



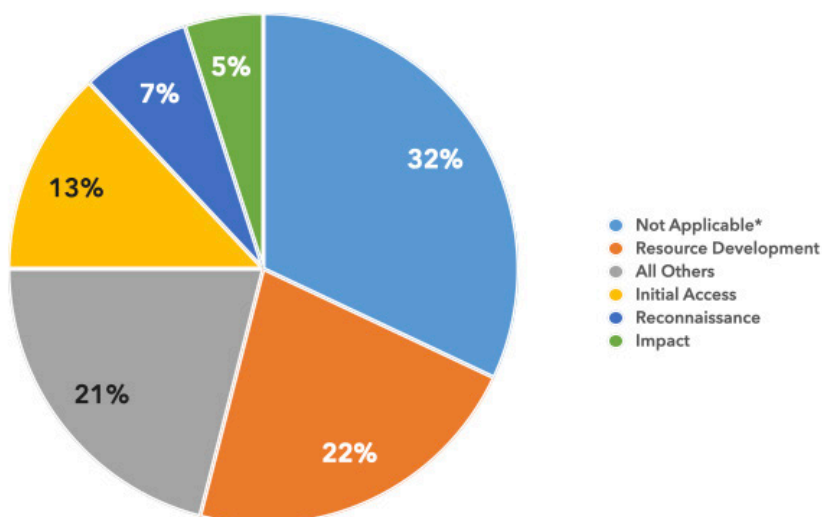
DoD CYBER CRIME CENTER

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

DIB–REPORTED CYBER THREATS CY2024 • Q1 (JAN–MAR)

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 CY24 Q1.

ALL REPORTED TACTICS: CY24 Q1

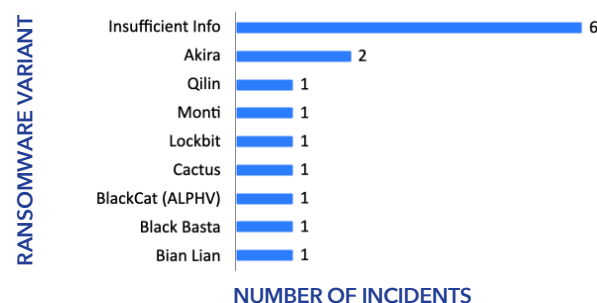


*Not Applicable refers to tactics that do not fall within MITRE ATT&CK framework (e.g., lost/stolen devices)

REPORTED RANSOMWARE CY24 Q1

Ransomware-related mandatory DIB reporting increased by 24.1% from CY23 Q4 to CY24 Q1

10.8% of all CY24 Q1 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 quarterly phishing Threat Activity Reports. To join the DIB CS Program, apply at <https://dibnet.dod.mil>.

COMMON PHISHING THEMES

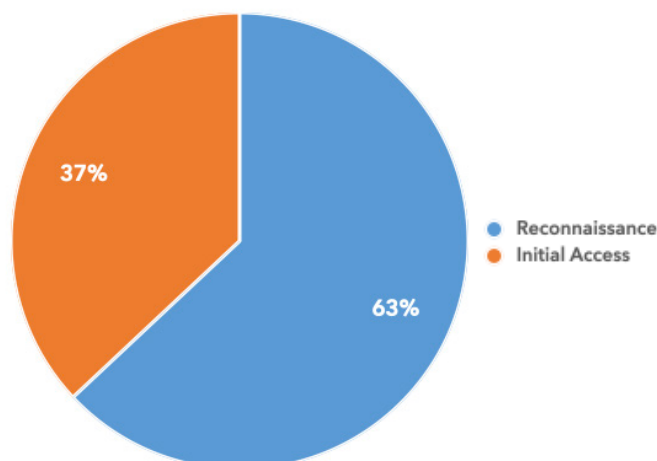
- Brand Impersonation (Microsoft, AWS)
- LinkedIn
- Hospitality
- Shipping and Invoicing
- Mobile Device Targeting

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: 21 June 2024

TOP-REPORTED CYBER EVENTS CY2024 • Q1 (JANUARY-MARCH)

Ivanti Secure Connect Active Exploitation

Narrative: On 10 Jan 24, Ivanti released a security advisory identifying two vulnerabilities within the Ivanti Connect Secure (ICS) and Policy Secure Gateways. CVE-2023-46805 (CVSS v3 score 8.2) is an authentication bypass vulnerability affecting the web component of ICS virtual private network (VPN) appliances and Ivanti Policy Secure that enables threat actors to access restricted resources. CVE-2024-21887 (CVSS v3 score 9.1) is a command injection vulnerability affecting the web components of ICS and Ivanti Policy Secure that may allow unauthenticated admins to execute arbitrary commands on vulnerable appliances. On 27 Feb 24, Mandiant disclosed that Chinese threat actors known as UNC5325 maintained persistence on affected ICS VPN appliances even after factory resets, system upgrades, and installed patches.

DCISE Reporting: Warning 24-055 - *Ivanti Zero-Day Active Exploitation*

Suspected APTs: UNC5325

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

Additional Information: <https://www.ivanti.com/blog/topics/security-advisory>

F5 BIG-IP Chinese Exploitation

Narrative: On 26 Oct 23, F5 released a security advisory pertaining to a remote code execution (RCE) vulnerability in the BIG-IP configuration utility. Tracked as CVE-2023-46747 (CVSS v3 score 9.8), the vulnerability allows a malicious actor "with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands." Mandiant assessed that as early as October 2023, Chinese threat actors UNC5174 used a mixture of custom tooling and the SUPERSHELL framework to exploit the vulnerability.

DCISE Reporting: Warning 24-019 - *F5 BIG-IP RCE Vulnerability*

Suspected APTs: UNC5174

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

Additional Information: <https://www.mandiant.com/resources/blog/initial-access-brokers-exploit-f5-screenconnect>

Citrix Zero-Day Active Exploitation

Narrative: On 16 Jan 24, Citrix released a Security Bulletin detailing two vulnerabilities affecting Citrix NetScaler ADC and Gateway appliances. The first vulnerability, tracked as CVE-2023-6548 (CVSS v3 score 5.5), allows authenticated remote code execution with low privileges on the Citrix Management Interface. The second vulnerability, tracked as CVE-2023-6549 (CVSS v3 score 8.2), is a denial of service (DoS) vulnerability. Citrix warned that these vulnerabilities were actively exploited. Citrix noted that the impacted NetScaler ADC and NetScaler Gateway version 12.1 is end-of-life (EOL) and customers should upgrade their appliance to mitigate the vulnerability.

DCISE Reporting: Warning 24-065 - *Citrix Zero-Days Actively Exploited*

TTPs: Exploit Public-Facing Application [T1190]

Additional Information: <https://www.bleepingcomputer.com/news/security/citrix-warns-of-new-netscaler-zero-days-exploited-in-attacks>

Phishing Campaigns Russian APT

Narrative: On 11 Mar 24, IBM X-Force published a blog post detailing ongoing phishing campaigns conducted by the Russian threat group tracked as ITG05. ITG05 shares overlapping activity with APT28 (also known as UAC-028, Fancy Bear, and Forest Blizzard), which is attributed to the Russian General Staff Main Intelligence Directorate (GRU). In November 2023, ITG05 sent phishing lures imitating government and non-governmental organizations (NGOs) worldwide, using themes related to various topics including cybersecurity and defense industrial production. Russian APTs affiliated with the GRU historically target the DIB for cyber espionage purposes and are likely to target organizations providing support to Ukraine.

DCISE Reporting: Advisory 24-200 - *Russian APT Phishing Campaigns*

TTPs: T1566-Phishing

Suspected APTs: ITG05

Additional Information: <https://thehackernews.com/2024/03/apt28-hacker-group-targeting-europe.html>