A FEDERAL CYBER CENTER

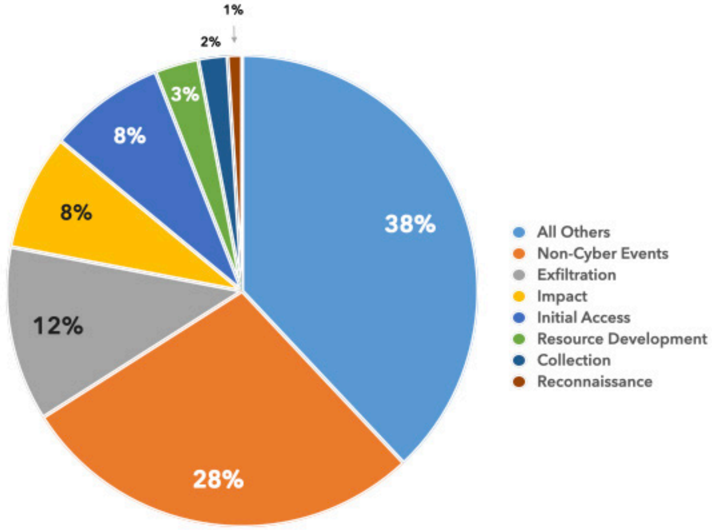
DoD CYBER CRIME CENTER

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

DIB–REPORTED CYBER THREATS CY2025 • Q3 (JUL–SEP)

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 CY25 Q3.

ALL REPORTED TACTICS: CY25 Q3



REPORTED RANSOMWARE CY25 Q3

Ransomware-related DIB reporting increased by **56%** from **CY25 Q2** to **Q3**

5% of all **CY25 Q3** mandatory reporting submitted to DC3 DCISE involved ransomware

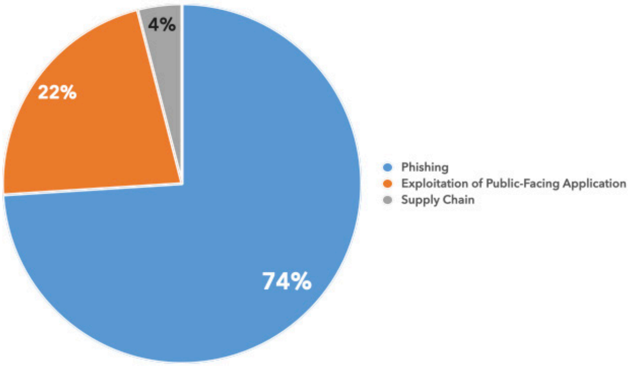
REPORTED VARIANTS CY25 Q3

Akira
BlackCat
Fog
Inc
Lynx
Nitrogen
Play
Qilin
Sinobi
World Leaks

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



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 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.

Pub Date: 17 December 2025

DIB-REPORTED CYBER THREATS CY2025 • Q3 (JULY-SEPTEMBER)

SharePoint Vulnerabilities
Actively Exploited

Narrative: On 19 Jul 25, Microsoft released emergency patches for two critical vulnerabilities, tracked as CVE-2025-53770 (CVSS v3 score 9.8) and CVE-2025-53771 (CVSS v3 score 6.3), affecting Microsoft SharePoint. CVE-2025-53770 is a vulnerability caused by the deserialization of untrusted data that could allow unauthorized attackers to achieve remote code execution (RCE). CVE-2025-53771 is a path traversal flaw that allows authorized attackers to perform spoofing. Threat actors exploited these two zero-day vulnerabilities, dubbed as "ToolShell," to conduct attacks on Microsoft SharePoint servers, impacting at least 54 organizations.

DCISE Reporting: DCISE Alert 25-013 - Actively Exploited SharePoint Vulnerabilities

Suspected APTs: Linen Typhoon, Violet Typhoon, Storm-2603

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

Additional Information: https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/

VMware Vulnerability
Actively Exploited

Narrative: On 29 Sep 25, Broadcom published an urgent bulletin detailing a patch for a security flaw in VMware Tools and VMware Aria Operations. CVE-2025-41244 (CVSS score: 7.8) is a local privilege escalation vulnerability that can be exploited by a local actor, with non-administrative privileges, to escalate privileges to root on a virtual machine (VM) where VMware Tools are managed by Aria Operations with Service Discovery Management Pack (SDMP) enabled. On 29 Sep 25, an NVISO Labs published a blog post detailing evidence of this exploit being used in the wild.

DCISE Reporting: DCISE Alert 25-019 - Actively Exploited VMware Tools

Suspected APTs: UNC5174, UNC3886

TTPs: Privilege Escalation [TA0004]

Additional Information: https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36149

Silk Typhoon TTPs
Chinese Activity

Narrative: On 21 Aug 25, Crowdstrike published details of a China-nexus threat actor, tracked as Silk Typhoon (also known as Murky Panda), conducting operations by leveraging extensive knowledge of cloud environments and custom application logistics. Silk Typhoon frequently targets government, technology, academia, legal, and professional entities in North America, likely focusing on sensitive information to meet intelligence collection requirements (ICRs). The group can access low-prevalence malware and rapidly weaponize n-day and zero-day vulnerabilities, along with leveraging trusted-relationship compromises in the cloud.

DCISE Reporting: DCISE Advisory 25-249 - Silk Typhoon Continues Supply Chain Attacks

Suspected APT: Silk Typhoon

TTPs: Supply Chain Compromise [T1195]

Additional Information: https://www.crowdstrike.com/en-us/blog/murky-panda-trusted-relationship-threat-in-cloud/

Salt Typhoon TTPs
Chinese Activity

Narrative: On 8 Sep 25, Silent Push security researchers published a blog post detailing previously unidentified Salt Typhoon infrastructure. The infrastructure was discovered using protonmail[.]com email addresses, where all addresses consisted of random characters followed by @protonmail[.]com. Salt Typhoon used these email addresses to register multiple malicious domains. All of the email addresses listed fake registrant names and addresses on the records, as the actors created American-based personas to register the domains.

DCISE Reporting: DCISE Advisory 25-254 - Salt Typhoon Infrastructure

Suspected APT: Salt Typhoon, UNC4841

TTP: Command and Control [TA0011]

Additional Information: https://www.silentpush.com/blog/salt-typhoon-2025/