View this email in your browser

AMERICAN
TECHNOLOGY
SERVICES

American Technology Services

# Cybersecurity News Roundup

## Weekly Insights and Updates

| March 14, 2025

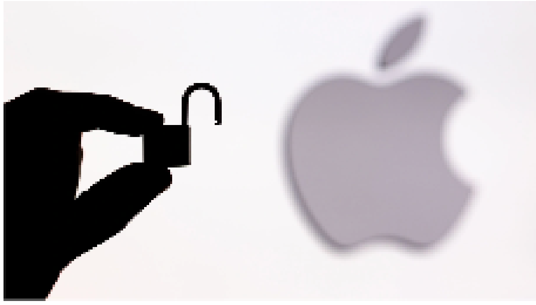
The biggest threats in cybersecurity aren't always the ones making headlines. A zero-day with a flashy exploit might grab attention. Still, the real danger often lies in the silent, long-term compromises—the ones lurking inside networks for months, quietly gathering intelligence before striking. This week's news highlights how deep attackers are embedding themselves into infrastructure, from China-backed hackers backdooring carrier-grade routers to ransomware groups scaling their operations with industrial efficiency.

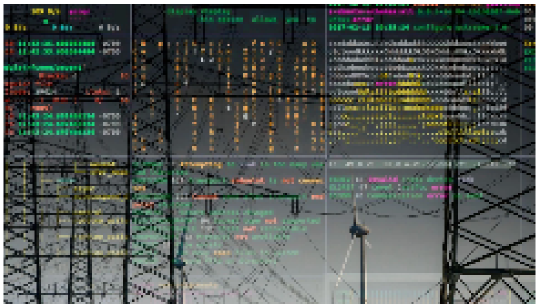
Security isn't just about reacting to breaches—it's about realizing when you've already been breached. Are your defenses built for the threats you can see or the ones already inside?

### China-Backed Hackers Embed in Juniper Routers

Mandiant uncovered a Chinese cyber-espionage campaign that compromised Juniper MX routers using the TinyShell backdoor. Organizations relying on Juniper devices should upgrade immediately and scan for hidden compromises.

Read More





### Apple Rushes Emergency Fix for WebKit Zero-Day

Apple patched a WebKit vulnerability (CVE-2025-24201) that allowed attackers to bypass security controls and execute malicious code. Users should update all Apple devices immediately to prevent further exploitation.

Read More

### Volt Typhoon Maintained 300-Day Access to Power Grid

A Chinese APT group infiltrated a Massachusetts power utility for nearly a year, gathering intelligence on critical infrastructure. Investigators warn this could be reconnaissance for future cyber sabotage.

Read More

### Microsoft's March Update Fixes Six Zero-Days

Microsoft released patches for six zero-day vulnerabilities, including a critical NTFS flaw enabling remote code execution. Security teams should patch immediately and strengthen defenses against phishing-based exploits.

Read More

### Facebook Warns of FreeType Exploit in the Wild

A newly disclosed FreeType 2 vulnerability (CVE-2025-27363) is actively exploited, allowing attackers to execute code on Linux, Android, and other systems. Organizations should update to FreeType 2.13.3 to prevent potential breaches.

Read More

### Medusa Ransomware Expands to 300+ Critical Targets

Medusa ransomware has escalated attacks on healthcare, education, and manufacturing using stolen credentials. Organizations must tighten access controls and limit lateral movement to reduce exposure.

Read More

### Firefox Users Must Update Before Certificate Expiry

Mozilla is warning users to update Firefox to version 128 or later before a root certificate expires on March 14. Outdated browsers will lose add-on functionality and face security risks.

Read More

### CISA Issues Urgent Warning on Ivanti EPM Attacks

CISA flagged three Ivanti Endpoint Manager (EPM) vulnerabilities as actively exploited, mandating immediate patching. Attackers are using these flaws to gain full system control.

Read More

### VMware Zero-Days Expose Thousands to VM Escapes

More than 41,000 VMware ESXi instances remain vulnerable to exploits that allow attackers to escape virtual machines. Cloud and enterprise environments should be patched immediately to prevent full system takeovers.

Read More

### GitHub-Hosted Malware Infects 1 Million Windows Users

A widespread malvertising campaign used GitHub to spread data-stealing malware to nearly 1 million PCs. Organizations should block risky sites and deploy endpoint protections to prevent similar attacks.

Read More

Cybersecurity often feels like a race to patch, a cycle of reacting to each newly discovered breach or vulnerability. But this week's stories hint at a more profound, unsettling truth—some of the most dangerous threats aren't coming; they're already here. Attackers aren't just breaching networks; they're embedding themselves in the very infrastructure organizations depend on, sometimes for months before anyone notices. The Volt Typhoon breach lasted 300 days. Chinese hackers planted backdoors in carrier-grade routers. Ransomware groups are no longer just hitting random targets—they're refining their methods and scaling operations like full-fledged businesses.

So what happens when the threats you're watching aren't the ones that get you? What if the malware that makes headlines distracts from the silent compromises already lurking in your systems? Patching zero days is necessary, but it's not a strategy—it's a reaction. True cybersecurity means assuming the breach, operating as if attackers have already slipped past your perimeter, and hunting them where they hide.

The hardest part of security isn't blocking an attack—it's questioning assumptions. Are your defenses built to protect against what's coming, or are they designed for threats that arrived long before you noticed? It's time to shift from reaction to resilience, from chasing alerts to anticipating where the real threats lie.

**Paying ransom isn't just a financial decision—it's a gamble on whether you're still compromised.**