View this email in your browser

AMERICAN
TECHNOLOGY
SERVICES

American Technology Services

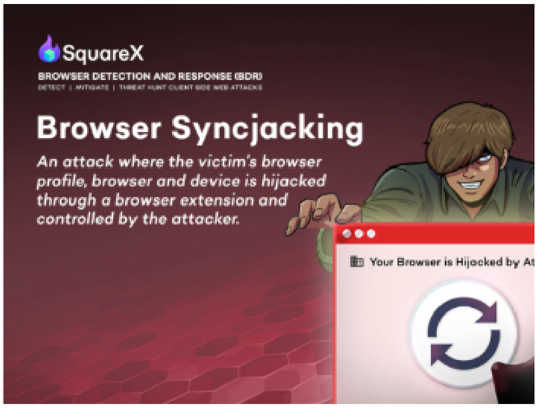
Cybersecurity News Roundup

Weekly Insights and Updates

| January 31, 2024

How much do you trust your browser extensions? What about the AI tools assisting in your daily workflow? In this week's cybersecurity round-up, we explore how attackers are turning everyday tools against us, from browser-based hijacking and AI-powered cyber ops to ransomware-as-a-service platforms that run like a Fortune 500 company. The battleground isn't just in sophisticated malware anymore—it's in the software we use and trust daily.

Meanwhile, vulnerabilities continue to surface in public-facing enterprise servers, widely used authentication systems, and even content delivery networks, exposing millions to account takeovers, data leaks, and real-world tracking risks. As security teams race to keep up, attackers industrialize cybercrime, automate deception, and exploit our blind spots with alarming efficiency.


SquareX
BROWSER DETECTION AND RESPONSE (BDR)
DETECT | MITIGATE | THREAT HUNT CLIENT SIDE WEB ATTACKS
Browser Syncjacking
An attack where the victim's browser profile, browser and device is hijacked through a browser extension and controlled by the attacker.
Your Browser is Hijacked by At

The Browser Extension That Can Take Over Your Device

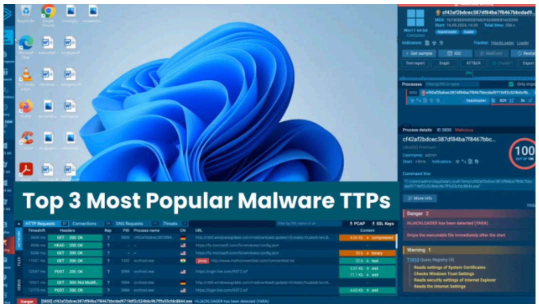
SquareX researchers reveal “Browser Syncjacking,” a method where malicious extensions silently sync a victim’s Chrome profile to an attacker’s Google Workspace—allowing full browser and device control. If it sounds like a nightmare scenario for enterprise security, it is.

Read More

Hackers Are Targeting Unpatched IIS, Apache, and SQL Servers

A Chinese-linked APT group is exploiting public-facing IIS, Apache Tomcat, and MSSQL servers, bypassing traditional security tools with DNS-based data exfiltration and PowerShell reverse shells. Keeping critical systems unpatched is an invitation to compromise.

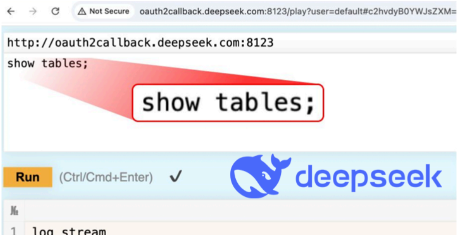
Read More



The Year's Top Malware Techniques Are More Subtle Than Ever

Attackers are hiding in plain sight by abusing PowerShell and CMD, evading detection with delayed execution tactics, and disguising malware as legitimate Windows processes. Defenders need to think like attackers—because traditional security tools aren't enough.

Read More



oauth2callback.deepseek.com:8123/play?user=default#c2hvdyB0YWJsZXM=

```
http://oauth2callback.deepseek.com:8123
show tables;
```

```
show tables;
```

```
1  log stream
```

AI Startup DeepSeek Leaks 1 Million Log Entries & Secret Keys

A misconfigured ClickHouse database exposed sensitive API secrets, chat logs, and backend credentials, demonstrating how AI companies continue to prioritize speed over security—a problem that could have catastrophic consequences.

Read More

57 Nation-State APT Groups Are Weaponizing AI

AI is now a cyber weapon. Threat actors from China, Iran, North Korea, and Russia are using Google's Gemini AI for phishing, malware development, job fraud, and cyber reconnaissance. Meanwhile, underground forums are selling rogue AI models designed to automate deception and crime.

Read More

Ransomware-as-a-Service Has Gone Corporate

The Lynx Ransomware Group runs like a full-fledged enterprise, offering affiliates ransomware kits, an automated victim dashboard, and an 80% revenue share. Cybercrime is no longer just a collection of hackers—it's an industrialized, scalable business model.

Read More

The Mirai Botnet is Back—This Time as a Service

A new Mirai variant, "Aquabot," is exploiting Mitel SIP phone vulnerabilities to build a global botnet for hire. The malware is being marketed on Telegram as a DDoS-as-a-service product, making mass disruption more accessible than ever.

Read More

Zyxel's Unpatched Zero-Day is Being Actively Exploited

CVE-2024-40891 has been known for six months—yet Zyxel has neither acknowledged it nor released a patch. Botnet operators are already exploiting it, turning thousands of unpatched CPE devices into attack vectors.

Read More

Airline Passengers Exposed by an OAuth Authentication Flaw

A misconfigured OAuth process in a major travel services provider allowed attackers to hijack airline users' accounts, steal loyalty points, and access personal data. OAuth flaws remain a massive attack surface for API-based account takeovers.

Read More

Signal and Discord Users Can Be Tracked via Cloudflare Flaw

A Cloudflare CDN bug allows attackers to deanonymize users with a single malicious image, revealing their location within a 250-mile radius. Zero-click attacks via push notifications make this an alarming privacy risk.

Read More

Cybercrime is evolving—not just in sophistication, but in efficiency. Attackers are weaponizing AI, automating deception, and scaling ransomware like a legitimate business. Meanwhile, organizations are still leaving critical security gaps unpatched, offering cybercriminals easy access to sensitive data, systems, and infrastructure.

This week's stories highlight a hard truth: security isn't just about defense—it's about vigilance. The weakest link is often not the technology, but the assumption that it's secure. Stay ahead of the threats, question what's trusted, and make cybersecurity a continuous strategy, not a reaction. Until next time—stay sharp, stay secure.

If an attacker can track your location by sending you an emoji, it's time to rethink privacy.

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