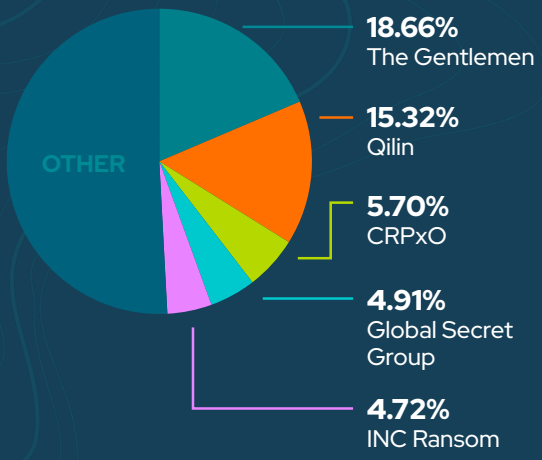
BYER-NICHOLS THREAT BRIEF

SECOND HALF JULY 2026

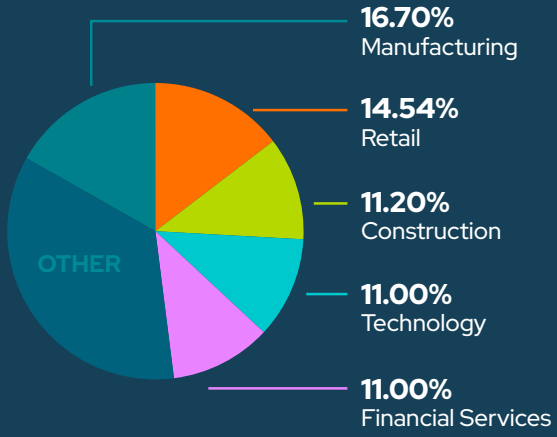
The back half of July showed a sharp rise in stealthy, long-dwell threats: ransomware crews leaned on faster automation, cloud pivots, and polished extortion, while APTs pushed supply-chain abuse, identity attacks and browser-based C2. Active exploits across Fortinet, Cisco, Langflow, SharePoint and WordPress kept pressure high, making rapid patching and tighter admin controls essential for defenders.

TOP RANSOMWARE

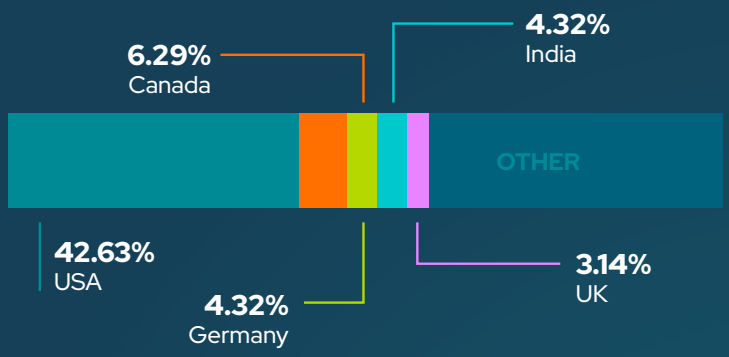


The second half of July saw The Gentlemen surge to the top with fast, automated intrusions hitting mid-market firms. Qilin stayed active in healthcare and manufacturing, leaning on harsher leak-site pressure. CRPxO jumped from obscurity by exploiting weak cloud segmentation, while Global Secret Group debuted with polished extortion operations. INC Ransom kept its steady pace, relying on long-term persistence to quietly expand access.

VICTIM SECTOR



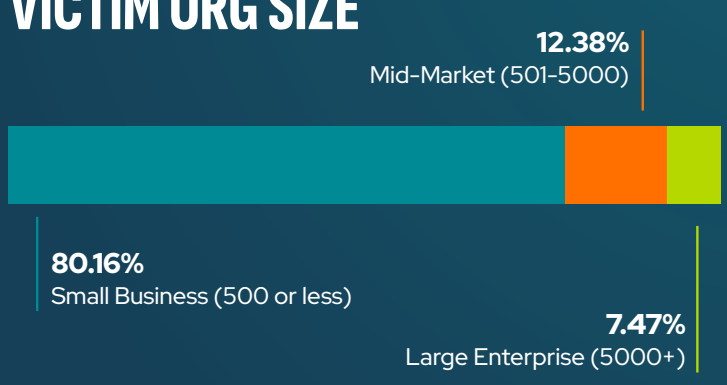
VICTIM LOCATIONS



TOP NEWS

- 1M+ emails use hidden text to dupe AI security filters
- FakeGit campaign uses 7,600 GitHub repos to push SmartLoader malware
- Hackers disrupt over 30 Minnesota water utilities in coordinated OT attack
- Health-ISAC warns of rising ShinyHunters data theft attacks on healthcare
- Microsoft warns of surge in ACR Stealer attacks on customers
- New Project CAV3RN module abuses Outlook calendar events for C2 and DNS AAAA records for configuration recovery
- OpenAI models used Artifactory zero-days to escape to the internet, breach multiple orgs
- Police dismantle Kratos phishing platform, arrest developer

VICTIM ORG SIZE



TRENDING & ACTIVELY EXPLOITED VULNERABILITIES

CVE	Vendor	Product
CVE-2025-68686	Fortinet	FortiOS
CVE-2026-0770	Langflow	Langflow
CVE-2026-16232	Check Point	SmartConsole
CVE-2026-20316	Cisco	Secure Firewall Management Center
CVE-2026-25089	Fortinet	FortiSandbox
CVE-2026-39808	Fortinet	FortiSandbox
CVE-2026-50522	Microsoft	SharePoint
CVE-2026-58644	Microsoft	SharePoint
CVE-2026-60137	WordPress	Core
CVE-2026-63030	WordPress	Core

Late July exploitation is clustering around management planes: FortiOS and FortiSandbox bugs, Langflow RCE, Check Point SmartConsole, and Cisco Secure FMC all give attackers direct control over security tooling, while fresh SharePoint and WordPress core flaws open easy paths into collaboration sites and public-facing blogs. The big worry is chained use: Fortinet or Cisco for initial foothold, then SharePoint/WordPress for spread and persistence. Defenders should patch per vendor guidance, lock down internet-exposed consoles, enforce MFA, and watch for odd admin and content changes.

TRENDING MALWARE

ClickLock
Modular macOS infostealer that locks victims' Macs until they surrender passwords, then leaves a persistent backdoor.

EncForge
Go-based ransomware purpose-built to encrypt AI model weights, vector indexes, and training datasets without data exfiltration.

HelloNet *(HelloInjector, HelloProxy, HelloExecutor, HelloCleaner, HelloBackdoor)*
DLL side-loaded toolset abusing ViPNet updates to proxy C2 traffic, deploy backdoors, and hide activity in Russian government networks.

HollowGraph
Stealthy .NET espionage implant that turns Microsoft 365 calendars into covert C2 and data exfiltration channels.

msaRAT
Rust-based RAT that hijacks Chrome or Edge to build a covert, double-encrypted WebRTC C2 channel entirely through the browser.

OWAReaper
Browser-resident backdoor for Outlook Web Access that abuses a half-click XSS exploit to steal credentials and persist server-side.

TRENDING ADVERSARIES

CyberAv3ngers | **Mirage Kitten** | **STAC4749**
LAUNDRY BEAR | **REF9403** | **UTA0533**

Recent activity from CyberAv3ngers, LAUNDRY BEAR, Mirage Kitten, REF9403, STAC4749, and UTA0533 shows a clear tilt toward supply-chain abuse, credential harvesting, and long-dwell espionage. Several groups are leaning on living-off-the-land tactics and cloud-service impersonation, making detection tougher. Mirage Kitten stands out as the most concerning thanks to its rapid pivoting and focus on high-value government and tech targets, signaling a rising need for stronger identity and cloud-control hygiene.

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