View this email in your browser

AMERICAN
TECHNOLOGY
SERVICES

American Technology Services

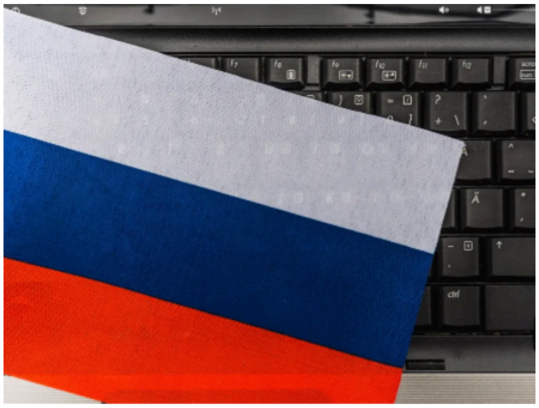
Cybersecurity News Roundup

Weekly Insights and Updates

| November 29, 2024

Ransomware gangs, state-sponsored hackers, and creative phishers are leveraging every possible angle to compromise systems and extract data. This week’s roundup dives into new and persistent tactics being deployed across industries, from healthcare to government operations. Attackers are exploiting zero-day vulnerabilities, misusing trusted platforms, and targeting organizations during high-stakes periods like holidays.

Critical incidents include ransomware attacks disrupting major healthcare providers, phishing campaigns that trick users with sophisticated lures, and malware campaigns using legitimate services like Google Drive and Bitbucket for command-and-control. Some attackers have disguised their malware as job application files or trusted software, blending seamlessly into expected workflows to evade detection. These incidents illustrate how adversaries are not only exploiting technical vulnerabilities but also weaponizing human trust.



Firefox and Windows Zero-Day Vulnerabilities Exploited

Russian hackers used zero-day flaws in Firefox and Windows to deploy backdoors via zero-click attacks. Timely updates remain vital to countering such sophisticated exploits.

Read More

Geico and Travelers Fined Over Data Breaches

Two major insurers face $11.3 million in fines after cyberattacks exposed sensitive customer data. See how penetration testing and multi-factor authentication (MFA) could have mitigated these breaches.

Read More

Hackers Exploit Holiday Downtime

Cybercriminals are exploiting holidays to target organizations, taking advantage of reduced IT staff availability. These attacks often involve ransomware or DDoS campaigns, disrupting operations during critical moments.

Read More

Espionage Linked to China Hits Paraguay

The "Flax Typhoon" hacking group infiltrated Paraguayan government systems, signaling the growing need for international collaboration to counter state-sponsored threats.

Read More

Hospital Cyberattack Halts Operations

A UK hospital resorted to manual processes after a cyberattack disrupted operations. This highlights the critical importance of continuity planning in healthcare.

Read More

APT36's ElizaRAT Leverages Trusted Platforms

APT36 exploits cloud services like Slack and Google Drive to control its ElizaRAT malware. Discover why trusted platforms are becoming vectors for cyber threats.

Read More

Legislators Push Healthcare Cybersecurity Act

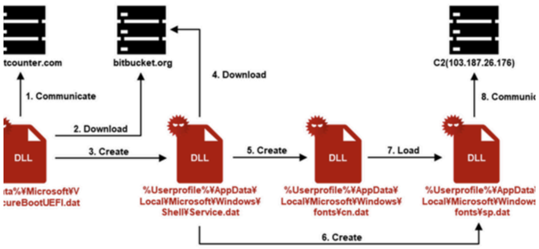
The bipartisan Health Care Cybersecurity and Resiliency Act seeks to bolster healthcare defenses, including mandated MFA to safeguard sensitive health data.

Read More

SharePoint Exploited in Phishing Campaigns

Attackers host malicious PDFs on SharePoint and distribute them via compromised emails. Learn strategies to secure collaboration platforms and prevent phishing.

Read More



APT28 Targets U.S. Organizations with Phishing

APT28 employs WiFi exploits and phishing schemes to compromise victims. Comprehensive endpoint protection can mitigate these innovative tactics.

Read More

SpyGlace Malware Exploits Job Application Themes

APT-C-60, a group aligned with South Korea, deploys SpyGlace malware through phishing emails that mimic job applications. By using legitimate platforms like Google Drive and Bitbucket, the group bypasses conventional security measures to deliver sophisticated backdoors.

Read More

Featured Articles by ATS

The Role of Security Patching

Security patches are an important defense against cyber threats, addressing vulnerabilities before they can be exploited. Timely updates protect systems and support secure, uninterrupted operations.

Read More

Managed Servers Keep You Operational

Managed servers provide business continuity and disaster recovery capabilities to maintain business operations during disruptions. Expert management reduces downtime and improves system reliability.

Read More

IT + Cloud: A Winning Combo

Combining managed IT services with cloud solutions offers adaptability, security, and streamlined workflows. This integration supports resource growth and keeps your business agile.

Read More

This week’s updates expose an unsettling truth: cyber attackers aren’t merely advancing—they’re outpacing those who aren’t ready. With precision tactics and psychological manipulation, these campaigns exploit any gap in preparedness. Organizations failing to train staff on phishing schemes or staying ahead of malware trends are effectively leaving their doors wide open to attack.

However, awareness alone won't secure your defenses. The accelerating pace of cyber threats calls for proactive, adaptive strategies. Dark web threat intelligence, consistent updates, and 24/7 monitoring can mean the difference between resilience and catastrophe. The message is clear: the best defenses don't wait to react—they move to anticipate. The time for action isn't tomorrow; it's today—because the attackers already have the advantage.

Sophisticated malware hides in plain sight by mimicking the tools we trust.

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