View this email in your browser

AMERICAN
TECHNOLOGY
SERVICES

American Technology Services

Cybersecurity News Roundup

Weekly Insights and Updates

| February 7, 2025

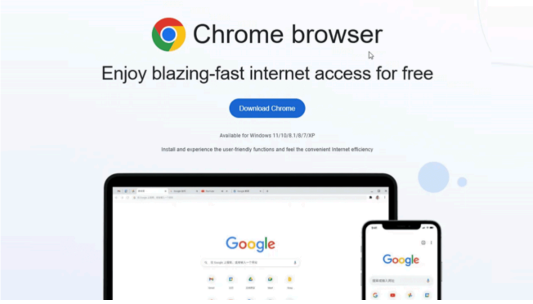
Cybercriminals are no longer lone hackers—they're operating with industrial efficiency, blending advanced phishing, supply chain exploits, and multi-stage malware to infiltrate even the most secure networks. This week, we spotlight three key trends shaping cybersecurity today: Phishing-as-a-Service (PhaaS), weaponized trust, and infrastructure exploits.

Additionally, we explore vulnerabilities affecting Veeam Backup software, man-in-the-middle exploits, and nation-state espionage campaigns leveraging PowerShell, Golang, and multi-layered payloads. With these threats evolving rapidly, organizations can no longer rely on outdated security models. Understanding how attackers operate is the first step to staying ahead.

Lazarus Group Uses LinkedIn Scams to Deliver Multi-Stage Malware

North Korea’s Lazarus Group is tricking professionals with fake LinkedIn job offers, deploying malware that steals credentials and crypto wallets across Windows, macOS, and Linux. This attack highlights the dangers of social engineering in professional networks.

Read More



Chrome browser

Enjoy blazing-fast internet access for free

Available for Windows 11/10/8.1/8/7/XP

Install and experience the user-friendly functions and feel the convenient internet efficiency

Fake Google Chrome Installers Spreading ValleyRAT Malware

Attackers are using bogus Chrome websites to distribute ValleyRAT, a trojan that logs keystrokes, monitors screens, and exfiltrates credentials. Employees should download software only from official sources to avoid falling victim to malware-laced installers.

Read More

Phishing-as-a-Service (PhaaS) Enables Scalable Cybercrime

Phishing kits like EvilProxy, ONNX, and W3LL offer subscription-based phishing services, allowing criminals to bypass MFA and hijack sessions. This industrialized approach to phishing means organizations must go beyond basic authentication protections.

Read More

Notorious Hacker Arrested After Breaching Government Agencies

A hacker responsible for over 40 cyberattacks against NATO, the U.S. Army, and Spanish government agencies has been arrested. The incident highlights how cybercriminals use stolen credentials for espionage and intelligence gathering.

Read More

British Engineering Firm IMI Discloses Cyber Breach

IMI, a global engineering company, suffered a security breach but has yet to disclose details on potential data theft. This follows a pattern of recent cyberattacks against industrial firms, emphasizing the need for stronger cybersecurity in critical sectors.

Read More

Attackers Exploit HTTP Client Tools to Hijack Microsoft 365 Accounts

Threat actors are leveraging HTTP clients like Axios and Node Fetch to conduct brute-force and Adversary-in-the-Middle (AiTM) attacks. With a 43% success rate, these tactics highlight why MFA alone is no longer enough to protect cloud accounts.

Read More

Kimsuky APT Deploys forceCopy Malware to Steal Browser Credentials

The North Korean hacking group Kimsuky is using spear-phishing emails and PowerShell-based keyloggers to extract credentials stored in web browsers. This attack demonstrates the importance of endpoint protection and credential security.

Read More

Lazarus Group’s Cross-Platform JavaScript Stealer Targets Crypto Wallets

Lazarus Group continues targeting the crypto sector, deploying a JavaScript-based stealer designed to exfiltrate cryptocurrency wallet data from browser extensions. Crypto firms and investors should secure assets using hardware wallets and offline storage.

Read More

Silent Lynx APT Uses PowerShell, Golang, and C++ in Multi-Stage Attacks

A newly discovered hacking group, Silent Lynx, is targeting government banks, embassies, and think tanks in Central Asia. Their multi-layered malware and use of Telegram bots for command-and-control suggest a highly sophisticated espionage campaign.

Read More

Veeam Backup Flaw Exposes Systems to Remote Code Execution via MitM Attacks

A critical vulnerability (CVE-2025-23114) in Veeam Backup software allows attackers to execute arbitrary code using a Man-in-the-Middle attack. Patches have been released, and affected organizations must update immediately to prevent exploitation.

Read More

Cybersecurity is no longer a game of defense—it's a race to outmaneuver an enemy that never sleeps. Attackers aren't just innovating; they're industrializing. Phishing-as-a-service operations churn out stolen credentials at scale, while malware campaigns hijack the very trust that businesses and professionals depend on. State-sponsored groups operate with military precision, embedding multi-stage payloads deep into cloud infrastructure, lurking within critical networks, and proving that cybercrime is a long game of strategy, patience, and infiltration.

Traditional defenses are obsolete in this new reality. When adversaries use automation, deception, and supply chain corruption to slip past detection, static security tools fail. Organizations must shift from reactive to preemptive—adopting zero-trust architectures, enforcing phishing-resistant authentication, and weaponizing threat intelligence to disrupt attacks before they detonate. The future of cybersecurity belongs to those who think like attackers, act before the breach, and refuse to be outplayed.

Criminals don't need malware if they can manipulate people into running their code.

Contact Us

INT.	+1 888 876 0302
USA	+1 703 876 0300

Our Offices

New York | Virginia | Atlanta

info@networkats.com
networkats.com

Share the insights!
Forward this email to a friend.

Our mailing address is:
250 Broadway, Suite 610
New York, NY 10007