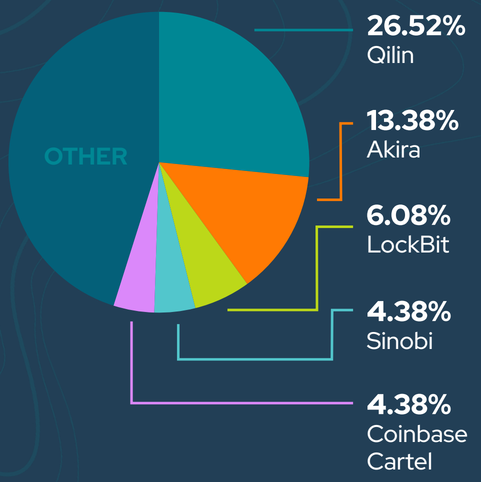
BYER-NICHOLS THREAT BRIEF

FIRST HALF DECEMBER 2025

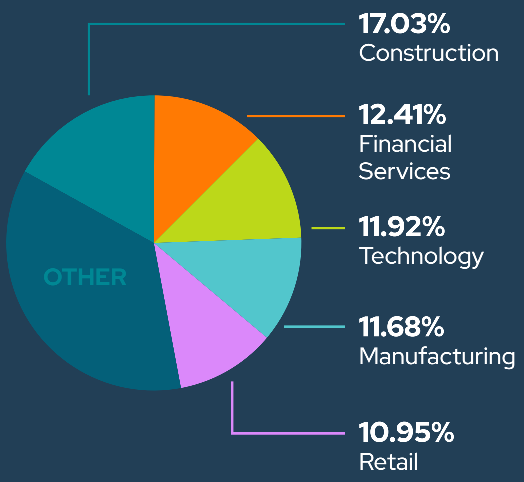
LockBit resurfaced and immediately re-entered the top 5, driving renewed ransomware activity. Coinbase Cartel's victim postings pushed the UAE into the top 5 target regions and elevated construction to the top victim sector. Across all major actors, exploitation of React2Shell dominated the period, with adversaries rapidly weaponizing the vulnerability in different ways.

TOP RANSOMWARE

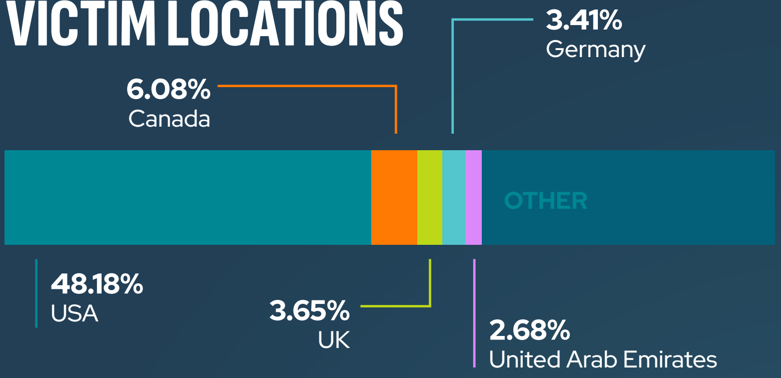


Qilin held a strong lead again this period, while Akira stayed firmly in the top tier. The major shift came from LockBit's return, re-entering the rankings at #3 with immediate impact. Sinobi continued its climb, and Coinbase Cartel jumped from the teens into the top 5, driven by its recent victim disclosures.

VICTIM SECTOR



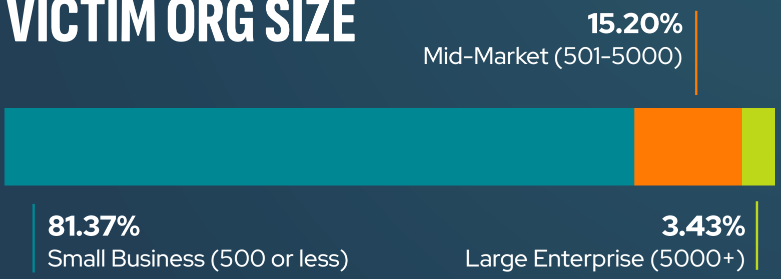
VICTIM LOCATIONS



TOP NEWS

- Contractors with hacking records accused of wiping 96 US government databases
- EU fines X $140 million over deceptive blue checkmarks
- Fortinet, Ivanti, and SAP Issue Urgent Patches for Authentication and Code Execution Flaws
- Marquis data breach impacts over 74 US banks, credit unions
- Over 10,000 Docker Hub images found leaking credentials, auth keys
- Police takes down Cryptomixer cryptocurrency mixing service
- React2Shell flaw exploited to breach 30 orgs, 77k IP addresses vulnerable
- ShadyPanda browser extensions amass 4.3M installs in malicious campaign

VICTIM ORG SIZE



TRENDING & ACTIVELY EXPLOITED VULNERABILITIES

CVE	VENDOR	PRODUCT
CVE-2025-14174	Google	Chromium
CVE-2025-14611	Gladinet	CentreStack and Triofox
CVE-2025-43529	Apple	Multiple Products
CVE-2025-48572	Android	Framework
CVE-2025-48633	Android	Framework
CVE-2025-55182	Meta	React Server Components
CVE-2025-58360	OSGeo	GeoServer
CVE-2025-6218	RARLAB	WinRAR
CVE-2025-62221	Microsoft	Windows
CVE-2025-66644	Array Networks	ArrayOS AG

Attackers focused on new flaws across Chromium, Apple, Android, and Windows. Meta's React Server Components issue tied directly into ongoing React2Shell exploitation. WinRAR, GeoServer, and ArrayOS AG vulnerabilities also saw increased targeting this period.

TRENDING MALWARE

Aisuru
Massive IoT botnet responsible for record DDoS attacks.

DroidLock
Android malware used for device locking and ransom extortion.

EtherRAT
Lightweight RAT enabling remote control and data theft.

Glassworm
Worm-like loader spreading quickly across networks.

Shai-Hulud 2.0
Updated stealer with improved evasion and data-harvest capabilities.

ValleyRAT
Modular RAT used in espionage campaigns with broad system access.

TRENDING ADVERSARIES

UNC5174
UNC6586
UNC6588
UNC6595
UNC6600
UNC6603

UNC5174, UNC6586, UNC6588, UNC6595, UNC6600, and UNC6603 all showed elevated activity during this period, with each leveraging React2Shell in different ways. These clusters focused on rapid exploitation, opportunistic targeting, and broad scanning behavior, contributing to the spike in intrusions tied to the vulnerability.

phish tank DIGITAL

PRODUCED & DISTRIBUTED BY
PHISH TANK DIGITAL

WRITTEN BY
JEREMY NICHOLS
Former Director of the Global Threat Intelligence Center

SUMMARIES & BIOS
GEOFF REHMET
Cybersecurity Expert