CYBER NEWSLETTER

Tuesday, Jan 13, 2026 • 05:45 UTC

THREAT PULSE

Zero-Days   0

Ransomware   0

Breaches   2

Phishing   1

Other   7

TOP 10

Lookback: 24h • Ranked by risk

BREACHES

BreachForums Breached, Exposing 324K Cybercriminals

Dark Reading • ■■■■ 63.1 • 7.7h

Massive data dump reveals real identities and details of administrators and members of the notorious hacker forum.

Why it matters: breach, recent.

https://www.darkreading.com/threat-intelligence/breachforums-breached-exposing-324k-cybercriminals

OTHER

n8n Supply Chain Attack Abuses Community Nodes to Steal OAuth Tokens

The Hacker News • ■■■■ 75.8 • 13.1h

Threat actors have been observed uploading a set of eight packages on the npm registry that masqueraded as integrations targeting the n8n workflow automation

Why it matters: supply chain, trusted source.

https://thehackernews.com/2026/01/n8n-supply-chain-attack-abuses.html

Iran-linked MuddyWater APT deploys Rust-based implant in latest campaign

CSO Online • ■■■■ 70.0 • 19.9h

Iran-linked advanced persistent threat group MuddyWater has deployed a Rust-based implant in an ongoing espionage campaign targeting organizations in Israel and

Why it matters: apt.

https://www.csoonline.com/article/4115379/iran-linked-muddywater-apt-deploys-rust-based-implant-in-latest-campaign.html

Notorious BreachForums hacking site hit by 'doomsday' leak of 324,000 criminal users

CSO Online • ■■■■ 63.0 • 8.2h

Prominent crime forum BreachForums has suffered a new and possibly fatal blow to its reputation after the revelation that a database of thousands of criminals using it was

Why it matters: breach, recent.

https://www.csoonline.com/article/4115660/notorious-breachforums-hacking-site-hit-by-doomsday-leak-of-324000-criminal-users.html

PHISHING

FBI Flags Quishing Attacks From North Korean APT

Dark Reading • ■■■■ 87.2 • 10.3h

A state-sponsored threat group tracked as "Kimsuky" sent QR-code-filled phishing emails to US and foreign government agencies, NGOs, and academic institutions.

Why it matters: apt, phishing.

https://www.darkreading.com/mobile-security/fbi-quishing-attacks-north-korean-apt

Shai-Hulud & Co.: Die Supply Chain als Achillesferse

CSO Online • ■■■■ 69.3 • 15.3h

FAMArtPhotography – shutterstock.com Heutige Anwendungen basieren auf zahlreichen Komponenten, von denen jede zusammen mit den Entwicklungsumgebungen

Why it matters: supply chain.

https://www.csoonline.com/article/4115440/shai-hulud-co-die-supply-chain-als-achillesferse.html

Malicious npm packages target the n8n automation platform in a supply chain attack

CSO Online • ■■■■ 67.0 • 17.9h

Threat actors were spotted weaponizing the n8n automation ecosystem this week, slipping malicious npm packages into its marketplace of community-maintained

Why it matters: supply chain.

https://www.csoonline.com/article/4115417/malicious-npm-packages-target-n8n-automation-platform-in-a-supply-chain-attack.html

CYBER NEWSLETTER

Tuesday, Jan 13, 2026 • 05:45 UTC

THREAT PULSE

Zero-Days   0

Ransomware   0

Breaches   2

Phishing   1

Other   7

TOP 10

1. FBI Flags Quishing Attacks From North Korean APT

2. n8n Supply Chain Attack Abuses Community Nodes to Steal OAuth Tokens

3. Iran-linked MuddyWater APT deploys Rust-based implant in latest campaign

4. Shai-Hulud & Co.: Die Supply Chain als Achillesferse

5. Malicious npm packages target the n8n automation platform in a supply chain attack

6. BreachForums Breached, Exposing 324K Cybercriminals

7. Notorious BreachForums hacking site hit by 'doomsday' leak of 324,000 criminal users

8. GoBruteforcer Botnet Targets 50K-plus Linux Servers

9. GoBruteforcer Botnet Targets Crypto Project Databases by Exploiting Weak Credentials

10. Critical vulnerability found in n8n workflow automation platform

Lookback: 24h • Ranked by risk

GoBruteforcer Botnet Targets 50K-plus Linux Servers

Dark Reading • ■■■■ 62.9 • 8.4h
Researchers detailed a souped-up version of the GoBruteforcer botnet that preys on servers with weak credentials and AI-generated configurations.
Why it matters: botnet, recent.
https://www.darkreading.com/threat-intelligence/gobruteforcer-botnet-targets-50k-plus-linux-servers

GoBruteforcer Botnet Targets Crypto Project Databases by Exploiting Weak Credentials

The Hacker News • ■■■■ 61.0 • 19.0h
A new wave of GoBruteforcer attacks has targeted databases of cryptocurrency and blockchain projects to co-opt them into a botnet that's capable of brute-forcing
Why it matters: botnet, trusted source.
https://thehackernews.com/2026/01/gobruteforcer-botnet-targets-crypto.html

Critical vulnerability found in n8n workflow automation platform

Cybersecurity Dive • ■■■■ 59.7 • 13.3h
The open-source platform is widely used across enterprise environments, leaving thousands of instances at risk.
Why it matters: critical.
https://www.cybersecuritydive.com/news/critical-vulnerability-n8n-automation-platform/809360/