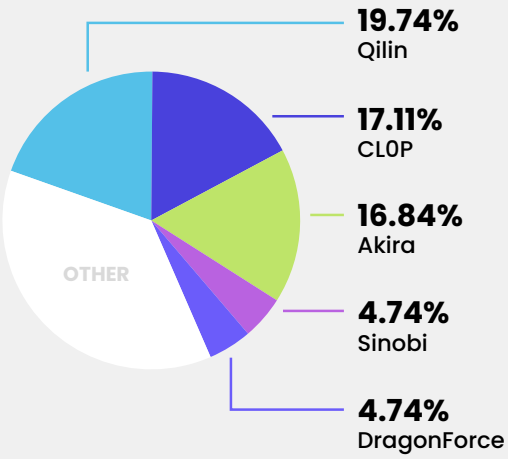
BYER-NICHOLS THREAT BRIEF

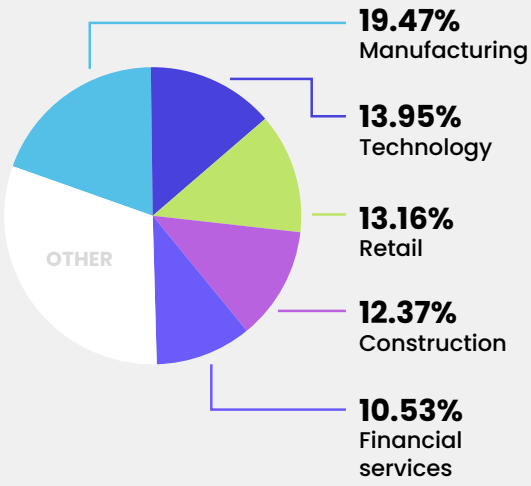
SECOND HALF NOVEMBER 2025

Qilin leads ransomware activity this period, with CL0P and Akira close behind. Newer and mid-tier groups like Sinobi and DragonForce show rising impact. Victims are primarily small US-based businesses, with manufacturing, technology, retail, and construction most affected.

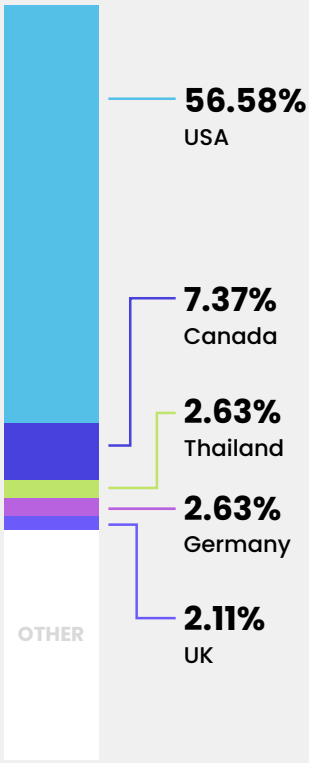
Top ransomware



Victim sector

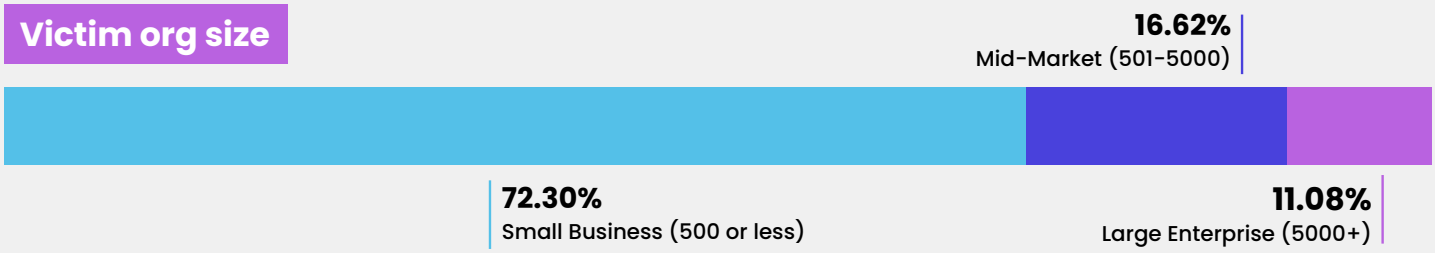


Victim locations



Qilin leads activity, with CL0P and Akira remaining major threats. Manufacturing, tech, retail, and construction top victim sectors, with small US-based businesses hit hardest. Canada rises in activity; Thailand and Germany appear as new hotspots.

Victim org size



Top news

- Azure hit by 15 Tbps DDoS attack using 500,000 IP addresses
- California man admits to laundering crypto stolen in $230M heist
- Cloudflare hit by outage affecting global network services, points to database issue
- Code beautifiers expose credentials from financial, government and technology organizations
- Crypto mixer founders sent to prison for laundering over $237 million
- Cybercriminals stole $262M by impersonating bank support teams
- New WrtHug campaign hijacks thousands of end-of-life ASUS routers
- Russian bulletproof hosting provider sanctioned over ransomware ties

Trending & actively exploited vulnerabilities

CVE	VENDOR	PRODUCT
CVE-2021-26829	OpenPLC	ScadaBR
CVE-2025-13223	Google	Chromium V8
CVE-2025-40601	SonicWall	SonicOS SSLVPN
CVE-2025-50165	Microsoft	Windows Graphics Component
CVE-2025-58034	Fortinet	FortiWeb

CVE	VENDOR	PRODUCT
CVE-2025-61757	Oracle	Fusion Middleware
CVE-2025-64459	Django Project	Django
CVE-2025-64755	Anthropic	Code AI
CVE-2025-8088	RARLAB	WinRar
CVE-2025-9501	BoldGrid	W3 Total Cache WordPress plugin

Trending malware

Amatera Stealer
Trending due to increased telemetry, with growing interest in its data-theft capabilities.

BadAudio
Emerging malware showing increased activity, likely tied to multimedia-focused attack vectors.

RondoDox
Active enough this period to warrant enhanced detection and threat-hunting focus.

RONINGLOADER
Loader family trending due to its use in staging additional payloads. Making its early detection an opportunity to break the kill chain before more damaging malware is deployed.

ShadowV2
Second-generation variant gaining traction, emphasizing the importance of updating signatures and behavior based detections to account for its evolution.

Sturnus
Rapidly spreading through phishing and loader ecosystems, showing increased momentum.

This period's trending adversaries span both state-aligned and criminal groups. Their activity reflects a mix of espionage, disruption, and financially motivated intrusions, highlighting how these actors rapidly shift between intelligence gathering and monetization.

Trending adversaries

APT24
Autumn Dragon
Bloody Wolf
Dragon Breath
PlushDaemon
TridentLocker

Trending adversaries blend state-aligned and criminal operations, spanning espionage, sabotage, and financial intrusion. Groups active this period show growing geopolitical alignment and disruptive capability, reinforcing the need to track how quickly these actors pivot between intelligence collection and monetization.

BYER CO

WRITTEN BY JEREMY NICHOLS, FORMER DIRECTOR OF THE GLOBAL THREAT INTELLIGENCE CENTER

EXECUTIVE SUMMARIES & ADVERSARY BIO'S BY GEOFF REHMET, CYBERSECURITY EXPERT

PRODUCED & DISTRIBUTED BY BYER CO'S CYBERSECURITY MARKETING DIVISION