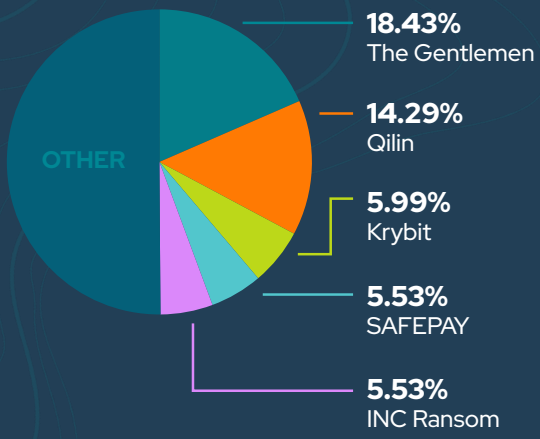
BYER-NICHOLS THREAT BRIEF

FIRST HALF JULY 2026

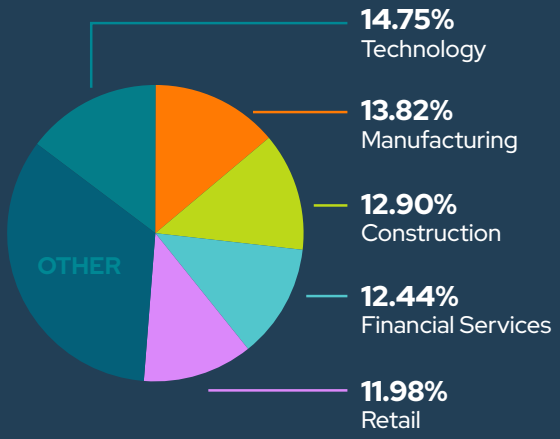
The first half of July showed threat actors pushing harder with hightouch intrusions, routerbased persistence, and faster ransomware playbooks. UAT7810's expanding ORB mesh and The Gentlemen's aggressive extortion stood out, while fresh web app exploits and AI-driven automation kept pressure on defenders. The big theme was speed and stealth: identity compromise, edge device abuse, and quick RCE chaining that demand tighter patching and sharper visibility across networks.

TOP RANSOMWARE

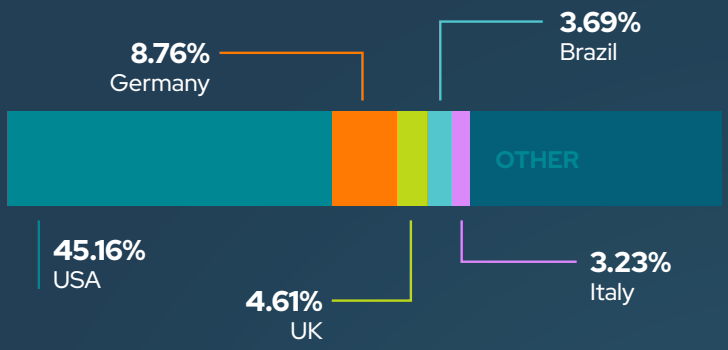


The first half of July saw The Gentlemen dominate ransomware activity, accounting for nearly 20% of observed victims. Qilin continued its steady rise, while Krybit and SAFEPAY posted notable increases, making both groups worth watching. INC Ransom remained consistent with its enterprise-focused, data theft-first operations. Overall, aggressive groups continue to lead while emerging actors gain momentum.

VICTIM SECTOR



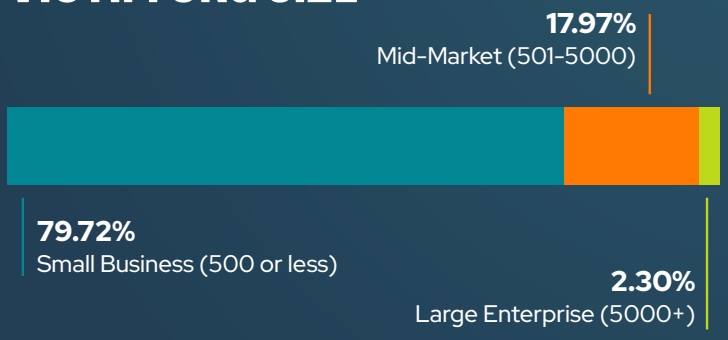
VICTIM LOCATIONS



TOP NEWS

- Ransomware thugs masquerade as Interpol to entice small biz
- Alleged Scattered Spider hacker extradited to the United States
- ARToken PhaaS exposes EvilTokens' Microsoft 365 phishing toolkit
- NetNut proxy network disrupted, 2 million infected devices cut off
- Former ransomware negotiator gets 4 years for BlackCat attacks
- Conditional access misconfigurations exposed 55 orgs with MFA on
- Police suspects Dutch hackers were involved in Odido breach
- Progress urges ShareFile admins to shut down servers over "credible" threat

VICTIM ORG SIZE



TRENDING & ACTIVELY EXPLOITED VULNERABILITIES

CVE	Vendor	Product
CVE-2026-56291	Balbooa	Forms
CVE-2026-48939	iCagenda	iCagenda
CVE-2026-48908	JoomShaper	SP Page Builder
CVE-2026-55255	Langflow	Langflow
CVE-2026-56290	Joomlack	Page Builder
CVE-2026-48282	Adobe	ColdFusion
CVE-2026-45659	Microsoft	SharePoint Server
CVE-2026-8451	Citrix	NetScaler (ADC & Gateway)
CVE-2026-20896	Gitea	Gitea Open Source Git Server
CVE-2026-46817	Oracle	E-Business Suite

The July activity trending vulnerabilities shows attackers zeroing in on easy to automate RCE bugs across Joomla builders, Langflow, ColdFusion, SharePoint, NetScaler, and Gitea. Most of the action has been quick webshell drops followed by credential theft and lateral movement, especially on ColdFusion and NetScaler. For defenders, the priority is tightening patch cycles, locking down exposed admin panels, and boosting monitoring around web apps and edge gateways.

TRENDING MALWARE

ChocoPoC
Python RAT hidden in trojanized PoC exploits that quietly steals researchers' data and grants remote shell access.

JadePuffer
Autonomous AI agent that runs a full ransomware playbook end-to-end at machine speed, slashing the skill and cost barrier for attacks.

BusySnake
Python infostealer used by an APT to burrow into critical infrastructure networks, exfiltrating credentials and sensitive data while staying hard to analyze.

GodDamn Ransomware
Hyadinafamily ransomware that uses a Microsoft-signed malicious driver to kill security tools, then steals credentials and encrypts networks.

LONGLEASH
Advanced router backdoor in a Chinalinked ORB network, turning SOHO devices into flexible C2 relays and tunnels for espionage operations.

DOGLEASH
Cbased passive backdoor for Linux networking gear that listens on a hidden port, executes shellcode, and quietly manages files and OS info.

TRENDING ADVERSARIES

Armored Likho

UAT-7810

O-UNC-066

Helix (Vishing Group)

Armored Likho, UAT7810, OUNC066, and Helix all leaned into hightouch intrusion work, with Likho pushing stealthy Python loaders and UAT7810 expanding routerbased ORB infrastructure that's tough to spot. OUNC066 kept exploiting exposed services for quick data theft, while Helix refined phishing to gain reliable initial access. The shared trend is identity compromise and living off the land tooling, and UAT7810 stands out as the most concerning thanks to its persistent edgedevice footholds.

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