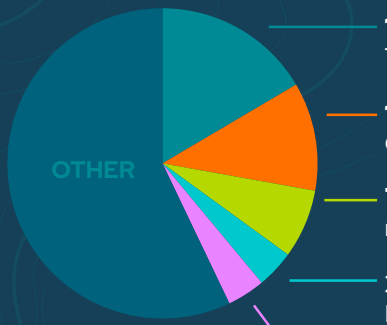
BYER-NICHOLS THREAT BRIEF

SECOND HALF OCTOBER 2026

Late October brought rising risk across endpoints, infrastructure, and the software supply chain. Ransomware leaders intensified activity, while espionage groups used AI, trusted applications, developer tools, and edge flaws to scale attacks and stay hidden. New malware targeted AI credentials, network keys, and government systems. With exploited bugs spanning VPNs, PHP, GitLab, Linux, and commerce platforms, defenders should patch fast, rotate exposed credentials, and hunt for compromise.

TOP RANSOMWARE



16.49% The Gentlemen

11.29% Qilin

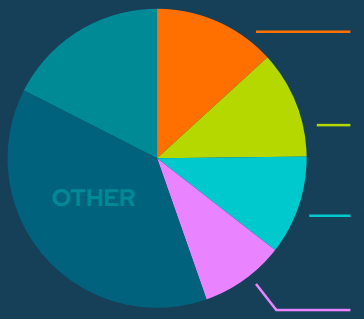
7.17% nOn

3.94% Booba Project

3.94% INC Ransom

The Gentlemen set the pace at 16.49%, continuing its strong run, with Qilin still applying pressure at 11.29% despite dropping to second. n0n's rapid ascent remained the period's standout story: 38 shipping and logistics claims appeared within 23 minutes, reportedly linked to one supplier compromise rather than dozens of separate attacks. Booba Project also surged from 23rd to fourth, while INC Ransom slipped one position. Together, the top three shaped October's spike, with U.S. organizations and manufacturers taking the brunt of activity.

VICTIM SECTOR



17.56% Technology

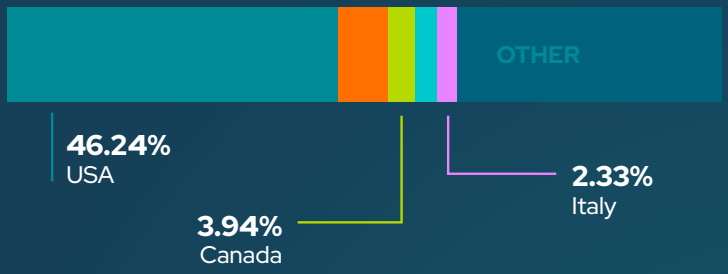
13.26% Financial Services

11.65% Manufacturing

10.75% Construction

9.14% Retail

VICTIM LOCATIONS



6.81% Germany

3.05% Spain

46.24% USA

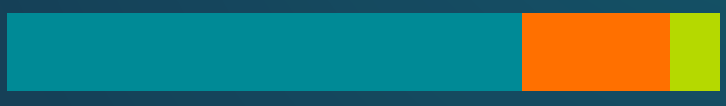
3.94% Canada

2.33% Italy

TOP NEWS

- AI coding agents hijacked via AGENTS.md, plus trojanized Claude Code extension for Cursor
- BAE Systems cyberattack disrupts US federal court operations
- GitLab warns of new max severity code execution vulnerability
- Hackers breach Microsoft 365 tenants via ConnectWise supply-chain attack
- OVHcloud GitHub compromise tied to GlassWorm threat actors
- PHP ships emergency patches for critical PHP2Shell flaws
- Tech giants block eMudhra Certificates tied to 8 compromised keys
- VAPOR PANDA uses AI-driven ARTEX to scale a global espionage campaign

VICTIM ORG SIZE



18.95% Mid-Market (501-5000)

73.29% Small Business (500 or less)

7.76% Large Enterprise (5000+)

TRENDING & ACTIVELY EXPLOITED VULNERABILITIES

CVE	Vendor	Product
CVE-2025-61624	Fortinet	Multiple Products
CVE-2026-102764	BeyondTrust	Remote Support
CVE-2026-109618	PHP Group	PHP
CVE-2026-109619	PHP Group	PHP
CVE-2026-111357	Ivanti	Connect Secure
CVE-2026-111497	Google	Brotli
CVE-2026-118527	Ivanti	Connect Secure
CVE-2026-46300	Linux	Kernel
CVE-2026-48356	Adobe	Commerce and Magento
CVE-2026-97229	GitLab	Community Edition and Enterprise Edition

This wave hits the full stack: Fortinet and BeyondTrust at the edge, Ivanti VPN chains reaching root, PHP2Shell and GitLab enabling unauthenticated code execution, Brotli exposing embedded runtimes, Linux providing privilege escalation, and Adobe Commerce/Magento opening a path through malicious uploads. Defenders should patch these CVEs now, prioritizing internet-facing and identity-bearing systems; rebuild affected containers, restrict management access, rotate exposed credentials, and hunt for compromise rather than treating an upgrade as proof the environment is clean.

TRENDING MALWARE

Aokigahara
Aokigahara steals AI-assistant credentials and other valuable data, potentially exposing developer identities, repositories, cloud services, and CI/CD pipelines.

BlackX
BlackX is a highly persistent UEFI bootkit that bypasses incompletely remediated Secure Boot protections to conceal espionage activity below Windows.

Candiru
Candiru is mercenary spyware capable of zero-click delivery through targeted advertisements and extensive theft of files, messages, credentials, and authenticated sessions.

KeyDrift
KeyDrift compromises Cisco SD-WAN controllers to maintain covert access, execute commands, and extract sensitive traffic-encryption key material.

MythicRatatoskr
MythicRatatoskr is a Go-based backdoor that hides command-and-control traffic in the Yggdrasil mesh network and enables broad post-compromise control.

SysGoRAT
SysGoRAT provides persistent, cross-platform remote access for espionage operations targeting government Linux infrastructure and sensitive communications.

TRENDING ADVERSARIES

APT41
BRONZE SANDCASTLE
CL-UNK-1211
GlassWorm
Storm-0940
Warp Panda

APT41, Bronze Sandcastle, CL-UNK-1211, GlassWorm, Storm-0940, and Warp Panda show the same shift: abusing trusted software, cloud services, developer tools, and AI to move fast and stay hidden. Their campaigns mix DLL sideloading, poisoned extensions, Linux web shells, edge exploits, token theft, and hypervisor evasion. Storm-0940 is the biggest concern because ARTEX helped it target hundreds and gain privileged cloud access in under three hours. Defenders should secure supply chains, patch exposed systems quickly, monitor signed binaries and service accounts, and hunt beyond endpoint logs.

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