

[View this email in your browser](#)



American Technology Services Cybersecurity News Roundup

Weekly Insights and Updates

| September 13, 2024

This week's developments go beyond the usual headlines, revealing a series of incidents that are shaking up what we know about digital security. From public infrastructure under siege to cutting-edge malware designed to infiltrate both Windows and Linux systems, these stories challenge the conventional wisdom about where the real threats lie.

What's particularly unsettling this week is how attackers are finding new ways to exploit familiar systems. From impersonating legitimate software to weaponizing personal information, these stories reveal the shifting tactics that could easily catch even the most prepared off guard. It's a reminder that in cybersecurity, what you don't know can hurt you.



TfL Faces Ongoing Cybersecurity Incident

Transport for London is navigating a complex cyberattack that hasn't yet disrupted services but raises critical questions about the security of public infrastructure. This incident could expose vulnerabilities in the systems millions rely on daily.

[Read More](#)



Windows Update Zero-Day Exploited

A critical flaw in Windows Update has allowed attackers to roll back essential security patches. This vulnerability challenges our assumptions about the security of automatic updates and what might come next.

[Read More](#)



CISA Launches Cyber Incident Reporting Portal

CISA has introduced a new portal for cyber incident reporting, marking a significant shift in how critical infrastructure sectors handle cybersecurity threats. The forthcoming requirements could reshape how organizations approach incident management.

[Read More](#)



Halliburton Customer Data Theft

Halliburton recently disclosed a cyberattack that resulted in the theft of sensitive customer data. The breach serves as a stark reminder of the vulnerabilities within the energy sector and the potential ripple effects.

[Read More](#)

Sextortion Scams Use Photos of Victims' Homes

Sextortion scams are taking a terrifying new turn by incorporating personal details like photos of victims' homes. This evolution in cybercrime brings new concerns about privacy and the psychological tactics used by attackers.

[Read More](#)

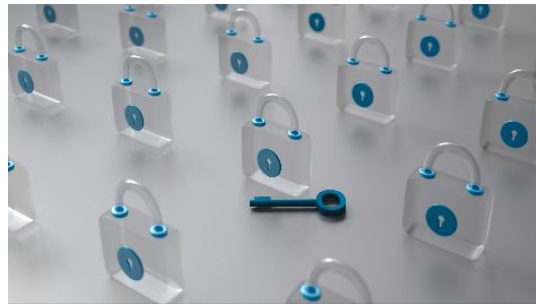
Sextortion



QR Code Phishing on the Rise

QR codes are everywhere, but so are the risks associated with scanning them. With the growing popularity of this technology, the danger of falling victim to “quishing” is more present than ever.

[Read More](#)



NIST's Post-Quantum Encryption Standards

As quantum computing looms on the horizon, NIST's new encryption standards are poised to redefine cybersecurity. These standards are more than just an update—they're a necessary evolution in the face of future quantum threats.

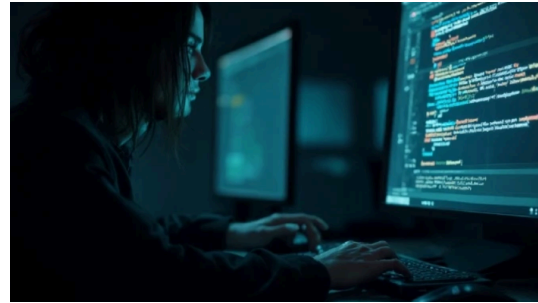
[Read More](#)



Avis Data Breach Affects 300,000 Customers

A data breach at Avis has compromised the personal information of hundreds of thousands of customers. This incident highlights ongoing challenges in data protection and the ever-present threat of cyberattacks.

[Read More](#)



Massive Data Breach Exposes 2.9 Billion Records

A massive data breach has exposed billions of records, putting countless individuals at risk. The sheer scale of this breach forces us to rethink how we protect and manage vast amounts of sensitive data.

[Read More](#)

New Cross-Platform Malware KTLVdoor

A newly discovered malware, KTLVdoor, is capable of attacking both Windows and Linux systems. The emergence of this cross-platform threat underscores the evolving tactics of sophisticated cybercriminals like Earth Lusca.

[Read More](#)

Featured Articles by ATS

Attack Surface Management

Every connected asset could be a potential vulnerability. Dive into the essentials of Attack Surface Management and discover why understanding your organization's digital footprint is critical for cybersecurity.

[Download PDF](#)

Preventing ATO Fraud

Account Takeover fraud is quietly becoming one of the most pervasive threats in cybersecurity. This article explores the tactics used by cybercriminals and the subtle signs that your accounts may be under attack.

[Download PDF](#)

The Growing Threat of DDoS Attacks

Distributed Denial of Service attacks are evolving, with the potential to bring down even the most resilient systems. Learn about the anatomy of these attacks and why they're more than just a temporary inconvenience.

[Download PDF](#)

Sometimes, the real story isn't in the headline—it's in the patterns that emerge between the lines. This week's roundup offers more than just news; it's a glimpse into the underlying currents shaping tomorrow's security environment. As we've seen from the

incidents and developments this week, cyber threats are becoming more sophisticated and widespread, affecting all sectors. Stay curious, stay aware.

Threats evolve, but with the right team, so does your defense.

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.

© 2024 American Technology Services All rights reserved.