View this email in your browser

Weekly Insights and Updates

| October 4, 2024

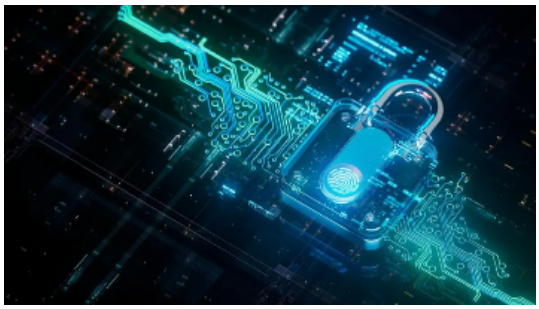
What if the greatest cybersecurity threat to your business wasn't from the outside, but from within your own systems? As hackers evolve, so do the vulnerabilities they exploit—whether it's your trusted apps, employees, or even routine processes. Uncover the hidden dangers lurking in plain sight and the insights you need to stay one step ahead.

Cybersecurity isn't a shield; it's a game of strategy. As threats grow more sophisticated, from financial extortion to mobile phishing, organizations need more than basic defenses. This week, we explore the unexpected players in the fight against cybercrime—CFOs, insider threats, and even your smartphone—and reveal how each could become your greatest vulnerability or your strongest ally.

North Korea's Stonefly APT Targets U.S. Companies

North Korean APT45 has shifted from espionage to extortion, attacking U.S. private companies for financial gain. Despite indictments and bounties, the group remains active.

Read More



Defending Critical Infrastructure through a Culture of Cybersecurity

Nation-state attacks on critical infrastructure are rising, and 42% of such organizations experienced breaches last year. Discover the best practices for creating resilient defenses.

Read More

NIST Invests $3M to Strengthen Cybersecurity Education

With a $3 million initiative, NIST aims to close the cybersecurity skills gap by supporting workforce development through educational programs and regional partnerships. Explore how your organization can benefit.

Read More

Moving DevOps Security Out of ‘The Stone Age’

DevOps environments offer agility but expand the attack surface. From insecure open-source libraries to cloud misconfigurations, security gaps persist.

Read More

Wells Fargo Data Breach Exposes Customer Information

A former employee’s unauthorized access to customer data at Wells Fargo has resulted in a major breach, affecting sensitive personal and financial information. See how insider threats can be mitigated through strong access control policies and real-time monitoring.

Read More

Third-Party Zero-Day Exploited in Rackspace Systems

Rackspace faces another security incident as a third-party zero-day vulnerability compromises customer data. Understand the importance of continuous

Cybersecurity Claims Show Wide Variability in Data Loss

A new report shows claims from cybersecurity incidents range from $1,000 to $500 million, with SMEs representing the majority of incidents.

monitoring and third-party risk management to prevent similar disruptions in your business.

Read More

Learn how ransomware and business email compromise (BEC) are driving these costs and what steps you can take to reduce your risk.

Read More

Google Play Store Apps Compromise Millions of Devices

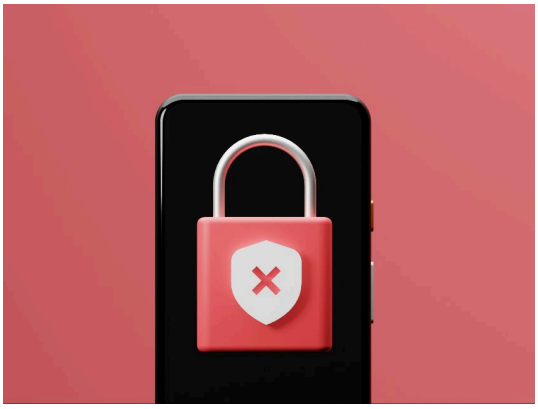
Even with Google tightening app security, dangerous apps continue to slip through. A recent report highlights the Necro Trojan found in modified versions of popular apps.

Read More

Mobile Phishing Attacks Surge Against Enterprises

Mishing, or mobile phishing, is now targeting enterprise mobile devices at unprecedented rates. With 76% of phishing sites using HTTPS, these attacks are harder to detect.

Read More



CFOs Suit Up for Cyberwar in the Evolving Risk Landscape

As stewards of financial data, CFOs are taking on greater responsibilities in cybersecurity. With financial data being a prime target, CFOs must work closely with IT leaders to protect sensitive information and align cybersecurity investments with broader business strategies.

Read More

As cyber threats become more unpredictable, it's clear that no system or role is immune. Whether it's through strategic collaboration, proactive defense, or recognizing vulnerabilities within, your organization's security depends on staying informed and adaptable. ATS is here to help turn awareness into action so that you are not just reacting to threats, but staying ahead of them.

In the code of every system lies both its defense and its undoing.

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