/react-router, where attackers injected an obfuscated credential stealer targeting GitHub Actions, AWS, Kubernetes and HashiCorp Vault environments. The attack exploited a pull_request_target workflow misconfiguration and GitHub Actions cache poisoning to obtain OIDC tokens, enabling valid signed package publication without compromising maintainer credentials. Trend Micro linked the campaign to TeamPCP, connecting it to earlier compromises of Checkmarx KICS, elementary-data and a trojanised @bitwarden/cli v2026.4.0 package distributed via Docker Hub and PyPI.

Sources:

- [Socket](#)
- [Wiz](#)
- [Trend Micro](#)
- [Endor Labs](#)

ShinyHunters Extorts Schools After Canvas Data Theft

Halcyon reported that ShinyHunters exploited a vulnerability in Instructure's Canvas Free-For-Teacher service on 25 April 2026, claiming theft of 3.65 TB of data containing roughly 275 million records from 8,809 educational institutions. Exposed data included names, institutional email addresses, student ID numbers and Canvas inbox messages, while the group later defaced login portals at around 330 schools after an initial ransom deadline passed. ShinyHunters subsequently shifted from demanding a single payment from Instructure to targeting affected schools individually, with a final negotiation deadline set for 12 May 2026.

Sources:

- [Halcyon](#)

Microsoft Patches Zero-Click Outlook RCE Flaw in May Patch Tuesday

Microsoft May 2026 Patch Tuesday resolved 120 vulnerabilities across Windows and applications, including 17 critical issues and no zero-days. CVE-2026-40361, a critical use-after-free flaw in a shared Microsoft Word and Outlook DLL, enables remote code execution when a victim previews or reads a specially crafted email, with the Preview Pane confirmed as an attack vector. Researcher Haifei Li noted the flaw allows zero-click attacks in Exchange Server environments, affecting Microsoft 365 Apps, Office 2019, Office LTSC and Word 2016.

Sources:

- [BleepingComputer](#)
- [SecurityWeek](#)
- [Microsoft Security Response Center](#)

Foxconn Confirms North American Factories Hit by Nitrogen Ransomware

Foxconn confirmed that several North American factories were impacted by a cyberattack attributed to the Nitrogen ransomware group, which listed the company on its leak site. Attackers claimed theft of approximately 8 TB of data comprising over 11 million files, including confidential documents and schematics linked to Apple, Intel, Google, Dell and Nvidia. Foxconn stated that its cybersecurity team activated incident response procedures and that affected facilities are resuming normal production while investigations continue.

Sources:

- [SecurityWeek](#)
- [The Register](#)

Threats

Kazuar Backdoor Evolves into Modular P2P Botnet

Microsoft Threat Intelligence detailed how Secret Blizzard, a Russian state-aligned threat actor, restructured the Kazuar backdoor into a modular peer-to-peer botnet targeting government and diplomatic organisations in Europe and Central Asia. The updated architecture uses Kernel, Bridge and Worker modules with leader election and inter-process communication via named pipes, mailslots and Windows messaging, reducing observable network activity. Command-and-control channels leverage HTTP, Exchange Web Services and WebSocket transport alongside anti-analysis checks, staged exfiltration and distributed data collection workflows.

Sources:

- [Microsoft Threat Intelligence](#)

BlackFile Operation Uses AiTM Vishing to Breach SaaS Platforms

Google Threat Intelligence Group tracked UNC6671, operating as BlackFile, conducting voice phishing campaigns that deploy adversary-in-the-middle techniques to compromise Microsoft 365 and Okta SSO environments in real time. The group captures credentials and MFA tokens before registering attacker-controlled MFA devices, then uses Python and PowerShell scripts leveraging Microsoft Graph APIs and session cookies to exfiltrate data from SharePoint, OneDrive, Salesforce and Zendesk at scale. Post-compromise activity is recorded as FileAccessed events, supporting extortion operations linked to the ShinyHunters and Scattered Spider ecosystems.

Sources:

- [Google Threat Intelligence Group](#)

The Gentlemen Ransomware Leak Exposes Internal Operations

Check Point Research analysed leaked internal chats and backend data from The Gentlemen ransomware-as-a-service operation, exposing nine operator accounts, affiliate coordination, ransom negotiations and infrastructure linked to roughly 332 published victims during 2026. Leaked conversations identified eight affiliate TOX IDs tied to 29 ransomware campaigns and showed administrator zeta88 directly deploying ransomware and managing payouts. The leak also revealed the group's evaluation of CVE-2024-55591, CVE-2025-32433 and CVE-2025-33073 for network intrusions using Fortinet and Cisco edge devices.

Sources:

- [Check Point Research](#)

TrickMo Android Banking Malware Routes C2 Traffic Through TON

ThreatFabric identified a redesigned TrickMo Android banking malware variant targeting banking, fintech and authenticator applications in France, Italy and Austria through campaigns masquerading as TikTok and streaming apps. The malware routes command-and-control traffic through The Open Network using embedded TON proxy infrastructure and .adnl endpoints, retaining capabilities including credential theft, screen streaming, SMS interception and full device remote control through abused accessibility services. The updated variant adds SSH tunnelling, SOCKS5 proxying and DNS reconnaissance commands, enabling compromised devices to function as encrypted network pivots.

Sources:

- [ThreatFabric](#)

Infrastructure & Exploits

Cisco SD-WAN Authentication Bypass Under Active Exploitation

CISA added CVE-2026-20182, an authentication bypass vulnerability in Cisco Catalyst SD-WAN Controller and Manager, to its Known Exploited Vulnerabilities catalog following confirmed active exploitation attributed to UAT-8616. Cisco Talos reported that multiple post-compromise clusters deployed webshells including XenShell, Godzilla and Behinder, alongside AdaptixC2, Sliver implants, XMRig mining and Nim-based backdoors. Additional flaws CVE-2026-20133, CVE-2026-20128 and CVE-2026-20122 in Cisco SD-WAN Manager were also exploited via publicly released proof-of-concept code.

Sources:

- [Cisco Talos](#)
- [Cybersecurity and Infrastructure Security Agency](#)

Fragnesia Linux Kernel Flaw Enables Root via Page Cache Corruption

Researchers disclosed Fragnesia, a local privilege escalation vulnerability in the Linux kernel's XFRM ESP-in-TCP subsystem tracked as CVE-2026-46300, affecting kernels prior to the 13 May 2026 patch. The flaw stems from improper handling of shared page fragments during skb coalescing, enabling attackers to manipulate AES-GCM decryption in queued TCP data and overwrite cached binaries such as `/usr/bin/su` without modifying files on disk. Researchers demonstrated exploitation using user and network namespaces with `CAP_NET_ADMIN`, while Ubuntu AppArmor restrictions on unprivileged user namespaces may partially mitigate the attack path.

Sources:

- [Wiz](#)
- [V12 Security](#)

cPanel Authentication Bypass Exploited to Deploy Persistent Backdoors

Qianxin XLab reported active exploitation of CVE-2026-41940, a critical unauthenticated authentication bypass in cPanel and WHM with a CVSS score of 9.8, by a threat group tracked as Mr_Rot13. Attackers deployed a Go-based infector that changes root passwords, implants SSH keys, installs PHP webshells and injects credential-stealing JavaScript into cPanel login pages, alongside a cross-platform backdoor named Filemanager for remote administration. XLab linked the activity to infrastructure dating back to 2020, including a previously undetected PHP backdoor uploaded to VirusTotal in 2022 using ROT13 and RC4 obfuscation.

Sources:

- [Qianxin XLab](#)

Windows Zero-Days YellowKey and GreenPlasma Enable BitLocker Bypass

Researchers disclosed two unpatched Windows zero-days, YellowKey and GreenPlasma, enabling BitLocker bypass and SYSTEM-level privilege escalation on Windows 11, Server 2022 and Server 2025. YellowKey exploits Windows Recovery Environment FsTx directory handling to bypass BitLocker via physical access during a reboot, while GreenPlasma enables privilege escalation to SYSTEM through arbitrary memory section object creation in SYSTEM-writable directory objects. A separate MiniPlasma proof-of-concept abuses the `cldfilt.sys` Cloud Filter driver to achieve SYSTEM privileges on fully patched Windows 11 builds.

Sources:

- [SecurityWeek](#)
- [BlackFort TEC](#)
- [BleepingComputer](#)

Microsoft Exchange XSS Flaw Exploited Through Crafted OWA Emails

Microsoft disclosed CVE-2026-42897, a critical spoofing vulnerability in on-premises Exchange Server caused by a cross-site scripting flaw actively exploited in the wild. The vulnerability allows attackers to send crafted emails that execute arbitrary JavaScript in Outlook Web Access browser sessions, affecting Exchange Server 2016, Exchange Server 2019 and Exchange Server Subscription Edition, with Exchange Online unaffected. Microsoft issued temporary mitigations through the Exchange Emergency Mitigation Service while a permanent update is being developed.

Sources:

- [The Hacker News](#)
- [Microsoft Security Response Center](#)

Intel and AMD Address 70 Vulnerabilities Across Product Lines

Intel and AMD released more than two dozen advisories during May 2026 Patch Tuesday, addressing 70 vulnerabilities affecting graphics drivers, firmware, processors and cloud management software. Intel patched a critical buffer overflow flaw CVE-2026-20794 in the Data Center Graphics Driver for VMware ESXi, while AMD fixed CVE-2026-0481 in the ROCm Device Metrics Exporter, which exposed an unauthenticated GPU-Agent gRPC service on port 50061. Additional high-severity issues affected Intel EMA, Vision software and QuickAssist Technology drivers, alongside AMD Secure Processor, EPYC platforms and Zen 2 cache operations.

Sources:

- [SecurityWeek](#)
- [Intel](#)
- [AMD](#)

Tools & Techniques

Google Links AI Tools to Zero-Day Exploit Development and Malware

Google Threat Intelligence Group reported that cybercriminals used an AI-generated Python exploit to target a zero-day two-factor authentication bypass flaw in a popular open-source web administration platform during a planned mass exploitation campaign. The report also

described PROMPTSPY, an Android backdoor that uses the Gemini API to autonomously navigate device interfaces, replay biometric authentication gestures and execute commands through accessibility services. Google linked additional AI-enabled activity to PRC, DPRK and Russia-aligned threat actors using large language models for exploit research, malware obfuscation, phishing reconnaissance and deepfake operations.

Sources:

- [Google Threat Intelligence Group](#)

AMOS macOS Infostealer Spreads via ClickFix Terminal Trick

Sophos MDR reported an AMOS macOS infostealer variant delivered through ClickFix-style social engineering that tricks users into executing Terminal commands, initiating a bootstrap script downloading secondary payloads with elevated privileges. The malware validates passwords locally, harvests macOS Keychain data, browser profiles and cryptocurrency wallet contents, performs virtual machine checks and establishes LaunchDaemon persistence before exfiltrating archived data to attacker-controlled servers. The campaign targets macOS users specifically through staged payload execution designed to evade standard endpoint detection methods.

Sources:

- [Sophos Managed Detection and Response](#)

GemStuffer Campaign Uses RubyGems to Exfiltrate UK Council Data

Socket identified a campaign named GemStuffer that published more than 155 malicious RubyGems packages which scraped UK local government ModernGov portals and exfiltrated collected data through uploaded .gem archives. Payloads fetched calendar and committee pages from Lambeth, Wandsworth and Southwark council portals, embedded the responses into valid gem packages, then pushed them to RubyGems using hardcoded API tokens. Ruby Central temporarily disabled new account registrations and throttled webhooks while responding to the coordinated spam-publishing activity.

Sources:

- [Socket](#)

AD CS Misconfigurations Abused for Privilege Escalation in Enterprise Environments

Palo Alto Networks Unit 42 detailed how attackers are abusing Active Directory Certificate Services misconfigurations, including ESC1 template flaws and shadow credentials, to impersonate privileged accounts and maintain persistent access. Tools including Certify, Certipy and pyWhisker

are being used to exploit permissive certificate templates, manipulate the msDS-KeyCredentialLink attribute and obtain Kerberos tickets through PKINIT authentication. Unit 42 linked these techniques to ransomware and state-backed operations, citing exploitation of CVE-2022-26923 and recent investigations involving Fighting Ursa and Fog ransomware.

Sources:

- [Palo Alto Networks Unit 42](#)

Policy & Legal

G7 Agencies Publish Minimum Elements for AI Software Bills of Materials

Cyber agencies from G7 nations and the European Commission published guidance defining minimum elements for Software Bills of Materials applied to AI systems, aiming to improve supply-chain transparency and cybersecurity across public and private sectors. The framework outlines seven clusters covering metadata, models, datasets, infrastructure, security properties and software dependencies, while noting that AI SBOMs alone are insufficient for supply-chain protection. The guidance states that AI SBOMs should integrate with vulnerability management tools, security advisories and broader cybersecurity monitoring mechanisms.

Sources:

- [Infosecurity Magazine](#)
- [Federal Office for Information Security](#)

German and Spanish Police Dismantle Relunched Crimenetwork Marketplace

German and Spanish authorities arrested a 35-year-old German national in Mallorca accused of rebuilding the Crimenetwork dark web marketplace days after its original administrator was arrested in December 2024. The relaunched platform accumulated more than 22,000 users, over 100 vendors and generated more than €3.6 million in revenue through commissions and seller licensing fees, trading stolen data, drugs and forged documents. Germany's BKA seized €194,000 in assets alongside user and transaction data, while the original Crimenetwork processed at least 1,000 BTC and 20,000 XMR between 2018 and 2024.

Sources:

- [Infosecurity Magazine](#)

Checkmarx Jenkins Plugin Compromised in Linked Supply Chain Attack

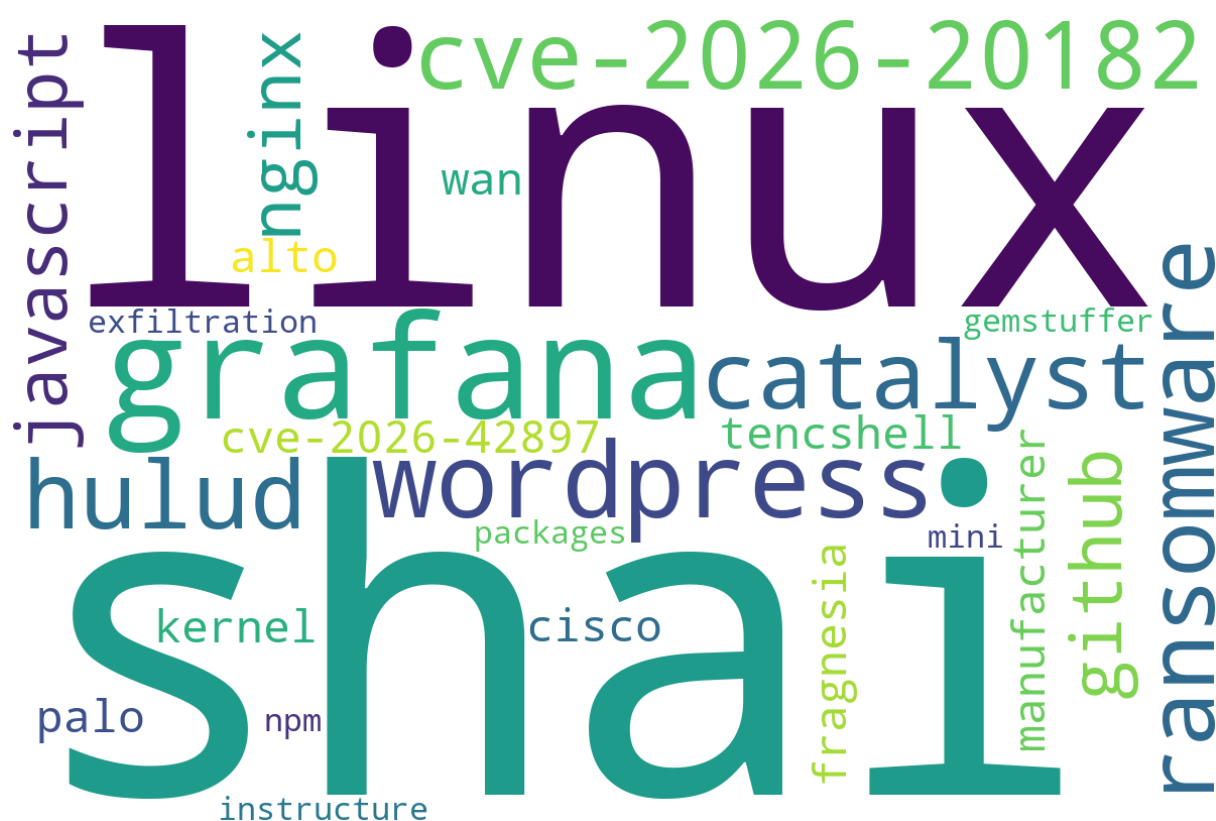
Checkmarx disclosed that a malicious version of its Jenkins AST Scanner plugin was published to the Jenkins Marketplace between 9 and 10 May 2026, affecting CI/CD pipelines us-

ing vulnerable plugin versions. The company released clean plugin versions including 2.0.13-848.v76e89de8a_053 and linked the compromise to the March 2026 TeamPCP attack on Trivy, which enabled unauthorised GitHub repository access and publication of malicious artefacts. Subsequent data leaks from the incident were attributed to the Lapsus\$ extortion group.

Sources:

- SecurityWeek
- Checkmarx

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/>