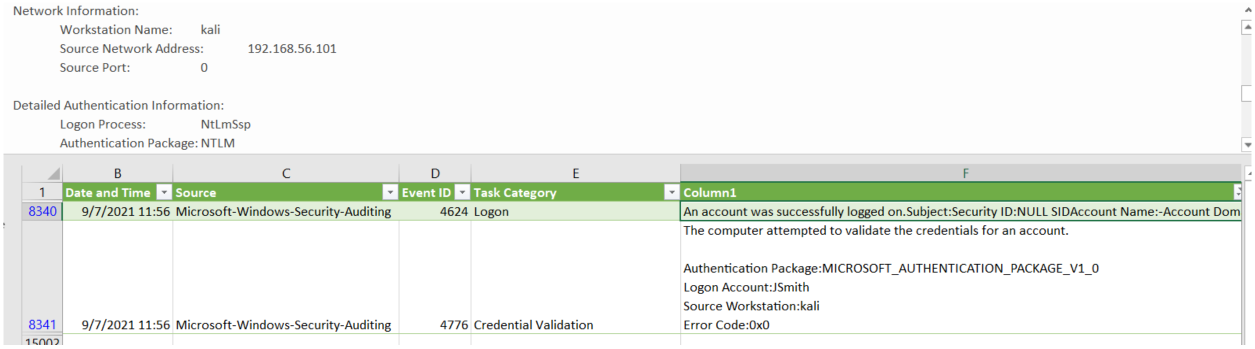
MGS 650 - Information Assurance

AKHILESH ANAND UNDRALLA
UNIVERSITY AT BUFFALO

11/01/2021

Part I - Initial Vector of Compromise

1. What is the name of the computer that engaged in the brute force attack?
A: The Workstation Name that engaged in the brute force attack is **kali**.

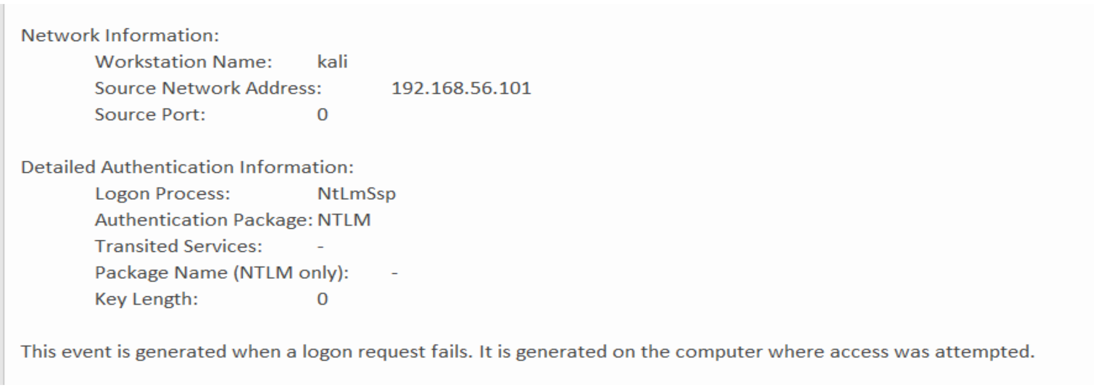


```
Network Information:
	Workstation Name:	kali
	Source Network Address:	192.168.56.101
	Source Port:		0

Detailed Authentication Information:
	Logon Process:		NtLmSsp
	Authentication Package:	NTLM
```

	B	C	D	E	F
1	Date and Time	Source	Event ID	Task Category	Column1
8340	9/7/2021 11:56	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:NULL SIDAccount Name:-Account Dom
8341	9/7/2021 11:56	Microsoft-Windows-Security-Auditing	4776	Credential Validation	The computer attempted to validate the credentials for an account. Authentication Package:MICROSOFT_AUTHENTICATION_PACKAGE_V1_0 Logon Account:JSmith Source Workstation:kali Error Code:0x0
15002					

Figure: ***kali*** engaged in the brute force attack and gained credential validation

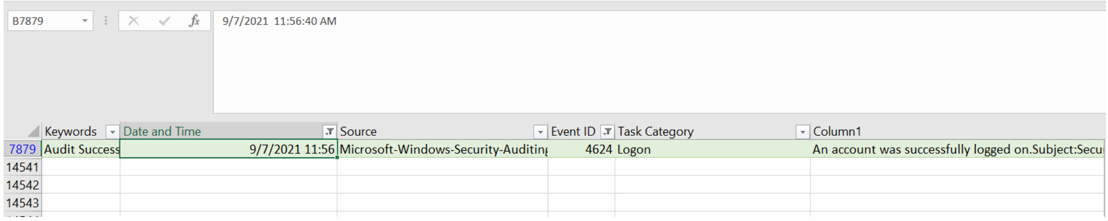
2. What is the IP address of the computer that engaged in the brute force attack?
A: The IP address of the computer that engaged in the brute force attack is **192.168.56.101**



```
Network Information:
	Workstation Name:	kali
	Source Network Address:	192.168.56.101
	Source Port:		0

Detailed Authentication Information:
	Logon Process:		NtLmSsp
	Authentication Package:	NTLM
	Transited Services:	-
	Package Name (NTLM only):	-
	Key Length:		0

This event is generated when a logon request fails. It is generated on the computer where access was attempted.
```

Figure: Event Log showing computer name and IP address

3. What is the approximate time that the attacker first successfully logged onto an account?
A: Time the attacker first successfully logged onto an account is **11:56:40 AM** on **9/7/2021**



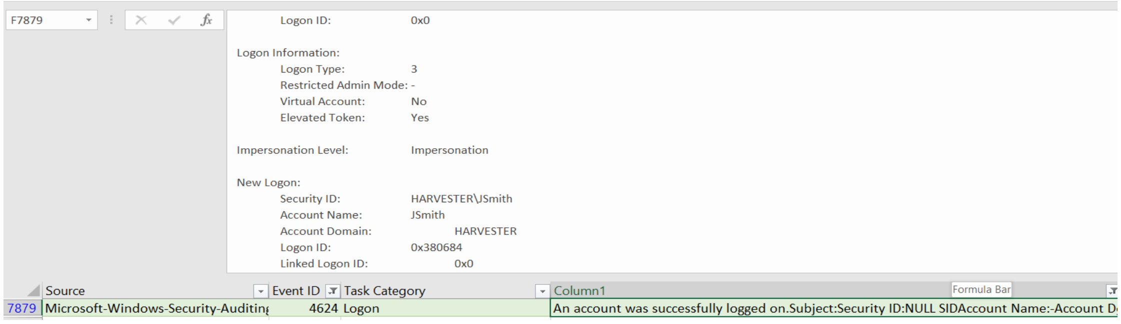
B7879 | 9/7/2021 11:56:40 AM

	Keywords	Date and Time	Source	Event ID	Task Category	Column1
7879	Audit Success	9/7/2021 11:56	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Secu
14541						
14542						
14543						

Figure: Security event log revealing the time of the attack

4. What is the name of the account that the attacker breached?
A: **JSmith** is the name of the account that the attacker breached. Active Directory Domain User Properties for JSmith (extracted from get-aduser Filter *)

```
DistinguishedName    : CN=Jim Smith,CN=Users,DC=harvester,DC=space
Enabled              : True
GivenName            : Jim
Name                 : Jim Smith
ObjectClass          : user
ObjectGUID           : b9f007b9-b5a0-4386-9ea5-7fb21779a78d
SamAccountName       : JSmith
SID                  : S-1-5-21-2585452321-3891222014-57903214-1103
Surname              : Smith
UserPrincipalName    : JSmith@harvester.space
```

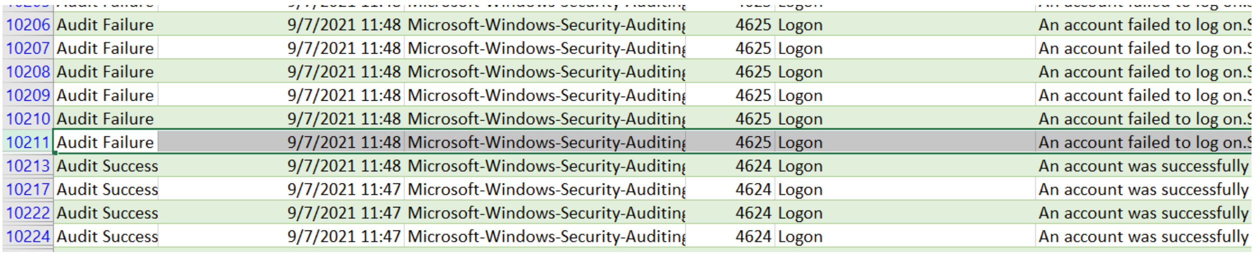


```
        Logon ID:               0x0

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

Impersonation Level:            Impersonation

New Logon:
        Security ID:            HARVESTER\JSmith
        Account Name:           JSmith
        Account Domain:                 HARVESTER
        Logon ID:               0x380684
        Linked Logon ID:                0x0
```

	Source	Event ID	Task Category	Column1
7879	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:NULL SIDAccount Name:-Account D

Figure: Security event log showing the account

5. At what approximate time did the attack start?
A: The attack was started at **11:48:55 AM** on 9/7/2021.



10206	Audit Failure	9/7/2021 11:48	Microsoft-Windows-Security-Auditing	4625	Logon	An account failed to log on.
10207	Audit Failure	9/7/2021 11:48	Microsoft-Windows-Security-Auditing	4625	Logon	An account failed to log on.
10208	Audit Failure	9/7/2021 11:48	Microsoft-Windows-Security-Auditing	4625	Logon	An account failed to log on.
10209	Audit Failure	9/7/2021 11:48	Microsoft-Windows-Security-Auditing	4625	Logon	An account failed to log on.
10210	Audit Failure	9/7/2021 11:48	Microsoft-Windows-Security-Auditing	4625	Logon	An account failed to log on.
10211	Audit Failure	9/7/2021 11:48	Microsoft-Windows-Security-Auditing	4625	Logon	An account failed to log on.
10213	Audit Success	9/7/2021 11:48	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully
10217	Audit Success	9/7/2021 11:47	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully
10222	Audit Success	9/7/2021 11:47	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully
10224	Audit Success	9/7/2021 11:47	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully

Figure: Security event log revealing the start of the attack

Executive Summary

Windows Server operating here as Domain Controller has been breached by an attacker and the device has been investigated using event logs as the primary source of examination. Primarily, Security logs are scrapped through the Event Viewer application and examined to determine how the attacker gained access to the system.

Mainly, two events, one that documents all the successful login attempts by the users and the other one that documents each and every failed attempt to logon to the local computer regardless of logon type, location of the user or type of account. In view of these considerations, 4624(login success) 4625 (login failure) are filtered to further examination. It is established that Remote Desktop logon attempts are responsible for the breach and determined that brute force is used as the method of attack. After filtering out all the system standard logs and limiting the search to reflect unusual and persistent failed login attempts, it is discovered that brute force attack was initiated at 11:48:55 AM on 9/7/2021 and account names *JNash*, *JDubrow, JPark, JSmith* and *Shiller* were used to attempt to break in to the device leveraging the control that restricts multiple login attempts. At 11:56:40 AM on 9/7/2021, the account name Jsmith was compromised to brute force by the attacker with IP address 192.168.56.101 and the account was used as the main source of the attack to install malware into the device. At 11:59:02 AM, 9/7/2021, the brute force attack was halted. Evidence shows brute force attack was conducted by the adversary with *kali* as the workstation.

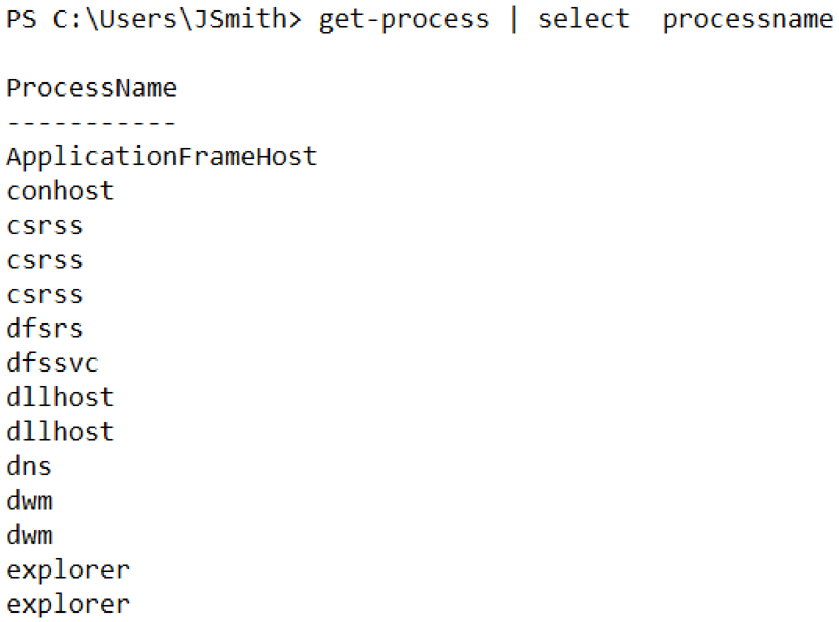
To prevent such attacks, it is advised that basic controls should be applied to IT systems through the review process of IT general control audit. Although there is a limit to the number of login attempts to each user there is no control to temporarily ban the IP with unusual and persistent logon attempts. Another common way to prevent brute force attack is through usage of captchas that prevents bots and automated tools from attempting multiple logins. Two factor Authentication and Web application firewalls are another way of preventing brute force attacks.

Part II – Post Breach Behavior

1. What are 3 different commands the attacker ran?
A: Following commands are used by the attacker after opening Windows PowerShell which was run as administrator.

```
get-process | select  processname

get-wmiobject -class Win32_Product

.\Listdlls.exe

get-process | where-object {$_.processname -eq "perl"}

.\Listdlls.exe -r "perl|6576"
```

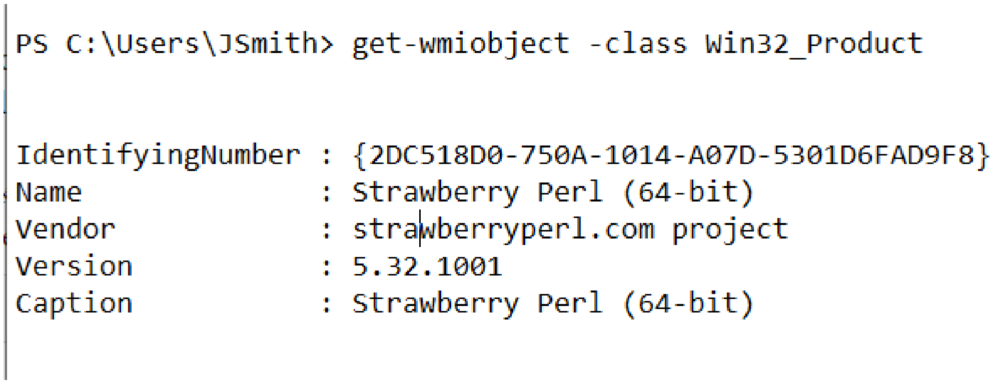
2. What do you think the purpose of one of these commands might be? (If you do not understand a command the PowerShell documentation previously linked may help.)
A: **First Command** - get-process | select processname lists out all the processes running at the moment on the device and selects the last column 'processname' to display.



```
PS C:\Users\JSmith> get-process | select  processname

ProcessName
-----------
ApplicationFrameHost
conhost
csrss
csrss
csrss
dfsrs
dfssvc
dllhost
dllhost
dns
dwm
dwm
explorer
explorer
```

Figure: Various commands run by the attacker

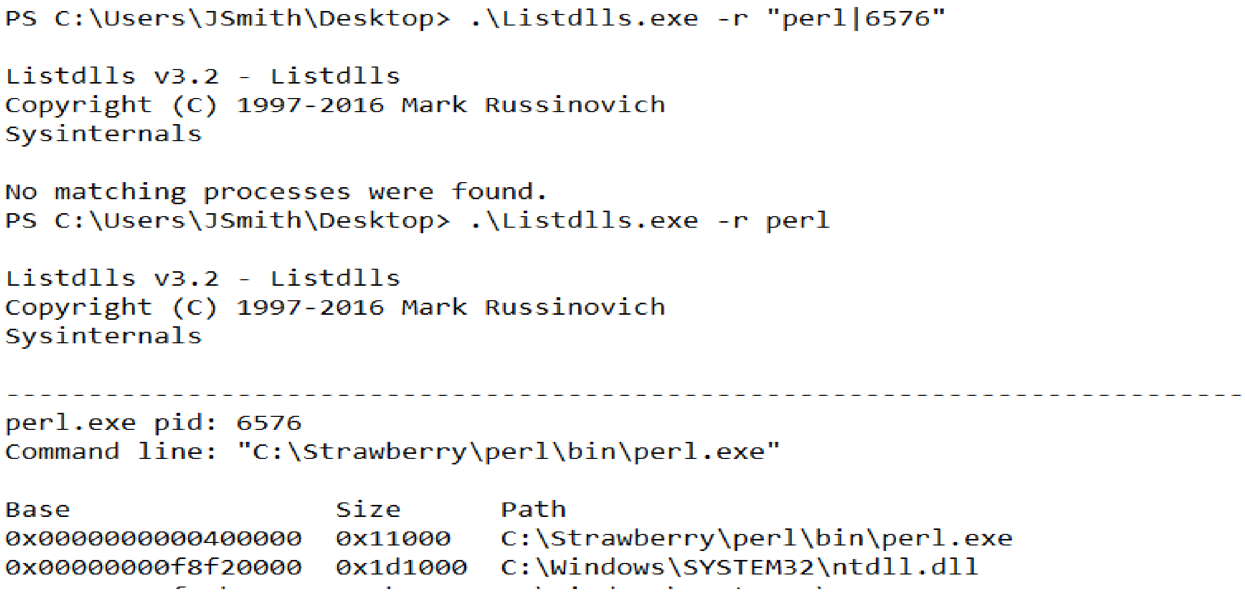
Second Command - get-wmiobject -class Win32_Product gives out the version information of the available WMI(Windows Management Instrumentation) classes, in this case 'perl' file located at C:\Users\JSmith>



```
PS C:\Users\JSmith> get-wmiobject -class Win32_Product


IdentifyingNumber : {2DC518D0-750A-1014-A07D-5301D6FAD9F8}
Name              : Strawberry Perl (64-bit)
Vendor            : strawberryperl.com project
Version           : 5.32.1001
Caption           : Strawberry Perl (64-bit)
```

Figure: Various commands run by the attacker

Third Command - .\Listdlls.exe runs the list of all the DLLs loaded by each process in the CLI interface.

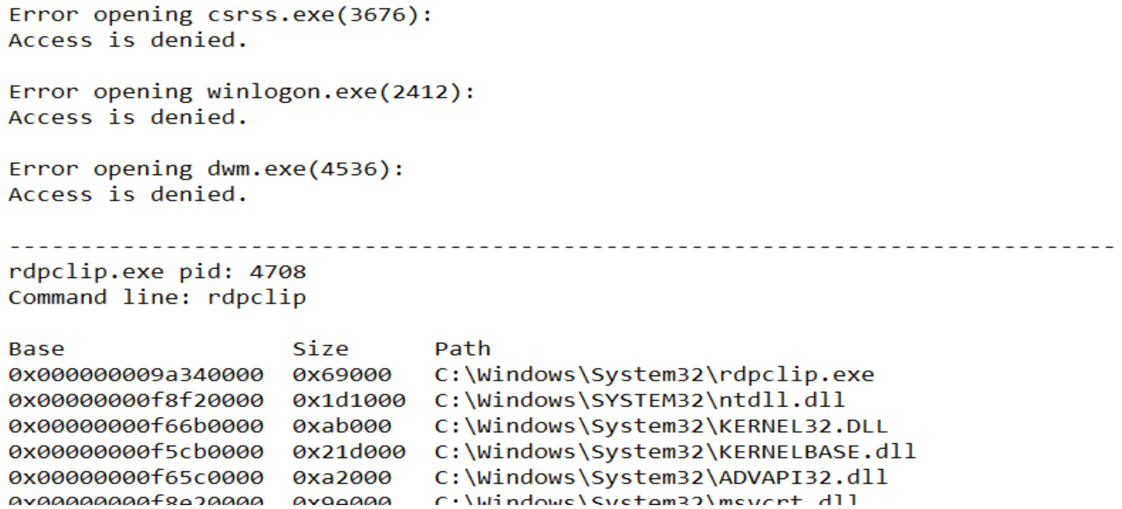


```
PS C:\Users\JSmith\Desktop> .\Listdlls.exe -r "perl|6576"

Listdlls v3.2 - Listdlls
Copyright (C) 1997-2016 Mark Russinovich
Sysinternals

No matching processes were found.
PS C:\Users\JSmith\Desktop> .\Listdlls.exe -r perl

Listdlls v3.2 - Listdlls
Copyright (C) 1997-2016 Mark Russinovich
Sysinternals

------------------------------------------------------------------------------
perl.exe pid: 6576
Command line: "C:\Strawberry\perl\bin\perl.exe"

Base                Size      Path
0x0000000000400000  0x11000   C:\Strawberry\perl\bin\perl.exe
0x00000000f8f20000  0x1d1000  C:\Windows\SYSTEM32\ntdll.dll
```

Figure: Various commands run by the attacker

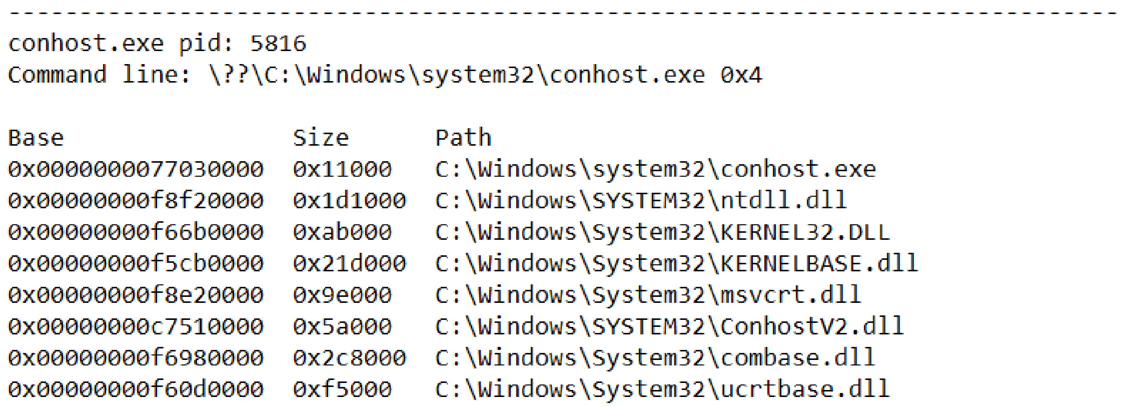
3. What specific process did the attacker seem to take an interest in? (Process in this context would be references to .exe files which are executable applications.)

A: Attacker seems to be interested in knowing all the open services running on the device. After getting the details the open processes by running ./Listdlls.exe. Attackers could transfer malicious files over to the device using an unsecure open process such rdpclip.exe which is open and can be used to share clip-board between the local computer and the remote desktop. Attacker also interested in replacing original file with malicious files with same name to achieve privilege escalation.



```
Error opening csrss.exe(3676):
Access is denied.

Error opening winlogon.exe(2412):
Access is denied.

Error opening dwm.exe(4536):
Access is denied.

------------------------------------------------------------------------------
rdpclip.exe pid: 4708
Command line: rdpclip

Base                Size      Path
0x000000009a340000  0x69000   C:\Windows\System32\rdpclip.exe
0x00000000f8f20000  0x1d1000  C:\Windows\SYSTEM32\ntdll.dll
0x00000000f66b0000  0xab000   C:\Windows\System32\KERNEL32.DLL
0x00000000f5cb0000  0x21d000  C:\Windows\System32\KERNELBASE.dll
0x00000000f65c0000  0xa2000   C:\Windows\System32\ADVAPI32.dll
0x00000000f8e20000  0x9e000   C:\Windows\System32\msvcrt.dll
```

Figure: Listdll running all the process - Found redclip.exe as open

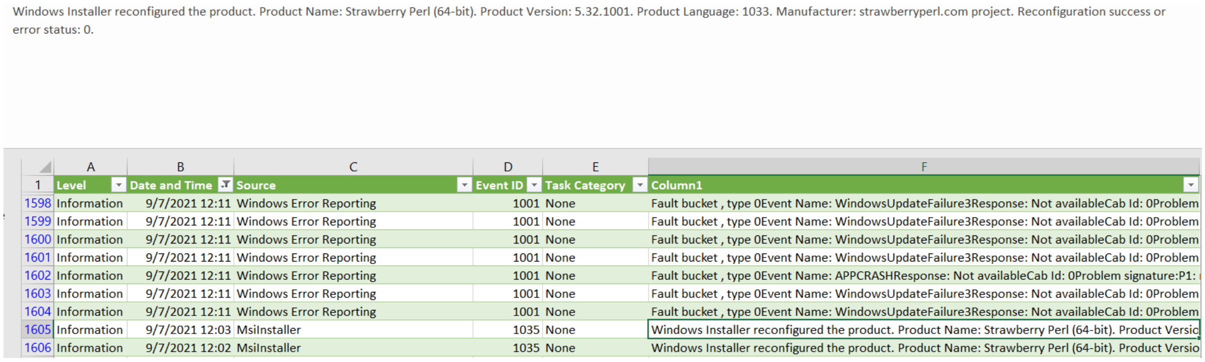


```
------------------------------------------------------------------------------
conhost.exe pid: 5816
Command line: \??\C:\Windows\system32\conhost.exe 0x4

Base                Size      Path
0x0000000077030000  0x11000   C:\Windows\system32\conhost.exe
0x00000000f8f20000  0x1d1000  C:\Windows\SYSTEM32\ntdll.dll
0x00000000f66b0000  0xab000   C:\Windows\System32\KERNEL32.DLL
0x00000000f5cb0000  0x21d000  C:\Windows\System32\KERNELBASE.dll
0x00000000f8e20000  0x9e000   C:\Windows\System32\msvcrt.dll
0x00000000c7510000  0x5a000   C:\Windows\SYSTEM32\ConhostV2.dll
0x00000000f6980000  0x2c8000  C:\Windows\System32\combase.dll
0x00000000f60d0000  0xf5000   C:\Windows\System32\ucrtbase.dll
```

Figure: Listdll running all the process - Found conhost.exe as open

Privilege Escalation

1. What application did the attacker use to set a trap for the administrative user?
A: The attacker used **perl.exe** file to set a trap for the administrative user by placing it in at the location C:\Users\JSmith of the JSmith account. The user is tricked to think that the file is an actual perl.exe since the **Strawberry Perl** is already being used in their current work environment.



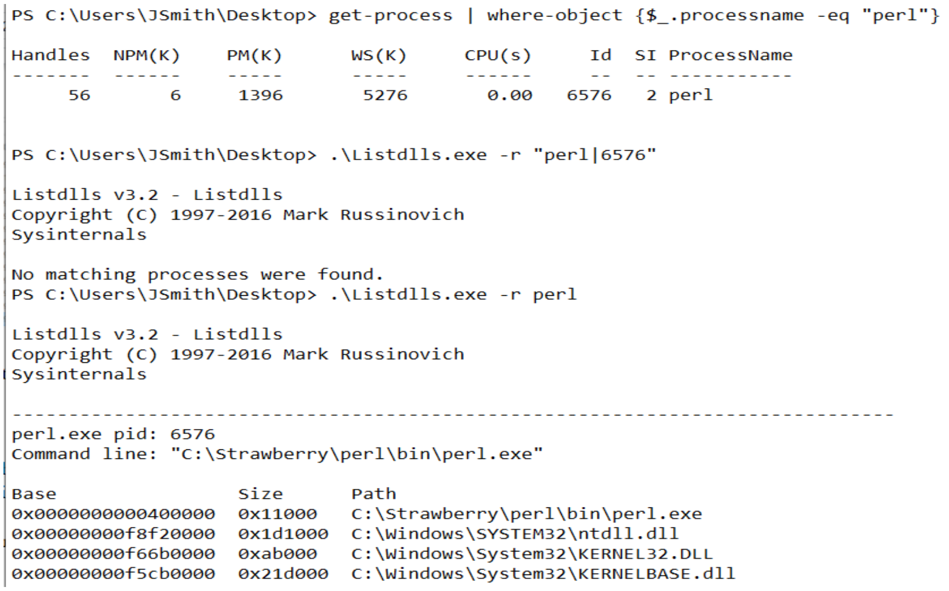
Windows Installer reconfigured the product. Product Name: Strawberry Perl (64-bit). Product Version: 5.32.1001. Product Language: 1033. Manufacturer: strawberryperl.com project. Reconfiguration success or error status: 0.

	A	B	C	D	E	F
1	Level	Date and Time	Source	Event ID	Task Category	Column1
1598	Information	9/7/2021 12:11	Windows Error Reporting	1001	None	Fault bucket , type 0Event Name: WindowsUpdateFailure3Response: Not availableCab Id: 0Problem
1599	Information	9/7/2021 12:11	Windows Error Reporting	1001	None	Fault bucket , type 0Event Name: WindowsUpdateFailure3Response: Not availableCab Id: 0Problem
1600	Information	9/7/2021 12:11	Windows Error Reporting	1001	None	Fault bucket , type 0Event Name: WindowsUpdateFailure3Response: Not availableCab Id: 0Problem
1601	Information	9/7/2021 12:11	Windows Error Reporting	1001	None	Fault bucket , type 0Event Name: WindowsUpdateFailure3Response: Not availableCab Id: 0Problem
1602	Information	9/7/2021 12:11	Windows Error Reporting	1001	None	Fault bucket , type 0Event Name: APPCRASHResponse: Not availableCab Id: 0Problem signature:P1:
1603	Information	9/7/2021 12:11	Windows Error Reporting	1001	None	Fault bucket , type 0Event Name: WindowsUpdateFailure3Response: Not availableCab Id: 0Problem
1604	Information	9/7/2021 12:11	Windows Error Reporting	1001	None	Fault bucket , type 0Event Name: WindowsUpdateFailure3Response: Not availableCab Id: 0Problem
1605	Information	9/7/2021 12:03	MsiInstaller	1035	None	Windows Installer reconfigured the product. Product Name: Strawberry Perl (64-bit). Product Versic
1606	Information	9/7/2021 12:02	MsiInstaller	1035	None	Windows Installer reconfigured the product. Product Name: Strawberry Perl (64-bit). Product Versio

Figure: Attacker using MsInstaller to reconfigure the legitimate Strawberry perl application (taken from Event Viewer -> Application Logs)

2. Did the attacker move the legitimate application?

A: The attacker tried to move the legitimate application and the command used by the attacker ./Listdlls.exe -r "perl | 6576" shows flag that reveals DLL that is relocated because they are not loaded at their base address.

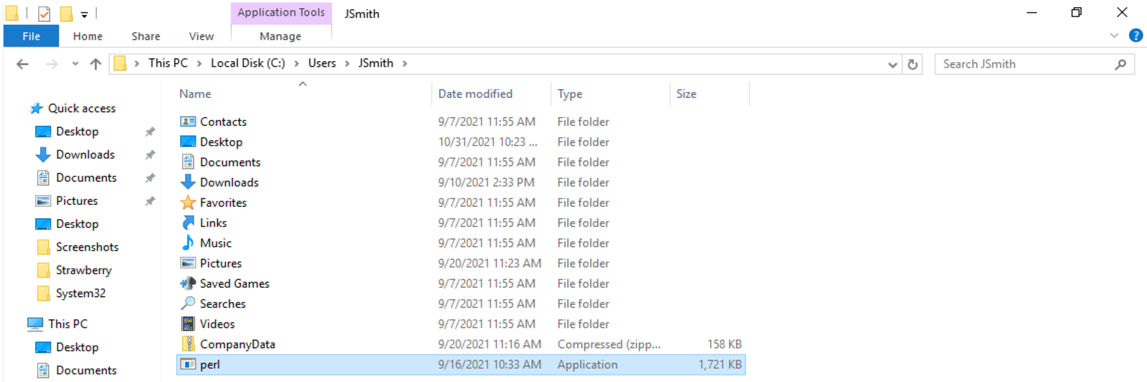


```
PS C:\Users\JSmith\Desktop> get-process | where-object {$_.processname -eq "perl"}

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)     Id  SI ProcessName
-------  ------    -----      -----     ------     --  -- -----------
     56       6     1396       5276       0.00   6576   2 perl


PS C:\Users\JSmith\Desktop> .\Listdlls.exe -r "perl|6576"

Listdlls v3.2 - Listdlls
Copyright (C) 1997-2016 Mark Russinovich
Sysinternals

No matching processes were found.
PS C:\Users\JSmith\Desktop> .\Listdlls.exe -r perl

Listdlls v3.2 - Listdlls
Copyright (C) 1997-2016 Mark Russinovich
Sysinternals

------------------------------------------------------------------------------
perl.exe pid: 6576
Command line: "C:\Strawberry\perl\bin\perl.exe"

Base                Size      Path
0x0000000000400000  0x11000   C:\Strawberry\perl\bin\perl.exe
0x00000000f8f20000  0x1d1000  C:\Windows\SYSTEM32\ntdll.dll
0x00000000f66b0000  0xab000   C:\Windows\System32\KERNEL32.DLL
0x00000000f5cb0000  0x21d000  C:\Windows\System32\KERNELBASE.dll
```

Figure: Attacker running commands to check relocated libraries

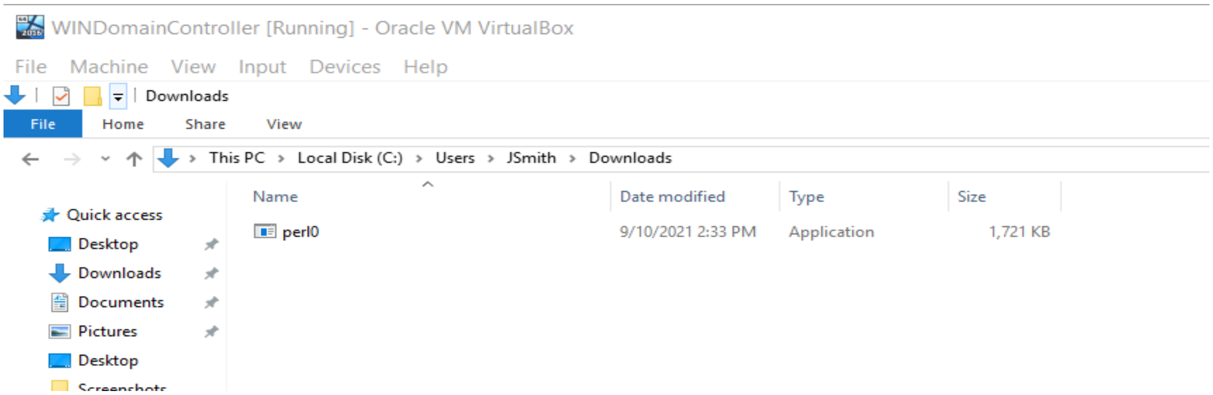
3. What file did the attacker replace the legitimate application with?

A: The attacker replaced the legitimate application with perl.exe at the location C:\Users\JSmith and also placed the **perl0.exe** in the download folder to set the trap. Attacker deleted one of the malicious file (moved to recycle bin) which was later detected and deleted immediately by the Windows Defender.



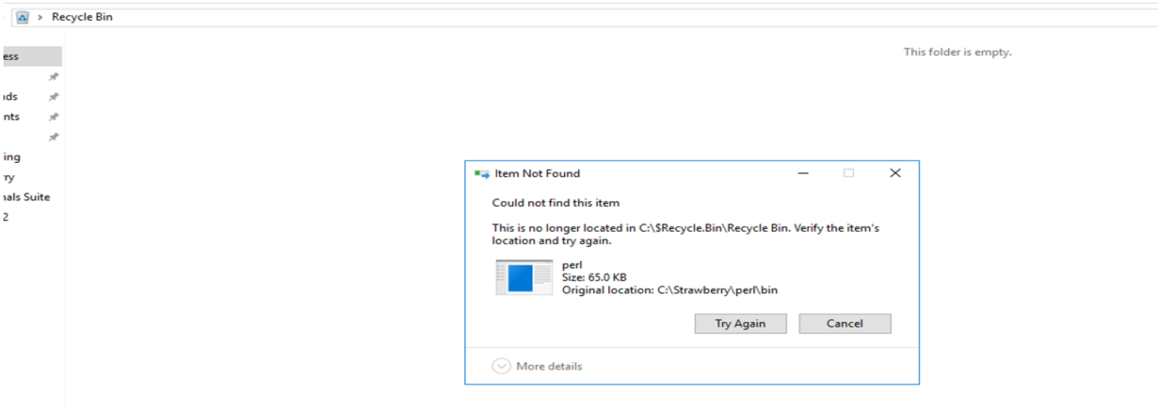
Name	Date modified	Type	Size
Contacts	9/7/2021 11:55 AM	File folder	
Desktop	10/31/2021 10:23 ...	File folder	
Documents	9/7/2021 11:55 AM	File folder	
Downloads	9/10/2021 2:33 PM	File folder	
Favorites	9/7/2021 11:55 AM	File folder	
Links	9/7/2021 11:55 AM	File folder	
Music	9/7/2021 11:55 AM	File folder	
Pictures	9/20/2021 11:23 AM	File folder	
Saved Games	9/7/2021 11:55 AM	File folder	
Searches	9/7/2021 11:55 AM	File folder	
Videos	9/7/2021 11:55 AM	File folder	
CompanyData	9/20/2021 11:16 AM	Compressed (zipp...	158 KB
perl	9/16/2021 10:33 AM	Application	1,721 KB

Figure: Malicious perl.exe at the location C:\Users\JSmith



Name	Date modified	Type	Size
perl0	9/10/2021 2:33 PM	Application	1,721 KB

Figure: Malicious perl0.exe at the location C:\Users\JSmith\Downloads



Could not find this item

This is no longer located in C:\$Recycle.Bin\Recycle Bin. Verify the item's location and try again.

perl
Size: 65.0 KB
Original location: C:\Strawberry\perl\bin

Figure: Malicious perl.exe found and deleted from the Recycle bin

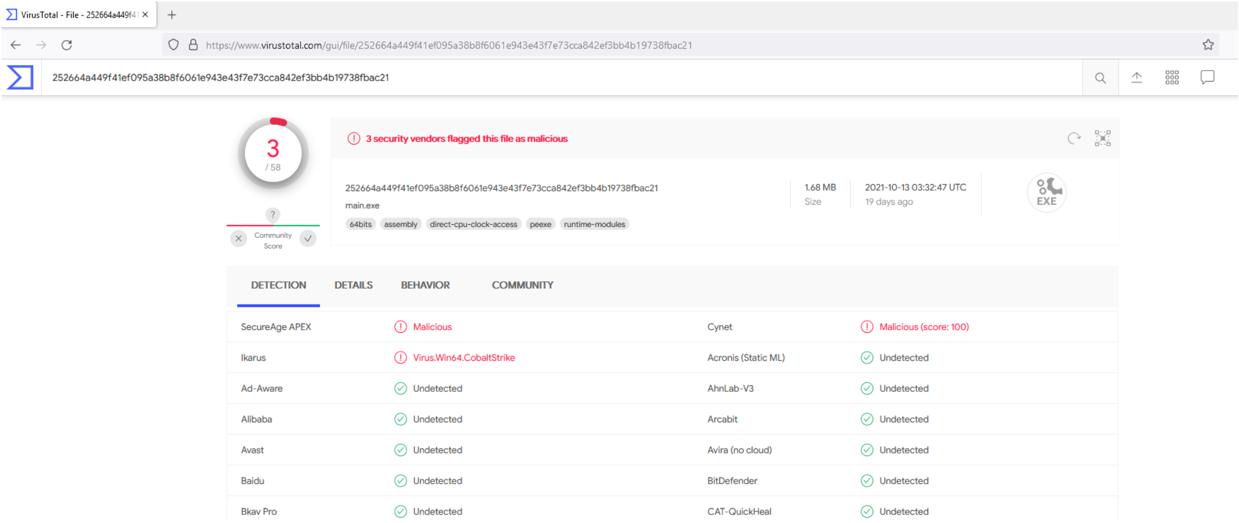
4. Submit the malicious file and legitimate file to https://www.virustotal.com . What are their hash values?

Hash values including MD5, SHA-1, SHA-256 for malicious perl.exe file are as follows:

MD5	**3bfed4c5ff7e5c7c401d1bd26ba458b5**
SHA-1	**55a5a4258d10edcce87536b0e2cc4dd68316b372**
SHA-256	**252664a449f41ef095a38b8f6061e943e43f7e73cca842ef3bb4b19738fbac21**
Vhash	016067555d1d15541az27!z
Authentihash	4565e90447d4c51106545335e08419097df64f2563f747c6280261143119cb1e
Imphash	4035d2883e01d64f3e7a9dccb1d63af5

SSDEEP
12288:KDhoO62l1fY0w5G3sTzjMVCJG3Jxq3teNqQMaaPhEB+TErMPStoh3IAFy8jlK1v:2ho9B15G8fjz6qaD+33Zo8jU1v

TLSH
T141852A52B8E254BAC17AE1304691D3717A327C654B326BD72FC4B6AA1A75FD42F3E300


VirusTotal - File - 252664a449f41
https://www.virustotal.com/gui/file/252664a449f41ef095a38b8f6061e943e43f7e73cca842ef3bb4b19738fbac21
252664a449f41ef095a38b8f6061e943e43f7e73cca842ef3bb4b19738fbac21
3
/ 58
?
Community Score
EXE
DETECTION
DETAILS
BEHAVIOR
COMMUNITY

3 security vendors flagged this file as malicious

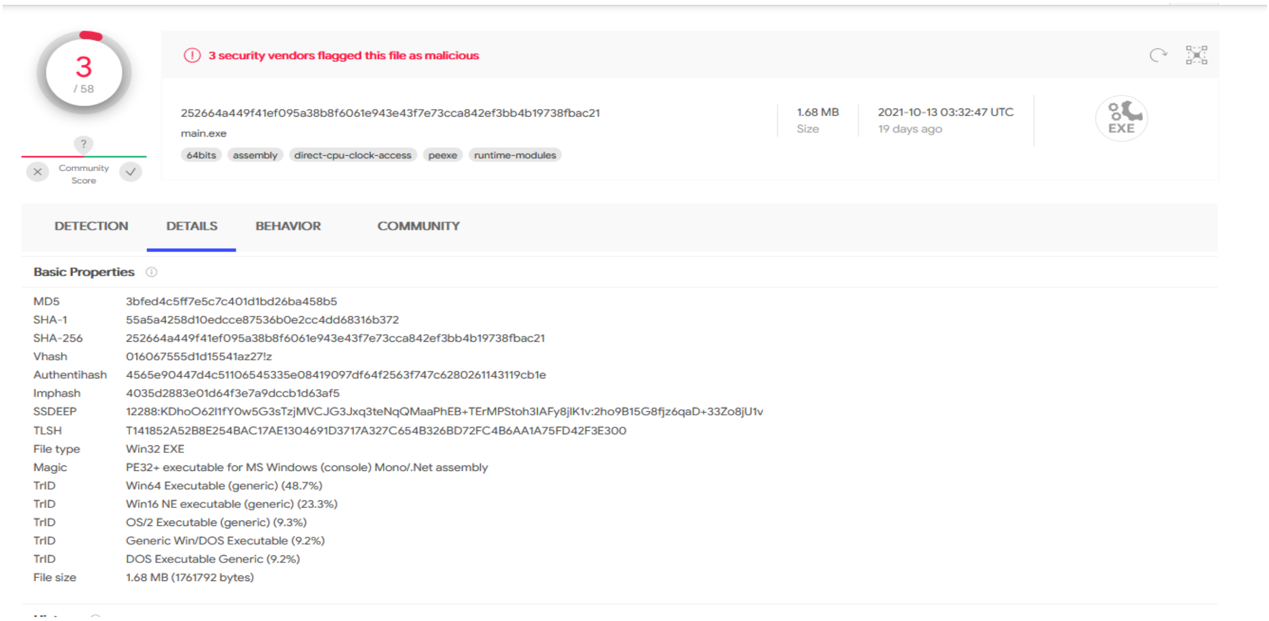
252664a449f41ef095a38b8f6061e943e43f7e73cca842ef3bb4b19738fbac21
main.exe
64bits assembly direct-cpu-clock-access peexe runtime-modules

1.68 MB
Size

2021-10-13 03:32:47 UTC
19 days ago

SecureAge APEX	Malicious	Cynet	Malicious (score: 100)
Ikarus	Virus.Win64.CobaltStrike	Acronis (Static ML)	✓ Undetected
Ad-Aware	✓ Undetected	AhnLab-V3	✓ Undetected
Alibaba	✓ Undetected	Arcabit	✓ Undetected
Avast	✓ Undetected	Avira (no cloud)	✓ Undetected
Baidu	✓ Undetected	BitDefender	✓ Undetected
Bkav Pro	✓ Undetected	CAT-QuickHeal	✓ Undetected

Figure: Malicious perl.exe (changed named as main.exe) on virustotal.com



3 security vendors flagged this file as malicious

252664a449f41ef095a38b8f6061e943e43f7e73cca842ef3bb4b19738fbac21
main.exe
64bits assembly direct-cpu-clock-access peexe runtime-modules

1.68 MB
Size

2021-10-13 03:32:47 UTC
19 days ago

Basic Properties

MD5	3bfed4c5ff7e5c7c401d1bd26ba458b5
SHA-1	55a5a4258d10edcce87536b0e2cc4dd68316b372
SHA-256	252664a449f41ef095a38b8f6061e943e43f7e73cca842ef3bb4b19738fbac21
Vhash	016067555d1d15541az27!z
Authentihash	4565e90447d4c51106545335e08419097df64f2563f747c6280261143119cb1e
Imphash	4035d2883e01d64f3e7a9dccb1d63af5
SSDEEP	12288:KDhoO62l1fYOw5G3sTzjMVCJG3Jxq3teNqQMaaPhEB+TErMPStoh3lAFy8jlK1v:2ho9B15G8fjz6qaD+33Zo8jU1v
TLSH	T141852A52B8E254BAC17AE1304691D3717A327C654B326BD72FC4B6AA1A75FD42F3E300
File type	Win32 EXE
Magic	PE32+ executable for MS Windows (console) Mono/.Net assembly
TrID	Win64 Executable (generic) (48.7%)
TrID	Win16 NE executable (generic) (23.3%)
TrID	OS/2 Executable (generic) (9.3%)
TrID	Generic Win/DOS Executable (9.2%)
TrID	DOS Executable Generic (9.2%)
File size	1.68 MB (1761792 bytes)

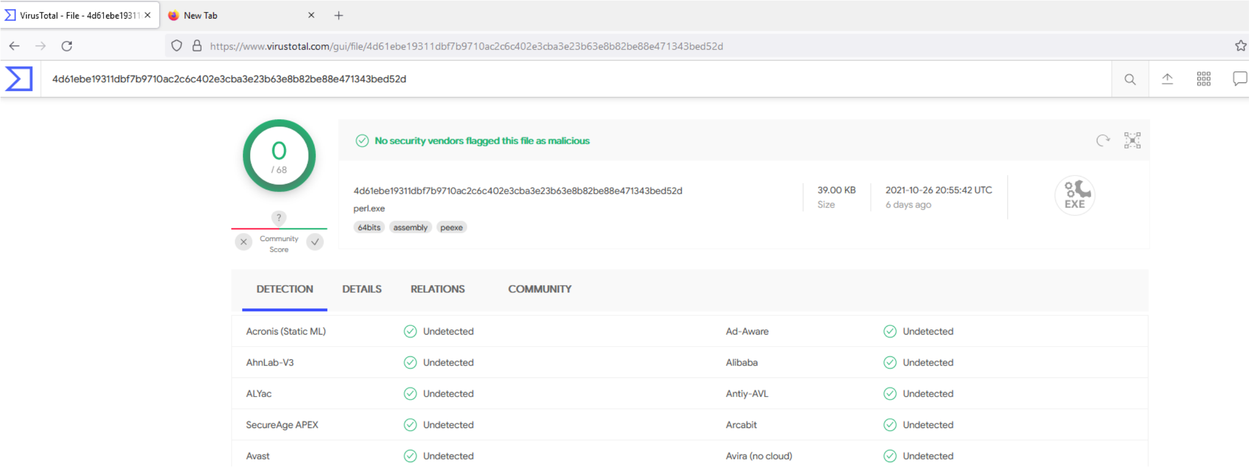
Figure: Malicious perl.exe details

Hash values including MD5, SHA-1, SHA-256 for legitimate perl.exe file are as follows:

MD5	**3686d8a7e98b82a6452f88fef293ca1a**
SHA-1	**ba0aa4d51c899f46020016990da4aa4fee894781**
SHA-256	**4d61ebe19311dbf7b9710ac2c6c402e3cba3e23b63e8b82be88e471343bed52d**
Vhash	0340a75d1515151c0d1d1az1818=z
Authentihash	617a4e8287cfd66789492c0259b89c52b57f15a745e0a972ded19ff8a8d14988
Imphash	67a6855fa04c28fd71f92ba73b95a0a5

SSDEEP
384:U6ok7XaBkRq4jCtlWp4IcH7c1y8OyEUDYVXXQTUVFFtFF9vXM/ewCue:Cd+/CLMgz8vEUDCFFtFF9vyC

TLSH
T13B03F80E7266D898C11A81B4D8E687F0E660FDF0D910073F227BFF663F717505A6626A


VirusTotal - File - 4d61ebe19311
New Tab
https://www.virustotal.com/gui/file/4d61ebe19311dbf7b9710ac2c6c402e3cba3e23b63e8b82be88e471343bed52d
4d61ebe19311dbf7b9710ac2c6c402e3cba3e23b63e8b82be88e471343bed52d
0
/ 68
?
Community Score
EXE
DETECTION
DETAILS
RELATIONS
COMMUNITY

No security vendors flagged this file as malicious

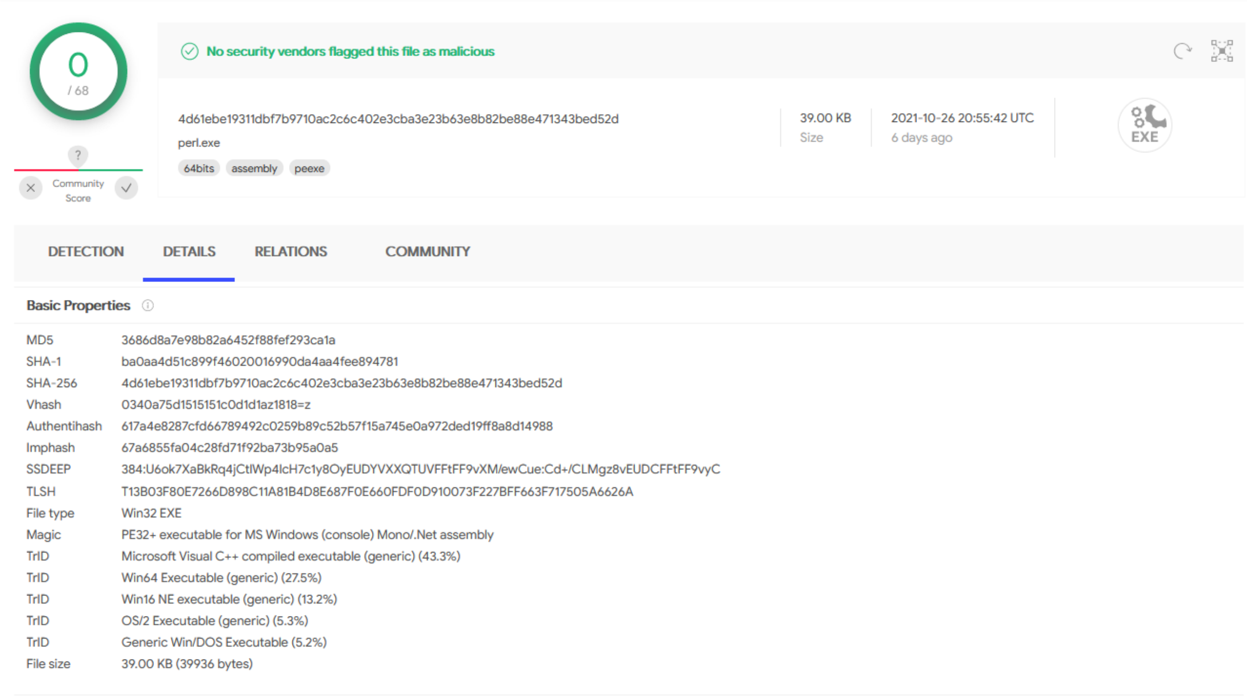
4d61ebe19311dbf7b9710ac2c6c402e3cba3e23b63e8b82be88e471343bed52d
perl.exe
64bits assembly peexe

39.00 KB
Size

2021-10-26 20:55:42 UTC
6 days ago

Acronis (Static ML)	Undetected	Ad-Aware	Undetected
AhnLab-V3	Undetected	Alibaba	Undetected
ALYac	Undetected	Antiy-AVL	Undetected
SecureAge APEX	Undetected	Arcabit	Undetected
Avast	Undetected	Avira (no cloud)	Undetected

Figure: Legitimate perl.exe on virustotal.com



No security vendors flagged this file as malicious

4d61ebe19311dbf7b9710ac2c6c402e3cba3e23b63e8b82be88e471343bed52d
perl.exe
64bits assembly peexe

39.00 KB
Size

2021-10-26 20:55:42 UTC
6 days ago

Basic Properties

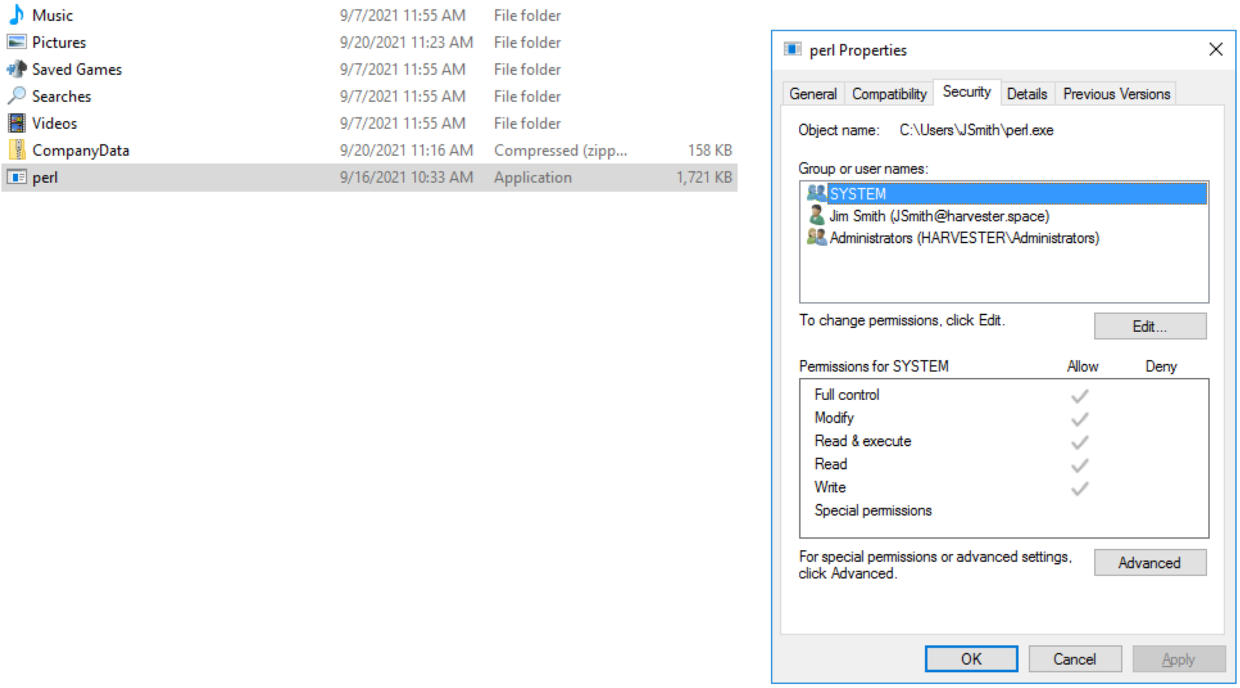
MD5	3686d8a7e98b82a6452f88fef293ca1a
SHA-1	ba0aa4d51c899f46020016990da4aa4fee894781
SHA-256	4d61ebe19311dbf7b9710ac2c6c402e3cba3e23b63e8b82be88e471343bed52d
Vhash	0340a75d1515151c0d1d1az1818=z
Authentihash	617a4e8287cfd66789492c0259b89c52b57f15a745e0a972ded19ff8a8d14988
Imphash	67a6855fa04c28fd71f92ba73b95a0a5
SSDEEP	384:U6ok7XaBkRq4jCtlWp4lcH7c1y8OyEUDYVXXQTUVFFtFF9vXM/ewCue:Cd+/CLMgz8vEUDCFFtFF9vyC
TLSH	T13B03F80E7266D898C11A81B4D8E687F0E660FDF0D910073F227BFF663F717505A6626A
File type	Win32 EXE
Magic	PE32+ executable for MS Windows (console) Mono/.Net assembly
TrID	Microsoft Visual C++ compiled executable (generic) (43.3%)
TrID	Win64 Executable (generic) (27.5%)
TrID	Win16 NE executable (generic) (13.2%)
TrID	OS/2 Executable (generic) (5.3%)
TrID	Generic Win/DOS Executable (5.2%)
File size	39.00 KB (39936 bytes)

Figure: Hash Values for perl.exe on virustotal.com

5. Explain what you think the attacker may have done to get access to the administrative user.

A: The attacker placed a malicious file name perl.exe among the files of JSmtih with administrator rights configured into the file so that it will impersonate administrator privileges when they are accessed. Since, there is already a legitimate file called perl.exe being used as a workplace application and the attacker has full access to JSmith account, a file trap with the exact same name such as this is used and ultimately to gain administrator access and successful privileges escalation by the attacker. Attacker could have removed the shortcut file of legitimate perl.exe and placed a shortcut for malicious perl.exe (of the downloaded file from C:\Users\JSmith\Downloads).

Also, the attacker placed an images file at the location C:\SharedFolders\proof.png that clearly read as a ransom note asking to pay in bitcoins.



Music	9/7/2021 11:55 AM	File folder	
Pictures	9/20/2021 11:23 AM	File folder	
Saved Games	9/7/2021 11:55 AM	File folder	
Searches	9/7/2021 11:55 AM	File folder	
Videos	9/7/2021 11:55 AM	File folder	
CompanyData	9/20/2021 11:16 AM	Compressed (zipp...	158 KB
perl	9/16/2021 10:33 AM	Application	1,721 KB

perl Properties

Object name: C:\Users\JSmith\perl.exe

Group or user names:

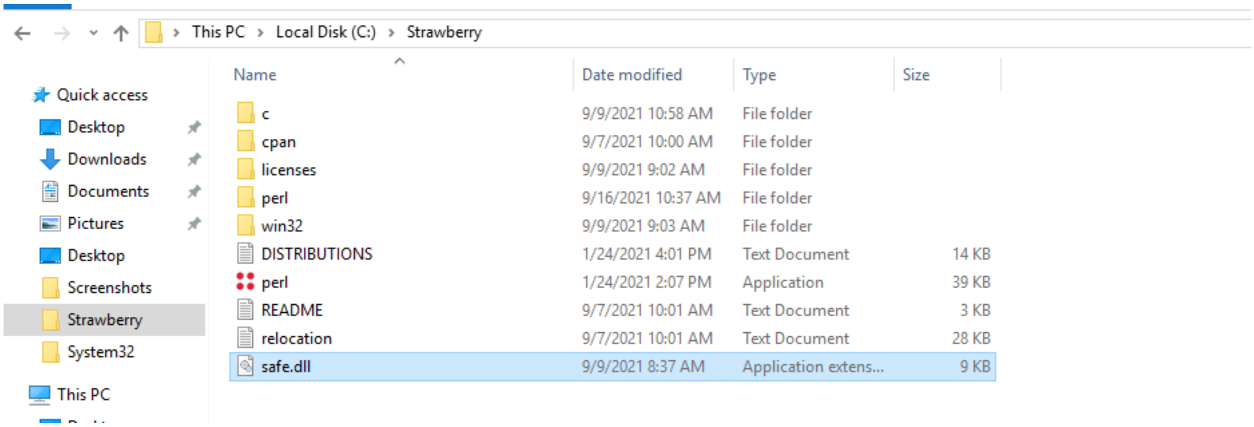
SYSTEM
Jim Smith (JSmith@harvester.space)
Administrators (HARVESTER\Administrators)

To change permissions, click Edit.

Permissions for SYSTEM	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
Read	✓	
Write	✓	
Special permissions		

For special permissions or advanced settings, click Advanced.

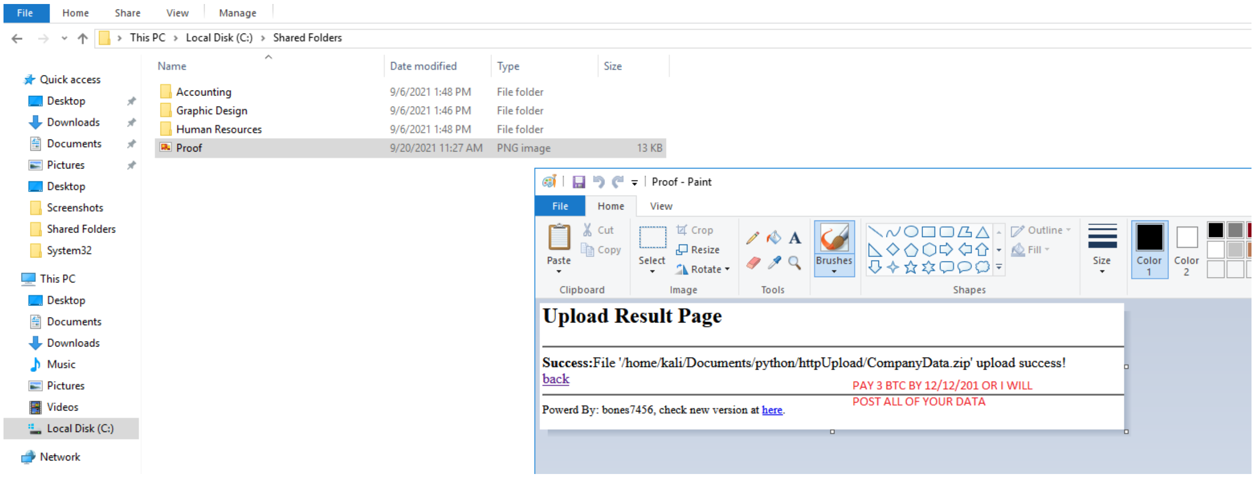
Figure: Permissions for the malicious perl.exe



This PC › Local Disk (C:) › Strawberry

Name	Date modified	Type	Size
c	9/9/2021 10:58 AM	File folder	
cpan	9/7/2021 10:00 AM	File folder	
licenses	9/9/2021 9:02 AM	File folder	
perl	9/16/2021 10:37 AM	File folder	
win32	9/9/2021 9:03 AM	File folder	
DISTRIBUTIONS	1/24/2021 4:01 PM	Text Document	14 KB
perl	1/24/2021 2:07 PM	Application	39 KB
README	9/7/2021 10:01 AM	Text Document	3 KB
relocation	9/7/2021 10:01 AM	Text Document	28 KB
safe.dll	9/9/2021 8:37 AM	Application extens...	9 KB

Figure: Legitimate perl.exe file located at C:\Strawberry



Name	Date modified	Type	Size
Accounting	9/6/2021 1:48 PM	File folder	
Graphic Design	9/6/2021 1:46 PM	File folder	
Human Resources	9/6/2021 1:48 PM	File folder	
Proof	9/20/2021 11:27 AM	PNG image	13 KB

Upload Result Page

Success: File '/home/kali/Documents/python/httpUpload/CompanyData.zip' upload success!

back

PAY 3 BTC BY 12/12/201 OR I WILL
POST ALL OF YOUR DATA

Powerd By: bones7456, check new version at here.

Figure: Ransom note by the attacker placed at the location C:\SharedFolders