A FEDERAL CYBER CENTER

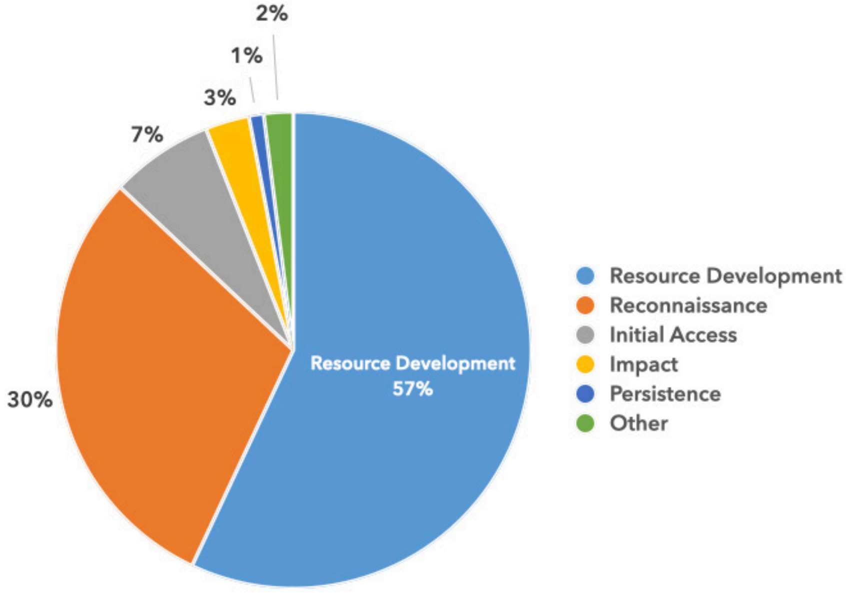
DOD CYBER CRIME CENTER

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

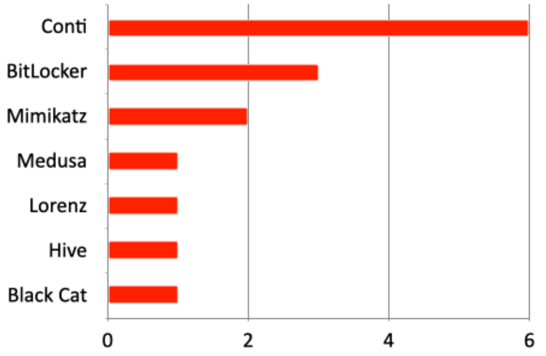
DIB-REPORTED CYBER THREATS CY2022 Q1 (JAN-MAR)

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 CY22 Q1.

ALL REPORTED TACTICS: CY22 Q1



REPORTED RANSOMWARE: CY22 Q1



Ransomware-related DIB reporting decreased by **2%** from **CY21 Q4** to **CY22 Q1**

19% of all **CY22 Q1** mandatory reporting submitted to DC3/DCISE involved ransomware

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**.

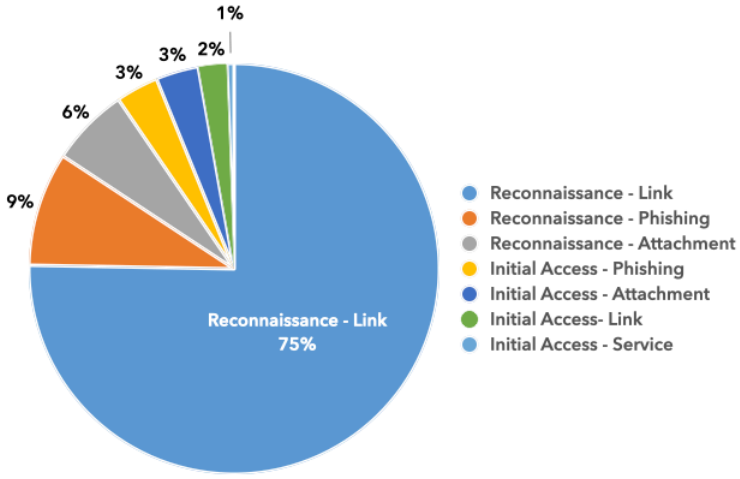
COMMON PHISHING THEMES

- New COVID variant details
- Reset Password Required
- Failed delivery attempt
- Immediate Action required
- Update Payment details
- Tax Refund Due

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: CY22 Q1



DCISE Tactics align with the MITRE ATT&CK Framework, located at https://attack.mitre.org/

Pub Date: 21 April 2022

DIB-REPORTED CYBER THREATS CY2022 • Q1 (JAN–MAR)

Russia-Ukraine
Ongoing War

Narrative: On 24 Feb 22, Russia launched a full-scale invasion of Ukraine. From the beginning of 2022 leading up to and during the invasion, there have been a wide range of cyber-attacks accompanying kinetic effects on the ground. These include DDOS attacks targeting Ukraine websites and banks; phishing and malware operations; a cyberattack against ViaSat SATCOM network; and seven different strains of wiper malware targeting Ukraine to include: WhisperKill, WhisperGate, HermeticWiper, IsaacWiper, CaddyWiper, DoubleZero, and AcidRain.

DCISE Reporting: Alert 22-014; Warning 22-045, 22-049, 22-052, 22-058, 22-060, 22-069; Advisory 22-033, 22-038, 22-055

Impact: Over the next several months, Russia may increase cyber operations against the DIB as a result of the war with Ukraine.

Suspected APTs: Gamaredon/Primitive Bear, APT28/Fancy Bear

TTPs: Spear-phishing, credential harvesting, brute force/password spray, vulnerability exploitation, and wipers.

Associated Malware: WhisperKill, WhisperGate, HermeticWiper, IsaacWiper, CaddyWiper, DoubleZero, and AcidRain

Additional Information:
https://www.cisa.gov/uscert/ncas/alerts/aa22-047a

Daxin Backdoor
Associated APT Activity

Narrative: On 28 Feb 22, Symantec reported a sophisticated type of malware backdoor, called Daxin. Daxin is being used by China-associated APT cyber operators in long-running campaigns against governments and critical infrastructure. Daxin is a Windows kernel driver with advanced communication features allowing it to obfuscate activity that can monitor network traffic, hijack legitimate TCP connections, and use it as C2. Daxin can establish complex communication pathways across multiple compromised computers at once, allowing operators to re-establish, connect, and encrypt communication channels.

DCISE Reporting: Advisory 22-049

Impact: Daxin is optimized for use against hardened targets, allowing operators to burrow deep into a target's network and exfiltrate data without raising suspicions.

Suspected APT: Chinese APT

TTPs: Backdoors, malicious software, network tunneling, C2 of infected nodes, hijack legitimate TCP/IP

Associated Malware: Daxin Backdoor

Additional Information: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/daxin-backdoor-espionage

Lazarus APT
Continued Activity

Narrative: On 28 Jan 22, Malwarebytes reported a Lazarus group spear-phishing campaign using Windows Update Client and GitHub for C2. On 10 Feb 22, the Google TAG discovered two North Korean campaigns, "Operation Dream Job" and "Operation AppleJeus," exploited a Chrome zero-day vulnerability (CVE-2022-0609) weeks before the 14 Feb 22 Chrome patch. The campaigns pushed malware via phishing emails, and used fake job lures and compromised websites, which enabled execution of arbitrary code and escape of the browser's security sandbox.

DCISE Reporting: Warning 22-065; Advisory 22-035, 22-040, 22-067

Impact: The operations targeted more than 335 individuals in 12 different industries and compromised at least two legitimate FinTech company websites.

Suspected APT: Lazarus APT

TTPs: The group impersonated a US defense contractor to send spear phishing emails with malicious documents attached.

Associated Malware: Macros embedded in a Word document and injection malware

Additional Information: https://blog.google/threat-analysis-group/countering-threats-north-korea/

Conti Data Leaks
Ransomware

Narrative: On 27 Feb 22, a Twitter user by the name of ContiLeaks released over 60,000 messages belonging to the Conti ransomware group, in response to the group's leaders' pro-Russian message on their official site. These conversations detail the group's activities, including unreported victims, private data leak URLs, bitcoin addresses, and discussions of operations. On 9 Mar 22, CISA updated an alert detailing TTPs and infrastructure relating to Conti ransomware. On 20 Mar 22, ContiLeaks released the source code for Conti Ransomware v3.0, a compiled locker, and a decryptor.

DCISE Reporting: Warning 22-057; Advisory 22-048, 22-057

Impact: The Conti Group remains active. The leaked source code may be used by other criminal groups.

Suspected APT: N/A

TTPs: Trickbot and Cobalt Strike

Associated Malware: Conti ransomware

Additional Information:
https://www.cisa.gov/uscert/ncas/alerts/aa21-265a

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.

To learn more about cyber risks to the DIB, contact us at **DC3.DCISE@us.af.mil**.