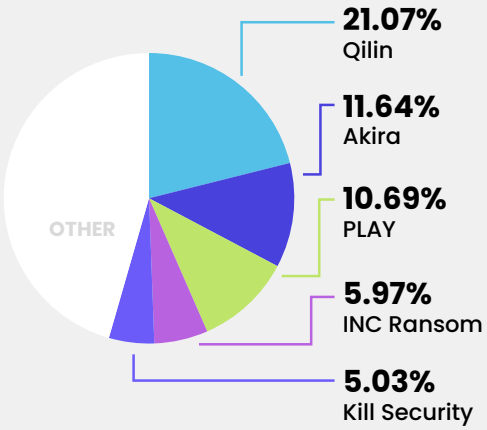
BYER-NICHOLS THREAT BRIEF

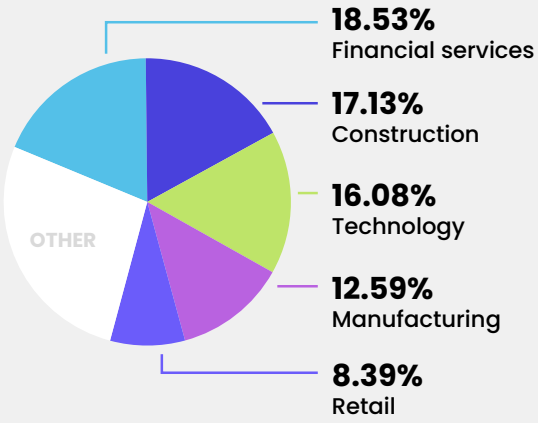
SECOND HALF SEPTEMBER 2025

Of concern in this period is a rise in attacks against Cisco ASA and IOS XE devices, highlighting the exposure of critical network infrastructure. On the malware side, Brickstorm and MetaStealer are showing increased activity, with several lightweight loaders tied to state-backed groups also in play. In terms of victims, the United States continues to dominate, though South Korea has emerged among the top five impacted countries due to a big Qilin dump.

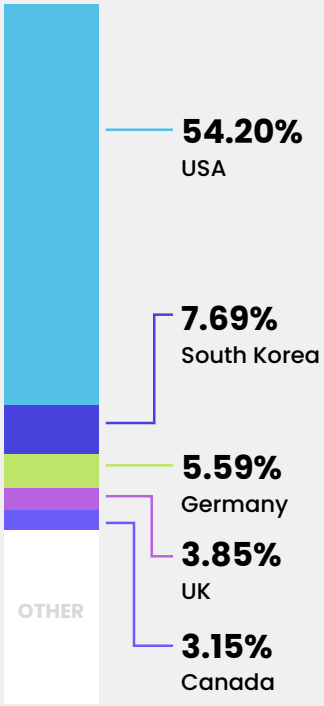
Top ransomware



Victim sector

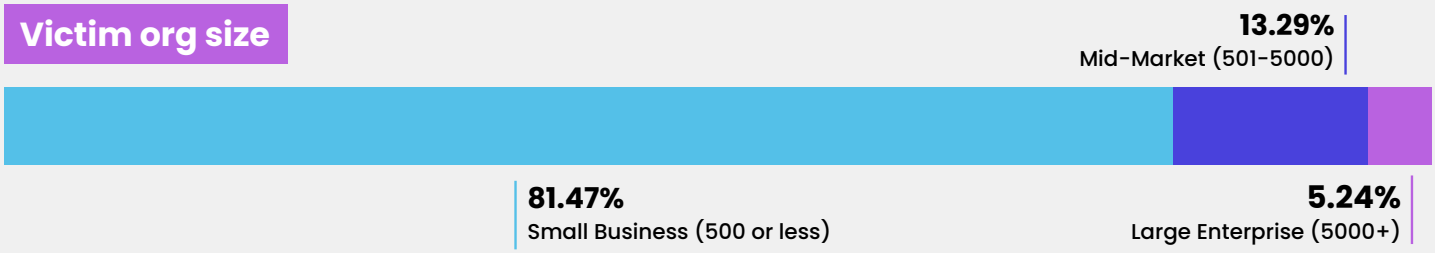


Victim locations



Qilin leads activity this period with 21% of observed incidents, maintaining the top spot. Akira (11.6%) continues its upward climb, moving from 4th to 2nd place. PLAY ransomware surged into the top 3, climbing from 12th place two periods ago. INC Ransom (6%) and Kill Security (5%) round out the top 5, with Kill Security making the most notable leap (27th > 7th > 5th).

Victim org size



Trending adversaries

ArcaneDoor
Espionage campaign exploiting Cisco devices.

Nimbus Manticore
Iran-linked APT using custom malware.

Phantom Taurus
China-based espionage group targeting government and telecommunications.

Scattered Spider
Social engineering crew turned ransomware. Still active despite arrests.

Storm-1516
Russian influence/disinformation operation.

UNC5174
China-linked stealth actor targeting VMWare zero day.

Trending & actively exploited vulnerabilities

CVE	VENDOR	PRODUCT
CVE-2021-21311	Adminer	Adminer
CVE-2025-10035	Fortra	GoAnywhere MFT
CVE-2025-10585	Google	Chromium V8
CVE-2025-20333	Cisco	Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense
CVE-2025-20352	Cisco	IOS and IOS XE
CVE-2025-20362	Cisco	Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense
CVE-2025-30247	Western Digital	My Cloud
CVE-2025-32463	Sudo	Sudo
CVE-2025-59689	Libraesva	Email Security Gateway
CVE-2025-9242	WatchGuard	Fireware OS

This period highlights critical flaws in Cisco ASA and IOS XE devices, exposing core infrastructure to takeover. Fortra's GoAnywhere MFT and Google's Chromium V8 were also actively exploited, with attackers leveraging them for data theft and browser-based attacks. A vulnerability in Western Digital My Cloud further underscores the risk to storage systems, making timely patching essential.

Trending malware

Brickstorm
MiniJunk
MetaStealer
Obscura
MiniBrowse
Shai-Hulud

Brickstorm has emerged as a disruptive malware aimed at large-scale compromise, while MetaStealer continues to grow as a Mac-focused infostealer. MiniBrowse and MiniJunk, linked to Nimbus Manticore, act as lightweight loaders for follow-on payloads. Obscura enhances evasion, and Shai-Hulud shows worm-like traits that raise concerns of self-propagation.

Top news

- Canada dismantles TradeOgre exchange, seizes $40 million in crypto
- Cloudflare mitigates new record-breaking 22.2 Tbps DDoS attack
- Google nukes 224 Android malware apps behind massive ad fraud campaign
- Police dismantles crypto fraud ring linked to €100 million in losses
- Police seizes $439 million stolen by cybercrime rings worldwide
- Self-propagating supply chain attack hits 187 npm packages
- UK arrests 'Scattered Spider' teens linked to Transport for London hack
- UK arrests suspect for RTX ransomware attack causing airport disruptions

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