CYBER NEWSLETTER

Thursday, Jan 15, 2026 • 05:51 UTC

THREAT PULSE

Zero-Days 4
Ransomware 2
Breaches 1
Phishing 1
Other 2

TOP 10

Lookback: 72h • Ranked by risk

ZERO-DAYS

Microsoft Fixes 114 Windows Flaws in January 2026 Patch, One Actively Exploited

The Hacker News • ■■■■ 128.4 • 20.2h
Microsoft on Tuesday rolled out its first security update for 2026, addressing 114 security flaws, including one vulnerability that it said has been actively exploited in the
Why it matters: actively exploited, in the wild.
https://thehackernews.com/2026/01/microsoft-fixes-114-windows-flaws-in.html

Microsoft Starts 2026 With a Bang: A Freshly Exploited Zero-Day

Dark Reading • ■■■■ 82.0 • 32.7h
The vendor's first Patch Tuesday of the year also contains fixes for 112 CVEs, nearly double the amount from last month.
Why it matters: zero-day.
https://www.darkreading.com/application-security/microsofts-starts-2026-bang-zero-day

RANSOMWARE

Ransomware-Banden erpressen Opfer mit Compliance-Verstößen

CSO Online • ■■■■ 75.9 • 39.0h
Digitala World – shutterstock.com Ransomware-Attacken zählen nach wie vor zu den häufigsten Angriffsmethoden. Wie aktuelle Analysen zeigen, drohen Cyberbanden ihren
Why it matters: ransomware.
https://www.csoonline.com/article/4116135/ransomware-banden-erpressen-opfer-mit-compliance-verstosen.html

PHISHING

January 2026 Microsoft Patch Tuesday: Actively exploited zero day needs attention

CSO Online • ■■■■ 122.6 • 28.0h
Eight critical vulnerabilities and an actively exploited zero day highlight Microsoft’s first Patch Tuesday announcements for 2026 . Most of the higher scoring
Why it matters: zero-day, actively exploited.
https://www.csoonline.com/article/4116437/january-2026-microsoft-patch-tuesday-actively-exploited-zero-day-needs-attention.html

Microsoft Patches Exploited Windows Zero-Day, 111 Other Vulnerabilities

SecurityWeek • ■■■■ 86.9 • 32.9h
Two vulnerabilities patched this month by Microsoft were disclosed publicly before fixes were released. The post Microsoft Patches Exploited Windows Zero-Day, 111
Why it matters: zero-day, trusted source.
https://www.securityweek.com/microsoft-patches-exploited-windows-zero-day-111-other-vulnerabilities/

Laughter in the dark: Tales of absurdity from the cyber frontline and what they taught us

Sophos News • ■■■■ 75.0 • 53.9h
From a quintuple-encryption ransomware attack to zany dark web schemes and AI fails, Sophos X-Ops looks back at some of our favorite weirdest incidents from the last few
Why it matters: ransomware.
https://sophos-production.contentstackapps.com/en-us/blog/laughter-in-the-dark-tales-of-absurdity

BREACHES

Robo-Advisor Betterment Discloses Data Breach

SecurityWeek • ■■■■ 98.5 • 19.0h
A threat actor breached Betterment’s systems, accessed customer information, and sent scam crypto-related messages. The post Robo-Advisor Betterment Discloses
Why it matters: data breach, breach.
https://www.securityweek.com/robo-advisor-betterment-discloses-data-breach/

CYBER NEWSLETTER

Thursday, Jan 15, 2026 • 05:51 UTC

THREAT PULSE

Zero-Days 4
Ransomware 2
Breaches 1
Phishing 1
Other 2

TOP 10

1. Microsoft Fixes 114 Windows Flaws in January 2026 Patch, One Actively Exploited
2. January 2026 Microsoft Patch Tuesday: Actively exploited zero day needs attention
3. Fortinet Fixes Critical FortiSIEM Flaw Allowing Unauthenticated Remote Code
4. Robo-Advisor Betterment Discloses Data Breach
5. Microsoft Patches Exploited Windows Zero-Day, 111 Other Vulnerabilities
6. Microsoft Starts 2026 With a Bang: A Freshly Exploited Zero-Day
7. FBI Flags Quishing Attacks From North Korean APT
8. Ransomware-Banden erpressen Opfer mit Compliance-Verstößen
9. Laughter in the dark: Tales of absurdity from the cyber frontline and what they taught us
10. SpyCloud Launches Supply Chain Solution to Combat Rising Third-Party Identity Threats

Lookback: 72h • Ranked by risk

FBI Flags Quishing Attacks From North Korean APT

Dark Reading • ■■■■ 80.4 • 58.4h
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

OTHER

Fortinet Fixes Critical FortiSIEM Flaw Allowing Unauthenticated Remote Code

The Hacker News • ■■■■ 103.6 • 18.0h
Fortinet has released updates to fix a critical security flaw impacting FortiSIEM that could allow an unauthenticated attacker to achieve code execution on susceptible
Why it matters: critical, remote code execution.
https://thehackernews.com/2026/01/fortinet-fixes-critical-fortisiem-flaw.html

SpyCloud Launches Supply Chain Solution to Combat Rising Third-Party Identity Threats

CSO Online • ■■■■ 73.7 • 16.9h
SpyCloud , the leader in identity threat protection, today announced the launch of its Supply Chain Threat Protection solution, an advanced layer of defense that
Why it matters: supply chain.
https://www.csoonline.com/article/4116536/spycloud-launches-supply-chain-solution-to-combat-rising-third-party-identity-threats.html