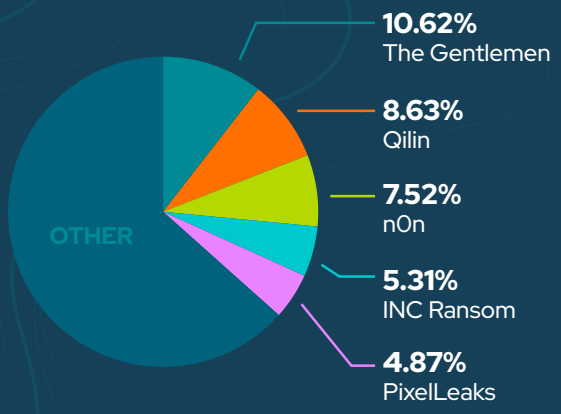
# BYER-NICHOLS THREAT BRIEF

phish tank DIGITAL

## FIRST HALF NOVEMBER 2026

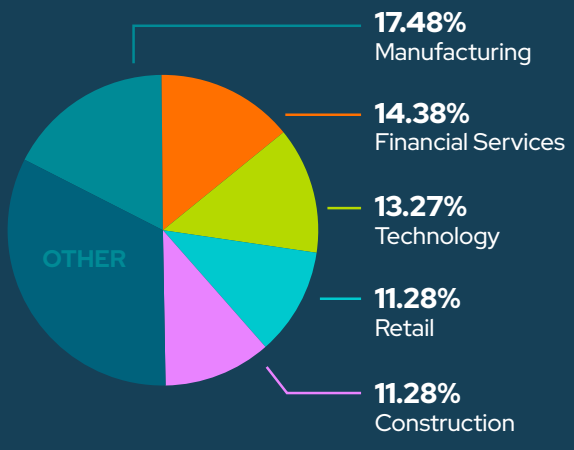
Early November brought continued high threat activity across ransomware, vulnerabilities, and malware. PixelLeaks entered the top five after listing 22 victims in roughly 10 days, while attackers targeted critical software and abused trusted cloud, browser, mobile, Linux, and remote-management tools.

## TOP RANSOMWARE

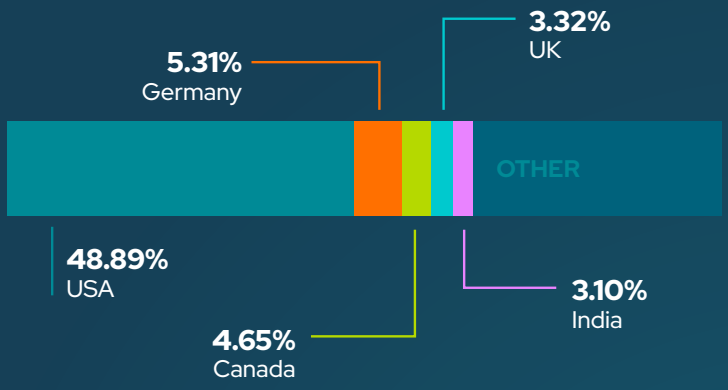



The Gentlemen retained first place at 10.62%, followed by Qilin at 8.63% and nOn at 7.52%, leaving the top three unchanged. INC Ransom moved from fifth to fourth with 5.31%. The main development was PixelLeaks, which entered the rankings in fifth place at 4.87% after listing 22 victims in roughly 10 days. Its immediate arrival among established operators makes the group the period's clearest ransomware watch item.

## VICTIM SECTOR



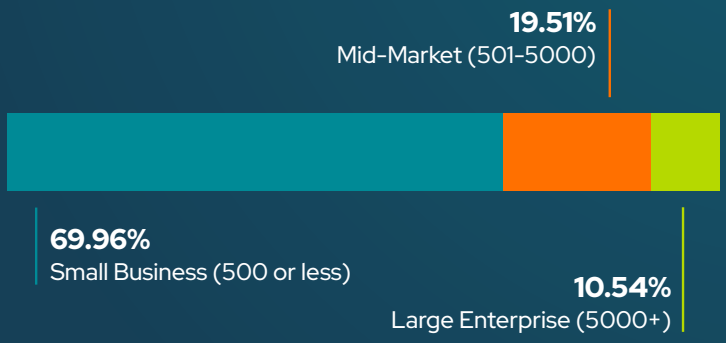

## VICTIM LOCATIONS




## TOP NEWS

- Binance says fake job interview led to $6.3 billion crypto heist
- Chinese hackers use ARTEX AI in automated attacks against 200 orgs
- eMudhra revokes 8 more CA certificates after private key mishap
- Google disrupts million-device XCPE Android malware botnet, bans TV box maker
- Hackers disrupt refrigeration systems at European supermarkets
- Massive Microsoft 365 outage disrupts Outlook, Teams, Copilot worldwide
- N-able disables cloud services following disclosure of "Able2Shell" exploit chains
- Police dismantle Gootloader, CastleRAT, StealC malware infrastructure

## VICTIM ORG SIZE



# TRENDING & ACTIVELY EXPLOITED VULNERABILITIES

| CVE | Vendor | Product |
|---|---|---|
| CVE-2026-111560 | Barracuda Networks | Multiple Products |
| CVE-2026-116606 | Barracuda Networks | Barracuda Email Security Gateway (ESG) |
| CVE-2026-116779 | SignalWire | FreeSwitch |
| CVE-2026-119977 | WordPress | WordPress Core |
| CVE-2026-123039 | Check Point | Multiple Products |
| CVE-2026-123218 | IBM | Aspera Faspex |
| CVE-2026-124194 | Microsoft | Office |
| CVE-2026-125350 | Google | Chromium |
| CVE-2026-19868 | SonicWall | SonicOS SSLVPN |
| CVE-2026-20320 | Cisco | BroadWorks |

The vulnerability volume remained unusually high, with more additions than a short brief could fully capture. This selected list prioritizes 10 actively exploited or high-impact flaws affecting Barracuda appliances, FreeSwitch, WordPress, Check Point, IBM Aspera Faspex, Microsoft Office, Chromium, SonicWall SSLVPN, and Cisco BroadWorks. Email, communications, browsers, and internet-facing infrastructure should lead remediation, followed by credential rotation and compromise hunting where exposed systems may have been reachable before patching.

# TRENDING MALWARE

**Antino**
Antino is a Rust-based Windows backdoor that uses Microsoft 365 services for command-and-control, file transfer, persistence, and covert espionage activity.

**ArcticRAT**
ArcticRAT is an AI-assisted Android remote-access trojan that targets cryptocurrency and financial data while enabling extensive surveillance and device control.

**Falcon C2**
Falcon C2 is a browser-based command-and-control framework that uses injected JavaScript and malicious extensions to steal sessions, communications, and credentials.

**RelayTrap**
RelayTrap hijacks legitimate ScreenConnect connection details to impersonate managed endpoints and target technicians for credential theft and lateral movement.

**SANSAR**
SANSAR is a Rust-based Linux cryptomining orchestrator that hides CPU and GPU theft through Tor, a kernel rootkit, and falsified monitoring data.

**SCKit**
SCKit abuses ScreenConnect environments to install rogue remote-access clients, persist on managed endpoints, and attempt technician-driven propagation.

# TRENDING ADVERSARIES

**APT29** | **SilentAir** | **TraderTraitor**
**Gorbag** | **SlippyNunchucks** | **Turla**

Early November's adversaries combined espionage, financial theft, supply-chain compromise, and abuse of trusted software. APT29 used compromised web infrastructure to support mobile exploitation, while Gorbag and SlippyNunchucks relied on familiar software and delivery channels to reach targets. TraderTraitor remained focused on cryptocurrency operations, and SilentAir and Turla continued stealth-focused campaigns. Across the set, the recurring risk is malicious activity hidden inside legitimate services, applications, and normal administrative traffic.

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