



AN OFFERING IN THE BLUE CYBER SERIES:

Unclassified Threat Briefing for DAF Small Businesses

Version 24 Aug 2021

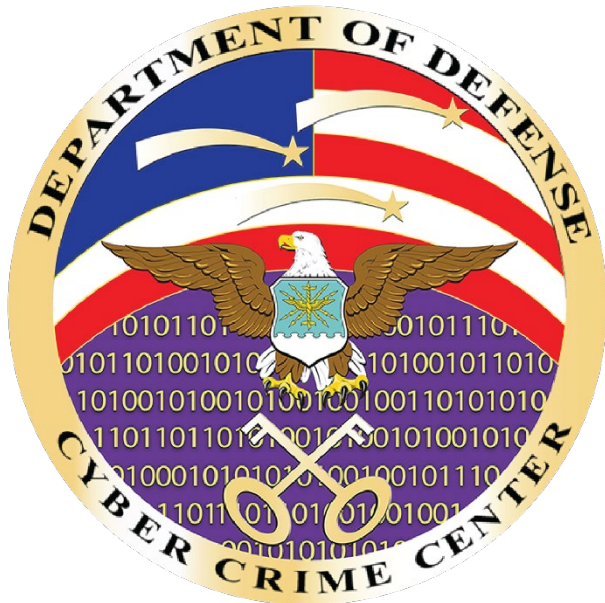
#9 in the Blue Cyber Education Series



DoD CYBER CRIME CENTER (DC3)

DoD—Defense Industrial Base Collaborative Information Sharing Environment

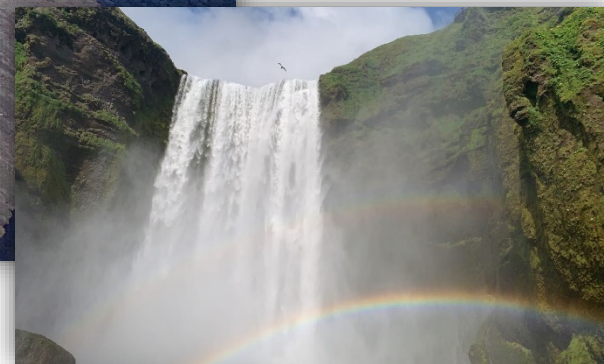
Unclassified Threat Brief (SBIR/STTR)



Aaron Southwick
Analyst, DCISE
24 Aug 21



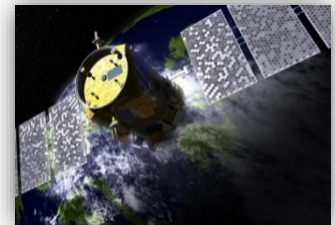
Introduction





Agenda

- About DCISE...
- BEC
- Ransomware
- MITRE ATT&CK
- Advanced Persistent Threats
- Common Vulnerabilities & Exposures
- Questions?





About DCISE...

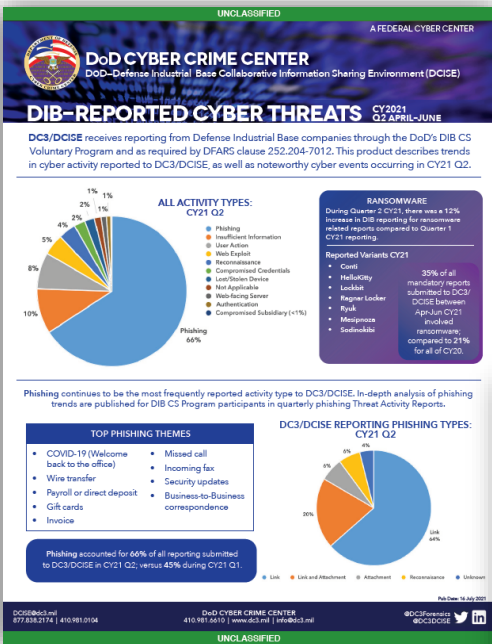




DoD-Defense Industrial Base Collaborative Information Sharing Environment (DCISE)

UNCLASSIFIED

Publicly Available Products



DoD CYBER CRIME CENTER (DC3)
DoD-Defense Industrial Base Collaborative Information Sharing Environment

Cyber Threat Roundup 15 July 2021

A collection of recent open-source items of interest to the Defense Industrial Base

Contents

- DNS-over-HTTPS Takes Another Small Step towards Global Domination.....2
- BOCASS Malware Abuses OBS Studio to Spy on Victims.....2
- China-Linked Hacking Group DEV-6322 behind SolarWinds Serv-U Zero-Day Attacks.....2
- TrickBot Malware Returns with a New VNC Module to Spy on Its Victims.....3
- Researchers Find Big Flaw in a Schneider Electric ICS System Popular in Building Systems, Utilities.....3
- New Law Will Help Chinese Government Stockpile Zero-Days.....4
- China-Linked LuminousMoth APT Targets Entities from Southeast Asia.....4
- SonicWall Warns of Imminent Ransomware Attacks Targeting Firmware Flaw.....5

DoD Cyber Crime Center-DC3 725 Tweets

Explore

Settings

DoD Cyber Crime Center (DC3) A FEDERAL CYBER CENTER

DoD Cyber Crime Center-DC3 @DC3Forensics

Official Twitter Page of the DoD Cyber Crime Center. Digital/multimedia forensics, cyber training, analysis, vulnerability sharing, and technical solutions.

Linthicum, MD dc3.mil Joined December 2018

397 Following 4,898 Followers

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 immediately 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://www.colonialpipeline.com/newsroom/2021/05/13/cyber-security-and-some-of-the-facts-about-ransomware>

EPILON RED RANSOMWARE

Narrative: On 28 May 21, a cyber security company published a report discrediting an enterprise Microsoft Exchange server as the initial point of entry. The ransomware also used a clone of Crypt-VRG, allowing an attacker to save passwords found on the system.

DC3/DCISE Reporting: Advisory 21-039 / Alet 21-014 / Alet 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://www.eset.com/us/newsroom/2021/05/28/epsilon-red-ransomware>

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 Alet 21-016

DC3/DCISE Alet 21-020, DC3/DCISE Advisory 21-034

Impact: The threat actor uses this CVE 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 phishing.

Suspected APT: UNC2450, UNC2177

TTP: SSI in early stages of information gathering (Masfand)

Associated Malware: EUDROPULSE, RADPULSE, PULSEBROKER, THINLOOD, PULSEJUMP, PACEMAKER, LIGHTPULSE, STEADYPULSE, RADPULSE, QUIETPULSE, ATRIM, and LOCKPICK

Additional Information: <https://www.pulse-secure.com/news/alerts/21-110a>

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 (CISAs), Cyber Resiliency Analysis, and quarterly engagement opportunities.

To learn more about the risk associated with systems outside of your perimeter, contact us at DC3@dc3.mil.

DC3/DCISE@dc3 | 877.838.2174 | 410.981.0194

DoD CYBER CRIME CENTER
410.981.0610 | www.dc3.mil | info@dc3.mil

DC3/Forensics | DC3/DCISE

DoD CYBER CRIME CENTER (DC3) A FEDERAL CYBER CENTER

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 1998, DC3 provides digital and multimedia (D/MM) forensics, specialized cyber training, technical solutions development, and cyber analytics for the following DoD mission areas: cybersecurity (CS) and critical infrastructure protection (CIP), law enforcement and counterintelligence (LE/C), document and media exploitation (DOMEX), and counterterrorism (CT). DC3 delivers capability via six functional organizations which create synergies and enable considerable capability for its size.


DC3 is designated as a federal cyber center by National Security Presidential Directive 54 / Homeland Security Presidential Directive 23, as a DoD center of excellence for D/MM forensics by DoD Directive 5505.13E, and serves as the operational focal point for the Defense Industrial Base Cybersecurity Program (DIB CS Program; 32 CFR Part 236). DC3 delivers capability with a team of approximately 430 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



TLP:WHITE
Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

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

**Private Industry Notification**
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

25 November 2020

PIN Number
20201125-001

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force** or **FBI CyWatch**.

Local Field Offices:
www.fbi.gov/contact-us/field

E-mail:
cywatch@fbi.gov

Phone:
1-855-292-3937

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This product was coordinated with DHS-CISA.

This PIN has been released **TLP: WHITE**. Subject to standard copyright rules, **TLP: WHITE** information may be distributed without restriction.

Cyber Criminals Exploit Email Rule Vulnerability to Increase the Likelihood of Successful Business Email Compromise

Summary

The COVID-19 pandemic prompted a mass shift to telework among many US businesses, resulting in increased use of web-based email applications. According to recent FBI reporting, cyber criminals are implementing auto-forwarding rules on victims' web-based email clients to conceal their activities. The web-based client's forwarding rules often do not sync with the desktop client, limiting the rules' visibility to cyber security administrators. Cyber criminals then capitalize on this reduced visibility to increase the likelihood of a successful business email compromise (BEC). BEC schemes resulted in more than \$1.7 billion in worldwide losses⁹ reported to the Internet Crime Complaint Center (IC3) in 2019. The FBI is sharing this information to inform companies of this email rule forwarding vulnerability, which may leave businesses more susceptible to BEC.



Ransomware

■ RaaS

- Toolkits, affiliates, share proceeds

■ Double Extortion

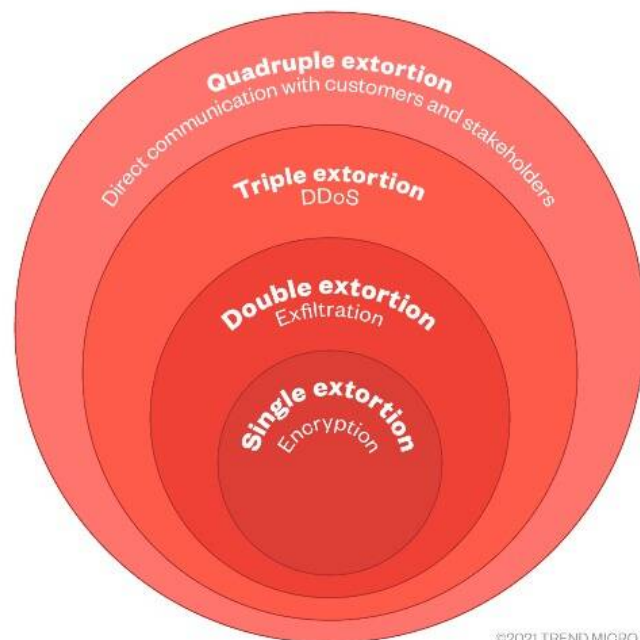
- Exfil data before encryption to leverage against victim

■ 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

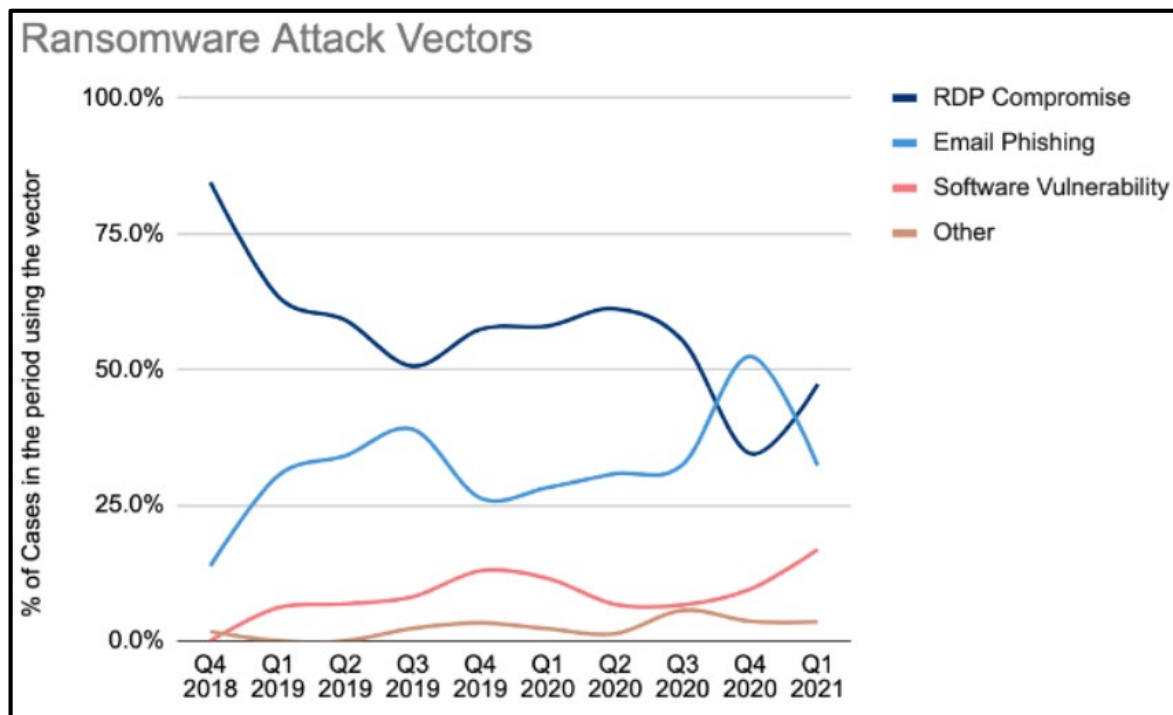
- **Most common cyber attack methods for gaining initial foothold in corporate networks:**
 - Phishing email
 - Brute force attacks against exposed remote desktop protocol (RDP) services
 - Software vulnerabilities
- **Most common ransomware over the last year**
 - Sodinokibi – also known as REvil
 - 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
 - Clon



Source: Coveware



MITRE ATT&CK

ATT&CK Matrix for Enterprise

layout: side ▾

show sub-techniques

hide sub-techniques

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	7 techniques	9 techniques	12 techniques	19 techniques	13 techniques	39 techniques	15 techniques	27 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (5)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Clipboard Data	Data from Cloud Storage Object	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (2)	Browser Extensions	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Dashboard	Remote Services (6)	Data from Configuration Repository (2)	Data Obfuscation (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (2)	Deploy Container	Input Capture (4)	Cloud Service Discovery	Replication Through Removable Media	Data from Information Repositories (2)	Dynamic Resolution (3)	Firmware Corruption	Disk Wipe (2)
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (7)	Create Account (3)	Execution Guardrails (1)	Direct Volume Access	Man-in-the-Middle (2)	Container and Resource Discovery	Software Deployment Tools	Fallback Channels	Encrypted Channel (2)	Inhibit System Recovery	Endpoint Denial of Service (4)
Search Open Technical Databases (5)		Trusted Relationship	Shared Modules	Create or Modify System Process (4)	Escape to Host	Exploitation for Defense Evasion	Modify Authentication Process (4)	Domain Trust Discovery	Taint Shared Content	Data from Local System	Ingess Tool Transfer	Exfiltration Over Physical Medium (1)	Firmware Corruption
Search Open Websites/Domains (2)		Valid Accounts (4)	Software Deployment Tools	Event Triggered Execution (15)	Event Triggered Execution (15)	File and Directory Permissions Modification (2)	Network Sniffing	File and Directory Discovery	Use Alternate Authentication Material (4)	Data from Network Shared Drive	Multi-Stage Channels	Exfiltration Over Web Service (2)	Network Denial of Service (2)
Search Victim-Owned Websites			System Services (2)	Event Triggered Execution (15)	Exploitation for Privilege Escalation	Hide Artifacts (7)	OS Credential Dumping (8)	Network Service Scanning		Data from Removable Media	Non-Application Layer Protocol	Scheduled Transfer	Resource Hijacking
			User Execution (3)	External Remote Services	Hijack Execution Flow (11)	Hijack Execution Flow (11)	Steal Application Access Token	Network Share Discovery		Data from Removable Media	Non-Standard Port	Transfer Data to Cloud Account	Service Stop
			Windows Management Instrumentation	Hijack Execution Flow (11)	Process Injection (11)	Impair Defenses (7)	Steal or Forge Kerberos Tickets (4)	Network Sniffing		Data Staged (2)	Protocol Tunneling		System Shutdown/Reboot
				Implant Internal Image	Scheduled Task/Job (7)	Indicator Removal on Host (6)		Password Policy Discovery		Email Collection (3)	Proxy (4)		
				Modify Authentication Process (4)	Valid Accounts (4)	Indirect Command Execution	Steal Web Session Cookie	Peripheral Device Discovery		Input Capture (4)	Remote Access Software		
				Office Application Startup (6)		Masquerading (6)	Two-Factor Authentication Interception	Permission Groups Discovery (3)		Man in the Browser	Traffic Signaling (1)		
						Modify Authentication Process (4)		Process Discovery		Man-in-the-Middle (2)			
								Query Registry					



MITRE ATT&CK

Phishing

Sub-techniques (3) ^	
ID	Name
T1566.001	Spearphishing Attachment
T1566.002	Spearphishing Link
T1566.003	Spearphishing via Service

Phishing: Spearphishing Attachment

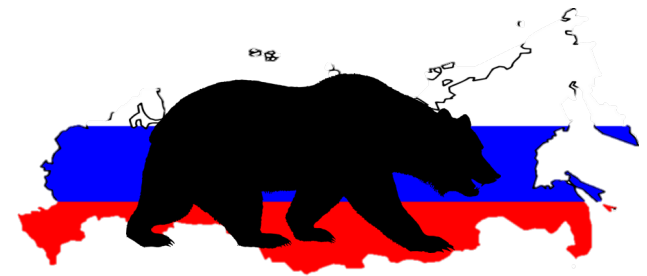
Other sub-techniques of Phishing (3) v

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)





APT40

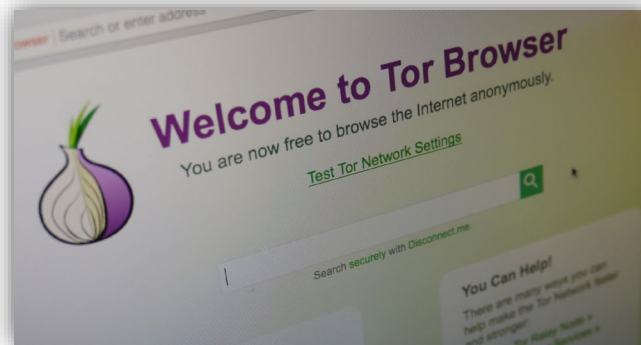
- July 2021, four Chinese nationals indicted for global computer intrusion campaign
- 2011-2018, Hainan State Security Department (HSSD) threat actors sought to obfuscate the Chinese Ministry of State Security (MSS) role in intellectual theft
 - Front company Hainan Xiandun Technology Development Co. 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





SolarWinds

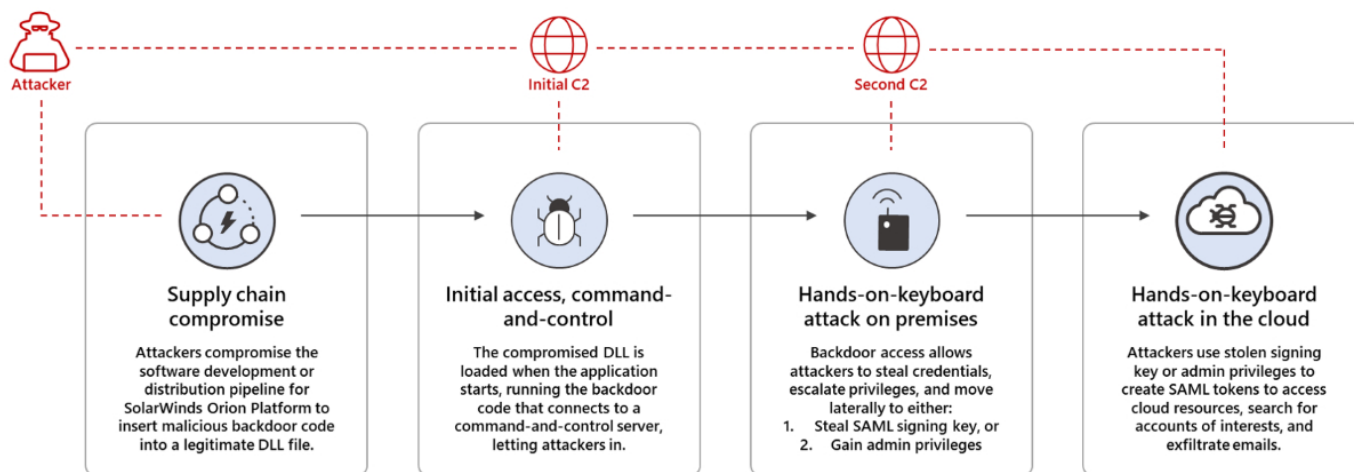


solarwinds



SolarWinds

- **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





APT29

- **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 servers 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



National Cyber
Security Centre
a part of GCHQ





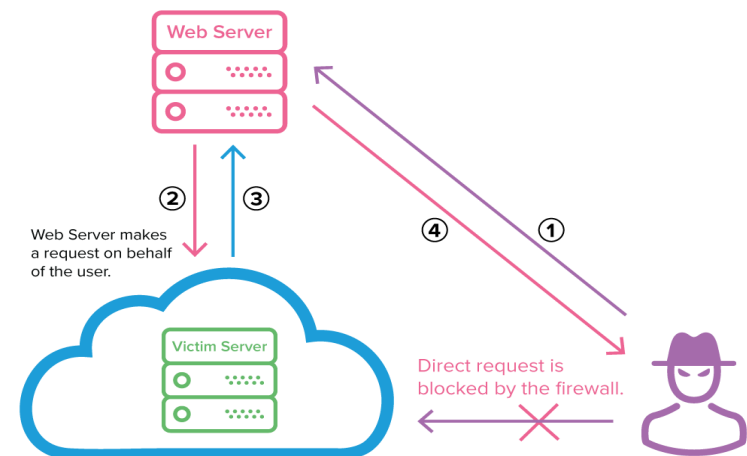
HAFNIUM





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]

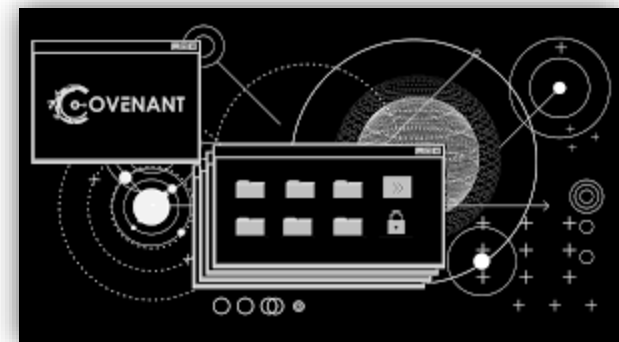
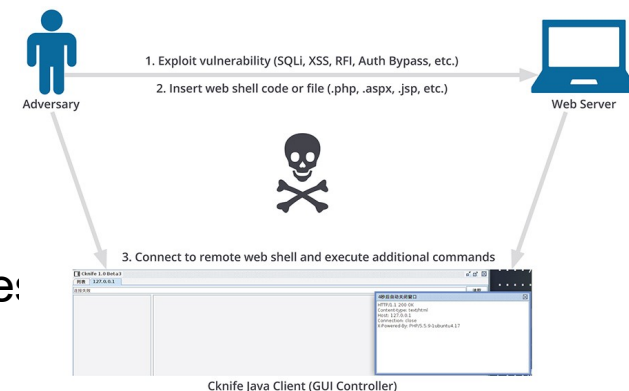




HAFNIUM

■ 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 service:
- 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





SonicWall

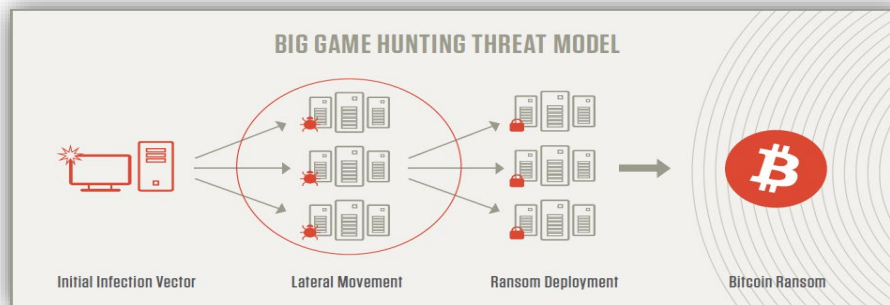
SONICWALL®

ZERO DAY EXPLOIT



SonicWall

- 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





SonicWall

- 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





Kaseya

- 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