THREAT REPORT

Enterprise Threat Landscape Q1 2026

Analysis of the top attack vectors, actively exploited vulnerabilities, and emerging threat actor TTPs impacting enterprise security teams globally in the first quarter of 2025.

47%
increase in ransomware attacks

3.2M
credential sets leaked in Q1 alone

12
critical zero-days exploited in the wild

Published by Mellivor Cybersecurity | April 2026 | 8 min read

Key Findings

• Ransomware attacks against enterprise targets increased 47% year-over-year, with manufacturing, healthcare, and financial services bearing the heaviest targeting.

• Initial access brokers continue to dominate the attack chain — 68% of enterprise breaches in Q1 traced back to compromised credentials purchased on underground markets.

• API exploitation emerged as a primary initial access vector for the first time, accounting for 23% of web application breaches — up from 9% in Q1 2025.

• Nation-state actors increasingly target operational technology and critical infrastructure, with a 3x increase in ICS-specific malware samples observed in Q1.

• AI-generated phishing content reached production quality, with measurable increases in click-through rates and credential harvesting success across targeted campaigns.

Top Attack Vectors — Q1 2026

1. Credential Compromise & Initial Access Brokerage

Stolen credentials remain the number one initial access vector. Over 3.2 million enterprise credential sets were leaked or sold on underground forums in Q1 alone. Attackers increasingly target Active Directory environments, exploiting weak, reused, and previously breached passwords to gain footholds before deploying ransomware or exfiltrating data.

> *Defence: Cynox detects leaked, weak, and reused passwords across Active Directory in real time, blocking compromised credentials the instant they appear. Silent Push maps adversary infrastructure and credential harvesting campaigns before attacks reach your users.*

2. API and Web Application Exploitation

API attacks grew 156% year-over-year, driven by the expanding API surface of enterprise SaaS, microservices, and partner integrations. Broken authentication, excessive data exposure, and injection attacks dominate the observed exploit landscape. Most organisations lack visibility into their full API inventory.

> *Defence: 42Crunch provides full-lifecycle API security from design through production. Wallarm delivers real-time API and application protection with automated API discovery across modern application architectures.*

3. Ransomware Evolution — Double and Triple Extortion

Ransomware groups have standardised double extortion (encryption + data leak threats) and increasingly employ triple extortion (adding DDoS pressure or targeting customers/partners). Mean time to encrypt dropped to under 4 hours from initial access in the fastest observed campaigns. Affiliates are shifting from phishing to exploiting internet-facing vulnerabilities and purchasing access

from initial access brokers.

> *Defence: Cybereason XDR provides operation-centric detection that correlates endpoint, network, and cloud signals to identify ransomware operations early. Labyrinth Security deploys deception technology that detects lateral movement and pre-encryption staging. Corero provides real-time DDoS protection against extortion-motivated volumetric attacks.*

4. OT/ICS Targeting

Attacks against operational technology continued to accelerate, with state-sponsored groups developing ICS-specific tooling. SCADA systems, industrial controllers, and building management systems are increasingly targeted as adversaries recognise the operational and safety impact of disrupting physical infrastructure.

> *Defence: Soteryan (Kryptos Logic) provides specialist OT and critical infrastructure security services. CYNOX (now focused on password intelligence) and Nanitor provide continuous vulnerability management across converged IT/OT environments.*

5. Browser-Based Attacks & Session Hijacking

Enterprise browsers became a primary attack surface in Q1, with adversary-in-the-middle (AitM) toolkits capable of bypassing MFA by stealing session tokens in real time. Browser-based credential theft, malicious extensions, and drive-by downloads accounted for a growing share of initial compromise events.

> *Defence: SURF Security provides enterprise browser security with full visibility and control over web-based activity, addressing credential theft and session hijacking at the browser layer.*

Most Exploited Vulnerabilities — Q1 2026

The following vulnerabilities were most actively exploited in campaigns targeting enterprise environments during Q1 2026. Organisations should verify patching status immediately.

CVE	Product	Description	CVSS	Threat Actor
CVE-2024-21762	Fortinet FortiOS	Out-of-bounds write enabling RCE on SSL VPN	9.8	Multiple APTs
CVE-2024-3400	Palo Alto PAN-OS	Command injection in GlobalProtect gateway	10.0	UTA0218
CVE-2024-1709	ConnectWise ScreenConnect	Authentication bypass in remote access	10.0	Ransomware affiliates
CVE-2024-47575	Fortinet FortiManager	Missing authentication for critical function	9.8	UNC5820
CVE-2023-46805	Ivanti Connect Secure	Authentication bypass in VPN gateway	8.2	UNC5221, UNC5325

Nanitor provides continuous vulnerability remediation and exposure management, prioritising risk reduction based on real-world exploitation intelligence — not just CVSS scores.

Recommendations for Q2 2026

• Audit Active Directory for compromised, weak, and reused credentials — deploy real-time credential screening and enforcement.

• Inventory all API endpoints and implement security testing across the full API lifecycle — shadow APIs are the fastest-growing blind spot.

• Review and test incident response playbooks for ransomware scenarios, including double and triple extortion variants.

• Deploy network detection and response capabilities to identify lateral movement, C2 communications, and pre-encryption staging.

• Implement enterprise browser security controls to address session hijacking and AitM toolkit attacks that bypass traditional MFA.

• Assess OT/ICS security posture and segment operational technology from IT networks with monitored, controlled crossing points.

• Integrate threat intelligence feeds into DNS-layer and network-layer controls for automated blocking of known adversary infrastructure.

• Conduct supply chain security reviews — assess critical vendor posture and contractual cybersecurity obligations.

Ready to build your security programme?

Mellivor works with 20+ specialist cybersecurity vendors across 12 security domains. Our advisory team can map the right technologies to your risk profile, compliance requirements, and operational environment — from initial assessment through deployment and ongoing optimisation.

Book a consultation: mellivorsecurity.com/contact

Explore our vendors: mellivorsecurity.com/vendors