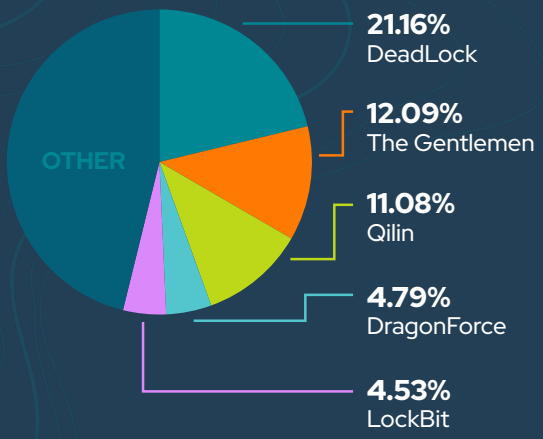
BYER-NICHOLS THREAT BRIEF

FIRST HALF JUNE 2026

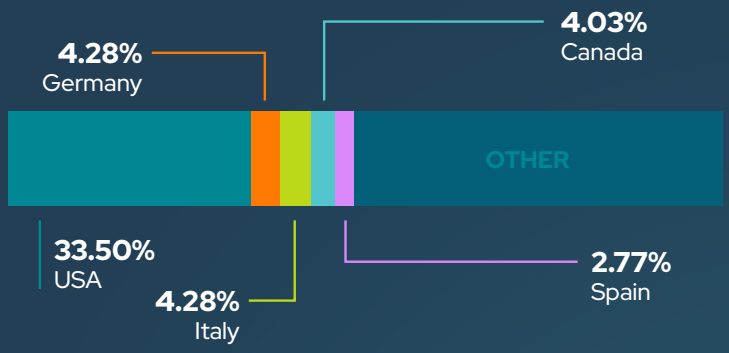
Threat activity in early June picked up across the board, with new malware families, faster cloud-pivoting intrusions, and a fresh wave of actively exploited vulnerabilities driving most of the noise. DeadLock's sudden rise, Shadow-Earth-066's automation push, and widespread credential-theft campaigns all signaled a shift toward speed and stealth. Meanwhile, zero-days in WebLogic, Android, and Cisco SD-WAN kept pressure on defenders to patch fast and watch identity systems closely.

TOP RANSOMWARE



DeadLock dominated early June with a sharp debut, driving over a fifth of observed activity and drawing attention for its fast-moving double-extortion playbook. The Gentlemen and Qilin continued their steady climb, each expanding victim lists through tailored phishing and opportunistic exploitation. DragonForce surged back into relevance after months of quiet, pairing data-leak pressure with noisy DDoS-style harassment. LockBit, though diminished, still surfaced in several opportunistic hits, showing the brand's resilience despite sustained law-enforcement pressure.

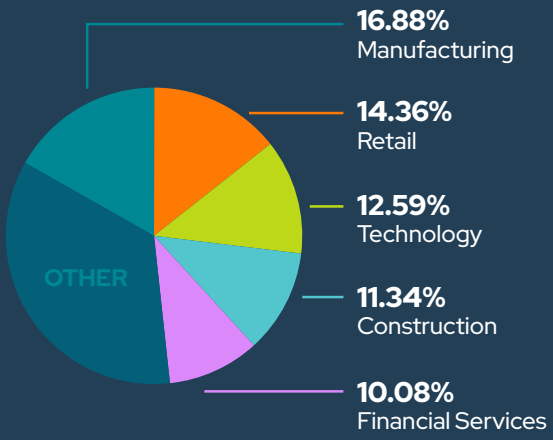
VICTIM LOCATIONS



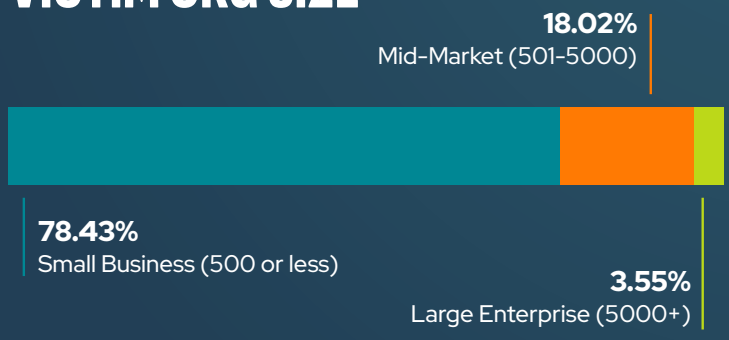
TOP NEWS

- Compromised Red Hat employee GitHub account leveraged in npm supply chain attack
- Coding Gaffe exposes Microsoft 365 accounts to widespread takeover
- FBI dismantled a massive Chinese phishing-as-a-service operation called Outsider Enterprise
- Microsoft Exchange "Ghost-Sender" flaw lets attackers spoof any email address, Microsoft Defender 'RoguePlanet' zero-day grants SYSTEM privileges
- Oracle PeopleSoft servers hacked in ShinyHunters data theft attacks
- Over 116,000 Minecraft systems infected in WeedHack malware campaign
- US government asks Anthropic to ban 'foreign national' access to Fable, Mythos
- VS Code zero-day lets hackers steal GitHub tokens in one click, Copilot 'SearchLeak' attack allows 1-click data theft

VICTIM SECTOR



VICTIM ORG SIZE



TRENDING & ACTIVELY EXPLOITED VULNERABILITIES

CVE	Vendor	Product
CVE-2024-21182	Oracle	WebLogic Server
CVE-2025-48595	Android	Framework
CVE-2026-10520	Ivanti	Sentry
CVE-2026-11645	Google	Chromium V8
CVE-2026-20245	Cisco	Catalyst SD-WAN Manager
CVE-2026-20262	Cisco	Catalyst SD-WAN Manager
CVE-2026-28318	SolarWinds	Serv-U
CVE-2026-35273	Oracle	PeopleSoft Enterprise PeopleTools
CVE-2026-42271	BerriAI	LiteLLM
CVE-2026-50751	CheckPoint	Security Gateway

Early June saw active exploitation span legacy middleware, mobile, network edge, and even AI tooling. WebLogic CVE-2024-21182 and Android CVE-2025-48595 are confirmed in-the-wild, enabling unauthenticated or elevated access, while fresh bugs in Ivanti Sentry, Chromium V8, Cisco SD-WAN, Serv-U, PeopleSoft, LiteLLM, and Check Point gateways widen the attack surface for RCE and tenant escape. Defenders should prioritize KEV-listed flaws, patch internet-facing services first, lock down management ports, and hunt for post-compromise activity in logs and EDR.

TRENDING MALWARE

Argamal RAT
A stealthy Windows RAT delivered through trojanized game installers that uses COM hijacking and sandbox-aware loaders to maintain long-term remote access.

Azureveil
Cloud-blending espionage backdoor that uses Azure Blob Storage dead-drops and Rust-based loaders to quietly exfiltrate data from targeted government networks.

FlutterShell
A cross-platform Flutter-based backdoor deployed via the FlutterBridge loader that enables covert command execution and file operations across major OS platforms.

GiftedCrook
A credential-stealing malware spread through CVE-2023-38831 WinRAR exploits that harvests browser data and messaging credentials for follow-on intrusion activity.

Miasma
A rapid-propagation supply-chain worm that compromises GitHub repositories and CI/CD pipelines by injecting malicious commits and stealing developer credentials.

NFCShare
An Android malware family that abuses NFC-based file-sharing prompts to install trojanized apps that exfiltrate device data and enroll victims into mobile botnets.

TRENDING ADVERSARIES

CL-CRI-1089
DriveSurge
Shadow-Earth-066
TA4922
UNC3753
Velvet Ant

CL-CRI-1089, DriveSurge, Shadow-Earth-066, TA4922, UNC3753, and Velvet Ant all pushed more aggressive credential-theft and cloud-pivoting activity this period, with most leaning on living-off-the-land techniques to stay quiet once inside. Several groups mixed commodity loaders with bespoke post-exploitation tooling, blurring attribution and speeding up lateral movement. TA4922 and UNC3753 stood out for targeting identity providers directly, while Velvet Ant kept refining its long-haul persistence in hybrid environments. The most concerning is Shadow-Earth-066, whose rapid shift to automation-driven reconnaissance suggests it's gearing up for broader, faster intrusions that defenders will need to detect early.

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