Hunting down Dofoil with Windows Defender ATP

cloudblogs.microsoft.com/microsoftsecure/2018/04/04/hunting-down-dofoil-with-windows-defender-atp/

April 4, 2018

Dofoil is a sophisticated threat that attempted to install coin miner malware on hundreds of thousands of computers in March, 2018. In previous blog posts we detailed how behavior monitoring and machine learning in Windows Defender AV protected customers from a massive Dofoil outbreak that we traced back to a software update poisoning campaign several weeks prior. Notably, customers of Windows 10 S, a special Windows 10 configuration that provides streamlined Microsoft-verified security, were not affected by the Dofoil outbreak.

In this blog post, we will expound on Dofoil's anti-debugging and anti-analysis tactics, and demonstrate how the rich detection libraries of Windows Defender Advanced Threat Protection and Windows Defender Exploit Guard can help during investigation.

We found that Dofoil was designed to be elusive to analysis. It checks its environment and stops running in virtual machine environments. It also checks for various analysis tools and kills them right away. This can make malware analysis and assessment challenging.

The following diagram shows the multi-stage malware execution process, which includes checks for traits of analysis environments during some stages.

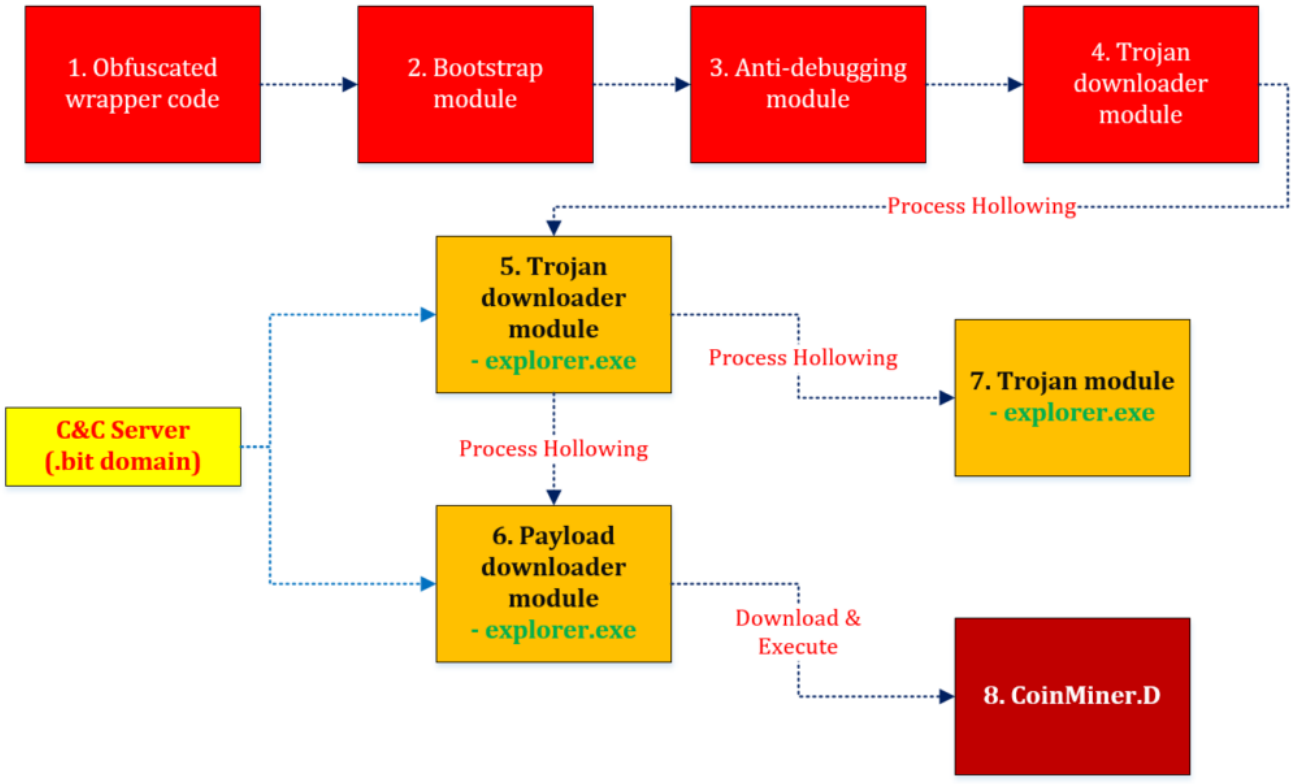


Figure 1. Dofoil multi-stage shellcode and payload execution flow

The table below describes the purpose of each stage. The first five stages have at least one or two different techniques that can deter dynamic or static malware analysis.

STAGES	DESCRIPTION

1. Obfuscated wrapper code	Anti-heuristics Anti-emulation
2. Bootstrap module	Performs self-process hollowing to load the next module
3. Anti-debugging module	Performs anti-debugging operation
4. Trojan downloader module	Performs system environment checks Performs anti-VM operation Injects itself to *explorer.exe* through process hollowing
5. Trojan downloader module in *explorer.exe*	Contacts C&C server to download trojan and run it using process hollowing technique
6. Payload downloader module in *explorer.exe*	Contacts C&C server to download the main payload
7. Trojan module	Steals credentials from various application settings and sends stolen into to the C&C server over HTTP channel
8. CoinMiner.D	Mines digital currencies

Table 1. Dofoil's multi-stage modules

Initial stages

The first three stages (i.e., obfuscated wrapper code, bootstrap module, anti-debugging module) use the following techniques to avoid analysis and identification.

ANTI-ANALYSIS TECHNIQUES	DESCRIPTION
Benign code insertion	Inserts a huge benign code block to confuse heuristics and manual inspection
Anti-emulation	Enumerates an arbitrary registry key *(HKEY_CLASSES_ROOT\Interface\{3050F557-98B5-11CF-BB82-00AA00BDCE0B}*) and compares the data with an expected value (*DispHTMLCurrentStyle*) to check if the malware runs inside an emulator
Self-process hollowing	Uses the process hollowing technique on the current process, making analysis extra difficult due to the altered code mapping
Debugger checks	Checks for debuggers, and modifies code to crash. This can add additional layer of confusion to researchers, who are bound to investigate the cause of the crashes. It checks for the *PEB.BeingDebugged* and *PEB.NtGlobalFlag* fields in the PEB structure. For example, *PEB.BeingDebugged* is set to *1* and *PEB.NtGlobalFlag* is set to *FLG_HEAP_ENABLE_TAIL_CHECK*|*FLG_HEAP_ENABLE_FREE_CHECK*| *FLG_HEAP_VALIDATE_PARAMETERS* when a debugger is attached to the process.

Table 2. Anti-analysis techniques

The first stage contains some benign-looking code before the actual malicious code. This can give the executable a harmless appearance. It can also make the emulation of the code difficult because emulating various API calls that are not present in many malware codes can be challenging.

The first-stage code also performs a registry key enumeration to make sure it has the expected value. When all checks are passed, it decodes the second-stage shellcode and runs it on the allocated memory. This shellcode un-maps the original main module's memory, and then decodes the third-stage shellcode into that memory – this is known as a self-process hollowing technique.

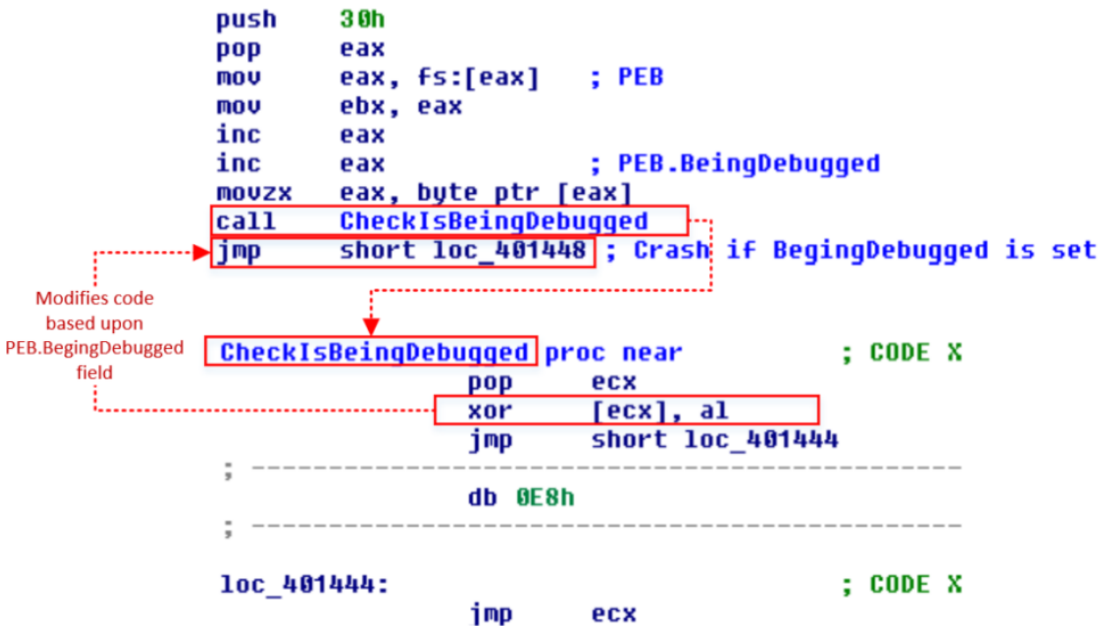


Figure 2. Self-modification based on PEB.BeingDebugged value

Windows Defender ATP's process tree can help with investigation by exposing these anti-debugging techniques.

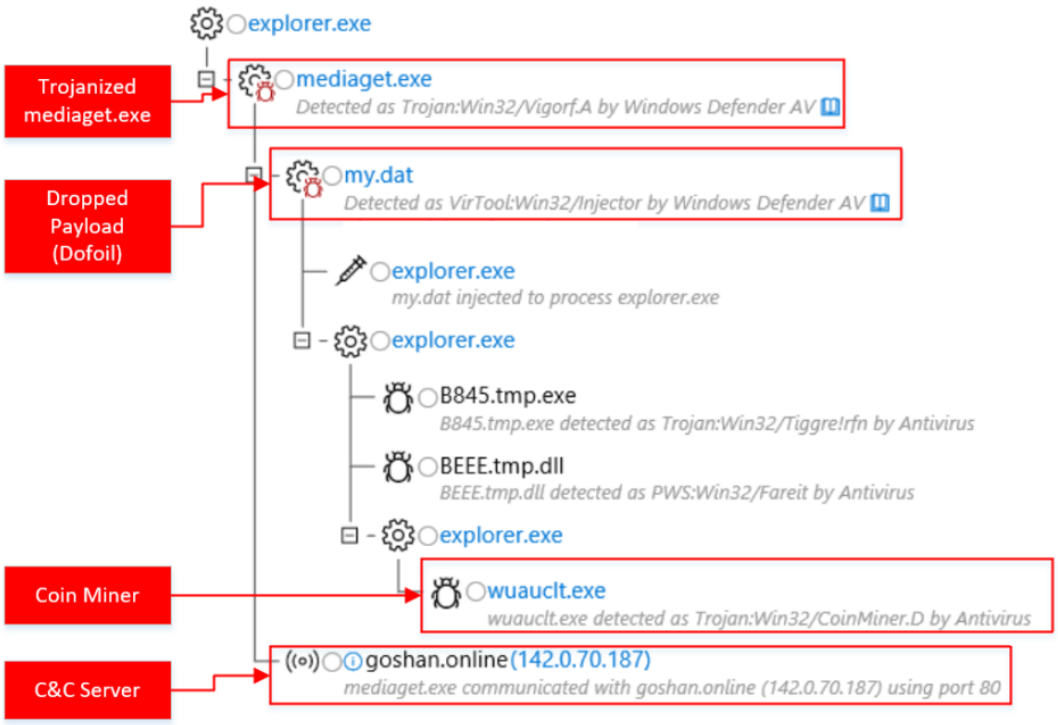


Figure 3. Windows Defender ATP process tree showing anti-debugging techniques

Trojan downloader module

The trojan downloader module performs various environment checks, including virtual environment and analysis tool checks, before downloading the payload.

ANTI-ANALYSIS TECHNIQUES	DESCRIPTION
Check module name	Checks if the main executable name contains the string “sample”
Check volume serial	Checks if current volume serial number is *0xCD1A40* or *0x70144646*
Check modules	Checks the presence of DLLs related to debuggers
Check disk-related registry keys	Checks the value of the registry key *HKLM\System\CurrentControlSet\Services\Disk\Enum* against well-known disk name patterns for virtual machines (*qemu*, *virtual*, *vmware*, *xen*, *ffffcce24*)
Process check	Checks running processes and kills those with processes names associated with analysis tools (*procexp.exe*, *procexp64.exe*, *procmon.exe*, *procmon64.exe*, *tcpview.exe*, *wireshark.exe*, *processhacker.exe*, *ollydbg.exe*, *idaq.exe*, *x32dbg.exe*)
Windows class name check	Checks the current Windows class names and exits when some well-known names are found (*Autoruns*, *PROCEXPL*, *PROCMON_WINDOW_CLASS*, *TCPViewClass*, *ProcessHacker*, *OllyDbg*, *WinDbgFrameClass*)

Table 3. Anti-analysis technique of Dofoil’s trojan downloader module

The list of target process names and Windows class names exist in custom checksum form. The checksum algorithm looks like the following:

```
loc_423BE6:                             ; C
                movzx   ebx, byte ptr [edx]
                and     bl, 0DFh
                xor     ah, bl
                rol     eax, 8
                xor     al, ah
                inc     edx
                loop    loc_423BE6
```

Figure 4. Shift and XOR custom checksum algorithm

The purpose of this checksum is to prevent malware researchers from quickly figuring out what analysis tools it detects, making analysis more time-consuming.

STRING	CHECKSUM
Autoruns	0x0E5C1C5D
PROCEXPL	0x1D421B41
PROCMON_WINDOW_CLASS	0x4B0C105A
TCPViewClass	0x1D4F5C43
ProcessHacker	0x571A415E
OllyDbg	0x4108161D
WinDbgFrameClass	0x054E1905

procexp.exe	0x19195C02
procexp64.exe	0x1C0E041D
procmon.exe	0x06185D0B
procmon64.exe	0x1D07120A
tcpview.exe	0x060B5118
wireshark.exe	0x550E1E0D
processhacker.exe	0x51565C47
ollydbg.exe	0x04114C14
x32dbg.exe	0x5F4E5C04
idaq.exe	0x14585A12

Table 4. String checksum table used for process names and Windows class names

Process hollowing

Dofoil heavily uses the process hollowing technique. Its main target for process hollowing is explorer.exe. The Dofoil shellcode launches a new instance of explorer.exe, allocates shellcode in heap region, and then modifies the entry point code to jump into the shellcode. This way, the malware avoids using *CreateRemoteThread* API, but can still achieve code injection.

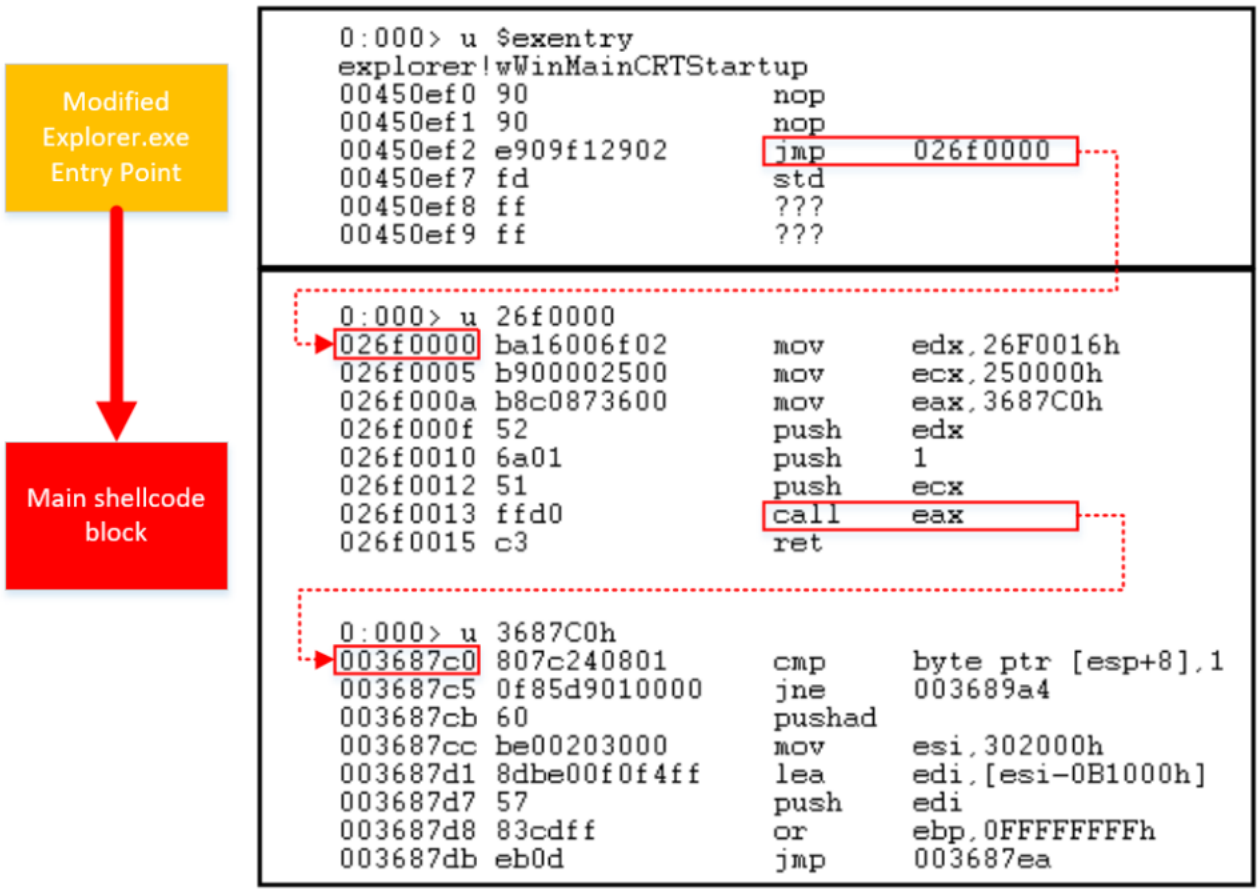


Figure 5. Modification of explorer.exe *entry point code*

Windows Defender ATP can detect the process hollowing behavior with advanced memory signals. The following process tree shows that the malware injects itself into explorer.exe using the process hollowing technique.

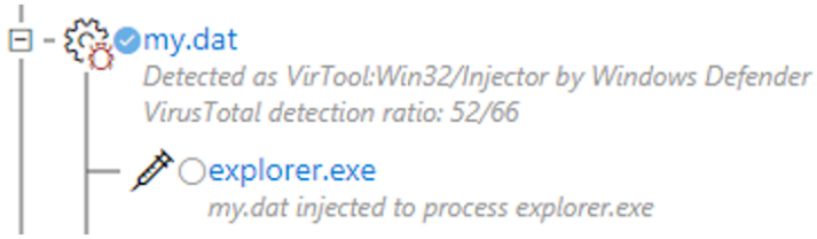


Figure 6. Windows Defender ATP alert process tree showing the first process hollowing

When the shellcode downloads another layer of payload, it spawns another explorer.exe to inject the payload into using process hollowing. Windows Defender ATP can save analysis time on these cases by pinpointing the malicious actions, eliminating the need for guessing what these newly spawned Windows system processes are doing.

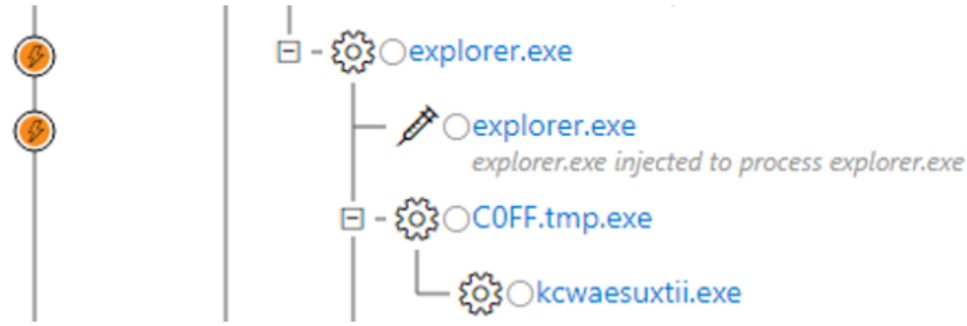


Figure 7. Windows Defender ATP alert process tree showing the second process hollowing

The process hollowing behavior can be detected through Exploit protection in Windows Defender Exploit Guard. This can be done by enabling the Export Address Filter (EAF) mitigation against explorer.exe. The detection happens when the shellcode goes through the export addresses of the modules to find the export address of the LoadLibraryA and GetProcAddress functions.

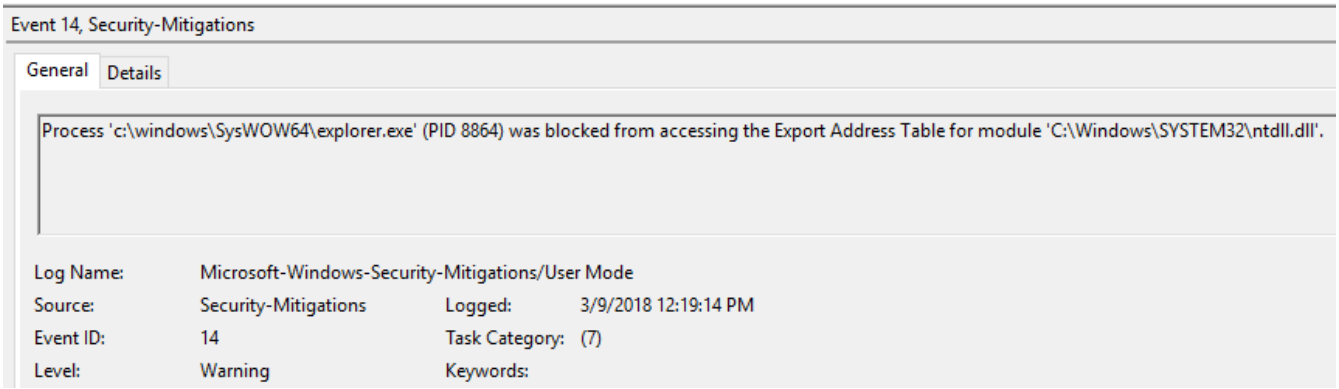


Figure 8. Export Address Filter (EAF) event exposed in Event viewer

Windows Defender Exploit Guard events are also exposed in the Windows Defender ATP portal:

Figure 9. Windows Defender ATP view of the Windows Defender Exploit Guard event

Adding Windows Defender Exploit Guard EAF audit/block policy to common system processes like explorer.exe, cmd.exe, or verclsid.exe can be useful in finding and blocking process hollowing or process injection techniques commonly used by malware. This policy can impact third-party apps that may behave like shellcode, so we recommend testing Windows Defender Exploit Guard with audit mode enabled before enforcement.

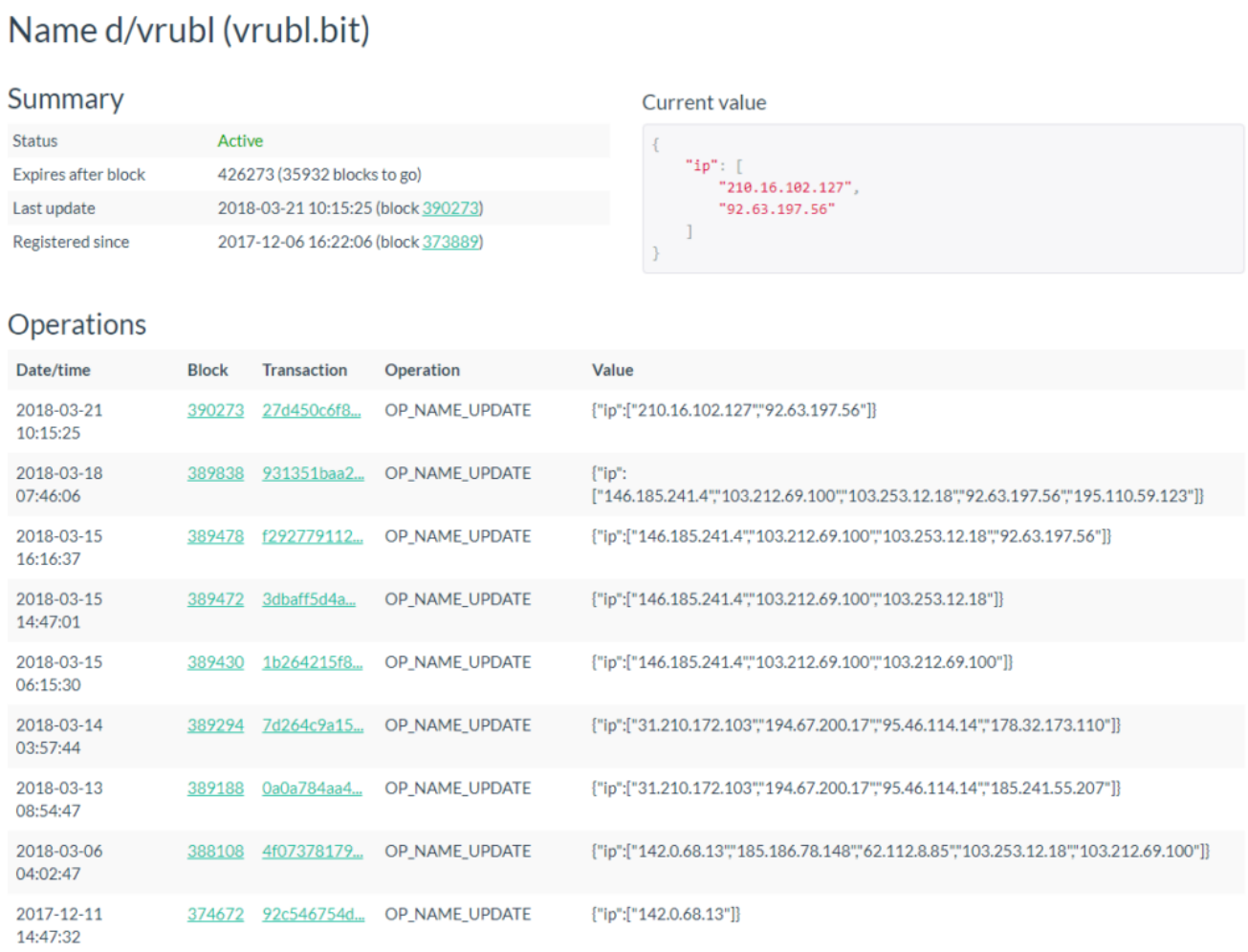
Command-and-control (C&C) and NameCoin domains

Dofoil's C&C connection is very cautious. The trojan code first tries to connect to well-known web pages and verifies that the malware has proper and real Internet connection, not simulated as in test environments. After it makes sure it has a real Internet connection, the malware makes HTTP connections to the actual C&C servers.

2	200	HTTP	www.bing.com	/	126,211	private...	text/html; charset=utf-8	explorer:1132	[#25]
3	301	HTTP	support.microsoft.com	/kb/4023057	0	max-ag...		explorer:1132	[#26]
4	200	HTTP	Tunnel to	support.microsoft.com:443	747			explorer:1132	[#27]
5	200	HTTP	Tunnel to	support.microsoft.com:443	561			explorer:1132	[#28]
6	200	HTTP	Tunnel to	support.microsoft.com:443	561			explorer:1132	[#29]
7	301	HTTP	support.microsoft.com	/kb/4023057	0	max-ag...		explorer:1132	[#30]
8	200	HTTP	Tunnel to	support.microsoft.com:443	747			explorer:1132	[#31]
9	200	HTTP	Tunnel to	support.microsoft.com:443	561			explorer:1132	[#32]
10	200	HTTP	Tunnel to	support.microsoft.com:443	561			explorer:1132	[#33]
11	301	HTTP	www.microsoft.com	/management	166	max-ag...	text/html; charset=UTF-8	explorer:1132	[#34]
12	404	HTTP	www.microsoft.com	/systemcenter/en/us	51,450	private	text/html	explorer:1132	[#35]
13	301	HTTP	www.microsoft.com	/management	166	max-ag...	text/html; charset=UTF-8	explorer:1132	[#36]
14	404	HTTP	www.microsoft.com	/systemcenter/en/us	51,450	private	text/html	explorer:1132	[#37]
15	404	HTTP	103.253.12.18	/15022018/	429,833		text/html; charset=window...	explorer:1132	[#38]

Figure 10. Access to known servers to confirm Internet connectivity

The malware uses NameCoin domain name servers. NameCoin is a decentralized name server system that provides extra privacy backed by blockchain technology. Except for the fact that the DNS client needs to use specific sets of NameCoin DNS servers, the overall operation is very similar to a normal DNS query. Because NameCoin uses blockchain technology, you can query the history of the domain name changes through blocks.



Name d/vrubl (vrubl.bit)

Summary

Status	Active
Expires after block	426273 (35932 blocks to go)
Last update	2018-03-21 10:15:25 (block 390273)
Registered since	2017-12-06 16:22:06 (block 373889)

Current value


```
{
    "ip": [
        "210.16.102.127",
        "92.63.197.56"
    ]
}
```


Operations

Date/time	Block	Transaction	Operation	Value
2018-03-21 10:15:25	390273	27d450c6f8...	OP_NAME_UPDATE	{"ip":["210.16.102.127","92.63.197.56"]}
2018-03-18 07:46:06	389838	931351baa2...	OP_NAME_UPDATE	{"ip": ["146.185.241.4","103.212.69.100","103.253.12.18","92.63.197.56","195.110.59.123"]}
2018-03-15 16:16:37	389478	f292779112...	OP_NAME_UPDATE	{"ip":["146.185.241.4","103.212.69.100","103.253.12.18","92.63.197.56"]}
2018-03-15 14:47:01	389472	3dbaff5d4a...	OP_NAME_UPDATE	{"ip":["146.185.241.4","103.212.69.100","103.253.12.18"]}
2018-03-15 06:15:30	389430	1b264215f8...	OP_NAME_UPDATE	{"ip":["146.185.241.4","103.212.69.100","103.212.69.100"]}
2018-03-14 03:57:44	389294	7d264c9a15...	OP_NAME_UPDATE	{"ip":["31.210.172.103","194.67.200.17","95.46.114.14","178.32.173.110"]}
2018-03-13 08:54:47	389188	0a0a784aa4...	OP_NAME_UPDATE	{"ip":["31.210.172.103","194.67.200.17","95.46.114.14","185.241.55.207"]}
2018-03-06 04:02:47	388108	4f07378179...	OP_NAME_UPDATE	{"ip":["142.0.68.13","185.186.78.148","62.112.8.85","103.253.12.18","103.212.69.100"]}
2017-12-11 14:47:32	374672	92c546754d...	OP_NAME_UPDATE	{"ip":["142.0.68.13"]}

Figure 11. Malicious hostname DNS entry changes over time (https://namecha.in/name/d/vrubl)

Windows Defender ATP can provide visibility into the malware's network activities. The following alert process tree shows the malware's .bit domain resolution activity and, after that, the connections to the resolved C&C servers. You can also view other activities from the executable, for example, its connections to other servers using SMTP ports.

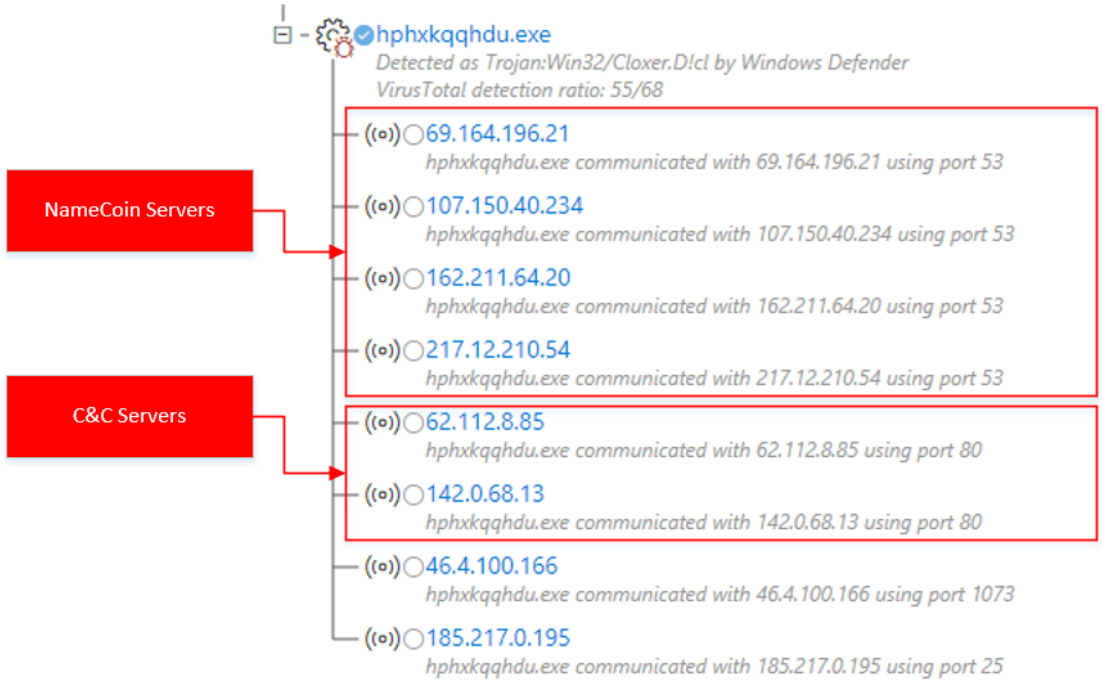


Figure 12. Windows Defender ATP alert process tree showing C&C server connection through NameCoin server name resolution

The Windows Defender ATP advanced hunting feature, which is currently in preview, can be used to hunt down more malware samples that possibly abuse NameCoin servers. For example, the following advanced hunting query finds recent connections to Dofoil C&C servers from your network. This can lead to extra insights on other threats that use the same NameCoin servers.

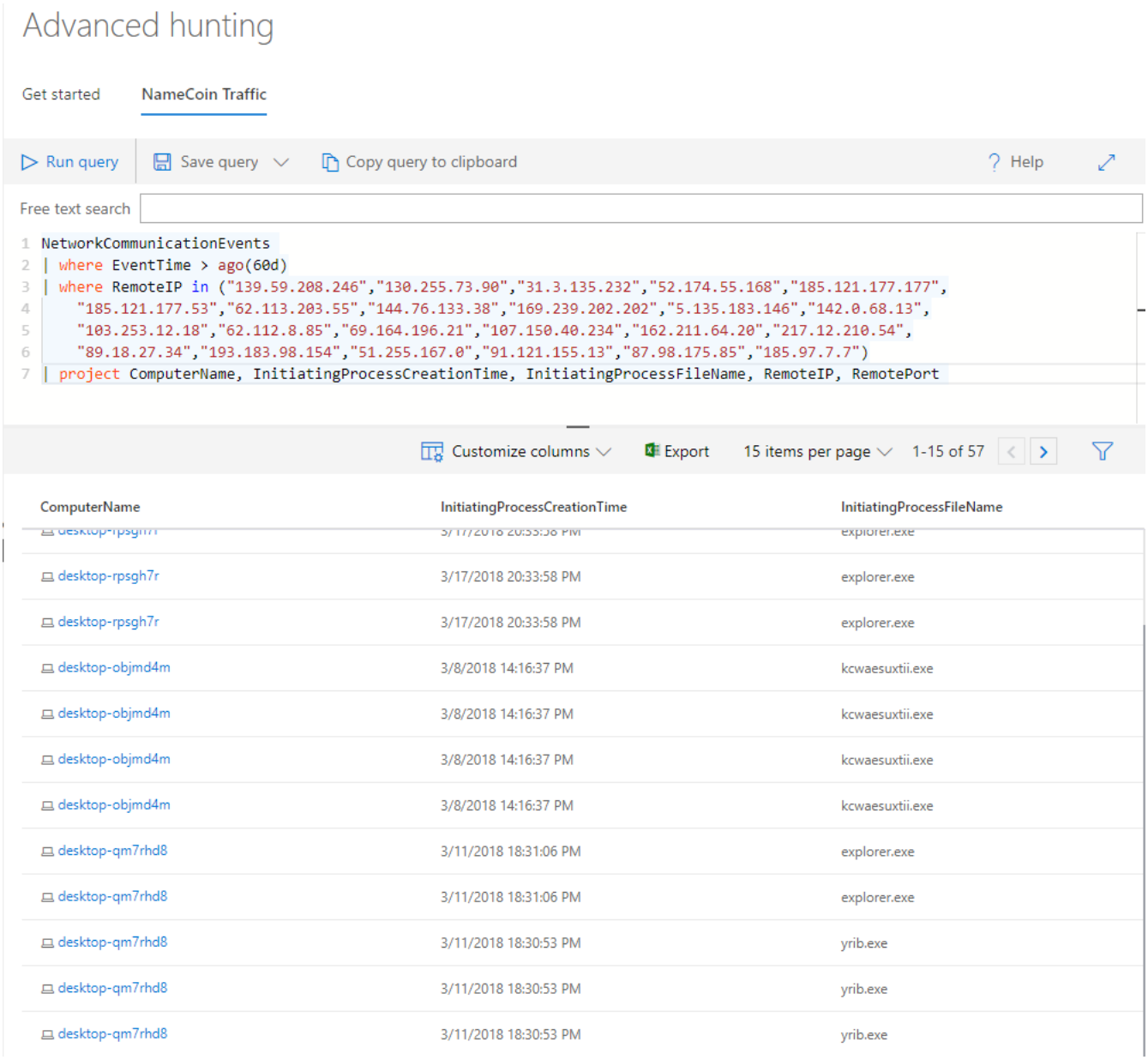


Figure 13. Advanced hunting for other threats using the same NameCoin servers

The purpose of using NameCoin is to prevent easy sinkholing of the domains. Because there are no central authorities on the NameCoin domain name records, it is not possible for the authorities to change the domain record. Also, malware abusing NameCoin servers use massive numbers of NameCoin DNS servers to make full shutdown of those servers very difficult.

Conclusion

Dofoil is a very evasive malware. It has various system environment checks and tests Internet connectivity to make sure it runs on real machines, not in analysis environments or virtual machines. This can make the analysis time-consuming and can mislead malware analysis systems.

In attacks like the Dofoil outbreak, Windows Defender Advanced Threat Protection (Windows Defender ATP) can help network defenders analyze the timeline from the victim machine and get rich information on process execution flow, C&C connections, and process hollowing activities. With the new advanced hunting capabilities in preview, you can run powerful custom queries and pivot freely to different sets of possible targets, malicious

entities, and suspicious activity. Windows Defender ATP can also be used as an analysis platform with fine-tuned visibility into system activities when set up in a lab environment. This can save time and resource during malware investigation.

In addition, Windows Defender Exploit Guard can be useful in finding malicious shellcodes that traverse export address tables. Windows Defender Exploit Guard can be an excellent tool for finding and blocking malware and exploit activities.

Windows Defender Exploit Guard events are surfaced in the Windows Defender ATP portal, which integrates protections from other Microsoft solutions, including Windows Defender AV and Windows Defender Application Guard. This integrated security management experience makes Windows Defender ATP a comprehensive solution for detecting and responding to a wide range of malicious activities across the network.

Windows 10 S, a special configuration of Windows 10, locks down devices against Dofoil and other attacks by working exclusively with apps from the Microsoft Store and using Microsoft Edge as the default browser. This streamlined, Microsoft-verified platform seals common malware entry points.

To test how Windows Defender ATP can help your organization detect, investigate, and respond to advanced attacks, **sign up for a free trial**.

Matt Oh, Stefan Sellmer, Jonathan Bar Or, Mark Wodrich
Windows Defender ATP Research

Indicators of compromise (IoCs)

TrojanDownloader:Win32/Dofoil.AB:

d191ee5b20ec95fe65d6708cbb01a6ce72374b309c9bfb7462206a0c7e039f4d

eaa63f6b500afedcaeb8d5b18a08fd6c7d95695ea7961834b974e2a653a42212

cded7aedca6b54a6d4273153864a25ccad35cba5cafeaec828a6ad5670a5973a

Trojan:Win32/Dofoil.AB:

070243ad7fb4b3c241741e564039c80ca65bfdf15daa4add70d5c5a3ed79cd5c

5f3efdc65551edb0122ab2c40738c48b677b1058f7dfcdb86b05af42a2d8299C

28ce9763a808c4a7509e9bf92d9ca80212a241dfa1aecd82caedf1f101eac692

5d7875abbbf104f665a0ee909c372e1319c5157dfc171e64ac2bc8b71766537f

Trojan:Win32/CoinMiner.D

2b83c69cf32c5f8f43ec2895ec9ac730bf73e1b2f37e44a3cf8ce814fb51f12

C&C URLs:

hxxp://levashov.bit/15022018/

hxxp://vrubl.bit/15022018/

C&C server:

vinik.bit

Related .bit domains (updated in same block as C&C server):

henkel.bit

makron.bit

makronwin.bit

NameCoin servers used by Dofoil:

139.59.208.246

130.255.73.90

31.3.135.232

52.174.55.168

185.121.177.177

185.121.177.53

62.113.203.55

144.76.133.38

169.239.202.202

5.135.183.146

142.0.68.13

103.253.12.18

62.112.8.85

69.164.196.21

107.150.40.234

162.211.64.20

217.12.210.54

89.18.27.34

193.183.98.154

51.255.167.0

91.121.155.13

87.98.175.85

185.97.7.7

Talk to us

Questions, concerns, or insights on this story? Join discussions at the Microsoft community and Windows Defender Security Intelligence.