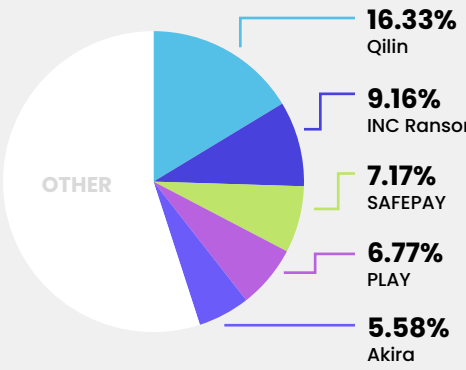
CYBERSECURITY DATA FOR JULY 01-15, 2025
DELIVERED TWICE A MONTH

BYER-NICHOLS THREAT BRIEF

Top ransomware

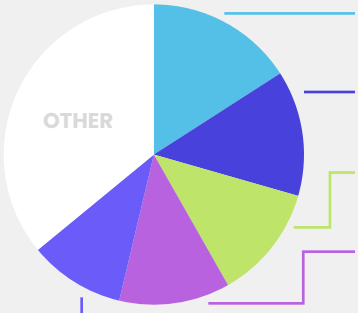


16.33% Qilin
9.16% INC Ransom
7.17% SAFEPAY
6.77% PLAY
5.58% Akira

Victim locations

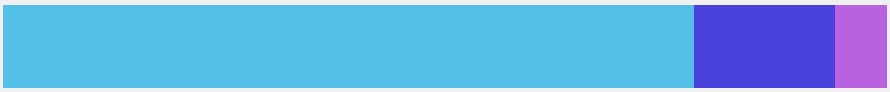
49.00% USA
7.57% Canada
5.18% Italy
3.98% UK
3.98% Germany

Victim sector



15.94% Manufacturing
13.55% Technology
12.35% Construction
11.95% Financial services
10.36% Retail

Victim org size



12.90% Mid-Market (501-5000)
80.65% Small Business (500 or less)
6.45% Large Enterprise (5000+)

Trending & actively exploited vulnerabilities

CVE	VENDOR	PRODUCT
CVE-2014-3931	Looking Glass	Multi-Router Looking Glass (MRLG)
CVE-2016-10033	PHP	PHPMailer
CVE-2019-5418	Rails	Ruby on Rails
CVE-2019-9621	Synacor	Zimbra Collaboration Suite (ZCS)
CVE-2025-47812	Wing FTP Server	Wing FTP Server

CVE	VENDOR	PRODUCT
CVE-2025-48927	TeleMessage	TM SGNL
CVE-2025-48928	TeleMessage	TM SGNL
CVE-2025-49719	Microsoft	SQL Server
CVE-2025-5777	Citrix	NetScaler ADC and Gateway
CVE-2025-6554	Google	Chromium V8

The first half of July 2025 saw significant cyber threats, with **Qilin ransomware** dominating attacks (16.3%), primarily targeting **small businesses (80.6%)** in the **manufacturing (15.9%) and technology (13.5%) sectors,** especially in the **U.S. (49%)**. Trending adversaries like **Gamaredon** and **Scattered Spider** were active, while critical vulnerabilities—including **CVE-2025-47812 (Wing FTP Server)** and **CVE-2025-6554 (Chromium V8)**—were widely exploited. High-profile incidents included a **North Korean IT worker scheme disruption, browser-based zero-day attacks**, and a **€10M investment fraud takedown**. Malware trends highlighted **Anatsa** and **GhOstRAT**, underscoring persistent risks to enterprises and individuals alike.

Top news

- Chrome Zero-Day, 'FoxyWallet' Firefox attacks threaten browsers
- US Department of Justice disrupts North Korean IT worker scheme across multiple US states
- Hunters International ransomware shuts down after World Leaks rebrand
- Police dismantles investment fraud ring stealing €10 million
- Chrome Store features extension poisoned with sophisticated Spyware
- Employee gets $920 for credentials used in $140 million bank heist
- North American APT uses Exchange Zero-Day to attack China

Trending malware

Anatsa
Atomic (AMOS)
Batavia
GhOstRAT
Interlock
NimDoor

Trending adversaries

Gamaredon
Scattered Spider
Silk Typhoon
TAG-140
UNC5174
Void Arachne

BYER CO

WRITTEN BY JEREMY NICHOLS, FORMER DIRECTOR OF THE GLOBAL THREAT INTELLIGENCE CENTER

PRODUCED & DISTRIBUTED BY BYER CO'S CYBERSECURITY MARKETING DIVISION