View this email in your browser

AMERICAN
TECHNOLOGY
SERVICES

American Technology Services

Cybersecurity News Roundup

Weekly Insights and Updates

| August 23 2024

In the constantly shifting digital frontlines of cybersecurity, where threats are evolving faster than ever, it’s easy to feel overwhelmed by the sheer volume of news. That’s where we come in—cutting through the noise to bring you the most critical updates that matter to your organization. This week's roundup highlights the most pressing developments across the cybersecurity landscape, from state-sponsored attacks to the rise of sophisticated malware targeting different platforms. These insights are designed to keep you ahead of the curve, whether you’re managing information security for a large enterprise or your personal devices.

This edition covers emerging threats from state-sponsored groups, new malware targeting macOS, and significant data breaches. Leverage this intelligence to strengthen your organization's digital defense strategy against advanced persistent threats.

Disinformation and Malware Spread via Azure and Google Services

A recent disinformation campaign exploited Microsoft Azure and Google to drive traffic to malicious websites. Learn how attackers are polluting search results and redirecting users to malware, emphasizing the need for vigilant cybersecurity practices.

Read More

Iran's Election Meddling Sparks U.S. Cybersecurity Concerns

Iranian hackers are ramping up efforts to infiltrate U.S. presidential campaigns using sophisticated cyber tactics. This state-sponsored activity underscores the importance of protecting democratic institutions from foreign interference.

Read More

Phishing Links: A Growing Threat

Phishing attacks are shifting away from email attachments to links, with a 130% surge in malicious links. Understand the implications of this trend and why your organization must strengthen email security protocols.

Read More

DDoS Attacks Surge in 2024

DDoS attacks have risen by 46% in the first half of 2024, with the gaming and technology sectors being the hardest hit. Explore the evolving nature of these attacks and how your organization can bolster its defenses.

Read More

NPD Breach Exposes 2.9 Billion Records

A massive breach at National Public Data has compromised nearly 3 billion records, including Social Security numbers. This article highlights the critical need for strong data protection and the severe consequences of such breaches.

Read More

Microsoft Patches Zero-Day Flaw Exploited by Lazarus Group

North Korea's Lazarus Group exploited a zero-day flaw in Windows, gaining SYSTEM privileges. Learn about this vulnerability and why timely patching is essential to prevent similar attacks on your systems.

Read More

RansomHub Group's New EDR-Killing Tool

The RansomHub group has developed a new tool designed to disable EDR software, making ransomware attacks more effective. Discover how this tool works and what it means for your endpoint security strategy.

Read More

Cyber Incident Disrupts Microchip Technology's Operations

Microchip Technology's operations were disrupted by a cyber incident, impacting its ability to fulfill orders. This event highlights the critical need for comprehensive cybersecurity measures in supply chains and manufacturing.

Read More

BlindEagle APT Targets Latin America

BlindEagle, a new APT group, is launching sophisticated attacks on Latin American organizations via weaponized emails. This article explores their tactics and the importance of strong email security and threat detection.

Read More

macOS Under Attack by New Malware

macOS is increasingly targeted by cybercriminals, with arise in infostealers, trojans, and ransomware. Stay informed about the growing threats to macOS and how to protect your systems from these evolving risks.

Read More

Featured Articles by ATS

SIM Swapping: The Growing Threat to Multi-Factor Authentication

SIM swapping is increasingly compromising the security of multi-factor authentication (MFA), allowing attackers to bypass SMS-based protections. This article breaks down the mechanics of SIM swapping, highlighting high-profile cases and offering strategies to strengthen your organization's defenses against this emerging threat.

Mastering Access Control: Protecting Your Data from Unauthorized Access

Access control is critical for safeguarding sensitive information in today’s digital landscape. Learn about the essential strategies and models, such as Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC), that can help your organization minimize the risk of data breaches and maintain strong security.

MDR vs. MSSP: Choosing the Right Cybersecurity Partner

Understanding the differences between Managed Detection & Response (MDR) and Managed Security Services Providers (MSSP) is key to selecting the right solution for your business. This article compares their capabilities, focusing on advanced threat detection, incident response, and infrastructure management, to guide you in making an informed decision.

Read More | Read More | Read More

This week's coverage underscores the sophisticated threat landscape confronting modern organizations. From extensive data breaches and zero-day vulnerabilities to the proliferation of ransomware and targeted assaults on critical infrastructure, these are indicators of dynamic challenges that can compromise your organization's security posture and reputation. ATS remains dedicated to translating threat intelligence into actionable strategies to improve resilience and fortify security frameworks.

In the world of ones and zeros, skepticism is a virtue, and verification is wisdom.

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.