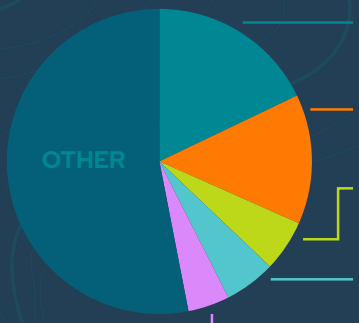
BYER-NICHOLS THREAT BRIEF

FIRST HALF MAY 2026

The first half of May was relatively routine overall, with ransomware activity continuing to heavily impact small businesses, which accounted for 79.06% of victims. Construction, retail, and financial services emerged as the most targeted sectors, while the United States remained the primary victim location at 45.08%. One notable development was the sudden emergence of Bavacai as a new ransomware-as-a-service (RaaS) operation, rapidly entering the top five ransomware actors after posting roughly 20 victims on May 6 before going quiet for the remainder of the reporting period.

TOP RANSOMWARE



17.88% Qilin

13.73% The Gentlemen

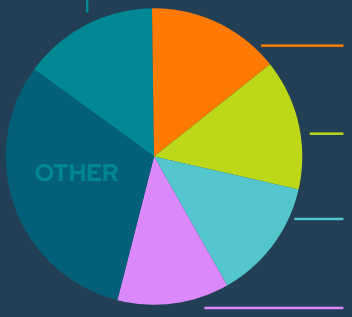
5.44% INC Ransom

5.44% Akira

4.40% Bavacai

Qilin surged to the top spot again in early May, continuing its high-volume double-extortion hits, while The Gentlemen stayed close behind with a steady stream of opportunistic breaches and fast leak-site turnarounds. INC Ransom kept up pressure on healthcare and professional services, and Akira resurfaced with renewed targeting of mid-market firms after a brief lull. Newcomer Bavacai drew attention with unusually noisy data-theft-first intrusions, making this period notable for both persistence from established crews and experimentation from emerging ones.

VICTIM SECTOR



14.77% Construction

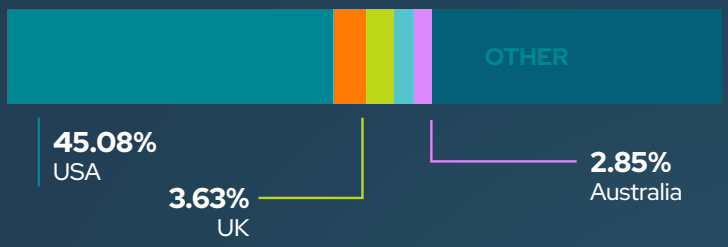
14.51% Retail

14.25% Financial Services

13.21% Technology

12.18% Manufacturing

VICTIM LOCATIONS



4.15% Canada

2.85% Italy

45.08% USA

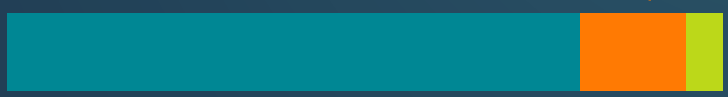
3.63% UK

2.85% Australia

TOP NEWS

- New Bluekit phishing service includes an AI assistant, 40 templates
- 76% of All Crypto Stolen in 2026 is now in North Korea
- Canvas login portals hacked in mass ShinyHunters extortion campaign
- DAEMON Tools trojanized in supply-chain attack to deploy backdoor
- New Linux 'Dirty Frag' zero-day gives root on all major distros
- Microsoft Edge stores passwords in process memory, posing enterprise risk
- Trellix source code breach claimed by RansomHouse hackers
- US ransomware negotiators get 4 years in prison over BlackCat attacks, Karakurt extortion gang 'cold case' negotiator gets 8.5 years in prison

VICTIM ORG SIZE



14.92% Mid-Market (501-5000)

79.06% Small Business (500 or less)

6.02% Large Enterprise (5000+)

TRENDING & ACTIVELY EXPLOITED VULNERABILITIES

CVE	Vendor	Product
CVE-2026-0300	Palo Alto Networks	PAN-OS
CVE-2026-20182	Cisco	Catalyst SD-WAN
CVE-2026-22679	Weaver	E-cology
CVE-2026-31431	Linux	Kernel
CVE-2026-42208	BerriAI	LiteLLM
CVE-2026-42897	Microsoft	Microsoft
CVE-2026-43284	Linux	Kernel (Dirty Frag)
CVE-2026-43500	Linux	Kernel (Dirty Frag)
CVE-2026-4670	Progress Software	MOVEit Automation
CVE-2026-6973	Ivanti	Endpoint Manager Mobile (EPMM)

Attackers heavily targeted enterprise infrastructure and edge technologies this period, with vulnerabilities impacting PAN-OS, Cisco SD-WAN, Linux Kernel, MOVEit Automation, and Microsoft products. Multiple Linux "Dirty Frag" vulnerabilities appearing simultaneously indicates increased focus on privilege escalation and infrastructure compromise.

TRENDING MALWARE

TCLBANKER
A fast-moving Brazilian banking trojan that spreads via trojanized installers and messaging-app worms to steal financial credentials through real-time browser monitoring and operator-driven overlays.

Beagle Backdoor
A Windows backdoor delivered through AI-themed malvertising that collects system data, establishes persistence, and enables follow-on payload delivery through a remote C2 channel.

BirdCall
An Android espionage tool from ScarCruft that abuses accessibility services to capture keystrokes, screen content, and messaging data through encrypted, modular C2 communications.

CloudZ A modular infostealer tied to the Pheno group that harvests browser data, credentials, and crypto-wallet information while using custom protocols and evasion tactics to avoid detection.

PCPJack
A cloud-propagating worm that compromises exposed services, steals data, and repurposes victim infrastructure to fuel further spread across cloud environments.

ZiChatBot
A PyPI-delivered Python malware linked to OceanLotus that masquerades as chat libraries to deploy second-stage payloads for system profiling and espionage operations.

TRENDING ADVERSARIES

CORDIAL SPIDER | **OceanLotus** | **SNARKY SPIDER**
HeartlessSoul | **ScarCruft** | **UAT-8302**

CORDIAL SPIDER, HeartlessSoul, OceanLotus, ScarCruft, SNARKY SPIDER, and UAT-8302 all leaned into stealthy credential theft, mobile-focused espionage, and supply-chain abuse this period, with OceanLotus standing out as the most concerning thanks to its polished developer-ecosystem compromises and long-term persistence. Several groups pushed cleaner loaders, tighter C2 discipline, and more social-engineering-driven delivery, while ScarCruft and HeartlessSoul expanded mobile surveillance tooling. The common thread is quieter, data-centric operations that blend into normal traffic, making early detection harder and forcing defenders to double down on identity controls and telemetry depth.

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