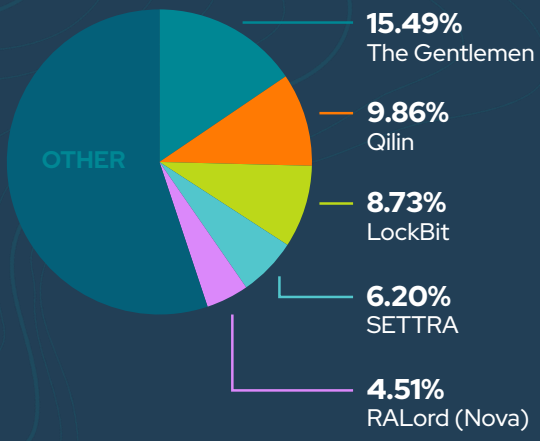
BYER-NICHOLS THREAT BRIEF

SECOND HALF JUNE 2026

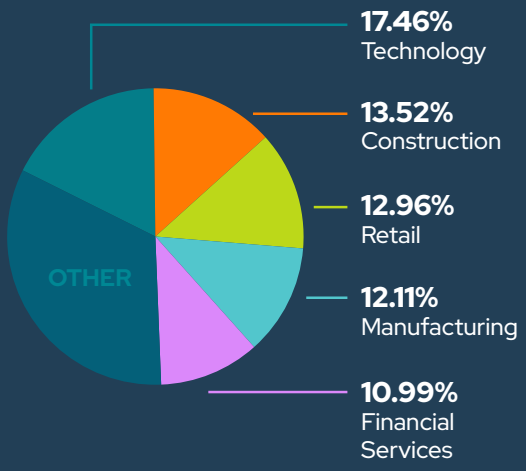
The second half of June remained active, with a few notable developments rather than any major shifts. SETTRA ransomware quickly climbed into the top five after posting 22 victims in a single week, while FortiBleed dominated vulnerability discussions as organizations continued responding to widespread exploitation. Although U.S. organizations remained the most impacted, victim disclosures were spread across a broader range of countries this reporting period.

TOP RANSOMWARE

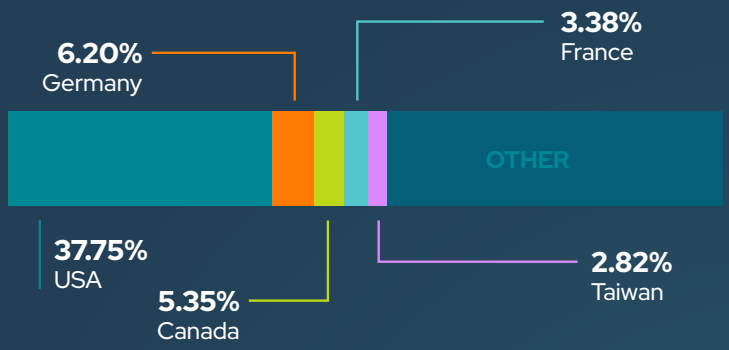


SETTRA was the standout this reporting period, rapidly entering the top five after listing 22 victims in the past week. The remaining groups continue to be familiar operators that have consistently appeared in recent reporting.

VICTIM SECTOR



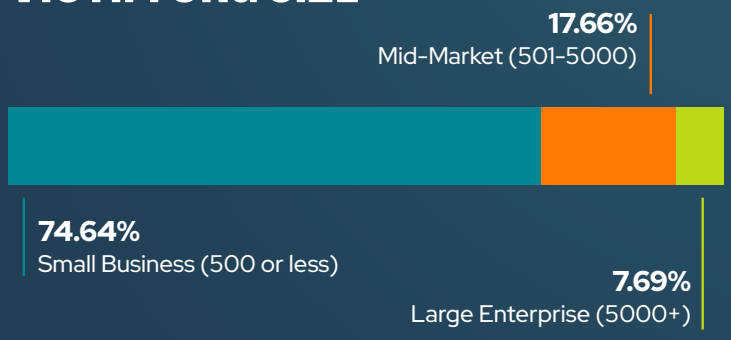
VICTIM LOCATIONS



TOP NEWS

- Amadey, StealC malware operations disrupted in Operation Endgame action
- DraftKings hacker 'Snoopy' sentenced to 18 months in prison
- FortiBleed leak exposes Fortinet VPN credentials for 73,000 devices, heist persists
- FTC warns of record $3.5 billion losses to imposter scams in 2025
- Klue OAuth breach victim list grows as Icarus hackers claim attack
- Police cleans nearly 15,000 SocGholish-infected sites tied to Evil Corp
- Security community slams US ban on exporting Mythos, Fable
- US offers $10 million for hackers targeting WhatsApp, Signal users

VICTIM ORG SIZE



TRENDING & ACTIVELY EXPLOITED VULNERABILITIES

CVE	Vendor	Product
CVE-2026-48558	SimpleHelp	SimpleHelp
CVE-2026-12569	PTC	Windchill and FlexPLM
CVE-2026-20230	Cisco	Unified Communications Manager
CVE-2025-67038	Lantronix	EDS5000
CVE-2026-34910	Ubiquiti	UniFi OS
CVE-2026-34909	Ubiquiti	UniFi OS
CVE-2026-34908	Ubiquiti	UniFi OS
CVE-2026-20253	Splunk	Enterprise
CVE-2026-48907	Widget Factory	Joomla Content Editor
CVE-2026-46817	Oracle	E-Business Suite

Nine Known Exploited Vulnerabilities (KEVs) were tracked this reporting period, alongside a critical Oracle E-Business Suite vulnerability reported as exploited in the wild but not yet added to CISA's KEV catalog. FortiBleed continued to dominate headlines as organizations responded to the widespread impact of the vulnerability.

TRENDING MALWARE

Backdoor.Turn
A Go-based backdoor that abuses Microsoft Teams' TURN relay servers to hide command-and-control traffic within legitimate Teams communications, helping attackers evade detection.

Djinn Stealer
A newly discovered cross-platform infostealer that targets cloud, AI, browser, and administrative credentials to enable follow-on attacks.

Mistic Backdoor
A stealthy backdoor linked to an initial access broker, providing persistent enterprise access that can be sold to ransomware operators.

OXLOADER
A malware loader designed to quietly deliver additional payloads, often serving as the initial stage of larger malware infections.

Rokarolla
A newly observed malware family used to establish persistence and provide remote access for follow-on malicious activity.

STOCKSTAY
A stealth-focused malware family that enables long-term access while attempting to avoid detection during enterprise intrusions.

TRENDING ADVERSARIES

CL-STA-1062
FishMonger
Icarus
ToddyCat
UNC4221
UNC5792

This reporting period featured a mix of financially motivated cybercriminals and state-sponsored threat actors. While several familiar groups remained active, the focus shifted toward emerging campaigns and newly observed activity rather than previously documented operations.

phish tank DIGITAL

PRODUCED & DISTRIBUTED BY
PHISH TANK DIGITAL

WRITTEN BY
JEREMY NICHOLS
Director, Security Programs & Strategy at SecureSky

SUMMARIES & BIOS
GEOFF REHMET
Cybersecurity Expert