View this email in your browser

Weekly Insights and Updates

| February 21, 2025

Cybercriminals are automating deception, exploiting unpatched systems, and manipulating human psychology at an unprecedented scale. Phishing is no longer an amateur game—it's a streamlined business model where AI-powered kits can clone entire websites in seconds. Meanwhile, zero-day exploits are surfacing faster than patches, and nation-state groups are turning deception into high-stakes corporate espionage.

This week's top threats reveal how attackers are infiltrating firewalls, databases, and executive inboxes, exploiting job seekers and IT infrastructure alike. The security landscape isn't just evolving—it's becoming a merciless battlefield where automation, intelligence, and deception collide.

Microsoft Console Exploited to Steal Credentials

Cybercriminals are abusing Microsoft Management Console (MMC) files to distribute the Rhadamanthys Infostealer, using a patched DLL flaw and social engineering tactics. By disguising malware as legitimate documents and exploiting trust in system utilities, attackers are stealing credentials from browsers, password managers, and crypto wallets.

Read More

Phishing Attacks Now Targeting Executives

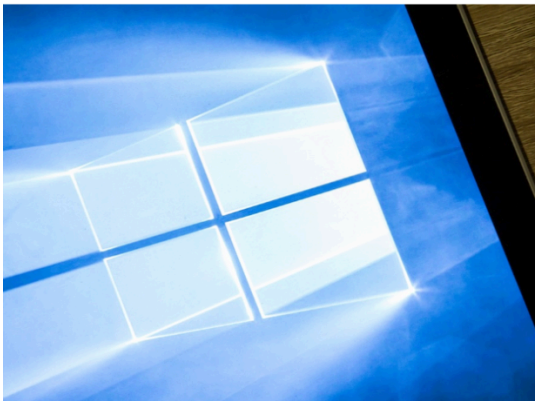
A Hackmosphere study found that 24% of CEOs clicked on phishing links, proving C-suite executives remain high-value cyber targets. Attackers used fake business proposals and industry conference invitations to bypass traditional email security and harvest credentials.

Read More

Palo Alto Firewall Vulnerability Under Attack

A critical authentication bypass flaw (CVE-2025-0108) in Palo Alto firewalls is under active attack, allowing hackers to remotely execute PHP scripts. Security firms report ongoing exploitation across 30+ IPs, with attackers chaining older vulnerabilities to deepen their access.

Read More



Chinese APT Exploiting New Windows Zero-Day

The Mustang Panda APT group is exploiting a Windows zero-day that lets attackers conceal malware in extracted RAR files, making them invisible in Windows Explorer. Microsoft has dismissed the flaw as low severity, but security experts warn it could become a stealthy vector for future attacks.

Read More

PostgreSQL Exploit Used in Treasury Attack

A PostgreSQL vulnerability (CVE-2025-1094) has been weaponized to remotely exploit BeyondTrust Remote Support systems, with confirmed breaches in the U.S. Treasury Department. Attackers used SQL injection via malformed UTF-8 sequences to gain full system control, forcing emergency patch releases.

Read More

Check Point Flaw Enables Ransomware Attacks

A Check Point firewall vulnerability (CVE-2024-24919) is being used to steal credentials and deploy the ShadowPad malware, a longtime espionage tool for Chinese-linked hackers. Victims have reported ransomware infections, lateral movement via VPNs, and DLL hijacking techniques designed for long-term persistence.

Read More

North Korean Hackers Lure Freelancers Into Traps

A North Korean-backed campaign is tricking freelance developers into downloading malware through fake job tests and trojanized repositories. Victims unknowingly install BeaverTail and InvisibleFerret, two modular backdoors designed to steal credentials, crypto wallets, and sensitive project data.

Read More

Microsoft Exchange Support Ending in 2025

On October 14, 2025, Microsoft will end all support for Exchange Server 2016 and 2019, leaving organizations vulnerable to security flaws and compliance violations. Businesses must begin migration now to Exchange Server SE, Microsoft 365, or Google Workspace before exposure becomes a liability.

Read More

MFA Friction and Implementation Pitfalls

Multi-factor authentication (MFA) is essential, but poor implementation can lead to user frustration, security gaps, and higher IT costs. Security teams must balance usability and protection by combining MFA with adaptive security policies, SSO, and risk-based authentication.

Read More

Darcula Phishing Kit Clones Websites Instantly

Cybercriminals no longer need coding skills—Darcula V3 can fully duplicate any website by simply pasting a URL into its automated phishing tool. With Telegram integration, real-time tracking, and anti-detection features, this PhaaS platform is lowering the barrier to large-scale, AI-driven phishing operations.

Read More

A phishing email that looks just like a real invoice. A firewall vulnerability that was patched too late. A CEO who clicks a link without thinking twice.

The nature of cyber threats has always been about deception—but now, deception is automated, scalable, and ruthlessly efficient. AI-driven phishing kits can duplicate any website with a single click. Zero-day exploits spread before patches can reach the network. Social engineering isn't just tricking employees—it's crafting entire narratives designed to manipulate human trust.

The battlefield isn't just on the network anymore. It's in the decisions we make, the emails we open, and the updates we ignore. Cybersecurity is no longer about defense—it's about anticipation, adaptation,

and understanding the game before it's played against you.

If attackers have automated deception, what are we doing to outthink them?

Hackers don't need to be smarter than you. They just need you to be distracted for five seconds.

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.