DoD–Defense Industrial Base Collaborative Information Sharing Environment (DCISE)

DOD CYBER CRIME CENTER (DC3)

DIB-REPORTED CYBER THREATS: CY 2026 | Q1 (JAN – MAR)

DC3 DCISE receives voluntary reporting from Defense Industrial Base (DIB) companies through the DoD's DIB Cybersecurity (CS) Program and mandatory reporting as required by DFARS clause 252.204-7012. This product describes trends in cyber activity reported to DC3 DCISE, as well as noteworthy cyber events occurring in CY26 Q1.

DIB REPORTING AT A GLANCE

62% Improper Handling/ Misconfiguration Indents

38% Unauthorized Access Incidents

45% Ransomware Incidents

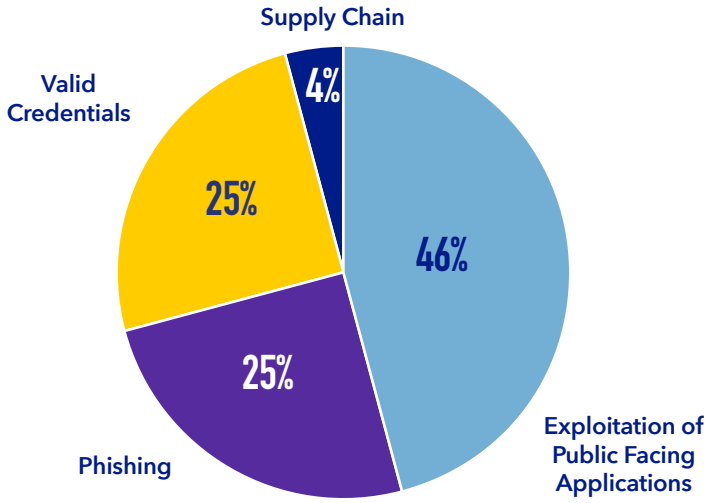
39% Unattributed Incidents

16% Suspected State-Sponsored Incidents

TOP THREE REPORTED RANSOMWARE VARIANTS

1. AKIRA
2. PLAY
3. PAYOUT KINGS

IDENTIFIED INITIAL ACCESS VECTORS



TECHNIQUE OF THE QUARTER:

A threat actor uses email bombing to flood a user's inbox, causing the application to malfunction. The threat actor then uses vishing techniques to masquerade as a Help Desk employee, requesting remote access to the victim's computer through a service like Microsoft Teams or Quick Assist.

Interested in joining the DIB CS Program? Contact us at DC3.DIB.CSRegistration@us.af.mil.

DCISE, a directorate within the DoD Cyber Crime Center, is the operational hub of the DoW's DIB Cybersecurity Program. DCISE develops and shares actionable threat products, performs cyber analysis and diagnostics, and provides remediation consultation for DIB participants.

@DC3DCISE DC3.DCISE@us.af.mil 887.838.2174 | 410.981.0104

DoD—Defense Industrial Base Collaborative Information Sharing Environment (DCISE)

DOD CYBER CRIME CENTER (DC3)

DIB-REPORTED CYBER THREATS: CY 2026 | Q1 (JAN – MAR)

IVANTI ENDPOINT MANAGER EXPLOITATION

Narrative: On 29 Jan 26, Ivanti disclosed two vulnerabilities tracked as CVE-2026-1281 and CVE-2026-1340 impacting Ivanti Endpoint Manager Mobile (EPMM). An unknown threat actor exploited CVE-2026-1281, a remote code execution (RCE) vulnerability, prior to disclosure. In March 2026, Iran-nexus MuddyWater actors also exploited the vulnerability. On 9 Feb 26, Ivanti patched a separate authentication bypass vulnerability affecting its Endpoint Manager (EPM) solution tracked as CVE-2026-1603.

Suspected Threat Actor: Unknown actors, MuddyWater

CVE(s): CVE-2026-1281 (RCE), CVE-2026-1340 (RCE), CVE-2026-1603 (Authentication Bypass)

TTP(s): Exploit Public-Facing Application [T1190]

DCISE Reporting: Alert 26-007, Alert 26-010

Open-Source Reporting: https://unit42.paloaltonetworks.com/ivanti-cve-2026-1281-cve-2026-1340/

5 BIG-IP FLAW ACTIVELY EXPLOITED

Narrative: On 27 Mar 26, CISA added CVE-2025-53521, affecting F5's BIG-IP Access Policy Manager (APM), to the Known Exploited Vulnerabilities (KEV) catalog. Initially categorized as a denial-of-service (DoS), the vulnerability was later labeled as an RCE vulnerability. F5 advised users to be aware of HTTP/S traffic containing HTTP 201 response codes and CSS content-type to disguise the actor's activity. There is no attribution to the reported activity; however, F5 products have historically been exploited by state-sponsored

Suspected Threat Actor: Unknown/ (China-nexus suspected via OSINT)

CVE(s): CVE-2025-53521 (RCE)

TTP(s): Exploit Public-Facing Application [T1190]

DCISE Reporting: Alert 26-013

Open-Source Reporting: https://my.f5.com/manage/s/article/K000156741

SUPPLY CHAIN COMPROMISE – TRIVY SCANNER

Narrative: On 20 Mar 26, Aqua Security announced a compromise of its vulnerability scanner, Trivy. Financially motivated threat actors, tracked as TeamPCP, pushed malicious binaries to Trivy v0.69.4 using continuous integration/continuous delivery secrets and deleting trusted tags. The threat actor published malicious releases of Trivy that are vulnerable to CVE-2026-33634, an embedded malicious code vulnerability, allowing a remote, privileged attacker to obtain potentially sensitive information.

Suspected Threat Actor: TeamPCP

CVE(s): CVE-2026-33634 (Embedded Malicious Code)

TTP(s): Supply Chain Compromise [T1195]

DCISE Reporting: Alert 26-012

Open-Source Reporting: https://github.com/aquasecurity/trivy/discussions/10425
https://github.com/advisories/GHSA-69fq-xp46-6x23

CAMPAIGN TARGETING SALESFORCE CUSTOMERS

Narrative: On 7 Mar 26, Salesforce disclosed an ongoing data theft campaign targeting misconfigured Experience Cloud sites. The financially motivated group ShinyHunters used a modified version of an open-source tool, Aura Inspector, to identify vulnerable objects and extract data through the abuse of overly permissive user settings. Salesforce urged customers to audit guest permissions and enforce a "Least Privilege" access model to defend against this activity.

Suspected Threat Actor: ShinyHunters

CVE(s): None - Exploitation of Misconfigured Guest Accounts

TTP(s): Exploit Public-Facing Application [T1190]

DCISE Reporting: Alert 26-011

Open-Source Reporting: https://www.salesforce.com/blog/protecting-your-data-essential-actions-to-secure-experience-cloud-guest-user-access/