A FEDERAL CYBER CENTER

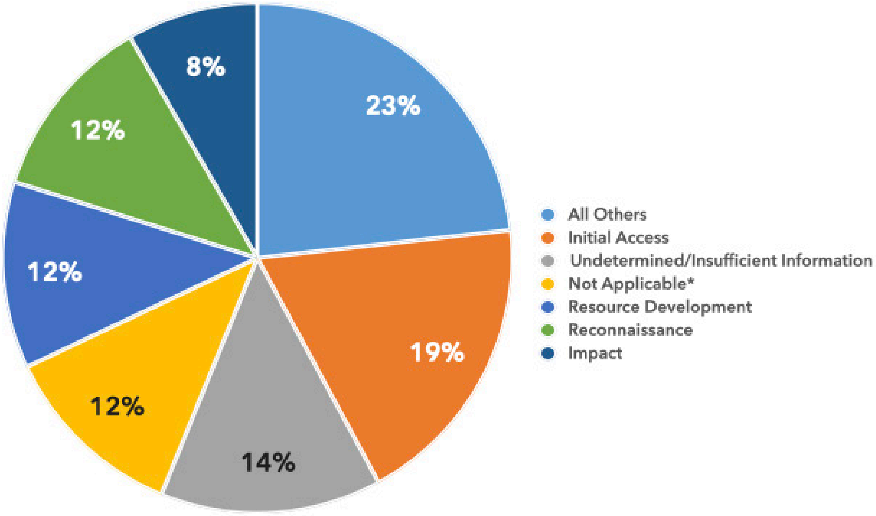
DoD CYBER CRIME CENTER

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

DIB-REPORTED CYBER THREATS CY2024 • Q2 (APR–JUN)

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 Q2.

ALL REPORTED TACTICS: CY24 Q2

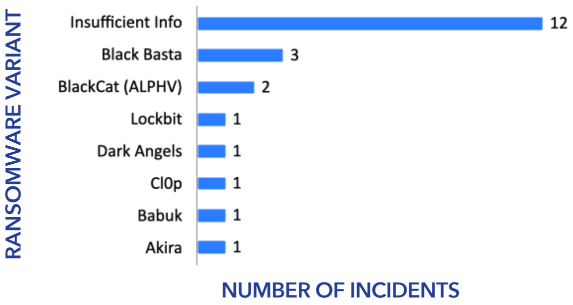


*Not Applicable refers to tactics that do not fall within MITRE ATT&CK framework (e.g., lost/stolen devices)

REPORTED RANSOMWARE CY24 Q2

Ransomware-related mandatory DIB reporting increased by **38.9%** from **CY24 Q1** to **Q2**

15% of all **CY24 Q2** 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.

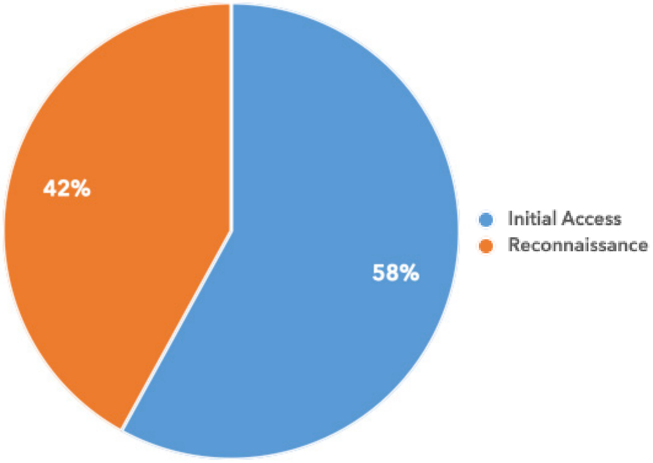
COMMON PHISHING THEMES

- Tech Support
- Job Recruitment
- Brand Impersonation (Microsoft, OneDrive, Okta)
- Shipping and Invoicing
- Voice Phishing (Vishing)
- QR Code Phishing (Quishing)

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: 16 August 2024

TOP-REPORTED CYBER EVENTS CY2024 • Q2 (APRIL-JUNE)

Palo Alto PAN-OS Zero-Day
Active Exploitation

Narrative: On 12 Apr 24, Palo Alto Networks released a security advisory addressing a critical vulnerability affecting the PAN-OS software GlobalProtect feature. The vulnerability, tracked as CVE-2024-3400 (CVSS v3 score 10), allows an unauthenticated attacker to execute arbitrary code with root privileges on the firewall. The vulnerability affects PAN-OS 10.2.9-h1 and prior, 11.0.4-h1 and prior, and 11.1.2-h3 and prior. On 12 Apr 24, Palo Alto Networks and Volexity published blog posts detailing activity tracked as Operation MidnightEclipse exploiting CVE-2024-3400, beginning as early as 26 Mar 24. The threat actors attempted to exploit the vulnerability to install a backdoor referred to as UPSTYLE, which allows the attacker to execute additional commands on the device.

DCISE Reporting: Alert 24-010 - *PAN-OS Command Injection Vulnerability Actively Exploited*

Suspected APT(s): Unknown

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

Additional Information: https://security.paloaltonetworks.com/CVE-2024-3400

Cisco Zero-Day
Active Exploitation

Narrative: On 24 Apr 24, Cisco disclosed two actively exploited vulnerabilities in Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defense (FTD) software. The vulnerabilities, tracked as CVE-2024-20359 (CVSS score 6.0) and CVE-2024-20353 (CVSS score 8.6), allow an attacker to execute arbitrary code with root-level privileges and create a denial of service (DoS) condition. Cisco Talos identified likely state-sponsored threat actor activity, tracked as UAT4356 (also STORM-1849), exploiting these vulnerabilities to implant custom malware and execute commands on government networks. Exploitation likely began in November 2023.

DCISE Reporting: Alert 24-011 - *Cisco ASA and FTD Software Actively Exploited*

Suspected APT(s): UAT4356 (also STORM-1849)

TTPs: Exploit Public-Facing Application [T1190], Exploitation for Privilege Escalation [T1068], Endpoint Denial of Service [T1499]

Additional Information: https://blog.talosintelligence.com/arcanedoor-new-espionage-focused-campaign-found-targeting-perimeter-network-devices/

Velvet Ant Activity
F5 BIG-IP Exploitation

Narrative: On 16 Jun 24, the Israeli cybersecurity company Sygnia published details of a Chinese-nexus threat group tracked as Velvet Ant abusing F5 BIG-IP load balancers to maintain persistence on victim networks and establish command and control (C2) channels for data exfiltration. Velvet Ant is a sophisticated threat group with robust capabilities and a methodical approach to espionage operations. Velvet Ant began its attack chain using two versions of PlugX, a modular remote access trojan (RAT) used by several threat actors associated with Chinese interests. The threat actor disabled endpoint security software prior to installing PlugX and used open-source tools, including Impacket, for lateral movement.

DCISE Reporting: Advisory 24-287 - *China Exploits F5 BIG-IP*

Suspected ATP(s): Velvet Ant

TTPs: Exploit Public-Facing Application [T1190], Exfiltration Over C2 Channel [T1041]

Additional Information: https://www.sygnia.co/blog/china-nexus-threat-group-velvet

UNC3886 Activity
Continued Persistence

Narrative: On 18 Jun 24, Mandiant published details of a China-nexus cyber espionage actor targeting prominent strategic organizations on a global scale. The threat actor, tracked as UNC3886, is linked to network intrusions involving malware installations on VMware ESXi hypervisors and the exploitation of a now-patched vulnerability in Fortinet FortiOS (CVE-2022-42475). The threat actor employs several layers of persistence to maintain access to compromised systems and uses publicly available rootkits, dubbed Reptile and Medusa, to evade detection, steal credentials, execute commands, and move laterally.

DCISE Reporting: Advisory 24-292 - *Chinese UNC3886 Continued Persistence*

Suspected APT(s): UNC388

TTPs: Exploit Public-Facing Application [T1190], Exploitation for Privilege Escalation [T1068], Exploitation for Credential Access [T1212]

Additional Information: https://cloud.google.com/blog/topics/threat-intelligence/uncovering-unc3886-espionage-operations