



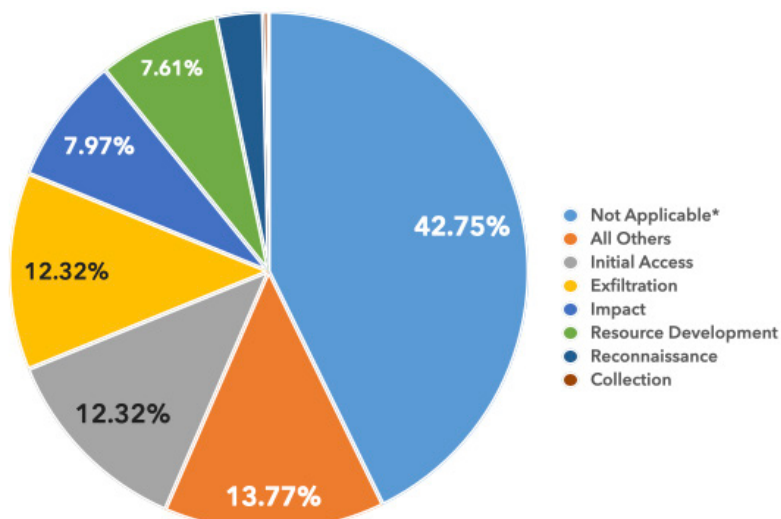
DoD CYBER CRIME CENTER

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

DIB–REPORTED CYBER THREATS CY2025 • 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 CY25 Q1.

ALL REPORTED TACTICS: CY25 Q1



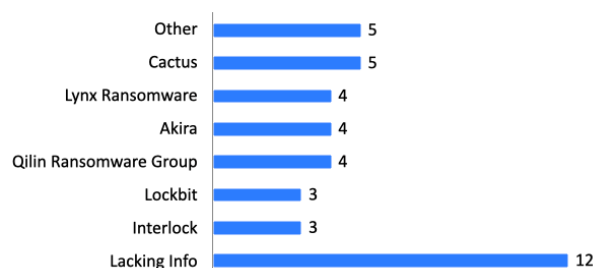
*Not Applicable refers to tactics that do not fall within MITRE ATT&CK framework (e.g., lost/stolen devices)

REPORTED RANSOMWARE CY25 Q1

Ransomware-related mandatory DIB reporting increased by 52% from CY24 Q4 to CY25 Q1

17% of all CY25 Q1 mandatory reporting submitted to DC3 DCISE involved ransomware

REPORTED RANSOMWARE VARIANTS CY25 Q1



REPORTED RANSOMWARE VARIANTS

Phishing continues to be a dominant tactic reported to DC3 DCISE. In-depth analyses of phishing trends are published for DIB CS Program participants in quarterly phishing Threat Activity Reports.

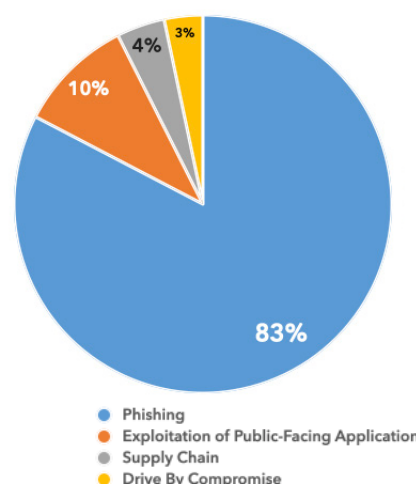
COMMON INITIAL ACCESS VECTORS

- Phishing and Sub-Techniques
- Exploit Public-Facing Applications
- Valid Accounts
- Drive-by Compromise
- External Remote Services
- Spearphishing

PHISHING AND SUB-TECHNIQUES:

Phishing is a tactic that has multiple sub-techniques, including "Spearphishing Link" and "Spearphishing Attachment". Where a sub-technique is not defined, the incident is categorized as "Phishing," when the sub-technique is identified it falls under the associated technique.

INITIAL ACCESS



Pub Date: 19 March 2025

TOP CYBER EVENTS CY2025 • Q1 (JANUARY-MARCH)

North Korean TTPs North Korean Activity

Narrative: On 23 Jan 25, the Federal Bureau of Investigation (FBI) released an alert detailing North Korean IT workers' recent malicious activity. The FBI observed North Korean IT workers unlawfully accessing company networks to exfiltrate proprietary and sensitive data, conduct cybercrime, and generate revenue on behalf of the regime. North Korean IT workers are conducting increasingly aggressive and sophisticated campaigns. Specifically, North Korean IT workers extort victims by holding stolen data hostage and in some cases releasing proprietary code. North Korean IT workers attempt to further compromise companies by copying code repositories to their own personal accounts and harvest sensitive credentials and session cookies to non-company devices.

DCISE Reporting: DCISE Advisory 25-083 – New North Korean IT Worker Tactics

Suspected APT: No APT Attribution

TTPs: Data from Information Repositories [T1213], Steal Web Session Cookies [T1539]

Additional Information: <https://www.ic3.gov/PSA/2025/PSA250123>

Silk Typhoon TTPs Chinese Activity

Narrative: On 5 Mar 25, Microsoft Threat Intelligence released a report detailing the Chinese espionage group, Silk Typhoon. On 5 Mar 25, the US Justice Department charged 12 Chinese hackers, including at least 2 linked to Silk Typhoon, with stealing data from US federal and state government organizations, including the US Department of Treasury in late 2024. According to Microsoft, Silk Typhoon shifted to new tactics targeting common IT solutions, including remote management tools and cloud applications to gain initial access. In Jan 2025, Microsoft observed Silk Typhoon exploiting an Ivanti zero-day tracked as CVE-2025-0282 (CVSS v3 score 9). Silk Typhoon targets a range of vulnerabilities including those that exist in Microsoft Exchange servers, Palo Alto firewalls, Citrix devices, and Ivanti devices.

DCISE Reporting: DCISE Advisory 25-115 – Silk Typhoon Targeting IT Supply Chain

Suspected APT: Silk Typhoon

TTPs: Steal Application Access Token [T1528], Create Account [T1136], Compromise Accounts [T1586]

Additional Information: <https://www.microsoft.com/en-us/security/blog/2025/03/05/silk-typhoon-targeting-it-supply-chain/>

VMware Vulnerabilities Active Exploitation

Narrative: On 4 Mar 25, Broadcom released an alert addressing VMware zero-day vulnerabilities affecting ESXi, Workstation, and Fusion. According to Broadcom, exploitation of the vulnerabilities has occurred in the wild. The alert covers CVE-2025-22224 (CVSS v3 score 9.3), CVE-2025-22225 (CVSS v3 score 8.2), and CVE-2025-22226 (CVSS v3 score of 7.1). CVE-2025-22224 is a heap-overflow vulnerability affecting ESXi and Workstation. CVE-2025-22225 is an arbitrary write vulnerability affecting ESXi. CVE-2025-22226 is an information disclosure flaw affecting the Host Guest File System (HGFS). Ransomware groups, including TargetCompany, Play, RansomHub, and Qilin are targeting ESXi.

DCISE Reporting: DCISE Warning 25-122 – Exploited VMware Zero Days

Suspected APT: TargetCompany, Play, RansomHub, Qilin

TTPs: Phishing [T1566], Supply Chain Compromise [T1195]

Additional Information: <https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390>

Ivanti Vulnerability Active Exploitation

Narrative: On 3 Apr 25, Ivanti released an advisory addressing an actively exploited vulnerability affecting Ivanti Connect Secure (version 22.7R2.5 and earlier), Pulse Connect Secure 9.x (end-of-support as of December 31, 2024), Ivanti Policy Secure and ZTA gateways. The vulnerability, tracked as CVE-2025-22457 (CVSS v3 score 9.0), is a stack-based overflow that allows a remote unauthenticated attack to achieve remote code execution (RCE). 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.

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

Suspected APT: UNC5221

TTP: Command and Control – Web Service [T1102]

Additional Information: https://forums.ivanti.com/s/article/April-Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-22457?language=en_US