



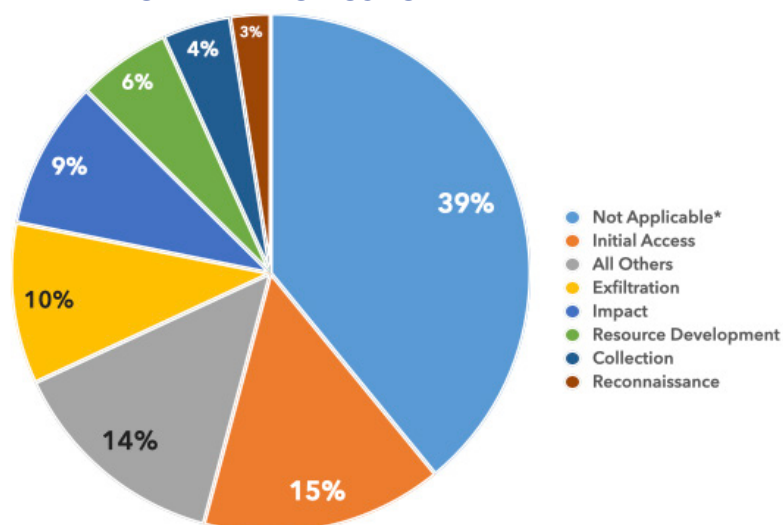
# DoD CYBER CRIME CENTER

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

## DIB–REPORTED CYBER THREATS CY2024 • Q4 (OCT–DEC)

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 Q4.

### ALL REPORTED TACTICS: CY24 Q4



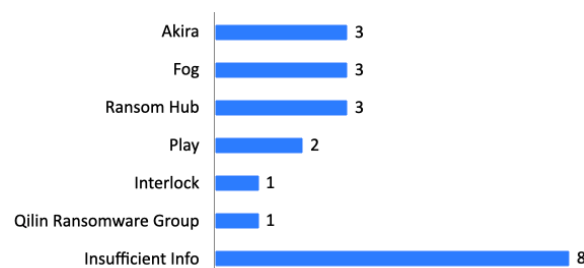
\*Not Applicable refers to tactics that do not fall within MITRE ATT&CK framework (e.g., lost/stolen devices)

### REPORTED RANSOMWARE CY24 Q4

Ransomware-related mandatory DIB reporting decreased by 13% from CY24 Q3 to Q4

14% of all CY24 Q4 mandatory reporting submitted to DC3 DCISE involved ransomware

### REPORTED RANSOMWARE VARIANTS CY24 Q4



### REPORTED RANSOMWARE VARIANTS

**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>.

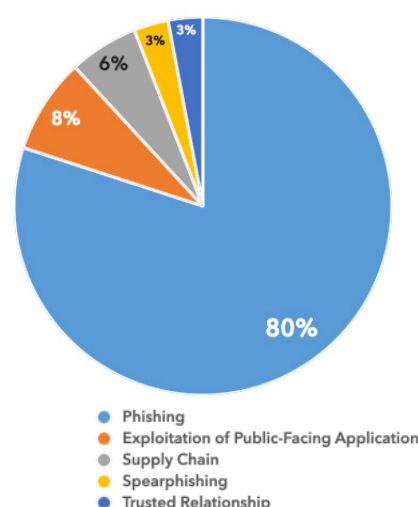
### COMMON INITIAL ACCESS VECTORS

- Phishing and Sub-Techniques
- Exploit Public-Facing Applications
- Valid Accounts
- Drive-by Compromise
- External Remote Services
- Spearphishing

### PHISHING AND SUB-TECHNIQUES:

Phishing is a tactic that has multiple sub-techniques, including "Spearphishing Link" and "Spearphishing Attachment". Where a sub-technique is not defined, the incident is categorized as "Phishing," when the sub-technique is identified it falls under the associated technique.

### INITIAL ACCESS



Pub Date: 19 February 2025

# TOP CYBER EVENTS CY2024 • Q4 (OCTOBER-DECEMBER)

## BeyondTrust Exploit Chinese Activity

**Narrative:** On 30 Dec 24, the Department of the Treasury sent a memo to Congress detailing a cybersecurity incident that they attributed to a Chinese state-sponsored Advanced Persistent Threat (APT) actor. The threat actors obtained an authentication key from BeyondTrust, a third-party software service provider, and used it to bypass security and remotely access several Treasury workstations. The key is used by BeyondTrust to secure a cloud-based service that provides remote technical support services. As a result, this level of access allowed the attackers to view unclassified documents on the compromised workstations..

**DCISE Reporting:** DCISE Warning 25-072 - Chinese Actors Exploit BeyondTrust

**Suspected APT:** Silk Typhoon

**TTPs:** Exploitation for Credential Access [T1212], External Remote Services [T1133]

**Additional Information:** <https://legacy.www.documentcloud.org/documents/25472740-letter-to-chairman-brown-and-ranking-member-scott/>

## Telecoms Targeted Chinese Activity

**Narrative:** On 5 Oct 24, the Wall Street Journal published a report detailing a cyberattack tied to the Chinese government targeting a number of US broadband providers. The threat actors, referred to as Salt Typhoon (also known as FamousSparrow and GhostEmperor), possibly accessed network infrastructure used to cooperate with lawful US requests for communications data." Salt Typhoon compromised Verizon Communications, AT&T, and Lumen Technologies infrastructure, likely in an effort to gather intelligence. Active since at least 2020, Salt Typhoon likely focuses on targeting communication networks and previously targeted entities in North American and Southeast Asia in August 2024.

**DCISE Reporting:** DCISE Advisory 25-013 - Salt Typhoon Activity

**Suspected APT:** Salt Typhoon

**TTPs:** File Transfer Protocols [T1071.002], Protocol Tunneling [T1572]

**Additional Information:** <https://www.wsj.com/tech/cybersecurity/u-s-wiretap-systems-targeted-in-china-linked-hack-327fc63b>

## Fortinet Vulnerability Active Exploitation

**Narrative:** On 23 Oct 24, Fortinet published a security advisory for an actively exploited critical vulnerability impacting FortiManager and FortiManager Cloud products. The vulnerability, tracked as CVE-2024-47575 (CVSS v3 score 9.8), is due to missing authentication for a critical function in the FortiGate to FortiManager protocol daemon (fgfmd) which may allow a remote unauthenticated attacker to execute arbitrary code or commands. In active exploitation attempts, threat actors use scripts to automate exfiltrating files from FortiManagers which contain IP addresses, credentials, and managed device configurations.

**DCISE Reporting:** DCISE Alert 25-001 - Actively Exploited Fortinet FortiManager Vulnerability

**Suspected ATP:** Unknown

**TTPs:** Exploit Public-Facing Application [T1190]

**Additional Information:** <https://www.fortiguard.com/psirt/FG-IR-24-423>

## Ivanti Vulnerability Active Exploitation

**Narrative:** Beginning in mid-December 2024, threat actors conducted zero-day exploitation of Ivanti Connect Secure, Policy Secure, and Neurons for ZTA gateways. The vulnerabilities are tracked as CVE-2025-0282 and CVE-2025-0283 (CVSS score 9.0 and 7.0, respectively). CVE-2025-0282 is a stack-based buffer overflow that could allow an unauthenticated attacker to achieve remote code execution (RCE). Mandiant detailed the exploitation activity of the aforementioned zero-day vulnerabilities attributed to UNC5337, a China-nexus cluster of espionage activity suspected to be part of the broader UNC5221 actor.

**DCISE Reporting:** DCISE Alert 25-003 - Ivanti Connect Secure Policy for ZTA Gateways

**Suspected APT(s):** China-nexus espionage group UNC5337

**TTPs:** Exploit Public-Facing Application [T1190], Protocol Tunneling [T1572]

**Additional Information:** <https://www.ivanti.com/blog/security-update-ivanti-connect-secure-policy-secure-and-neurons-for-zta-gateways>