DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative

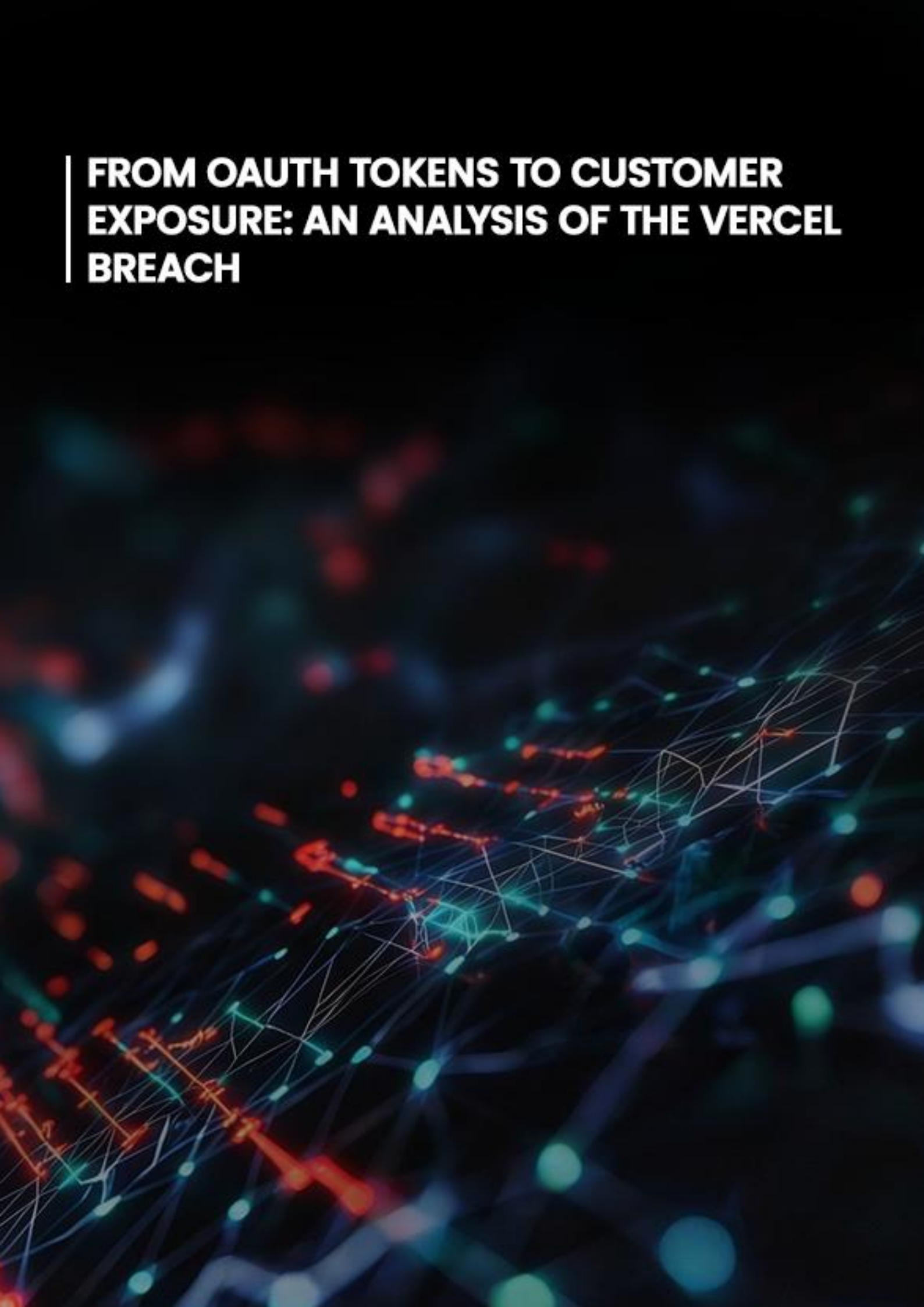
DSCI THREAT INTELLIGENCE AND RESEARCH INITIATIVE

THREAT REPORT

APRIL 2026

Contents

FROM OAUTH TOKENS TO CUSTOMER EXPOSURE: AN ANALYSIS OF THE VERCEL BREACH



Overview

An OAuth-based supply chain attack targeting Vercel has exposed critical weaknesses in modern SaaS ecosystems. In February 2026, a supply chain attack originated by a malware infection at Context.ai from Lumma Stealer compromised Google Workspace OAuth tokens and pivoted into Vercel's internal environment. The attack enabled adversaries to abuse over permissioned OAuth access and enter into the organizational environment while bypassing conventional security controls.

This incident shows how OAuth tokens can serve as high-value access points when over-permissioned or insufficiently monitored. Also, Vercel approach to keep only sensitive data at rest and not to encrypt the non-sensitive data, created an opportunity for attacker to extract meaningful information once internal access is achieved.

This incident stands out because it showed some existing weaknesses in modern SaaS ecosystems:

- Misuse of OAuth trust relationships as a compromised third-party integration can become an entry point into another organization's internal environment.
- The CEO stated that the attackers' speed hinted that some AI-assisted operations were used.

Timeline

Late March 2026

- Attackers gained foothold into Vercel-linked accounts
- Accessed internal resources tied to affected users

Early April 2026

ShintHunters gathered data from Vercel's environment and started selling them on BreachForums

April 10, 2026

Some exposed credentials were detected in the wild few days before disclosure

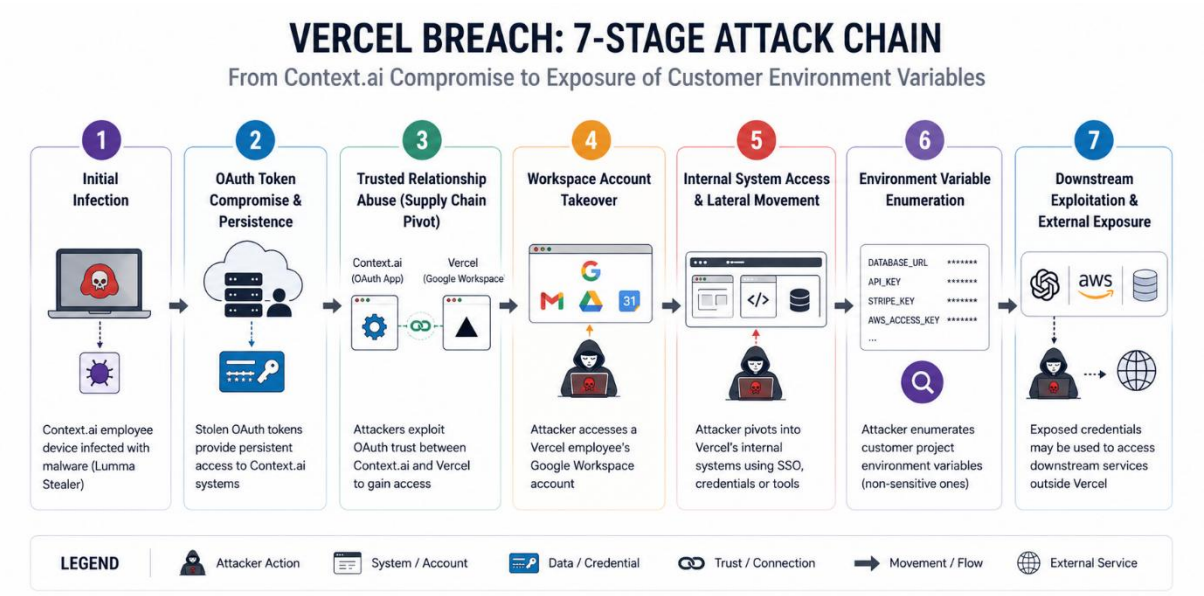
April 19, 2026

- Vercel shares a security update that a limited set of customers whose non-sensitive environment credentials were stored unencrypted were compromised
- Guillermo Rauch confirms the attack chain

April 20, 2026

- Vercel shared recommendation steps to the users who were compromised

Attack Chain



Stage 1

The attack begins with a compromise at Context.ai which had an OAuth application integrated with Google Workspace accounts used by Vercel employees.

- The device of an employee of Context.ai was infected with Lumma Stealer in February 2026.
- The infection occurred after downloading malicious game exploit scripts. The malware stole:
    - Credentials
    - Session cookies
    - OAuth token

Stage 2

The attackers gained access to Context.ai's AWS environment and exfiltrated OAuth tokens to gain persistent access to Context.ai's AWS systems.

These tokens become the primary weapon in the attack because after gaining OAuth tokens:

- No password is required
- Can easily bypass MFA
- Tokens are valid after password resets

OAuth tokens act as long-lived keys as they are not monitored closely.

Stage 3

Attackers identified and exploited the OAuth trust relationship between Context.ai and Vercel. Authorized third-party apps acted as a bridge and access was inherited into Vercel-linked environments.

Stage 4

Using OAuth access, the attacker pivoted into a Vercel employee's Google Workspace account.

They gained access to:

- Email (for credentials)
- Google Drive (documents)
- Calendar (operational visibility)
- Other connected SaaS tools

Stage 5

From the compromised workspace account, the attacker moved into Vercel's internal systems. The paths likely used by the attacker are:

- SSO-based access
- Internal tools linked to Workspace
- Credentials or links found in email/Drive

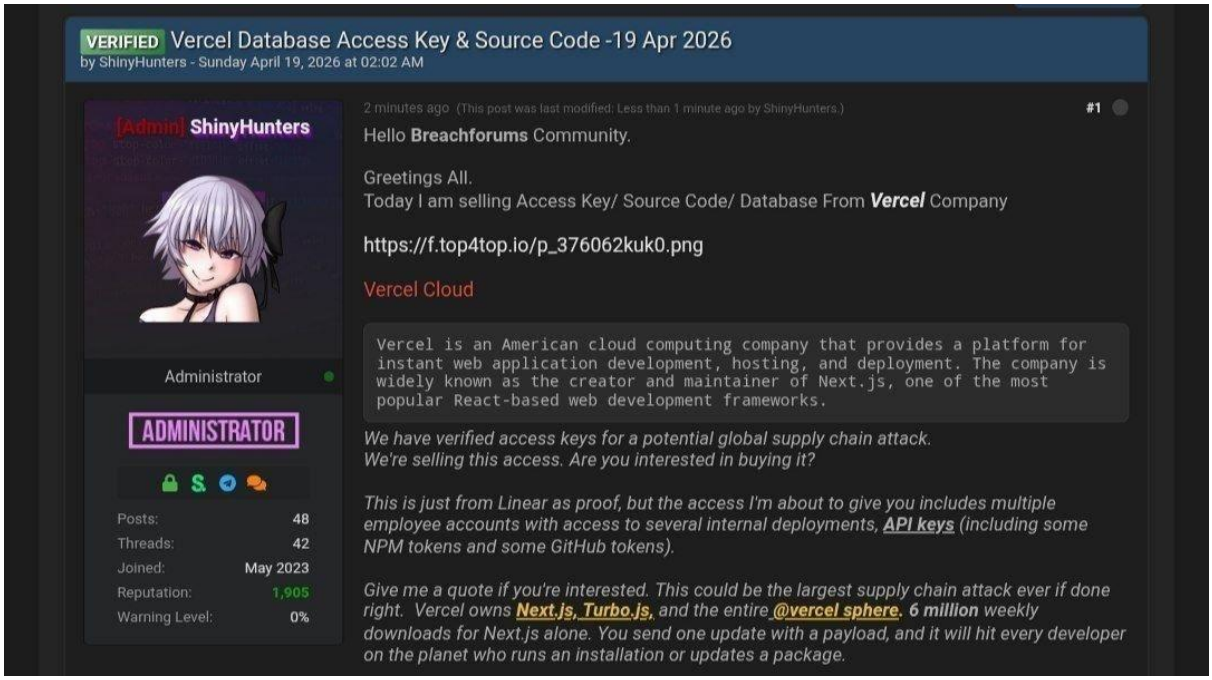
Stage 6

The attacker accessed and enumerated customer project environment variables within Vercel. They keep sensitive variables encrypted at rest, but non-sensitive variables are stored in plaintext at rest.

Thes non-sensitive variables were used to gain further access.

Stage 7

Some exposed environment variables likely contained API keys or service credentials. A public report indicated an API key leak alert on April 10, 2026, and the key existed only in Vercel. It shows that initial access can quickly turn into a real-world impact beyond the platform.



Impact Assessment

Confirmed Impact

- Attackers successfully compromised Google Workspace account to gain access to internal systems.
- Exposure of non-sensitive environment variables that were not encrypted at rest
- Limited subset of customers was affected.
- Potential exposure of API keys/tokens that were stored insecurely.

Potential Risks

- Exposure of credentials embedded in environment variables as non-sensitive variables may still contain:
  - API keys
  - Service tokens
  - Internal endpoints
- Attackers can access other projects and third-party services (e.g., APIs, databases) and perform malicious actions outside Vercel's environment.

Not Affected (Based on Current Evidence)

- Encrypted sensitive environment variables that are encrypted at rest were not exposed.
- There is no evidence of compromise to Vercel's core hosting platform, deployment pipelines or underlying infrastructure.
- The incident didn't result in platform-wide exposure and appears limited in scope.

Design-level Security Issue

The environment variables are used to store API keys, database connection strings, access tokens and configuration values for apps and serverless functions. Each variable also had a sensitive flag which was used to determine how securely it was handled.

The critical issue was simple as security was optional and not default because:

- Every new environment variable was treated as non-sensitive by default.
- Developers had to manually mark each secret as sensitive.
- If they do not mark it as sensitive, then variable is not encrypted at rest, and it remains broadly accessible internally.

Due to this, secrets like DATABASE_URL, API_KEY, AWS_SECRET_ACCESS_KEY, AUTH0_SECRET, GITHUB_TOKENS, etc. are often added quickly and many secrets may unintentionally remain unprotected. So, any system where security requires manual opt-

in and there are no guardrails or warnings will inevitably lead to low adoption and inconsistent protection.

Tactic, Technique and Procedures (TTPs)

Tactic	Technique (ID)	Technique (Name)	Procedure/Description
Initial Access	T1199	Trusted Relationship	Abuse of OAuth trust between Context.ai and Vercel
	T1566	Phishing	Infection via malicious download (game exploit scripts) leading to malware execution
Execution	T1204.002	User Execution – Malicious File	Victim executed malicious file leading to Lumma Stealer infection
Persistence	T1550.001	Use Alternate Authentication Material – Application Access Token	OAuth tokens used for persistence access
Credential Access	T1078	Valid Accounts	Access to Google Workspace account of Vercel employee
	T1552.001	Unsecured Credentials – Credentials in Files	Enumeration of environment variables
	T1528	Steal Application Access Token	Stealing OAuth tokens
Discovery	T1087	Account Discovery	Detection of internal projects and tools
Lateral Movement	T1078.004	Valid Accounts – Cloud Accounts	Potential use of exposed API keys for external services
Collection	T1213	Data from Information Repositories	Access to Google Drive, internal configs and stored data

Indicators of Compromise

OAuth Client ID	110671459871-30f1spbu0hptbs60cb4vsmv79i7bbvqj.apps.googleusercontent.com

Recommendations

Immediate Actions

- Rotate all API keys, tokens and environment variables that were not marked as sensitive.
- Enable multi-factor authentication by adding at least two steps like adding a configuration app and a passkey.
- Enable sensitive flag on all environment variables containing tokens, API keys, credentials, etc.
- Audit Google Workspace OAuth app permissions.
- Revoke suspicious or unused third-party integrations.
- Review logs for anomalous OAuth activity.

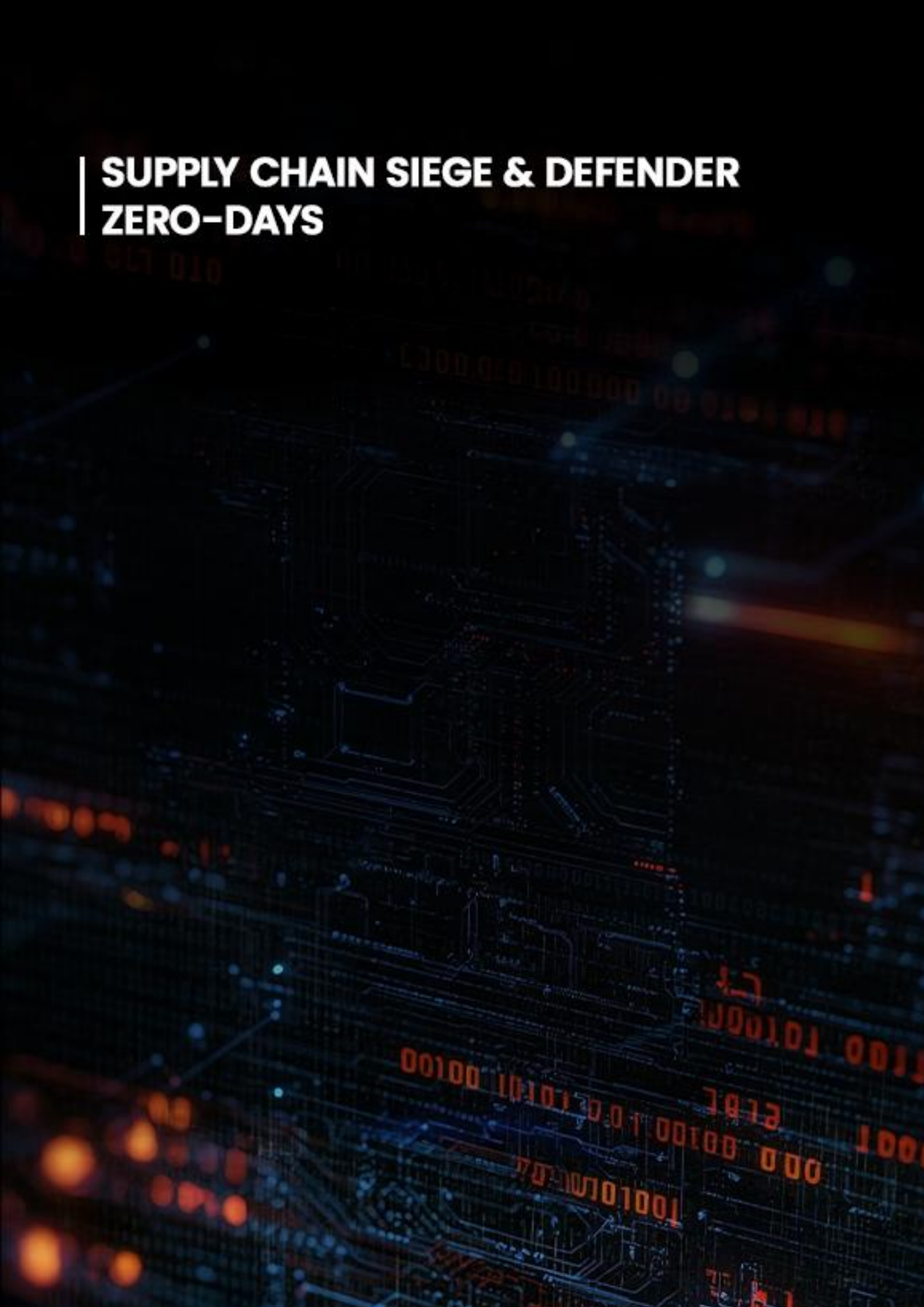
Short-Term Controls

- Enforce least privilege for OAuth scopes.
- Implement OAuth apps approval workflows.
- Classify and secure all environment variables and not just sensitive.

Long-Term Strategy

- Deploy SaaS Security Posture Management (SSPM) tools.
- Monitor OAuth token behavior and anomalies.
- Establish governance for AI and shadow IT adoption.
- Integrate OAuth telemetry into SIEM/XDR.

SUPPLY CHAIN SIEGE & DEFENDER ZERO-DAYS



Overview

April 2026 has been dominated by an unprecedented wave of software supply chain compromises targeting the open-source ecosystem, a trio of Windows Defender zero-days that left enterprise endpoints exposed for weeks, and the emergence of ransomware-as-a-cartel operations striking high-value retail targets across the United Kingdom.

The convergence of these threat vectors - supply chain poisoning enabling initial access, zero-days providing privilege escalation, and ransomware cartels monetizing the resulting footholds - represents a compounding risk environment that is qualitatively more dangerous than any single threat category in isolation.

The month's defining events center on **three major supply chain compromises**: the **Axios npm package hijack** (attributed to North Korean state actor Sapphire Sleet/UNC1069, affecting 100M+ weekly downloads), the **Vercel platform breach** via a cascading OAuth supply chain through Context AI (with stolen data offered for **$2M** on BreachForums), and the **ongoing fallout from the TeamPCP/Trivy campaign** that breached the European Commission's AWS infrastructure and entered a ransomware extortion phase via the newly formed **Vect RaaS** operation. A self-propagating npm worm dubbed **CanisterSprawl** added a novel dimension - autonomously spreading through stolen developer tokens and hijacking packages across ecosystems.

Simultaneously, a random security researcher operating as **"Chaotic Eclipse"** released three Windows Defender zero-day exploits - **BlueHammer**, **RedSun**, and **UnDefend** - protesting Microsoft's vulnerability disclosure process. BlueHammer (**CVE-2026-33825**) was weaponized within seven days of public release and patched on April 14; **RedSun and UnDefend remain unpatched** as of report date, with active exploitation confirmed by Huntress threat intelligence.

The **DragonForce ransomware cartel**, operating with **Scattered Spider** affiliates, struck **Marks & Spencer** - one of the UK's largest retailers - forcing the suspension of online ordering and causing significant operational disruption across the organization's estate. The attackers gained initial access by social-engineering M&S's outsourced IT helpdesk, exfiltrated Active Directory credentials, and deployed DragonForce ransomware across VMware ESXi infrastructure. Meanwhile, **Qilin** has cemented its position as the most active ransomware group globally with 107 confirmed victims in the past 30 days, deploying a BYOVD-based EDR killer capable of neutralizing 300+ security products.

On the geopolitical front, the **Iran-US-Israel cyber conflict** entered its second month with Iran beginning limited internet restoration after a 47-day blackout, while Handala Hack escalated operations with targeted threats against US defense engineers in Israel. The **DOJ/FBI disrupted APT28's DNS hijacking network** (Operation Masquerade), neutralizing a GRU-controlled infrastructure of 18,000+ compromised TP-Link routers across 120 countries.

Key Information:

Three major supply chain compromises: Axios (North Korea), Vercel/Context.ai (criminal), TeamPCP/Trivy to Vect ransomware pipeline

CanisterSprawl: First self-propagating npm supply chain worm observed in the wild

Three Windows Defender zero-days (BlueHammer, RedSun, UnDefend) - two remain unpatched

DragonForce cartel + Scattered Spider hit Marks & Spencer; online ordering suspended, ESXi infrastructure encrypted

Qilin moves forward in the ransomware landscape (107 victims/30 days) with BYOVD EDR killer disabling 300+ security tools

The Gentlemen surge to 320+ victims with 90/10 affiliate split recruiting experienced operators

Microsoft April Patch Tuesday: 163 CVEs including wormable RCE flaws (CVE-2026-33824, CVE-2026-33827)

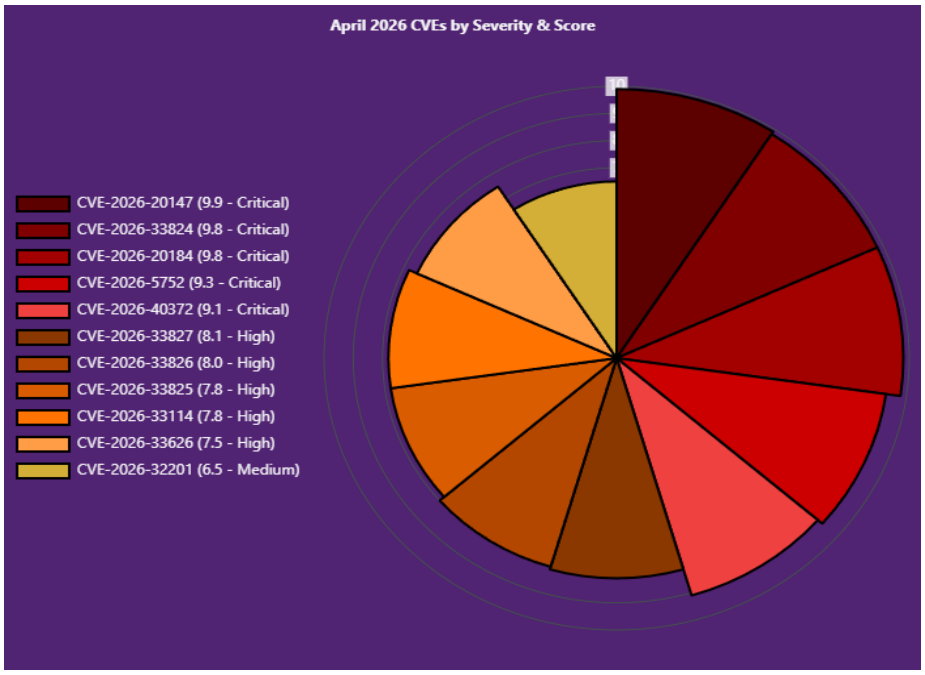
APT28 DNS hijacking network dismantled (Operation Masquerade) - 18,000+ routers across 120 countries

European Commission breached via Trivy supply chain - 340GB data stolen by ShinyHunters

Sectors Most Impacted: Retail, Software/Technology, Government, Healthcare, Manufacturing, Financial Services, Critical Infrastructure

Geographic Hotspots: United Kingdom (M&S retail attack), United States (supply chain/federal targets), European Union (EC breach), Middle East (Iran conflict), Global (npm ecosystem)

CVE Chart of the Month



Supply Chain Compromise - The April Siege

April 2026 marks the most concentrated period of software supply chain attacks ever recorded, with four distinct campaigns simultaneously targeting the open-source ecosystem. The common thread across all four is the exploitation of trust - in package registries, in CI/CD pipelines, in OAuth integrations, and in security tools themselves.

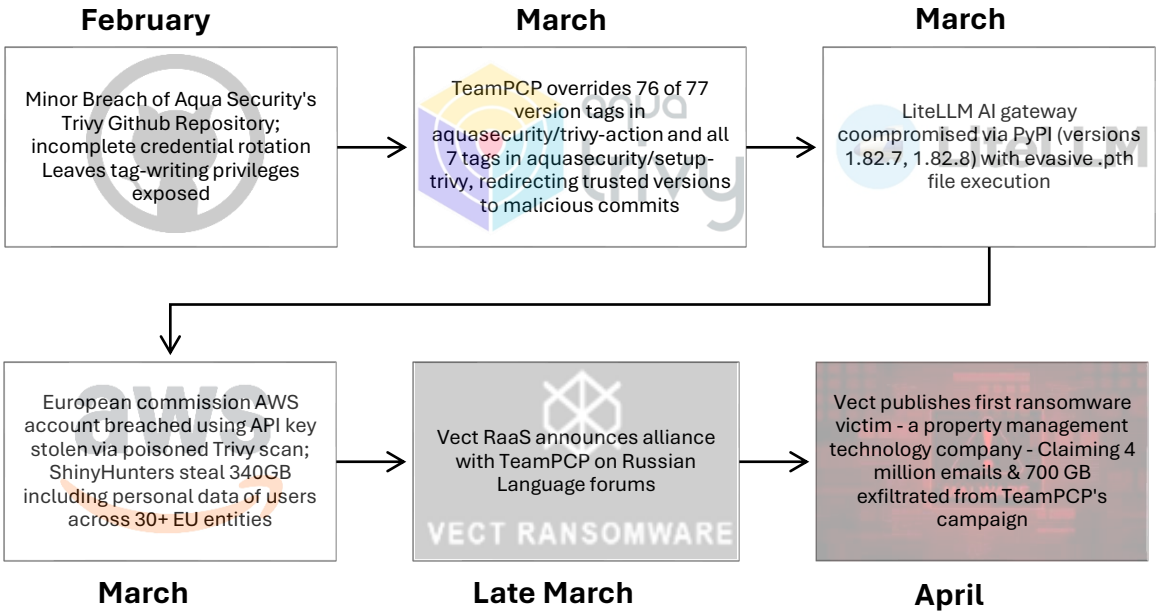
Axios npm Package Compromise - North Korean State Operation

Technical Analysis: The attackers compromised a maintainer's npm credentials and published backdoored versions that introduced plain-crypto-js@4.2.1 as a runtime dependency. This fake package executed automatically through a postinstall hook with no user interaction required. Upon successful C2 connection, a second-stage RAT was deployed based on the target operating system. The existence of node_modules/plain-crypto-js/ in any project is sufficient evidence of compromise.

Attribute	Detail
Target	Axios npm package (JavaScript HTTP client)
Weekly Downloads	~100 million
Malicious Versions	1.14.1, 0.30.4 (published March 31, 2026)
Safe Versions	1.14.0, 0.30.3
Attribution	Sapphire Sleet (Microsoft) / UNC1069 (Google GTIG) - North Korea-nexus
Attack Vector	Compromised maintainer account; injected malicious dependency plain-crypto-js@4.2.1
Payload	Cross-platform RAT (macOS, Windows, Linux) delivered via postinstall hook
C2 Infrastructure	142.11.206.73; sfrclak[.]com:8000
CISA Alert	Issued April 20, 2026

Analyst Assessment: The attribution to North Korean state actors (Sapphire Sleet/UNC1069) is significant - it confirms that Pyongyang has expanded from targeting cryptocurrency platforms and IT worker fraud to directly poisoning the global software supply chain. Given Axios's 100M+ weekly downloads, even a brief window of exposure (March 31 to detection) likely resulted in thousands of compromised CI/CD environments. The financial motivation aligns with North Korea's documented use of cyber operations to generate state revenue, but the RAT payload also provides espionage capabilities.

TeamPCP/Trivy - Security Scanner to Ransomware Pipeline



Attribute	Detail
Threat Actor	TeamPCP
Initial Compromise	Aqua Security's Trivy vulnerability scanner (March 19, 2026)
Scope	GitHub Actions, Docker Hub, npm, PyPI, OpenVSX - 5 ecosystems poisoned
CVE	CVE-2026-33634 (CVSS 9.4)
Downstream Victims	European Commission AWS infrastructure (340GB stolen), 30+ EU entities
Ransomware Phase	Vect RaaS (first victim published April 15, 2026)
Alliance	TeamPCP + Vect RaaS partnership announced late March 2026

Analyst Assessment: This campaign represents a paradigm shift: the weaponization of security tools themselves as attack vectors. Organizations that diligently ran vulnerability scans were the ones most exposed. The subsequent Vect RaaS alliance transforms what began as a supply chain data theft into a ransomware extortion pipeline - every organization compromised during the Trivy campaign is now a potential ransomware target. The European Commission breach confirms that even sophisticated government entities with dedicated security teams (CERT-EU) can fall victim when the supply chain is poisoned at the tool level.

Vercel Platform Breach - OAuth Cascade Attack

Attribute	Detail
Victim	Vercel (web development platform)
Disclosure	April 19, 2026
Root Cause	Lumma Stealer infection at Context.ai (February 2026)
Attack Path	Infostealer at Context.ai -> stolen Google Workspace OAuth tokens -> Vercel's enterprise Google Workspace -> internal systems
Key Vulnerability	A Vercel employee signed up for Context AI's service using their enterprise account and granted "Allow All" OAuth permissions
Threat Actor	ShinyHunters
Asking Price	$2 million on BreachForums for customer API keys, source code, and database data
Impact	Potentially hundreds of users across many organizations affected
Malicious OAuth App	110671459871-30f1spbu0hptbs60cb4vsmv79i7bbvqj.apps.googleusercontent.com

Analyst Assessment: The Vercel breach illustrates the growing danger of SaaS-to-SaaS supply chain attacks. The kill chain began with a commodity infostealer (Lumma) at a third-party AI company, cascaded through OAuth trust relationships, and ultimately compromised a platform hosting thousands of developer projects. The critical failure was permissive OAuth scoping - a single employee's "Allow All" consent decision created an enterprise-wide exposure. This attack pattern is highly likely to be replicated, as the combination of infostealers and overly permissive OAuth integrations exists across virtually every enterprise SaaS environment.

CanisterSprawl - Self-Propagating npm Worm

Attribute	Detail
Discovery	Socket and StepSecurity, April 2026
Type	Self-propagating supply chain worm
Propagation	Steals npm tokens -> publishes poisoned versions of victim's packages -> repeats
Known Compromised	16+ packages from Namastex Labs (agentic AI tooling)
Payload	1,143-line credential harvester via npm postinstall hook
Targets	npm tokens, cloud credentials (AWS/GCP/Azure), SSH keys, Kubernetes tokens, Docker configs, git credentials, browser data, crypto wallets
Exfiltration	HTTPS webhook + ICP (Internet Computer Protocol) canister
Named After	ICP canister used for C2/exfiltration

Analyst Assessment: CanisterSprawl represents a novel threat class - a true supply chain worm capable of autonomous propagation without attacker intervention. By stealing developer npm tokens and immediately publishing poisoned versions of their packages, the worm spreads exponentially through the dependency graph. The use of ICP canisters for exfiltration is particularly concerning as it leverages decentralized infrastructure that is resistant to traditional takedown methods. While the current campaign appears limited to Namastex Labs' ecosystem, the technique is trivially replicable against any npm package maintainer.

Supply Chain Threat Assessment

The four concurrent supply chain campaigns share a common strategic implication: the trust model underlying open-source software distribution is under systematic attack from both state and criminal actors simultaneously. Organizations should assume that any dependency update, CI/CD action, or third-party SaaS integration is a potential attack vector until independently verified.

Critical Vulnerabilities & Zero-Day Exploitation

Windows Defender Triple Zero-Day

The most consequential vulnerability disclosure of April 2026 was not a vendor patch but a protest. On April 3, a security researcher operating under the alias "Chaotic Eclipse" published a fully functional Windows local privilege escalation exploit on GitHub, dubbed BlueHammer. Within two weeks, two additional Defender zero-days - RedSun and UnDefend - followed, all released as protest against Microsoft's Security Response Center disclosure process.

Exploit	CVE	Type	Status (as of report date)	Active Exploitation
BlueHammer	CVE-2026-33825	LPE via Defender update + VSS abuse	**Patched** (April 14)	Yes - weaponized since April 10
RedSun	Pending	LPE via Defender cloud file rollback	**UNPATCHED**	Yes - confirmed
UnDefend	Pending	Defender update blocking (DoS)	**UNPATCHED**	Yes - confirmed

BlueHammer (CVE-2026-33825) - Patched

BlueHammer exploits the interaction between Microsoft Defender's update workflow, Volume Shadow Copy Service, the Windows Cloud Files API, and opportunistic locks. A race condition in Defender's file remediation logic enables arbitrary file overwrite, escalating a low-privileged user to NT AUTHORITY\SYSTEM. All legitimate, documented Windows features - no exotic exploitation required.

- **Disclosure:** April 3, 2026 (PoC on GitHub)
- **Weaponization:** April 10, 2026 (7 days to exploitation)
- **Patch:** April 14, 2026 (Defender Antimalware Platform update)

RedSun - UNPATCHED

RedSun abuses Defender's cloud file rollback mechanism. When Defender detects a cloud-tagged file, it attempts to restore it to its original location **without validating the target path**. Attackers redirect the write operation to a privileged directory, achieving

SYSTEM-level access. RedSun was independently assessed as a second LPE flaw and remains unpatched as of report date.

UnDefend - UNPATCHED

UnDefend can be executed by a standard unprivileged user to block Defender from receiving definition updates. Over time, this silently degrades antivirus protection, making the system blind to new malware. This vulnerability is particularly insidious because its effects are gradual and may not trigger immediate alerts.

Analyst Assessment: The simultaneous disclosure of three Defender zero-days - targeting the security product itself rather than the operating system - creates a layered attack scenario: UnDefend degrades detection capability while BlueHammer or RedSun provides privilege escalation. Huntress has confirmed that a hands-on-keyboard threat actor gained initial access through a compromised SSL VPN on April 10 and escalated privileges using one of these exploits. The fact that two of three remain unpatched nearly a month after disclosure is deeply concerning for organizations relying on Defender as their primary endpoint protection. Microsoft's delayed response to the researcher's initial private disclosure - the stated motivation for the public release - merits examination as a systemic process failure.

Microsoft April 2026 Patch Tuesday

Microsoft's April 2026 Patch Tuesday was the **second-largest on record**, addressing **163 CVEs** (8 Critical, 154 Important, 1 Moderate) across Windows, Office, SharePoint, and related products.

Critical Vulnerabilities Requiring Immediate Attention:

CVE	Product	Type	CVSS	Wormable	Notes
CVE-2026-33824	Windows IKE Service Extensions	Double-free RCE	9.8	Yes	Unauthenticated; block UDP 500/4500 if IKE unused
CVE-2026-33827	Windows TCP/IP	Race condition RCE	8.1	Yes	Unauthenticated; affects IPv6/IPsec environments
CVE-2026-32201	SharePoint Server	Spoofing	6.5	No	Actively exploited zero-day - view/modify exposed information

CVE-2026-33825	Windows Defender	LPE (BlueHammer)	7.8	No	Patch for BlueHammer; RedSun/UnDefend remain open

Analyst Assessment: The presence of two wormable, unauthenticated RCE vulnerabilities (CVE-2026-33824 and CVE-2026-33827) in network-facing services demand priority patching. CVE-2026-33824's 9.8 CVSS score and wormable classification in Windows IKE - a service commonly enabled in VPN and IPsec deployments - make it a high-probability target for mass exploitation if a weaponized exploit becomes available. Organizations should prioritize patching and consider blocking UDP 500/4500 where IKE is not required.

Actively Exploited Vulnerabilities - April 2026

CVE	Product	Type	CVSS	Exploitation Context
CVE-2026-33825	Windows Defender	LPE (BlueHammer)	7.8	Weaponized from PoC within 7 days; patched April 14
CVE-2026-32201	SharePoint Server	Spoofing	6.5	Actively exploited zero-day; patched in April Patch Tuesday
CVE-2026-33634	Trivy/LiteLLM	Supply chain compromise	9.4	TeamPCP campaign; ongoing downstream exploitation
CVE-2023-50224	TP-Link WR841N	Auth bypass	6.5	APT28 DNS hijacking campaign; routers compromised since 2024
RedSun (pending)	Windows Defender	LPE	-	UNPATCHED; active exploitation confirmed
UnDefend (pending)	Windows Defender	AV definition blocking	-	UNPATCHED; active exploitation confirmed

Ransomware Landscape - April 2026

Ecosystem Overview

Ransomware volume has stabilized at an elevated "new normal" in Q1 2026, with attack volumes holding steady both quarter-over-quarter and year-over-year. The late-2025 surge has effectively recalibrated the baseline. The most significant structural development is the maturation of cartel and white-label operating models, exemplified by DragonForce's devastating UK retail campaign.

Metric	April 2026 Status
Most active group	Qilin (107 victims/30 days, ~14% of all tracked activity)
Fastest growing group	The Gentlemen (35 victims in Q4 2025 -> 182 in Q1 2026, 420% growth)
Most impactful campaign	DragonForce/Scattered Spider attack on Marks & Spencer (UK)
New entrant of note	Vect RaaS (alliance with TeamPCP; supply chain-to-ransomware pipeline)
Key trend	BYOVD EDR killers capable of neutralizing 300+ security products
Key trend	Shift toward data theft/extortion-only models (reduced encryption reliance)

DragonForce Cartel - Marks & Spencer Attack

The most consequential ransomware incident of April 2026 struck one of the United Kingdom's largest and most recognized retailers.

Attribute	Detail
Victim	Marks & Spencer (M&S) - UK retailer, 1,000+ stores, ~65,000 employees
Public Disclosure	April 22, 2026
Initial Intrusion	Approximately February 2025 (pre-positioned access)
Ransomware Deployed	DragonForce (white-label variant) on VMware ESXi hosts
Attribution	Scattered Spider (initial access) + DragonForce cartel (ransomware platform)

Immediate Impact	Online ordering suspended; contactless payments disrupted; Click & Collect services offline
IT Helpdesk Outsourcer	Tata Consultancy Services (TCS)
Status	Active incident; full damage assessment ongoing

Attack Chain (M&S):

1. **Initial access (Feb 2025):** Scattered Spider affiliates compromised M&S's IT helpdesk (outsourced to TCS) via social engineering - operators impersonated an internal IT employee and called the third-party service desk to obtain a password reset.

2. **Credential harvesting:** Using the reset credentials, attackers accessed Active Directory and exfiltrated the NTDS.dit file (the domain credential database containing all user password hashes).

3. **Ransomware deployment (April 2026):** DragonForce white-label ransomware was deployed across M&S's VMware ESXi infrastructure, encrypting virtualized workloads.

DragonForce Cartel Model: DragonForce operates as a Ransomware-as-a-Service (RaaS) cartel, allowing affiliates to create their own brands while leveraging shared infrastructure - petabytes of storage, 24/7 monitoring, file analysis, decryption services, and dry-run testing support. Scattered Spider has partnered with DragonForce after previously working with BlackCat, RansomHub, and Qilin. The cartel offers a white-label model where affiliates operate under their own brand names while using DragonForce's backend tooling.

Analyst Assessment: The M&S attack demonstrates the operational maturity of the cartel model - Scattered Spider provides world-class social engineering for initial access, and DragonForce provides the ransomware platform and infrastructure. The extended dwell time (approximately two months between initial access and ransomware deployment) suggests the attackers conducted extensive reconnaissance and data staging before detonation. The targeting of an outsourced IT helpdesk as the initial compromise vector is a critical lesson - the weakest point in M&S's security perimeter was a third-party contractor's phone-based identity verification process. Organizations relying on outsourced service desks should immediately review identity verification procedures for privileged operations such as password resets. The full financial impact of this incident is not yet quantifiable but is expected to be significant given the disruption to online and in-store operations. Additional UK retailers should be on heightened alert - the DragonForce cartel model enables rapid pivoting to new targets, and the UK retail sector may face further attacks in the near term.

Qilin - Market Dominance with BYOVD Innovation

has consolidated its position as the most active ransomware operation globally, claiming 107+ confirmed victims in the past 30 days - approximately 14% of all tracked ransomware activity. Since inception in late 2022, Qilin has reached 1,800+ total victims.

BYOVD EDR Killer:

Qilin has deployed a sophisticated BYOVD (Bring Your Own Vulnerable Driver) technique to neutralize endpoint security:

- A malicious DLL (msimg32.dll) is loaded via DLL side-loading
- Two vulnerable drivers are deployed: rwdrv.sys (renamed ThrottleStop.sys from TechPowerUp LLC) for physical memory access, and hlpdrv.sys to terminate protected EDR processes
- The technique is capable of terminating 300+ EDR drivers from virtually every security vendor

Analyst Assessment: The ability to systematically disable every major EDR product before encryption represents a significant evolution in ransomware capability. Traditional EDR-centric defensive strategies are insufficient when attackers can blind the sensor layer at the kernel level. Organizations should layer defenses beyond EDR - network detection, behavioral analytics at the hypervisor level, and immutable logging - to maintain visibility when endpoint agents are neutralized.

The Gentlemen - Rapid Ascent

The Gentlemen RaaS operation has experienced explosive growth, expanding from 35 victims in Q4 2025 to 182 in Q1 2026 - a **420% quarterly increase** making it the second most active group by victim count. Total claimed victims exceed 320 since mid-2025.

Attribute	Detail
Affiliate Split	90/10 (affiliate/operator) - highest in the market
Target Sectors	Manufacturing, Technology, Healthcare
Geographic Focus	United States, UK, Germany

Botnet Scale	1,570+ likely corporate victims (per Check Point Research access to live C2)
Initial Access	Exposed VPNs, firewalls, remote access gateways

Analyst Assessment: The 90/10 affiliate split - 10 percentage points more generous than the industry-standard 80/20 - is the primary driver of The Gentlemen's rapid growth, pulling experienced operators from other gangs. Check Point's access to a live C2 server revealing 1,570+ likely corporate victims (far exceeding the 320 publicly claimed) suggests that the true scope of compromise is significantly larger than DLS postings indicate. Healthcare targeting without ethical restraint is particularly concerning.

Vect RaaS - Supply Chain to Ransomware Pipeline

VECT RANSOMWARE is a newly emerged RaaS operation (detailed research is covered in the - February Threat Report 2026) that began recruiting on Russian-language forums in late December 2025. Its significance lies not in victim volume but in its operational model: an **explicit alliance with TeamPCP** to monetize supply chain compromises through ransomware extortion.

On April 15, Vect published its first known victim - a property management technology company - claiming exfiltration of 4 million emails and 700GB of data sourced from TeamPCP's Trivy campaign. This represents a new threat model: **supply chain breach as a ransomware acquisition channel**.

Ransomware Trends Assessment

1. **Cartel models are now operational reality.** The DragonForce/Scattered Spider attack on M&S proves the cartel approach works - specialized initial access brokers (Scattered Spider) paired with infrastructure providers (DragonForce) deliver devastating results against major enterprises.

2. **BYOVD EDR killers are becoming standard equipment.** Both Qilin and Warlock independently developed kernel-level EDR neutralization, a capability that will proliferate across the ecosystem.

3. **Supply chain-to-ransomware pipelines are forming.** The TeamPCP/Vect alliance creates a model where supply chain data theft is systematically converted to ransomware extortion.

4. **Aggressive affiliate recruitment is accelerating fragmentation.** The Gentlemen's 90/10 split is reshuffling the affiliate talent pool, likely pulling experienced operators from less generous programs.

5. **Data theft without encryption is growing.** Threat actors favor extortion-only operations, reducing operational complexity while maintaining pressure through exposure threats.

Geopolitical Cyber Operations

Iran-US-Israel Conflict – a follow up to our previous report

The cyber dimension of the Iran-US-Israel conflict entered its second month in April 2026. Following the February 28 initiation of Operation Epic Fury/Roaring Lion, Iran endured a 47-day near-complete internet blackout before beginning limited restoration on approximately April 17, with access restricted to websites and applications mirrored on Iran's National Information Network.

Key April Developments:

Date	Event	Significance
April 1	FDD publishes comprehensive Handala assessment	Confirms MOIS affiliation; operational since 2023
April 7	DOJ disrupts APT28 DNS hijacking (Operation Masquerade)	GRU infrastructure neutralized; 18,000+ routers freed
April 17	Iran begins limited internet restoration	47-day blackout partially lifted; NIN-only access

Ongoing	Handala "Operation Lockheed Martin" Phase 2	Claims access to data of 28 US defense engineers in Israel
Ongoing	Electronic Operations Room coordination	Formalized Iranian cyber retaliation structure continues

Handala Hack - Escalating Operations

Handala Hack, confirmed as a front for Iran's Ministry of Intelligence and Security (MOIS), continued to escalate operations in April, building on its March campaigns:

- Claimed 23 ransomware victims in March alone (more than half its 2026 total of 33).
- The Stryker Corporation wiper attack (March, 200,000+ devices) remains under joint CISA/FBI investigation.
- "Operation Lockheed Martin" Phase 2 claims access to personal data of 28 senior US defense engineers working on F-35, F-22, and THAAD systems in Israel.
- DOJ seized four Handala-associated domains used for psychological operations and transnational repression.

Analyst Assessment: Handala's operational tempo and target selection - healthcare companies, defense engineers, law enforcement officials - indicate a deliberate strategy to maximize psychological impact beyond technical damage. The 48-hour ultimatum issued to US defense engineers to "cease cooperation and leave Israel" blends cyber operations with coercion, crossing into transnational repression territory. Despite DOJ enforcement actions, the group's MOIS backing ensures continued operational capability.

Operation Masquerade - APT28 DNS Hijacking Disruption

On April 7, 2026, the DOJ and FBI announced a court-authorized operation to neutralize a GRU-controlled DNS hijacking network.

Attribute	Detail
Threat Actor	APT28 / Fancy Bear / Forest Blizzard (GRU Military Unit 26165)
Operation Name	Operation Masquerade

Compromised Devices	18,000+ TP-Link WR841N routers (120+ countries at peak, December 2025)
Vulnerability	CVE-2023-50224 (TP-Link authentication bypass)
Technique	DNS hijacking to redirect requests to GRU-controlled servers; AitM attacks against encrypted traffic
Targets	Microsoft Outlook Web Access and other legitimate services mimicked for credential harvesting
Data Stolen	Unencrypted passwords, authentication tokens, emails, and sensitive information
Remediation	FBI sent commands to US routers: collected evidence, reset DNS settings, blocked GRU re-access

Analyst Assessment: The scale of APT28's router compromise network - 18,000+ devices across 120 countries - demonstrates the ongoing threat posed by unpatched consumer-grade networking equipment. The DNS hijacking technique is particularly dangerous because it is transparent to the end user and can intercept encrypted session tokens. The FBI's court-authorized remediation of US-based routers sets an important precedent for active defense against state-sponsored infrastructure abuse but leaves the vast majority of compromised devices in other jurisdictions unaddressed.

Chinese APT Operations - UAT-9244/Salt Typhoon

China-linked threat actors continued targeting telecommunications infrastructure with previously undocumented malware:

Malware	Platform	Capability
TernDoor	Windows	Backdoor via DLL side-loading (wsprint.exe loading rogue BugSplatRc64.dll)
PeerTime	Linux	C/C++ and Rust variants; BitTorrent protocol for C2; process masquerading
BruteEntry	Edge devices	Mass-scanning proxy node; brute-forces Postgres, SSH, Tomcat servers

Cisco Talos tracks this activity as UAT-9244, assessing with high confidence, it is closely associated with FamousSparrow and Tropic Trooper based on tooling overlap and victimology. Targets include South American telecommunications networks. A definitive connection to Salt Typhoon has not been established.

Major Data Breaches & Incidents

European Commission AWS Breach

Attribute	Detail
Victim	European Commission (Europa.eu platform)
Date	March 24 (access); March 27 (disclosure); April 3 (CERT-EU confirmation)
Threat Actor	ShinyHunters (via TeamPCP supply chain)
Initial Access	AWS API key compromised via poisoned Trivy scan (March 19)
Post-Exploitation	TruffleHog used to scan for secrets; new access key attached to existing AWS user
Data Stolen	340GB - personal data (names, usernames, emails) from 30+ EU entities; 51,992 outbound email files
Impact	Data from multiple Union institutions potentially exposed

Adobe - Alleged BPO Supply Chain Breach

China-linked threat actors continued targeting telecommunications infrastructure with previously undocumented malware:

Attribute	Detail
Threat Actor	Mr. Raccoon
Claim	13 million customer support tickets, 15,000 employee records, HackerOne bug bounty submissions
Attack Path	Phishing -> compromised workstation at Indian BPO vendor -> manager credentials -> bulk data export
Key Detail	"They allowed you to export all tickets in one request from an agent" - suggesting an access control misconfiguration enabling mass data export
Status	**Unverified** - Adobe has not officially confirmed or denied these claims
Confidence	D3 (Not Usually Reliable / Possibly True) - single-source claim lacking vendor confirmation

Analyst Note: The specificity of Mr. Raccoon's technical claims (BPO attack path, mass export misconfiguration, HackerOne submissions) lends some credibility, but without Adobe's confirmation this remains an unverified threat actor assertion. If confirmed, the exposure of HackerOne bug bounty submissions would be particularly dangerous - providing attackers with a catalog of vulnerability research on Adobe products. Organizations should monitor for downstream credential abuse from the alleged 13M support tickets.

Basic-Fit - European Gym Chain

Attribute	Detail
Victim	Basic-Fit (Europe's largest gym chain, 1,400+ clubs)
Date	April 8 (unauthorized access); April 13 (public disclosure)
Members Affected	Up to 1 million across Netherlands, Belgium, Luxembourg, France, Spain, Germany
Data Exposed	Full names, physical addresses, email addresses, phone numbers, dates of birth, bank account details, membership information, recent club visit history, mobile device descriptions
Not Exposed	Passwords, identification documents
Detection	Automated system monitoring; access stopped within minutes of discovery
Status	No evidence of public data exposure or misuse as of report date

Booking.com - Reservation Data Breach

Attribute	Detail
Victim	Booking.com (global travel booking platform)
Date	April 2026
Data Exposed	Full names, physical addresses, booking dates and details, email addresses, phone numbers, hotel-specific notes and requests

Risk	Exposed reservation data enables highly targeted phishing campaigns - attackers can reference specific hotel stays, dates, and personal preferences to craft convincing lures
Status	Under investigation

Grinex Cryptocurrency Exchange

Attribute	Detail
Victim	Grinex (cryptocurrency exchange)
Date	April 2026
Attribution	State-sponsored threat group (specific nation-state not publicly attributed)
Financial Loss	Exceeding $13 million
Impact	Exchange operations suspended; customer withdrawals halted
Significance	Continues the pattern of state-sponsored targeting of cryptocurrency platforms for revenue generation, consistent with North Korean and other state actor TTPs

Law Enforcement Operations

Operation Masquerade - APT28 Router Network

Covered in Section 5.3. Court-authorized FBI operation neutralized GRU DNS hijacking network of 18,000+ TP-Link routers. Evidence collected, DNS settings reset, and GRU re-access methods blocked on US-based devices.

W3LL Phishing Network Dismantled

The FBI and Indonesian Police dismantled the W3LL phishing network - a sophisticated phishing-as-a-service ecosystem built around the W3LL Panel (aka OV6 panel). The platform enabled criminals to mimic legitimate login pages and bypass multi-factor authentication to compromise enterprise Microsoft 365 accounts, facilitating an estimated $20M in fraud attempts.

DDoS-for-Hire Services Crackdown

A coordinated international operation beginning April 13 targeted DDoS-for-hire (booter/stresser) services:

Action	Count
Warning emails/letters sent	Tens of thousands
Arrests	4
Domain seizures	53
Search warrants	25
US domain seizures	8 (including Vac Stresser, Mythical Stress)

Handala Domain Seizures

The DOJ seized four domains used by Iran's MOIS (via Handala persona) for cyber-enabled psychological operations and transnational repression targeting Iranian diaspora communities.

Emerging Techniques, Tactics & Procedures

BYOVD EDR Killers - Proliferation Across Groups

The Bring Your Own Vulnerable Driver technique for disabling endpoint security has proliferated beyond individual groups to become a shared operational standard:

- **Qilin**: msimg32.dll via DLL side-loading; rwdrv.sys + hlpdrv.sys driver pair; 300+ EDR products targetable
- **Warlock (Water Manual)**: Legitimate NSec driver (NSecKrnl.sys) for kernel-level security product termination
- **Common pattern**: Both groups disable security first, then deploy ransomware - this sequence is now the norm rather than the exception

Self-Propagating Supply Chain Worms

CanisterSprawl represents the first documented self-propagating supply chain worm in the npm ecosystem - autonomous token theft and package poisoning without human operator intervention. Key novel elements:

- Decentralized C2 via ICP canisters (censorship-resistant)
- Cross-ecosystem credential harvesting (npm, AWS, GCP, Azure, SSH, Kubernetes)
- Automatic propagation through stolen maintainer tokens

OAuth Cascade Attacks

The Vercel breach via Context AI establishes a replicable attack pattern:

- Compromise any SaaS vendor with overly permissive OAuth integrations to a target.
- Leverage infostealers (Lumma, etc.) at the weakest link in the OAuth chain.
- Cascade through trust relationships to reach high-value targets.

Security Tool Weaponization

The TeamPCP campaign and the Defender zero-day trilogy share a common theme: turning security infrastructure against its operators.

- **Trivy**: Vulnerability scanners became malware delivery mechanisms.
- **Defender**: The endpoint protection product became the privilege escalation vector.
- **Implication**: Security tools must be treated as high-value targets in their own right, not assumed to be trustworthy.

AI-Augmented Operations

The surge in AI assisted offensive campaigns is higher than ever and is constantly evolving. As per CISA's Q1 2026 report, AI-enhanced ransomware attacks demonstrate a higher success rate than traditional variants, that too in short time. The FBI IC3 report's first dedicated AI section (22,364 complaints, $893M losses) confirms AI-enabled fraud is now a mainstream threat category.

Cross-Campaign Link

ShinyHunters appears in both Campaign 2 (EU Commission data exfiltration via TeamPCP's Trivy access) and Campaign 3 (selling Vercel data on BreachForums for $2M). This suggests either shared operational infrastructure or direct actor overlap between the two criminal campaigns.

MITRE ATT&CK Highlights - April 2026

The following MITRE ATT&CK techniques were most prominently observed throughout the month's threat activity:

Tactic	Technique ID	Technique Name	Observed Context
Initial Access	T1195.002	Supply Chain Compromise: Compromise Software Supply Chain	Axios npm, Trivy/LiteLLM, CanisterSprawl, Vercel/Context AI
	T1566	Phishing	W3LL phishing network; Scattered Spider helpdesk social engineering
	T1199	Trusted Relationship	Vercel breached via Context AI OAuth trust; Adobe alleged BPO vendor compromise
Execution	T1204.003	User Execution: Malicious Image/File	Axios postinstall hook; CanisterSprawl postinstall hook
Persistence	T1098.001	Account Manipulation: Additional Cloud Credentials	EC breach - new AWS access key attached to existing user
Privilege Escalation	T1068	Exploitation for Privilege Escalation	BlueHammer/RedSun Defender zero-days for SYSTEM access
Defence Evasion	T1562.001	Impair Defenses: Disable or Modify Tools	Qilin/Warlock BYOVD EDR killers (300+ products); UnDefend Defender update blocking
	T1574.002	Hijack Execution Flow: DLL Side-Loading	Qilin msimg32.dll side-loading; TernDoor via wsprint.exe

Credential Access	T1528	Steal Application Access Token	CanisterSprawl npm token theft; Vercel OAuth token compromise
	T1003.003	OS Credential Dumping: NTDS	M&S attack - NTDS.dit exfiltration from Active Directory
Discovery	T1526	Cloud Service Discovery	EC breach - TruffleHog used to scan for AWS secrets
Lateral Movement	T1021.001	Remote Services: Remote Desktop Protocol	APT28 credential harvesting for downstream RDP access
Collection	T1557	Adversary-in-the-Middle	APT28 DNS hijacking for credential interception
Exfiltration	T1567	Exfiltration Over Web Service	CanisterSprawl exfil to ICP canisters; TeamPCP data staging
Impact	T1486	Data Encrypted for Impact	DragonForce on M&S ESXi; Qilin operations; Vect RaaS

Sector Impact Assessment

Sector	Threat Level	Key Drivers
Retail	CRITICAL	DragonForce/Scattered Spider M&S attack; UK retail sector at elevated risk
Software/Technology	CRITICAL	Axios, Trivy, Vercel, CanisterSprawl supply chain compromises
Government	HIGH	European Commission breach; APT28 DNS hijacking; Iran operations
Healthcare	HIGH	The Gentlemen targeting; Handala wiper precedent (Stryker); ongoing Iran conflict
Financial Services	HIGH	Grinex exchange compromise; cryptocurrency fraud ($11.36B losses)
Manufacturing	HIGH	Qilin primary targeting; The Gentlemen primary sector
Critical Infrastructure	HIGH	APT28 router compromise; Iranian SCADA/PLC targeting; Salt Typhoon telecom ops
Education	MODERATE	Spring Lake Park ransomware; Qilin opportunistic targeting

Defensive Recommendations

Immediate Actions:

- **Patch CVE-2026-33825 (BlueHammer):** Apply Microsoft Defender Antimalware Platform (update released April 14). Verify Defender platform version is current on all endpoints.
- **Audit for RedSun/UnDefend indicators:** With no patches available, implement compensating controls: monitor Defender service health, alert on definition update failures, consider supplementary AV/EDR layering.
- **Verify Axios npm versions:** Check all projects for versions 1.14.1 or 0.30.4. Search for node_modules/plain-crypto-js/ as a compromise indicator.
- **Scan for Trivy supply chain indicators:** Audit CI/CD pipelines using aquasecurity/trivy-action or aquasecurity/setup-trivy. Rotate all secrets exposed to CI/CD environments that ran Trivy between March 19-24.
- **Patch CVE-2026-33824 (CVSS 9.8):** Wormable Windows IKE RCE. Block UDP 500/4500 if IKE is not required. Apply April Patch Tuesday updates immediately.
- **Audit OAuth integrations:** Review all third-party SaaS OAuth grants in enterprise Google Workspace and Microsoft 365. Revoke overly permissive "Allow All" scopes. Search for the malicious OAuth app ID associated with the Vercel breach.

Short-term Hardening:

- **Deploy BYOVD mitigations:** Enable Windows Defender Application Control (WDAC) or Hypervisor-Protected Code Integrity (HVCI) to block unsigned/vulnerable driver loading. Maintain a blocklist of known BYOVD drivers (rwdrv.sys, NSecKrnl.sys).
- **Implement npm/dependency lockfiles:** Enforce lockfile-only installs (npm ci instead of npm install). Pin dependency versions. Deploy Socket or similar supply chain security tooling.
- **Harden IT helpdesk identity verification:** Implement callback verification for all password reset requests. Require multi-factor verification of caller identity. The M&S breach originated from a social-engineered helpdesk password reset.
- **Layer beyond EDR:** Deploy network detection and response (NDR), behavioral analytics at the hypervisor level, and immutable logging infrastructure that survives EDR neutralization.
- **TP-Link router security:** Audit for TP-Link WR841N routers. Verify that DNS settings are pointing to legitimate resolvers. Apply firmware updates. Change default credentials.

Strategic Recommendations:

- **Assume supply chain compromise:** Treat every dependency update, CI/CD action, and SaaS integration as a potential attack vector. Implement verification pipelines for critical dependencies.
- **Prepare for EDR failure scenarios:** BYOVD EDR killers are now standard ransomware equipment. Architect detection infrastructure to maintain visibility even when endpoint agents are neutralized.
- **Review third-party service desk contracts:** Mandate identity verification standards (MFA-protected callback, video verification) in outsourced IT support agreements. The M&S attack originated from social engineering of a third-party helpdesk operator - a pattern that is highly likely to be replicated against other organizations.
- **Implement SaaS-to-SaaS governance:** Catalog all OAuth integrations across the organization. Enforce least-privilege scoping. Alert on new OAuth grants with broad permissions.
- **Monitor for Vect RaaS targeting:** Organizations that may have been exposed to the Trivy supply chain compromise should proactively engage incident response - the TeamPCP/Vect alliance means compromised organizations are now ransomware targets.

Threat Forecast - May 2026

Forecast	Likelihood	Rationale
Additional Defender zero-day exploitation	**Almost Certain**	Two of three remain unpatched; PoC code publicly available
DragonForce cartel targets additional UK/European retailers	**Highly Likely**	M&S attack validates the cartel model; Scattered Spider remains operational despite prior arrests; UK retail sector is highly likely under active reconnaissance
Vect RaaS victim count acceleration	**Likely**	TeamPCP's supply chain access provides a pipeline of pre-compromised targets
Further npm/PyPI supply chain compromises	**Highly Likely**	CanisterSprawl technique is replicable; open-source trust model under systematic attack
CVE-2026-33824 (IKE RCE) weaponization	**Likely**	CVSS 9.8 wormable vulnerability; historically, such flaws are weaponized within 30-60 days
Continued Iran-aligned cyber operations	**Almost Certain**	Despite internet restoration, Handala and affiliated groups maintain external operational capability
Increased BYOVD EDR killer adoption	**Highly Likely**	Proven technique by Qilin and Warlock; low barrier to replication
AI-enhanced phishing and deepfake escalation	**Highly Likely**	FBI IC3 report confirms mainstream adoption; CISA reports 73% higher success rates

Threat Intelligence Sharing Initiative

As part of the continuous threat intelligence efforts, a dedicated initiative has been launched to publish weekly Threat Intelligence (TI) reports within the LinkedIn group of the Data Security Council of India (DSCI).

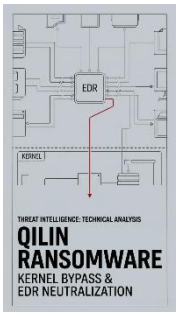
These reports cover focused topics including:

- Dark Web Intelligence & Monitoring
- Cyber Threat Intelligence
- Vulnerability Assessment Insights

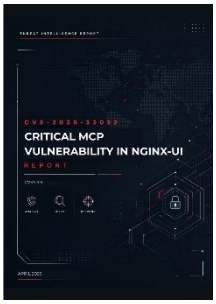
We invite you to join the DSCI LinkedIn group and stay updated with research-driven intelligence reports shared by the team.

Qilin Ransomware DW Analysis

APT28: Operation MacroMaze



Analysis of Weaponized CVEs



Omnibar: Malicious AI browser

DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative

ABOUT DSCI

The Data Security Council of India (DSCI), a Nasscom initiative, is a premier think tank on data protection, cyber security and emerging tech in India. DSCI engages with governments, regulators, industry, and academia to build a secure and trusted cyberspace through policy advocacy, thought leadership, and capacity-building initiatives.

Data Security Council of India
4th Floor, Nasscom Campus, Plot No. 7-10, Sector 126, Noida, UP-201303

data-security-council-of-india/ DSCI_Connect dsci.connect

dsci.connect dscivideo security chips

All Rights Reserved © DSCI 2026