A FEDERAL CYBER CENTER

DoD CYBER CRIME CENTER

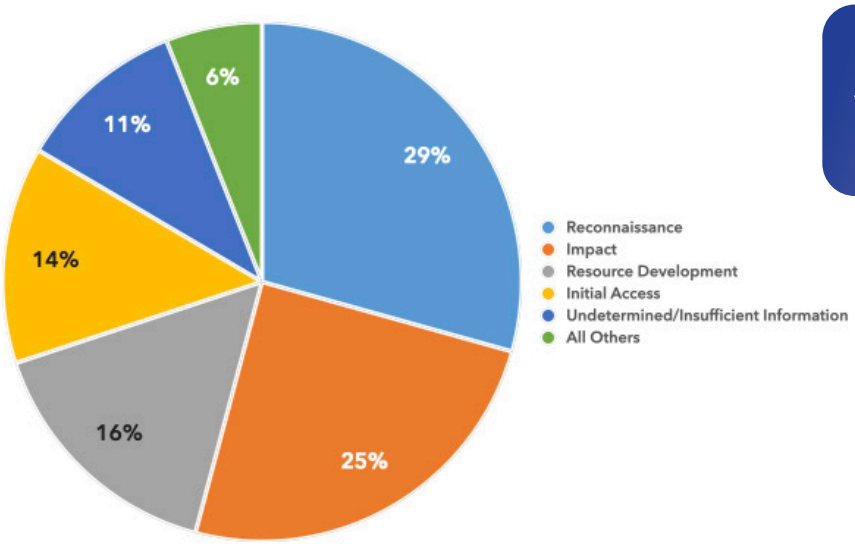
DoD–Defense Industrial Base Collaborative Information Sharing Environment (DCISE)

DIB-REPORTED CYBER THREATS

CY2023 Q1 (JAN-MAR)

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 CY23 Q1.

ALL REPORTED TACTICS: CY23 Q1

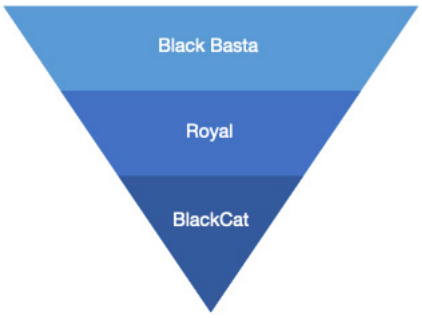


REPORTED RANSOMWARE CY23 Q1

Ransomware-related DIB reporting increased by **169%** from **CY22 Q4** to **CY23 Q1**

33% of all **CY23 Q1** 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 bi-annual phishing Threat Activity Reports. To join the DIB CS Program, apply at **https://dibnet.dod.mil**.

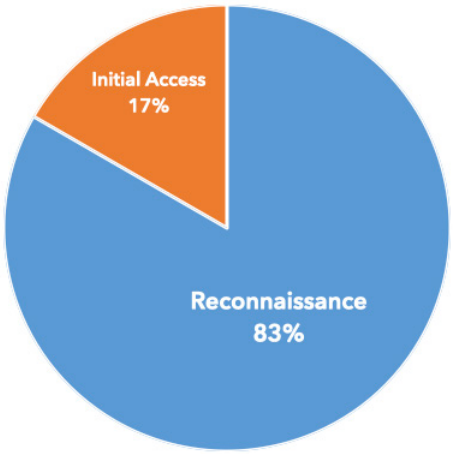
COMMON PHISHING THEMES

- LinkedIn
- Brand Impersonations
- Business Email Compromise
- Job Offers
- Prize/Awards
- Password Resets

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: 18 May 2023

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

DIB-REPORTED CYBER THREATS CY2023 • Q1 (JAN-MAR)

Fortinet
Chinese Exploitation

Narrative: On 16 Mar 23, Mandiant reported abuse of Fortinet vulnerabilities, likely by Chinese threat actors. In mid-2022, Mandiant coordinated with Fortinet to investigate the exploitation and deployment of malware across various Fortinet products including FortiManager and FortiAnalyzer. The actor used two new malware strains in the Fortinet activity: THINCRUST (backdoor) and CASTLETAP (ICMP port-knocking passive backdoor).

DCISE Reporting: Advisory 23-129 – China Associated Fortinet Activity, Warning 23-066 – FortiOS Zero-Day (CVE-2022-41328)

Suspected APT: UNC3886

TTPs: Stored data Manipulation (T1565.001)

Associated Malware: VIRTUALPITA, THINCRUST, and CASTLETAP

Additional Information: https://www.mandiant.com/resources/blog/fortinet-malware-ecosystem & https://www.mandiant.com/resources/blog/esxi-hypervisors-detection-hardening

North Korean APTs
Ransomware Activity

Narrative: On 9 Feb 23, the Cybersecurity and Infrastructure Security Agency (CISA) published an alert (AA23-040A) detailing how the Democratic People's Republic of Korea (DPRK) state-sponsored threat actors orchestrated ransomware attacks, targeting Healthcare and Public Health (HPH) organizations to fund their national objectives. North Korean advanced persistent threat (APTs) have historically used the following malware: BitLocker, Deadbolt, ech0raix, GonnaCry, Hidden Tear, Jigsaw, LockBit 2.0 My Little Ransomware, NxRansomware, Ryuk, and YourRansom.

DCISE Reporting: Advisory 23-093 – North Korean APT Ransomware Activity, Advisory 22-107 – Maui Ransomware

Suspected APT: North Korean APTs

TTP: Acquire Infrastructure (T1583), Gain Access (TA0001)

Associated Malware: Maui, H0lyGh0st, WannaCry

Additional Information: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-040a

SonicWall
Chinese Malware

Narrative: On 8 Mar 23, Mandiant published a report detailing a suspected Chinese malware that has the ability to persist on SonicWall devices after firmware updates are applied. Operators are targeting unpatched SonicWall Secure Mobile Access (SMA) 100 series appliances to install the malware for long-term persistence. The malware allows operators to steal user credentials and provides command shell access.

DCISE Reporting: Warning 23-065 – Persistent Chinese Malware Infecting SonicWall

Suspected APT: UNC4540

TTPs: Boot or Logon Initialization Scripts (T1037)

Associated Malware: TinyShell

Additional Information: https://www.mandiant.com/resources/blog/suspected-chinese-persist-sonicwall & https://www.sonicwall.com/support/knowledge-base/upgrade-path-for-sma100-series/190314100423452/

Cisco
High Severity Vulnerability

Narrative: On 8 Mar 23, Cisco released an advisory describing a vulnerability within their bidirectional forward detection (BFD) hardware offload feature. The vulnerability, tracked as CVE-2023-20049 (CVSSv3 score 8.6), allows an "unauthenticated, remote attacker to cause a line card to reset, resulting in a denial-of-service (DoS) condition." Patches for this vulnerability were included in IOS XR software versions 7.5.3, 7.6.2, and 7.7.1.

DCISE Reporting: Warning 23-064 – Cisco routers Exposed to high Severity Vulnerability

Additional Information: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bfd-XmRescbT & https://www.securityweek.com/vulnerability-exposes-cisco-enterprise-routers-to-disruptive-attacks/

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