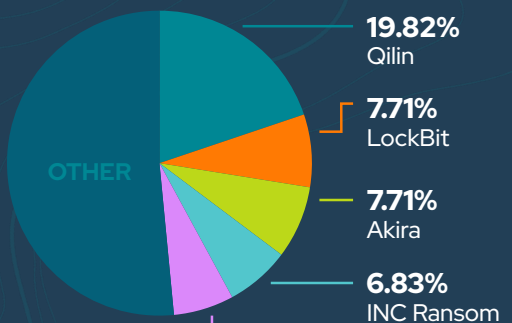
BYER-NICHOLS THREAT BRIEF

FIRST HALF MARCH 2026

Ransomware activity in early March 2026 remained fragmented, led by Qilin with continued pressure across manufacturing, technology, and construction sectors, while small businesses made up the vast majority of victims. The threat landscape featured a mix of established and emerging adversaries, alongside active exploitation of vulnerabilities across major platforms like Apple, Google, and enterprise software, reinforcing a broad, opportunistic attack environment.

TOP RANSOMWARE



19.82% Qilin

7.71% LockBit

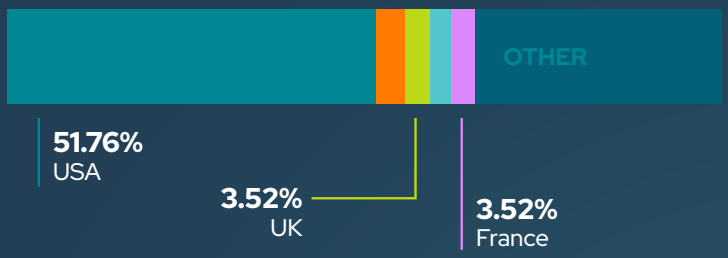
7.71% Akira

6.83% INC Ransom

6.39% DragonForce

Qilin led ransomware activity at 19.82%, maintaining its top position, while LockBit, Akira, and INC Ransom showed continued presence despite shifts in ranking. DragonForce also remained active, indicating a fragmented but competitive threat landscape.

VICTIM LOCATIONS



3.74% Germany

3.52% Canada

51.76% USA

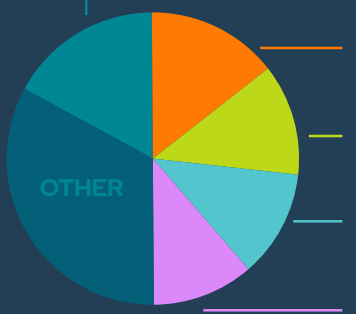
3.52% UK

3.52% France

TOP NEWS

- Compromised Site Management Panels are a Hot Item in Cybercrime Markets
- CyberStrikeAI tool adopted by hackers for AI-powered attacks
- Drone strikes damaged AWS data centers in Middle East
- Europol-coordinated action disrupts Tycoon2FA phishing platform
- Fake Claude Code install guides push infostealers in InstallFix attacks
- FBI seizes LeakBase cybercrime forum, data of 142,000 members
- Google says 90 zero-days were exploited in attacks last year, paid $17.1 million for vulnerability reports in 2025
- ShinyHunters claims ongoing Salesforce Aura data theft attacks

VICTIM SECTOR



16.96% Manufacturing

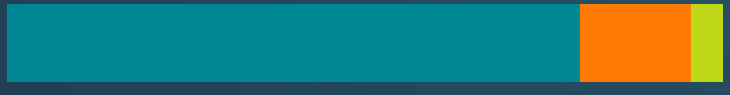
14.54% Technology

12.33% Construction

11.89% Financial Services

11.23% Retail

VICTIM ORG SIZE



13.50% Mid-Market (501-5000)

82.08% Small Business (500 or less)

4.42% Large Enterprise (5000+)

TRENDING & ACTIVELY EXPLOITED VULNERABILITIES

CVE	Vendor	Product
CVE-2021-30952	Apple	Multiple Products
CVE-2023-41974	Apple	iOS and iPadOS
CVE-2023-43000	Apple	Multiple Products
CVE-2025-26399	SolarWinds	Web Help Desk
CVE-2025-68613	n8n	n8n
CVE-2026-1603	Ivanti	Endpoint Manager (EPM)
CVE-2026-21385	Qualcomm	Multiple Chipsets
CVE-2026-22719	Broadcom	VMware Aria Operations
CVE-2026-3909	Google	Skia
CVE-2026-3910	Google	Chromium V8

Actively exploited vulnerabilities span major vendors including Apple, Google, Ivanti, and VMware, indicating widespread targeting of both enterprise systems and consumer technologies.

TRENDING MALWARE

A0Backdoor
Lightweight backdoor used for persistent access and remote command execution on compromised systems.

BadPaw Loader
Malware loader designed to deliver additional payloads, often used as an initial infection vector.

BlackSanta
Backdoor malware associated with data theft and system control, typically deployed post-compromise.

GhostSocks
Proxy-based malware that routes attacker traffic through infected machines to obscure origin.

KadNap Botnet
Botnet malware used to control large networks of infected devices for coordinated attacks.

MeowMeow Backdoor
Backdoor enabling unauthorized access and potential data exfiltration from compromised hosts.

TRENDING ADVERSARIES

APT28
Handala
ShinyHunters
Silver Dragon
UAT-9244
UNC6426

Multiple adversaries including APT28, ShinyHunters, and UNC6426 were active, reflecting a mix of established and emerging threat actors operating simultaneously across campaigns.

phish tank DIGITAL

PRODUCED & DISTRIBUTED BY
PHISH TANK DIGITAL

WRITTEN BY
JEREMY NICHOLS
Former Director of the Global Threat Intelligence Center

SUMMARIES & BIOS
GEOFF REHMET
Cybersecurity Expert