View this email in your browser

AMERICAN TECHNOLOGY SERVICES

American Technology Services

Cybersecurity News Roundup

Weekly Insights and Updates

| March 21, 2025

Security is supposed to be the last line of defense—but what happens when it becomes the entry point? This week, attackers didn’t just exploit vulnerabilities in unpatched software; they went after security tools themselves. A widely used WordPress security plugin contained a flaw that allowed full server takeovers. A backup and disaster recovery solution had a critical vulnerability that opened entire IT environments to attackers. Even AI-driven cloud security—marketed as the future of cyber defense—is being deployed with dangerous misconfigurations, handing bad actors unrestricted access.

Meanwhile, cybercriminals are refining their methods. Ransomware gangs are creating custom-built backdoors to make detection harder. Nation-state actors are outsourcing attacks to organized crime groups to muddy attribution. AI is being used to scale phishing, deepfake fraud, and large-scale deception. The threats are evolving, and organizations that rely on the assumption that security tools alone will protect them are making a dangerous bet. This week’s headlines are a reminder that true security requires constant scrutiny—not just of attackers, but of the very tools meant to keep them out.

Jaguar Land Rover's Data Exposed in Alleged Breach

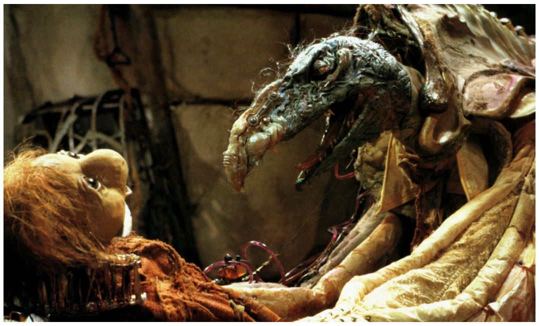
Hackers claim to have leaked JLR's tracking data, source code, and employee information. This raises concerns about intellectual property theft and targeted attacks on high-value individuals.

Read More

VenomRAT Delivered via Fake Purchase Orders

Attackers are hiding VenomRAT inside virtual hard disk files attached to phishing emails. The malware enables data theft, keylogging, and hidden remote access.

Read More



Ukraine's Defense Sector Targeted by Dark Crystal RAT

Cyber-espionage campaigns are using Signal messages to infect Ukrainian defense organizations with a powerful RAT. This underscores the dangers of secure messaging apps being weaponized.

Read More

RansomHub's Betruger Backdoor Streamlines Ransomware Attacks

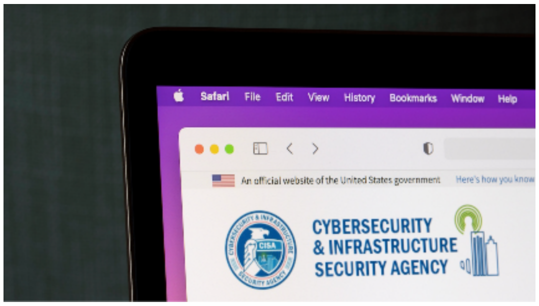
A new custom backdoor is minimizing the need for additional hacking tools before ransomware deployment. The shift toward bespoke malware makes detection more challenging.

Read More

Nation-States and Organized Crime Form Cyber Alliances

Europol warns that geopolitical actors are outsourcing cyberattacks to criminal groups. AI-driven threats and deepfakes are further complicating attribution.

Read More


Safari File Edit View History Bookmarks Window Help
An official website of the United States government
Here's how you know
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA

CISA Sounds Alarm on Nakivo Exploit

A critical Nakivo Backup vulnerability is being actively exploited, allowing unauthorized file access. Organizations must patch immediately to prevent data breaches.

Read More

WP Ghost Plugin Flaw Enables Server Takeover

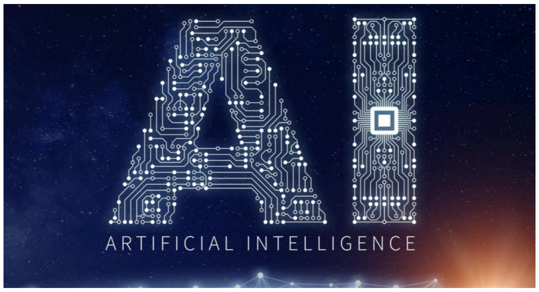
A critical remote code execution vulnerability in a popular WordPress security plugin puts over 200,000 websites at risk. Site owners should update immediately.

Read More

Google Acquires Wiz in $32B Security Deal

Google’s record-breaking acquisition of Wiz aims to strengthen multi-cloud security with AI-driven threat detection. This underscores the growing demand for automated cloud defense.

Read More



AI Cloud Deployments Riddled with Security Mistakes

A Tenable report reveals that organizations are granting excessive permissions by default, increasing the attack surface for AI-powered cloud services.

Read More

Microsoft Warns of Multifunctional StilachiRAT

A newly discovered remote access Trojan combines credential theft, reconnaissance, and cryptocurrency targeting. Its stealth tactics make detection and mitigation particularly difficult.

Read More

This week's news illustrates that cybersecurity isn't just about having the right tools—it's about knowing where they can fail. A strong security posture isn't built on a checklist of software solutions; it requires continuous validation, risk assessments, and expert oversight. The biggest threats aren't always external—sometimes, they come from the very systems organizations trust to protect them.

That's where ATS comes in. We help organizations deploy security solutions with the right configurations, active monitoring, and ongoing testing to keep up with new vulnerabilities and emerging attack methods. Whether it's closing gaps in cloud security, strengthening defenses against ransomware, or evaluating the security of your existing infrastructure or vendors, we provide expertise that goes beyond technology. Because in cybersecurity, what you *think* is protecting you could be the biggest risk of all. Let's make sure it isn't.

Your security stack is only as good as the strategy behind it.

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