



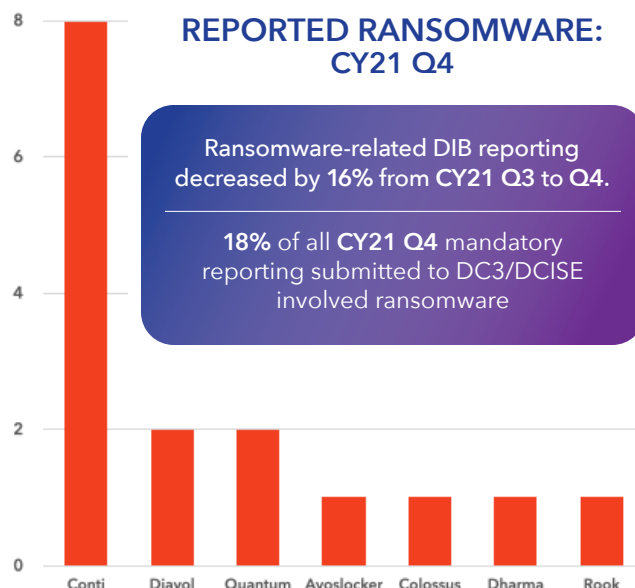
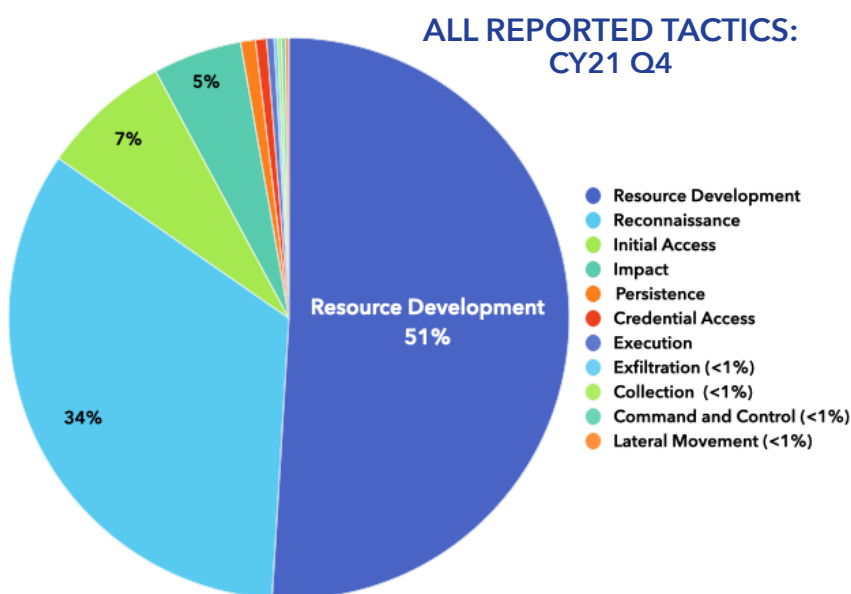
DoD CYBER CRIME CENTER

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

DIB–REPORTED CYBER THREATS

CY2021
Q4 OCTOBER–DECEMBER

DC3/DCISE receives voluntary reporting from Defense Industrial Base (DIB) companies through the DoD’s DIB Cybersecurity 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 CY21 Q4.



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

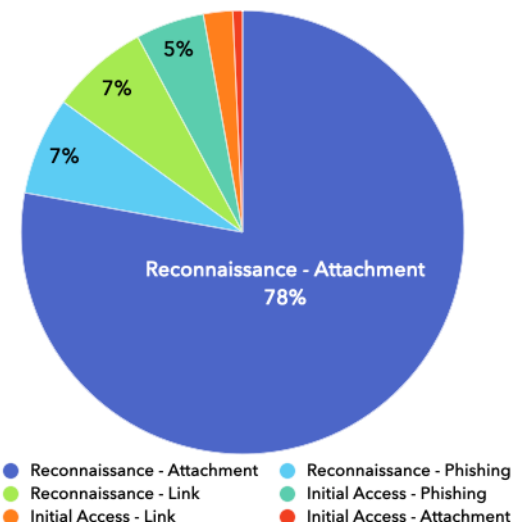
• Employment related	• Fake invoices / financial statements
• Spoofed addresses and CEO fraud	• Missed faxes
• Copyright infringement	• COVID (Omicron related)

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 TRENDS: CY21 Q4



Rev. Date: 26 May 2022

DIB-REPORTED CYBER THREATS CY2021 • Q4 OCTOBER-DECEMBER



APT-29 / Cozy Bear Continued Activity

Narrative: On 6 Dec 21, Mandiant researchers reported Russian-state activity attributed to APT-29 (AKA Cozy Bear or Nobelium) throughout 2021. The report detailed recently observed TTPs, including use of a new malware, Ceeloader. Ceeloader allows backdoor access to networks, installation of additional malware, network tracing, and other malicious behavior.

DCISE Reporting: Warnings: 22-021, 22-023; Advisory 22-001

Impact: APT-29 continues to conduct cyber espionage leveraging stealthy TTPs. Targeting cloud service providers provides a large downstream pool of victims. APT-29 may become increasingly active due to the ongoing geopolitical situation between Russia and Ukraine.

Suspected APT: APT-29

TTP: Use of legitimate credentials, use of proxy services, custom malware, abuse of multifactor authentication via push notifications

Associated Malware: Ceeloader, CRYPTBOT, Foggyweb

Additional Information:

<https://www.mandiant.com/resources/russian-targeting-gov-business>



Log4j Vulnerability Active Exploit

Narrative: On 24 Nov 21, Alibaba's Cloud Security Team reported a vulnerability tracked as CVE-2021-44228 (CVSS score 10.0), also known as Log4Shell. The vulnerability allowed for unauthenticated remote code execution by searching for, or changing, their browser's user agent to a specific string. Cloudflare and Cisco Talos researchers found evidence that CVE-2021-44228 was exploited as early as 1-2 Dec 21. On 14 Dec 21, Microsoft reported they had observed Iranian, Chinese, and North Korean APTs leveraging the vulnerability.

DCISE Reporting: Alert 22-008, Warning 22-024

Impact: Operators used the vulnerability to execute shell scripts downloading cryptominers, Mirai, Muhstik malware, Cobalt Strike beacons, and other malware.

Suspected APTs: Hafnium, Iranian, and North Korean operators

TTP: Exploitation of CVE-2021-44228

Associated Malware: Mirai, Muhstik, Cobalt Strike

Additional Information: <https://therecord.media/log4shell-attacks-expand-to-nation-state-groups-from-china-iran-north-korea-and-turkey/>



Zoho ManageEngine Associated APT Activity

Narrative: On 2 Dec 21, Palo Alto's Unit 42 published a report detailing APT activity occurring from Sep-Nov 21 exploiting vulnerabilities concerning Zoho's ManageEngine ADSelfService product tracked as CVE-2021-40539 and CVE-2021-37415. Two more vulnerabilities regarding ManageEngine were found in Nov-Dec 21: CVE-2021-44077 and CVE-2021-44515.

DCISE Reporting: Alert 22-007, Warning 21-098; Advisories: 22-010, 22-013

Impact: The APT campaign compromised 13 companies, spanning the technology, energy, health, education, finance, and defense industries.

Suspected APT: APT-27

TTP: Exploitation of CVE-2021-40539 and CVE-2021-37415

Associated Malware: Godzilla webshell

Additional Information:

<https://unit42.paloaltonetworks.com/tiltedtemple-manageengine-servicedesk-plus>



Russia-Ukraine Rising Tension

Narrative: On 3 Dec 21, US intelligence reports publicly disclosed Russian forces amassed approximately 50 battlefield tactical groups along Ukraine's eastern and south borders. Russia has steadily built its forces along the Ukrainian border for months with 70,000 personnel at the borders and the possibility of 175,000 military personnel being deployed.

DCISE Reporting: Warning 22-021

Impact: Over the next several months, Russia may increase cyber operations against the DIB in the event of conflict with Ukraine.

Suspected APTs: APT-28, APT-29

TTP: N/A

Associated Malware: TinyTurla, Foggyweb, SkinnyBoy

Additional Information: <https://int.nyt.com/data/documenttools/us-intelligence-russia-military-ukraine/76cba5d3fd32c10e/full.pdf>

ABOUT DC3/DCISE

DC3/DCISE is the operational hub of DoD's Defense Industrial Base (DIB) Cybersecurity Program. DC3/DCISE develops and shares actionable threat products, and performs cyber analysis, diagnostics, and remediation consultations for DIB Participants. Additional services available to Partners include the Electronic Malware Submission platform, several pilot programs (CSaaS), Cyber Resiliency Analysis, and quarterly engagement opportunities.

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