

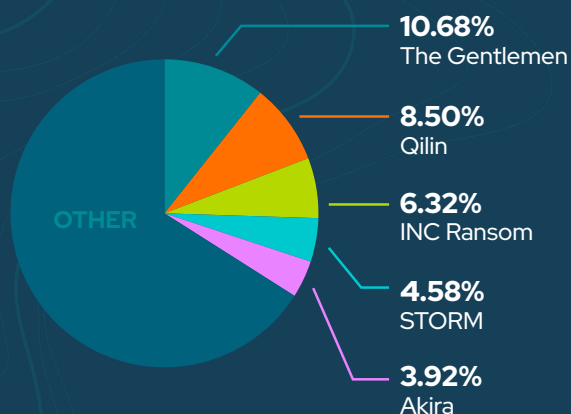
BYER-NICHOLS THREAT BRIEF

SECOND HALF SEPTEMBER 2026



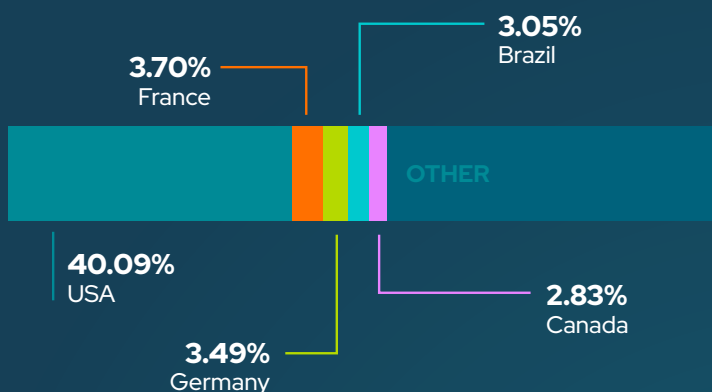
Late September reinforced how quickly threats are converging around trusted access. Ransomware remained active as The Gentlemen and Qilin led the field, while INC Ransom gained ground. At the same time, espionage groups leaned on identities, supply chains and exposed services, with AI-assisted cloud attacks adding a new wrinkle. Exploitation of SharePoint, NetScaler, Check Point, Cisco and F5 flaws makes rapid patching, identity security and post-compromise hunting key priorities.

TOP RANSOMWARE



The Gentlemen held first place at 10.68%, with Qilin close behind, continuing the two groups' sustained dominance; both were already leading victim disclosures in mid-September. INC Ransom was the biggest mover, jumping from ninth to third, while STORM rose to fourth and Akira held fifth. The wider picture remains fluid: newer crews such as STORM are gaining ground, while Akira continues to pose a concern through double extortion and VPN-driven access.

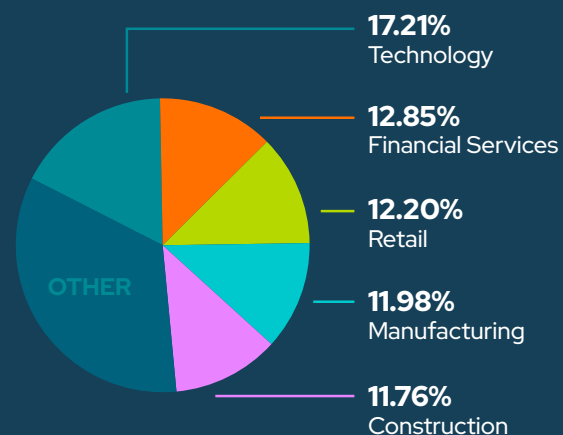
VICTIM LOCATIONS



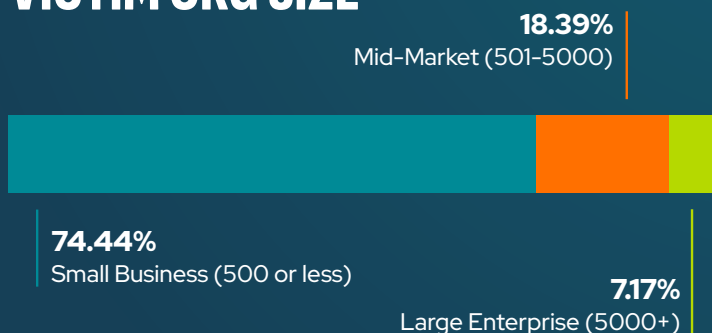
TOP NEWS

- Brevo supply-chain attack injected ClickFix scripts on customer sites
- Gyazo server flaw exploited to steal 23.6 million user records
- Microsoft disrupts EvilTokens device code phishing service
- Nightmare Eclipse defender zero-day blocks Microsoft antivirus updates
- New Settra ransomware variant deploys MeshAgent RMM
- Russian State hackers use new RedFlick technique to push malware
- Salesbleed abuses Salesforce agents for Slack phishing
- ShinyHunters hacks Clop leak site and threatens to extort The Gang

VICTIM SECTOR



VICTIM ORG SIZE



TRENDING & ACTIVELY EXPLOITED VULNERABILITIES

CVE	Vendor	Product
CVE-2026-65660	Microsoft	SharePoint
CVE-2026-71362	Adobe	Commerce and Magento
CVE-2026-76460	Cisco	Identity Services Engine
CVE-2026-76504	Cisco	Catalyst SD-WAN Manager
CVE-2026-85102	Check Point	Multiple Products
CVE-2026-86950	Apple	Multiple Products
CVE-2026-88771	Citrix	NetScaler
CVE-2026-88772	Citrix	NetScaler
CVE-2026-93616	Check Point	Multiple Products
CVE-2026-94127	F5	BIG-IP APM

This period's selected vulnerabilities concentrate on enterprise collaboration, commerce, identity, network management, and edge infrastructure. SharePoint, Adobe Commerce and Magento, Cisco ISE and SD-WAN, Check Point, Apple, Citrix NetScaler, and F5 BIG-IP all create high-value paths into widely deployed environments. Internet-facing management planes should lead the patch queue, especially where authentication bypass or active exploitation can turn one exposed appliance into broader network access.

TRENDING MALWARE

Carbonato

Carbonato compromises exposed Docker hosts and combines worm-like propagation with a Telegram-controlled AI agent that prioritizes credential theft.

NeedyMantis

NeedyMantis is a modular post-compromise malware framework built to maintain long-term, covert access to selected Windows environments.

PAYLOAD

PAYLOAD abuses Active Directory Group Policy to cause domain-wide disruption and support extortion, potentially without deploying Windows ransomware binaries.

Rapuncel

Rapuncel is a Windows infostealer that uses fake software downloads and a signed kernel driver to disable security products before stealing valuable credentials and data.

RatHat

RatHat is an Android banking trojan that combines Accessibility and ADB abuse with AI-assisted automation to steal credentials and remotely control compromised devices.

SparrowWocky

SparrowWocky is a stealthy modular Windows backdoor that gives cyberespionage operators extensive remote control, surveillance, and data-theft capabilities.

TRENDING ADVERSARIES

FamousSparrow

JadePuffer

NightEagle

Star Blizzard

Storm-3069

WaterPlum

Late September's adversaries were mostly established actors returning with new scale or tooling. FamousSparrow expanded Latin American government espionage with SparrowWocky, NightEagle broadened into Russian targets, and Star Blizzard streamlined phishing through RedFlick. JadePuffer pushed automation furthest with agentic ransomware, while Storm-3069 used NeedyMantis for persistent access and WaterPlum's fake-interview campaign reached at least 30,000 devices. The common thread is faster, more durable compromise through automation and trusted workflows.



PRODUCED & DISTRIBUTED BY
PHISH TANK DIGITAL



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



SUMMARIES & BIOS
GEOFF REHMET
Cybersecurity Expert