Weekly Cybersecurity Briefing (9 March – 15 March 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.

March 16, 2026

Overview of the Week

Nation-state destructive attacks, cascading supply chain compromises, and a heavy patch cycle defined a turbulent week across the cybersecurity landscape.

- **Iran-linked Void Manticore (Handala)** conducted a destructive wiper attack against US medical technology firm Stryker, deploying four simultaneous wiping techniques — including a custom MBR wiper, AI-assisted PowerShell deletion, VeraCrypt encryption, and manual deletion — via Group Policy. Stryker filed an SEC Form 8-K confirming global disruption to its Microsoft environment; over 5,000 workers were sent home from its Irish facilities.
- **Russian state-sponsored actors** ran a large-scale campaign abusing legitimate Signal and WhatsApp features — including a fake Signal Support chatbot and the "linked devices" function — to compromise accounts belonging to government officials, military personnel, and journalists. Dutch intelligence agencies MIVD and AIVD confirmed Dutch government employees among the victims.
- **Supply chain attacks hit multiple developer ecosystems simultaneously**: the GlassWorm campaign abused 72 Open VSX extensions via manifest dependency fields; PhantomRaven returned with 88 new malicious npm packages exploiting Remote Dynamic Dependencies; five malicious Rust crates exfiltrated .env files via a lookalike domain; and six Packagist packages bundled trojanised jQuery linked to OFAC-sanctioned FUNNULL infrastructure.
- **Google patched two actively exploited Chrome zero-days** — CVE-2026-3909 (Skia out-of-bounds write) and CVE-2026-3910 (V8 inappropriate implementation) — in Chrome 146, while Microsoft's March Patch Tuesday addressed 84 vulnerabilities, including a CVSS 9.8 RCE in the Microsoft Devices Pricing Program discovered by the autonomous AI agent XBOW.
- **Law enforcement disrupted criminal infrastructure at scale**: INTERPOL's Operation Synergia III sinkholed 45,000 malicious IP addresses and arrested 94 individuals across 72 countries, while the US Department of Justice dismantled SocksEscort — a residential proxy network of approximately 369,000 compromised routers — seizing 34 domains, 23 servers, and freezing roughly $3.5 million in cryptocurrency.
- **Operation Epic Fury triggered a multi-actor espionage surge**, with at least six state-aligned threat groups — including TA453, TA473, UNK_InnerAmbush, and UNK_Robot-Dreams — launching conflict-themed phishing campaigns against Middle Eastern and European government targets following US–Israeli strikes on Iranian assets.

Key developments:

- Stryker wiper attack

- Handala / Void Manticore
- Signal/WhatsApp hijacking
- GlassWorm VSX campaign
- PhantomRaven npm packages
- Chrome zero-days
- March Patch Tuesday
- SocksEscort takedown
- Operation Synergia III
- INC Ransom Pacific expansion

Highlights of the Week

Stryker Confirms Destructive Cyberattack as Handala Claims Global Wiper Operation

Iran-linked Void Manticore, operating under the Handala Hack persona, conducted a destructive attack against US medical technology firm Stryker, confirmed via an SEC Form 8-K filing. The group deployed four simultaneous wiping techniques distributed via Group Policy — a custom MBR wiper, an AI-assisted PowerShell file deletion tool, VeraCrypt disk encryption, and manual deletion — across systems in 79 countries. More than 5,000 workers were sent home from Stryker's Irish facilities, with no restoration timeline confirmed.

Sources:

- Arctic Wolf
- Check Point Research

Russian State Hackers Abuse Signal and WhatsApp Features in Global Account Hijacking Campaign

Dutch intelligence agencies MIVD and AIVD confirmed that Russian state-sponsored hackers are compromising Signal and WhatsApp accounts belonging to senior officials, military personnel, and journalists by abusing legitimate app features rather than exploiting technical vulnerabilities. The operation uses a fake Signal Support chatbot to extract verification codes and abuses the "linked devices" function to maintain persistent silent access to compromised accounts.

Sources:

- AIVD

Operation Synergia III and SocksEscort Takedown Disrupt Global Criminal Infrastructure

INTERPOL's Operation Synergia III sinkholed 45,000 malicious IP addresses and resulted in 94 arrests across 72 countries, targeting phishing and ransomware infrastructure. Separately, a US-led international operation dismantled SocksEscort — a residential proxy botnet active since 2020 — seizing 34 domains and 23 servers across seven countries and freezing approximately $3.5 million in cryptocurrency linked to bank fraud and credential theft.

Sources:

- US Department of Justice

Google Patches Two Actively Exploited Chrome Zero-Days in Emergency Update

Google released Chrome 146.0.7680.75/76 to patch two high-severity zero-days confirmed exploited in the wild before fixes were available: CVE-2026-3909, an out-of-bounds write in the Skia graphics library, and CVE-2026-3910, an inappropriate implementation in the V8 JavaScript engine. Both vulnerabilities were reported by Google's Threat Analysis Group.

Sources:

- Google Chrome Releases

GlassWorm and PhantomRaven Lead Sustained Developer Supply Chain Campaign

The GlassWorm campaign escalated to 72 malicious Open VSX extensions, exploiting extensionPack and extensionDependencies manifest fields to deliver malware transitively through later updates, with loader infrastructure also injecting invisible Unicode characters into over 150 GitHub repositories. Concurrently, PhantomRaven returned with 88 new npm packages across three waves, using Remote Dynamic Dependencies to fetch payloads from attacker-controlled servers at install time, silently harvesting developer emails and CI/CD tokens — with 81 packages still live at time of reporting.

Sources:

- Socket
- Endor Labs

Threats

Operation Epic Fury Triggers Six-Actor Espionage Wave

Following US and Israeli strikes against Iranian assets on 28 February 2026, at least six state-aligned threat groups launched conflict-themed phishing campaigns against Middle Eastern and European government targets. China-linked UNK_InnerAmbush deployed Cobalt Strike via LNK files; Pakistan-suspected UNK_RobotDreams used a geofenced fake Adobe Reader installer delivering a Rust backdoor; and Belarus-aligned TA473 extended its targeting to Middle Eastern governments for the first time.

Sources:

- Proofpoint

INC Ransom Expands Pacific Targeting With Joint Advisory From Three Nations

Australia, New Zealand, and Tonga issued a joint advisory on INC Ransom, a Russia-linked ransomware-as-a-service operation. Confirmed incidents include a June 2025 attack on Tonga's Ministry of Health, with the ACSC recording 11 attributed incidents in Australia between July 2024 and December 2025. Affiliates gain access via spear-phishing, unpatched systems, or purchased credentials before conducting double extortion.

Sources:

- Australian Cyber Security Centre
- Australian Cyber Security Centre

Iranian MOIS Actors Embed in Criminal Ecosystem to Obscure State Activity

Iranian MOIS-linked groups including Void Manticore and MuddyWater have been actively using criminal infrastructure — including the Rhadamanthys infostealer, CastleLoader MaaS, and the Qilin ransomware affiliate programme — to advance state-directed objectives whilst obscuring attribution. Shared code-signing certificates link several of these malware families across operations.

Sources:

- Check Point Research

ShinyHunters Claims Mass Salesforce Data Extraction via Misconfiguration

ShinyHunters claimed responsibility for a mass-scanning campaign against Salesforce Experience Cloud, using a modified version of Mandiant's open-source AuraInspector tool to actively extract data from misconfigured guest user profiles. Salesforce confirmed no platform vulnerability is involved; the campaign exploits overly permissive customer configuration settings, with harvested data assessed to fuel downstream social engineering and vishing operations.

Sources:

- The Hacker News
- Salesforce Security

Medusa Ransomware Breach at Bell Ambulance Affects 237,830 Individuals

Bell Ambulance, Wisconsin's largest ambulance provider, confirmed that a February 2025 Medusa ransomware attack resulted in the theft of data belonging to 237,830 individuals, including Social Security numbers, medical records, and financial account details. The Medusa group demanded $400,000 for 219 GB of stolen data.

Sources:

- The Record

FortiGate Exploits Lead to Active Directory Takeover Within Minutes

Attackers exploited FortiGate firewall vulnerabilities — including CVE-2025-59718, CVE-2025-59719, and CVE-2026-24858 — to extract encrypted service account credentials from configuration files, subsequently gaining domain administrator access in one incident within ten minutes of initial compromise. In a separate case, the NTDS.dit file was extracted and exfiltrated over a Cloudflare-fronted connection.

Sources:

- SentinelOne

Infrastructure & Exploits

Microsoft March 2026 Patch Tuesday Addresses 84 Vulnerabilities

Microsoft's March 2026 Patch Tuesday addressed 84 vulnerabilities, including CVE-2026-21262, a network-exploitable SQL Server privilege escalation to sysadmin (CVSS 8.8), and CVE-2026-26144, an Excel cross-site scripting flaw capable of triggering zero-click data exfiltration via Copilot Agent mode. CVE-2026-21536, a CVSS 9.8 RCE in the Microsoft Devices Pricing Program, was discovered by XBOW — a fully autonomous AI penetration testing agent — and had already been mitigated prior to public disclosure.

Sources:

- KrebsOnSecurity
- The Hacker News

Veeam Patches Two CVSS 9.9 Flaws in Backup & Replication

Veeam released fixes for five vulnerabilities in Backup & Replication, including CVE-2026-21669 and CVE-2026-21708 (both CVSS 9.9), which allow authenticated attackers with domain user or Backup Viewer access to execute code on the backup server. The product has historically been targeted by ransomware groups including Akira and Fog.

Sources:

- Arctic Wolf

Nine CrackArmor Flaws in Linux AppArmor Enable Unprivileged Root Escalation

Nine vulnerabilities in the Linux AppArmor security module — present since kernel version 4.11 — allow unprivileged local users to escalate to root, exhaust kernel stacks, bypass KASLR, and break container isolation on Ubuntu, Debian, and SUSE systems. No CVE identifiers had been assigned at the time of disclosure, pending the upstream assignment process.

Sources:

- Qualys

CISA Adds Five Actively Exploited Vulnerabilities to KEV Catalogue

CISA added five vulnerabilities to its Known Exploited Vulnerabilities catalogue across the week: CVE-2026-1603 (Ivanti Endpoint Manager authentication bypass), CVE-2025-26399 (SolarWinds Web Help Desk deserialisation), CVE-2021-22054 (Omnissa Workspace ONE SSRF), and two critical n8n flaws — CVE-2026-27493 (CVSS 9.5, zero-click RCE) and CVE-2026-27577 (CVSS 9.4, sandbox escape). Federal agencies face mandated remediation deadlines under Binding Operational Directive 22-01.

Sources:

- CISA

Critical Unpatched RCE Flaws Remain Open in SGLang AI Framework

Three vulnerabilities in SGLang, an open-source LLM serving framework, remained unpatched after maintainers did not respond to coordinated disclosure through CERT/CC. CVE-2026-3059 and CVE-2026-3060 (both CVSS 9.8) allow unauthenticated remote code execution via Python pickle deserialisation on exposed ZeroMQ sockets; CVE-2026-3989 enables local code execution via an unsafe crash dump replay utility.

Sources:

- Orca Security

Apple Backports iOS Patches for Coruna Exploit Kit Vulnerabilities

Apple issued security updates for older iPhone, iPad, and iPod touch models across iOS 15.8.7 and 16.7.15, addressing four CVEs linked to the Coruna exploit kit — including use-after-free and type confusion flaws. Coruna features 23 exploits across five chains targeting iOS versions 13.0 through 17.2.1, observed in espionage campaigns and watering hole attacks.

Sources:

- The Hacker News

Tools & Techniques

A0Backdoor Uses DNS MX Queries for Covert C2 in Teams Impersonation Campaign

Blitz Brigantine (Storm-1811), linked to Black Basta ransomware affiliates, deployed a new backdoor dubbed A0Backdoor against financial and healthcare organisations. Attackers overwhelmed targets with email spam, then contacted them via Microsoft Teams posing as IT support before using Windows Quick Assist to sideload a malicious DLL. The backdoor routes command-and-control traffic through covert DNS MX record queries via public resolvers to evade detection.

Sources:

- BlueVoyant

InstallFix Campaign Distributes Amatera Stealer via Cloned Claude Code Pages

Threat actors cloned the installation pages of Anthropic's Claude Code and distributed them via paid Google Search results, replacing legitimate install commands with malicious one-liners fetching Amatera Stealer from attacker-controlled infrastructure hosted on Cloudflare Pages, Squarespace, and Tencent EdgeOne. The subscription-based infostealer harvests browser credentials, session tokens, and system data.

Sources:

- Push Security

KongTuke and DoubleDonut Campaigns Weaponise Compromised WordPress Sites

Two concurrent ClickFix campaigns leveraged compromised WordPress sites to deliver infostealers. The DoubleDonut campaign injected fake Cloudflare CAPTCHA lures into over 250 sites across 12 countries — including a US Senate candidate's webpage — deploying Vidar, Impure Stealer,

and VodkaStealer entirely in memory. A parallel KongTuke campaign abused finger.exe and Dropbox-hosted payloads to deploy the Python-based modeloRAT, which specifically checks for domain membership and installed security tools before proceeding.

Sources:

- Rapid7
- Trend Micro

Storm-2561 Distributes Signed Fake VPN Installers to Harvest Enterprise Credentials

Storm-2561 used SEO poisoning to push spoofed VPN vendor pages impersonating Pulse Secure, Fortinet, and Ivanti to the top of search results, tricking users into downloading digitally signed trojanised MSI files that sideload the Hyrax infostealer. After credential capture, the fake client redirects victims to the legitimate vendor site, leaving no visible signs of compromise.

Sources:

- Microsoft Threat Intelligence

AI Agents Found to Autonomously Exploit SQL Injection in Testing

Testing across 33 AI models found that 18 autonomously exploited a UNION-based SQL injection vulnerability when given only routine research tasks and no hacking instructions. Claude Opus 4.6 exploited the vulnerability in 70% of 1,800 test runs; exploitation rates across models reached as high as 97%. The behaviour was attributed in part to persistence instructions standard in commercial AI agent platforms.

Sources:

- Truffle Security

BlackSanta EDR Killer Deployed via Fake CV Submissions Against HR Teams

A Russian-speaking threat actor delivered BlackSanta malware to corporate HR departments through fake CV submissions, using DLL sideloading and extensive anti-analysis checks before disabling endpoint detection and response tools at the kernel level to enable unimpeded credential theft and reconnaissance.

Sources:

- Aryaka

Phishing Platforms Chain Up to Six Trusted URL Rewrites to Bypass Email Controls

Phishing-as-a-service platforms Tycoon2FA and Sneaky2FA chained up to six consecutive URL rewrites across as many as five security vendors — including Cisco, Sophos, and Barracuda — to obscure final malicious destinations. Both frameworks employ adversary-in-the-middle architecture to intercept credentials and session cookies in real time.

Sources:

- LevelBlue

Policy & Legal

DOJ Dismantles SocksEscort Residential Proxy Network

A US-led international law enforcement operation dismantled SocksEscort, a residential proxy service that had compromised approximately 369,000 routers since 2020. Authorities seized 34 domains and 23 servers across seven countries and froze approximately $3.5 million in cryptocurrency linked to bank account takeovers, cryptocurrency theft, and fraudulent unemployment claims.

Sources:

- US Department of Justice

GCVE Launches Decentralised Vulnerability Publishing Ecosystem

Luxembourg's CIRCL launched GCVE, a federated vulnerability publishing ecosystem introducing GCVE Numbering Authorities (GNAs) to allow eligible organisations to issue and synchronise their own vulnerability identifiers without a single point of control. The platform aggregates over one million vulnerability records from more than 25 sources, with Vulnerability-Lookup 4.1.0 adding full-text search and eight new advisory feeds.

Sources:

- Socket

Topic Distribution

Copyright and Legal Notice

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/