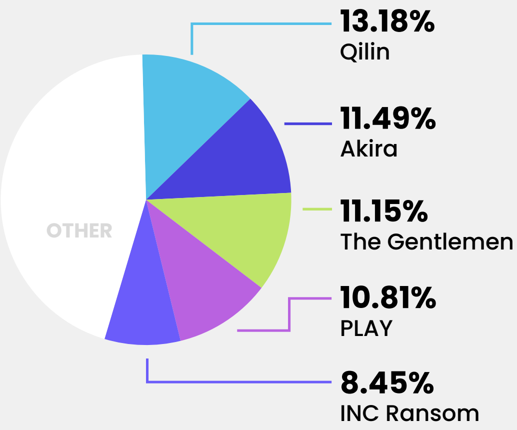
BYER-NICHOLS THREAT BRIEF

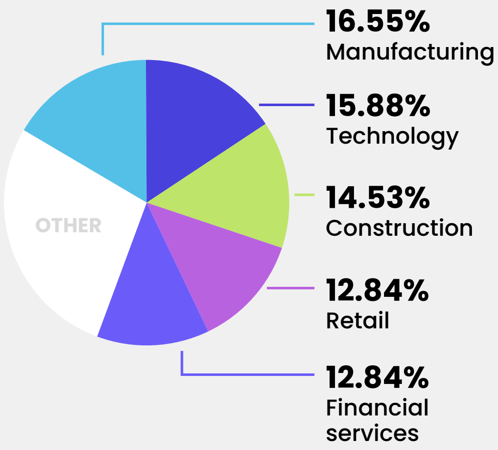
FIRST HALF SEPTEMBER 2025

Of concern in this period is an increase in attackers compromising devices from vendors including SonicWall and especially TP-Link. With many of these being consumer devices, compromises often go undetected for long periods, if they are ever noticed. On the malware side, two malware variants that target Android devices are showing notable activity. In terms of victim locations, a notable change is that two Asian countries (India and South Korea) are featuring in the top five.

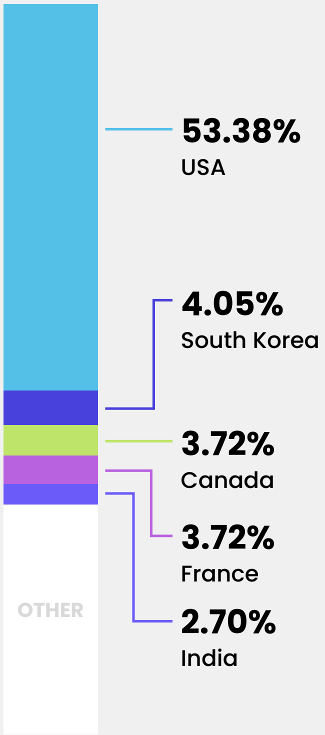
Top ransomware



Victim sector

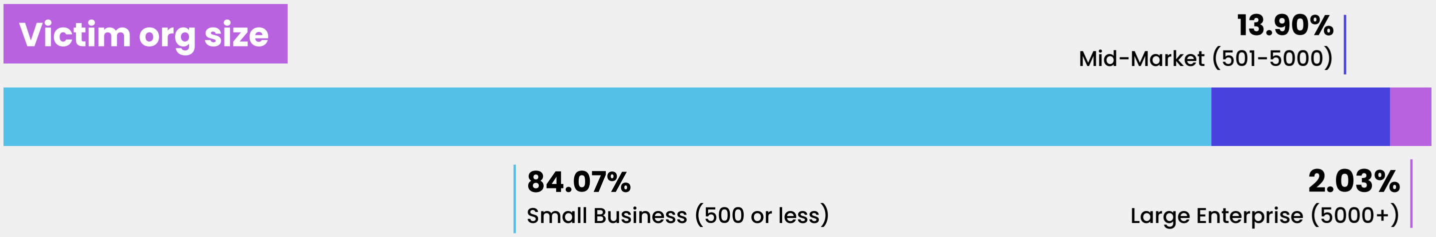


Victim locations



Once again, Qilin claims the top spot, but with a steadily decreasing percentage of attacks. Akira is the only other actor from our previous top 5 that still manages to stake a place. Three new actors, namely The Gentlemen, PLAY and INC Ransom make their way into the top 5. The Gentlemen, a previously undocumented group is notable for its use of highly tailored tools to bypass enterprise endpoint protection.

Victim org size



Trending malware

Brokewell
An infostealer that captures credentials, intercepts MFA codes and drains crypto wallets

HybridPetya
Malware that bypasses UEFI Secure Boot

EggStreme
A backdoor which enables reconnaissance, lateral movement and data theft

RatOn
An Android banking trojan

SnakeDisk
A previously unknown USB worm

StealC
An infostealer with that relies on sophisticated social engineering

Trending & actively exploited vulnerabilities

CVE	VENDOR	PRODUCT
CVE-2020-24363	TP-Link	TL-WA855RE
CVE-2023-50224	TP-Link	TL-WR841N
CVE-2024-40766	SonicWall	SonicOS
CVE-2025-38352	Linux	Kernel
CVE-2025-48543	Android	Runtime
CVE-2025-5086	Dassault Syst√®mes	DELMIA Apriso
CVE-2025-53690	Sitecore	Multiple Products
CVE-2025-55177	Meta Platforms	WhatsApp
CVE-2025-6202	SK Hynix	DDR5
CVE-2025-9377	TP-Link	Multiple Routers

In this period, we have seen significant activity relating to 3 vulnerabilities that impact TP-Link devices that have reached end of life. While TP-Link has released patches, it is advisable for owners of these devices replace them rather than continue using obsolete hardware whose firmware is not being actively maintained. Another notable vulnerability is CVE-2025-55177 which is a "zero-click" vulnerability affecting WhatsApp on iOS and MacOS and which allows processing of content from an arbitrary URL on a target's device. There is evidence that this vulnerability has been exploited in the wild.

Trending adversaries

APT29 **Mustang Panda** **WhiteCobra**

APT28 **The Gentlemen** **Yurei**

APT28 and APT29, better known as Fancy Bear and Cozy Bear are up to their tricks again. Both are Russian state-sponsored groups involved in espionage. Of particular note, APT28 has been detected using a new Microsoft Outlook backdoor called NotDoor. Not to be outdone by the Russians, the Chinese group Mustang Panda has been noted for its exploits in targeting a Philippine military company in an espionage campaign. Users of the VSCode and OpenVSX marketplaces should take note of WhiteCobra, an actor responsible for planning 24 malicious extensions.

Top news

- AI-powered malware hit 2,180 GitHub accounts in "s1ngularity" attack
- Cloudflare blocks largest recorded DDoS attack peaking at 11.5 Tbps, DDoS defender targeted in 1.5 Bpps denial-of-service attack
- Hackers breach fintech firm in attempted $130M bank heist
- Hackers hijack npm packages with 2 billion weekly downloads in supply chain attack
- Hackers steal 3,325 secrets in GhostAction GitHub supply chain attack
- Hackers use new HexStrike-AI tool to rapidly exploit n-day flaws
- US charges admin of LockerGoga, MegaCortex, Nefilim ransomware
- US offers $10 million bounty for info on Russian FSB hackers

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