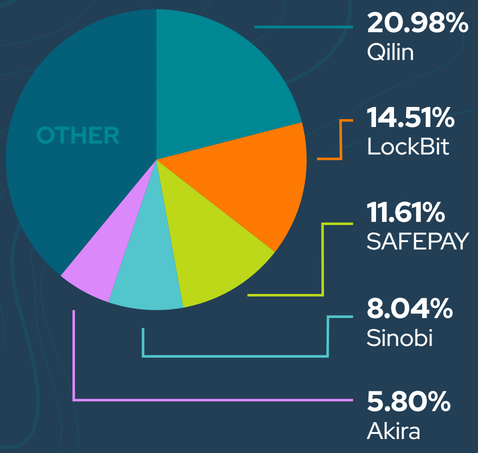
BYER-NICHOLS THREAT BRIEF

SECOND HALF DECEMBER 2025

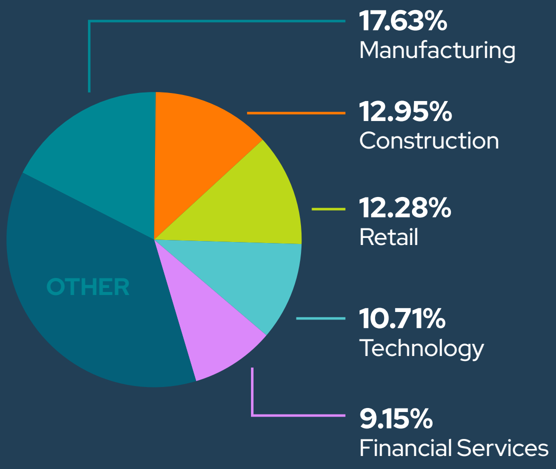
As 2025 ended vendor reports slowed down. Even reports of emerging threats slowed down a little. Could the bad guys also be taking a break? The reality seems less comforting as we are still seeing plenty of victims and we are also seeing a significant number of actively exploited vulnerabilities. On a positive note, we have seen successes reported in the disruption of threat actor groups, including an Interpol-led action which resulted in decryption of 6 ransomware strains and hundreds of arrests.

TOP RANSOMWARE

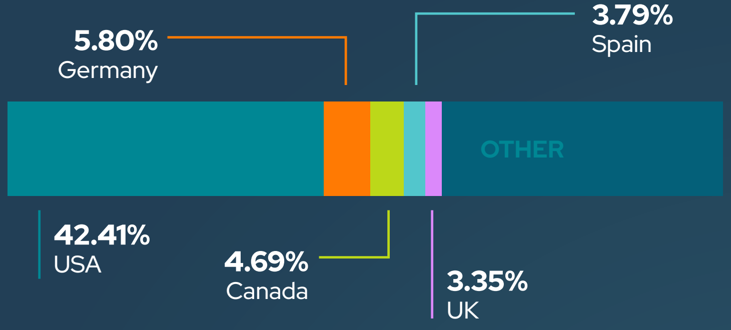


Qilin, one of the most prolific ransomware groups of 2025 closed the year as the most visible trending ransomware actor – for the third period running. Qilin had listed over 1000 victims on its leaks site by late December, and its activity remained aggressive and industrialized, scaling attacks across manufacturing, financial services, healthcare and government sectors.

VICTIM SECTOR



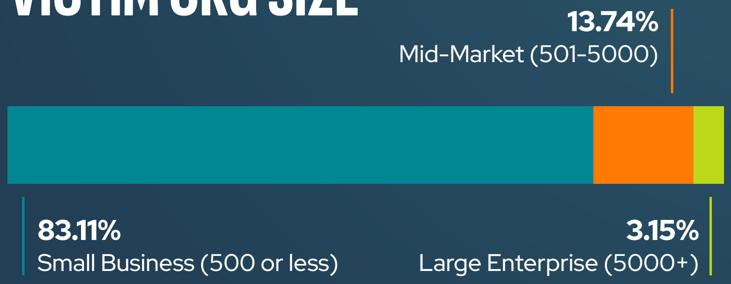
VICTIM LOCATIONS



TOP NEWS

- Amazon disrupts Russian GRU hackers attacking edge network devices
- Critical React2Shell flaw exploited in ransomware attacks
- France arrests Latvian for installing malware on Italian ferry
- Hackers drain $3.9M from Unleash Protocol after multisig hijack
- Interpol-led action decrypts 6 ransomware strains, arrests hundreds
- Trust Wallet confirms extension hack led to $7 million crypto theft
- US cybersecurity experts plead guilty to BlackCat ransomware attacks
- US seizes E-Note crypto exchange for laundering ransomware payments

VICTIM ORG SIZE



TRENDING & ACTIVELY EXPLOITED VULNERABILITIES

CVE	VENDOR	PRODUCT
CVE-2023-52163	Digiever	DS-2105 Pro
CVE-2025-13915	IBM	API Connect
CVE-2025-14733	WatchGuard	Firebox
CVE-2025-14847	MongoDB	MongoDB & MongoDB Server
CVE-2025-20393	Cisco	Multiple Products
CVE-2025-37164	HPE	OneView
CVE-2025-40602	SonicWall	SMA1000 appliance
CVE-2025-59374	ASUS	Live Update
CVE-2025-59718	Fortinet	Multiple Products
CVE-2025-59719	Fortinet	FortiGate

Actively exploited vulnerabilities highlight a surge in attacks against network edge devices, management platforms, and update mechanisms, enabling initial access, privilege escalation, or remote code execution. Firewalls (FortiGate, WatchGuard, SonicWall), infrastructure managers (HPE OneView, Cisco), and trusted update or database components (ASUS Live Update, MongoDB) are key targets, increasing blast radius and lateral movement risk. Defenders should urgently patch, restrict management interfaces, rotate credentials, monitor for exploitation indicators, and segment critical systems to limit impact.

TRENDING MALWARE

Cellik
Android remote-access trojan that gives attackers near-complete control of infected devices.

GachiLoader
A newly discovered Node.js-baed malware that specializes in evading security tools.

MacSync
A MacOS infostealer that disguises itself as a legitimate, code-signed, application.

RondoDox
A stealthy botnet that compromises internet-facing routers, DVRs and CCTV systems

SantaStealer
A Windows-based infostealer that recently surfaced on Russian-language hacking forums.

ToneShell
A next-generation, stealthy backdoor used by Mustang Panda

TRENDING ADVERSARIES

Evasive Panda

LongNosedGoblin

Mustang Panda

NoName057(16)

TA2723

UNK_AcademicFlare

Threat groups like Evasive Panda, LongNosedGoblin, Mustang Panda, NoName057(16), TA2723, and AcademicFlare are showing a clear shift toward stealthier, long term intrusions using DNS manipulation, AitM attacks, and EDR evasion. Many abuse trusted channels such as software updates and academic lures. Their mix of espionage and disruption is increasingly sophisticated. Defenders should harden identity controls, use behavior based detection, secure DNS, retain logs, and prepare for DDoS style attacks.

PRODUCED & DISTRIBUTED BY
PHISH TANK DIGITAL

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

SUMMARIES & BIOS
GEOFF REHMET
Cybersecurity Expert