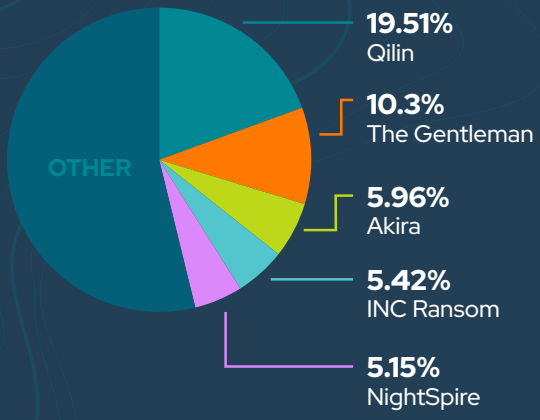
BYER-NICHOLS THREAT BRIEF

SECOND HALF FEBRUARY 2026

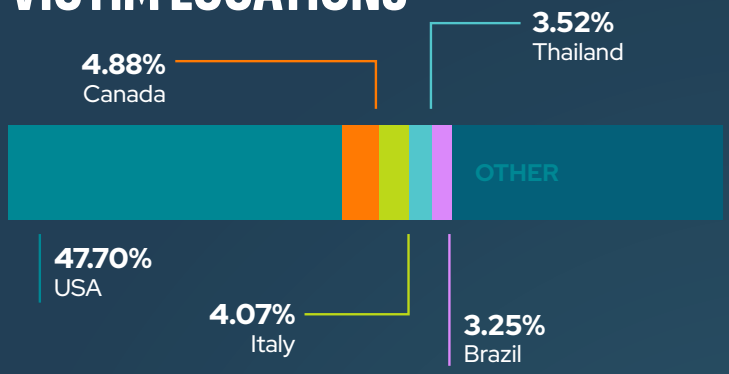
Ransomware activity remained fragmented, led by Qilin, with technology and retail topping targeted sectors. Large enterprise victims increased to 16 this period, though activity was spread across multiple operators. Meanwhile, established actors resurfaced, CISA KEV added 11 actively exploited vulnerabilities, and threat activity continues to reflect overlap between financially motivated and state-aligned operations.

TOP RANSOMWARE



Ransomware activity this period was led by Qilin (19.51%), maintaining its dominant position. The Gentlemen (10.3%)held steady in the top tier, while Akira (5.96%) remained consistently active. INC Ransom (5.42%) and NightSpire (5.15%) both climbed from prior periods, signaling sustained operational momentum among mid-tier actors. Overall activity reflects continued fragmentation, with no single cartel monopolizing operations, and multiple groups maintaining steady victim volumes across sectors.

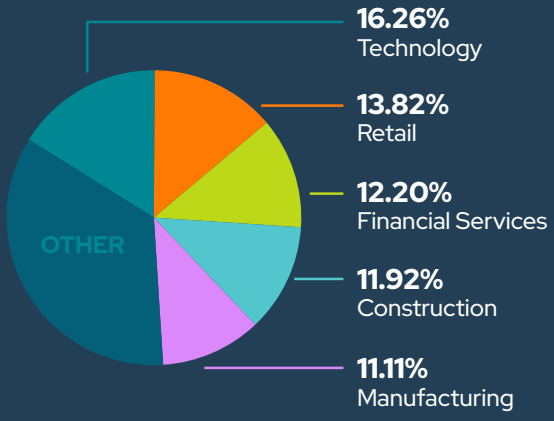
VICTIM LOCATIONS



TOP NEWS

- Infostealer malware found stealing OpenClaw secrets for first time
- $4.8M in crypto stolen after Korean tax agency exposes wallet seed
- AI platforms can be abused for stealthy malware communication
- APT37 hackers use new malware to breach air-gapped networks
- Chinese cyberspies breached dozens of telecom firms, govt agencies
- Microsoft says bug causes Copilot to summarize confidential emails
- Poland arrests suspect linked to Phobos ransomware operation
- Ransomware payment rate drops to record low as attacks surge

VICTIM SECTOR



VICTIM ORG SIZE

TRENDING & ACTIVELY EXPLOITED VULNERABILITIES

CVE	Vendor	Product
CVE-2020-7796	Synacor	Zimbra Collaboration Suite
CVE-2021-22175	GitLab	GitLab
CVE-2022-20775	Cisco	SD-WAN
CVE-2024-7694	TeamT5	ThreatSonar Anti-Ransomware
CVE-2025-49113	Roundcube	Webmail
CVE-2025-68461	Roundcube	Webmail
CVE-2026-20127	Cisco	Catalyst SD-WAN Controller and Manager
CVE-2026-22769	Dell	RecoverPoint for Virtual Machines (RP4VMs)
CVE-2026-2441	Google	Chromium
CVE-2026-25108	Soliton Systems K.K	FileZen

Recent activity highlights exploitation across collaboration platforms, SD-WAN infrastructure, webmail systems, virtualization recovery platforms, browsers, and file management software.

TRENDING MALWARE

Keenadu
Emerging malware observed in targeted intrusion activity, likely used for persistence and post-exploitation within compromised environments.

HONESTCUE
Loader-style malware used to establish initial footholds and deliver secondary payloads during targeted campaigns.

Massiv
Backdoor malware associated with remote command execution and data exfiltration in enterprise networks.

Predator
Commercial-grade spyware known for stealthy surveillance capabilities, including device monitoring and data collection.

PromptSpy
Malware leveraging AI-related lures or tooling themes to evade detection and conduct information theft.

RESURGE
Post-exploitation malware focused on maintaining access and enabling lateral movement after initial compromise.

TRENDING ADVERSARIES

APT37
Lazarus
ShinyHunters
UNC2814
UNC3886
UNC6201

Recent reporting highlights renewed activity from established actors including APT37 and Lazarus, alongside data-theft-focused ShinyHunters and multiple UNC-tracked clusters. Activity spans espionage, cryptocurrency theft, and enterprise network intrusions, often leveraging phishing, credential abuse, and vulnerability exploitation. The resurgence of these groups reinforces continued overlap between financially motivated operations and state-aligned threat activity.

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