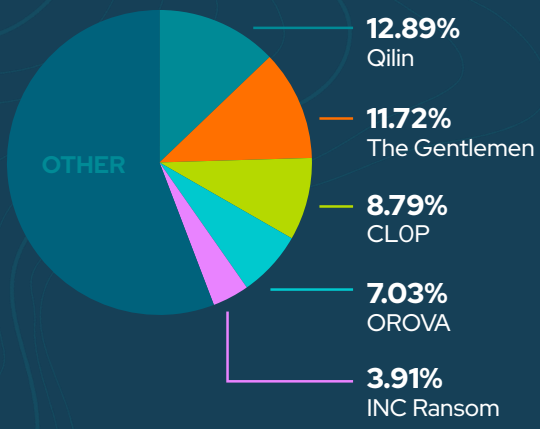
BYER-NICHOLS THREAT BRIEF

FIRST HALF AUGUST 2026

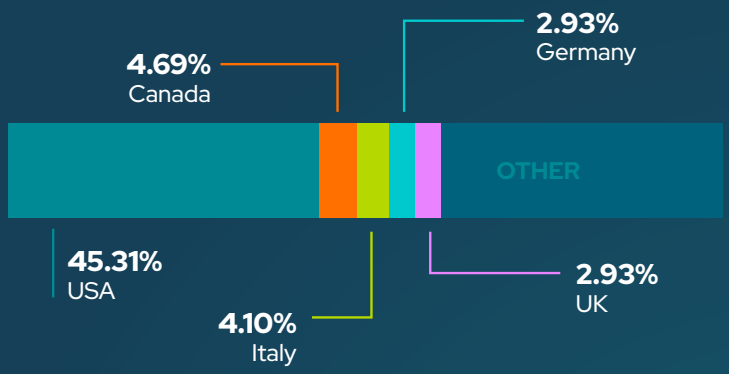
Threat activity stayed busy in early August, with ransomware crews pushing sharper extortion tactics, cloud-aware espionage groups refining their stealth, and a wave of edge-device and management-tool exploits giving attackers quick footholds. Botnets and stealers kept expanding through unpatched IoT and browser weaknesses, while social-engineering-driven mobile fraud added a fresh twist. Overall, fast patching, tighter access controls, and closer log scrutiny mattered more than ever as actors shifted tools and targets with little warning.

TOP RANSOMWARE



Qilin leads with steady activity and aggressive leak-site pressure, while The Gentlemen keep up their quick, opportunistic hits. CL0P remains influential despite lower numbers, shifting to selective high-value targets after its earlier mass-impact campaigns. Newcomer OROVA is the standout, experimenting with fresh infrastructure and extortion tactics. INC Ransom continues its consistent mid-tier operations, often hitting environments where downtime hurts most.

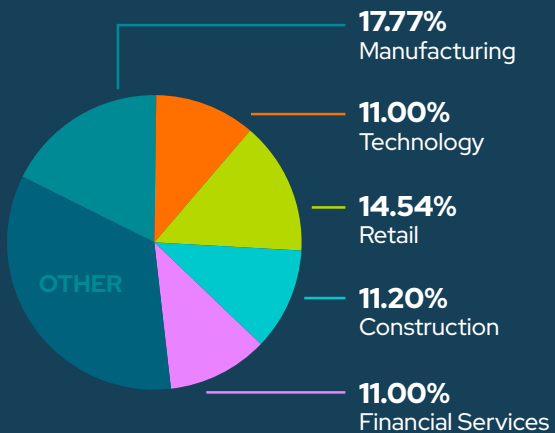
VICTIM LOCATIONS



TOP NEWS

- Device code phishing up 1,500% in 2026
- White House taps security firms for offensive hack-back operations
- Ransomware hits Colombian justice ministry days before presidential transition
- Flaws in Google APK for Python unlock agent-to-agent
- Attack AI notetaker lets hackers spy on government, corporate video calls
- Multistate water system attacks Widen, Iran suspected
- Hackers arrested over €30M bank fraud exploiting service provider flaw
- Belgium's eID authentication opens citizen accounts to RCE

VICTIM SECTOR



VICTIM ORG SIZE

TRENDING & ACTIVELY EXPLOITED VULNERABILITIES

CVE	Vendor	Product
CVE-2026-20349	Cisco	Secure Firewall Adaptive Security Appliance (ASA) and Secure Firewall Threat Defense (FTD)
CVE-2026-68820	Microsoft	Windows Ancillary Function Driver for WinSock
CVE-2026-72898	Metabase	Metabase
CVE-2026-8037	Progress	LoadMaster
CVE-2026-63077	JetBrains	TeamCity
CVE-2026-18556	N-able	N-central
CVE-2026-34486	Apache	Tomcat
CVE-2026-9198	IBM	Langflow
CVE-2026-18577	N-able	N-central
CVE-2026-69414	Microsoft	Microsoft Malware Protection Engine (aka ShieldBreak)

Attackers are leaning hard on edge and management gear this fortnight, with Cisco ASA/FTD, Metabase, LoadMaster, TeamCity, N-central, and Tomcat bugs all seeing active exploitation for remote code execution and lateral movement. Windows WinSock and ShieldBreak engine flaws add a nasty client and AV angle, turning everyday endpoints into launchpads. Langflow exposure raises AI-service and data-leak risk. Priority moves: patch fast, lock down internet-facing admin portals, enforce strong auth, and watch logs and IPS for odd config changes and new services spinning up.

TRENDING MALWARE

AmnesiaStealer
Chromium-focused info-stealer that abuses browser extensions to siphon credentials, cookies, and session data for account takeover and further compromise.

CHAINDROP
Self-propagating npm worm that steals developer secrets and uses blockchain-resolved C2 to silently republish poisoned packages across the software supply chain.

DeadLock
Rust-based double-extortion ransomware that couples fast, resource-aware encryption with blockchain-backed, decentralized infrastructure to resist takedown.

Evooo1Bot
Mirai-derived Linux botnet that turns edge devices into multi-purpose DDoS nodes, SOCKS proxies, and exploit launchpads against a wide range of IoT and network gear.

Kimwolf v7
Android/IoT botnet that uses ENS-resolved and Tor-backed C2 plus HTTP/2 browser-like floods to make DDoS traffic look indistinguishable from real users.

WindRelay
Android NFC relay malware paired with SpyNote RAT that turns victims' phones into live contactless card proxies for real-time payment and cash-out fraud.

TRENDING ADVERSARIES

Armored Likho | **Head Mare** | **Jewelbug**
GOLD EMBRACE | **HoneyMyte** | **UNC6671**

Armored Likho, GOLD EMBRACE, Head Mare, HoneyMyte, Jewelbug, and UNC6671 all lean heavily on stealthy, long-game intrusions, blending custom loaders, living-off-the-land tactics, and tight targeting of government or tech sectors. Several are refining cloud-focused tradecraft, while others push sharper social-engineering lures and cleaner post-exploitation workflows. Jewelbug and HoneyMyte stand out for disciplined espionage operations, but UNC6671 is the most concerning thanks to its rapid tooling shifts and willingness to pivot quickly across victim environments, making detection and containment tougher for defenders.

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