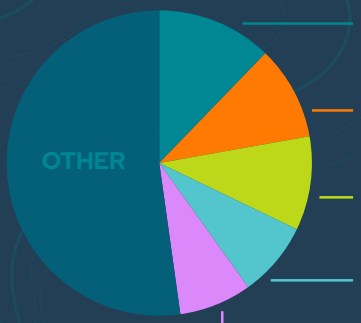
BYER-NICHOLS THREAT BRIEF

FIRST HALF APRIL 2026

Early April saw ransomware crews reshuffle, with DragonForce surging and LockBit showing a stubborn rebound. Infostealers and RATs stayed busy, from CrystalRAT and OmniStealer to Storm's server-side credential theft. Nationstate and criminal actors alike leaned on fast exploitation of fresh bugs, making rapid patching and tighter monitoring of exposed services the top defensive priorities.

TOP RANSOMWARE



12.18% DragonForce

9.92% The Gentlemen

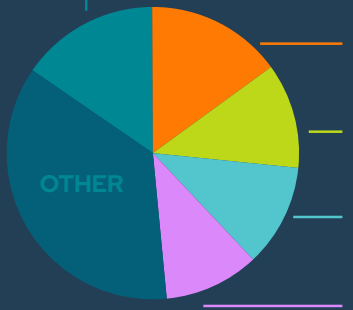
9.92% Akira

7.93% Qilin

7.65% Lockbit

DragonForce leads early April with a sharp rise in activity, leaning on fastmoving doubleextortion hits, while The Gentlemen continue their swingy pattern with a mix of midmarket manufacturing and services victims. Akira remains steady, sticking to its trademark VPNbased intrusions and quickturn encryption playbook, and Qilin stays active but selective, favoring data-theft extortion. LockBit, despite law enforcement pressure, shows a notable rebound driven by affiliates retooling infrastructure and resurfacing with fresh leaksite activity.

VICTIM SECTOR



15.30% Manufacturing

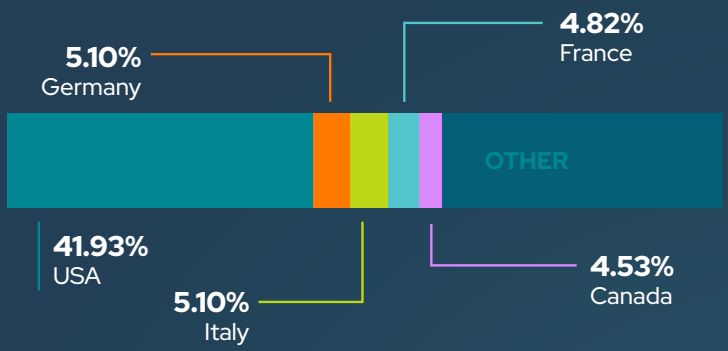
15.01% Technology

11.61% Construction

11.33% Financial Services

10.48% Retail

VICTIM LOCATIONS



5.10% Germany

4.82% France

41.93% USA

5.10% Italy

4.53% Canada

TOP NEWS

- Americans lost a record $21 billion to cybercrime last year
- Claude Code leak used to push infostealer malware on GitHub
- Device code phishing attacks surge 37x as new kits spread online
- FBI takedown of W3LL phishing service leads to developer arrest, German authorities identify REvil and GandCrab ransomware bosses
- Disgruntled researcher leaks "BlueHammer" Windows zero-day exploit
- New EvilTokens service fuels Microsoft device code phishing attacks
- New GPUBreach attack enables system takeover via GPU rowhammer
- Traffic violation scams switch to QR codes in new phishing texts, New VENOM phishing attacks steal senior executives' Microsoft logins

VICTIM ORG SIZE

17.29% Mid-Market (501-5000)

76.08% Small Business (500 or less)

6.63% Large Enterprise (5000+)

TRENDING & ACTIVELY EXPLOITED VULNERABILITIES

CVE	Vendor	Product
CVE-2020-9715	Adobe	Acrobat
CVE-2023-21529	Microsoft	Exchange Server
CVE-2023-36424	Microsoft	Windows
CVE-2025-60710	Microsoft	Windows
CVE-2026-1340	Ivanti	Endpoint Manager Mobile (EPMM)
CVE-2026-21643	Fortinet	FortiClient EMS
CVE-2026-34621	Adobe	Acrobat & Reader
CVE-2026-3502	TrueConf	Client
CVE-2026-35616	Fortinet	FortiClient EMS
CVE-2026-5281	Google	Dawn

Attackers are leaning hard on old and new flaws across Acrobat, Exchange, Windows, Ivanti Endpoint Manager Mobile, Fortinet's FortiClient management servers, TrueConf clients, and Google's Dawn platform, using them for quick, reliable initial access. The big worry is how a single malicious PDF or exposed management console can turn into full domain compromise. Fast patching, tighter email and PDF filtering, and close monitoring of management servers are the key moves for defenders right now.

TRENDING MALWARE

CrystalRAT
A polished malware-as-a-service RAT that blends credential theft, surveillance features, and antianalysis tricks while distracting victims with screenmanipulation pranks.

LucidRook
A Luabased stager used in targeted spearphishing that performs deep system reconnaissance and encrypted data exfiltration while evading detection through modular payload loading.

NoVoice
A large-scale Android rootkit campaign that used Playstore trojans and 22 exploits to gain persistent device level control and steal sensitive data even after factory resets.

OmniStealer
A multiplatform infostealer that hides its payload chain across blockchains and targets browsers, password managers, and cryptowallet extensions for broad credential theft.

Storm Infostealer
A next-generation stealer that bypasses endpoint protections by exfiltrating encrypted browser credential stores for server side decryption and seamless session hijacking.

STX RAT
A stealthy remote access trojan that delivers in-memory payloads, evades analysis with strong cryptography, and provides attackers with hidden VNCstyle control and credential harvesting.

TRENDING ADVERSARIES

APT41
CyberAv3ngers
Storm-1175
UAT-10362
UAT-10608
UNC6783

APT41, CyberAv3ngers, Storm1175, UAT10362, UAT10608, and UNC6783 are all leaning hard on fast exploitation of internet-facing systems, with several jumping on fresh Ndays to get quick footholds. APT41 remains the most agile, while CyberAv3ngers keep hammering OT gear with simple but effective tactics. Storm1175's rapid ransomware pivots raise the highest operational risk, and the UAT clusters continue targeted phishing and automated credential harvesting. The shared trend is speed—defenders need tighter patch cycles and stronger external surface monitoring.

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