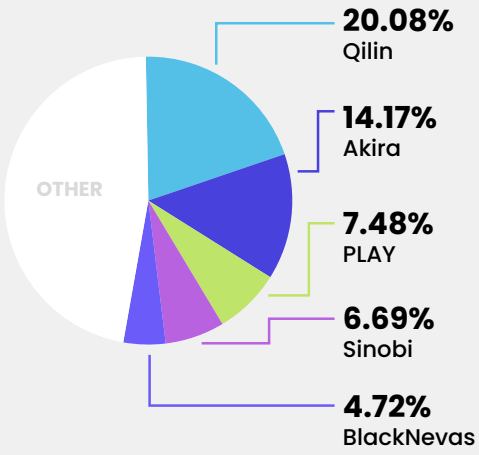
BYER-NICHOLS THREAT BRIEF

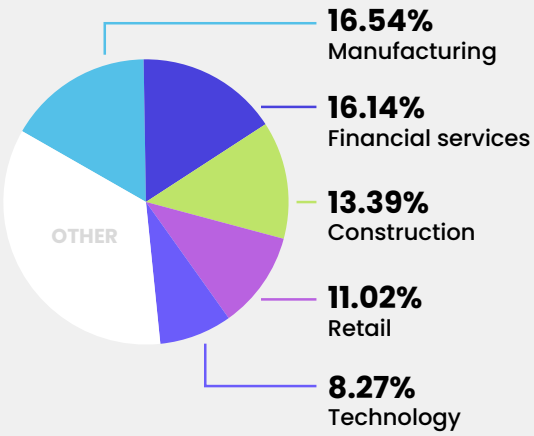
FIRST HALF AUGUST 2025

Small businesses continue to dominate the ranks of breach victims at 84.25%. When we consider that small businesses represent about half of employment globally and about 44% of US GDP they fall victim to more than their fair share of cyber-attacks. This is a symptom of the fact that many SMBs lag larger enterprises in their security posture and capabilities. Lacking the financial resources of large enterprises, a cyber breach is also more likely to put an SMB out of business. Smaller businesses must focus on addressing cyber risk — their survival depends on it.

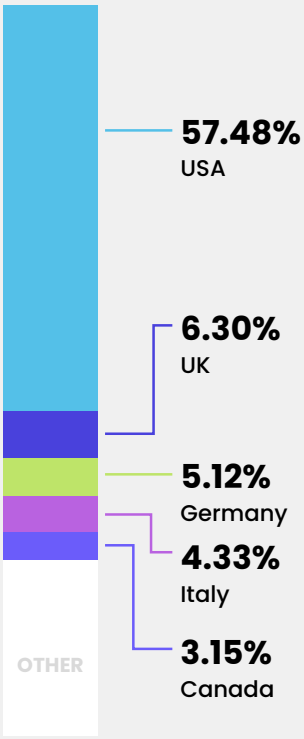
Top ransomware



Victim sector



Victim locations



Victim org size

Trending malware

4L4MD4R

A newly discovered ransomware, based on open source code. It spreads via a failed PowerShell attack and demands a ransom of 0.005 BTC. This malware is written in GoLang and compressed using UPX. It is based on the open source Mauri870 code.

EDRKillShifter

There have been renewed reports of threat actors using malware to disable Endpoint Detection and Response (EDR) in order to remain undetected. One notable example appears to be an evolution of EDRKillShifter, which was developed by RansomHub.

MucorAgent

A Russian-aligned group known as Curly COMrades has been targeting judicial and government bodies, mainly in Eastern Europe. As part of their efforts to maintain persistence they have been deploying the MucorAgent backdoor. They are targeting Domain Controllers to extract user credentials.

SparkKitty

iOS and Android phones are the target of SparkKitty, which sends images and information from an infected phone to the attacker.

Plague

Plague is a backdoor that specifically targets the authentication framework of Linux, disguising itself as a Pluggable Authetication Module (PAM). The design of hijacking the system that authenticates users makes this malware difficult to detect and resistant to removal.

XZ backdoor

While this backdoor is not new, it has recently resurfaced when researchers discovered dozens of container images in Docker Hub containing infected versions of XZ Utils.

Top news

- Critical zero-day bugs crack open CyberArk, HashiCorp password vaults
- Hacker extradited to US for stealing $3.3 million from taxpayers
- Microsoft pays record $17 million in bounties over the last 12 months, increases Zero Day Quest prize pool to $5 million
- New 'Shade BIOS' Technique Beats Every Kind of Security
- New Ghost Calls tactic abuses Zoom and Microsoft Teams for C2 operations
- ShinyHunters Tactics now Mirror Scattered Spider
- SonicWall urges admins to disable SSL VPN amid rising attacks
- Over $300 million in cybercrime crypto seized in anti-fraud effort

Trending adversaries

Curly COMrades **ShinyHunters** **Violet Typhoon**

Linen Typhoon **Storm-2603**

Active vulnerabilities

CVE	VENDOR	PRODUCT
CVE-2020-25078	D-Link	DCS-2530L & DCS-2670L Devices
CVE-2020-25079	D-Link	DCS-2530L & DCS-2670L Devices
CVE-2022-40799	D-Link	DNR-322L
CVE-2025-25256	Fortinet	FortiSIEM
CVE-2025-53786	Microsoft	Exchange
CVE-2025-54948	Trend Micro	Apex One
CVE-2025-54987	Trend Micro	Apex One
CVE-2025-8088	RARLAB	WinRAR
CVE-2025-8875	N-able	N-Central
CVE-2025-8876	N-able	N-Central

Among ransomware actors, Qilin has solidified its position in first place, growing from 13% to just over 20% of attacks. Akira has also strengthened its position, moving to number 2 with just over 14% of attacks (up from just under 10%). The remaining positions in the top 5 ransomware actors are taken by new players: PLAY, Sinobi and BlackNevas. BlackNevas, a crypto-ransomware actor also known as Trial_Recovery, while first seen in September 2024, is notable for its recent reappearance after a hiatus of several months.

Amongst trending adversaries, it is worth noting Curly COMrades, which is an APT group with apparent links to the Russian Federation. The name "Curly COMrades" is derived from their use of curl.exe for Command and Control (C2) communications and data exfiltration. Their main targets appear to be in Eastern Europe, particularly organizations in EU-aspirant nations Moldova and Georgia. Once they infiltrate a network they set up multiple reverse proxy tunnels to relays under their control. These tunnels are ultimately used to exfiltrate data, apparently for espionage purposes. Indicators of Compromise and TTPs are listed in Bitdefender's report and can be used to create detection rules. While targets are currently primarily in Georgia and Moldova, Russian groups are notorious for targeting any country that supports Ukraine.

Vulnerabilities that warrant attention include 3 affecting D-Link equipment and dating back to 2020 and 2022 (CVE-2020-25078, CVE-2020-25079, CVE-2022-40799). Of particular concern is a recently announced high-severity vulnerability in on-premises Microsoft Exchange Server 2019 deployments (CVE-2025-53786). Microsoft strongly recommends that affected organizations promptly apply hotfixes which were provided in April 2025. Organizations with vulnerable systems exposed to the Internet should consider isolating them until they are patched.

BYER CO

WRITTEN BY JEREMY NICHOLS, FORMER DIRECTOR OF THE GLOBAL THREAT INTELLIGENCE CENTER

EXECUTIVE SUMMARIES & ADVERSARY BIO'S BY GEOFF REHMET, CYBERSECURITY EXPERT

PRODUCED & DISTRIBUTED BY BYER CO'S CYBERSECURITY MARKETING DIVISION