View this email in your browser

AMERICAN TECHNOLOGY SERVICES

American Technology Services

Cybersecurity News Roundup

Weekly Insights and Updates

| October 25, 2024

Cybersecurity remains one of the defining challenges of our time, as recent events show that the threat environment is evolving and escalating at an alarming pace. Attackers are becoming more sophisticated, finding creative ways to exploit vulnerabilities and bypass advanced defenses.

This week's cybersecurity news brings urgent updates on new regulations aimed at strengthening protections, emerging attack tactics that target trusted services, and the latest strategies for safeguarding sensitive information across industries From state-sponsored campaigns leveraging geopolitical tensions to the use of artificial intelligence in phishing schemes, the digital battlefield is constantly shifting. As industries and governments grapple with this complex and unpredictable environment, the stakes have never been higher for ensuring strong defenses in the face of persistent cyber threats that know no borders or boundaries.

Service for America: Building a Cyber Talent Pipeline

The Service for America campaign is bridging the gap in cybersecurity talent by prioritizing skills-based hiring and expanding career pathways. Discover how this initiative creates opportunities for diverse talent to enter the cyber workforce and addresses the nearly half a million job openings in the field.

Read More

CMMC 2.0: The Final Rule is Here

With the final rule for CMMC 2.0 now published, defense contractors must prepare for mandatory compliance by mid-2025. Learn what this means for businesses in the Defense Industrial Base and the penalties for non-compliance as the DoD aims to improve cybersecurity across its supply chain.

Read More

AI in Influence Operations: New Insights and Disruptions

OpenAI's latest threat report details how malicious actors are using AI to influence operations, albeit with limited success. Get the latest insights on AI's role in covert campaigns and how it challenges and strengthens global cybersecurity defenses.

Read More

Legislative Push for Healthcare Cybersecurity

A new federal bill is set to mandate stronger cybersecurity standards for the healthcare sector. With funding allocated for improvements, this legislation aims to bolster defenses against rising threats, though some experts say it may not be enough to fully address the sector's vulnerabilities.

Read More

Microsoft's Call for Stronger Global Cyber Defense

The latest Microsoft Digital Defense Report highlights a surge in cyber threats linked to geopolitical tensions. Nation-state actors and criminal groups increasingly share tactics, signaling a need for stronger defense and international cooperation to mitigate risks.

Read More

Microsoft
Microsoft Digital Defense Report 2024
The foundations and new frontiers of cybersecurity

Iranian Cyber Actors Targeting Critical Infrastructure

Reducing Complexity for Better Cybersecurity

A joint advisory from CISA, the FBI, NSA, and international partners warns about ongoing brute force and password spraying attacks targeting critical infrastructure. Learn about the tactics used and steps to strengthen your defenses against these threats.

Read More

Complexity is the enemy of effective cybersecurity. Learn how consolidating tools, adopting unified platforms, and leveraging AI can simplify operations, improve visibility, and enhance threat detection, reducing risks associated with today's dynamic threat landscape.

Read More

Modernizing Security Operations for Evolving Threats

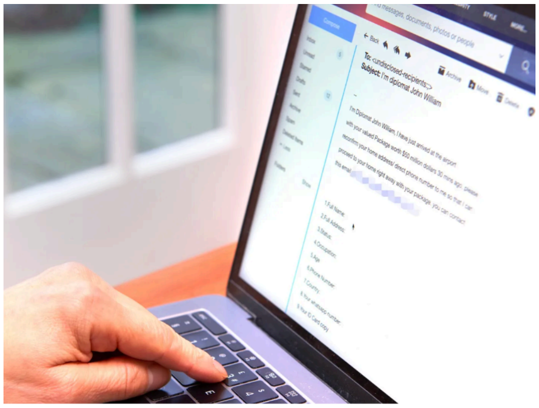
The traditional security model is no longer sufficient. Explore how zero-trust principles, automation, and AI are reshaping security operations to keep pace with sophisticated attackers and expanding digital environments.

Read More

Phishing Attacks: Exploiting Trusted Services

Cybercriminals increasingly use legitimate file-hosting services like OneDrive and Dropbox to deliver phishing payloads, bypassing traditional security measures. Find out how these tactics work and what can be done to protect against such sophisticated attacks.

Read More



Hackers Outsmarting Phishing Defenses with Obfuscation

Egress data reveals how attackers evade phishing filters by using benign elements, making emails appear safe. With obfuscation techniques becoming more common, organizations must rethink their email security approach to stay protected.

Read More

As cybersecurity continues to dominate the global conversation, it is clear that no sector is immune from the threats we face. The need for a stronger, more agile cybersecurity posture is undeniable, and this week's developments underscore the urgency. From healthcare to national defense, the challenge is not merely reacting to incidents but anticipating and preventing them. The path to resilient cybersecurity lies in embracing proactive defense strategies and leveraging advanced technologies. As the risks escalate, the pressure is on for leaders to adapt and ensure their organizations are prepared for the next wave of threats. Stay ahead by staying informed—your security depends on it.

Phishing attacks thrive on trust—be skeptical to stay safe.

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