A FEDERAL CYBER CENTER

DoD CYBER CRIME CENTER

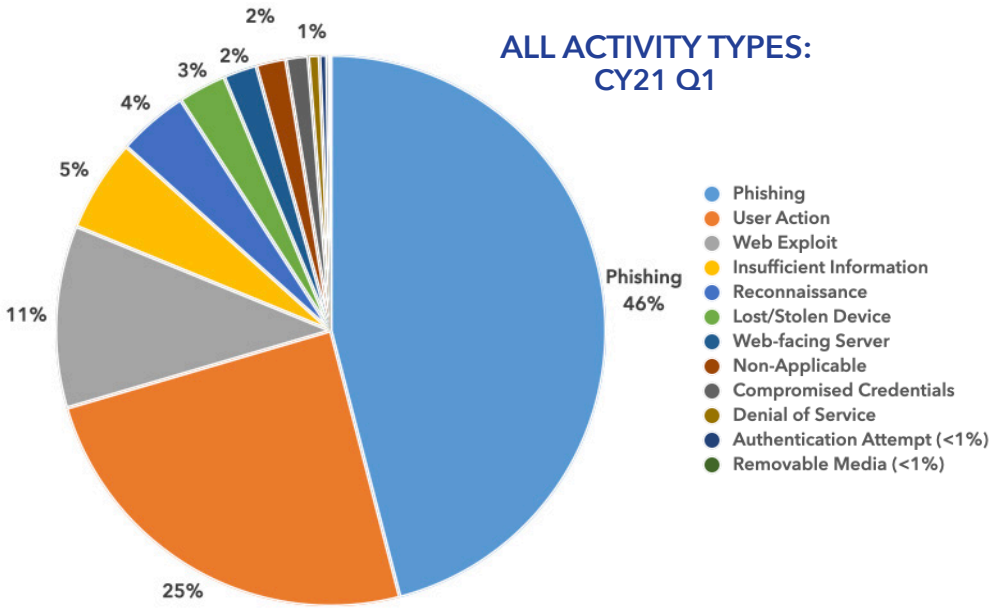
DoD–Defense Industrial Base Collaborative Information Sharing Environment (DCISE)

DIB-REPORTED CYBER THREATS

CY2021 Q1 JANUARY-MARCH

DC3/DCISE receives reporting from Defense Industrial Base companies through the DoD's DIB CS Voluntary 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 Q1.

ALL ACTIVITY TYPES: CY21 Q1



RANSOMWARE

There was a 2% increase in DIB reporting for ransomware related reports for Quarter 1 CY21 reporting versus Quarter 4 CY20 reporting.

Reported Variants CY21 Q1

- Clop
- Sodinokibi
- Lockbit
- Conti
- Darkside
- DoppelPaymer
- Avaddon

30% of all mandatory reports submitted to DC3/DCISE between Jan-Mar CY21 involved ransomware; compared to **21%** for all of CY20.

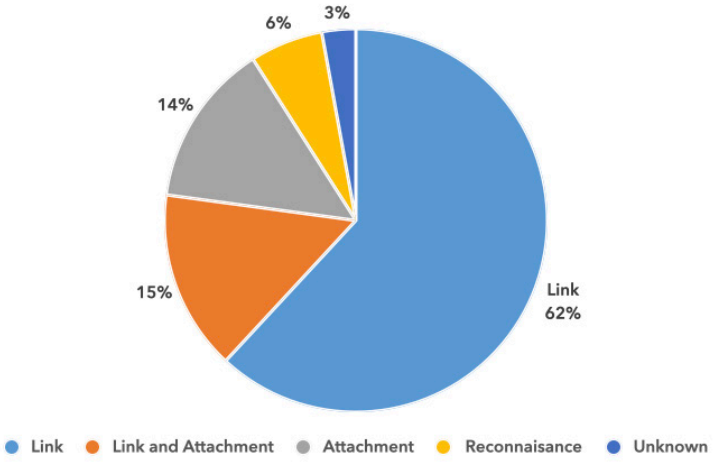
The most frequently reported activity type to DC3/DCISE is phishing. In-depth analysis of the reported phishing trends are published for DIB CS Program participants in quarterly phishing Threat Activity Reports.

TOP PHISHING THEMES

- COVID-19
- Remote Work
- Wire transfer
- Payroll or direct deposit
- Gift cards
- Invoice
- Missed call
- Incoming fax
- Slack
- Zoom

Phishing accounted for **46%** of all reporting submitted to DC3/DCISE in CY21 Q1; versus **51%** during CY20 Q4.

DC3/DCISE REPORTING PHISHING TYPES: CY21 Q1



Pub Date: 16 July 2021

DCISE@dc3.mil
877.838.2174 | 410.981.0104

DoD CYBER CRIME CENTER
410.981.6610 | www.dc3.mil | info@dc3.mil

@DC3Forensics
@DC3DCISE

DIB-REPORTED CYBER THREATS CY2021 • Q1 JANUARY-MARCH

PURPLE FOX
Malware Adopts Wormable Behavior

Narrative: Purple Fox is an active malware campaign targeting Windows machines. Until recently, Purple Fox operators infected machines by using exploit kits and phishing emails. Guardicore Labs identified a new infection vector of this malware where internet-facing Windows machines are breached through SMB password brute force.

DC3/DCISE Reporting: DIBNet Post

Impact: As observed, after infecting vulnerable machines, the malware uses them to host malicious payloads. Presently, Purple Fox malware compromised roughly 2000 servers.

Suspected APT: N/A

TTP: SMB password brute force, phishing, DLL side-loading

Associated Malware: Rootkit

Additional Information:
https://latesthackingnews.com/2021/03/28/purple-fox-malware-adopts-wormable-behavior-to-target-windows-systems

HAFNIUM
MS Exchange Server Compromise

Narrative: On 2 Mar 21, Microsoft released out-of-band security updates for vulnerabilities in its Exchange Server. Microsoft observed targeted attacks against on-premises Exchange Servers, permitting access to email accounts and installation of malware.

DC3/DCISE Reporting: Alert 21-014 / Warning 21-027 / Advisory 21-028 / DIBNet Post: IOC's

Impact: Over 100,000 organizations effected worldwide. Hackers gained access to organizations' emails and potentially highly-sensitive information.

Suspected APT: China (HAFNIUM)

TTP: Server-side request forgery, insecure deserialization, post-authentication arbitrary file write, webshell.

Associated Malware: ShadowPad, Opera Cobalt Strike loader, IIS backdoor, and DLTMiner.

Additional Information:
https://us-cert.cisa.gov/ncas/alerts/aa21-062a

CODECOV
Extortion and Data Theft

Narrative: On 15 Apr 21, Codecov publicly reported their bash uploader contained a backdoor from 31 Jan 21 that potentially sent authentication tokens and other sensitive data to malicious C2. Codecov has a customer base of over 29,000 companies, including Atlassian, Google, and Palo Alto. The compromise went unnoticed for nearly 3 months.

DC3/DCISE Reporting: Warning 21-037 / Advisory 21-035 / Alert 21-017

Impact: The malicious web shell is capable of bypassing user authentication requirements and interacting with a backend SQL server to list and download the files hosted on the FTA

Suspected APT: N/A

TTP: Supply chain attack, compromised credentials

Associated Malware: N/A

Additional Information:
https://us-cert.cisa.gov/ncas/alerts/aa21-055a

SOLARWINDS
Orion Supply-Chain Weaponized Updates

Narrative: In early 2020, hackers secretly broke into Texas-based SolarWind's systems and added malicious code into the company's software system. The system, called "Orion," is widely used by companies to manage IT resources.

DC3/DCISE Reporting: Alerts 21-006, 21-007 / Warning 21-010 / Advisories 21-008, 21-011, 21-015

Impact: Largest and most sophisticated supply chain attack in US History. Thousands of private and government organizations fell victim. Hackers gained access to the data and networks of targeted organizations.

Suspected APT: Russia (NOBELIUM)

TTP: Password guessing, password spraying, misconfiguration, webshell

Associated Malware: SUNBURST, SUNSPOT, SUPERNOVA

Additional Information:
https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure

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 **DCISE@dc3.mil**.

DCISE@dc3.mil
877.838.2174 | 410.981.0104

DoD CYBER CRIME CENTER
410.981.6610 | www.dc3.mil | info@dc3.mil

@DC3Forensics
@DC3DCISE