A FEDERAL CYBER CENTER

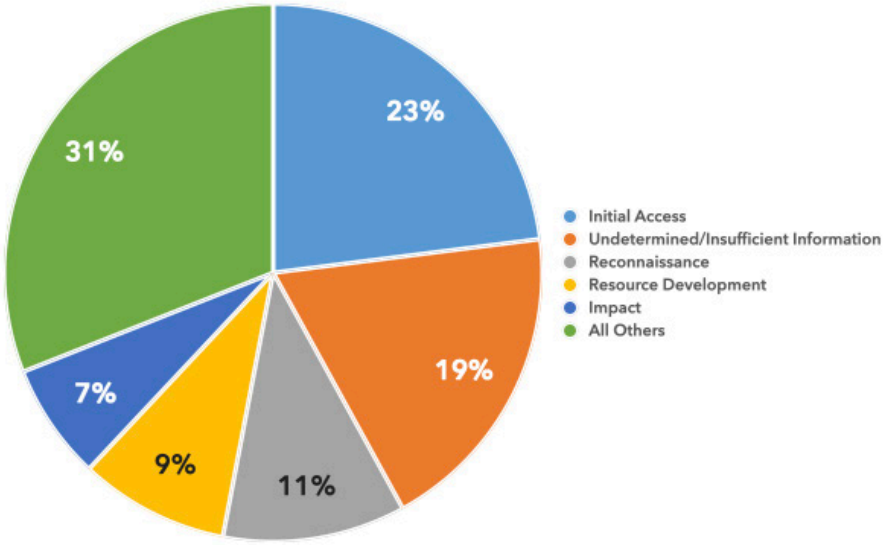
DoD CYBER CRIME CENTER

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

DIB-REPORTED CYBER THREATS CY2023 • Q2 (APRIL–JUNE)

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 CY23 Q2.

ALL REPORTED TACTICS: CY23 Q2

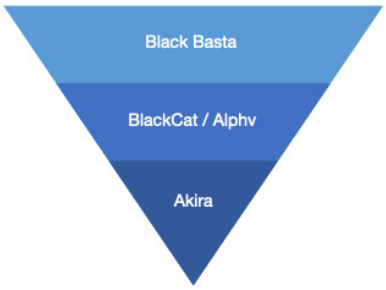


REPORTED RANSOMWARE CY23 Q2

Ransomware-related DIB reporting decreased by **54%** from **CY23 Q1** to **Q2**

Ransomware was involved in **14.2%** of all mandatory reporting submitted to DC3/DCISE during **CY23 Q2**.

MOST REPORTED VARIANTS (MOST-TO-LEAST REPORTED)



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 bi-annual phishing Threat Activity Reports. To join the DIB CS Program, apply at **https://dibnet.dod.mil**.

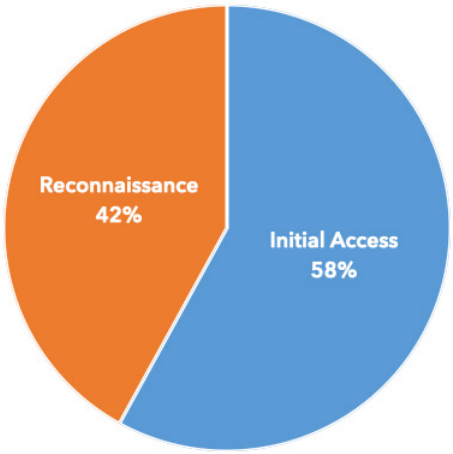
COMMON PHISHING THEMES

- LinkedIn
- Brand Impersonations
- Business Email Compromise
- Pandemic-Related
- Job Offers
- Prizes/Awards
- Password Resets
- Current Events

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 TACTICS (MANDATORY AND VOLUNTARY REPORTS)



Pub Date: 23 August 2023

DC3.DCISE@us.af.mil
877.838.2174 | 410.981.0104

DoD CYBER CRIME CENTER
410.981.6610 | www.dc3.mil | DC3.Information@us.af.mil

@DC3Forensics • @DC3DCISE
DC3 Cyber Crime Center

TOP-REPORTED CYBER EVENTS CY2023 · Q2 (APRIL–JUNE)

MOVEit
Ransomware Event

Narrative: On 31 May 23, Progress Software Corporation published a critical zero-day vulnerability, CVE-2023-34362 (CVSSv3 / 9.8), that allows for privilege escalation and unauthorized access of MOVEit Transfer environments. Mandiant identified the earliest evidence of exploitation likely occurred on 27 May 23. On 6 Jun 23, CL0P ransomware group claimed responsibility for this activity and threatened to post stolen data if victims did not pay an extortion fee. This campaign has overlapping targeting, infrastructure, certificate, and data leak site activity of both UNC4857 and FIN11 threat actors. Targeted organizations include a wide range of industries in Canada, India, and the United States.

DCISE Reporting: DCISE Alert 23-017 – MoveIT Zero Day, DCISE Warning 23-107 – MOVEit Exploited by Cl0p Ransomware Group

TTPs: Data Exfiltration (TA0010-Exfiltration/T1041-Exfiltration Over C2 Channel, TA0001-Initial Access/T1190-Exploit Public-Facing Application)

Additional Information: https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023

Zyxel
Botnet Campaign

Narrative: On 25 May 23, Palo Alto Networks' Unit 42 reported on a Mirai Botnet variant IZ1H9 campaign in which the same unnamed threat group actively exploited various internet of things (IOT) devices to include an unspecified remote code execution (RCE) vulnerability on Zyxel devices. Compromised devices could be fully controlled by attackers and become a part of the botnet. On 20 Jun 23, Zyxel discovered a widely exploited vulnerability, CVE-2023-27992 (CVSSv3 / 9.8), affecting several of their network-attached storage (NAS) firmware devices. IOT devices are regularly targeted due to their low security and have been linked to DDoS toolkits, trojans, ransomware, Mirai botnet, and other botnet malware families.

DCISE Reporting: DCISE Warning 23-114 – Zyxel NAS Vulnerability Exploited, DCISE Warning 23-105 – Mirai Botnet DDoS on Zyxel Devices, DCISE Warning 23-087 – Zyxel RCE Vulnerability, DCISE Warning 23-101 – Multiple New Zyxel Vulnerabilities

Associated Malware: Mirai Botnet

Additional Information: https://www.zyxel.com/global/en/support/security-advisories

VMware
Chinese Exploitation

Narrative: On 13 Jun 23, Mandiant published a report providing details of UNC3886, a Chinese cyber espionage group, exploiting a zero-day authentication bypass vulnerability within VMware Tools (vmtools). The vulnerability, CVE-2023-20867 (CVSSv3 / 3.9), enables threat actors to execute privileged commands across Windows, Linux, and PhotonOS guest virtual machines (VMs). UNC3886 has primarily targeted firewall and virtualization technologies that do not support end point detection and response (EDR) of defense, technology, and telecommunication organizations located in the United States and the Asia-Pacific regions.

DCISE Reporting: DCISE Warning 23-111 – VMware ESXi Zero-Day Exploited by Chinese Hacking Group

Suspected APT: UNC3886

Additional Information: https://www.vmware.com/security/advisories.html

Volt Typhoon
Targeting Critical Infrastructure

Narrative: In Jun 23, a joint advisory was released from multiple federal agencies identifying a Chinese state-sponsored cyber actor, Volt Typhoon, targeting critical infrastructure organizations in Guam and the United States. On 24 May 23, the Secureworks Counter Threat Unit highlighted several successful compromises as well as techniques used by the threat group from Jun 21 to May 23 to include the following: living-off-the-land (LotL) to evade detection; leveraging a single-factor Citrix environment; exploiting a public-facing ManageEngine ADSelfService Plus server; exploiting a Paessler PRTG Network Monitor server; and using native Windows tools to gain access, move laterally, and perform reconnaissance activities on compromised networks.

DCISE Reporting: DCISE Alert 23-016 – Chinese State-Sponsored Volt Typhoon Activity, DCISE Warning 23-100 – Volt Typhoon Activity Update

Additional Information: https://media.defense.gov/2023/May/24/2003229517/-1/-1/0/CSA_Living_off_the_Land.PDF

DC3.DCISE@us.af.mil
877.838.2174 | 410.981.0104

DoD CYBER CRIME CENTER
410.981.6610 | www.dc3.mil | DC3.Information@us.af.mil

@DC3Forensics • @DC3DCISE
DC3 Cyber Crime Center

TOP-REPORTED CYBER EVENTS CY2023 · Q2 (APRIL–JUNE)

Barracuda
Zero-day Exploited

Narrative: On 19 May 23, Barracuda identified a zero-day vulnerability, CVE-2023-2868 (CVSSv3 / 9.8), within their Email Security Gateway (ESG) appliance. On 20 May 23, Barracuda identified that the vulnerability led to unauthorized access to a subset of email gateway appliances. On 15 Jun 23, Mandiant identified a suspected China-nexus actor, UNC4841, as targeting a set of Barracuda ESG appliances to use as a vector for espionage campaigns. UNC4841 sent emails to victim organizations containing malicious file attachments designed to gain initial access to Barracuda ESG appliances, send emails to other victim appliances, move laterally into the network, and maintain persistence on ESG appliances. Mandiant also identified evidence of data staging and exfiltration in a subset of impacted ESG appliances.

DCISE Reporting: DCISE Warning 23-113 – Barracuda ESG Exploited by China

Additional Information: https://www.mandiant.com/resources/blog/barracuda-esg-exploited-globally

Fortinet
Active Exploitation

Narrative: On 13 Jun 23, FortiGuard Labs, published an advisory detailing CVE-2023-27997 (CVSSv3 / 9.8), a Secure Sockets Layer (SSL) Virtual Private Network (VPN) vulnerability, as being actively exploited in the wild. Fortinet described the activity as likely advanced persistent threat (APT) actors targeting unpatched devices in government, manufacturing, and critical infrastructure networks.

DCISE Reporting: DCISE Warning 23-110 – Fortinet SSL VPN Vulnerability Exploited

Additional Information: https://www.fortinet.com/blog/psirt-blogs/analysis-of-cve-2023-27997-and-clarifications-on-volt-typhoon-campaign

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 the risks associated with systems outside of your perimeter, contact us at **DC3.DCISE@us.af.mil**.

DC3.DCISE@us.af.mil
877.838.2174 | 410.981.0104

DoD CYBER CRIME CENTER
410.981.6610 | www.dc3.mil | DC3.Information@us.af.mil

@DC3Forensics • @DC3DCISE
DC3 Cyber Crime Center