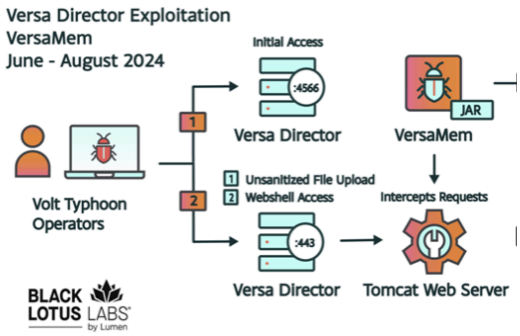
View this email in your browser

Weekly Insights and Updates

| August 30, 2024

This week's cybersecurity briefing examines critical digital security challenges across industries. We analyze the intensifying threats in manufacturing and healthcare sectors, where malicious actors target vital infrastructure and compromise patient care systems. Additionally, we highlight significant software vulnerabilities, including a recently discovered Chromezero-day exploit, underscoring the necessity for updated patch management protocols.

Our roundup extends to crucial risk mitigation strategies, encompassing the legal implications of security non-compliance and the implementation of NSA-recommended best practices. We also include news on the multifaceted nature of current threats, from sophisticated state operations to targeted scams affecting students returning to academic environments.



Chinese Volt Typhoon Exploits Versa Director Flaw

Nation-state actors are exploiting a zero-day vulnerability in Versa Director, targeting the IT sector globally. This incident highlights the importance of timely patch management and the ongoing threat posed by sophisticated cyber espionage groups.

Read More

Manufacturing: The Top Targeted Industry in 2024

Manufacturing remains the most targeted industry for cybercrime, with a significant increase in ransomware and database leaks. Organizations in this sector must prioritize cybersecurity to protect against these persistent threats.

Read More

Managing Cyber Risk in Public Companies

Nearly 700 cyber incidents were reported among Russell 3000 companies, emphasizing the critical need for comprehensive third-party risk management and accurate cybersecurity assessments to mitigate potential financial and operational impacts.

Read More

Georgia Tech Lawsuit for Cybersecurity Violations

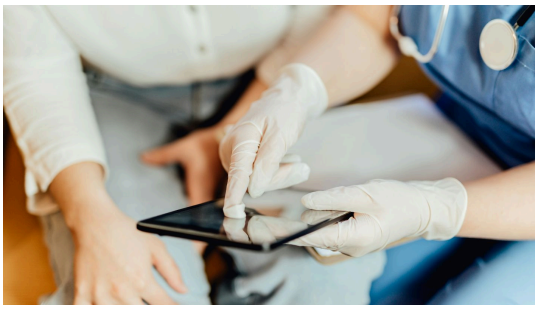
The U.S. government has filed a lawsuit against Georgia Tech for failing to meet DoD cybersecurity requirements. This case serves as a stark reminder of the legal and operational consequences of non-compliance with cybersecurity regulations.

Read More

Navigating Healthcare Cybersecurity Storm

Healthcare organizations are facing a surge in cyberattacks, impacting patient care and operational continuity. Learn strategies to enhance cyber resilience and reduce risk across all operational areas in this essential sector.

Read More



Healthcare's Ransomware Readiness Problem

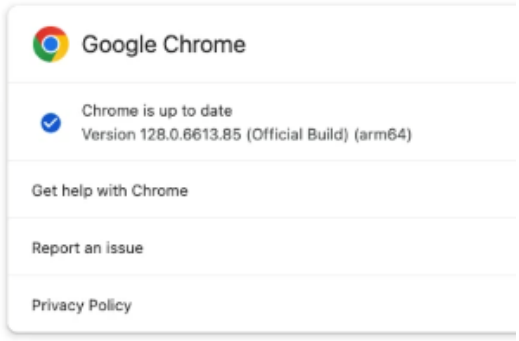
Ransomware is a critical threat to healthcare, with many hospitals unprepared to handle such attacks effectively. This article highlights the urgent need for better cybersecurity infrastructure and response strategies.

Read More

Back-to-School Scams Targeting Young Adults

As students return to school, they are increasingly targeted by scams. From textbook fraud to fake job offers, learn how to protect yourself and your loved ones from these common back-to-school scams.

Read More



New Chrome Zero-Day: Patch Now!

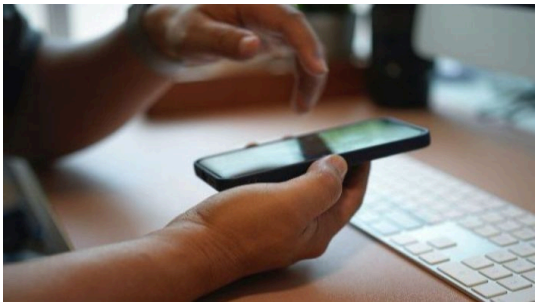
A new Chrome zero-day vulnerability (CVE-2024-7971) has been actively exploited in the wild. Users are urged to update their browsers immediately to protect against potential exploits.

Read More

Focus on Exposure Management

Effective exposure management is key to reducing your organization's attack surface and prioritizing vulnerabilities. This proactive approach allows you to focus on the most critical threats, ensuring a more secure digital environment.

Read More



NSA's Mobile Security Recommendations

The NSA advises regularly powering off your phone and following other best practices to protect against mobile threats. These simple yet effective measures can help safeguard your personal and professional data from cyberattacks.

Read More

Featured Articles by ATS

Spot the Signs of a Hack

Detecting a cyberattack early can save your business from severe damage. Learn the key indicators of a potential breach and discover the immediate

Penetration Testing 101

Understand the importance of penetration testing in safeguarding your organization’s digital assets. This guide breaks down the

Security Advisory: Iranian Cyber Threats

Recent intelligence reveals a surge in Iranian cyber activities targeting U.S. elections and critical infrastructure as the nation nears nuclear weapons

steps to take if your systems are compromised.

Read More

process and highlights how proactive vulnerability assessments can protect against real-world cyber threats.

Read More

capability. Learn how these developments heighten the risk for U.S. organizations and the urgent steps needed to bolster cybersecurity defenses.

Download PDF

The threats we face in cybersecurity are continuously evolving, making it imperative to stay informed and proactive. As our Security Operations team continues monitoring emerging threats, we invite you to stay connected and secure with ATS by your side.

The most significant cyber risk is assuming you're not at risk.

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