View this email in your browser

AMERICAN
TECHNOLOGY
SERVICES

American Technology Services

Cybersecurity News Roundup

Weekly Insights and Updates

| September 6, 2024

Imagine waking up to find that your organization's most trusted tools have been turned against you, or that your airport's operations have been crippled by a single malicious actor. This isn't a plot from the latest cyber-thriller—it's the reality businesses face. We dive into the most unsettling and sophisticated cyber threats that have emerged recently, revealing how close they are to our everyday operations and what they mean for you.

This edition doesn't just report the latest cyber news—it features the threats that are redefining the rules of engagement. From ransomware that mimics old internet mysteries to state-sponsored espionage using everyday tools, these stories reveal a new era of cybersecurity challenges you can't afford to ignore.

Zero-Click Exploit Now Public

A proof-of-concept exploit for a severe Windows TCP/IP vulnerability (CVE-2024-38063) is now accessible, making it easier for cybercriminals to launch attacks. Microsoft urges immediate patching to mitigate this risk.

Read More

Citrine Sleet Targets Cryptocurrency

North Korean group Citrine Sleet exploits a Chromium zero-day, primarily targeting the cryptocurrency sector. The group's sophisticated tactics highlight the need for continuous vigilance and security updates.

Read More

Fake GlobalProtect Delivers Malware

A new malware campaign spoofs GlobalProtect VPN software to distribute WikiLoader malware. This shift from phishing to SEO poisoning marks an alarming trend in cyberattack strategies.

Read More

Google Sheets Used for Malware Control

A novel malware campaign utilizes Google Sheets as a command-and-control mechanism, part of a broader espionage effort targeting multiple sectors globally. The innovative use of everyday tools in cyberattacks is a wake-up call for all organizations.

Read More

Seattle Airport Hacked

A cyberattack on Seattle-Tacoma Airport's systems has caused widespread disruptions, exposing vulnerabilities in critical infrastructure. This incident serves as a stark reminder of the need for robust cybersecurity defenses.

Read More

Flight Information Display
Monitors are currently down.
Check with air carriers or
download airline app for
updated flight information.

Halliburton Hit by Cyberattack

Halliburton's recent cyberattack led to significant disruptions and data exfiltration, raising concerns about the adequacy of cybersecurity measures in the oil services sector.

Read More

Iranian Hackers Ramp Up Ransomware

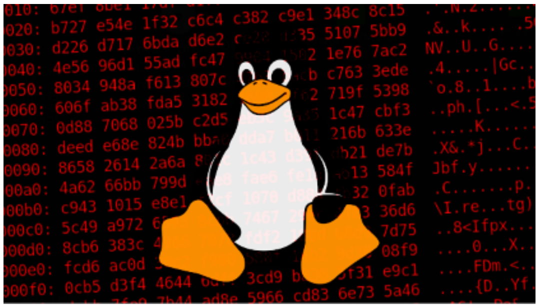
U.S. agencies warn of increased ransomware activity by Iranian group Pioneer Kitten, targeting critical sectors. The group's collaboration with other ransomware actors highlights the growing complexity of cyber threats.

Read More

RansomHub's Expanding Threat

The RansomHub ransomware group has attacked 210 victims across critical sectors since February 2024. Their rapid growth underscores the rising threat of ransomware-as-a-service (RaaS) models.

Read More



Rust-based Ransomware Emerges

Cicada3301's Shadowy Origins

A new Rust-based ransomware, Cicada3301, targets both Windows and Linux systems, sharing many similarities with the infamous BlackCat variant. This cross-platform threat represents the next evolution in ransomware attacks.

Read More

Despite its name, the new Cicada3301 ransomware has no ties to the original internet mystery group. This misattribution highlights the challenges in tracking and identifying the true origins of cyber threats.

Read More

Featured Articles by ATS

FTC and the Safeguards Rule

Are you meeting the FTC's stringent data protection requirements? ATS offers expert services to help businesses close security gaps and fully comply with these critical regulations.

Read More

Is Social Engineering Targeting You?

Social engineering leverages human psychology to bypass technical defenses, making it one of the most dangerous cybersecurity threats. Penetration testing can expose these vulnerabilities, enabling organizations to fortify their defenses against manipulative tactics like phishing and pretexting.

Read More

Malware vs. Ransomware: Different Tactics, Big Danger

While both malware and ransomware are malicious, they have distinct objectives and methods of attack. Protect your business by understanding these differences and ensuring your cybersecurity measures are up to the task.

Read More

In a world where yesterday’s defenses are no match for today’s attacks, complacency isn’t an option. The threats we’ve covered in this edition aren’t just news—they’re a glimpse into the future of cyber warfare, where the stakes are higher and the tactics are more insidious than ever. At ATS, we’re not just observers; we are your first line of defense.

Prepare for the unexpected, because the hackers already have.

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

Unsubscribe <<Email Address>> from this list.