View this email in your browser

Weekly Insights and Updates

| March 28, 2025

Zero-days, credential abuse, and covert surveillance aren't just industry buzz—they're what your systems are up against this week. From widespread attacks on core Windows components to encrypted messaging platforms turned inside out, the perimeter of what counts as "secure" is tightening fast. The latest threats don't scream at your firewall—they slip through your inbox, ride in browser ads, or quietly disable your EDR before deploying ransomware in virtual environments you thought were safe.

Across these ten headlines, one pattern emerges: adversaries are adapting faster. They're combining tools, misusing encryption, and leveraging infrastructure most people take for granted—like Google Ads or iMessage. This roundup isn't just a collection of warnings. It's a mirror to what's happening now and a briefing on what to expect next. Let's get into it.

Zero-Day Targets NTLM Credentials

A newly discovered Windows vulnerability allows attackers to steal NTLM password hashes by tricking users into simply viewing a malicious file. Microsoft hasn't patched it yet, but researchers released a temporary fix to close the gap.

Read More

Time to Stop Using Passwords

The Atlantis AIO tool is automating massive credential-stuffing campaigns across 140+ services using stolen credentials. It's also bypassing two-factor protections by hijacking session cookies in real-time.

Read More

Time to Stop Using Passwords

The Atlantis AIO tool is automating massive credential-stuffing campaigns across 140+ services using stolen credentials. It's also bypassing two-factor protections by hijacking session cookies in real-time.

Read More

Even the Experts Can Slip

Cybersecurity leader Troy Hunt was tricked into logging into a fake Mailchimp portal, leading to the theft of 16,000 subscriber records. The phish exploited urgency and subtle social cues to bypass his usual caution.

Read More

Lucid Turns Encryption Against You

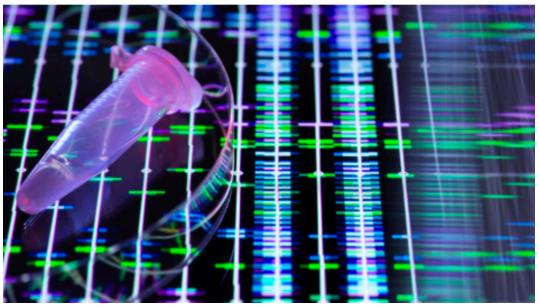
Lucid, a phishing-as-a-service operation, is exploiting iMessage and RCS protocols to run hyper-targeted, geofenced scams. The attacks impersonate delivery and tax brands with near-perfect accuracy and evade detection with expiring links.

Read More

OPSEC Breakdown at the Highest Level

U.S. officials used the encrypted app Signal to share war plans—accidentally including a journalist in the group chat. The incident highlights dangerous misunderstandings of what qualifies as secure communication for classified operations.

Read More



Genetic Data Now a Privacy Gamble

The consumer genetics company filed for Chapter 11 bankruptcy, raising concern over the future ownership and use of its 15 million-user genetic database. Legal protections vary by region, and potential buyers could repurpose the data.

Read More

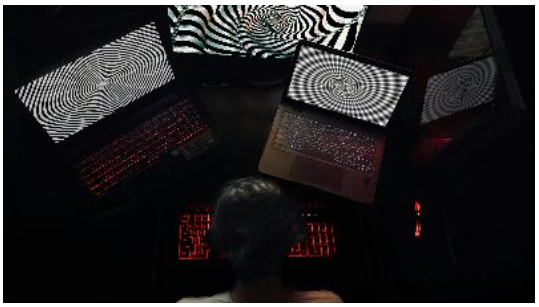
Chinese Gambling Scam Injects JS at Scale

A campaign using JavaScript and fake overlays has infected over 150,000 legitimate websites to redirect users to gambling sites. Some variants spoof well-known betting brands using copied logos and UI.

Read More

Espionage Masquerading as Extortion

RedCurl, a cyber-espionage group, is now deploying ransomware that targets hypervisors



New RaaS Tools Blind Security Software

without touching user endpoints. The attacks appear to be data-driven and selective, avoiding broad disruptions to maintain stealth.

Read More

RansomHub's custom EDRKillShifter tool is now circulating among ransomware crews to disable endpoint defenses pre-attack. EDR killers are increasingly used to blind detection systems before file encryption ever begins.

Read More

Some weeks feel like a pattern. Others—like this one—feel like a warning. The line between state-sponsored operations, cybercrime-for-hire, and opportunistic malware campaigns is blurring fast. We're seeing attacks that are technically elegant, behaviorally manipulative, and engineered for silence until it's too late.

Every story this week carries the same subtext: threat actors are better resourced, more coordinated, and increasingly unafraid to experiment. Sometimes, it's the bait that's convincing. Sometimes, it's the infrastructure you trusted. Sometimes, it's a mistake by someone who should know better. The difference now is how quiet the breach can be—and how quickly the damage spreads.

If you're reading this newsletter, you're already thinking critically—and that matters. We're here to keep you informed, aware, and one step ahead. When you need help interpreting what's coming next or want support translating this threat intel into action, we're ready.

The new phishing doesn't scream. It whispers in UX patterns and urgency tones.

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