



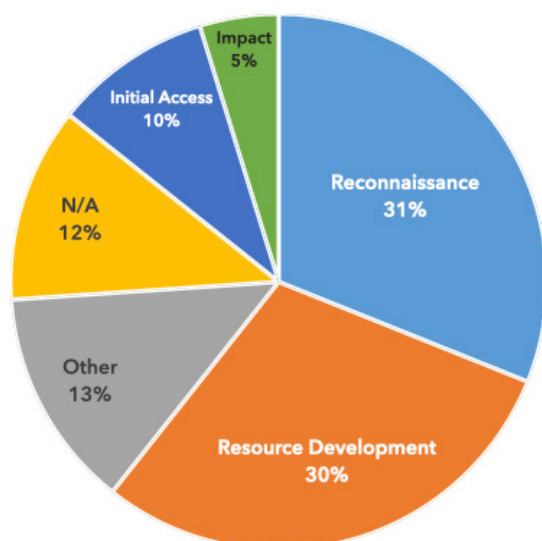
DoD CYBER CRIME CENTER

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

DIB–REPORTED CYBER THREATS CY2022 Q2 (APR–JUN)

DC3/DCISE receives voluntary reporting from Defense Industrial Base (DIB) companies through the DoD's DIB Cybersecurity 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 CY22 Q2.

ALL REPORTED TACTICS (VOLUNTARY AND MANDATORY REPORTS)



REPORTED RANSOMWARE

Ransomware-related DIB reporting increased by 4% from CY22 Q1 to CY22 Q2

23% of all CY22 Q2 mandatory reporting submitted to DC3/DCISE involved ransomware



MOST REPORTED RANSOMWARE TO DCISE

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 PHISHING THEMES

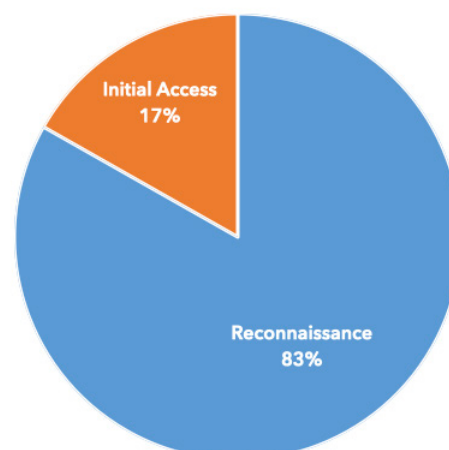
- Outstanding Invoices
- Payment for commonly known vendors
- IRS/Tax related
- Tech support
- Business email compromise
- Streaming services
- Package delivery
- Advanced fees

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 (VOLUNTARY AND MANDATORY REPORTS)



Pub Date: 4 August 2022

DIB-REPORTED CYBER THREATS CY2022 • Q2 (APR-JUN)

Atlassian Confluence

Active Exploitation

Narrative: On 2 Jun 22, Atlassian released an advisory detailing CVE-2022-26134 (CVSS v3 score 9.8), a vulnerability allowing unauthenticated operators to execute remote code. The vulnerability was originally discovered by the cybersecurity firm Volexity during an incident response, who observed malicious operators leveraging the vulnerability along with a web shell known as Behinder as well as China Chopper. Volexity assessed that Chinese APT operators were responsible.

DCISE Reporting: Alert 22-025

Suspected APT: Possible Chinese APT

TTP: Exploitation of a public facing service (T1190)

Associated Malware:

Behinder web shell, China Chopper web shell

Additional Information:

<https://www.volexity.com/blog/2022/06/02/zero-day-exploitation-of-atlassian-confluence/>

VMware

Exploited by Iranian APT

Narrative: On 18 May 22, CISA released an alert detailing the exploitation of VMware vulnerabilities by APTs. The two vulnerabilities, CVE-2022-22954 (CVSS v3 score 9.8) and CVE-2022-22960 (CVSS v3 score 7.8), allow server-side template injection resulting in remote code execution and escalation of root privileges. On 23 Jun 22, CISA released an alert to emphasize APTs, to include Iranian APT35, continued to exploit the Log4Shell vulnerability (CVE-2021-44228, CVSS v3 score 10.0) in VMware Horizon Systems.

DCISE Reporting: Alert 22-023, Warning 22-071

Suspected APTs: APT35

TTP: Exploitation of a public facing service (T1190)

Associated Malware:

Dingo J-spy web shell

Additional Information:

<https://www.cisa.gov/uscert/ncas/alerts/aa22-138b>
<https://www.cisa.gov/uscert/ncas/alerts/aa22-174a>

Microsoft Follina

Multiple APT Exploitation

Narrative: On 27 May 22, a security researcher identified a zero-day vulnerability affecting Microsoft office known as Follina. Tracked as CVE-2022-30190 (CVSS v3 score 7.8), the vulnerability allows operators to execute malicious PowerShell commands via the Microsoft Diagnostic Tool (MSDT), allowing operators to escalate privileges and bypass Windows Defender detection. China and Russia APT groups reportedly employed Follina.

DCISE Reporting: Alert 22-024, Advisory 22-103

Suspected APT: APT28, TA413, Twisted Panda

TTPs: Phishing (T1566)

Associated Malware: Cobalt Strike, Credo

Additional Information: <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30190>

F5 BIG-IP Vulnerability

Used to Wipe Devices

Narrative: On 4 May 22, F5 issued a security advisory for an unauthenticated remote code execution (RCE) vulnerability affecting BIG-IP. Tracked as CVE-2022-1388 (CVSS v3 score 9.8) the vulnerability may allow an operator to gain complete control of system. The vulnerability reportedly affected over 16,000 devices publicly exposed to the internet and represents a large security risk for corporations. On 9 May 22, SANS ISC reported the vulnerability was used in destructive attacks attempting to erase a device's file system, though the attacks did not appear widespread.

DCISE Reporting:

Alert 22-022, Warning 22-090, Warning 22-098

Suspected APT: N/A

TTP: Data destruction (T1485)

Associated Malware: N/A

Additional Information:

<https://www.cisa.gov/uscert/ncas/alerts/aa22-138a>

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.

To learn more about the risks associated with systems outside of your perimeter, contact us at DC3.DCISE@us.af.mil.