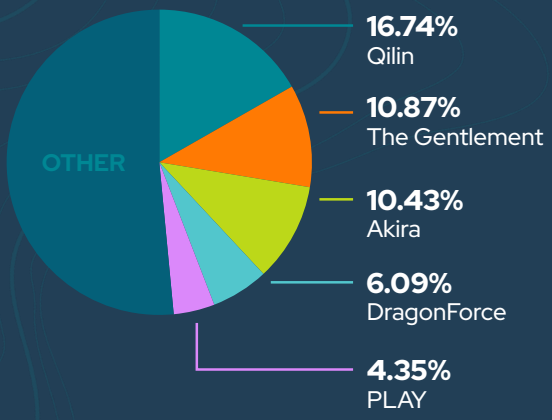
BYER-NICHOLS THREAT BRIEF

SECOND HALF MARCH 2026

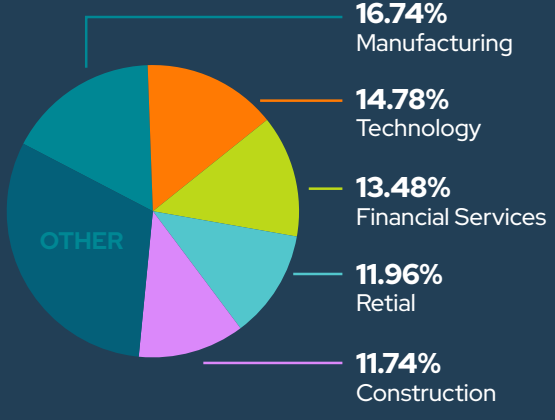
Threat activity spiked as APT36, TA446, and UNC1069 leaned into credential theft and cloud-identity abuse, while Bearlyfy escalated politically driven ransomware. Silver Fox and TeamPCP pushed opportunistic access and data theft, and major exploits hit Apple, F5, Cisco, SharePoint, and NetScaler. Priorities for defenders include identity hardening, rapid patching, and post-compromise hunting.

TOP RANSOMWARE

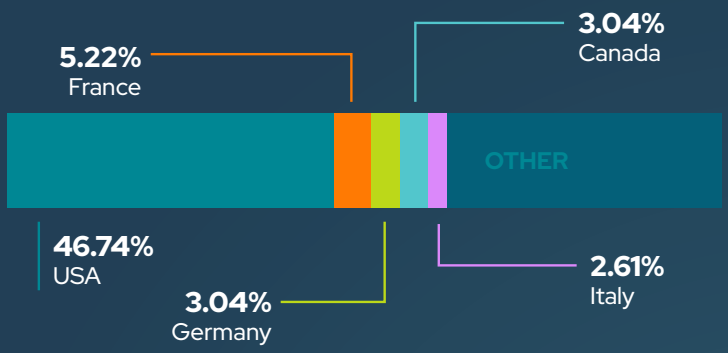


Qilin held the top spot again in late March, continuing to hit manufacturing and logistics firms with fast-moving double-extortion attacks, while The Gentlemen surged after a run of high-visibility leaks tied to poorly secured VPN appliances. Akira stayed active with steady pressure on mid-market enterprises, and DragonForce grabbed attention by mixing ransomware with its hacktivist-style DDoS and data-leak operations. PLAY remained consistent, leaning on living-off-the-land techniques and opportunistic exploitation of edge devices, keeping it a persistent concern for organizations with exposed infrastructure.

VICTIM SECTOR



VICTIM LOCATIONS



TOP NEWS

- Cisco source code stolen in Trivy-linked dev environment breach
- Europe sanctions Chinese and Iranian firms for cyberattacks, FCC bans new routers made outside the USA over security risks
- European Commission investigating breach after Amazon cloud account hack
- GlassWorm malware hits 400+ code repos on GitHub, npm, VSCode, OpenVSX
- Hacker charged with stealing $53 million from Uranium crypto exchange
- Stryker attack wiped tens of thousands of devices, no malware needed
- Tycoon2FA phishing platform returns after recent police disruption
- Yanluowang ransomware access broker gets 81 months in prison, Russia arrests suspected owner of LeakBase cybercrime forum

VICTIM ORG SIZE

TRENDING & ACTIVELY EXPLOITED VULNERABILITIES

CVE	Vendor	Product
CVE-2025-31277	Apple	Multiple Products
CVE-2025-32432	Craft CMS	Craft CMS
CVE-2025-43510	Apple	Multiple Products
CVE-2025-43520	Apple	Multiple Products
CVE-2025-47813	Wing FTP Server	Wing FTP Server
CVE-2025-53521	F5	BIG-IP
CVE-2025-66376	Synacor	Zimbra Collaboration Suite (ZCS)
CVE-2026-20131	Cisco	Secure Firewall Management Center (FMC)
CVE-2026-20963	Microsoft	SharePoint
CVE-2026-3055	Citrix	NetScaler

Late March saw active exploits across a wide range: Apple zero-days in multiple products, Craft CMS and Wing FTP bugs hitting internet-facing apps, F5 BIG-IP and Zimbra flaws abused for initial access, plus high-impact RCEs in Cisco FMC, SharePoint, and Citrix NetScaler driving ransomware and data theft. Priorities: patch on emergency timelines, lock down management and SSO/SAML endpoints, restrict exposure, enable robust logging, and hunt for post-compromise activity.

TRENDING MALWARE

DarkSword Exploit Kit
DarkSword chains multiple iOS zero-days to silently take over devices and steal sensitive data.

DeepLoad
Malware loader that uses AI-generated junk code and PowerShell lures to hide payloads and steal credentials.

GenieLocker
Custom ransomware used in targeted sabotage and extortion campaigns against Russian organizations.

GlassWorm
Supply chain malware that spreads through poisoned developer ecosystems to steal credentials and push second-stage payloads.

Infinity Stealer
Infostealer that targets macOS via ClickFix lures to grab browser data, Keychain items, and crypto-wallet info.

RoadK1ll
A stealthy WebSocket implant that enables quiet lateral movement inside compromised networks.

TRENDING ADVERSARIES

APT36 | **Bearlyfy** | **Silver Fox** | **TA446** | **TeamPCP** | **UNC1069**

APT36, Bearlyfy, Silver Fox, TA446, TeamPCP, and UNC1069 all leaned into credential theft, social-engineering lures, and quiet persistence this period, with several groups mixing classic phishing with browser-based exploits and cloud-identity abuse. APT36 and TA446 kept up their long-game espionage targeting government and research sectors, while Bearlyfy pushed more destructive, politically motivated ransomware. Silver Fox and TeamPCP focused on opportunistic access and data theft, and UNC1069 continued its stealthy cloud-pivoting tradecraft. UNC1069 stands out as the most concerning thanks to its ability to blend into enterprise identity systems and maintain long-term access.

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