AN OFFERING IN THE BLUE CYBER SERIES:

Unclassified Threat Briefing for DAF Small Businesses

Version 24 Aug 2021

#9 in the Blue Cyber Education Series
Unclassified Threat Brief (SBIR/STTR)

Aaron Southwick
Analyst, DCISE
24 Aug 21
Agenda

- About DCISE…
- BEC
- Ransomware
- MITRE ATT&CK
- Advanced Persistent Threats
- Common Vulnerabilities & Exposures
- Questions?
DoD-Defense Industrial Base
Collaborative Information Sharing Environment (DCISE)

About DCISE...

- Large, Mid, & Small CDCs
- University Affiliated Research Centers
- Supply Chain Vendors
- Joint-development Partners
- Commercial Solution and Service Providers
- Federally Funded Research and Development Centers (FFRDCs)

- 77,700+ hours of no-cost forensics and malware analysis
- Disseminated 12,300+ cyber reports
- 518,000+ actionable, non-attributional indicators
Publicly Available Products

DoD Cyber Crime Center (DC3)

Cyber Threat Roundup

A collection of major open source levels of interest to the Defense Industrial Base

Contents

1. CYBER CRIME CENTER (C3)
2. CYBER CRIME CENTER (C3)
3. CYBER CRIME CENTER (C3)
4. CYBER CRIME CENTER (C3)
5. CYBER CRIME CENTER (C3)

TOP PRIORITY THEMES

- 14% - 14%
- 14% - 14%
- 14% - 14%
- 14% - 14%
- 14% - 14%

DC3 REPORTED CYBER THREATS CY21-Q2

- Cyber Threats
- Exploits
- Malware
- Ransomware
- Other

PUBLICLY AVAILABLE PRODUCTS

- UNCLASSIFIED
- UNCLASSIFIED
- UNCLASSIFIED

@DC3DCISE, @DC3Forensics
@DC3VDP

DoD Cyber Crime Center DC3

@DC3Forensics


Linthicum, MD
4,872 Followers

Follow

DoD Cyber Crime Center (DC3)

Military

Linthicum Heights, Maryland - 24,203 followers

Federal Cyber Center

Follow

About us

Established as an entity within the Department of the Air Force in 1996, DC3 provides digital and multimedia forensics, specialized cyber training, technical solutions development, and cyber analysis for the following DoD mission areas: cybersecurity (CS) and critical infrastructure protection (CIP), law enforcement and counterintelligence (LECI), document and media exploitation (DME/DE), and counterterrorism (CT). DC3 delivers capability via its functional organizations which create synergies and enable considerate capability by the size.

DC3 is designated as a federal cyber center by National Security Presidential Directive 64 / Homeland Security Presidential Directive 23, as a DoD center of excellence for DME/DE forensics by DoD Directive 6055.31E, and serves as the operational focal point for the Defense Industrial Base Cybersecurity Program (DIBC) Program. DC3 delivers capability with a team of approximately 400 people comprised of Department of the Air Force civilians, Air Force and Navy military personnel, and contractors for specialized staff support.

In 2015, DC3 was designated as a Cyber Center of Excellence (COC) by the Department of Defense Directive 8570.1M, and serves as the operational focal point for the Defense Industrial Base Cybersecurity Program (DIBC) Program. DC3 delivers capability with a team of approximately 400 people comprised of Department of the Air Force civilians, Air Force and Navy military personnel, and contractors for specialized staff support.
Credential Harvesting

- Microsoft 365 #1
- Reported themes
  - Invoice
  - Missed call
  - Incoming fax
  - Slack
  - Zoom
- Initial access for BEC
- Sandbox detection to evade defenders

Cyber Criminals Exploit Network Access and Privilege Escalation

Summary

Cyber criminals are focusing their operations to target employees of companies worldwide who maintain network access and an ability to escalate network privilege. During COVID-19 shelter-in-place and social distancing orders, many companies had to quickly adapt to changing environments and technology. With these restrictions, network access and privilege escalation may not be fully monitored. As more tools to automate services are implemented on companies’ networks, the ability to keep track of who has access to different points on the network, and what type of access they have, will become more difficult to regulate.
Business Email Compromise

- Post-credential harvesting
  - Auto-forwarding rules

- Not “technical”
  - No link
  - No malware

- May exploit deference to authority

- Reported schemes
  - Wire transfer
  - Payroll or direct deposit
  - Gift cards
Ransomware

- **RaaS**
  - Toolkits, affiliates, share proceeds

- **Double Extortion**
  - Exfil data before encryption to leverage against victim

- **Triple Extortion**
  - Threats to conduct DDoS attack against victim, followed by ransomware payload

- **Quadruple Extortion**
  - Notify victim’s customers, patients, or other affiliates so they pressure victim to pay

“USG strongly discourages payment and encourages all to report any ransomware activity to appropriate agencies and law enforcement.”
Ransomware

- Most common cyber attack methods for gaining initial foothold in corporate networks:
  - Phishing email
  - Brute force attacks against exposed remote desktop protocol (RDP) services
  - Software vulnerabilities

- Most common ransomware over the last year
  - Sodinokibi – also known as REvil
  - Conti
  - Avaddon
  - Mespinoza
  - HelloKitty
Ransomware

- RDP regains top spot
- Small to medium-sized organizations preferred
  - 73% - ≤1000 employees
  - 33% - Phishing
- 2020 Q4 payments
  - Average - $220K
  - Median - $78K
- Reported variants
  - Sodinokibi
  - Conti V2
  - Lockbit
  - Clop

Source: Coveware
## ATT&CK Matrix for Enterprise

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>10 techniques</td>
<td>7 techniques</td>
<td>9 techniques</td>
<td>12 techniques</td>
<td>19 techniques</td>
<td>13 techniques</td>
<td>39 techniques</td>
<td>15 techniques</td>
<td>27 techniques</td>
<td>17 techniques</td>
<td>16 techniques</td>
<td>9 techniques</td>
<td>13 techniques</td>
<td></td>
</tr>
</tbody>
</table>

- **Initial Access**
  - Active Scanning (3)
  - Phishing (3)
  - Drive-by Compromise
  - Compromise Infrastructure
  - Compromise/Exploit Public-Facing Application
  - Exploitation using Known Vulnerabilities
  - Privileged Credentials
  - Exploitation of Privilege Escalation

- **Execution**
  - Scripting Interpreter
  - Command and Scripting Interpreter

- **Persistence**
  - Initial Access
  - Establishing Persistence
  - Exploitation for Client Execution
  - Inter-Process Communication

- **Privilege Escalation**
  - Privilege Escalation

- **Defense Evasion**
  - Anti-Reverse Engineering
  - Exploitation of Privilege Escalation

- **Credential Access**
  - Drive Force
  - Access Token Manipulation

- **Discovery**
  - Initial Access

- **Lateral Movement**
  - Initial Access

- **Collection**
  - Initial Access

- **Command and Control**
  - Initial Access

- **Exfiltration**
  - Initial Access

- **Impact**
  - Initial Access
Phishing

Sub-techniques (3)

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1566.001</td>
<td>Spearphishing Attachment</td>
</tr>
<tr>
<td>T1566.002</td>
<td>Spearphishing Link</td>
</tr>
<tr>
<td>T1566.003</td>
<td>Spearphishing via Service</td>
</tr>
</tbody>
</table>

Phishing: Spearphishing Attachment

Other sub-techniques of Phishing (3)

Adversaries may send spearphishing emails with a malicious attachment in an attempt to gain access to victim systems. Spearphishing attachment is a specific variant of spearphishing. Spearphishing attachment is different from other forms of spearphishing in that it employs the use of malware attached to an email. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email and usually rely upon User Execution to gain execution. Spearphishing may also involve social engineering techniques, such as posing as a trusted source.
Advanced Persistent Threat (APT)

- A sophisticated, sustained cyberattack conducted by experienced, well-funded, nation-state sponsored actors for the purpose of espionage, financial gain, hacktivism, or destruction

- Targeting:
  - Healthcare
  - Telecommunications
  - Manufacturing
  - Maritime
  - Aviation
  - Financial services
  - Universities
  - Research & Development (R&D)
- July 2021, four Chinese nationals indicted for global computer intrusion campaign
- 2011-2018, Hainan State Security Department (HSSD) threat actors sought to obfuscate the Chinese Ministry of State Security (MSS) role in intellectual theft
  - Front company Hainan Xiandun Technology Development Co. Ltd.
  - Trade secrets
  - Confidential business information
  - Sensitive technologies
  - Infectious-disease research
APT40 TTPs

- Spear-phishing email messages
- Fictitious online profiles linked to doppelganger domain names
- Compromised credentials
- Sophisticated malware
- Anonymizing services e.g., The Onion Router (TOR), Darkweb
- Steganography on GitHub
- Threat actor provisioned Dropbox accounts
December 2020, sophisticated cyber actors “trojanized” a legitimate SolarWinds Orion DLL resulting in a supply chain attack

SUNBURST and SUPERNOVA malware

- SUNBURST follows the TTPs discussed, SUPERNOVA allows adversaries another method of access and is believed to have originated from another APT
- SUPERNOVA leverages a different trojanized .NET DLL that is not digitally signed and was built to run in-memory
15 Apr 21, White House publicly attributes Russian Foreign Intelligence Service (SVR) as perpetrator for exploiting the SolarWinds Orion platform

Beginning 2018 shift to targeting cloud resources

- Exploitation of Microsoft Office 365 environments following network access gained through modified SolarWinds software
- Zero-day vulnerabilities to expose user credentials
- “low and slow” password spraying
- Consistent modification of permissions

WellMess malware

- Targeted vaccine research repositories and Active Directory sever of victims
Remote Services CVEs On The Rise

- Malicious cyber actors increasingly targeting unpatched Virtual Private Network (VPN) vulnerabilities
  - Citrix VPN appliances and Pulse Secure VPN servers are “attractive targets”
- March 2020 brought an abrupt shift to work-from-home
  - Microsoft Office 365 collaborative cloud services
- Cybersecurity weaknesses
  - Disregard for patches
  - Susceptible to rising ransomware attacks
Microsoft Exchange Server CVEs

- **CVE-2021-26855** - server-side request forgery (SSRF) vulnerability [Critical]
- **CVE-2021-26857** - insecure deserialization vulnerability in the Unified Messaging service [Medium]
  - Insecure deserialization: untrusted user-controllable data is deserialized by a program
- **CVE-2021-26858** - post-authentication arbitrary file write vulnerability in Exchange allows attacker to write a file to any path on the server [Medium]

![Diagram of Exchange server communication](image)
HAFNIUM exploits internet-facing Exchange servers using the following TTPs:

- Combination of zero-day exploits and unpatched CVEs
- Open-source frameworks like Covenant for C2
- China Chopper web shells allowing remote services
- PowerCat from GitHub
- Procdump to dump LSASS process memory for credential harvesting
- 7-Zip to compress stolen data for exfiltration
- Exchange PowerShell snap-ins to export mailbox data to file sharing sites
March 2021, Mandiant Managed Defense identified three zero-day vulnerabilities being exploited in the wild

- **CVE-2021-20021** – Unauthorized administrative account creation [Critical]
- **CVE-2021-20022** – Post-authentication arbitrary file upload [High]
- **CVE-2021-20023** – Post-authentication arbitrary file read [Low]

10 Jun 21, Binary Defense article identified SonicWall devices still vulnerable to attack for **CVE-2019-7481**, Structured Query Language (SQL) injection

  - Big Game Hunting (BGH) ransomware actors identified by CrowdStrike
- 22 Jun 21, SonicWall acknowledged the patch issued for **CVE-2020-5135** was unsuccessful and recommends immediately downloading the newest patch
- 14 Jul 21, SonicWall issued an urgent security notice to warn of imminent ransomware attacks targeting known “already patched” firmware vulnerabilities
  - Security defects in SMA 100 series and SRA products running unpatched and end-of-life 8.x firmware
Kaseya

Zero-day Supply Chain Ransomware Attack
2 Jul 21, Kaseya urged its customers to immediately shut down versions of Virtual System Administrator (VSA) and suspend service

4 Jul 21, Kaseya released detection tool for VSA Software as a Service (SaaS) to assist with REvil indicators of compromise

6 Jul 21, threat actors conduct phishing campaign against Kaseya clients

21 Jul 21, Kaseya obtains universal decryptor for REvil ransomware victims

- CVE-2021-30116 – Credential leak and business logic flaw
- CVE-2021-30119 – Cross Site Scripting vulnerability
- CVE-2021-30120 – 2FA bypass
Summary

- DCISE!
- Credential Harvesting
- BEC
- Ransomware
- Advanced Persistence Threats
- Common Vulnerabilities and Exposures

Don’t forget to check out our publicly available products on DIBNet-U
Questions?

Thank you for Attending!!!

Aaron Southwick
Analyst
DCISE Hotline: (410) 981-0104
DCISE@dc3.mil
Resources and more modules like this are coming every day!

This presentation and other presentations in the DAF CISO Blue Cyber Educational Series and be found on the DAF CISO webpage:  www.safcn.af.mil/ciso/

- Select Quick Link:
  Small Business Cybersecurity Information

Please provide questions, feedback or if you just want to talk about your cyber security/data protection questions to Kelley.Kiernan@us.af.mil

- Daily Office Hours for answering/researching your questions about DAF Small Business cybersecurity and data protection!