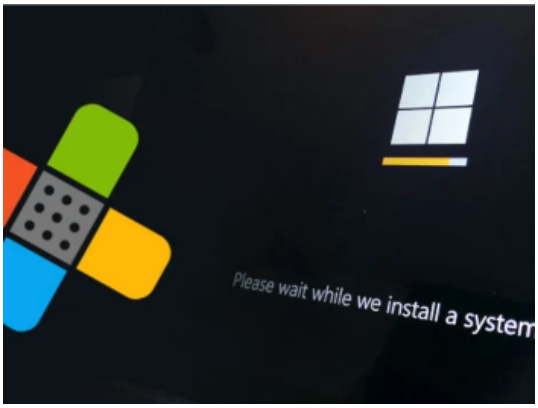
View this email in your browser

Weekly Insights and Updates

| February 14, 2025

Imagine a hacker sitting in a dimly lit room—except they're not typing furiously on a keyboard. Instead, they're asking an AI to write the perfect phishing email, generate undetectable malware, or map out an entire cyberattack strategy in seconds. The old image of cybercrime is gone. Today, attackers aren't just getting in through firewalls—they're manipulating the very tools businesses rely on.

Ransomware gangs crumble under government takedowns, but their replacements are leaner, faster, and more ruthless. AI models meant for productivity are being hijacked for phishing, fraud, and digital extortion. Nation-state hackers aren't just after intelligence; they're embedding themselves inside global supply chains and corporate networks. When cybercriminals stop breaking in and start blending in, visibility is everything.



Microsoft Fixes 63 Security Flaws, Two Exploited

Microsoft fixed 63 vulnerabilities, including two under active exploitation. A remote code execution flaw (CVE-2025-21198, CVSS 9.0) in HPC Pack is the most severe, and agencies must patch by March 4, 2025.

Read More

Ivanti Patches Severe Vulnerabilities in VPN Services

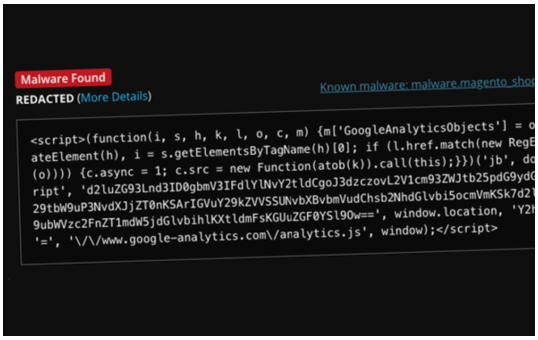
Ivanti fixed four critical flaws, including a buffer overflow (CVE-2025-22467, CVSS 9.9) that enables remote code execution. Ivanti products remain a prime nation-state target, making patching a priority.

Read More

FBI, Europol Shut Down 8Base Ransomware Group

The FBI, Europol, and NCA seized 8Base ransomware's leak sites, arresting four members. The operation disrupted over 100 cybercrime servers, significantly weakening Ransomware-as-a-Service operations.

Read More



Credit Card Skimmers Found in Google Tag Manager

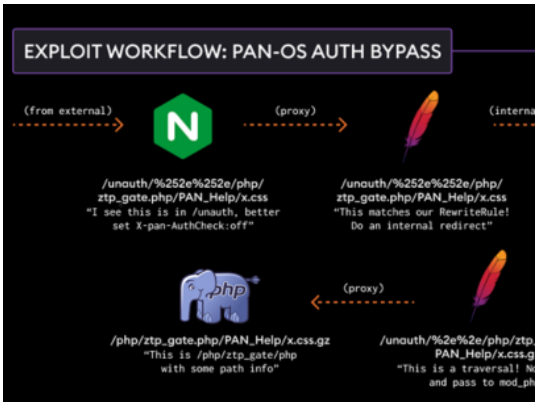
Hackers are injecting skimmers into Magento checkout pages via Google Tag Manager. Stolen payment data is sent to attacker-controlled servers, making immediate GTM security audits essential.

Read More

Palo Alto Fixes PAN-OS Authentication Bypass

A high-severity authentication bypass (CVE-2025-0108, CVSS 7.8) in PAN-OS allowed unauthorized PHP script execution. Organizations should restrict internet access to the management interface immediately.

Read More



AI Chatbots Used by State-Backed Hackers

Hackers linked to China, Iran, Russia, and North Korea are using Google Gemini AI for phishing, reconnaissance, and malware research. AI is reshaping cybercrime, making AI security governance essential.

Read More

Ransomware Payments Drop 35% Despite Attacks

Despite record-setting attacks, total ransom payments fell from $1.25 billion to $814 million in 2024. Crackdowns and stronger enterprise defenses are making ransomware less profitable—but not disappearing.

Read More

Russian Hosting Provider Sanctioned for LockBit Support

The U.S., U.K., and Australia sanctioned Zservers, a Russian bulletproof hosting provider that facilitated LockBit ransomware. This blocks transactions and increases pressure on cybercriminal infrastructure.

Read More

Microsoft Exposes Russia's Sandworm Cyber Operations

DeepSeek AI Poses High Security Risks

Microsoft identified BadPilot, a Sandworm subgroup targeting critical industries. The group exploits unpatched Microsoft Exchange, Zimbra, and RMM software to infiltrate high-value networks worldwide.

Read More

Chinese AI model DeepSeek failed 98.8% of malware creation tests, exposing severe security gaps. Researchers warn businesses should block DeepSeek to prevent data leaks and supply chain attacks.

Read More

Cybercrime isn't just a hacker in a hoodie—it's nation-states, AI tools, and entire underground economies. Attackers don't need to break down your firewall if they can just convince your AI to let them in. They don't need zero-days when your VPN is still unpatched.

This week proves one thing: cybersecurity is a moving target. The wins matter—ransomware groups are collapsing, threat actors are being sanctioned—but the threats keep evolving. Staying ahead isn't about reacting. It's about knowing where the next attack is coming from. ATS is here to help. Let's secure what's next. See you next week.

AI doesn't need to be sentient to be dangerous in the wrong hands.

Contact Us

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

info@networkats.com
networkats.com

Our Offices

New York | Virginia | Atlanta

Share the insights!
Forward this email to a friend.

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