View this email in your browser

AMERICAN
TECHNOLOGY
SERVICES

American Technology Services

Cybersecurity News Roundup

Weekly Insights and Updates

| March 7, 2025

Cybersecurity doesn't pause, doesn't breathe — and neither do the adversaries hunting for cracks in the skin of global systems. Every shift in tech, every pivot in how we work, every tremor in geopolitics, they ride it like a wave, carving fresh tunnels into networks, slipping into the bloodstream of digital infrastructure before anyone feels the cold.

This week's stories sketch out a stark evolution: these aren't hit-and-run attacks or isolated breaches anymore. The line between trusted and compromised is dissolving. Attackers aren't just circling the walls — they're nesting inside the machinery itself. IT service providers, software supply chains, and the cloud platforms businesses treat like oxygen — they've become vectors, weapons, footholds. The systems we build our futures on are being rewired into silent entry points for anyone bold enough to exploit them.

Chinese state-backed hackers are burrowing deep into IT ecosystems, siphoning credentials like lifeblood, while North Korean operatives slip into developer roles, laundering stolen access into missile fuel and regime survival. The motives twist from espionage to cold profit to global leverage — a dance of theft and strategy, all feeding the same storm.

Add to that the ongoing churn of ransomware groups vying for dominance in the wake of LockBit's disruption, and it's clear that the stakes are only getting higher for security teams. Defending a single perimeter is no longer enough. Today's reality demands a clear understanding of how these overlapping threats converge — and how to defend against the ripple effects they create.

Phishers Use SharePoint to Deploy Havoc Malware

A new phishing campaign hides malware delivery inside trusted Microsoft services, using SharePoint and Graph API to mask malicious traffic. This approach highlights how attackers are blending social engineering with sophisticated obfuscation to bypass traditional defenses.

Read More

North Korean IT Worker Scheme Funds Weapons Programs

North Korean hackers are posing as developers and engineers to secure remote jobs at US and Japanese companies — not for espionage, but to fund nuclear weapons programs. This campaign emphasizes the need for thorough background checks and identity verification during hiring.

Read More

Silk Typhoon Targets IT Supply Chains for Initial Access

China-linked Silk Typhoon has shifted focus to IT service providers, compromising remote management and identity platforms to gain access to downstream customers. By exploiting trusted relationships, this tactic helps attackers bypass traditional defenses and gather intelligence.

Read More

Lotus Blossom Targets Critical Infrastructure in Southeast Asia

The long-active espionage group Lotus Blossom is deploying custom malware to maintain persistent access across government, telecom, and manufacturing sectors in Southeast Asia. Their use of cloud services like Dropbox and Zimbra for command-and-control illustrates how attackers are adapting to modern infrastructure.

Read More

VMware Vulnerabilities Actively Exploited in the Wild

Three newly discovered VMware vulnerabilities — including a critical flaw allowing code execution on the host hypervisor — are being exploited in active attacks. Organizations using ESXi, Workstation, and Fusion should apply Broadcom’s emergency patches immediately.

Read More

Silk Typhoon Expands Supply Chain Campaigns Using Stolen API Keys

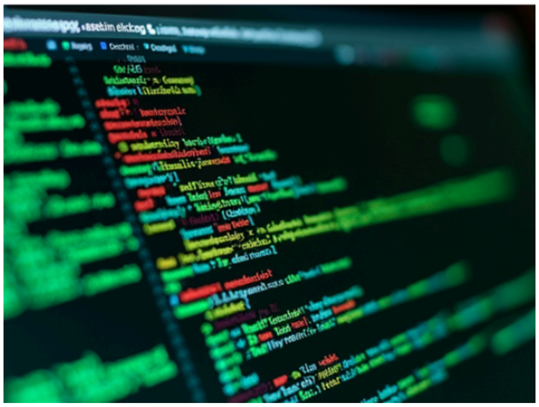
New reporting confirms Silk Typhoon’s use of stolen API keys and privileged credentials to infiltrate downstream customer environments. Combined with zero-day exploitation, this approach highlights the need for stronger identity governance and continuous API monitoring.

RDP Risks Surge as Hackers Target New Ports

While RDP remains essential for IT teams, attackers are ramping up scanning and exploitation attempts, including shifting focus to lesser-known ports like 1098. With Microsoft regularly patching critical RDP flaws, organizations must pair timely updates with stronger access controls and monitoring.

Read More

Read More



Over 1,000 WordPress Sites Compromised with Persistent Backdoors

Attackers have injected malicious JavaScript into over 1,000 WordPress sites, planting multiple backdoors to maintain access even if some are removed. This wave of infections highlights the need for continuous website monitoring and proactive security reviews of plugins and third-party code.

Read More

Medusa Ransomware Expands with Double Extortion Attacks

Medusa ransomware operators have hit over 40 organizations in 2025 alone, demanding ransoms as high as $15 million. Leveraging known vulnerabilities and remote management tools, they continue to refine their methods for both encryption and data theft.

Read More

EncryptHub Deploys Ransomware and Stealers via Trojanized Apps

The threat actor EncryptHub is delivering ransomware and stealers through phishing, fake software downloads, and even paid malware distribution services. Their development of a custom remote access platform signals ongoing evolution and potential commercialization of their toolset.

Read More

This week’s stories leave no room for doubt: the modern breach doesn’t kick down the front door. It slides in quietly, through the side entrances we built ourselves — the vendors we trust, the platforms we depend on, the apps that blend into the background of daily operations. What looks like business as usual is often the first step of compromise.

Security teams aren’t just fighting isolated flare-ups anymore. They’re up against whole ecosystems — sprawling, coordinated networks of state-backed operators, ransomware syndicates, and cybercriminal supply chains, each feeding off the other’s work. Espionage, extortion, disruption — all braided together, all targeting not just systems, but the connective tissue that holds businesses together.

For security and IT leaders, survival means pulling back the lens. It’s no longer just about patching the cracks in your own walls — it’s about knowing every fracture point across your supply chain, your platforms, your partners. It’s understanding that your risk doesn’t stop at your doorstep — it runs through every tool you rely on, every vendor you trust, every piece of code your business touches.

Supply chain security, third-party monitoring, and unflinching visibility across both cloud and on-prem environments aren’t checkboxes anymore — they’re the bedrock of resilience. Without them, you’re blind to the breaches already in motion.

That’s where ATS steps in. Our cybersecurity specialists don’t just help organizations react — we help them evolve. Advanced threat monitoring, incident response, advisory services, and proactive programs are built to adapt as fast as the threat landscape twists and fractures. In a world this interconnected, resilience isn’t about walls — it’s about awareness, agility, and the right partners in your corner, anticipating the next move before it lands.

Because in this environment, falling behind isn’t an option — and staying still is the first step to falling.

The riskiest threat is the one disguised as business as usual.

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