



DoD CYBER CRIME CENTER

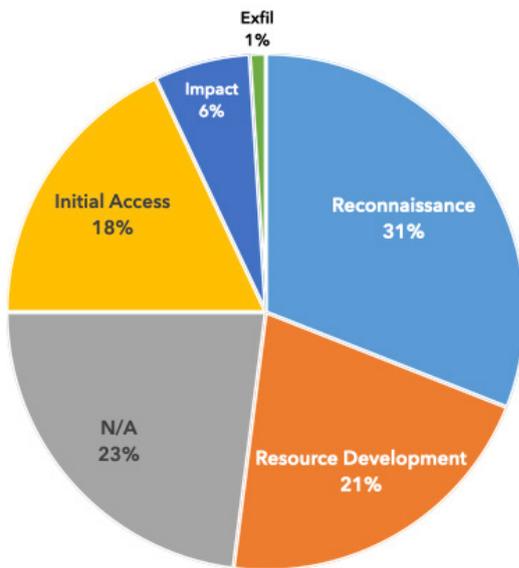
DoD–Defense Industrial Base Collaborative Information Sharing Environment (DCISE)

DIB–REPORTED CYBER THREATS

CY2022 Q4 (OCT–DEC)

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 Q4.

ALL REPORTED TACTICS: CY22 Q4

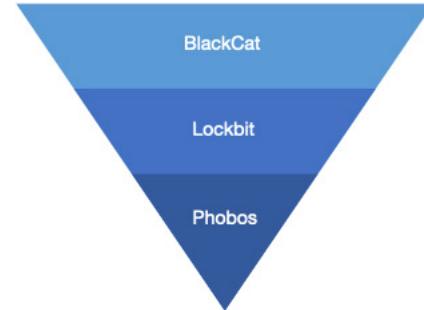


REPORTED RANSOMWARE CY22 Q4

Ransomware-related DIB reporting increased by 6% from CY22 Q3 to CY22 Q4

16% of all CY22 Q4 mandatory reporting submitted to DC3/DCISE involved ransomware

MOST REPORTED VARIANTS (MOST-TO-LEAST REPORTED)



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

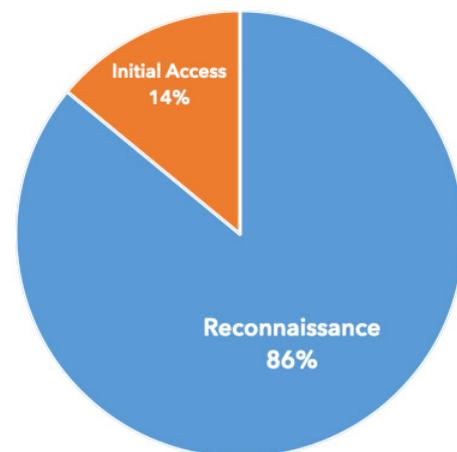
- LinkedIn
- Brand Impersonation
- Business Email Compromise
- Job Offers
- Prize/Award
- Password Reset

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: 3 February 2023

DIB-REPORTED CYBER THREATS CY2022 • Q4 (OCT-DEC)

APT5 Targeting

Citrix CVE-2022-27518

Narrative: On 6 Dec 22, the National Security Agency reported on APT5, a China-affiliated threat group known for targeting high-tech manufacturing and military technology in the United States, Europe, and Asia, that demonstrated capabilities in leveraging CVE-2022-27518 found in Citrix Application Delivery Controller (ADC) deployments. The vulnerability contains an authentication bypass exposure which allows an attacker to execute code as an administrator. APT5 is also known as "UNC2630" and "MANGANESE."

DCISE Reporting: Alert 23-008, Warning 23-029

Suspected APT: APT5 (UNC2630)

TTPs: T1190-Exploit Public-Facing Application

Associated Malware: Unknown

Additional Information: <https://media.defense.gov/2022/Dec/13/2003131586/-1/-1/0/CSA-APT5-CITRIXADC-V1.PDF>

Iranian APT Targets USG

CVE-2021-44228

Narrative: On 16 Nov 22, the Cybersecurity and Infrastructure Security Agency (CISA), released an alert (AA22-320A) detailing how a federal network was compromised by Iranian state-sponsored APT actors. As early as February 2020, the US Merit Systems Protection was likely compromised by actors using the Log4Shell vulnerability (CVE-2021-44228) on an unpatched VMware Horizon server. Since the Log4Shell vulnerabilities were exploited in this attack, the threat actors obtained access to a VMware service account with administrator and system-level access.

DCISE Reporting: Advisory 23-040

Suspected APTs: Unknown

TTP: T1190-Exploit Public-Facing Application, T1059.001-PowerShell command, T1098-Account Manipulation

Associated Malware: Unknown

Additional Information: <https://www.cisa.gov/uscert/ncas/alerts/aa22-320a>

Use of Wipers

Endurance Ransomware and Iran APT Activity

Narrative: On 15 Nov 22, a user on Breach Forums advertised an alleged database containing 2.34GB of data from multiple US government agencies after being impacted by Endurance Wiper ransomware. The malware source code bears similarity to Shamoon 4 wiper. On 7 Dec 22, ESET researchers documented a supply chain attack that occurred in February 2022 which leveraged a data wiper dubbed "Fantasy." The attack is attributed to Iranian-linked advanced persistent threat (APT) known as "Agrius."

DCISE Reporting: Warning 23-20, Advisory 23-50

Suspected APT: APT33, APT Agrius

TTPs: T1485-Data Destruction

Associated Malware: Endurance Wiper, Shamoon 4 Wiper

Additional Information: <https://www.welivesecurity.com/2022/12/07/fantasy-new-agrius-wiper-supply-chain-attack/-wiper-supply-chain-attack/>

Russian APT Activity

Russian APT Targeting Ukraine and NATO

Narrative: On 20 Dec 22, researchers from Palo Alto Networks Unit 42 published an article highlighting Russian APT Trident Ursa's activity and focused targeting efforts against Ukraine. A multitude of indicators of compromise (IoCs), to include IP addresses, domains, and malware hashes, were gathered to highlight and share current overall understanding of Trident Ursa's operations. On 30 Aug 22, Trident Ursa launched an attack targeting a petroleum refining company in a NATO country, but was unsuccessful.

DCISE Reporting: Advisory 23-061

Suspected APT: APT Trident Ursa

TTP: T1190-Exploit Public-Facing Application

Associated Malware: Unknown

Additional Information: <https://unit42.paloaltonetworks.com/trident-ursa/>

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.