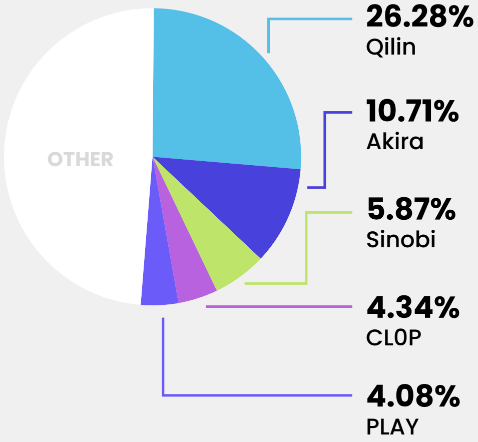
BYER-NICHOLS THREAT BRIEF

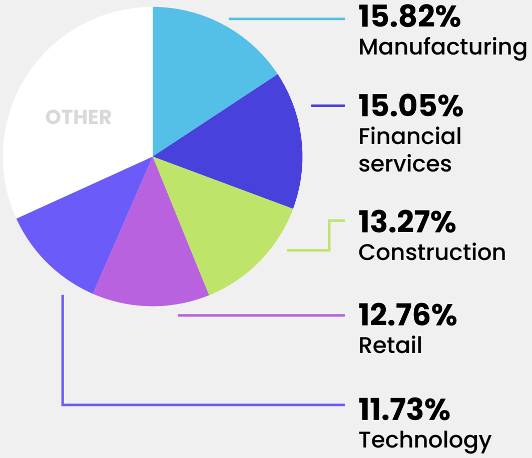
SECOND HALF OCTOBER 2025

The recent theft of source code from F5 has seen over a quarter of a million F5 BIG-IP instances exposed to potential remote attacks via the Internet. Regardless of the theft of F5's source code, this incident underscores the point that management interfaces of network infrastructure devices should not be left exposed to access via the Internet.

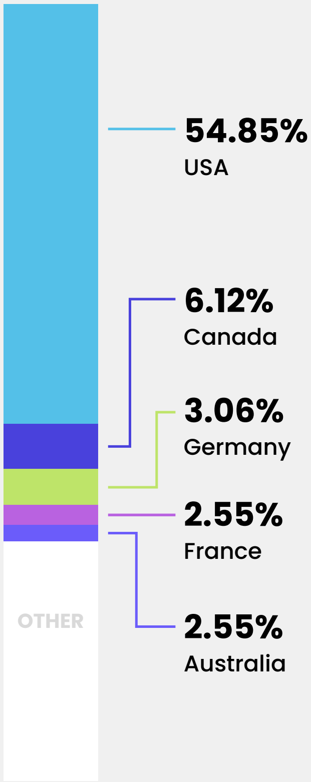
Top ransomware



Victim sector

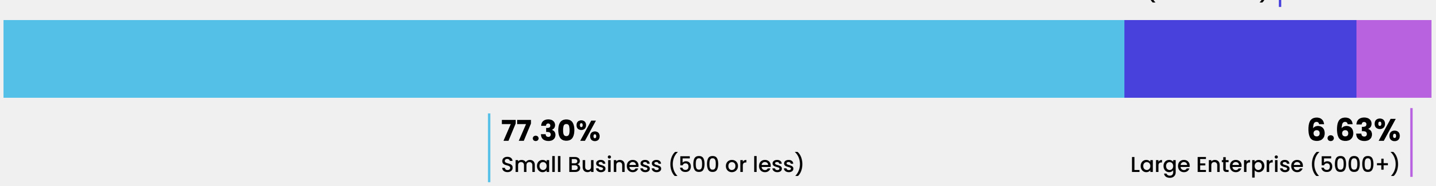


Victim locations



After only posting 5 victims since May, and none since early July, Clop has made a dramatic entry back onto the ransomware scene with 18 victims in roughly 3 weeks. Clop is noted for its use of multi-level extortion techniques, and is believed to have extorted over $500 million in ransom payments. Clop has used large-scale phishing campaigns and tends now to focus on pure extortion with "encryption-less ransomware" – an increasingly common trend amongst ransomware actors as more potential victims defend against crypto-ransomware with well-tested backups.

Victim org size



Trending malware

CLEARSHOT
A multi-stage malware loader

GlassWorm
Worm that spreads through VS Code extensions

Odyssey Stealer
MacOS Infostealer, signed with a valid Apple Developer ID

RADTHIEF
Infostealer that abuses blockchain smart contracts

Trending & actively exploited vulnerabilities

CVE	VENDOR	PRODUCT
CVE-2022-48503	Apple	Multiple Products
CVE-2025-24893	XWiki	Platform
CVE-2025-2746	Kentico	Xperience CMS
CVE-2025-2747	Kentico	Xperience CMS
CVE-2025-33073	Microsoft	Windows

CVE	VENDOR	PRODUCT
CVE-2025-41244	Broadcom	VMware Aria Operations and VMware Tools
CVE-2025-54236	Adobe	Commerce and Magento
CVE-2025-54253	Adobe	Experience Manager (AEM) Forms
CVE-2025-59287	Microsoft	Windows
CVE-2025-61884	Oracle	E-Business Suite

While we are seeing a high number of actively exploited vulnerabilities in this period, one that particularly warrants attention is CVE-2025-59287. The severity of this vulnerability in the Windows Server Update Service (WSUS) has resulted in Microsoft issuing an out-of-band update to address it. The concerning issue about this vulnerability is that it allows an unauthenticated actor to achieve remote code execution with system privileges. Organisations using affected products should act immediately.

Trending adversaries

- **APT27**
- **APT31**
- **MuddyWater**
- **Star Blizzard**
- **Tick**
- **UNC5142**

Amongst trending adversaries, UNC5142, a financially motivated threat actor, is particularly notable for its use of techniques that abuse blockchain to achieve greater resiliency and make take-downs more difficult. Another concerning actor is Star Blizzard, which as Russian intelligence links, and is involved in spear-phishing Western think tanks and defense firms for espionage purposes.

Top news

- 266,000+ F5 BIG-IP instances exposed to remote attacks, 75,000+ WatchGuard security devices vulnerable to critical RCE
- Prosper data breach impacts 17.6 million accounts
- Europol dismantles SIM box operation renting numbers for cybercrime
- Experian fined $3.2 million for mass-collecting personal data
- AWS outage crashes Amazon, PrimeVideo, Fortnite, Perplexity and more
- Hackers exploit 34 zero-days on first day of Pwn2Own Ireland, 56 on day two
- Cursor, Windsurf IDEs riddled with 94+ n-day Chromium vulnerabilities
- LinkedIn phishing targets finance execs with fake board invites

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