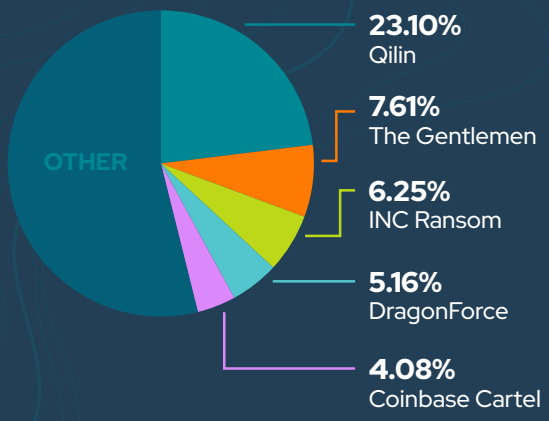
BYER-NICHOLS THREAT BRIEF

SECOND HALF APRIL 2026

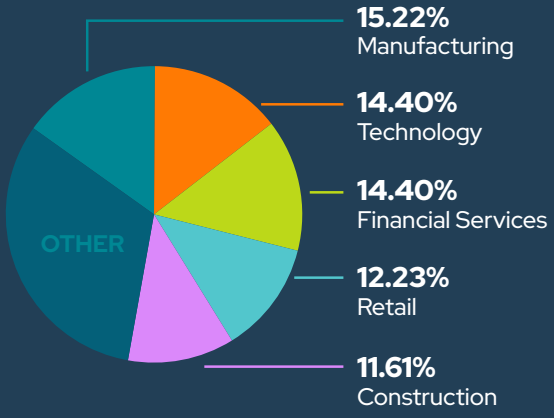
Qilin leads ransomware activity at 23.10%, followed by The Gentlemen (7.61%) and INC Ransom (6.25%). Manufacturing (15.22%) is the most targeted sector, with technology and financial services close behind (14.40% each). The United States accounts for 42.93% of victims, far exceeding other countries. Small businesses represent the majority of victims at 71.12% (+6.97%), while mid-market (20.16%) and large enterprises (8.72%) both declined.

TOP RANSOMWARE

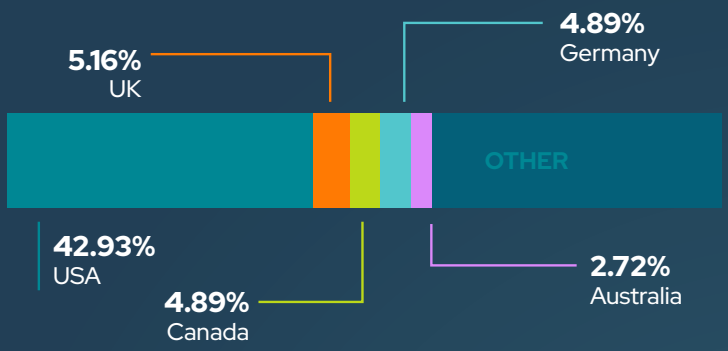


Ransomware activity is led by Qilin (23.10%), significantly outpacing other groups. The Gentlemen and INC Ransom follow at much lower shares, while DragonForce shows fluctuation from prior rankings and Coinbase Cartel appears further down the list. Overall, activity is spread across several groups, with one clear leader and a competitive mid-tier.

VICTIM SECTOR



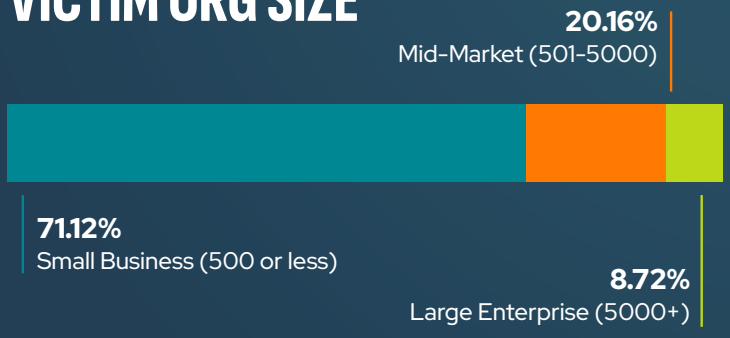
VICTIM LOCATIONS



TOP NEWS

- Alleged Silk Typhoon hacker extradited to US for cyberespionage
- Americans lost over $2.1 billion to social media scams in 2025, per U.S. Federal Trade Commission
- China's Apple App Store infiltrated by crypto-stealing wallet apps
- Feuding Ransomware Groups 0APT and KryBit Leak Each Other's Data
- New npm supply-chain attack self-spreads to steal auth tokens
- North Korea's Lazarus suspected of stealing US$290 million in KelpDAO cyberattack
- Ransomware negotiator pleads guilty to BlackCat scheme, Scattered Spider hacker pleads guilty to crypto theft charges
- Supply chain attacks hit Checkmarx and Bitwarden developer tools

VICTIM ORG SIZE



TRENDING & ACTIVELY EXPLOITED VULNERABILITIES

CVE	Vendor	Product
CVE-2025-29635	D-Link	DIR-823X
CVE-2025-32975	Quest	KACE Systems Management Appliance (SMA)
CVE-2025-48700	Synacor	Zimbra Collaboration Suite (ZCS)
CVE-2026-20122	Cisco	Catalyst SD-WAN Manger
CVE-2026-20128	Cisco	Catalyst SD-WAN Manager
CVE-2026-20133	Cisco	Catalyst SD-WAN Manager
CVE-2026-32202	Microsoft	Windows
CVE-2026-33825	Microsoft	Defender
CVE-2026-34197	Apache	ActiveMQ
CVE-2026-41940	WebPros	cPanel & WHM and WP2 (WordPress Squared)

Exploitation is concentrated on widely used enterprise systems, especially Cisco SD-WAN and Microsoft products, along with platforms like Zimbra, ActiveMQ, and cPanel, highlighting risk across core infrastructure and web services.

TRENDING MALWARE

AgingFly
Lightweight backdoor used for stealthy persistence and data exfiltration.

FIRESTARTER
Loader malware designed to deploy additional payloads and enable lateral movement.

GoGra
Information stealer targeting credentials, browser data, and system details.

Lotus Wiper
Destructive malware focused on wiping files and disrupting systems.

Ngate
Network-focused malware used for remote access and command execution.

Snow
Modular malware capable of adapting payloads for espionage or financial theft.

TRENDING ADVERSARIES

BlackFile
BlueNoroff
GopherWhisper
Sapphire Sleet
TGR-STA-1030
UNC6692

This period highlights a mix of financially motivated and state-linked threat actors, including groups like BlackFile and UNC6692 alongside more established operators such as BlueNoroff and Sapphire Sleet. Their presence reflects continued activity across both cybercrime and espionage campaigns, with an emphasis on data theft, financial targeting, and advanced intrusion techniques.

phish tank DIGITAL

PRODUCED & DISTRIBUTED BY
PHISH TANK DIGITAL

WRITTEN BY
JEREMY NICHOLS
Director, Security Programs & Strategy at SecureSky

SUMMARIES & BIOS
GEOFF REHMET
Cybersecurity Expert