McAfee
Together is power.

The Hitchhiker guide to Incident Response and Threat Intelligence

Thomas Roccia| Security Researcher
McAfee Advanced Threat Research

γειά σου / Bonjour!

#Whoami

Thomas ROCCIA

Security Researcher, Advanced Threat Research

https://securingtomorrow.mcafee.com/author/thomas-roccia/

@fr0gger_

McAfee

Agenda

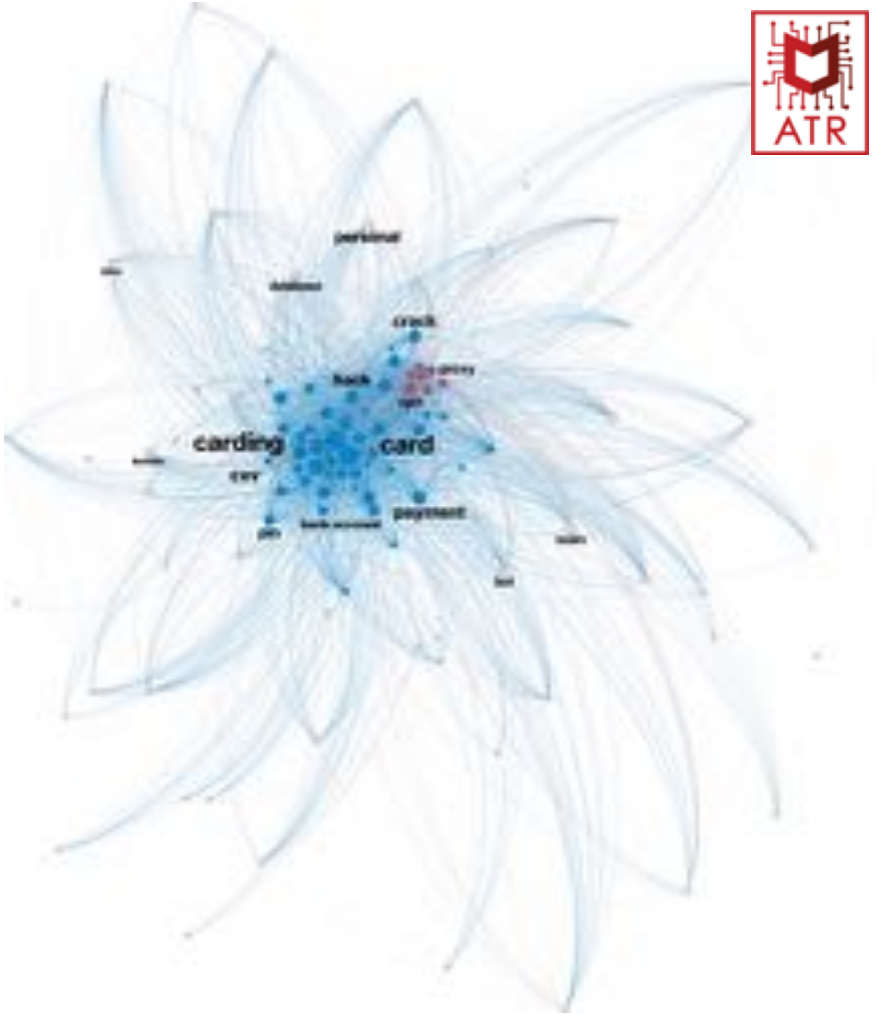
- Introduction
- Incident Response
- Threat Intelligence
- Threat Hunting

279 days

Security Incidents Facts

41,686 security incidents reported in 2018

2,013 of them were data breach



Security Incidents Facts

- Threat Actors Motivations:

Money is one of the most dominant motivation

Espionage is used to steal industrial secrets or is motivated by politic

Within minutes a breach happens, within an hour the data is exfiltrated

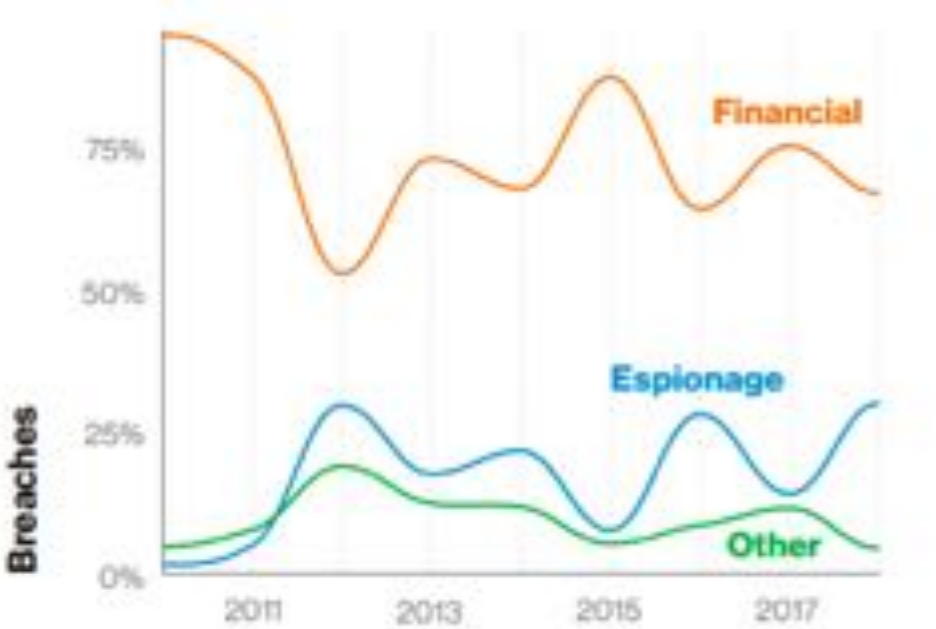


Figure 7. Threat actor motives in breaches over time

Security Incidents Facts

- The average cost of a data breach is $3.9 million
- Attackers are gaining more capabilities over the time
- Attacks are more complex than ever
- Incident Response is a process to contain and understand a breach.
- Threat Intelligence is a process that can leverage and improve your protection capabilities.

What You Will Learn

Skills and Knowledge

- Attack steps
- Incident Response Process
- Threat Intelligence and Threat Hunting
- YARA Hunting

Incident Response

What is a Security Incident?

A security incident is an event that leads to a violation of an organization’s security policies and puts sensitive data at risk of exposure.

These include but are not limited to:

- Attempts (either failed or successful) to gain unauthorized access to a system or its data.
- Unwanted disruption or denial of service.
- The unauthorized use of a system for the processing or storage of data.
- Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.

What is an Incident Response?

Incident response is a term used to describe the process by which an organization handles a data breach or cyberattack, including the way the organization attempts to manage the consequences of the attack or breach (the “incident”).

Ultimately, the goal is to effectively manage the incident so that the damage is limited and both recovery time and costs, as well as collateral damage such as brand reputation, are kept at a minimum.

Why Incident Response is Crucial?

"This is not IF, but WHEN you will be attacked!"

Protect your Business

Protect your Data

Protecting data assets throughout the incident response process includes countless tasks and responsibilities for the IR team.

Protect your Reputation

If a security breach is not properly handled quickly, the company risks losing some or all its customer base. A data breach doesn't instill confidence in your customers.

Protect your Revenue

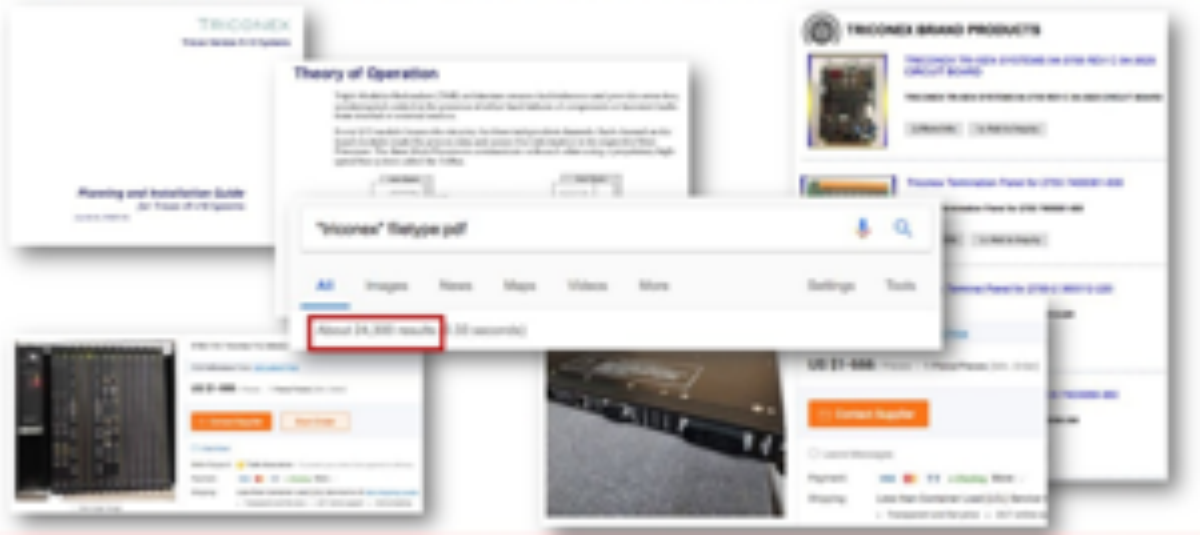
A thorough incident response process safeguards your organization from a potential loss of revenue. .

Attackers Operation: Intrusion Kill Chain

Kill Chain

Stage 1 - Reconnaissance

- Attacker collects information about the targeted organization:
  - Passive Reconnaissance
    - Social Media information
    - Public website
    - Available information
    - Google Dork
    - Whois, DNS…
  - Active Reconnaissance
    - Structure of organisation
    - Scan open ports
    - Security vulnerabilities



Kill Chain

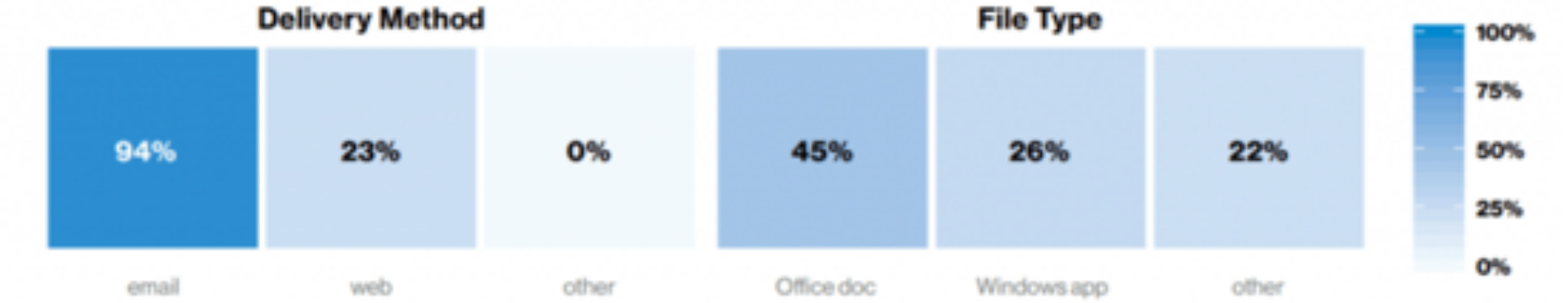
Stage 2 - Weaponization

- Attacker uses information obtained during the Reconnaissance stage to determine how the attack must be performed.
  - Vulnerability Exploitation
  - Selection of the payload

Kill Chain

Stage 3 - Delivery

- Attacker delivers the exploit to the targeted organization.
  - Spam containing malicious attachment or link
  - Waterholing



Kill Chain

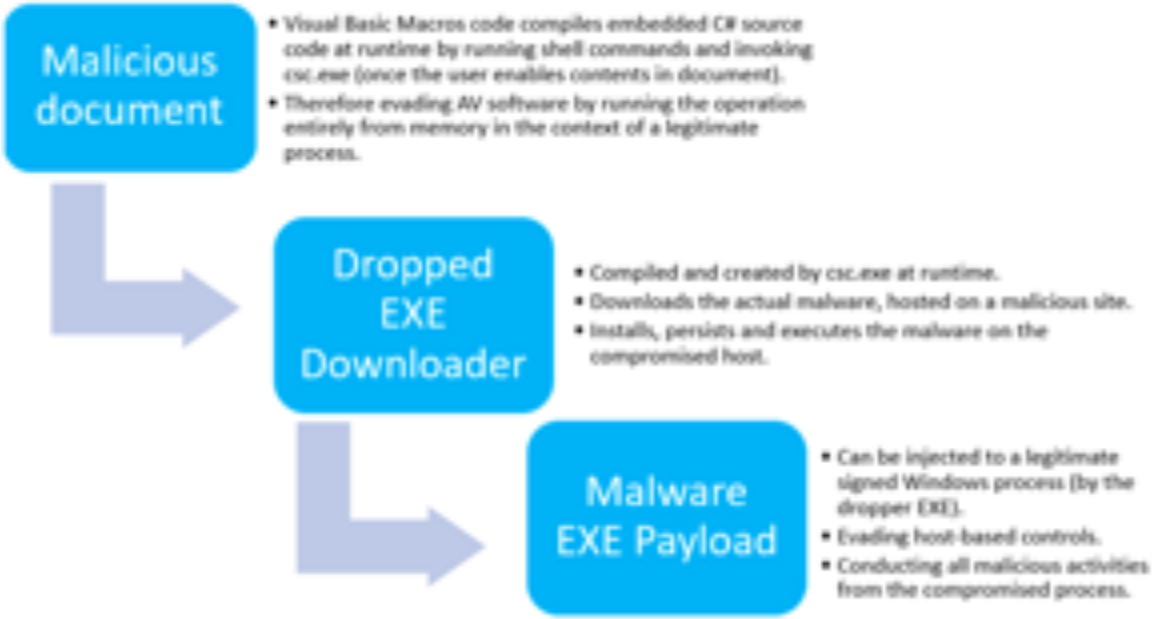
Stage 4 - Exploitation

- At this stage, the exploit takes advantage of the discovered vulnerabilities and delivers the payload.

Kill Chain

Stage 5 - Installation

- At this stage, the payload installs itself, and tries to hide its activity to avoid detection or deletion.

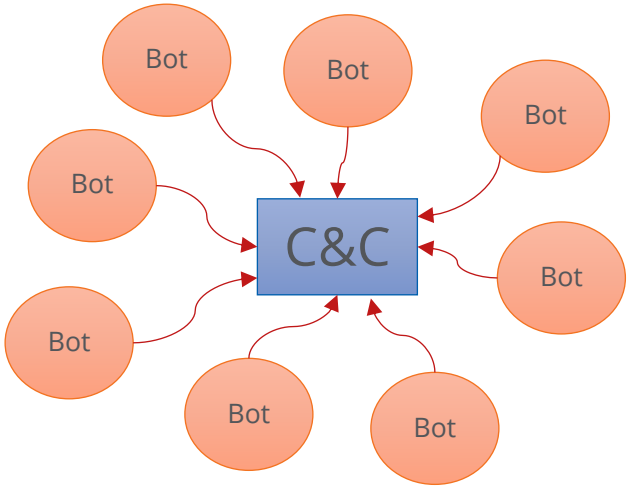


Kill Chain

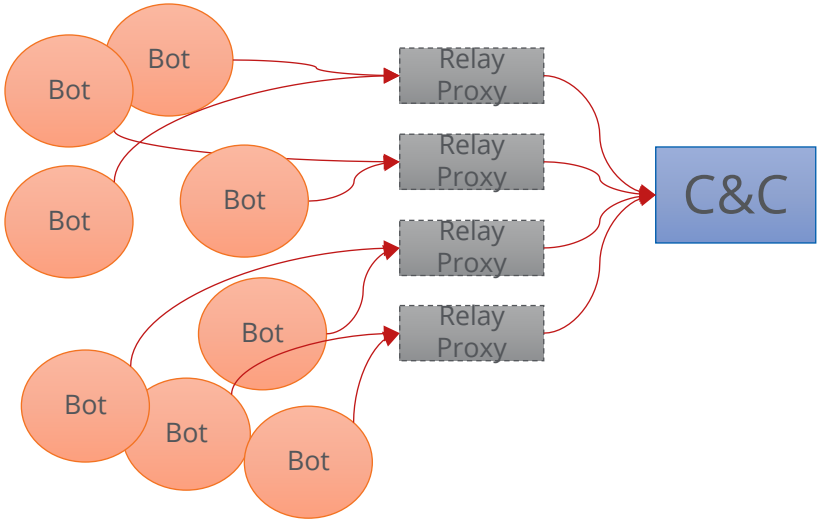
Stage 6 – Command and control

- At this stage, the payload waits for incoming commands from the attacker.

Centralized Architecture



Centralized Distributed Architecture



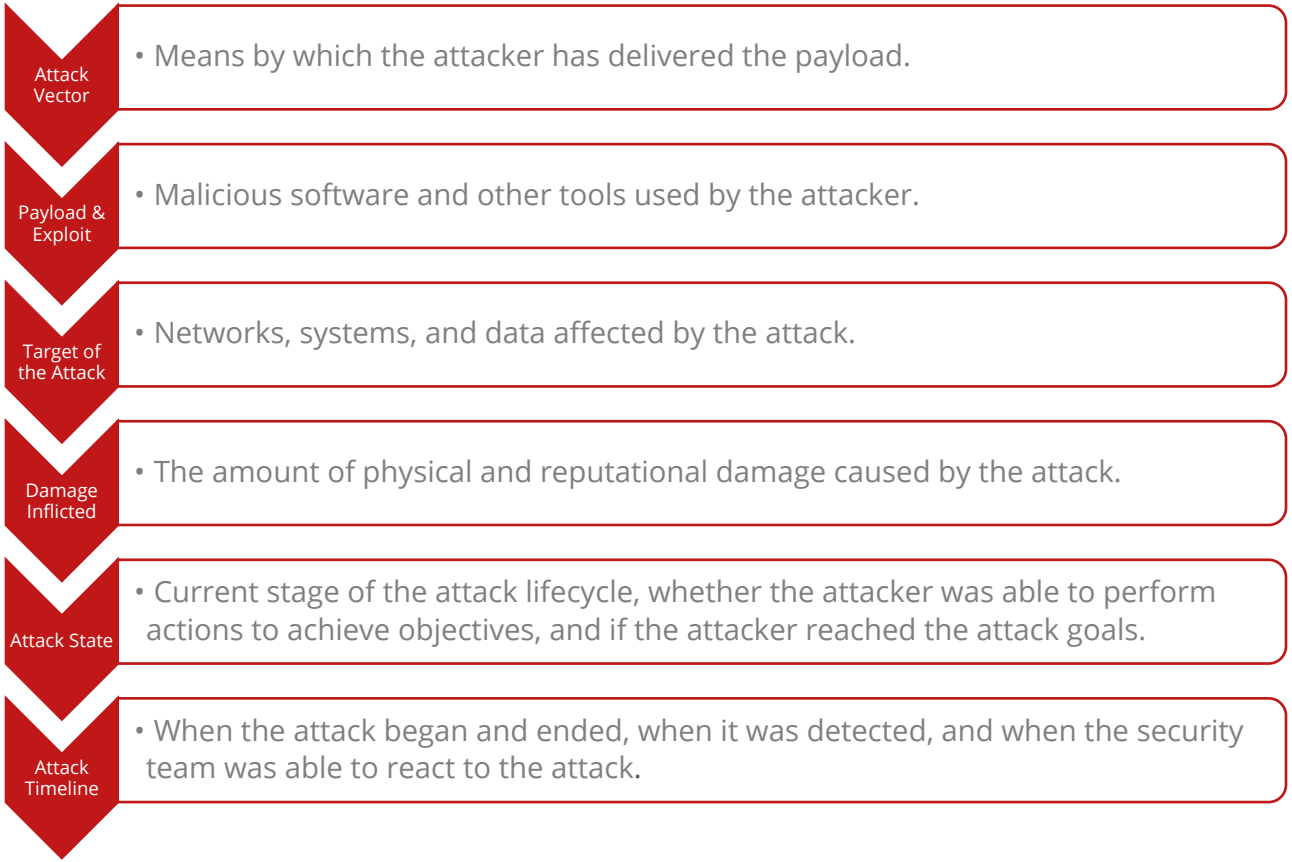
Kill Chain

Stage 7 – Actions on Objective

- At this stage, the attacker uses the payload and other software that was downloaded in the course of the attack to achieve the goals of the attack.

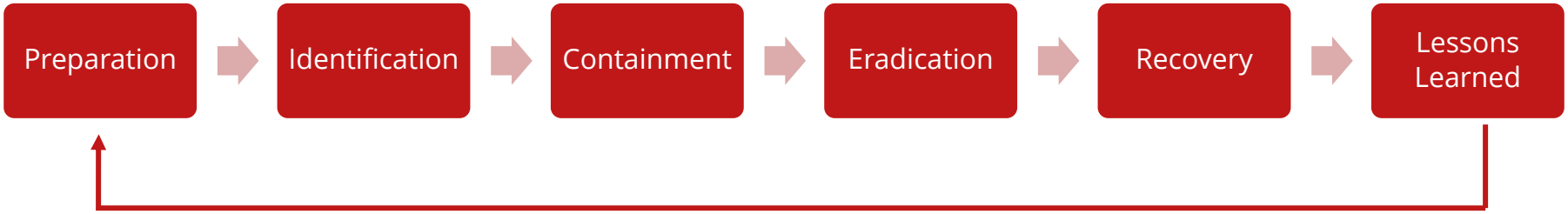
- Once the attacker compromises one of the organization's assets, he or she will try to steal, change, or destroy data available on the compromised asset.

Incident Response Goals



Incident Response Process

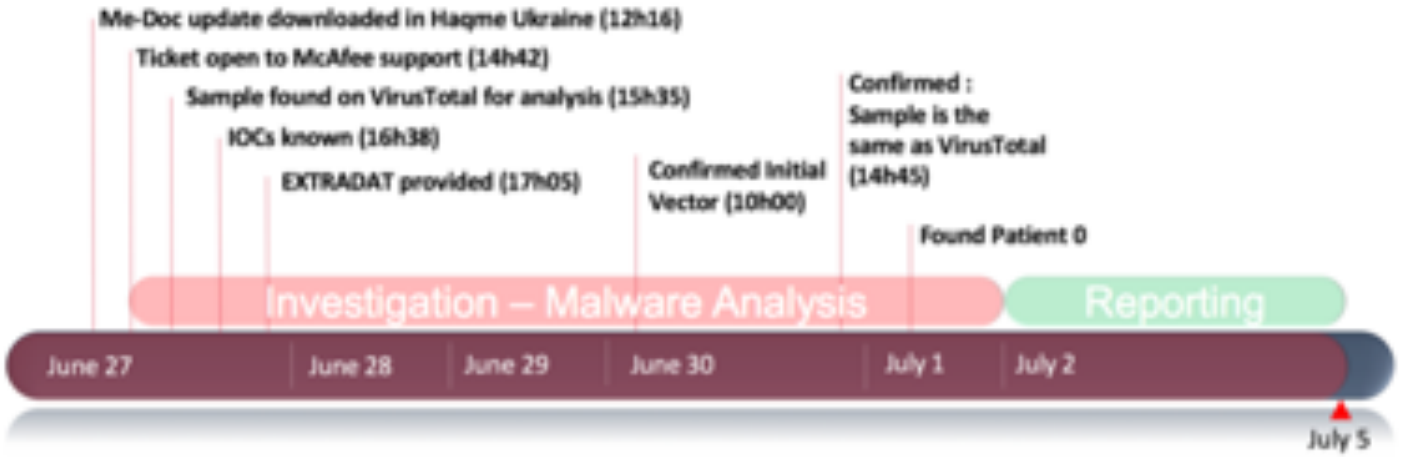
- The process of incident response includes the following phases:



NotPetya

Timeline

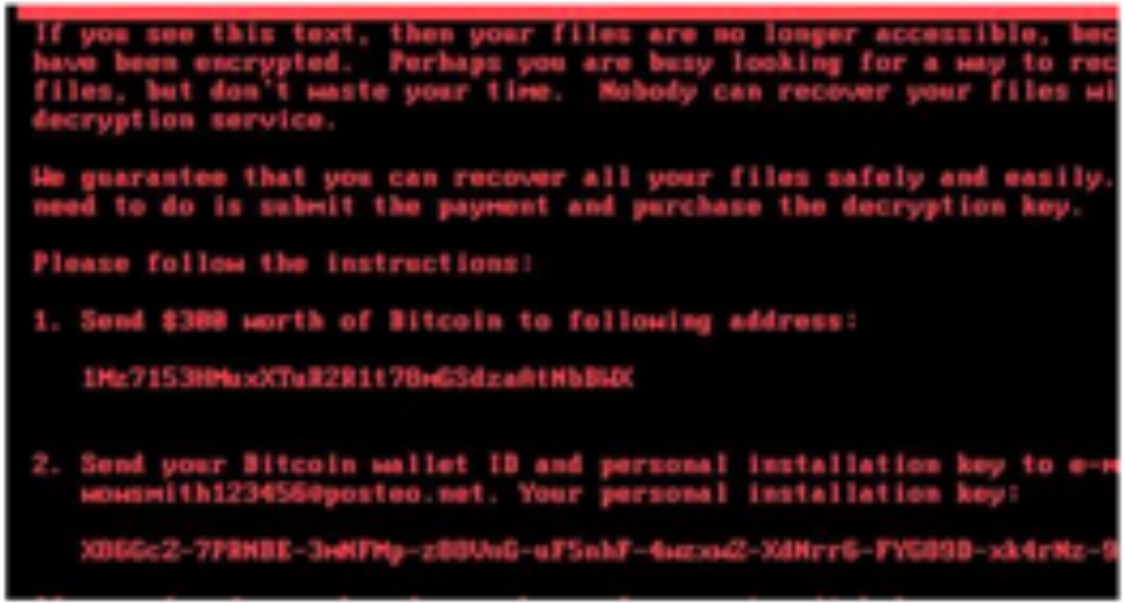
- Incident Response



NotPetya

Identification

- Context collection – First at the incident (tension, pressure…)



NotPetya

Containment

- NotPetya was using propagation mechanisms
  - Eternal Blue
  - Mimikatz
  - Psexec and WMIC
- Discovery of a vaccine
- Shutdown services?

NotPetya

Eradication

- Finding the initial vector of infection Me-Doc
- Starting to rebuild infected machines and servers
- Restoring backup

NotPetya

Recovery

- Monitoring network
- Monitoring server's behavior

NotPetya

Lessons Learned

- What did we learned?
- What were the main points of failure?
- What worked, what didn't?
- What can be improved?

Threat Intelligence

What is Threat Intelligence?

Threat intelligence is knowledge that allows you to prevent or mitigate cyberattacks.

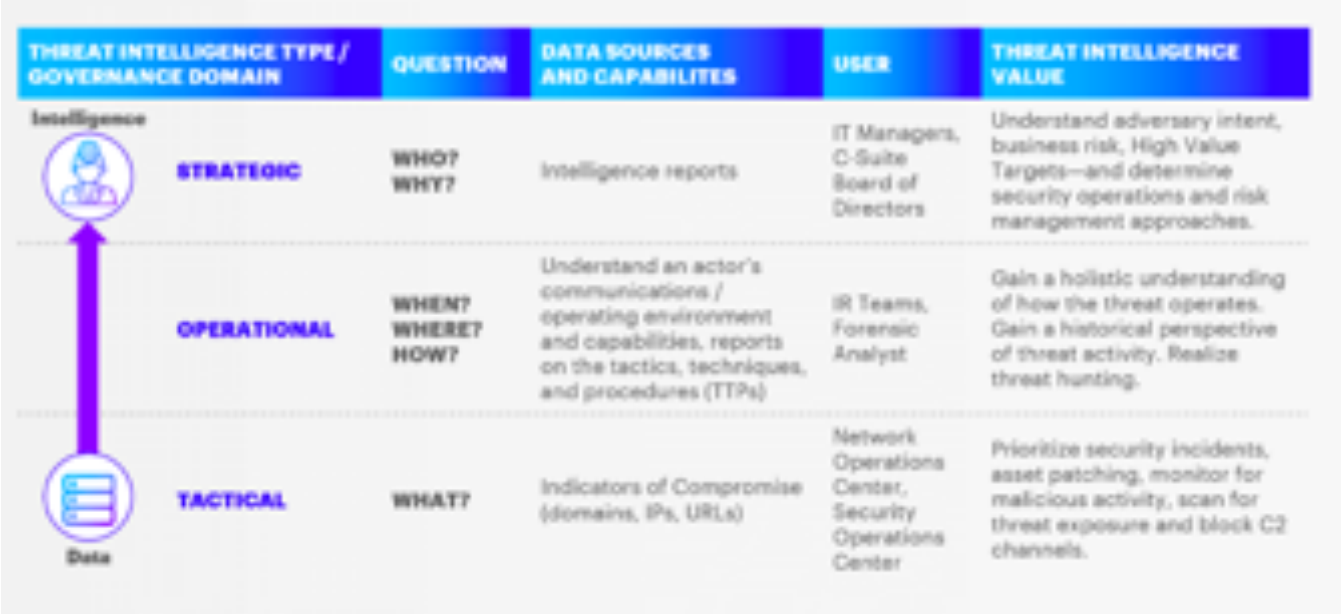
Rooted in data, threat intelligence gives you context that helps you make informed decisions about your security by answering questions like

- who is attacking you?
- what their motivations and capabilities?
- what IOC in your systems to look for?

Threat Intelligence

What is Threat Intelligence?

- This intelligence can be used to inform decisions regarding the subject's response to that menace or hazard.
- Threat intelligence is often broken down into three subcategories:



THREAT INTELLIGENCE TYPE / GOVERNANCE DOMAIN	QUESTION	DATA SOURCES AND CAPABILITIES	USER	THREAT INTELLIGENCE VALUE
STRATEGIC	WHO? WHY?	Intelligence reports	IT Managers, C-Suite Board of Directors	Understand adversary intent, business risk, High Value Targets—and determine security operations and risk management approaches.
OPERATIONAL	WHEN? WHERE? HOW?	Understand an actor's communications / operating environment and capabilities, reports on the tactics, techniques, and procedures (TTPs)	IR Teams, Forensic Analyst	Gain a holistic understanding of how the threat operates. Gain a historical perspective of threat activity. Realize threat hunting.
TACTICAL	WHAT?	Indicators of Compromise (domains, IPs, URLs)	Network Operations Center, Security Operations Center	Prioritize security incidents, asset patching, monitor for malicious activity, scan for threat exposure and block C2 channels.

Threat Intelligence offers a key element of a **mature** Security Operations Center that seeks to move from a reactive to a proactive stance.

IR & CTI

Preparation

Detection & Analysis

Containment, Eradication, Recovery

Post Incident

Direction

Collection

Processing

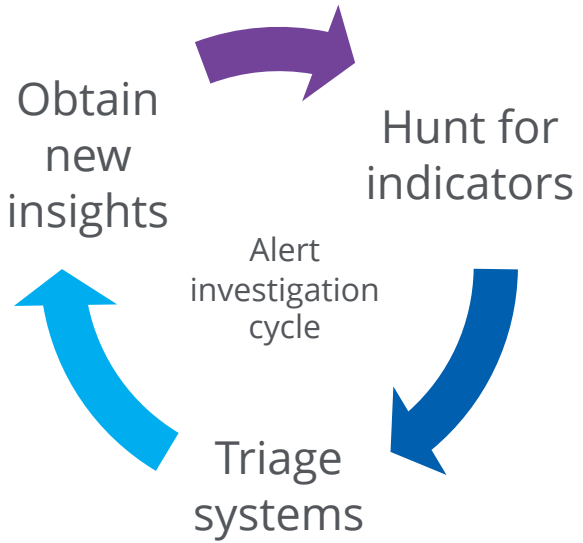
Analysis & Production

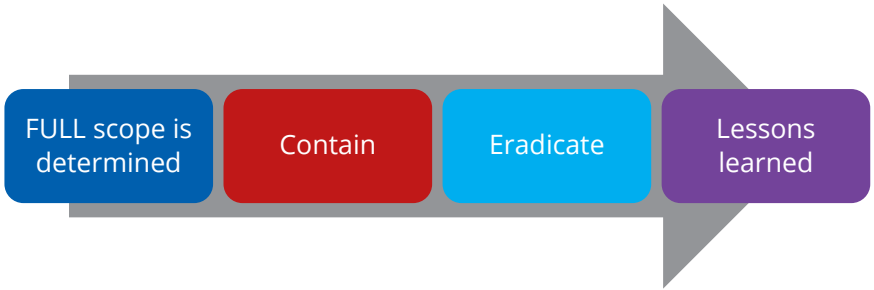
Dissemination

Feedback

Hunting & smart **incident response**

And why you shouldn't hunt on a Friday





http://blog.ismaelvalenzuela.com/2018/10/11/intelligence-driven-defense-successfully-embedding-cyber-threat-intel-in-security-operations/

Key findings from McAfee Threat Hunting Survey

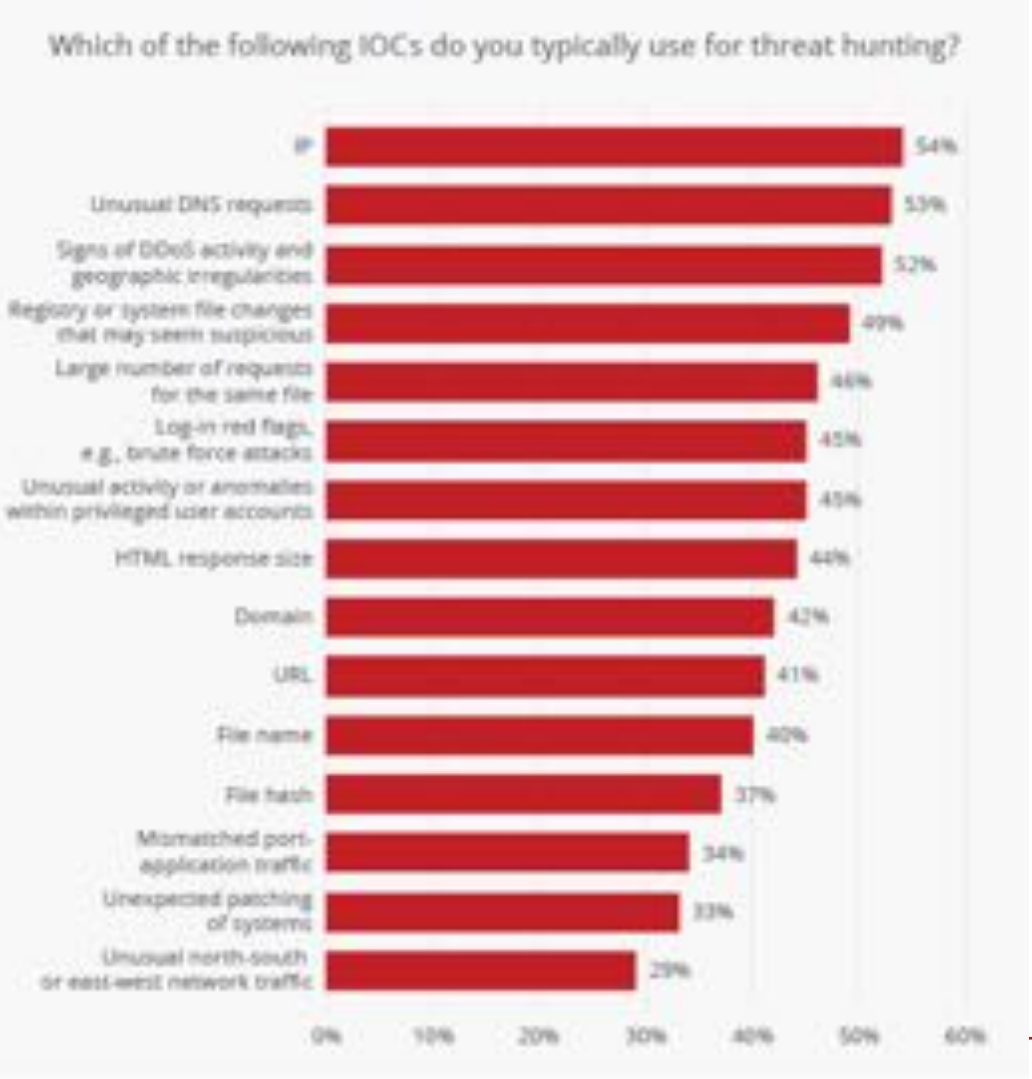
Indicators of compromise typically used by threat hunters

Use of activity logs

Log type	Percent of respondents
Firewall/IPS-denied traffic	76%
DNS	69%
Proxy	60%
Web and email filter	59%
Server	59%
Windows events (domain)	57%
Packet inspection (sniff)	45%

Figure 14: The most common logs used for threat hunting

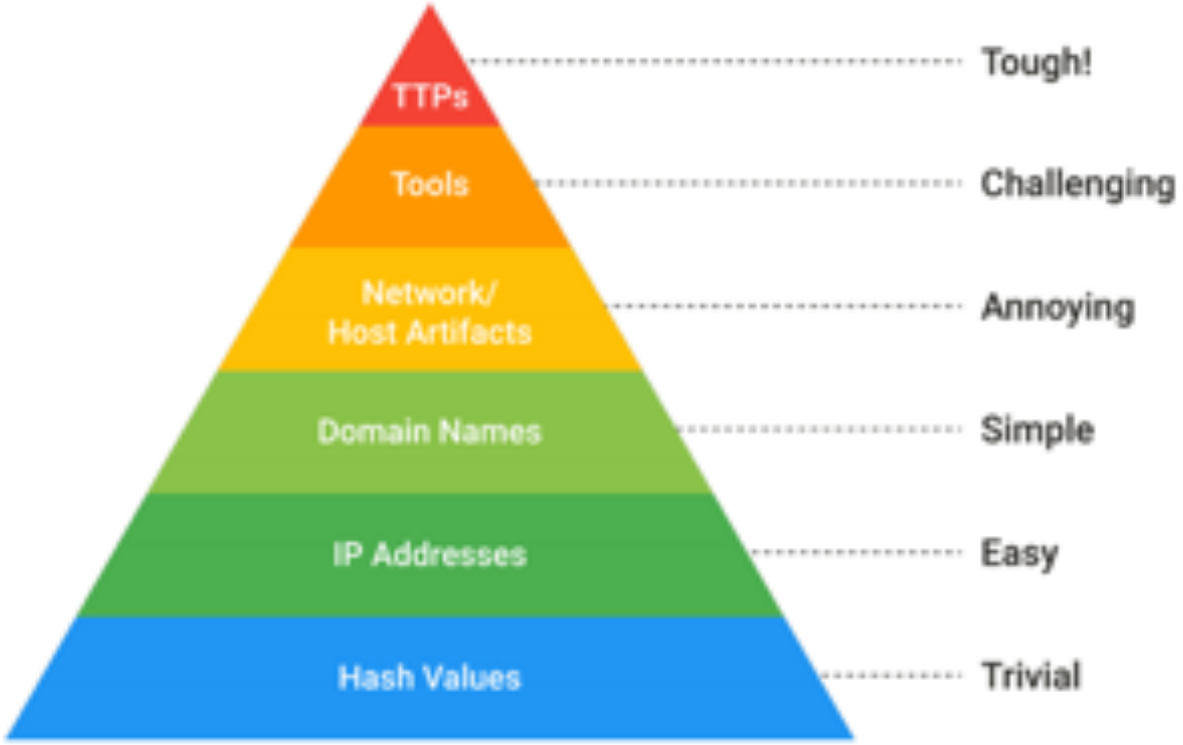
Source: McAfee Threat Hunting Survey, May 2017



Source: McAfee Threat Hunting Survey 2017

Threat Intelligence

The Pyramid of Pain / Indicators Value



Source: http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

Know the enemy

- We are not fighting binaries, but attackers with strong motivation
- Attackers can change IOCs very quickly, the fact someone has seen it doesn't mean you'll see it
- Essential to chose the right **hypothesis** and the right **questions** to gather context and think critically

Tactics, Techniques and Procedure

TTP is a military term describing the operations of enemy forces.

In InfoSec TTP is an approach for profiling and contextualizing cyberattack operations.

Tactics describes how an attacker operates during his operation.
(Infrastructure reused, amount of entry point, compromised targets...)

Techniques describes the approach used to facilitate the tactical phase.
(Tools used, malware, phishing attacks....)

Procedures describes a special sequence of actions used by attackers to execute each step of their attack cycle.

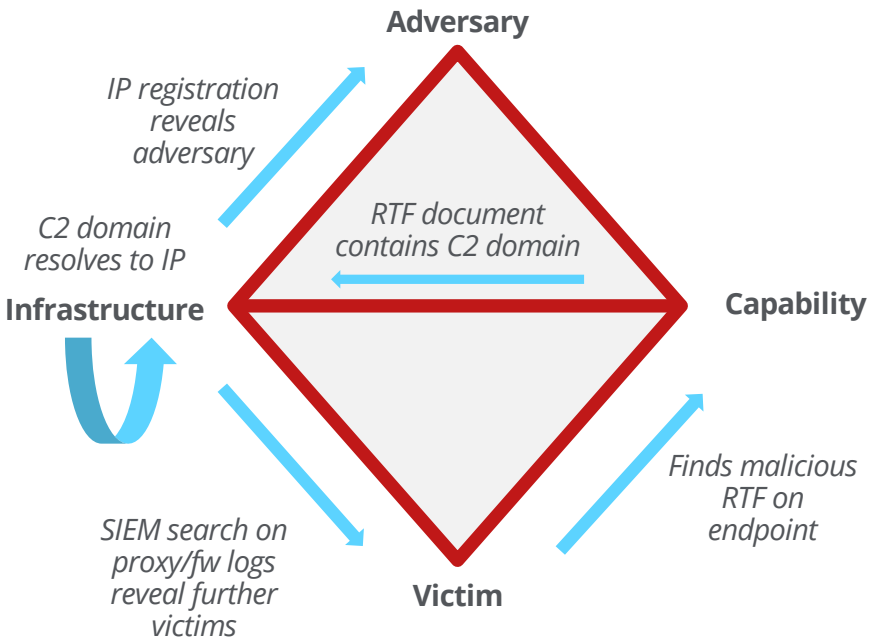
Diamond Model of Intrusion Analysis

Different approaches for analytical pivoting

Focus on the adversary tactics, techniques, procedures (TTPs) and motivations.

Leverages threat intelligence to determine adversary's infrastructure and capabilities to hunt for attacker's IOCs & IOAs.

Adversary-centered



Victim-centered

Investigation starts when evidence of an attack is found on the victim's network.

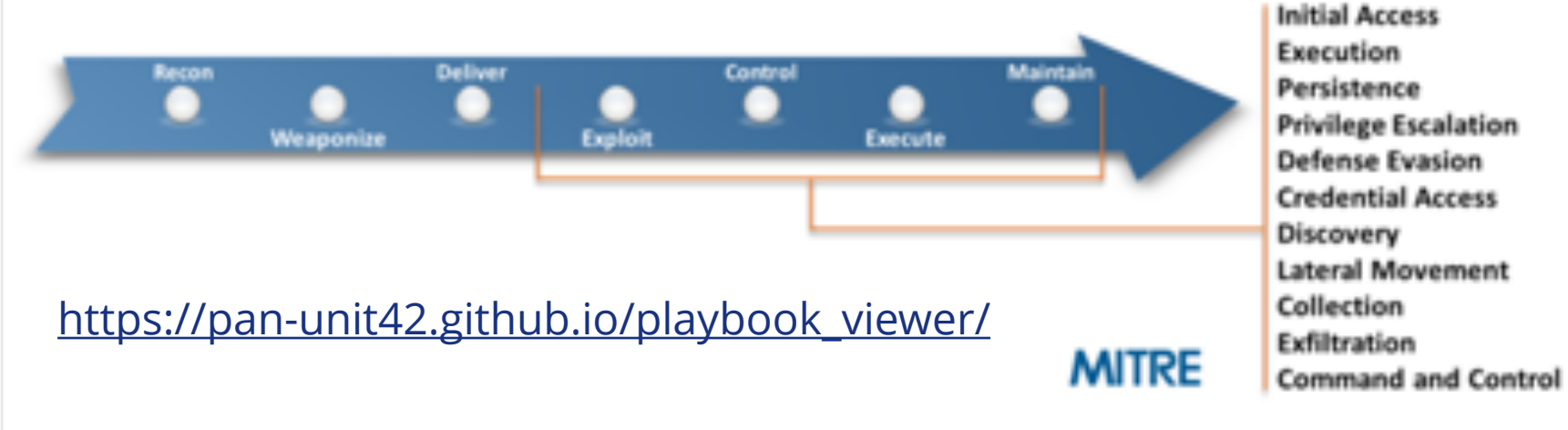
Analyst **inspects victim artifacts**, typically on an endpoint, to reveal the other components of the diamond

The MITRE ATT&CK model and tactics categories

https://attack.mitre.org/wiki/Main_Page

- The MITRE Att&ck Matrix is a table that groups and organizes post-exploitation tactics & techniques

- MITRE Att&ck Matrix testing is ONLY Visibility, NOT protection, performance nor usability.



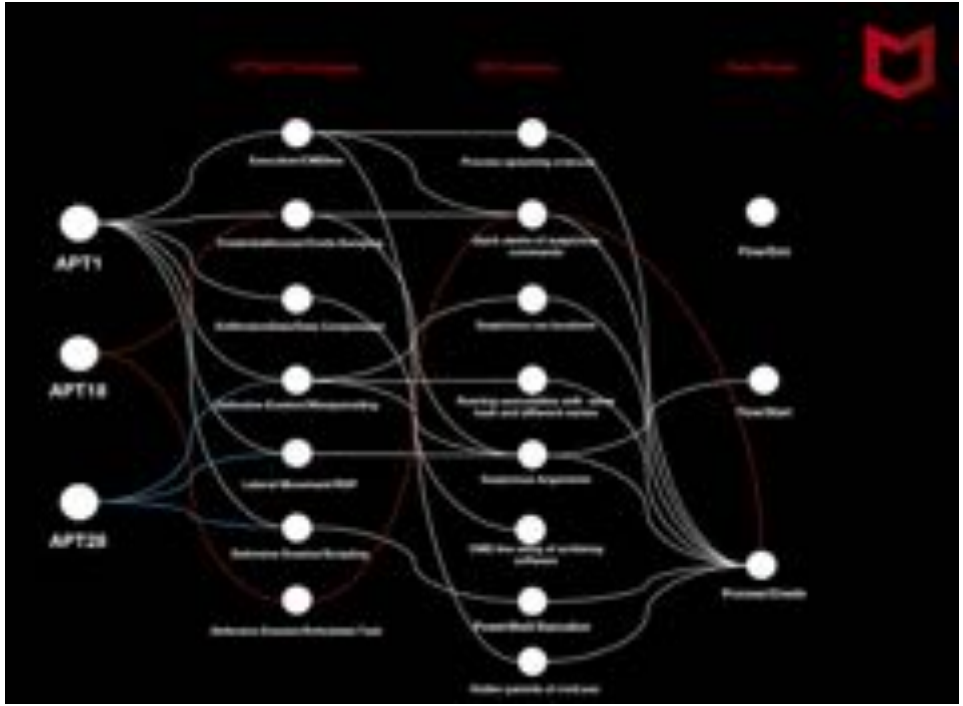
https://pan-unit42.github.io/playbook_viewer/

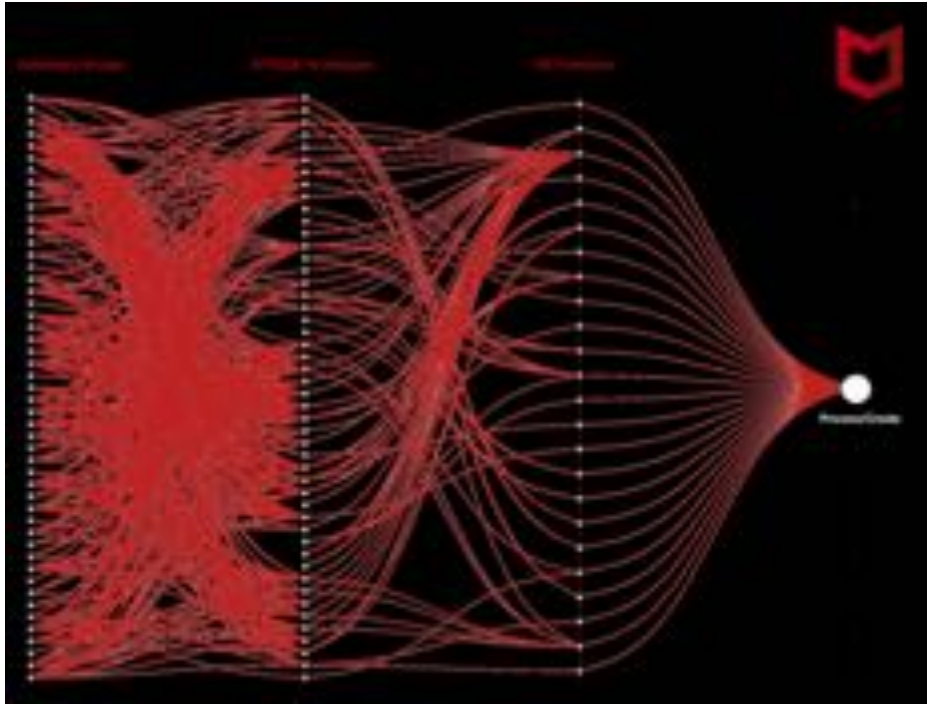
How to apply the model?

MITRE ATT&CK

- RISK/GAP Analysis
  - The model can be used to determine which techniques can be observed by which technology and where there might be risk since some gaps exist in detecting possible attack scenarios. Keywords are visibility and risk mitigation.
- RED Teaming
  - To determine the risk/gap analysis, often companies have a red-team in place that will conduct actor role playing. With the knowledge and skills of adversaries and known tools/techniques and procedures used in historical events, the team will execute these scenarios against the organization.
- SOC Assessment
  - At the same time as the red-teaming exercise is executed, the soc-team will be tested on maturity. Will the attacks being detected, which products would give me the visibility, what is the story these discovered techniques are telling me and what if we missed events?
- Threat Hunting

Connecting the dots





Recap

- Incident Response allows to limit the damage of a Security Incident
- Threat Intelligence allows to be proactive in threat research to protect the network and system.
- Incident Response and Threat Intelligence are complementary

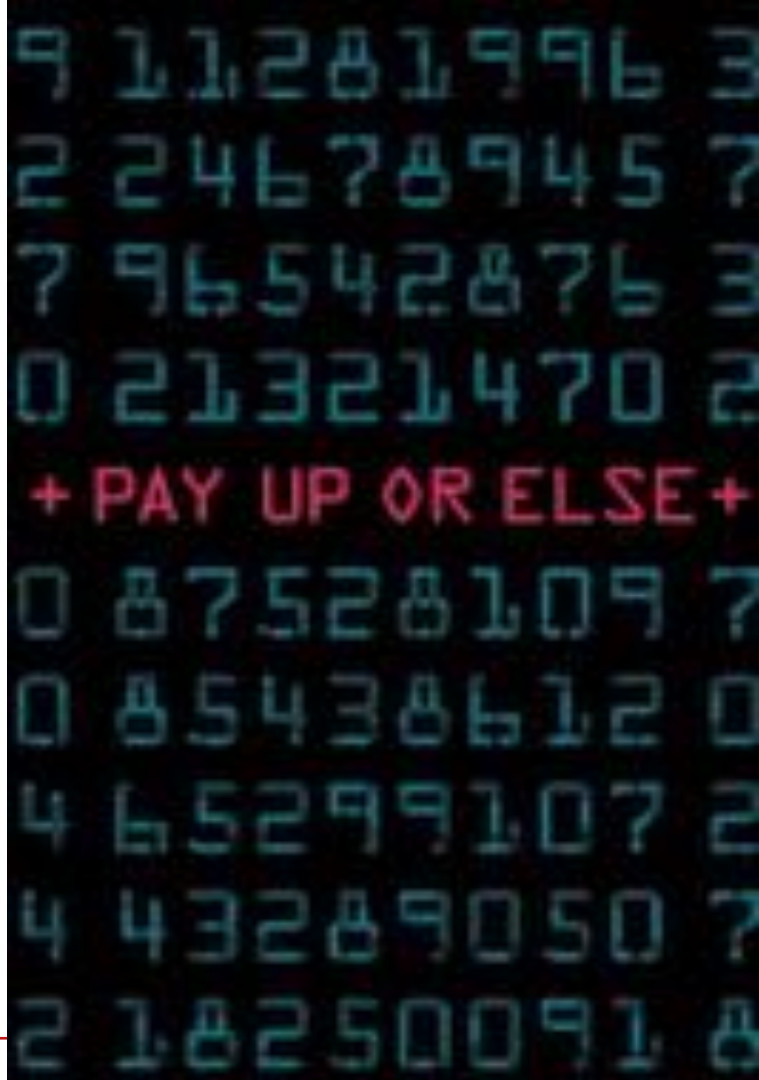
Law Enforcement Collaboration

Law enforcement engagement can help reduce incident response times

Case study: Data theft from a Billion dollar International company. The company is being extorted with the disclosure of sensitive data.

- CISO'S QUESTIONS
  - How did they get in?
  - What data is gone? Were did it go?
  - If we pay, will it stop?

- Actions by Law Enforcement
  - Seizing infrastructure involved
  - Preserving valuable data
  - Established what was stolen and provided Strategic Intel.



Law Enforcement as an offensive counter measure

Internet service provider under DDoS Attack

Aug 2015 the biggest cable company in the Netherlands was attacked, resulting in an internet outage for 2,5 million customers.

- Actors claiming to be Anonymous extorted the company
- Security team of Liberty Global did a emergency migration of infrastructure and system hardening
- International media attention
- Law enforcement served an deterrence and public reassurance.
- First arrests with in a week, in 1 month time the rest of the group.

Olympic Destroyer

Deletes all the Shadow Copies

Deletes the backups catalog

No repair possible from recovery console

Deletes System and Security event logs

```
call    ds:AdjustTokenPrivileges
push    offset aDeleteShadowsA ; "delete shadows /all /quiet"
mov     ebx, offset aCWindowsSystem ; "c:\\Windows\\system32\\vssadmin.exe"
call    Invoke_CMD
mov     ebx, offset aWbadminExe ; "wbadmin.exe"
mov     dword ptr [esp+30h+var_30], offset aDeleteCatalogQ ; "delete catalog -quiet"
call    Invoke_CMD
mov     ebx, offset aBcdeditExe ; "bcdedit.exe"
mov     dword ptr [esp+30h+var_30], offset aSetDefaultBoot ; "/set {default} bootstatuspolicy ignoreallfailures &"
                                ; "bcdedit /set {default} recoveryenabled no',0"
call    Invoke_CMD
mov     ebx, offset aWevtutilExe ; "wevtutil.exe"
mov     dword ptr [esp+30h+var_30], offset aClSystem ; "cl System"
call    Invoke_CMD
mov     dword ptr [esp+30h+var_30], offset aClSecurity ; "cl Security"
call    Invoke_CMD
```

SERVICE_DISABLED 0x00000004	A service that cannot be started. Attempts to start the service result in the error code ERROR_SERVICE_DISABLED.

```
lea     ecx, [ebp+dwBytes]
push    ecx             ; pcbBytesNeeded
push    esi             ; cbBufSize
push    esi             ; lpServiceConfig
push    eax             ; hService
mov     [ebp+dwBytes], esi
call    ebx ; QueryServiceConfigW
push    [ebp+dwBytes]   ; dwBytes
push    8               ; dwFlags
call    edi ; GetProcessHeap
push    eax             ; hHeap
call    ds:HeapAlloc
push    esi             ; lpDisplayName
push    esi             ; lpPassword
push    esi             ; lpServiceStartName
push    esi             ; lpDependencies
push    esi             ; lpdwTagId
push    esi             ; lpLoadOrderGroup
push    esi             ; lpBinaryPathName
push    0FFFFFFFFh      ; dwErrorControl
push    4               ; dwStartType
push    0FFFFFFFFh      ; dwServiceType
push    [ebp+hService]  ; hService
mov     [ebp+lpServiceConfig], eax
call    ds:ChangeServiceConfigW
lea     eax, [ebp+dwBytes]
push    eax             ; pcbBytesNeeded
push    [ebp+dwBytes]   ; cbBufSize
push    [ebp+lpServiceConfig] ; lpServiceConfig
push    [ebp+hService]  ; hService
call    ebx ; QueryServiceConfigW
test    eax, eax
jz      short loc_4013F5
```

Olympic Destroyer – ATT&CK Matrix

Persistence	Privilege escalation	Defensive Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	C2
Modify Existing Service	Valid Accounts	Indicator Removal on host	Credential Dumping	Account Discovery	Remote File Copy	Command-line interface	Data from local system		
Valid Accounts		Modify Registry	Credentials in Files	Process Discovery		RunDLL32			
		Valid Accounts		Query Registry		Scripting			
				Remote System Discovery		WMI			
				System Owner/User Discovery					
				System Service Discovery					
				System Time Discovery					

“Security is more powerful when Private sector and Law Enforcement are working together”

Might even apply to hunting pirates ;-)

Hunting Like a Sir

Agenda

- How to Hunt?
- What is YARA?
- Basic Rules
- Managing Dataset
- How to build a string and code rule
- VTHunting

What is Threat Hunting?

Threat hunting is the process of proactively looking for new threats and studying threat actors behaviors and methods.

How to Hunt?

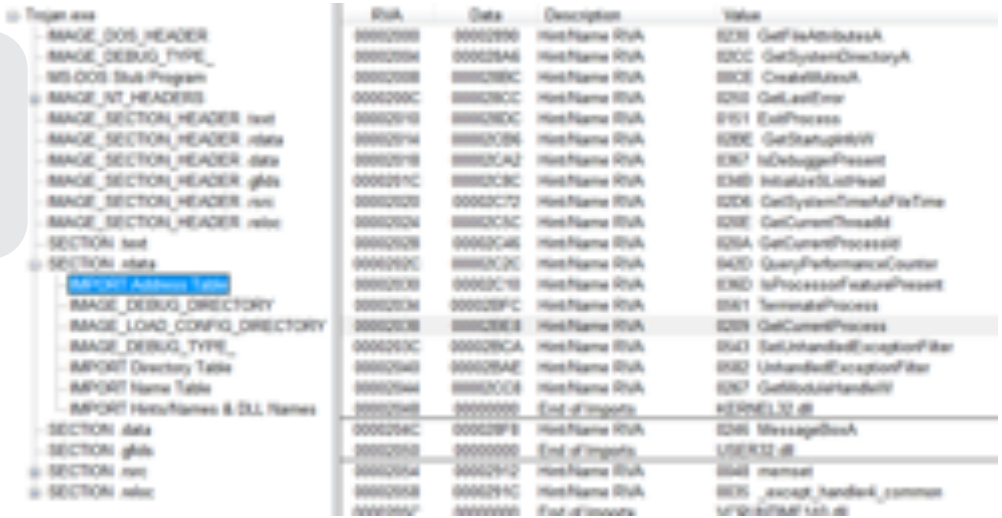
Examples

- Malware
  - IMPhash
  - Certificate
  - Unique Mutex names
  - RichPE header
  - Unique strings
  - PDB path
  - Code similarity of blocks of code…
- Domain/IP:
  - Seen before in campaigns?
  - Who registered it / owns it
  - Is name equal to victim related registered domains
  - What code is present on the domain…

ImpHash

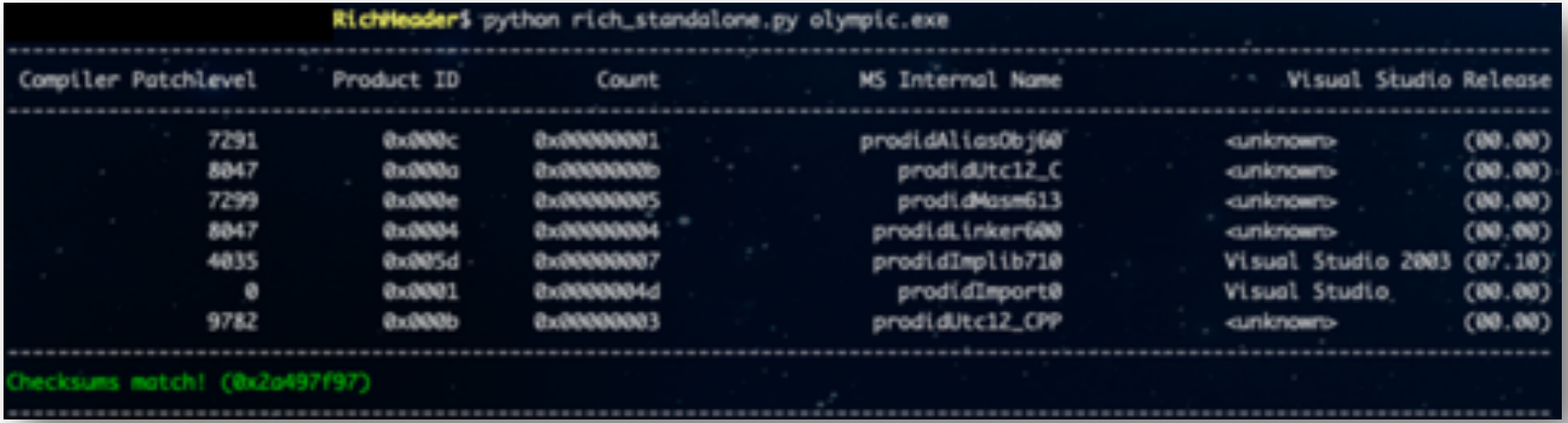
- ImpHash is a fingerprint of PE Import Address Table

```
import pefile
file = pefile.PE('tasksche.exe')
file.get_imphash()
 '68f013d7437aa653a8a98a05807afeb1'
```



Rich PE Hash

- Rich PE hash is a fingerprint of the Rich Pe Header.



SSdeep

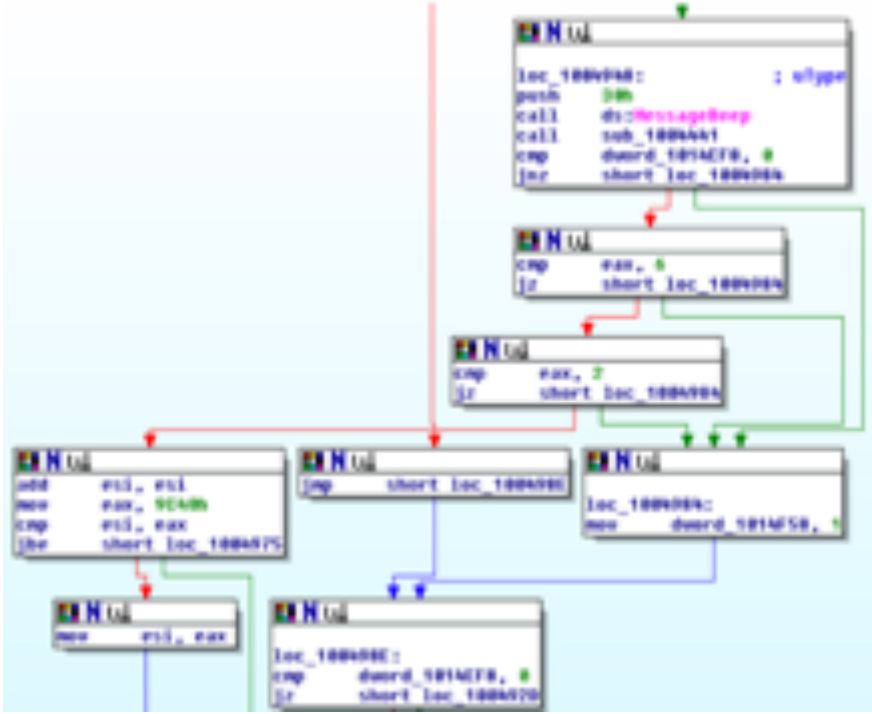
- Ssdeep is used to find the similarity between 2 samples.
- 2 samples with 2 different hashes may have a similar Ssdeep.

```
Ssdeep gandcrab-44f8fc3bdc8b4cc530808baf9eaf923e613c2b975630b6eff18a1609d6062a49
       gandcrab-c78c033b5d2dd2c89fd6b91773c425040bca886198ced0b6f1d62ef090dd4be0

3072:lRPI6YetSOYyM1PUVDAWpcB3/Az/O9xn6Ln+q7E/kfTOQ5N:lRNYmSlPdOO3/Y/Wyh7B7OQn,"gandcra
b-44f8fc3bdc8b4cc530808baf9eaf923e613c2b975630b6eff18a1609d6062a49"

3072:rRPI6YetSOYyM1PUVDAWpcB3/Az/O9xn6Ln+q7E/kfTOQ5N:rRNYmSlPdOO3/Y/Wyh7B7OQn,"gandcra
b-c78c033b5d2dd2c89fd6b91773c425040bca886198ced0b6f1d62ef090dd4be0"
```

Machoke Hash

- Machoke hash is based on Control Flow Graph hashing.
- It allows to find similar samples with shared code.

```
gandcrab-
44f8fc3bdc8b4cc530808baf9eaf923e613c2b975630b6eff18a1609d6062a49
Machoc Hash:
4c9f9a3bffc59c2930cfcd35a9bfb1062723a7897c91cb3a1a02300ef33a8b1e
1ae1c305b619b77f0906d68c4d3411e3db8a17a3db8a17a3db8a17a836a726b6
f55aefbd0cc9b34462042163db8a17a3db8a17a3db8a17a3db8a17aaac7593c2
53a6128142959477b78ead70b85aa1840d939b939f2a55c645d5605042556e77
b8201e25f3dec2dfa3a4f1a02300e7c91cb3a3b1cbce0b64559e73db8a17a3db
8a17a624bf342b619b773db8a17a3db8a17ae172a93c1a02300e1a02300e1a02
300e61f47511a02300e521d408bab698f6a86e1857eccab38bb1a02300eb30e0
0271a02300e6b473a5a3db8a17adf3847e31a02300ea1e9b3ee1a02300efe9aa
debc19ce261a02300e1a02300e1a02300ebe71a1953db8a17a6249a7c13db8a1
7a1a02300ec4d3411e221e19599a97c6a73db8a17a3db8a17ae11fd9295713ec
027316d7466d9e40c31a2a588a9eb0256ca0ed2787466bb5e11fd929588a9033
47b3348256dffc8a47d6aa353db8a17a6d8878fd8344fc1a948df206bc2fe749
3db8a17a99bafa1cc0db65c3fff00ed23db8a17ac19ce26711f8adfe2e0de51e
2e0de512eee4cd8202f79708ffb7da2cfbc7c3e33b1193faa17a723db8a17a21
3e233a1a02300e3db8a17a3db8a17a3db8a17a7221130e3adfbf76c754b63a27
23a789ecf7077657c44fab6233966457c44fabbf90a3c8a5db61a3476d9547a7
fa370bd9595a1b719c2734f396fe0f1a02300e1a02300e1a02300e4f28d1051a
02300e
```



https://blog.conixsecurity.fr/machoke-hashing/

Radiff2


```
radiff2 true false

radiff2 -s /bin/true /bin/false

radiff2 -c genuine cracked

radiff2 -C /bin/false /bin/true

radiff2 -g main /bin/true /bin/false | xdot -
```

SuperPEHasher Library

```
python pehasher.py gandcrab-44f8fc3bdc8b4cc530808baf9eaf923e613c2b975630b6eff18a1609d6062a49
md5:            c55e1055d809e4d79a1894b2a1cc2792
sha1:           f3eba35b2fbcf1bae975a18c9daf7044c32f982e
sha256:         44f8fc3bdc8b4cc530808baf9eaf923e613c2b975630b6eff18a1609d6062a49
sha512:
2b1c4788450f976e66cc25eb34a76593d8a7bc8682f381891f079153a9c39aad98ff1f66667dce71882976f4196761dcb
a55a01f694016b988939107c2e54061
ssdeep:         3072:lRPI6YetSOYyM1PUVDAWpcB3/Az/O9xn6Ln+q7E/kfTOQ5N:lRNYmSlPdOO3/Y/Wyh7B7OQn
ImpHash:        44698852dc2c3447fc5207d6d6a42d0a
ImpFuzzy:       48:9fGl5vkBnvsftXQK9WE/1/QXZ11E+txkSEUCKECBeg8mG:dGl50nvAtXQQWawTumG
RicHash xored:  3de6156bf478daec428ed80570b4b00c4cfe5df7ac883def8f5a0bdb33ab7215
RicHash clear:  9f9a30b48b7efa76789d9368477ce1379912d45b0e625981ab74554a761f4f59
MinHash:        -1740250892
PeHash:         dfbaa25093d46503cc17ddf7fa751f7792c6c2fa
Machoc Hash:
4c9f9a3bffc59c2930cfcd35a9bfb1062723a7897c91cb3a1a02300ef33a8b1e1ae1c305b619b77f0906d68c4d3411e3d
[Truncated] 7077657c44fab6233966457c44fabbf90a3c8a5db61a3476d9547a7f
```

What Is Yara?

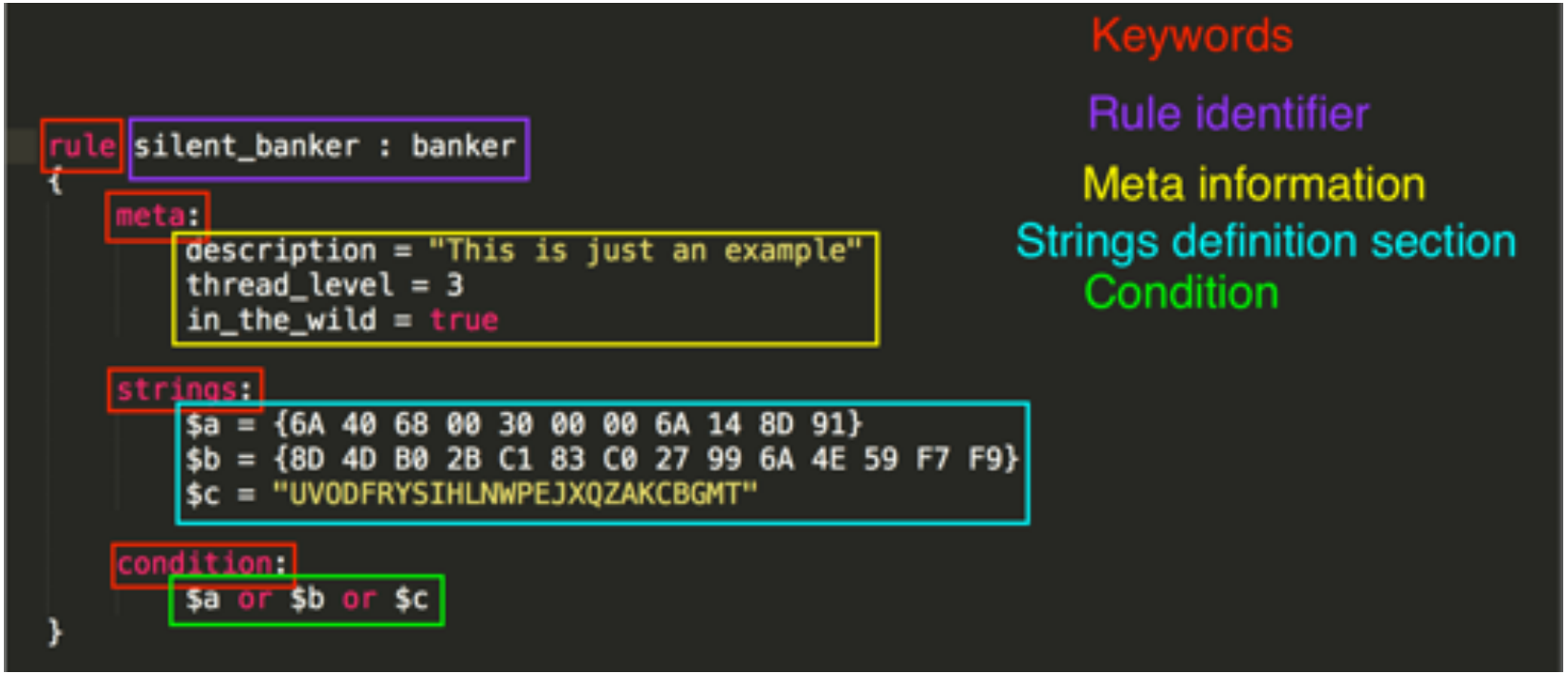
- YARA is a tool aimed at (but not limited to) helping malware researchers to identify and classify malware samples.

- With YARA you can create descriptions of malware families (or whatever you want to describe) based on textual or binary patterns.

https://virustotal.github.io/yara/

Writing YARA Rules

Example



Yara Modules

PE Module

```
import "pe"
rule Is_DLL
    {
        condition:
            pe.characteristics & pe.DLL
     }
```

Hash Module

```
import "hash
rule simple_hash_rule
   {
       condition:
            hash.md5(0, filesize) == "7c3d183ed1f9008eea7ba5d8a8fd21d7"
}
```

Hunting with ImpHash


```
import "pe"
rule Check_imphash
    {
        condition:
            pe.imphash == "44698852dc2c3447fc5207d6d6a42d0a"
     }
```

Hunting with RichHash


```
rule sodin_richhash {
  meta:
      description = "Rule to detect sodinokibi with Rich PE Hash"
  condition:
      hash.sha256(pe.rich_signature.clear_data) ==
"ceb177d473a8c58fac3282d8ffdec81a58c602d14b5b936dc7124f4b51bfeb49"
}
```

Data source

- Virus Total
- Virusbay
- Malpedia
- Open source data

Yara Rule process creation

Analysis similar binaries

Identify unique patterns strings, code…

Build the rule with your findings

Test on a cleaned dataset

Deploy to the service of choice and wait

Monitor Everything

https://www.youtube.com/watch?v=XMZ-c2Zwzjg

Strings Rule and Code Rule


```
rule Test_STR
{
   strings:
      $m1 = "onion"
      $m2 = "Offset"
      $m3 = "3FZbgicpjq2GjdwV8e"
   condition: 2 of ($m1,$m2,$m3)
}
```

```
rule Test_Hex
{
  strings:
     $hex_string = {DE AD BE EF}
condition:
     $hex_string
}
```

YaraGenerator


```
python yaraGenerator.py ../ransomware/sodinokibi/ -r sodin_test -f exe

rule sodin_test
{
strings:
        $string0 = "7777mmmm"
        $string1 = "pppp>>>>"
        $string2 = "Lj66lZ"
        $string3 = "55j_WW"
        [truncated]
        $string15 = "xxJo%%\\r..8$"
        $string17 = "YYYYGGGG"
        $string18 = "kkkkoooo"
condition:
        18 of them
}
```

VTHunting Tool

What is VTHunting?

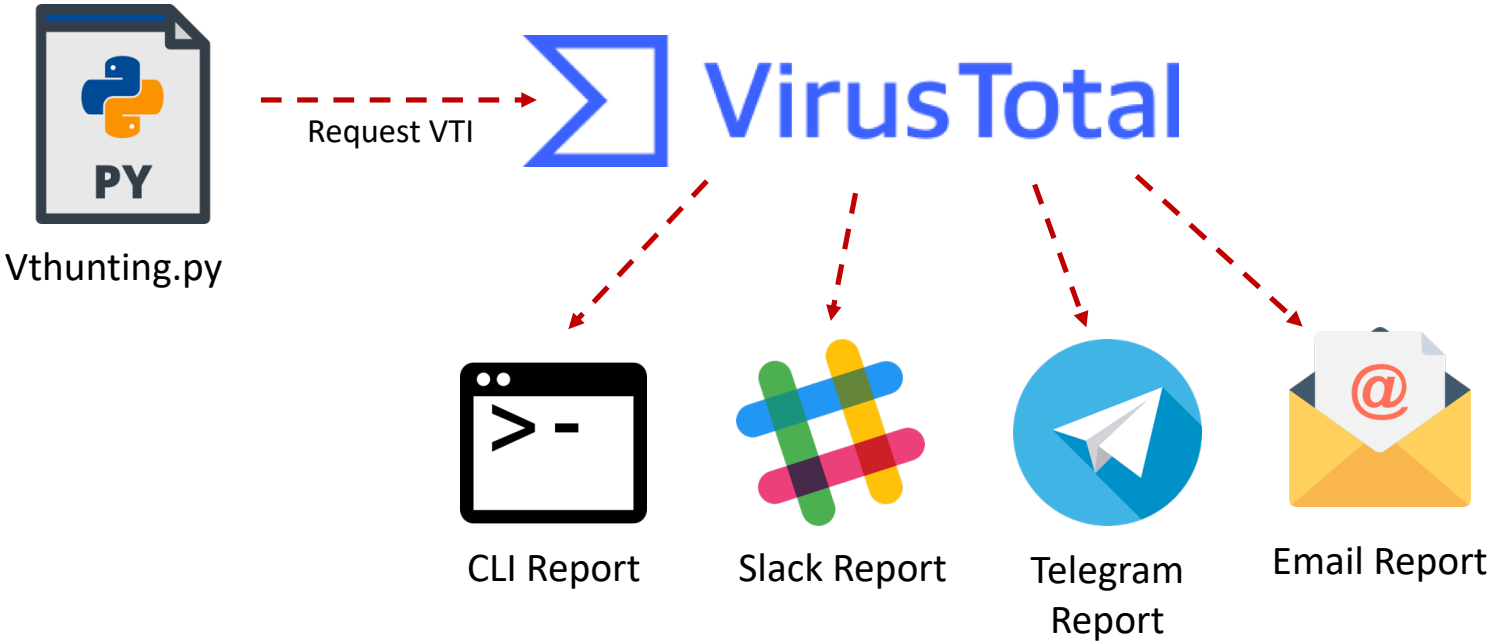
- VTHunting is a tiny tool coded in Python
- Used to collect Malware Hunting Report from VirusTotal
- Centralize reports notification in one place

Disclaimer: You need a VirusTotal Intelligence API

https://github.com/fr0gger/vthunting

VTHunting Tool

Vthunting Functionnalities



VTHunting Tool

How to use it?

- Configuring with cron to generate daily, weekly or monthly report

```
# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  *  user command to be executed

15 10  * * * /usr/local/bin/vthunting -r -t -e -s >> vthunt.log
```

VTHunting Tool

Report Example

Recap

- Multiple ways to identify code similarity
- Be aware to false flags
- Yara hunting with code and/or strings
- Vthunting to automate your threat hunting

Thank you!

Thomas Roccia, Security Researcher, ATR


McAfee™
Together is power.