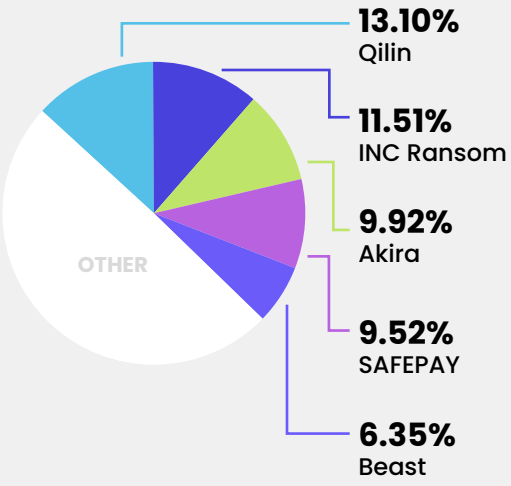
BYER-NICHOLS THREAT BRIEF

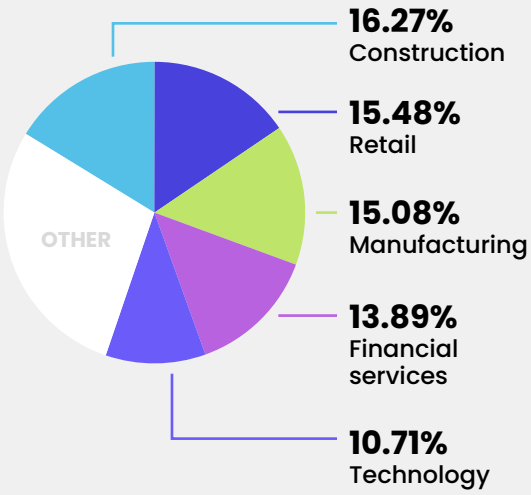
SECOND HALF JULY 2025

In this second edition of our brief we thought it would be a good idea to share a little background on how we gather the findings presented here. We track open source intelligence (OSINT) threat feeds as well as vendor bulletins and blogs. The insights gathered are cross-referenced against the CISA known exploited vulnerability catalog. The results are augmented with additional data sources such as details of ransomware leaks, bringing us to a view of significant recent activity.

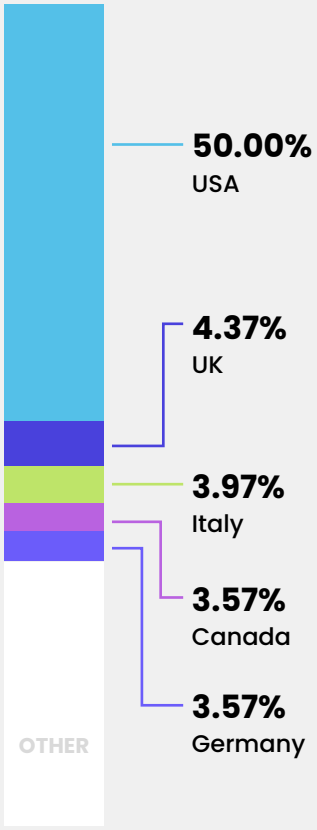
Top ransomware



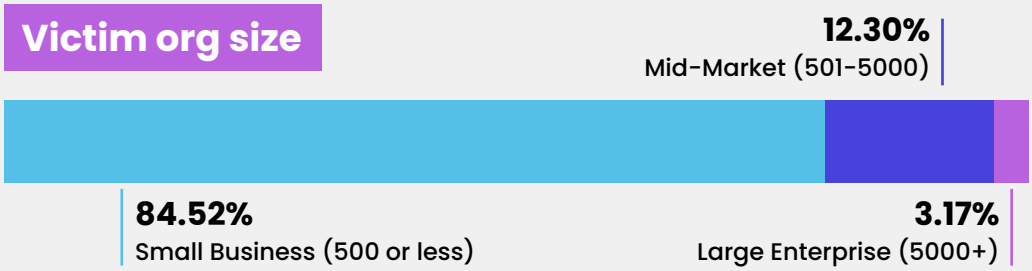
Victim sector



Victim locations



Victim org size



Trending malware

Coyote	Matanbuchus
Interlock	OVERSTEP
Koske	SafePay

Since our previous brief, Qilin and INC ransomware remain the two most dominant types of ransomware. We do however have a new entrant in the top 5, with Beast representing 6.35% of ransomware attacks. The majority of victims remain small businesses, edging up from 80.6% to 84.52%. Small businesses face a very real risk of business failure in the event of a cyber breach, underscoring the urgent need for them to implement robust security measures.

Trending adversaries

APT41
Chinese state sponsored espionage group. Last seen almost a year ago. Now targeting African governments.

Fire Ant
Stealthy cyber-espionage campaign targeting vulnerabilities in ESXi and vCenter.

NoName057(16)
Pro-Russian Hacktivist group performing DDoS attacks, mostly targeting government and public sector, particularly during Russian business hours.

Scattered Spider
After a lull in activity caused by arrests, Scattered Spider seems to have become active again. Recent campaigns appear to have focused on compromising VMWare ESXi environments. Google's Threat Intelligence Group reports that they have gained access to vCenter Server Appliances (VCSA), enabled SSH access and then installed remote access tools, including Teleport, to achieve persistence. From there they have moved to ex-filtrate Active Directory Databases and deploy ransomware directly into hypervisors. What has been striking about these attacks is the velocity at which they have acted.

ShinyHunters
It is now believed that ShinyHunters may be behind Salesforce breaches at companies like Qantas, Allianz Life, LVMH, and Adidas. There is also now suspicion that ShinyHunters may have links to Scattered Spider.

Storm-2603
Recently identified threat actor, associated with the ToolShell campaign. The group's TTPs suggest a combination of APT behavior with financially motivated ransomware deployment.

Active vulnerabilities

CVE	VENDOR	PRODUCT
CVE-2025-20281	Cisco	Identity Services Engine
CVE-2025-20337	Cisco	Identity Services Engine
CVE-2025-25257	Fortinet	FortiWeb
CVE-2025-2775	SysAid	SysAid On-Prem
CVE-2025-2776	SysAid	SysAid On-Prem
CVE-2025-49704	Microsoft	SharePoint
CVE-2025-49706	Microsoft	SharePoint
CVE-2025-53770	Microsoft	SharePoint
CVE-2025-54309	CrushFTP	CrushFTP
CVE-2025-6558	Google	Chromium

Top news

- 4 Chinese APTs attack Taiwan's semiconductor industry
- BlackSuit leak sites seized, Gunra evolves to Linux, Chaos ransomware rises but FBI seizes $2.4M from operation
- Hacker steals $27 million in BigONE exchange crypto breach
- Lumma infostealer malware returns after law enforcement disruption
- Salt Typhoon infiltrates US National Guard for a year, US nuclear weapons agency hacked in ToolShell attacks
- Spikes in malicious activity precede new CVEs in 80% of cases
- UK to ban public sector orgs from paying ransomware gangs
- US soldier pleads guilty to extorting 10 firms, US woman gets 8 years for aiding North Koreans infiltrate 300 firms

Amongst adversaries, Scattered Spider remains active, despite arrests. In a new development, it is believed that ShinyHunters may be linked to Salesforce breaches at companies including Qantas, Allianz Life, LVMH and Adidas. Critical vulnerabilities that warrant attention include multiple vulnerabilities to Microsoft SharePoint Server (CVE-2025-49704, CVE-2025-49706, CVE-2025-53770) which are being actively exploited and Cisco Identity Services Engine (CVE-2025-2081, CVE-2025-20337). Both Microsoft and Cisco have released updates which should be applied immediately to address these vulnerabilities.

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