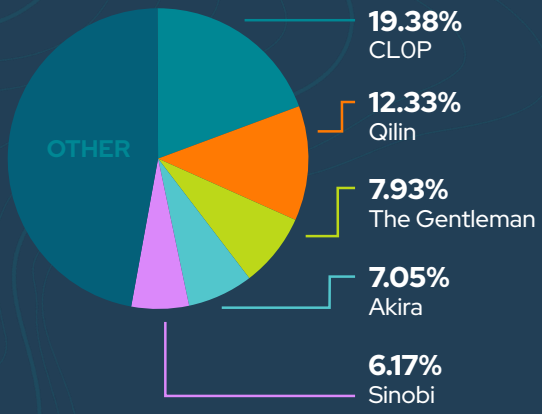
BYER-NICHOLS THREAT BRIEF

SECOND HALF JANUARY 2026

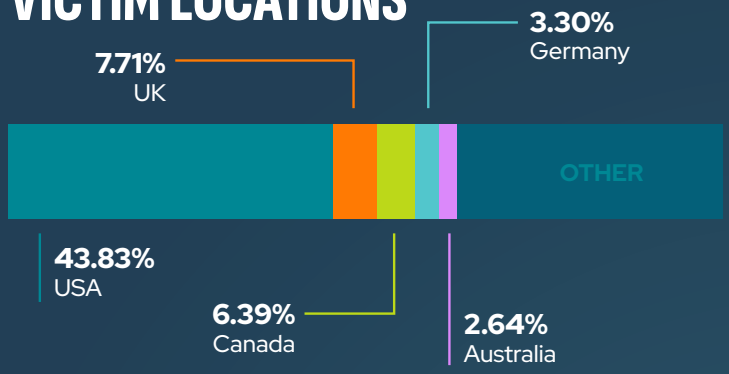
Ransomware stayed hot in late January, with Cl0p jumping to the top after its huge Cleo linked victim dump, while Qilin, Akira, Sinobi and The Gentlemen kept pressure on manufacturing and mid market orgs. At the same time, exploitation of vCenter, SmarterMail, Zimbra, Ivanti EPMM and Fortinet gear drove a wave of opportunistic intrusions. Threat actors like Sandworm, Konni and ShinyHunters leaned on phishing, credential theft and stealthy C2, with Sandworm remaining the most worrying due to its destructive track record.

TOP RANSOMWARE



Cl0p surged to the top in late January 2026, driven by a massive leak of victims tied to its Cleo campaign—likely exploiting supply-chain weaknesses. Qilin held steady in second, continuing its aggressive targeting of manufacturing and mid-sized enterprises. Akira and Sinobi remain active with fast encryption and double-extortion tactics, while The Gentlemen group is gaining traction through tailored phishing and data leak threats. The shift toward faster, more surgical campaigns and tighter ransom timelines is becoming a clear trend.

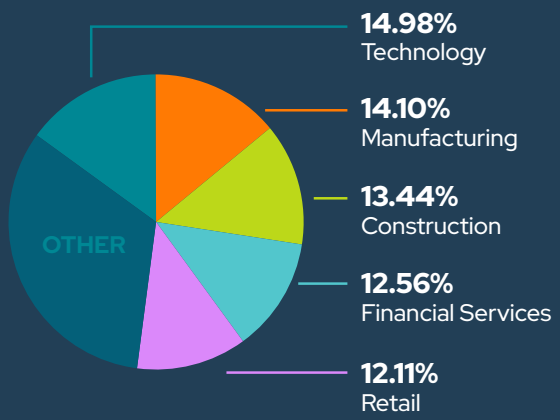
VICTIM LOCATIONS



TOP NEWS

- Black Basta boss makes it onto Interpol's 'Red Notice' list
- Crypto wallets received a record $158 billion in illicit funds last year
- Jordanian pleads guilty to selling access to 50 corporate networks
- Konni hackers target blockchain engineers with AI-built malware
- New ClickFix attacks abuse Windows App-V scripts to push malware
- New malware service Stanley guarantees phishing extensions on Chrome web store
- US convicts ex-Google engineer for sending AI tech data to China
- US to deport Venezuelans who emptied bank ATMs using malware

VICTIM SECTOR



VICTIM ORG SIZE

TRENDING & ACTIVELY EXPLOITED VULNERABILITIES

CVE	VENDOR	PRODUCT
CVE-2024-37079	Broadcom	VMware vCenter Server
CVE-2025-34026	Versa	Concerto
CVE-2025-52691	SmarterTools	SmarterMail
CVE-2025-68645	Synacor	Zimbra Collaboration Suite (ZCS)
CVE-2026-1281	Ivanti	Endpoint Manager Mobile (EPMM)
CVE-2026-20045	Cisco	Unified Communications Manager
CVE-2026-21509	Microsoft	Office
CVE-2026-23760	SmarterTools	SmarterMail
CVE-2026-24061	GNU	InetUtils
CVE-2026-24858	Fortinet	Multiple Products

Late January 2026 exploits hit a nasty mix of edge and core: VMware vCenter, Versa Concerto, SmarterMail (two bugs), Zimbra, Ivanti EPMM zero-day RCEs, Cisco Unified Comms, Microsoft Office, GNU InetUtils, and multiple Fortinet products. The big worry is internet-facing management and mail systems being used for initial access and lateral movement. Defenders should fast-track patches and hotfixes, lock down and segment exposed services, enforce MFA on admin access, and monitor logs/IDS closely for new exploit and post-compromise activity.

TRENDING MALWARE

Android.Click.415
Malware that uses AI-driven automation to perform ad-click fraud by silently opening browser windows

DynoWiper
A destructive wiper attributed to Russia's Sandworm group, deployed in a failed December 2025 attack on Poland's energy sector

GhostPoster
A browser extension-based malware campaign that infected over 840,000 users

Osiris
A newly identified ransomware strain that hit a Southeast Asian food company in late 2025

PDFSider
A stealthy Windows backdoor used by ransomware groups and APTs

Ploutus
ATM-targeting malware used in jackpotting schemes to force machines to dispense all cash

TRENDING ADVERSARIES

KongTuke | **NoName057(16)** | **ShinyHunters**
Konni | **Sandworm** | **UAT-8837**

KongTuke, Konni, NoName057(16), Sandworm, ShinyHunters, and UAT-8837 are trending for their mix of espionage, hacktivism, and data theft. Most are leaning into browser-based lures, credential harvesting, and destructive payloads, often targeting government, telecom, and crypto sectors. Sandworm stands out as the most dangerous—its infrastructure attacks and wiper campaigns pose serious risks to national stability. Common threads include phishing, proxy-based C2, and modular loaders. Defenders should expect stealthy persistence and politically charged targeting.

phish tank DIGITAL

PRODUCED & DISTRIBUTED BY
PHISH TANK DIGITAL

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

SUMMARIES & BIOS
GEOFF REHMET
Cybersecurity Expert