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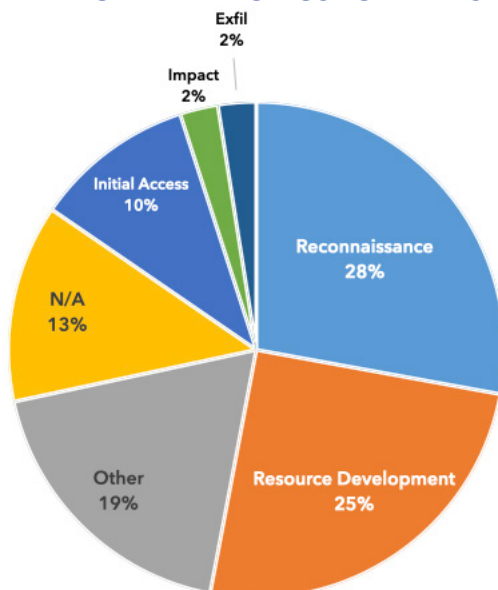
DoD CYBER CRIME CENTER
DoD–Defense Industrial Base Collaborative Information Sharing Environment (DCISE)

DIB–REPORTED CYBER THREATS   CY2022 Q3 (JUL–SEP)

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 Q3.

ALL REPORTED TACTICS: CY22 Q3

- Exfil 2%
- Impact 2%
- Initial Access 10%
- N/A 13%
- Other 19%
- Reconnaissance 28%
- Resource Development 25%

REPORTED RANSOMWARE CY22 Q3

Ransomware-related DIB reporting decreased by **13%** from **CY22 Q2** to **CY22 Q3**

10% of all **CY22 Q3** mandatory reporting submitted to DC3/DCISE involved ransomware

MOST REPORTED VARIANTS (MOST-TO-LEAST REPORTED)

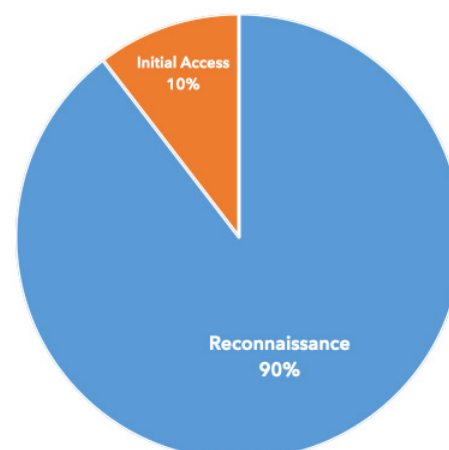- BlackBasta
- BlackCat
- Babuk
- Hive
- Makop

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

- Invoice
- Tax related
- Callback
- PayPal
- Queen Elizabeth II
- Payment
- Business email compromise
- Subscriptions
- Job offers
- MonkeyPox

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)

- Initial Access 10%
- Reconnaissance 90%

Pub Date: 31 October 2022

DIB-REPORTED CYBER THREATS CY2022 • Q3 (JUL–SEP)

Zimbra
Active Exploitation

Narrative: On 10 Aug 22, Volexity disclosed operators exploiting a remote code execution (RCE) vulnerability (CVE-2022-27925) affecting Zimbra. Initially the activity was associated with espionage-oriented operators but later used by other threat operators. On 16 Aug 22, CISA reported threat operators exploited multiple CVEs against Zimbra's services. CVE-2022-27924, CVE-2022-27925 chained with CVE- 2022-37042, CVE-2022-30333, and CVE-2022-24682 were exploited.

DCISE Reporting: Advisory 23-008, Warning 22-122, Alert 22-028

Suspected APT: Unknown

TTP: Exploit Public-Facing Application (T1190)

Associated Malware: Cobalt Strike

Additional Information: https://www.cisa.gov/uscert/ncas/alerts/aa22-228a & https://www.volexity.com/blog/2022/08/10/mass-exploitation- of-unauthenticated-zimbra-rce-cve-2022-27925/

Lazarus
Three RATs

Narrative: On 8 Sep 22, researchers at Cisco Talos published a report on North Korean state-sponsored APT activity occurring from February to July 2022. The APT, tracked as the "Lazarus Group" (also known as "APT38" or "Hidden Cobra"), targeted the energy sector in the United States, Canada, and Japan. The group gained initial access through VMware vulnerabilities. After initial access, the group was observed using three different custom malwares: VSingle, YamaBot, and MagicRAT.

DCISE Reporting: Advisory 22-121, CRF-22160-005-SUP01

Suspected APTs: Lazarus/APT38

TTP: Stage Capabilities (T1608), Create Account (T1136), Remote Services (T1021)

Associated Malware: VSingle, YamaBot, MagicRAT

Additional Information: https://blog.talosintelligence.com/2022/09/lazarus-three- rats.html

VMware ESXi Servers
Backdoors Discovered

Narrative: On 29 Sep 22, Mandiant researchers published details of a novel malware, tracked as "VirtualPita" and "VirtualPie", which establishes persistence on VMware ESXi hypervisors. Mandiant assessed the operator is tied to China-based operators, tracked as UNC3886. The malware allows the operators to maintain persistent administrator access to the hypervisor, send commands to a VM, transfer files between the ESXi hypervisor and guest machines, tamper with logging services, and execute arbitrary commands from a guest VM to another VM running on the same hypervisor.

DCISE Reporting: Warning 22-141

Suspected APT: UNC3886

TTPs: Remote Services (T1021), Boot or Logon Autostart Execution (T1547)

Associated Malware: VirtualPita, VirtualPie

Additional Information: https://www.mandiant.com/resources/blog/esxi-hypervisors- malware-persistence

Atlassian
New Vulnerabilities

Narrative: On 20 Jul 22, Atlassian released details on CVE-2022- 26138 (CVSS v3 x 9.8), affecting Confluence. The vulnerability allows an operator to obtain a hardcoded password. On 29 Jul 22, CISA added CVE-2022-26138 to the Known Exploited Vulnerability Catalogue (KEV). On 24 Aug 22, Atlassian released details of a separate vulnerability affecting BitBucket and Data Center products, tracked as CVE-2022-36804 (CVSS v3 x 9.9). On 30 Sep 22, CVE- 2022-36804 was added to the KEV.

DCISE Reporting: Warning 22-138, Alert 22-027

Suspected APT: Unknown

TTP: Exploit Public-Facing Application (T1190)

Associated Malware: Unknown

Additional Information: https://confluence.atlassian.com/doc/questions-for-confluence- security-advisory-2022-07-20-1142446709.htm & https://confluence.atlassian.com/bitbucketserver/bitbucket- server-and-data-center-advisory-2022-08-24- 1155489835.html

--- 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**.

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

@DC3Forensics • @DC3DCISE
DC3 Cyber Crime Center

UNCLASSIFIED