A FEDERAL CYBER CENTER
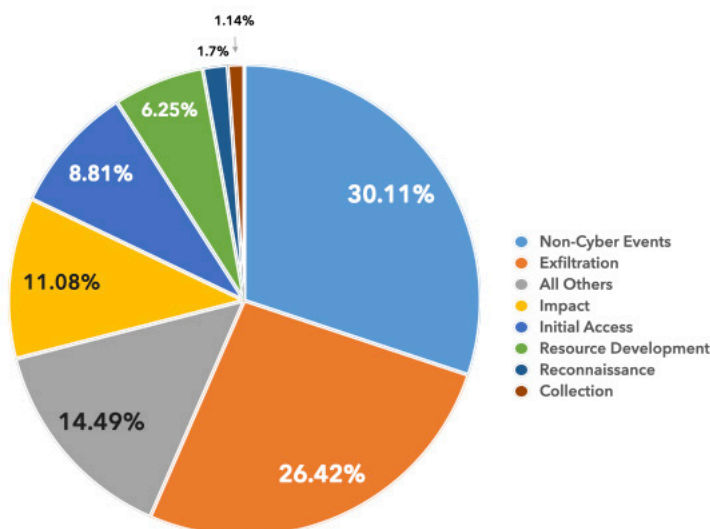
DoD CYBER CRIME CENTER
DoD–Defense Industrial Base Collaborative Information Sharing Environment (DCISE)

DIB-REPORTED CYBER THREATS CY2025 · Q2 (APR-JUN)

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 CY25 Q2.

ALL REPORTED TACTICS: CY25 Q2

- 30.11% Non-Cyber Events
- 26.42% Exfiltration
- 14.49% All Others
- 11.08% Impact
- 8.81% Initial Access
- 6.25% Resource Development
- 1.7% Reconnaissance
- 1.14% Collection

REPORTED RANSOMWARE CY25 Q2

Ransomware-related DIB reporting decreased by **63%** from **CY25 Q1** to **Q2**

**12%** of all **CY25 Q2** mandatory reporting submitted to DC3 DCISE involved ransomware

REPORTED VARIANTS CY25 Q2

Abyss	Play
Akira	Qilin
Blacksuit	Ransomhub
Cactus	Run Some Wares
Dragonforce	Safepay
Interlock	

EMERGING PHISHING TACTICS

- Voice phishing and deepfakes
- AI-enabled phishing (provides personalization, mimics legitimate messages)
- Quishing (QR code phishing)
- Employment related themes
- Brand impersonation
- Smishing (SMS phishing)

INITIAL ACCESS

- 80% Phishing
- 15% Exploitation of Public-Facing Application
- 5% Supply Chain
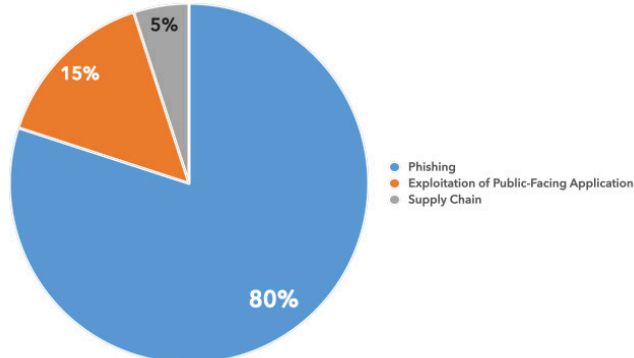
To learn more about the risks associated with systems outside of your perimeter, contact us at **DC3.DCISE@us.af.mil**.

About DCISE

The DoD-Defense Industrial Base Collaborative Information Sharing Environment (DCISE), a directorate within the DoD Cyber Crime Center, is the operational hub of DoD's Defense Industrial Base (DIB) Cybersecurity Program. DCISE develops and shares actionable threat products, performs cyber analysis and diagnostics, and provides remediation consultation for DIB participants.

DC3.DCISE@us.af.mil
877.838.2174 | 410.981.0104

DoD CYBER CRIME CENTER
410.981.6610 | www.dc3.mil | DC3.Information@us.af.mil

𝕏 @DC3Forensics · @DC3DCISE
DC3 Cyber Crime Center

UNCLASSIFIED

TOP CYBER EVENTS CY2025 · Q2 (APRIL-JUNE)

Ivanti Vulnerability
Active Exploitation

Narrative: On 3 Apr 25, Mandiant released details surrounding the active exploitation of CVE-2025-22457 (CVSS 3.1 score 9.8). Mandiant observed active exploitation as early as mid-March 2025, which resulted in the deployment of two newly identified malware families referred to as TRAILBLAZE and BRUSHFIRE. TRAILBLAZE is an in-memory only dropper and BRUSHFIRE is a passive backdoor. The threat actors also deployed the previously reported SPAWN ecosystem malware. SPAWN is associated with a China-nexus espionage actor Mandiant tracks as UNC5221. Mandiant notes the UNC5221 is associated with conducting zero-day exploitation of edge devices since at least 2023. Similar to previous activity, this most recent exploitation attempts to modify Ivanti's Integrity Check Tool (ICT) in order to evade detection.

DCISE Reporting: DCISE Alert 25-007 - Actively Exploited Ivanti Connect Secure Vulnerability

Suspected APT: UNC5221

TTPs: Exploit Public-Facing Application [T1190], Deploying Malware in Memory [TA0002]

Additional Information: https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-exploiting-critical-ivanti-vulnerability

SAP NetWeaver
Active Exploitation

Narrative: On 13 May 25, SAP released Security Notes addressing a critical vulnerability in NetWeaver servers. The vulnerability, tracked as CVE-2025-42999 (CVSS v3 score 9.1), is due to insecure deserialization in SAP NetWeaver Visual Composer Development Server. If a privileged user uploads untrusted or malicious metadata, it could be deserialized in a way that compromises the host system, potentially exposing sensitive data, corrupting system files, or causing a denial-of-service (DoS). Onapsis Research Labs (ORL), a cybersecurity firm, identified the vulnerability and notified SAP, prompting a patch for CVE-2025-42999 to eliminate residual risk CVE-2025-31324 (CVSS v3 score 10.0).

DCISE Reporting: DCISE Alert 25-011 - China Exploiting SAP NetWeaver Vulnerability

Suspected APT: UN5221

TTPs: Stage Capabilities [T1608], Data from Information Repositories [T1213], Network Denial of Service [T1498]

Additional Information: https://support.sap.com/en/my-support/knowledge-base/security-notes-news/may-2025.html

Commvault Vulnerability
Active Exploitation

Narrative: On 17 Apr 25, Commvault published a security advisory addressing a critical vulnerability in the Commvault Command Center installation. The vulnerability, tracked as CVE-2025-34028 (CVSS v3 score 10), is a path traversal remote code execution vulnerability affecting the Command Center Innovation product for Windows and Linux (versions 11.38.0-11.38.19, resolved in 11.38.20 and later). Successful exploitation could lead to a complete compromise of the Command Center environment. A proof-of-concept to exploit this vulnerability is available, however, there is no known exploitation of this vulnerability in the wild.

DCISE Reporting: DCISE Alert 25-008 - Critical Commvault Command Center Vulnerability

Suspected APT: No Attribution

TTPs: Exploit Public-Facing Application [T1190], Exploitation of Remote Services [T1210]

Additional Information: https://documentation.commvault.com/securityadvisories/CV_2025_04_1.html

Fortinet VPNs
Active Exploitation

Narrative: On 10 Apr 25, Fortinet published a blog post detailing the activity of a threat actor that gained access to Fortinet devices through the exploitation of unpatched vulnerabilities and maintained read-only access to the devices after the original access vector was mitigated. The threat actor exploited vulnerabilities including, but not limited to, CVE-2022-42475 (CVSS 3.1 score 9.8), CVE-2023-27997 (CVSS 3.1 score 9.8), and CVE-2024-21762 (CVSS 3.1 score 9.8). The threat actor used a symbolic link (symlink) connecting the user filesystem and the root filesystem in a folder to serve language files for the Secure Sockets Layer Virtual Private Network (SSL VPN).

DCISE Reporting: DCISE Warning 25-159 - Persistence on FortiGate VPNs Via Symlinks

Suspected APT: No Attribution

TTP: Exploit Public-Facing Application [T1190]

Additional Information: https://www.fortinet.com/blog/psirt-blogs/analysis-of-threat-actor-activity

DC3.DCISE@us.af.mil
877.838.2174 | 410.981.0104

DoD CYBER CRIME CENTER
410.981.6610 | www.dc3.mil | DC3.Information@us.af.mil

 @DC3Forensics · @DC3DCISE
 DC3 Cyber Crime Center

UNCLASSIFIED