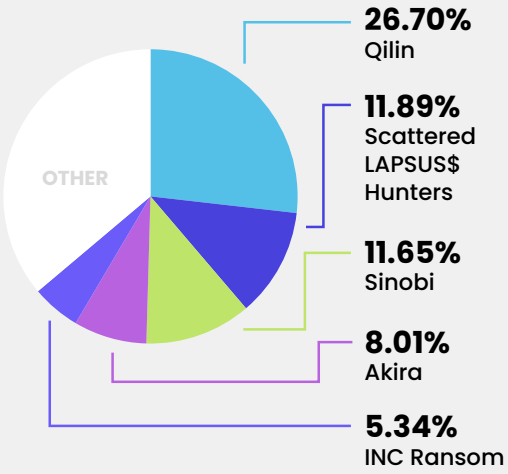
# BYER-NICHOLS THREAT BRIEF

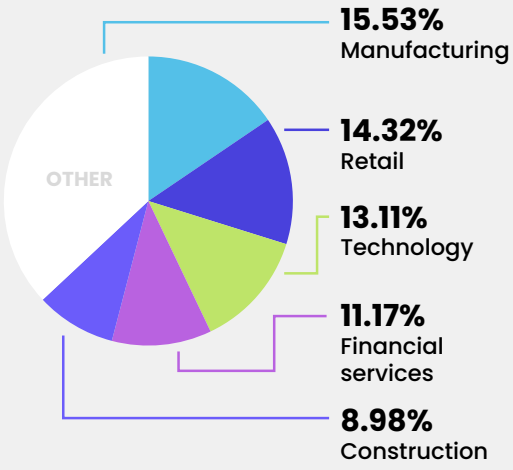
## FIRST HALF OCTOBER 2025

The emergence of the Scattered LAPSUS$ Hunters "Trinity of Chaos" has made headlines in recent weeks with their daring extortion attempts of large enterprises whose data they had stolen from SalesForce instances. On the malware front, four of the top six trending variants target Android devices. In terms of victim locations, France and Spain make new appearances in the top 5, with the countries in the top 5 outside North America all being in Western Europe.

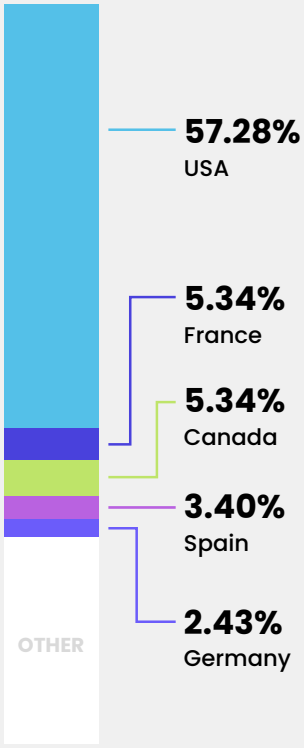
## Top ransomware




## Victim sector

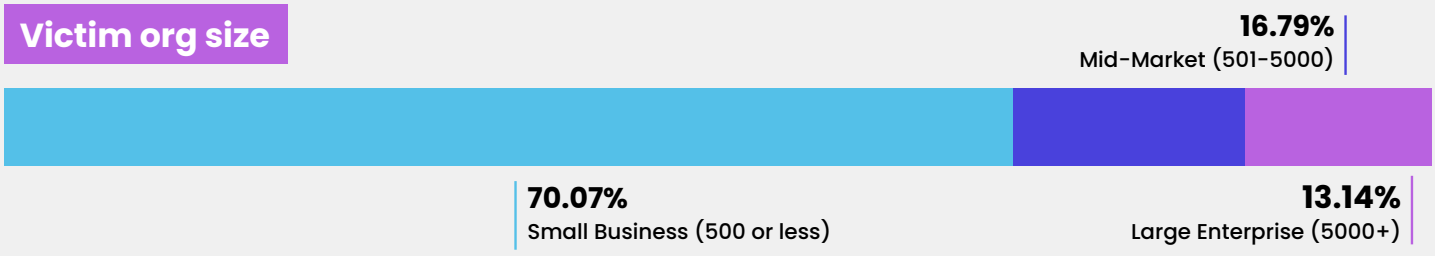



## Victim locations




While Qilin continues to be the most prevalent ransomware actor, the Scattered LAPSUS$ Hunters "trinity of chaos" has jumped into second spot with an associated flurry of media attention as a result of their high-profile extortion activity. Tied to the their attention-grabbing heists has been a noticeable uptick in the proportion of large bump the proportion of large enterprises falling victim to breaches. After a lull of about a month, we are also seeing Sinobi back in the top 5.

## Victim org size




## Trending malware

**ClayRat**
A rapidly evolving spyware campaign targeting Russian users.

**Klopatra**
An Android banking trojan.

**ProSpy**
Android malware impersonating Signal and ToTok.

**PureRat**
Phishing campaign suspected to be of Vietnamese origin.

**RondoDox**
Botnet campaign targeting DVRs, routers and CCTV systems.

**ToSpy**
Android malware suspected to originate in the UAE.

## Trending & actively exploited vulnerabilities

| CVE | VENDOR | PRODUCT |
|---|---|---|
| CVE-2025-10035 | Forta | GoAnywhere MFT |
| CVE-2025-21043 | Samsung | Mobile Devices |
| CVE-2025-24990 | Microsoft | Windows |
| CVE-2025-27915 | Synacor | Zimbra Collaboration Suite (ZCS) |
| CVE-2025-4008 | Smartbedded | Meteobridge |
| CVE-2025-47827 | IGEL | IGEL OS |
| CVE-2025-54253 | Adobe | Experience Manager (AEM) Forms |
| CVE-2025-59230 | Microsoft | Windows |
| CVE-2025-61882 | Oracle | E-Business Suite |
| CVE-2025-6264 | Rapid7 | Velociraptor |

Recent trending vulnerabilities span major vendors—Microsoft, Adobe, Oracle, Samsung, and others—impacting critical enterprise platforms, mobile devices, and collaboration tools. Exploitation could enable data theft, remote code execution, or service disruption. Security managers should prioritize rapid patching, monitor for exploitation indicators, and reinforce endpoint and application hardening across both infrastructure and user-facing systems. Arguably the greatest immediate risk exists in CVE-2025-54253 (Adobe AEM Forms) as it allows remote code execution without user interaction, and has a public proof-of-concept exploit.

## Trending adversaries

**Crimson Collective**
**Flax Typhoon**
**Storm-1175**
**Storm-2603**
**Storm-2657**
**TwoNet**

Turning to trending adversaries, Crimson Collective targets tech firms and cloud environments for data theft and extortion. Flax Typhoon, a state-sponsored group, spies on Taiwanese organizations using legitimate software. Storm-1175 and 2603 deploy ransomware via GoAnywhere and SharePoint exploits, while Storm-2657 is responsible for hijacking US university payrolls. Pro-Russian TwoNet disrupts critical infrastructure. The most concerning of these is probably Flax Typhoon, due to its state backing and critical targets.

## Top news

- Adobe Analytics bug leaked customer tracking data to other tenants
- Clop exploited Oracle zero-day for data theft since early August
- HackerOne paid $81 million in bug bounties over the past year, Zeroday Cloud hacking contest offers $4.5 million in bounties, Apple now offers $2 million for zero-click RCE vulnerabilities
- Hackers claim Discord breach exposed data of 5.5 million users
- LinkedIn sues ProAPIs for using 1M fake accounts to scrape user data
- North Korean hackers stole over $2 billion in crypto this year, US seizes $15 billion in crypto from 'pig butchering' kingpin
- Red Hat confirms security incident after hackers claim GitHub breach
- SonicWall firewall configs stolen for all cloud backup customers


# 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**