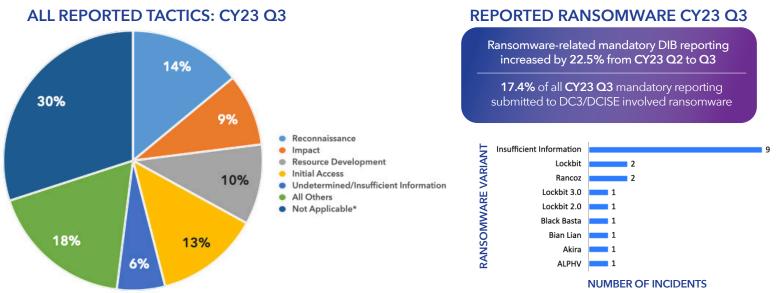A FEDERAL CYBER CENTER

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

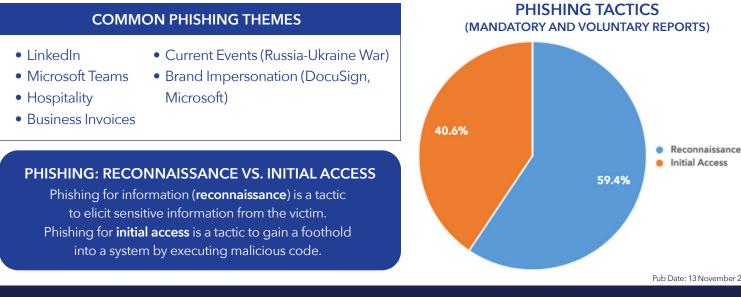# DIB-REPORTED CYBER THREATS CY2023 · Q3 (JUL–SEP)

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 CY23 Q3.

ALL REPORTED TACTICS: CY23 Q3

- Reconnaissance
- Impact
- Resource Development
- Initial Access
- Undetermined/Insufficient Information
- All Others
- Not Applicable*

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

REPORTED RANSOMWARE CY23 Q3

Ransomware-related mandatory DIB reporting increased by **22.5%** from **CY23 Q2** to **Q3**

17.4% of all **CY23 Q3** mandatory reporting submitted to DC3/DCISE involved ransomware

RANSOMWARE VARIANT

Variant	Number of Incidents
Insufficient Information	9
Lockbit	2
Rancoz	2
Lockbit 3.0	1
Lockbit 2.0	1
Black Basta	1
Bian Lian	1
Akira	1
ALPHV	1

NUMBER OF INCIDENTS

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 bi-annual phishing Threat Activity Reports. To join the DIB CS Program, apply at **https://dibnet.dod.mil**.

COMMON PHISHING THEMES

- LinkedIn
- Microsoft Teams
- Hospitality
- Business Invoices
- Current Events (Russia-Ukraine War)
- Brand Impersonation (DocuSign, Microsoft)

PHISHING: RECONNAISSANCE VS. INITIAL ACCESS
Phishing for information (**reconnaissance**) is a tactic to elicit sensitive information from the victim. Phishing for **initial access** is a tactic to gain a foothold into a system by executing malicious code.

PHISHING TACTICS
(MANDATORY AND VOLUNTARY REPORTS)

- Reconnaissance — 59.4%
- Initial Access — 40.6%

Pub Date: 13 November 2023

TOP-REPORTED CYBER EVENTS CY2023 · Q3 (JULY–SEPTEMBER)

Barracuda ESG Vulnerability
Chinese Exploitation

Narrative: On 15 Jun 23, Mandiant researchers identified a suspected Chinese APT known as UNC 4841 actively exploiting a remote command injection vulnerability in the Barracuda Email Security Gateway (ESG) appliance, tracked as CVE-2023-2868 (CVSS v3 score 9.4), affecting versions 5.1.3.001-1.2.0.006. As early as 10 Oct 22, UNC4841 sent emails containing malicious file attachments designed to exploit the vulnerability for initial access. UNC4841 deployed backdoors, including a novel backdoor named SUBMARINE, and other custom utilities for data exfiltration.

DCISE Reporting: DCISE Warning 23-113 – *Barracuda ESG Exploited by China*, DCISE Warning 23-098 – *Barracuda Zero Day*, DCISE Advisory 23-255 – *Submarine Malware on Barracuda ESG*

TTPs: Exploit Public-Facing Application [T1190], Phishing [T1566], Exfiltration [TA0010]

Associated Malware: SALWATER, SEASIDE, SUBMARINE, SKIPJACK, SEASPRAY, SEASPY

Additional Information:
https://www.mandiant.com/resources/blog/barracuda-esg-exploited- globally

Cisco ASA SSL VPNs
Active Exploitation

Narrative: On 29 Aug 23, Rapid7 published a report detailing the exploitation of Cisco ASA SSL VPNs. Since at least March 2023, attackers targeted physical and virtual Cisco ASA SSL VPN appliances in credential-stuffing and brute-force attacks. The brute- force attacks took advantage of appliances where multi-factor authentication (MFA) was not enabled or enforced for all users. Several incidents resulted in the deployment of Akira and LockBit ransomware variants.

DCISE Reporting: DCISE Advisory 23-287 – *Exploitation of Cisco ASA SSL VPNs*

TTPs: Brute Force [T1110], Credential Stuffing [T1110.004] Associated Malware: LockBit, Akira

Additional Information:
https://www.rapid7.com/blog/post/2023/08/29/under-siege-rapid7- observed-exploitation-of-cisco-asa-ssl-vpns/

Adobe ColdFusion
Critical Vulnerability

Narrative: On 11 Jul 23, Adobe released a security bulletin detailing CVE-2023-29300 (CVSS v3 Score 9.8), a remote code execution (RCE) vulnerability. Unauthenticated operators may exploit the vulnerability in low complexity attacks. According to Bleeping Computer, it is unknown how CVE-2023-29300 is being exploited; however, Project Discovery published a blog post containing a proof-of-concept exploit for the vulnerability.

DCISE Reporting: DCISE Alert 23-020 – *Adobe ColdFusion Vulnerability Actively Exploited*

TTPs: Exploit Public-Facing Application [T1190], Server Software Component: Web Shell [T1505], Modify Authentication Process [T1556]

Additional Information:
https://www.bleepingcomputer.com/news/security/critical-coldfusion- flaws-exploited-in-attacks-to-drop-webshells/

Atlassian Confluence Vulnerability
Chinese Exploitation

Narrative: On 10 Oct 23, Microsoft Threat Intelligence released a series of tweets revealing a China-linked actor known as Storm-0062 exploited a critical Atlassian Confluence vulnerability beginning as early as 14 Sep 23. The vulnerability, tracked as CVE-2023-22515 (CVSS v3 score 9.8), is a privilege escalation vulnerability that allows an attacker to create a Confluence administrator account, affecting Atlassian Confluence Data Center and Server 8.0.0 and later. Atlassian patched the vulnerabilities in versions 8.4.3, 8.3.3, and 8.5.2.

DCISE Reporting: DCISE Alert 24-001 – *Suspected Atlassian Exfiltration Activity*, DCISE Warning 24-012 – *China Exploits Atlassian Confluence*

Suspected APTs: Storm-0062 (also known as DarkShadow, Oro0lyxy)

TTPs: Exploit Public-Facing Application [T1190], Exploitation for Privilege Escalation [T1068], Exfiltration [TA0010]

Additional Information:
https://therecord.media/chinese-govt-hackers-exploiting-atlassian

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
in DC3 Cyber Crime Center

UNCLASSIFIED