



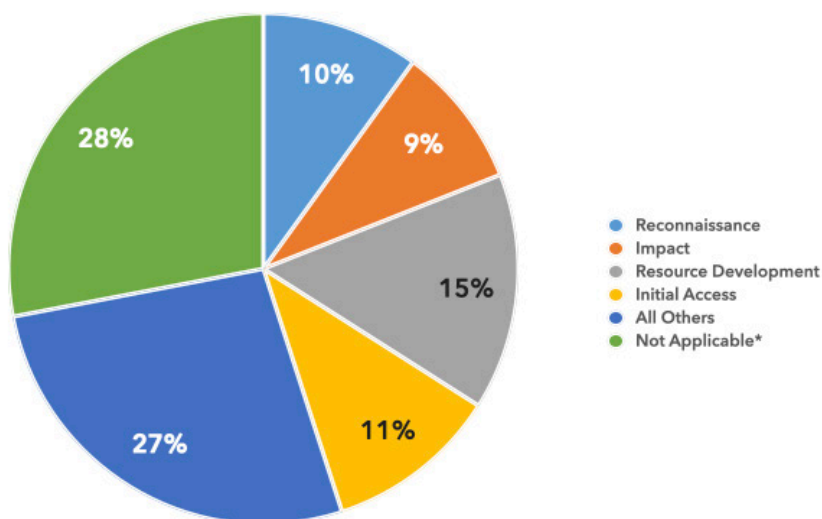
DoD CYBER CRIME CENTER

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

DIB-REPORTED CYBER THREATS CY2023 • Q4 (OCT-DEC)

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 Q4.

ALL REPORTED TACTICS: CY23 Q4

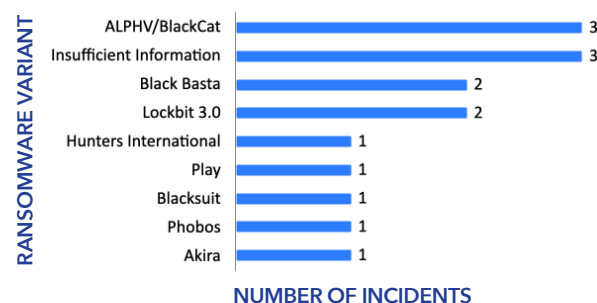


*Not Applicable refers to tactics that do not fall within MITRE ATT&CK framework (e.g., lost/stolen devices)

REPORTED RANSOMWARE CY23 Q4

Ransomware-related mandatory DIB reporting decreased by 16.7% from CY23 Q3 to Q4

8.7% of all CY23 Q4 mandatory reporting submitted to DC3/DCISE involved ransomware



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

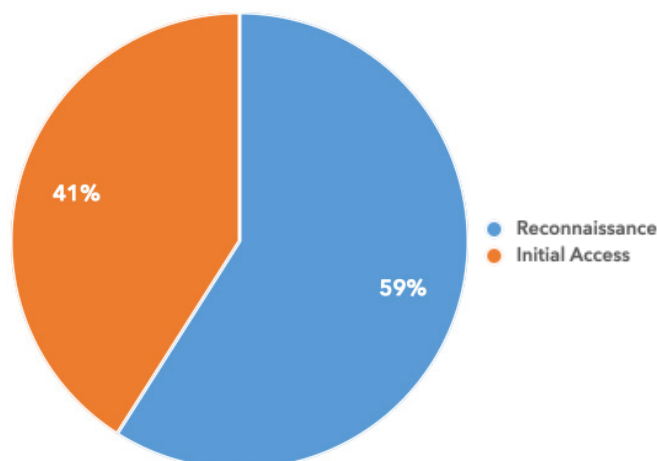
- Brand Impersonation (PayPal, Microsoft)
- Business Email Compromise
- Healthcare
- Hospitality
- LinkedIn

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)



Pub Date: 8 February 2024

TOP-REPORTED CYBER EVENTS CY2023 • Q4 (OCTOBER-DECEMBER)

Barracuda Chinese Exploitation

Narrative: On 24 Dec 23, the network and email security firm Barracuda reported on active exploitation of their Email Security Gateway (ESG) appliances. The activity is attributed to a China nexus actor tracked as UNC4841. UNC4841 was observed targeting a vulnerability in a third-party library (Spreadsheet::ParseExcel) to deploy malicious Excel email attachments on vulnerable ESG appliances. The vulnerability, tracked as CVE-2023-7102 (CVSS score not yet determined), is an arbitrary code execution (ACE) vulnerability that affects unpatched ESG appliances through a parameter injection.

DCISE Reporting: DCISE Advisory 23-264 - *SEASPY and WHIRLPOOL Backdoors*, DCISE Warning 23-113 - *Barracuda ESG Exploited by China*, DCISE Warning 23-098 - *Barracuda Zero Day*

Suspected APTs: UNC4841

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

Associated Malware: SALWATER, SEASPY

Additional Information: <https://www.barracuda.com/company/legal/esg-vulnerability>

Atlassian Confluence Chinese Exploitation

Narrative: On 10 Oct 23, Microsoft Threat Intelligence released a series of tweets revealing nation-state actor Storm-0062 (also known as OroOlyxy) exploited CVE-2023-22515, affecting Atlassian Confluence Data Center and Server 8.0.0 and later. CVE-2023-22515 (NIST CVSS v3 score 9.8; Atlassian CVSS v3 score 10.0) is a critical privilege escalation vulnerability caused by broken authentication and sessions management that allows an attacker to create a Confluence administrator account within the application.

DCISE Reporting: DCISE Warning 24-012 - *China Exploits Atlassian Confluence*, DCISE Alert 24-001 - *Suspected Atlassian Exfiltration Activity*, DCISE Alert 24-003 - *Atlassian Improper Authorization Vulnerability*

Suspected APTs: Storm-0062

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

Additional Information: <https://thehackernews.com/2023/10/microsoft-warns-of-nation-state-hackers.html>

CitrixBleed Active Exploitation

Narrative: On 25 and 31 Oct 23, researchers at Assetnote and Mandiant, respectively, published information regarding the exploitation of CVE-2023-4966 (CVSS v3 score 9.4, published on 10 Oct 23), referred to as "CitrixBleed." CVE-2023-4966 can result in the takeover of legitimate user sessions and affects Citrix NetScaler ADC and NetScaler Gateway. The vulnerability is remotely exploited by unauthenticated attackers. On 17 Oct 23, Mandiant reported the vulnerability was exploited by at least six cybercrime groups beginning in August 2023, with attacks targeting government organizations and technology companies.

DCISE Reporting: DCISE Warning 24-010 - *Critical NetScaler Flaw*, DCISE Warning 24-010 - *Citrix Hypervisor Vulnerabilities*, DCISE Advisory 24-043 - *CitrixBleed Exploitation*

TTPs: Exploitation for Privilege Escalation [T1068], Exfiltration [TA0010]

Associated Malware: LockBit, Medusa

Additional Information: <https://www.bleepingcomputer.com/news/security/new-critical-citrixnetscaler-flaw-exposes-sensitive-data/>

Fortinet Vulnerability Active Exploitation

Narrative: On 12 Dec 23, Fortinet released three advisories identifying vulnerabilities within various Fortinet products. The most severe of the vulnerabilities, tracked as CVE-2023-42678 (CVSS v3 8.3), is a double-free vulnerability that allows an authenticated attacker to achieve arbitrary code execution. The remaining two vulnerabilities, tracked as CVE-2022-27488 (CVSS v3 7.5) and CVE-2023-36639 (CVSS v3 7.0), allow for cross-site scripting forgery and execution of unauthorized code, respectively. The vulnerabilities were exploited during the second half of 2023 with previous Fortinet exploits linked to Chinese cyberespionage groups.

DCISE Reporting: DCISE Alert 24-004 - *Fortinet FortiSIEM Critical Command Injection Vulnerability*, DCISE Warning 24-013 - *Fortinet Vulnerabilities*, DCISE Warning 24-045 - *Multiple Fortinet Vulnerabilities*

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

Additional Information: <https://www.fortiguard.com/psirt/FG-IR-23-196>