



DoD CYBER CRIME CENTER

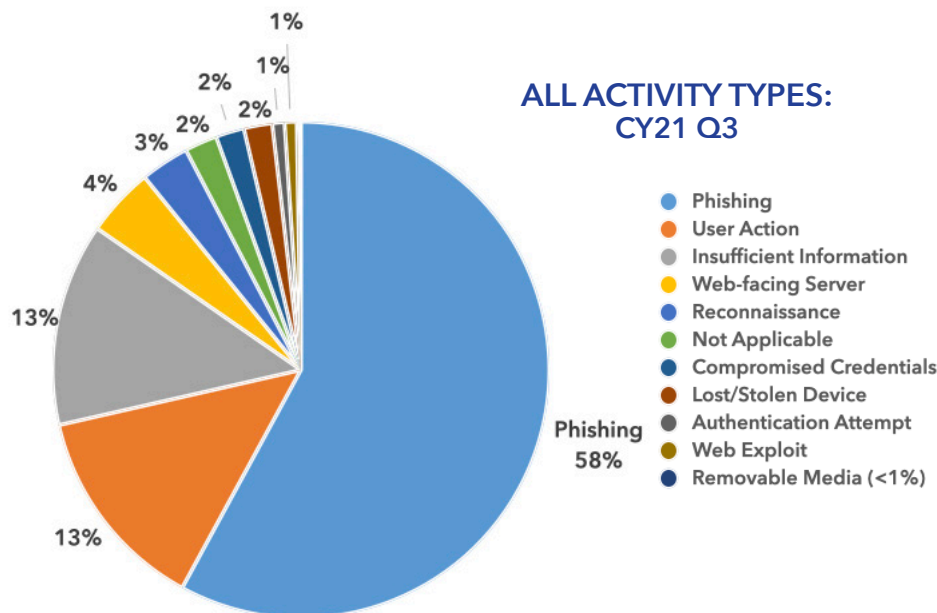
DoD–Defense Industrial Base Collaborative Information Sharing Environment (DCISE)

DIB-REPORTED CYBER THREATS

CY2021
Q3 JULY–SEPTEMBER

DC3/DCISE receives reporting from Defense Industrial Base companies through the DoD's Voluntary DIB CS Program and 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 Q3.

ALL ACTIVITY TYPES: CY21 Q3



RANSOMWARE

Ransomware-related DIB reporting increased by 14% from CY21 Q2 to Q3.

Reported Variants CY21 Q3

- Babuk
- Billgates
- Blackmatter
- Cl0p
- Conti
- Lockbit
- Makop
- PYSA
- Revil
- Sodinokibi

34% of all mandatory reports submitted to DC3/DCISE between Jul-Sep CY21 involved ransomware; compared to 21% for all of CY20.

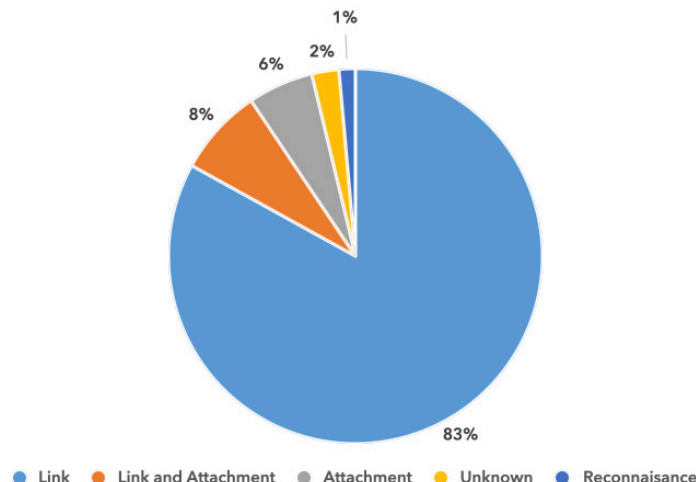
Phishing continues to be the most frequently reported activity type to DC3/DCISE. In-depth analysis of phishing trends are published for DIB CS Program participants in quarterly phishing Threat Activity Reports. To join the DIB CS Program, apply at <https://dibnet.dod.mil>.

TOP PHISHING THEMES

- COVID-19 (Remote work)
- Failed delivery
- Gift cards
- Incoming Fax
- Vacation Policy
- Invoice
- Password Check
- Payroll or Direct Deposit
- Security Updates

Phishing accounted for 66% of all reporting submitted to DC3/DCISE in CY21 Q2; and 52% during CY21 Q3.

DC3/DCISE REPORTING PHISHING TYPES: CY21 Q3



Rev. Date: 26 May 2022

DIB-REPORTED CYBER THREATS CY2021 • Q3 JULY-SEPTEMBER



WINDOWS PRINTNIGHTMARE

Narrative: On 16 Jul 21, security researcher Benjamin Delpy publicly disclosed a new zero-day vulnerability in the Windows Print Spooler service. The vulnerability, dubbed PrintNightmare and tracked as CVE-2021-36958, exploits the Windows Point and Print feature to perform remote code execution and gain local SYSTEM privileges. The new vulnerability is the third CVE associated with PrintNightmare, targeting Windows devices.

DC3/DCISE Reporting: Alert 21-024, Alert 21-027, Warning 21-068, Warning 21-071, Warning 21-072

Impact: An attacker who successfully exploits this vulnerability could install programs, view/change/delete data, or create new accounts with full user rights. Ransomware gangs have utilized the bug to gain elevated privileges on compromised devices.

Suspected Operator: N/A

TTP: Privilege Escalation

Associated Malware: Magniber

Additional Information:

https://twitter.com/hashtag/printnightmare?src=hashtag_click



CONTI RANSOMWARE

Narrative: On 5 Aug 21, security researchers reported a disgruntled affiliate of the Conti Ransomware Gang leaked the group's playbook. The data posted in an online Russian-speaking hacking forum included IP addresses for the group's Cobalt Strike command-and-control (C2) servers and a 113 MB archive that contains numerous tools and training material for how Conti performs ransomware attacks.

The group provides ransomware-as-a-service (RaaS), a service by which the ransomware developers typically receive 20 to 30 percent of the ransom earned by affiliates.

DCISE Reporting: Warning 21-078

Impact: With ransomware attacks on the rise, the leaked information provides threat actors with the tools and technical knowledge needed to conduct attacks. The United States government has implemented the "Rewards for Justice" program to solicit tips on foreign malicious cyberactivity against US critical infrastructure through reward payments.

Suspected Operator: Conti

TTP: Ransomware-as-a-Service

Associated Malware: Cobalt Strike, Mimikatz, Atera Agent, AnyDesk

Additional Information: <https://www.bleepingcomputer.com/news/security/angry-conti-ransomwareaffiliate-leaks-gangs-attack-playbook/>



KASEYA VSA SAAS REvil RANSOMWARE

Narrative: On 2 Jul 21, Kaseya, provider of the Virtual System Administrator (VSA) Software as a Service (SaaS) package, having discovered that Russia-linked REvil ransomware actors were able to conduct attacks targeting the software, urged customers to immediately shut down instances of VSA running on their servers. A subsequent phishing campaign spoofed Microsoft Security update emails to victims, attempting to gain initial access. On 21 July 21, Kaseya obtained and provided a universal decryptor for REvil ransomware victims.

DCISE Reporting: Alert 21-025, Warning 21-062, Warning 21-064, Advisory 21-050, Advisory 21-056

Impact: Roughly 60 Managed Service Providers (MSP) were attacked, affecting approximately 1,500 businesses, which resulted in downstream customers becoming encrypted and asked to pay ransom for their data. This supply chain attack could be used as a new TTP for ransomware groups to propagate their payload to a broader array of victims.

Suspected Operator: Russia-linked group REvil

TTP: Ransomware, supply chain

Associated Malware: Sodinokibi

Additional Information:

<https://www.kaseya.com/potential-attack-on-kaseya-vsa/>



ATLASSIAN CONFLUENCE SCANNING ACTIVITY

Narrative: On 3 Sep 21, threat intelligence firm Bad Packets revealed the detection of mass scanning and exploitation activity targeting the Atlassian Confluence RCE vulnerability CVE-2021-26084 from hosts in multiple countries. The vulnerability is an Object-Graph Navigational Language (OGNL) injection issue that potentially allows unauthenticated users to execute arbitrary code on servers running affected version of the products. Atlassian Confluence is a web-based team collaboration platform for managing workspaces and projects that organizations can run locally on their own servers.

DCISE Reporting: Advisory 21-070, Warning 21-094

Impact: The vulnerability allows an attacker to inject code into expected user input that would be evaluated and executed by the application out of context. Attackers could then include command line (bash) commands that would be executed on the operating system. Confluence is used by Cleared Defense Contractors (CDCs) and the United States Government (USG). At-risk data includes business intelligence, trade secrets, and proprietary information. On-premise instances are at risk; cloud-based Atlassian Confluence customers are not affected by the vulnerability.

Suspected Operator: Unknown Nation-State APT

TTP: Initial Access, Trusted Relationship

Associated Malware: N/A

Additional Information: <https://confluence.atlassian.com/doc/confluence-security-advisory-2021-08-25-10779606215.html>

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.