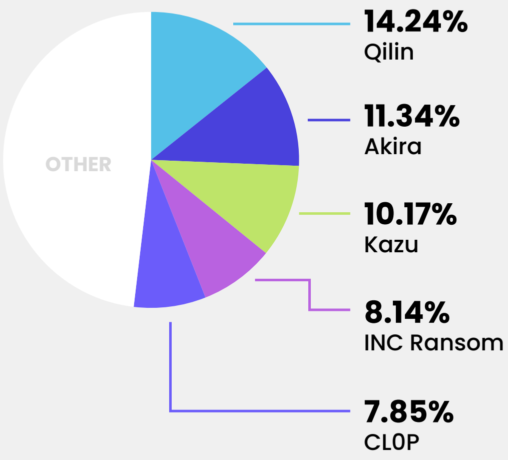
BYER–NICHOLS THREAT BRIEF

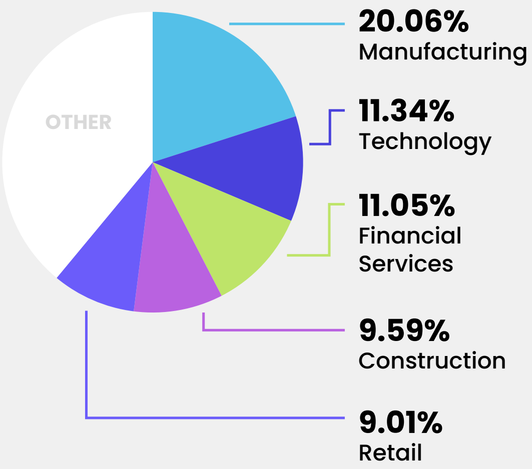
FISRT HALF NOVEMBER 2025

One of the most concerning developments over this period has been the discovery of “zero-click” vulnerabilities in Samsung mobile devices, which have already been actively exploited by the Landfall spyware. We have also seen a newcomer in the ransomware space — Kazu, which is a group focused on data theft. Meanwhile, Akira, a perennial ransomware actor is now believed to have made over $244 million from its malicious activities.

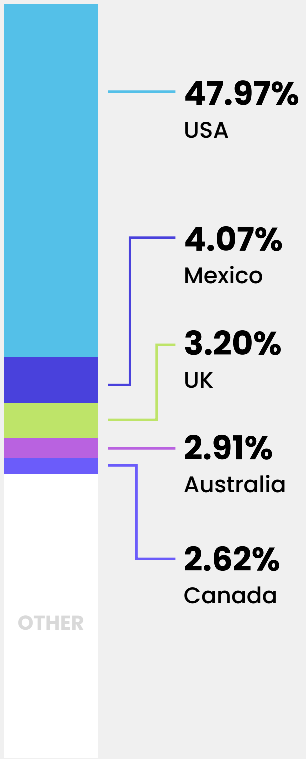
Top ransomware



Victim sector

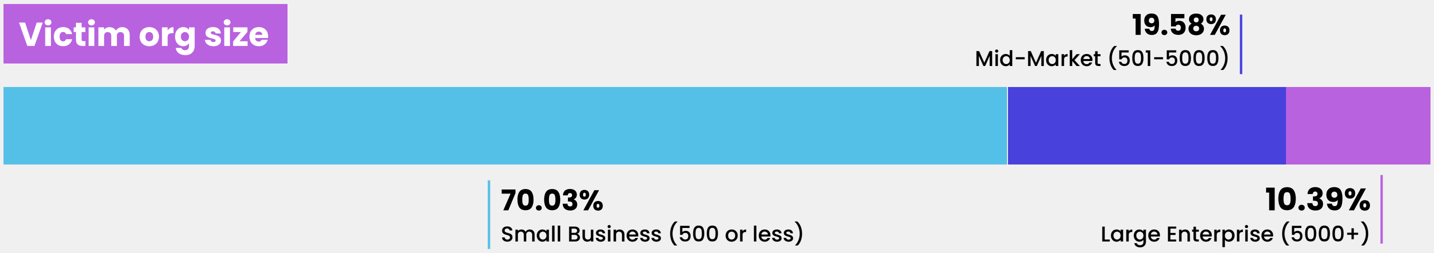


Victim locations



CL0P, who made a resurgence in the previous period remains active in the top 5. A relative newcomer is Kazu, and actor focused on data theft, which has only shown visible activity in this period. Amongst its victims are Doctor Alliance in Texas, which provides billing and management to physicians as well government agencies in Colombia. Indications are that Kazu is exploiting vulnerabilities in web applications.

Victim org size



Top news

- “Bitcoin Queen” gets 11 years in prison for $7.3 billion Bitcoin scam
- Hacker steals over $120 million from Balancer DeFi crypto protocol
- Open VSX rotates access tokens used in supply-chain malware attack
- Police arrests suspects linked to €600 million crypto fraud ring
- SonicWall says state-sponsored hackers behind security breach in September
- US announces new strike force targeting Chinese crypto scammers
- US Congressional Budget Office hit by suspected foreign cyberattack
- US sanctions North Korean bankers linked to cybercrime, IT worker fraud

Trending malware

Glassworm
Self-propagating malware that infects Visual Studio Code extensions on the Open VSX marketplace

Landfall
A previously unknown Android spyware family delivered through malicious DNG image files

Promptflux
An experimental malware strain that uses Google's Gemini chatbot to continuously rewrite its own code

PromptSteal
Malware tool that leverages Hugging Face–hosted language models to generate short Windows commands for reconnaissance and data theft

SesameOp
A novel backdoor that uses the OpenAI Assistants API as its command and control channel

SleepyDuck
A remote access trojan that infiltrates systems by posing as a legitimate Solidity extension for Visual Studio Code

Trending adversaries

APT37

Sandworm

UAC-0099

Curly COMrades

Tick

A common trend through the trending adversaries we are seeing in this period is nation state alignment of sponsorship for purposes of sabotage or espionage. Some groups are being particularly meticulous in establishing stealthy persistent access, such as the Russian-aligned Curly COMrades who are using Hyper-V to run Linux VMs on victim machines as a method of avoiding detection by EDR tools.

Trending & actively exploited vulnerabilities

Active vulnerabilities during this period predominantly reflect flaws which allow unauthenticated Remote Code Execution (RCE) or privilege escalation, leading to full system compromise. The targets are diverse, including enterprise software (Gladinet file sharing), the Windows kernel and the network perimeter (Watchguard firewalls). A particularly concerning vulnerability is CVE-2025-21042, a "zero-click" exploit affecting Samsung mobile devices, and which is being actively exploited by the Landfall spyware.

CVE	VENDOR	PRODUCT
CVE-2025-12480	Gladinet	Triofox
CVE-2025-62215	Microsoft	Windows
CVE-2025-9242	WatchGuard	Firebox
CVE-2025-21042	Samsung	Mobile Devices
CVE-2025-48703	CWP	Control Web Panel
CVE-2025-11371	Gladinet	CentreStack and Triofox
CVE-2025-61932	Motex	Lanscope Endpoint Manager
CVE-2025-64446	Fortinet	Fortiweb
CVE-2025-59367	ASUS	DSL Series Routers
CVE-2025-20354	Cisco	Unified Contact Center Express

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