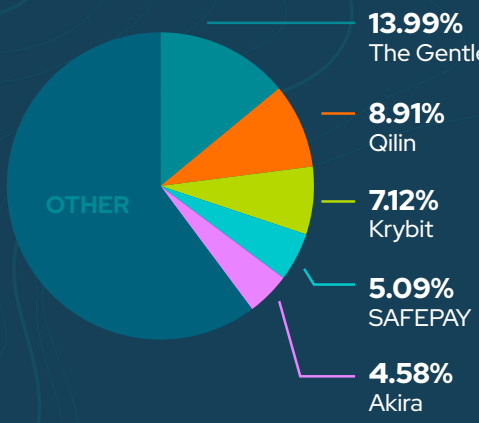
BYER-NICHOLS THREAT BRIEF

FIRST HALF SEPTEMBER 2026

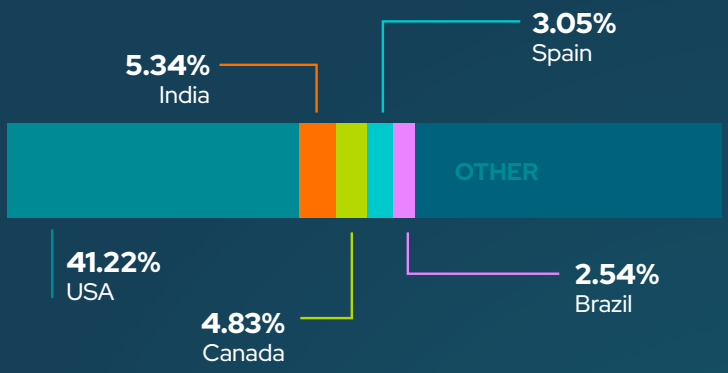
Early September was defined less by ransomware disruption than by an unusually heavy vulnerability window and a fresh malware set. The Gentlemen retook the ransomware lead, mid-market victims expanded, and critical enterprise flaws plus Microsoft and Chromium zero-days raised patching pressure as actors paired identity-driven access with newer cross-platform and remote-control tooling.

TOP RANSOMWARE



The Gentlemen moved back into first as Qilin eased from 17.71% to 8.91%. Krybit and Akira returned to the top five, while SAFEPAY's jump from #46 is better read as a rebound for a group that regularly circulates in the top 15. Overall, this was the usual up-and-down rotation rather than a structural shift in ransomware activity.

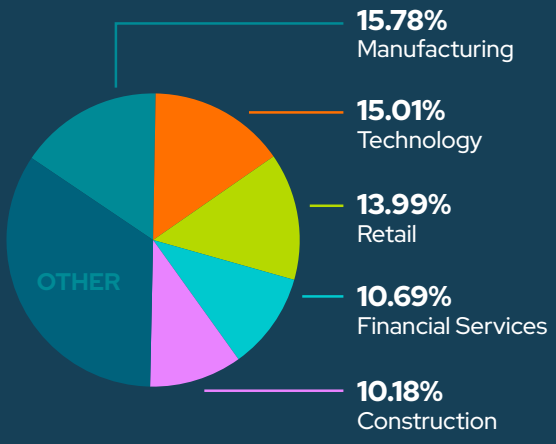
VICTIM LOCATIONS



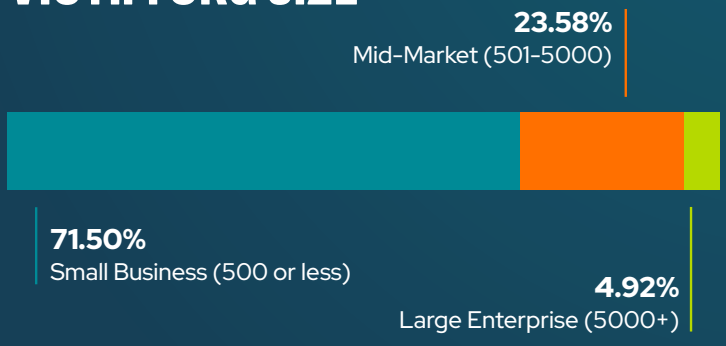
TOP NEWS

- ClickFix campaign compromises 31 orgs, abuses polygon blockchain
- Old, unpatched flaws give attackers access to Philippines nuclear agency
- US charges Russian for infecting 80,000 freelancers with malware
- Two exploited zero-days and 113 critical vulnerabilities among 972 September CVEs
- China-based AI companies target US models with industrial-scale knowledge distillation
- Threat actor generates 1M personalized fraud emails in 3 days
- Japan's digital agency says VPN flaw exposed 246,000 personnel records
- Hackers abused Claude to extract secrets from 1.8M Android apps

VICTIM SECTOR



VICTIM ORG SIZE



TRENDING & ACTIVELY EXPLOITED VULNERABILITIES

CVE	Vendor	Product
CVE-2026-19490	Citrix	NetScaler
CVE-2026-20079	Cisco	Secure Firewall Management Center (FMC) & Security Cloud Control (SCC) Firewall Management
CVE-2026-75650	Adobe	Commerce & Magento
CVE-2026-81963	Microsoft	Windows
CVE-2026-82329	JFrog	Artifactory
CVE-2026-84869	ConnectWise	ScreenConnect
CVE-2026-85046	Google	Chromium V8
CVE-2026-85706	GitLab	Community Edition & Enterprise Edition
CVE-2026-85880	Microsoft	Windows
CVE-2026-87491	Google	Chromium V8

The vulnerability window was unusually crowded, with CISA adding more than 20 flaws during the period. The selected ten focus on the highest-criticality enterprise exposures across NetScaler, Cisco firewall management, Adobe Commerce and Magento, Artifactory, ScreenConnect, and GitLab, plus exploited Microsoft Windows and Chromium V8 zero-days. Prioritize internet-facing management systems first, then accelerate browser and endpoint patching where exploitation can reach users quickly.

TRENDING MALWARE

BambooToken
Multi-platform espionage malware that uses MQTT and DLL sideloading to quietly control and profile Windows and Linux hosts.

Cyclops Blink
A modular botnet and backdoor, now upgraded for modern Linux appliances, used by Sandworm-linked actors for deep network visibility.

NodeRabbit
Cross-platform JavaScript RAT delivered via trojanized coding challenges, giving attackers persistent remote control and file/system access.

PollCat
Cross-platform RAT paired with NodeRabbit, using obfuscated JavaScript and HTTP C2 to execute commands, move files, and maintain stealthy persistence.

REVSTEALER
Feature-rich infostealer that blends anti-analysis, wallet and credential theft, gaming account targeting, and Polygon-based fallback C2.

VectraRAT
Malware-as-a-service remote access trojan that offers turnkey control, data theft, and flexible modules to subscribing threat actors.

TRENDING ADVERSARIES

BREEZE COMET
Cordial Spider
Gambling Goblin
Mirage Kitten
Springs / Spring Ring
UAC-0099

BREEZE COMET and Gambling Goblin reflect financially motivated operations, from manipulating Brazilian payment systems to hijacking government sites for gambling traffic. Cordial Spider and Springs lean on vishing and trusted SSO or collaboration workflows, while Mirage Kitten expands cross-platform espionage with NodeRabbit and PollCat and UAC-0099 experiments with prompt injection to hinder AI-assisted analysis. The mix is evenly split between newer and established actors, but identity abuse and novel tooling are the strongest common threads.

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