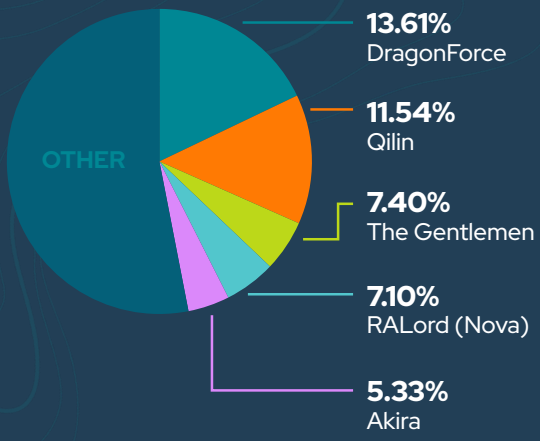
BYER-NICHOLS THREAT BRIEF

SECOND HALF MAY 2026

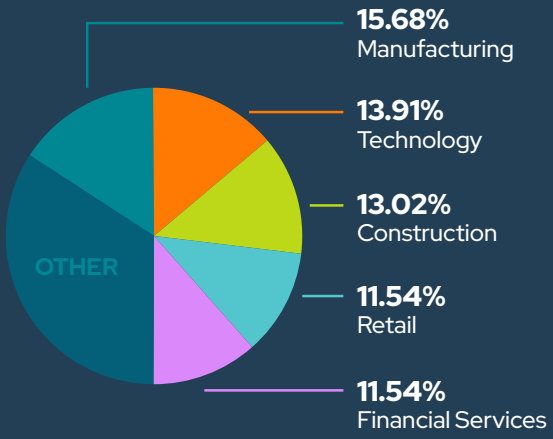
Activity remained relatively routine overall, though a few ransomware groups saw notable movement. DragonForce returned to the top five most active ransomware operators after another surge in victim postings, continuing its pattern of alternating between quiet periods and sudden spikes in activity. RALord (Nova) also broke into the top five for the first time after posting an unusually high number of victims compared to its typical volume. On the vulnerability front, CISA added more than 15 new Known Exploited Vulnerabilities (KEVs), highlighting the continued pace at which actively exploited flaws are being identified and tracked.

TOP RANSOMWARE

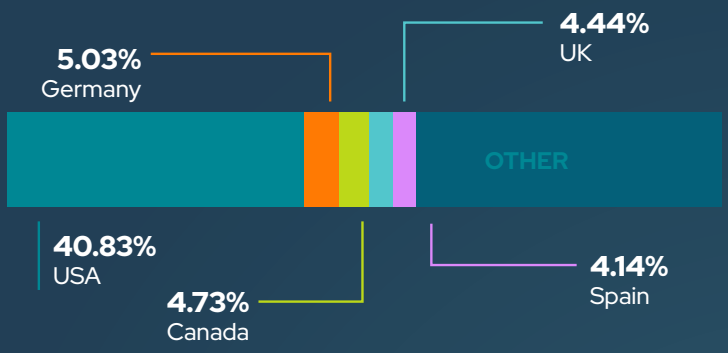


DragonForce emerged as the most active ransomware group during the period, followed by Qilin and The Gentlemen. RALord (Nova) made a notable appearance in the top rankings, while Akira remained a consistent threat actor.

VICTIM SECTOR



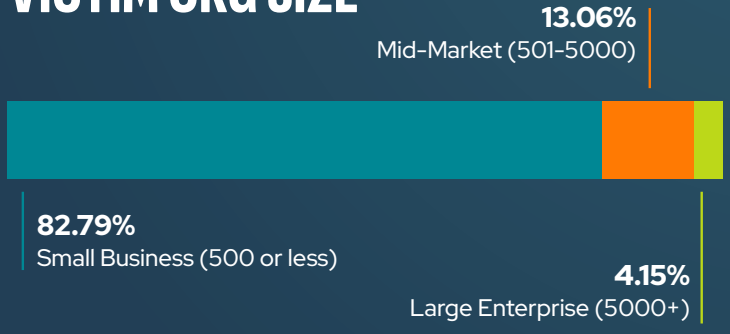
VICTIM LOCATIONS



TOP NEWS

- CISA exposes secrets, credentials in 'Private' repo
- Dutch government disrupts malware botnet with 17 million infected devices
- Fake FIFA sites target soccer fans looking for World Cup tickets to steal money and data
- Google API Keys remain active after deletion
- Grafana says stolen GitHub token let hackers steal codebase
- Hackers earn $1,298,250 for 47 zero-days at Pwn2Own Berlin 2026
- Microsoft rejects critical Azure vulnerability report, no CVE issued
- Tables turn on 'The Gentlemen' RaaS gang with data leak

VICTIM ORG SIZE



TRENDING & ACTIVELY EXPLOITED VULNERABILITIES

CVE	Vendor	Product
CVE-2025-34291	Langflow	Langflow
CVE-2026-0257	Palo Alto Networks	PAN-OS
CVE-2026-34926	Trend Micro	Apex One
CVE-2026-41091	Microsoft	Defender
CVE-2026-45321	TanStack	TanStack
CVE-2026-45498	Microsoft	Defender
CVE-2026-48027	Nx	Nx Console
CVE-2026-48172	LiteSpeed	cPanel Plugin
CVE-2026-8398	Daemon	Daemon Tools Lite
CVE-2026-9082	Drupal	Core

Actively exploited vulnerabilities impacted widely used enterprise technologies including PAN-OS, Microsoft Defender, Apex One, Drupal, and Langflow. The diversity of affected platforms underscores the importance of timely patching across security, infrastructure, and application environments.

TRENDING MALWARE

EchoCreep
A Discord-based backdoor used by China-nexus operators to run commands, move files, and quietly maintain long-term access under the cover of normal collaboration traffic.

GraphWorm
A Go-based backdoor that hides C2 inside Microsoft Graph and OneDrive activity, enabling stealthy command execution and data exfiltration through trusted cloud services.

PHANTOMPULSE
A cross-platform RAT delivered via malicious Obsidian vaults that uses blockchain and messaging-app infrastructure for resilient C2 and stealthy, plugin-driven execution.

Showboat
A Linux post-exploitation toolkit used in telecom intrusions to provide remote shells, proxying, and covert persistence for long-running espionage operations.

SHub Reaper
A macOS infostealer/backdoor that abuses AppleScript and fake vendor prompts to steal credentials, browser data, and crypto assets while evading built-in protections.

TamperedChef
A malvertising-driven infostealer campaign that ships trojanized productivity apps with long-dormant payloads designed to harvest credentials and maintain quiet persistence.

TRENDING ADVERSARIES

Bling Libra | **Cloud Atlas** | **Secret Blizzard**
Chatty Spider | **Screening Serpens** | **Webworm**

Threat activity remained diverse this period, with groups including Bling Libra, Chatty Spider, Cloud Atlas, Screening Serpens, Secret Blizzard, and Webworm continuing to employ a mix of social engineering, credential theft, espionage, and network intrusion tactics. Their ongoing operations highlight the persistent risk posed by both financially motivated cybercriminals and state-linked threat actors targeting organizations across multiple sectors.

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