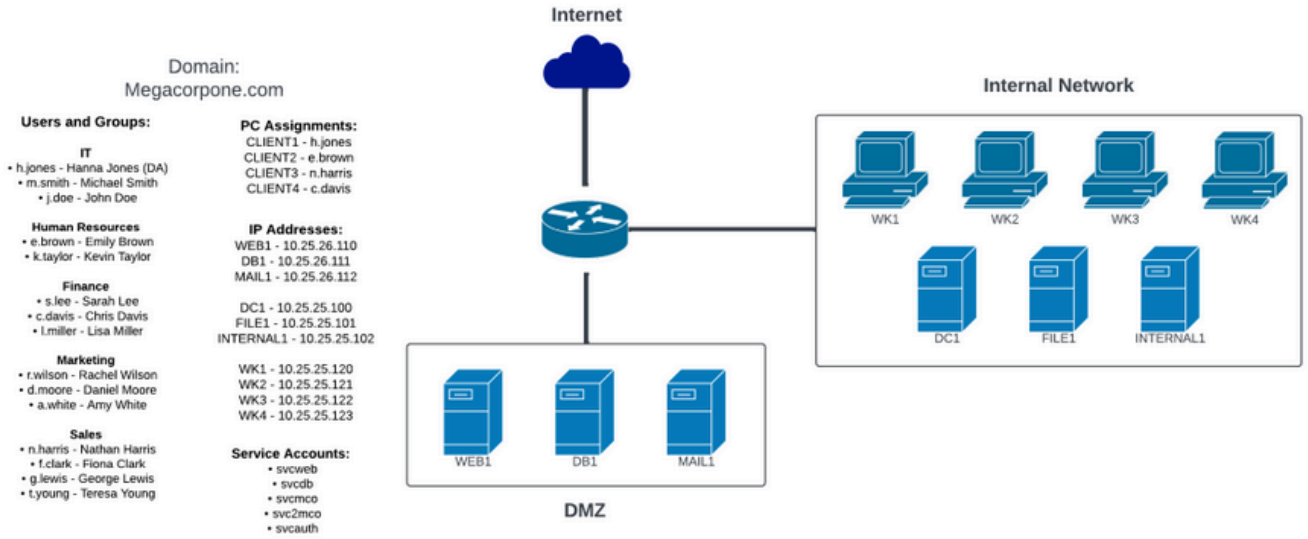


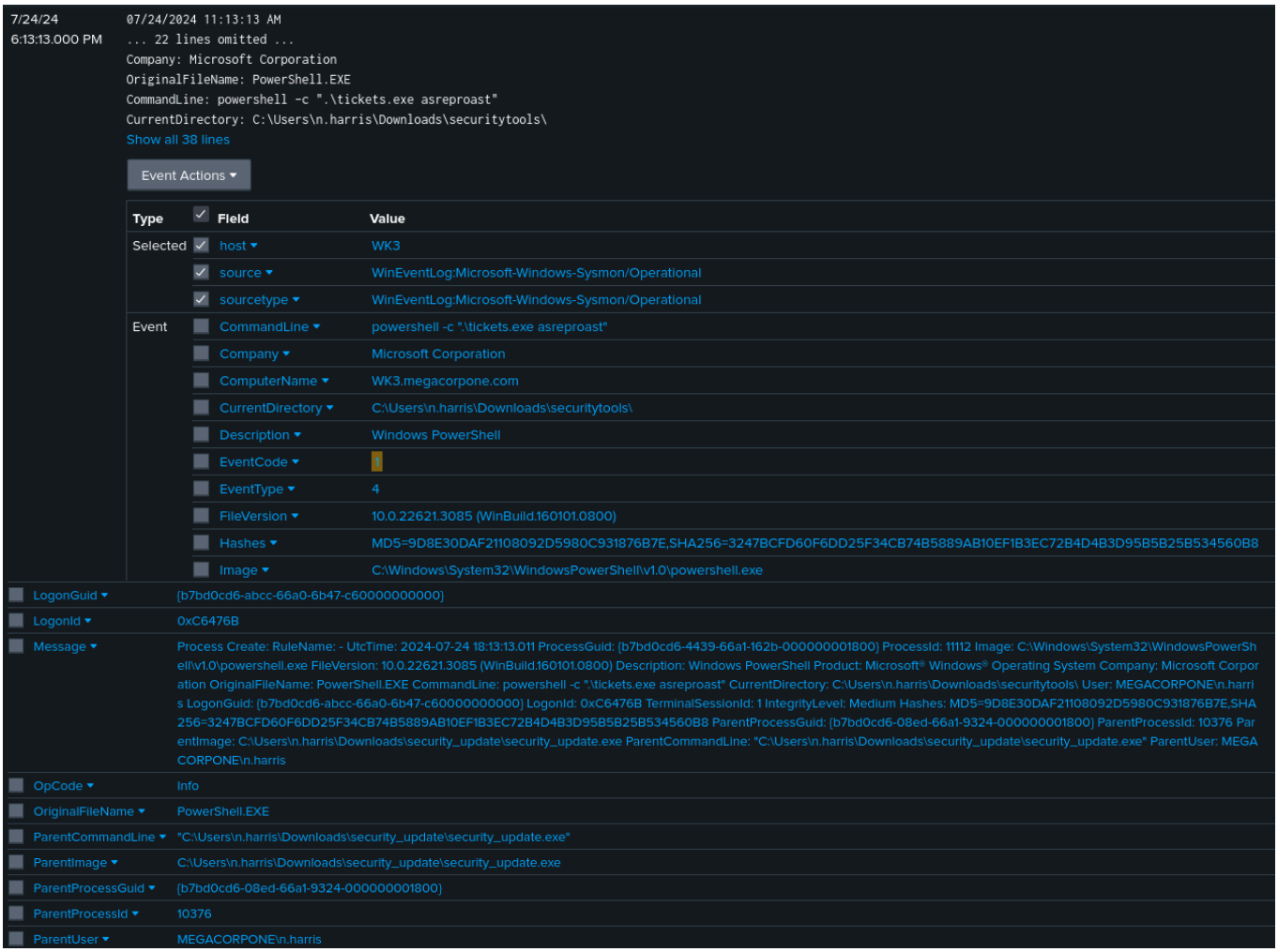
提供されているIoc情報をもとにInitialAccessにPhishingの記載があったため何かしらのファイルがアップロードされたのではないかと考え調査を進めました。

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。
ここ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\WindowsPowerShell\v1.0\powershell.exe

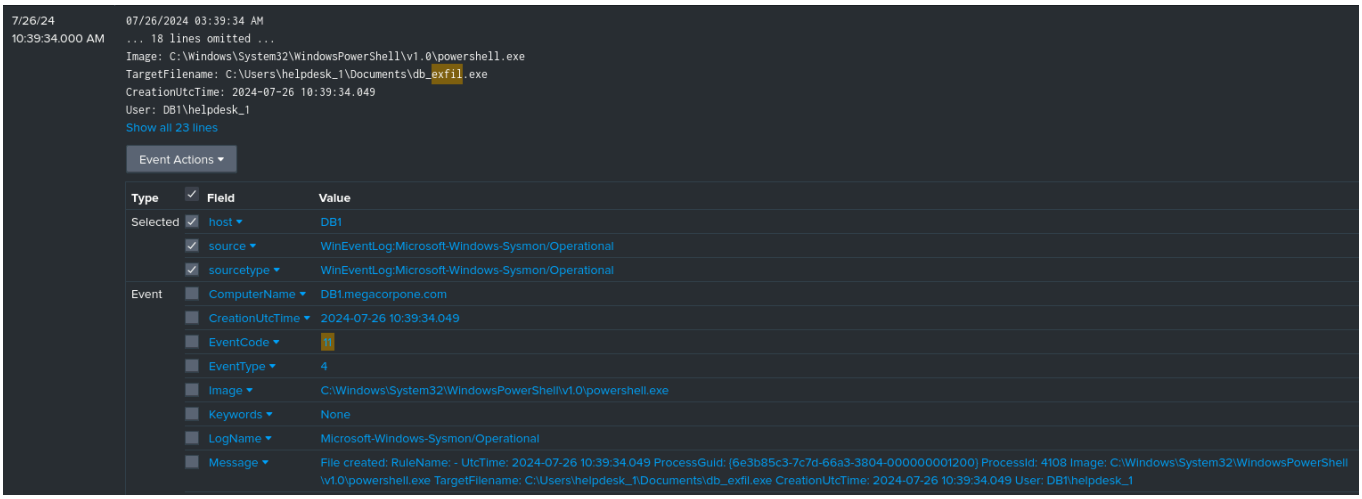
次にダウンロードされたtickets.exeについて調査を始めました。
index=* tickets.exe
powershellからtickets.exeを実行しasreproastを行っている痕跡を見つけました。
ここでユーザーの情報を割り出していると考えられます。



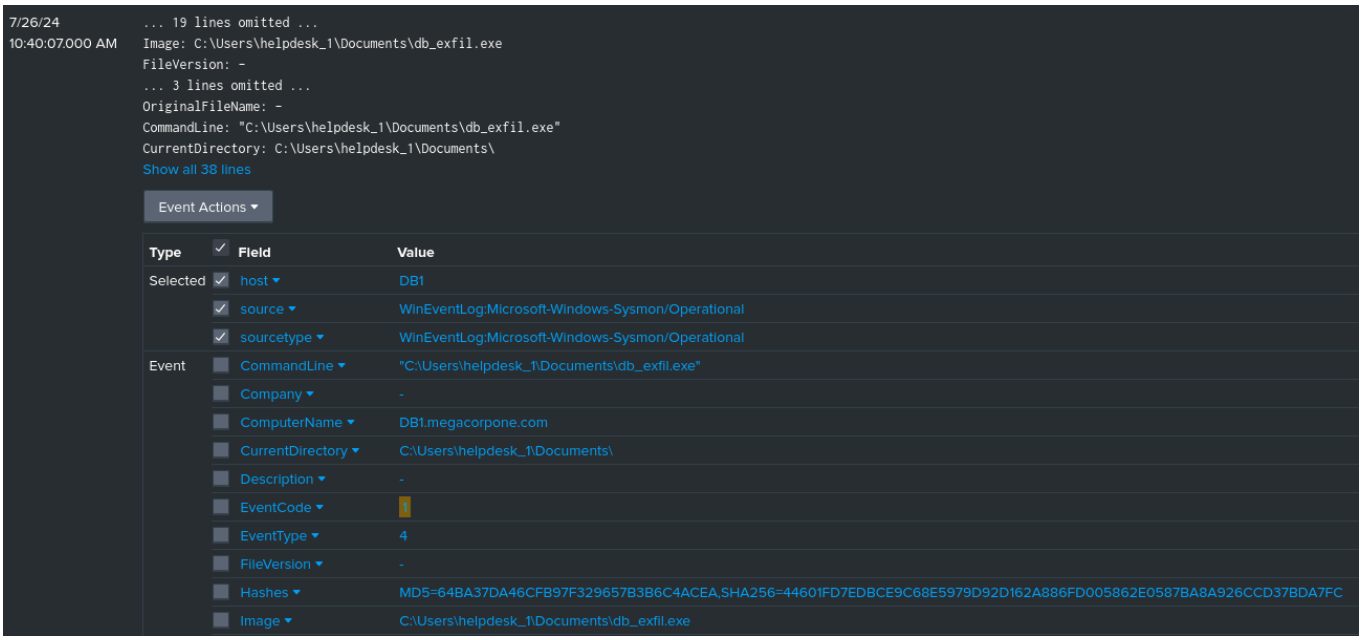
次にasreproastを行っている痕跡をみつけたので資格情報の流出が行われたのではないかと考え調査を進めました。

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。



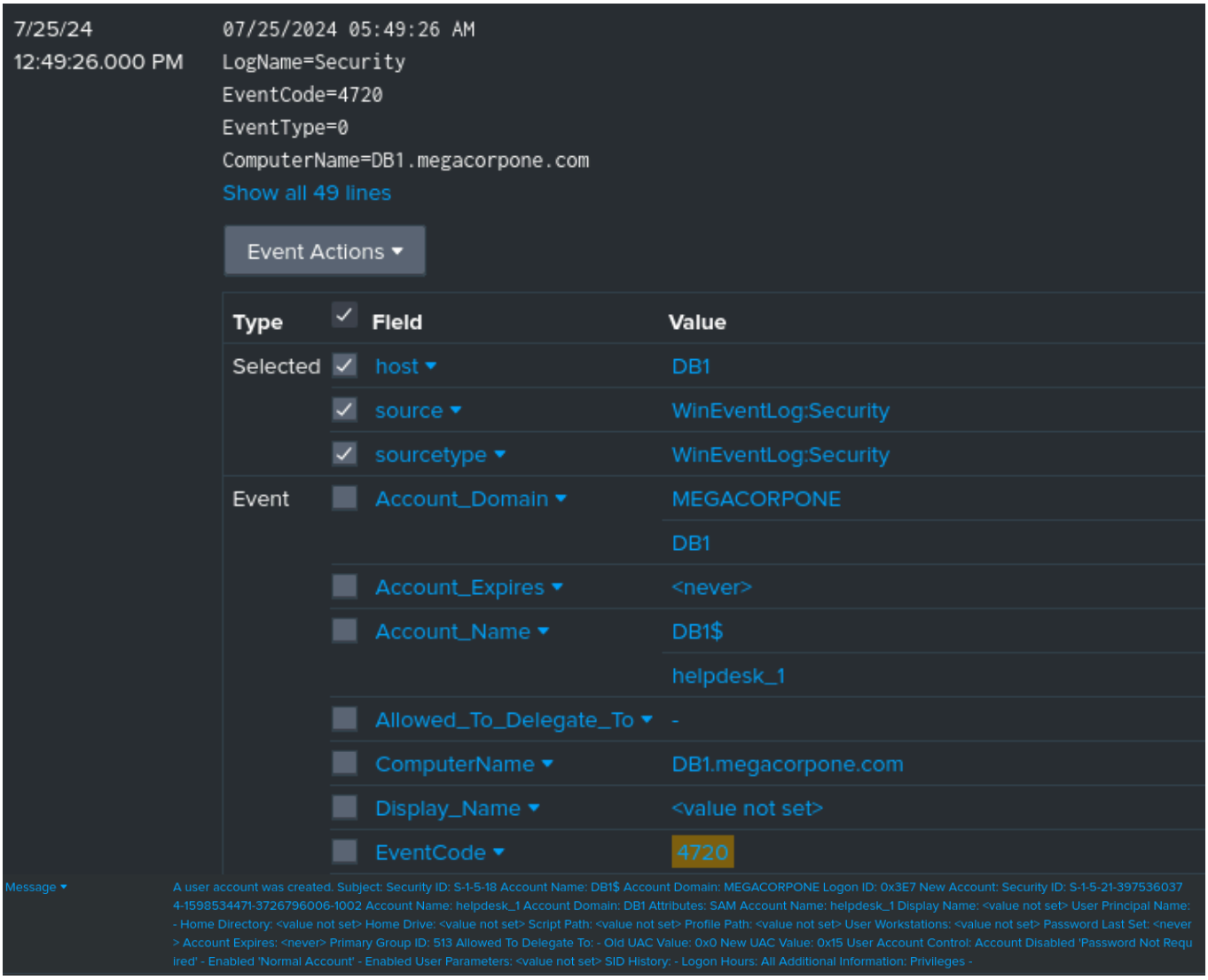
さらにdb_exfil.exeがEventCode=1で実行されたのを確認した。



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に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。



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。