



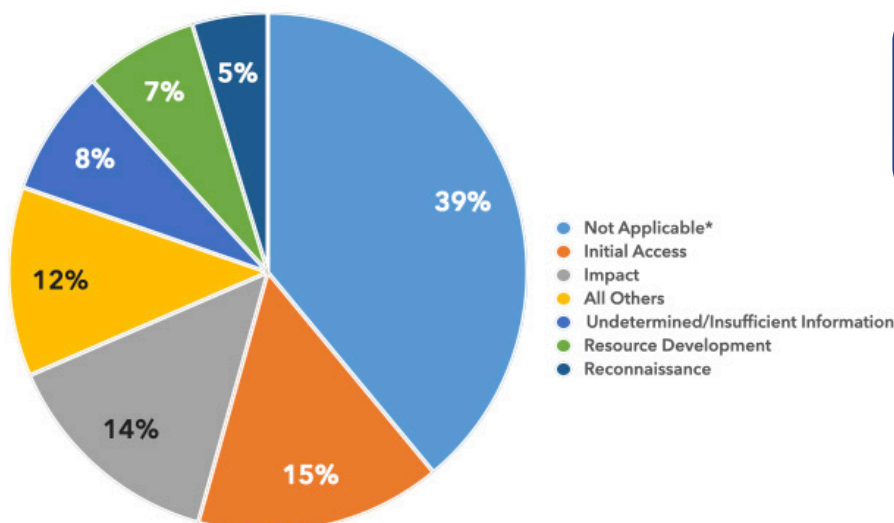
DoD CYBER CRIME CENTER

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

DIB–REPORTED CYBER THREATS CY2024 • Q3 (JUL–SEP)

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 CY24 Q3.

ALL REPORTED TACTICS: CY24 Q2



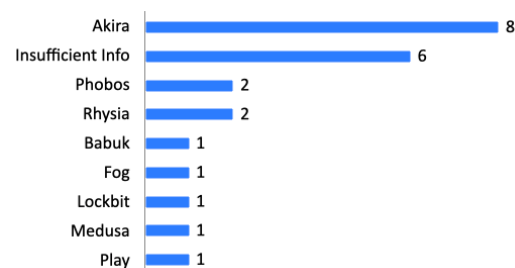
*Not Applicable refers to tactics that do not fall within MITRE ATT&CK framework (e.g., lost/stolen devices)

REPORTED RANSOMWARE CY24 Q3

Ransomware-related mandatory DIB reporting increased by 17% from CY24 Q2 to Q3

12% of all CY24 Q3 mandatory reporting submitted to DC3 DCISE involved ransomware

REPORTED VARIANTS CY24 Q3



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.

To join the DIB CS Program, apply at <https://dibnet.dod.mil>.

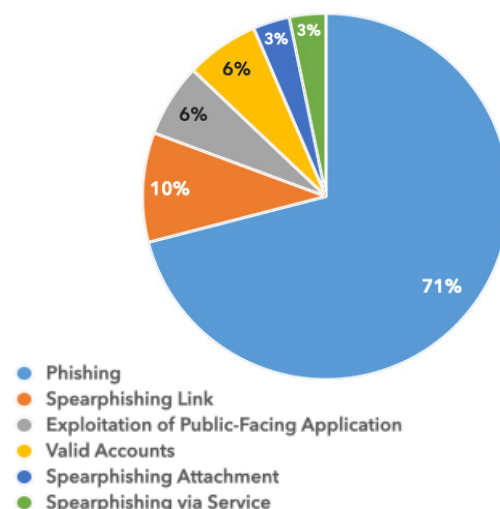
COMMON INITIAL ACCESS VECTORS

- 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: 22 November 2024

TOP CYBER EVENTS CY2024 • Q3 (JULY-SEPTEMBER)

Microsoft Zero-Day Chinese Activity

Narrative: On 27 Aug 24, Black Lotus Labs reported on the active exploitation of a zero-day vulnerability affecting Versa Director servers. The vulnerability, tracked as CVE-2024-39717 (CVSS v3 score 7.2), is found in Versa software-defined wide area network (SD-WAN) applications and affects all Versa Director versions prior to 22.1.4. Researchers identified a custom-tailored web shell referred to as "VersaMem." Versa Director servers, often used by internet service providers (ISPs) and managed service providers (MSPs), manage network configurations for clients running SD-WAN software. Based on observed TTPs, Black Lotus Labs attributes the zero-day exploitation of CVE-2024-39717 and use of the VersaMem web shell to the Chinese threat group tracked as Volt Typhoon.

DCISE Reporting: DCISE Warning 24-209 - Chinese Volt Typhoon Exploits Versa Director

Suspected APT(s): Volt Typhoon

TTPs: Exploit Public-Facing Application [T1190]

Additional Information: https://blog.lumen.com/taking-the-crossroads-the-versa-director-zero-day-exploitation/?utm_source=feedly&utm_medium=rss&utm_campaign=taking-the-crossroads-the-versa-director-zero-day-exploitation

Contagious Interview North Korean Activity

Narrative: In August 2024, the Department of Treasury's Office of Cybersecurity and Critical Infrastructure Protection (OCCIP) and DoD's Cyber Crime Center published a joint report describing Contagious Interview's associated tactics, techniques, and procedures (TTPs). Contagious Interview is a cluster of malicious cyber activity that targets cryptocurrency entities, individuals, and organizations. Evidence suggests a possible North Korean association with Contagious Interview activity includes job interview-themed and skills assessment-themed social engineering, use of Astrill virtual private network (VPN), targeting of cryptocurrency, and laundering through mixers such as Tornado.cash and Railgun.

DCISE Reporting: DCISE Advisory 24-333 - Contagious Interview TTPs

Suspected APT(s): Contagious Interview

TTPs: Exploit Public-Facing Application [T1190], Exploitation for Privilege Escalation [T1068], Exploitation for Credential Access [T1212]

Additional Information: <https://unit42.paloaltonetworks.com/two-campaigns-by-north-korea-bad-actors-target-job-hunters/targeting-perimeter-network-devices/>

Windows Zero-Day Active Exploitation

Narrative: On 10 Sep 24, Microsoft released its September 2024 Patch Tuesday security update, including four zero-day vulnerabilities. The four zero-day vulnerabilities include CVE-2024-43491 (CVSS v3 9.8), a remote code execution (RCE) that reintroduces a variety of vulnerabilities to previous programs. An attacker could exploit previously patched vulnerabilities in Windows 10 version 1507 systems having Windows security updates released on 12 Mar 24, or other updates released through August 2024.

DCISE Reporting: DCISE Warning 24-218 - Four Actively Exploited Windows Zero-Days

Suspected APT(s): Unknown

TTPs: Exploit Public-Facing Application [T1190], Exploitation for Privilege Escalation [T1068]

Additional Information: <https://msrc.microsoft.com/update-guide/releaseNote/2024-Sep>

Ivanti Vulnerability Chinese Exploitation

Narrative: On 19 Sep 24, Ivanti released an advisory detailing a vulnerability in their Cloud Service Application (CSA) version 4.6 tracked as CVE-2024-8963 (CVSS v3 score 9.4). This is a path traversal vulnerability that could allow remote unauthenticated attackers to access restricted functions. Threat actors can exploit CVE-2024-8963 in conjunction with CVE-2024-8190 to bypass admin authentication and execute arbitrary commands on the appliance.

DCISE Reporting: DCISE Alert 24-013 - Ivanti CSA Active Exploitation

Suspected APT(s): China-nexus espionage group UNC5221

TTPs: Exploit Public-Facing Application [T1190]

Additional Information: https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-CSA-4-6-Cloud-Services-Appliance-CVE-2024-8963?language=en_US