



提供されているloc情報をもとにInitialAccessにPhishingの記載があったため何かしらのファイルがアップロードされたのではないかと考え調査を進めました。

```
index=* EventCode=1
| where like(Image, "%Downloads%")
| sort _time
| table _time host Image CommandLine ParentImage Hashes User
```

ここでn.harrisがsecurity\_update.exeとtickets.exeをダウンロードしている痕跡を発見しました。

さらにn.harrisによってsecurity\_update.exeが開かれたことを確認できました。

これが初期アクセスと考えられます

2024-07-24 14:00:13	WK3	C:\Users\n.harris\Downloads\security_update\security_update.exe	"C:\Users\n.harris\Downloads\security_update\security_update.exe"	C:\Windows\explorer.exe
2024-07-24 18:13:13	WK3	C:\Users\n.harris\Downloads\securitytools\tickets.exe	"C:\Users\n.harris\Downloads\securitytools\tickets.exe" asreproast	C:\Windows\System32\WindowsPowerShellv1.0\powershell.exe

次にダウンロードされたtickets.exeについて調査を始めました。

```
index=* tickets.exe
```

powershellからtickets.exeを実行しasreproastを行っている痕跡を見つけました。

ここでユーザーの情報を割り出していると考えられます。

7/24/24	07/24/2024 11:13:13 AM	
6:13:13.000 PM	... 22 lines omitted ...	
Company:	Microsoft Corporation	
OriginalFileName:	PowerShell.EXE	
CommandLine:	powershell -c ".\tickets.exe asreproast"	
CurrentDirectory:	C:\Users\n.harris\Downloads\securitytools\	
Show all 38 lines		
Event Actions ▾		
Type	✓ Field	Value
Selected	✓ host ▾	WK3
	✓ source ▾	WinEventLog:Microsoft-Windows-Sysmon/Operational
	✓ sourcetype ▾	WinEventLog:Microsoft-Windows-Sysmon/Operational
Event	CommandLine ▾	powershell -c ".\tickets.exe asreproast"
	Company ▾	Microsoft Corporation
	ComputerName ▾	WK3.megacorpone.com
	CurrentDirectory ▾	C:\Users\n.harris\Downloads\securitytools\
	Description ▾	Windows PowerShell
	EventCode ▾	1
	EventType ▾	4
	FileVersion ▾	10.0.22621.3085 (WinBuild.160101.0800)
	Hashes ▾	MD5=9D8E30DAF21108092D5980C931876B7E,SHA256=3247BCFD60F6DD25F34CB74B5889AB10EF1B3EC72B4D4B3D95B5B25B534560B8
	Image ▾	C:\Windows\System32\WindowsPowerShellv1.0\powershell.exe
LogonGuid	[b7bd0cd6-abcc-66a0-6b47-c60000000000]	
LogonId	0xC6476B	
Message	Process Create: RuleName: - UtcTime: 2024-07-24 18:13:13.011 ProcessGuid: [b7bd0cd6-4439-66a1-162b-000000001800] ProcessId: 11112 Image: C:\Windows\System32\WindowsPowerShellv1.0\powershell.exe FileVersion: 10.0.22621.3085 (WinBuild.160101.0800) Description: Windows PowerShell Product: Microsoft® Windows® Operating System Company: Microsoft Corporation OriginalFileName: PowerShell.EXE CommandLine: powershell -c ".\tickets.exe asreproast" CurrentDirectory: C:\Users\n.harris\Downloads\securitytools\ User: MEGACORPONE\n.harris LogonGuid: [b7bd0cd6-abcc-66a0-6b47-c60000000000] LogonId: 0xC6476B TerminalSessionId: 1 IntegrityLevel: Medium Hashes: MD5=9D8E30DAF21108092D5980C931876B7E,SHA256=3247BCFD60F6DD25F34CB74B5889AB10EF1B3EC72B4D4B3D95B5B25B534560B8 ParentProcessGuid: [b7bd0cd6-08ed-66a1-9324-000000001800] ParentProcessId: 10376 ParentImage: C:\Users\n.harris\Downloads\security_update\security_update.exe ParentCommandLine: "C:\Users\n.harris\Downloads\security_update\security_update.exe" ParentUser: MEGA CORPONE\n.harris	
OpCode	Info	
OriginalFileName	PowerShell.EXE	
ParentCommandLine	"C:\Users\n.harris\Downloads\security_update\security_update.exe"	
ParentImage	C:\Users\n.harris\Downloads\security_update\security_update.exe	
ParentProcessGuid	[b7bd0cd6-08ed-66a1-9324-000000001800]	
ParentProcessId	10376	
ParentUser	MEGACORPONE\n.harris	

次にasreproastを行っている痕跡をみつけたので資格情報の流出が行われたのではないかと考え調査を進めました。

index=windows\_sysmon EventCode=11

"encrypt" OR  
 "exfil" OR  
 "upload" OR  
 "rclone" OR  
 "custom.exe"

EventCode=11でdb\_exfil.exeが作成されたのを確認した。

取得した資格情報を利用してデータ流出フェーズで使用されたと考えられる。

```

7/26/24 07/26/2024 03:39:34 AM
10:39:34.000 AM ... 18 lines omitted ...
Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
TargetFilename: C:\Users\helpdesk_1\Documents\db_exfil.exe
CreationUtcTime: 2024-07-26 10:39:34.049
User: DB1\helpdesk_1
Show all 23 lines

Event Actions ▾



| Type     | Field           | Value                                                                                                                                                                                                                                                                                                                   |
|----------|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Selected | host            | DB1                                                                                                                                                                                                                                                                                                                     |
|          | source          | WinEventLog:Microsoft-Windows-Sysmon/Operational                                                                                                                                                                                                                                                                        |
|          | sourcetype      | WinEventLog:Microsoft-Windows-Sysmon/Operational                                                                                                                                                                                                                                                                        |
| Event    | ComputerName    | DB1.megacorpone.com                                                                                                                                                                                                                                                                                                     |
|          | CreationUtcTime | 2024-07-26 10:39:34.049                                                                                                                                                                                                                                                                                                 |
|          | EventCode       | 1                                                                                                                                                                                                                                                                                                                       |
|          | EventType       | 4                                                                                                                                                                                                                                                                                                                       |
|          | Image           | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe                                                                                                                                                                                                                                                               |
|          | Keywords        | None                                                                                                                                                                                                                                                                                                                    |
|          | LogName         | Microsoft-Windows-Sysmon/Operational                                                                                                                                                                                                                                                                                    |
|          | Message         | File created: RuleName = UtcTime: 2024-07-26 10:39:34.049 ProcessGuid: {6e3b85c3-7c7d-66a3-3804-000000001200} ProcessId: 4108 Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe TargetFilename: C:\Users\helpdesk_1\Documents\db_exfil.exe CreationUtcTime: 2024-07-26 10:39:34.049 User: DB1\helpdesk_1 |


```

さらにdb\_exfil.exeがEventCode=1で実行されたのを確認した。

```

7/26/24 ... 19 lines omitted ...
10:40:07.000 AM Image: C:\Users\helpdesk_1\Documents\db_exfil.exe
FileVersion: -
... 3 lines omitted ...
OriginalFileName: -
CommandLine: "C:\Users\helpdesk_1\Documents\db_exfil.exe"
CurrentDirectory: C:\Users\helpdesk_1\Documents\
Show all 38 lines

Event Actions ▾



| Type     | Field            | Value                                                                                                        |
|----------|------------------|--------------------------------------------------------------------------------------------------------------|
| Selected | host             | DB1                                                                                                          |
|          | source           | WinEventLog:Microsoft-Windows-Sysmon/Operational                                                             |
|          | sourcetype       | WinEventLog:Microsoft-Windows-Sysmon/Operational                                                             |
| Event    | CommandLine      | "C:\Users\helpdesk_1\Documents\db_exfil.exe"                                                                 |
|          | Company          | -                                                                                                            |
|          | ComputerName     | DB1.megacorpone.com                                                                                          |
|          | CurrentDirectory | C:\Users\helpdesk_1\Documents\                                                                               |
|          | Description      | -                                                                                                            |
|          | EventCode        | 1                                                                                                            |
|          | EventType        | 4                                                                                                            |
|          | FileVersion      | -                                                                                                            |
|          | Hashes           | MD5=64BA37DA46CFB97F329657B3B6C4ACEA,SHA256=44601FD7EDBCE9C68E5979D92D162A886FD005862E0587BA8A926CCD37BDA7FC |
|          | Image            | C:\Users\helpdesk_1\Documents\db_exfil.exe                                                                   |


```

次にdb\_exfil.exeを実行したユーザーhelpdesk\_1は環境のトポロジの情報がないユーザーだったので悪意のある目的で作成されたユーザーと考え調査を進めました。

index=\* EventCode=4720

EventCode=4720でNew Accountとしてhelpdesk\_1が作られているのを確認しました。

7/25/24 07/25/2024 05:49:26 AM  
12:49:26.000 PM LogName=Security  
EventCode=4720  
EventType=0  
ComputerName=DB1.megacorpone.com  
[Show all 49 lines](#)

**Event Actions ▾**

Type	Field	Value
Selected	host	DB1
	source	WinEventLog:Security
	sourcetype	WinEventLog:Security
Event	Account_Domain	MEGACORPONE
	DB1	
	Account_Expires	<never>
	Account_Name	DB1\$ helpdesk_1
	Allowed_To_Delegate_To	-
	ComputerName	DB1.megacorpone.com
	Display_Name	<value not set>
	EventCode	4720

Message ▾ A user account was created. Subject: Security ID: S-1-5-18 Account Name: DB1\$ Account Domain: MEGACORPONE Logon ID: 0x3E7 New Account: Security ID: S-1-5-21-3975360374-1598534471-3726796006-1002 Account Name: helpdesk\_1 Account Domain: DB1 Attributes: SAM Account Name: helpdesk\_1 Display Name: <value not set> User Principal Name: - Home Directory: <value not set> Home Drive: <value not set> Script Path: <value not set> Profile Path: <value not set> User Workstations: <value not set> Password Last Set: <never> Account Expires: <never> Primary Group ID: 513 Allowed To Delegate To: - Old UAC Value: 0x0 New UAC Value: 0x15 User Account Control: Account Disabled 'Password Not Required' - Enabled 'Normal Account' - Enabled User Parameters: <value not set> SID History: - Logon Hours: All Additional Information: Privileges -

さらにhelpdesk\_1について調査を進めたところgarfield-apt2 から、DB1 に対して helpdesk\_1 でログオンが行われたのを確認した。

garfield-apt2は取得した資格情報を使って内部ネットワークへ侵入・横展開するための攻撃者操作用マシン（踏み台）として使用されたと考えられる。

7/26/24 07/26/2024 02:51:17 AM  
9:51:17.000 AM LogName=Security  
EventCode=4624  
EventType=0  
ComputerName=DB1.megacorpone.com  
SourceName=Microsoft Windows security auditing.  
Type=Information  
RecordNumber=33237  
Keywords=Audit Success  
TaskCategory=Logon  
OpCode=Info  
Message=An account was successfully logged on.

Subject:

Security ID:	S-1-0-0
Account Name:	-
Account Domain:	-
Logon ID:	0x0

Logon Information:

Logon Type:	3
Restricted Admin Mode:	-
Virtual Account:	No
Elevated Token:	No

Impersonation Level: Impersonation

```
New Logon:  
    Security ID: S-1-5-21-3975360374-1598534471-3726796006-1002  
    Account Name: helpdesk_1  
    Account Domain: DB1  
    Logon ID: 0x246EF0  
    Linked Logon ID: 0x0  
    Network Account Name: -  
    Network Account Domain: -  
    Logon GUID: {00000000-0000-0000-0000-000000000000}  
  
Process Information:  
    Process ID: 0x0  
    Process Name: -  
  
Network Information:  
    Workstation Name: garfield-apt2  
    Source Network Address: 10.25.26.254  
    Source Port: 0  
  
Detailed Authentication Information:  
    Logon Process: NtLmSsp  
    Authentication Package: NTLM  
    Transited Services: -  
    Package Name (NTLM only): NTLM V2  
    Key Length: 128
```

## 結論

攻撃者は、正規ソフトウェアを装ったsecurity\_update.exeを用いてユーザーn.harrisに実行させることで初期アクセスを獲得した。

その後、攻撃者は tickets.exe を PowerShell から実行し、AS-REP Roasting を行うことで Active Directory 環境内の資格情報を取得したと考えられる。

続いて、攻撃者は Security EventCode 4720 により helpdesk\_1 ユーザーアカウントを新規作成し、これを永続化メカニズムとして利用した。

取得・作成した資格情報を用い、攻撃者は外部マシン「garfield-apt2」を踏み台として NTLM 認証によるネットワークログオン (EventCode 4624) を実施し、DB1 ホストへの横方向移動に成功した。

最終的に、DB1 上で db\_exfil.exe が高権限で実行され (Sysmon EventCode 1) 、外部ホストへの通信が確認されたことから、機密情報の流出が発生した可能性が極めて高いと判断される。