

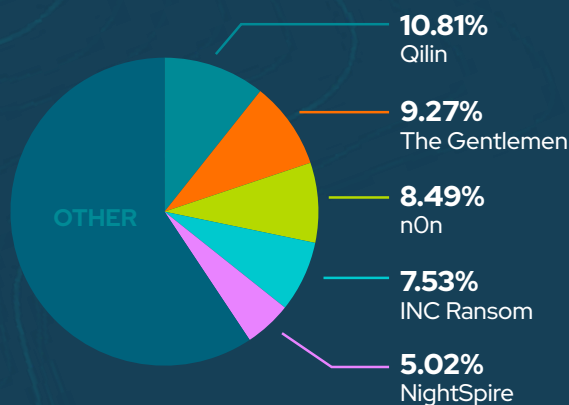
BYER-NICHOLS THREAT BRIEF

FIRST HALF OCTOBER 2026



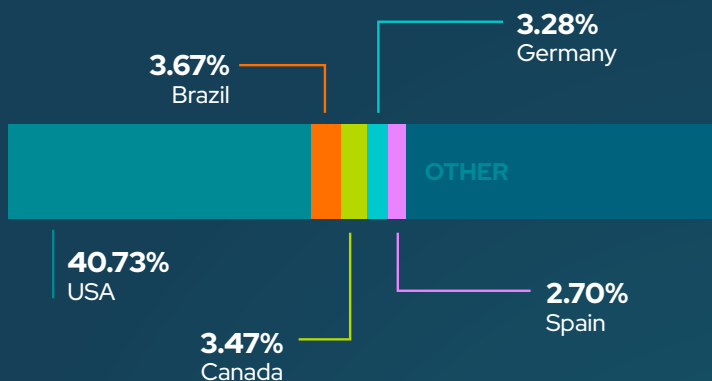
Early October showed attackers moving quickly against trusted infrastructure. Exploited flaws hit firewalls, email gateways, VPNs, backup servers and enterprise apps, while espionage groups paired tailored phishing with stealthy RATs, AI-assisted tools and memory-resident implants. Ransomware stayed fluid as nOn and NightSpire surged beside established crews. The priority is clear: patch exposed systems fast, restrict admin access, rotate credentials and hunt for persistence after remediation.

TOP RANSOMWARE



Qilin led the first half of October with 10.81%, narrowly ahead of The Gentlemen, while INC Ransom remained a familiar top-tier presence. Qilin also claimed engineering consultancy EPTISA, and INC listed German architecture firm Architekt von Danwitz, although both remain actor claims. The real story was volatility: newcomer nOn surged from sixth to third at 8.49%, suggesting unusually rapid scaling, while NightSpire leapt from 43rd to fifth after only recently reaching the top 25. Together, these shifts show established brands sharing the spotlight with fast-moving challengers.

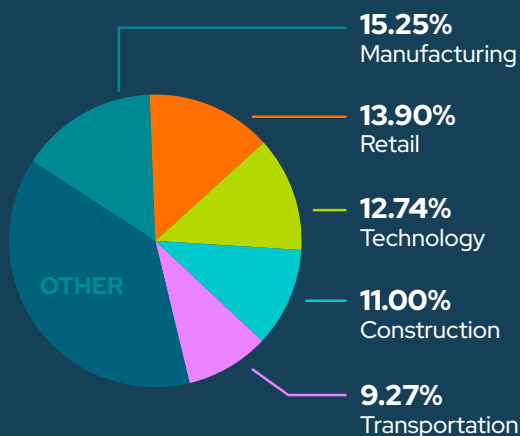
VICTIM LOCATIONS



TOP NEWS

- DOJ charges 14 and raids 40+ Texas laptop farms in a North Korean IT worker scheme
- FBI arrests a third suspected ShinyHunters member after the FBIjobs.gov incident
- GhostAction supply-chain wave hits about 1,900 GitHub accounts and 30,000 repositories
- Hackers stole Pentagon personnel records of over 3 million people
- Hackers hijacked French supermarket refrigeration controllers, heating freezers to 50°C at hundreds of stores
- Microsoft's X account hacked in crypto pump-and-dump scheme
- Police dismantle KillSec ransomware gang allegedly led by 16-year-old
- Seven domains tied to Flax Typhoon scanning and phishing tools seized

VICTIM SECTOR



VICTIM ORG SIZE



TRENDING & ACTIVELY EXPLOITED VULNERABILITIES

CVE	Vendor	Product
CVE-2026-0322	Palo Alto Networks	PAN-OS
CVE-2026-102489	Zammad GmbH	Zammad
CVE-2026-102490	Zammad GmbH	Zammad
CVE-2026-104286	Fortinet	FortiMail
CVE-2026-104935	Ivanti	Connect Secure
CVE-2026-105134	Ahsay	AhsayCBS
CVE-2026-21589	Atlassian	Multiple Products
CVE-2026-76519	Cisco	Secure Email Gateway
CVE-2026-88779	Citrix	NetScaler
CVE-2026-96951	Microsoft	Windows

October's exploited flaws span PAN-OS, Zammad, FortiMail, Ivanti Connect Secure, AhsayCBS, Atlassian products, Cisco Secure Email Gateway, Citrix NetScaler and Windows. The main concern is internet-facing infrastructure: several bugs enable unauthenticated file access or writes, command execution, root compromise, session hijacking or disruption. AhsayCBS attacks planted web shells and miners after earlier fixes were incomplete. Patch every listed CVE now, limit management access, verify fixed builds, rotate exposed credentials, and hunt for persistence or prior compromise.

TRENDING MALWARE

ASHVEIN

ASHVEIN is a Windows RAT and infostealer that enables credential theft, surveillance, data collection, and remote control in targeted espionage operations.

ClingSTUN

ClingSTUN compromises unpatched Linux and IoT devices, then turns them into persistent proxy nodes using public STUN services to support covert connectivity.

Hirudo

Hirudo is an Android banking trojan that replaces legitimate banking apps with patched copies to bypass security checks and facilitate account takeover.

PEERSTITCH

PEERSTITCH is a memory-resident FortiGate implant that hides inside legitimate daemons, enabling stealthy traffic interception and unauthorized VPN access.

PoeLLM

PoeLLM exploits vulnerable internet-facing services, mines cryptocurrency, and expands its botnet while deriving command infrastructure from words hidden in an online poem.

SysGoRAT

SysGoRAT is a cross-platform Go-based RAT that provides durable remote access, command execution, interactive shells, and proxying in espionage-focused intrusions.

TRENDING ADVERSARIES

Armory Castle

CL-UNK-1211

TA419

UAC-0099

UAT-6275

UNC5820

Trending threat actors point to an espionage-heavy cycle built around trusted access: Armory Castle and UNC5820 exploit edge-management products, while TA419, UAC-0099 and UAT-6275 use tailored lures, credential theft and custom remote-access tools. CL-UNK-1211 adds AI-generated payloads, web shells and Linux targeting. UNC5820 is the most concerning because one FortiManager breach exposed data for more than 500 firewalls and enabled a stealthy in-memory implant. Defenders should patch edge systems quickly, protect admin credentials, monitor trusted processes and hunt beyond disk-based indicators.



PRODUCED & DISTRIBUTED BY
PHISH TANK DIGITAL



WRITTEN BY
JEREMY NICHOLS
Director, Security Programs
& Strategy at SecureSky



SUMMARIES & BIOS
GEOFF REHMET
Cybersecurity Expert