# CYBER NEWSLETTER

Monday, Jan 12, 2026 • 18:51 UTC

## THREAT PULSE

| | |
|---|---|
| Zero-Days | 0 |
| Ransomware | 0 |
| Breaches | 1 |
| Phishing | 1 |
| Other | 8 |

## TOP 10

1. n8n Supply Chain Attack Abuses Community Nodes to Steal OAuth Tokens
2. Iran-linked MuddyWater APT deploys Rust-based implant in latest campaign
3. Shai-Hulud & Co.: Die Supply Chain als Achillesferse
4. Malicious npm packages target the n8n automation platform in a supply chain attack
5. GoBruteforcer Botnet Targets Crypto Project Databases by Exploiting Weak Credentials
6. Critical vulnerability found in n8n workflow automation platform
7. GoFundMe Ignores Own Rules by Hosting a Legal-Defense Fund for the ICE Agent Who
8. Trend Micro patches critical flaws in its Apex Central software
9. MuddyWater Launches RustyWater RAT via Spear-Phishing Across Middle East Sectors
10. ■ Weekly Recap: AI Automation Exploits, Telecom Espionage, Prompt Poaching & More

Lookback: 72h • Ranked by risk

## BREACHES

### GoFundMe Ignores Own Rules by Hosting a Legal-Defense Fund for the ICE Agent Who

WIRED Security • ■■■■ 61.5 • 0.0h

The fundraiser for the ICE agent in the Renee Good killing has stayed online in seeming breach of GoFundMe’s own terms of service, prompting questions about selective

*Why it matters: breach, breaking.*

https://www.wired.com/story/gofundme-ice-jonathan-ross-renee-good-fundraiser/

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

CSO Online • ■■■■ 79.1 • 9.0h

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, recent.*

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

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

CSO Online • ■■■■ 74.3 • 4.4h

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

*Why it matters: supply chain, breaking.*

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

## PHISHING

### MuddyWater Launches RustyWater RAT via Spear-Phishing Across Middle East Sectors

The Hacker News • ■■■■ 51.2 • 56.3h

The Iranian threat actor known as MuddyWater has been attributed to a spear-phishing campaign targeting diplomatic, maritime, financial, and telecom entities in the

*Why it matters: phishing, trusted source.*

https://thehackernews.com/2026/01/muddywater-launches-rustywater-rat-via.html

## OTHER

### n8n Supply Chain Attack Abuses Community Nodes to Steal OAuth Tokens

The Hacker News • ■■■■ 79.4 • 2.2h

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

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

CSO Online • ■■■■ 74.2 • 7.0h

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, recent.*

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

# CYBER NEWSLETTER

Monday, Jan 12, 2026 • 18:51 UTC

## THREAT PULSE

| | |
|---|---|
| Zero-Days | 0 |
| Ransomware | 0 |
| Breaches | 1 |
| Phishing | 1 |
| Other | 8 |

## TOP 10

1. n8n Supply Chain Attack Abuses Community Nodes to Steal OAuth Tokens
2. Iran-linked MuddyWater APT deploys Rust-based implant in latest campaign
3. Shai-Hulud & Co.: Die Supply Chain als Achillesferse
4. Malicious npm packages target the n8n automation platform in a supply chain attack
5. GoBruteforcer Botnet Targets Crypto Project Databases by Exploiting Weak Credentials
6. Critical vulnerability found in n8n workflow automation platform
7. GoFundMe Ignores Own Rules by Hosting a Legal-Defense Fund for the ICE Agent Who
8. Trend Micro patches critical flaws in its Apex Central software
9. MuddyWater Launches RustyWater RAT via Spear-Phishing Across Middle East Sectors
10. ■ Weekly Recap: AI Automation Exploits, Telecom Espionage, Prompt Poaching & More

Lookback: 72h • Ranked by risk

### GoBruteforcer Botnet Targets Crypto Project Databases by Exploiting Weak Credentials

The Hacker News • ■■■■ 69.2 • 8.1h

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 • ■■■■ 63.4 • 2.4h

The open-source platform is widely used across enterprise environments, leaving thousands of instances at risk.

*Why it matters: critical, breaking.*

https://www.cybersecuritydive.com/news/critical-vulnerability-n8n-automation-platform/809360/

### ■ Weekly Recap: AI Automation Exploits, Telecom Espionage, Prompt Poaching & More

The Hacker News • ■■■■ 49.3 • 5.2h

This week made one thing clear: small oversights can spiral fast. Tools meant to save time and reduce friction turned into easy entry points once basic safeguards were

*Why it matters: trusted source, breaking.*

https://thehackernews.com/2026/01/weekly-recap-ai-automation-exploits.html

### Trend Micro patches critical flaws in its Apex Central software

CSO Online • ■■■■ 52.4 • 66.1h

Security company Trend Micro has been compelled to issue a patch for its own Apex Central software management tool after vulnerability management platform

*Why it matters: critical.*

https://www.csoonline.com/article/4115151/trend-micro-patches-critical-flaws-in-its-apex-central-software.html