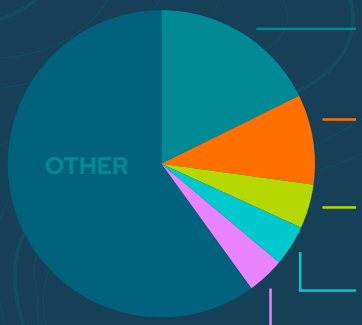
BYER-NICHOLS THREAT BRIEF

SECOND HALF AUGUST 2026

Late August centered on infrastructure and access, with Qilin widening its ransomware lead, technology becoming the top victim sector, and the U.S. remaining dominant despite another decline in share. Vulnerabilities clustered around major enterprise platforms, while malware leaned toward stealers, loaders, banking fraud, and remote access. Speed remains the common thread, making rapid patching and stronger identity controls increasingly critical.

TOP RANSOMWARE



17.71% Qilin

9.48% The Gentlemen

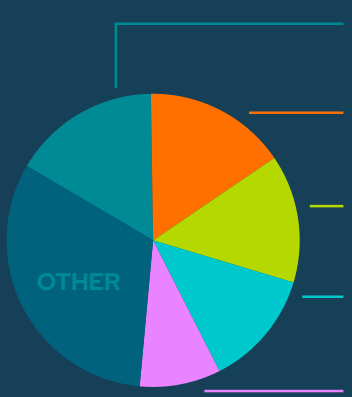
4.65% Dire Wolf

4.29% INC Ransom

3.94% Lockbit

Qilin separated from the pack, climbing to 17.71% and adding 4.82 percentage points while holding the top spot. The Gentlemen stayed #2 but cooled to 9.48%. Dire Wolf is the real mover, jumping from ninth to third, while INC Ransom remained steady and LockBit returned to the top five. Notably, the top-five share fell from 44.34% to 40.07%, so Qilin's surge is happening inside a more fragmented field rather than a broader consolidation.

VICTIM SECTOR



16.28% Technology

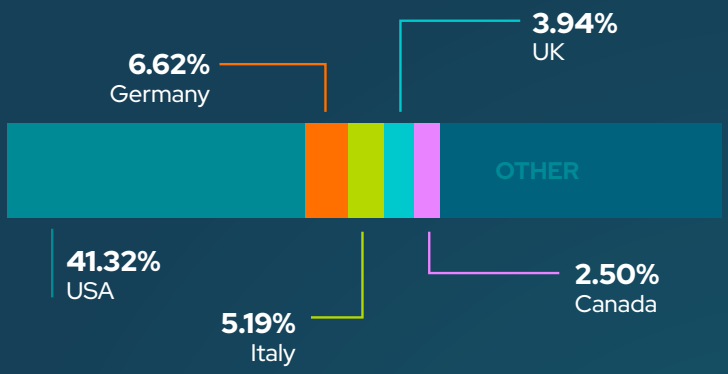
15.74% Manufacturing

14.13% Financial Services

12.88% Construction

8.94% Retail

VICTIM LOCATIONS



6.62% Germany

3.94% UK

41.32% USA

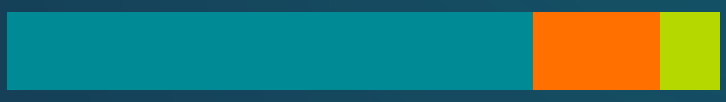
5.19% Italy

2.50% Canada

TOP NEWS

- Chinese ZBT routers sold worldwide contain backdoors
- Claude desktop malvertising campaign hit 29 organizations with SectopRAT
- Delta flight carrying DEF CON "hackers" hit by Wi-Fi attack mid-air
- Interpol's Jackal IV disrupts West African crime infrastructure
- NovaCookies' kit steals Microsoft 365 sessions for $320 a month
- Post-DEF CON phishing uses malicious Google Doc to deliver malware
- Russian Hackers phish EU officials over messaging apps

VICTIM ORG SIZE



16.99% Mid-Market (501-5000)

76.57% Small Business (500 or less)

6.44% Large Enterprise (5000+)

TRENDING & ACTIVELY EXPLOITED VULNERABILITIES

CVE	Vendor	Product
CVE-2026-21962	Oracle	HTTP Server and Oracle Weblogic Server Proxy Plug-in
CVE-2026-33824	Microsoft	Internet Key Exchange (IKE) Service Extensions
CVE-2026-53362	Linux	Kernel
CVE-2026-55040	Microsoft	SharePoint
CVE-2026-59310	Broadcom	VMware vCenter
CVE-2026-65400	Apple	macOS
CVE-2026-73570	Synacor	Zimbra Collaboration Suite (ZCS)
CVE-2026-81578	PaperCut	NG/MF
CVE-2026-82078	PaperCut	NG/MF
CVE-2026-8452	Citrix	NetScaler ADC and NetScaler Gateway

Late August's exploited-vulnerability list is concentrated in enterprise infrastructure rather than everyday end-user software: Oracle/WebLogic, SharePoint, VMware vCenter, Zimbra, PaperCut, and Citrix NetScaler all sit in high-value administrative or collaboration paths. Microsoft IKE and the Linux kernel broaden the exposure into core operating-system components, while two PaperCut entries reinforce how often attackers return to centralized management platforms with broad network reach. Internet-facing admin services and management tools should remain at the front of the patch queue.

TRENDING MALWARE

Amatera Stealer
Information-stealing malware-as-a-service and ACR Stealer successor built to harvest credentials and sensitive endpoint data while improving anti-analysis evasion.

C2Looper
Rust-based backdoor that uses GitHub as command-and-control and supports reconnaissance, arbitrary command execution, and second-stage payload delivery.

MacSync Stealer
macOS-focused information stealer that uses ClickFix-style social engineering, rotating infrastructure, and scripted collection to steal credentials and sensitive files.

SynkLoader
Modular loader delivered through Microsoft Teams phishing that combines memory-resident components, credential phishing, tunneling, and hands-on-keyboard access.

ToxicPanda 2.0
Android banking trojan and remote-access tool built for on-device fraud through overlays, Accessibility abuse, PIN capture, and expanded remote control.

ValleyRAT
Windows remote-access trojan used in evolving campaigns that rely on fake installers, malicious email, staged payload delivery, and anti-analysis techniques.

TRENDING ADVERSARIES

AurOra
ClOp
Dark Caracal
Mabna Institute
Storm-1175
Transparent Tribe

AurOra brings a newer AI-assisted criminal angle, while ClOp remains the most recognizable mass-exploitation specialist in the set. Dark Caracal, Mabna Institute, and Transparent Tribe skew toward longer-term espionage and intelligence collection, while Storm-1175 operates at ransomware speed, weaponizing exposed web-facing systems and newly disclosed flaws quickly. Together, the group shows the current split clearly: persistent intelligence collection on one side and rapid exploitation-for-impact on the other.

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