



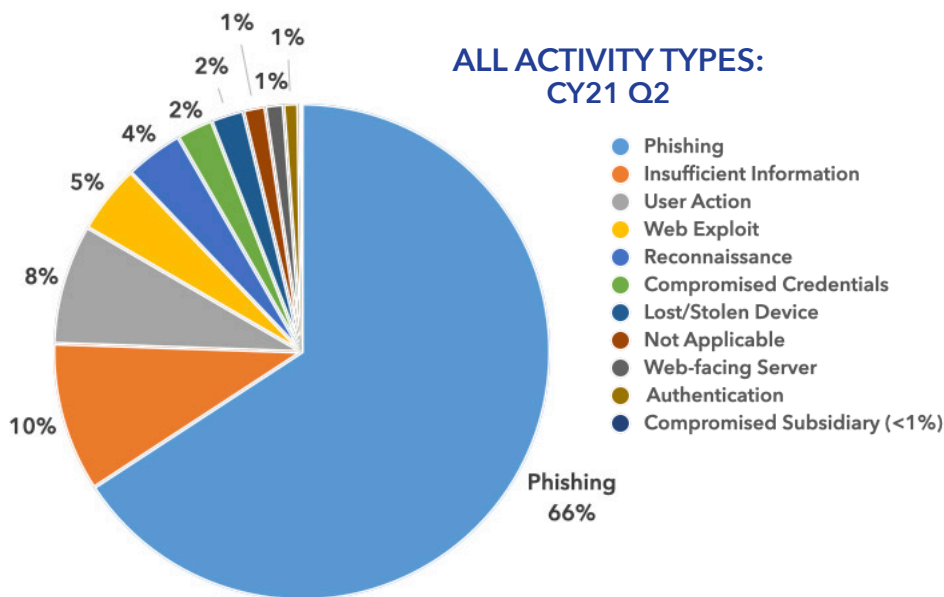
DoD CYBER CRIME CENTER

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

DIB–REPORTED CYBER THREATS CY2021 Q2 APRIL–JUNE

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 Q2.

ALL ACTIVITY TYPES: CY21 Q2



RANSOMWARE

During Quarter 2 CY21, there was a 12% increase in DIB reporting for ransomware related reports compared to Quarter 1 CY21 reporting.

Reported Variants CY21

- Conti
- HelloKitty
- Lockbit
- Ragnar Locker
- Ryuk
- Mesipnoza
- Sodinokibi

35% of all mandatory reports submitted to DC3/DCISE between Apr-Jun CY21 involved ransomware; compared to 21% for all of CY20.

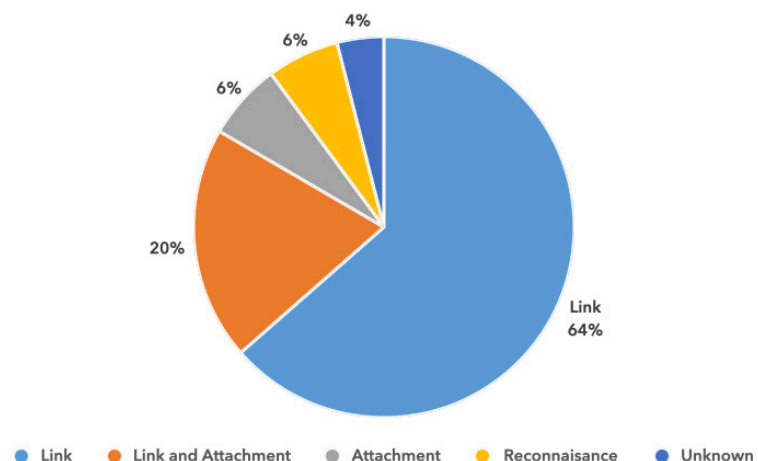
Phishing continues to be the most frequently reported activity type to DC3/DCISE. In-depth analysis of phishing trends are published for DIB CS Program participants in quarterly phishing Threat Activity Reports.

TOP PHISHING THEMES

- | | |
|---|---------------------------------------|
| • COVID-19 (Welcome back to the office) | • Missed call |
| • Wire transfer | • Incoming fax |
| • Payroll or direct deposit | • Security updates |
| • Gift cards | • Business-to-Business correspondence |
| • Invoice | |

Phishing accounted for **66%** of all reporting submitted to DC3/DCISE in CY21 Q2; versus **45%** during CY21 Q1.

DC3/DCISE REPORTING PHISHING TYPES: CY21 Q2



Rev. Date: 26 May 2022

DIB-REPORTED CYBER THREATS CY2021 • Q2 APRIL-JUNE



COLONIAL PIPELINE Darkside Ransomware

Narrative: On May 7, the Colonial Pipeline Company learned it was the victim of a cybersecurity attack. In response they proactively took certain systems offline to contain the threat which temporarily halted all pipeline operations, and affected some of the company's IT systems.

DC3/DCISE Reporting: DIBNet Post

Impact: Colonial Pipeline is the largest fuel pipeline in the United States and transports refined petroleum products between refineries located in the Gulf Coast and markets throughout the southern and eastern United States. The shortage caused by suspending Colonial Pipeline product delivery led to an increase in gas prices.

Suspected APT: N/A

TTP: Ransomware-as-a-Service

Associated Malware: Ransomware

Additional Information:

<https://us-cert.cisa.gov/ncas/current-activity/2021/05/11/joint-cisa-fbi-cybersecurity-advisory-darkside-ransomware>



RUSSIAN USAID PHISHING

Narrative: On 27 May 21, Russian threat actors, APT 29, were observed using four new malware families: a HTML attachment named 'EnvyScout,' a downloader known as 'BoomBox,' a loader known as 'NativeZone,' and a shell code downloader and launcher named 'VaporRage.'

DC3/DCISE Reporting: Advisory 21-040 / Warning 21-046

Impact: Russian actors targeted government agencies, think tanks, consultants, and non-governmental agencies. The US Department of Justice seized two internet domains used in these phishing attacks.

Suspected APT: APT 29 (Russia)

TTP: Phishing

Associated Malware:

EnvyScout, BoomBox, NativeZone, VaporRange

Additional Information:

<https://www.bleepingcomputer.com/news/security/microsoft-russian-hackers-used-4-new-malware-in-usaid-phishing>



EPSILON RED RANSOMWARE

Narrative: On 28 May 21, a cyber security company published a report documenting a ransomware named Epsilon Red. The attackers leveraged an enterprise Microsoft Exchange server as the initial point of entry. The ransomware also used a clone of Copy-VSS, allowing an attacker to save passwords found on the system.

DC3/DCISE Reporting: Advisory 21-039 / Alert 21-014 / Alert 21-020

Impact: Epsilon Red has leveraged Microsoft Exchange vulnerability in an attack against US-based businesses. The ransomware is available publicly on Github.

Suspected APT: N/A

TTP: Ransomware

Associated Malware: Epsilon Red

Additional Information:

<https://news.sophos.com/en-us/2021/05/28/epsilon-red>



PULSE SECURE VPN

Narrative: On 20 Apr 21, Pulse Secure posted an out-of-cycle advisory related to remote code execution (RCE) vulnerability CVE-2021-22893, discovered in April 2021. This CVE is an authentication bypass vulnerability that can allow a remote, unauthenticated user to perform remote arbitrary file execution on the Pulse Connect gateway.

DC3/DCISE Reporting: DC3/DCISE Alert 21-018, DC3/DCISE Alert 21-020, DC3/DCISE Advisory 21-034

Impact: The threat actor is using this access to place webshells on the Pulse Connect Secure appliance for further access and persistence. The known webshells allow for a variety of functions, including authentication bypass, multi-factor authentication bypass, password logging, and persistence through patching.

Suspected APT: UNC2630, UNC2717

TTP: Still in early stages of information gathering (Mandiant)

Associated Malware: SLOWPULSE, RADIALPULSE, PULSECHECK, THINBLOOD, PULSEJUMP, PACEMAKER, SLIGHTPULSE, STEADYPULSE, RADIUS, QUIETPULSE, ATRIUM, and LOCKPICK

Additional Information:

<https://us-cert.cisa.gov/ncas/alerts/aa21-110a>

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.