A FEDERAL CYBER CENTER

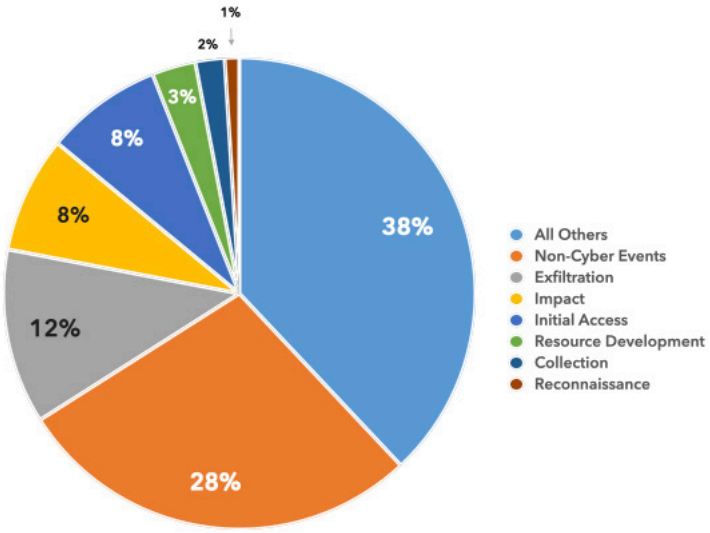
DoD CYBER CRIME CENTER

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

DIB-REPORTED CYBER THREATS CY2025 • Q4 (OCT-DEC)

DC3 DCISE receives voluntary reporting from Defense Industrial Base (DIB) companies through the DoW'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 CY25 Q4.

ALL REPORTED TACTICS: CY25 Q4



REPORTED RANSOMWARE: CY25 Q4

Ransomware-related DIB reporting decreased by **26%** from **CY25 Q3** to **Q4**

14% of all **CY25 Q4** mandatory reporting submitted to DC3 DCISE involved ransomware

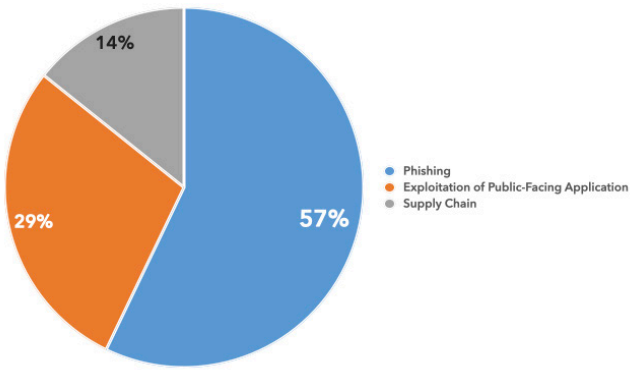
REPORTED VARIANTS CY25 Q3

Abyss Locker
Akira
INC
Nitrogen
Play
Qilin

EMERGING PHISHING TACTICS

- Voice phishing and deepfakes
- AI-enabled phishing (provides personalization, mimics legitimate messages)
- Quishing (QR code phishing)
- Employment-related themes
- Brand impersonation
- Smishing (SMS phishing)

INITIAL ACCESS TECHNIQUES: CY25 Q4



To learn more about the risks associated with systems outside of your perimeter, contact us at **DC3.DCISE@us.af.mil**.

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 DoW'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.

Pub Date: 11 February 2026

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

𝕏 @DC3Forensics • @DC3DCISE
DC3 Cyber Crime Center

DIB-REPORTED CYBER THREATS CY2025 • Q4 (OCTOBER–DECEMBER)

F5 Security Incident
Chinese Activity

Narrative: On 15 Oct 25, F5 published the details of a security incident involving unauthorized access to internal company systems. On 9 Aug 25, F5 discovered that a state-sponsored threat actor exfiltrated files containing source code and information about undisclosed vulnerabilities in the BIG-IP product development environment and engineering knowledge management platform. On 22 Oct 25, security researchers uncovered the BRICKSTORM malware on F5 systems. BRICKSTORM is reported to be affiliated with China-nexus threat actor UNC5221.

DCISE Reporting: DCISE Alert 26-001 – F5 Security Incident, DCISE Advisory 26-005 – China BRICKSTORM Malware

Suspected APT: UNC5221

TTPs: Exfiltration Over C2 Channel [T1041], Valid Accounts [T1078]

Additional Information:
https://my.f5.com/manage/s/article/K000154696
https://cloud.google.com/blog/topics/threat-intelligence/brickstorm-espionage-campaign/

Cisco ASA Vulnerabilities
Actively Exploited

Narrative: On 31 Oct 25, Recorded Future's The Record published updated information about a China-nexus threat actor, known as Storm-1849, scanning for and exploiting vulnerabilities in Cisco Adaptive Security Appliances (ASAs). The vulnerabilities, tracked as CVE-2025-20333 (CVSS v3 score 9.9) and CVE-2025-20362 (CVSS v3 score 6.5), can be chained together to gain access to vulnerable devices before manipulating them, allowing their access to persist through reboots and system upgrades. Targeted entities include financial institutions, defense contractors, federal agencies, and military organizations within the United States, Europe, and Asia.

DCISE Reporting: DCISE Warning 26-029 – Actively Exploited Cisco ASA Vulnerabilities

Suspected APT: Storm-1849

TTP: Exploit Public-Facing Application [T1190]

Additional Information: https://therecord.media/chinese-hackers-scan-exploit-firewalls-government

Chinese Actors Target US Organizations
Chinese Activity

Narrative: On 6 Nov 25, Symantec by Broadcom published a report on China-linked threat actors targeting organizations involved in US policy. On 5 Apr 25, attackers initiated a malicious campaign by conducting a mass scan of a server, attempting to exploit a wide range of critical vulnerabilities, including Atlassian Object-Graph Navigation Language (OGNL) Injection (CVE-2022-26134), Log4j (CVE-2021-44228), Apache Struts (CVE-2017-9805), and GoAhead remote code execution (RCE) (CVE-2017-17562). These activities, aligned with historical trends and current geopolitical tensions, are notable for the use of shared tools across multiple groups (Kelp, Space Pirates, and APT41), making definitive attribution difficult.

DCISE Reporting: DCISE Advisory 26-031 – China-linked Actors Target US Organizations

Suspected APTs: Kelp, Space Pirates, APT41

TTPs: Exploit Public-Facing Application [T1190], Active Scanning [T1595]

Additional Information: https://www.security.com/threat-intelligence/china-apt-us-policyblog/murky-panda-trusted-relationship-threat-in-cloud/

React2Shell Vulnerability
Chinese Activity

Narrative: On 12 Dec 25, Google Threat Intelligence Group (GTIG) released a report detailing multiple threat actors exploiting CVE-2025-55182 (CVSS v4 score 10.0), otherwise known as React2Shell. CVE-2025-55182 is an unauthenticated remote code execution (RCE) vulnerability in React Server Components. GTIG disclosed five China-nexus cyber actors exploiting React2Shell to deliver multiple malware files on victim's networks. Additionally, open-source reporting uncovered North Korean (DPRK) and ransomware attackers exploited the React2Shell flaw.

DCISE Reporting: DCISE Advisory 26-048 – Multiple Threat Actors Exploit React2Shell Flaw

Suspected APTs: UNC5454, UNC6600, UNC6603, UNC5342, Jackpot Panda, Weaxor Ransomware

TTP: Exploit Public-Facing Application [T1190]

Additional Information: https://cloud.google.com/blog/topics/threat-intelligence/threat-actors-exploit-react2shell-cve-2025-55182/

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

𝕏 @DC3Forensics • @DC3DCISE
DC3 Cyber Crime Center