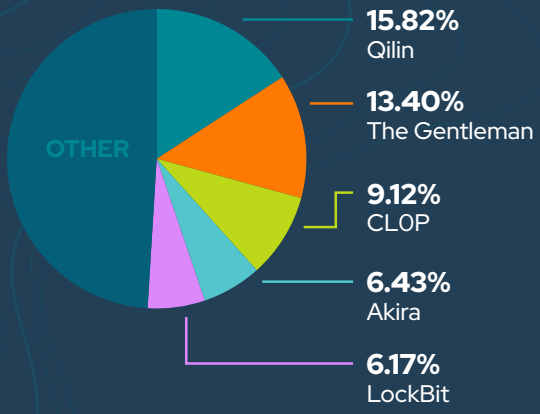
BYER-NICHOLS THREAT BRIEF

FIRST HALF FEBRUARY 2026

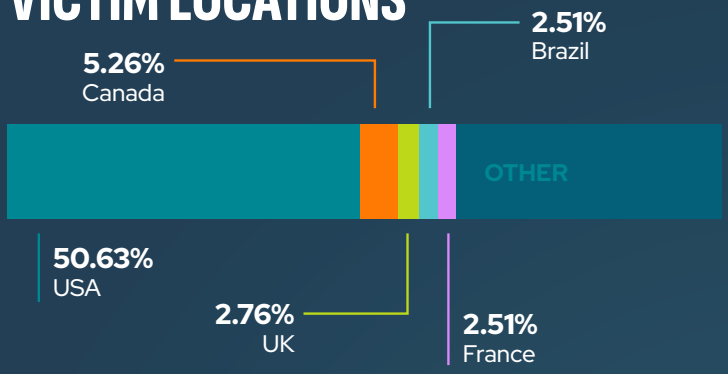
In early February, APT activity leaned hard on cloud abuse, identity compromise, and long-dwell access, with UNC3886 standing out for its persistence. Exploited bugs across Notepad++, SolarWinds, Apple, and Microsoft underscored the need for fast patching and tighter identity controls. Ransomware crews stayed active, with Qilin and The Gentlemen driving most cases while Cl0p's earlier huge Cleo-linked victim dump kept pressure high despite fewer new hits.

TOP RANSOMWARE



Qilin led early-February activity with steady, opportunistic hits on mid-market firms, while The Gentlemen continued their swingy pattern of data-leak-driven extortion. Cl0p's numbers stayed elevated after its earlier massive Cleo-linked victim dump, which reshaped the landscape despite fewer fresh intrusions. Akira kept up its fast-moving double-extortion playbook, and LockBit—though quieter—remained persistent through affiliates recycling older access paths.

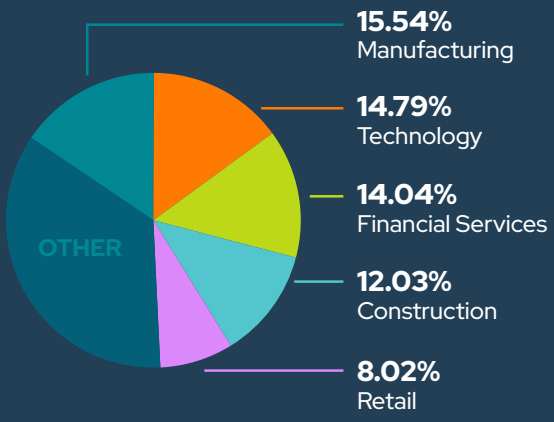
VICTIM LOCATIONS



TOP NEWS

- Notepad++ update feature hijacked by Chinese state hackers for months
- Exposed MongoDB instances still targeted in data extortion attacks
- Coinbase confirms insider breach linked to leaked support tool screenshots
- Malicious MoltBot skills used to push password-stealing malware
- Owner of Incognito dark web drugs market gets 30 years in prison
- Step Finance says compromised execs' devices led to $40M crypto theft
- Fugitive behind $73M 'pig butchering' scheme gets 20 years in prison
- Police arrest seller of JokerOTP MFA passcode capturing tool

VICTIM SECTOR



VICTIM ORG SIZE

TRENDING & ACTIVELY EXPLOITED VULNERABILITIES

CVE	VENDOR	PRODUCT
CVE-2025-15556	Notepad++	Notepad++
CVE-2025-40536	SolarWinds	Web Help Desk
CVE-2025-40551	SolarWinds	Web Help Desk
CVE-2026-20700	Apple	Multiple Products
CVE-2026-21510	Microsoft	Windows
CVE-2026-21513	Microsoft	Windows
CVE-2026-21514	Microsoft	Office
CVE-2026-21519	Microsoft	Windows
CVE-2026-21525	Microsoft	Windows
CVE-2026-21533	Microsoft	Windows

Early February saw active exploitation across a pretty mixed stack: a Notepad++ bug, two SolarWinds Web Help Desk flaws, a broad Apple multi-product issue, and a run of Windows and Office CVEs. The big worry is chaining—attackers using a simple app bug or help-desk exposure to gain initial access, then pivoting via Windows and Office privilege-escalation and RCE paths. Teams should fast-track patching for internet-facing Web Help Desk instances, push Apple and Microsoft updates, tighten identity and macro controls, and watch EDR for post-exploit lateral movement.

TRENDING MALWARE

CastleLoader
A stealthy first-stage loader used in targeted attacks against government and critical-infrastructure organizations

DarkNimbus
A cross-platform backdoor (Windows and Android) used for surveillance, data theft, and staging follow-on malware.

HYPERCALL
Part of a North Korean malware toolkit used by UNC1069 in financially motivated intrusions against cryptocurrency and DeFi organizations.

SSHStalker
A newly discovered Linux botnet that blends 2009-era IRC botnet techniques with modern automated mass-scanning and compromise.

WAVESHAPER
WAVESHAPER is another component of UNC1069's expanding malware arsenal, used in targeted attacks on crypto-sector organizations.

ZeroDayRAT
A commercial mobile spyware platform openly marketed on Telegram, offering full remote control of Android devices.

TRENDING ADVERSARIES

Storm-2603 | **UNC1069** | **UNC4895**
TGR-STA-1030 | **UNC3886** | **Violet Typhoon**

Storm-2603, TGR-STA-1030, UNC1069, UNC3886, UNC4895, and Violet Typhoon all leaned heavily on stealthy access, cloud abuse, and long-dwell espionage in recent weeks. Most are doubling down on identity compromise, living-off-the-land tooling, and quietly pivoting through hybrid cloud environments. UNC3886 remains the most concerning thanks to its persistence tricks and focus on high-value infrastructure. Defenders should expect more identity-driven lateral movement and cloud-focused tradecraft.

PRODUCED & DISTRIBUTED BY
PHISH TANK DIGITAL

WRITTEN BY
JEREMY NICHOLS
Former Director of the Global Threat Intelligence Center

SUMMARIES & BIOS
GEOFF REHMET
Cybersecurity Expert