資安威脅情資掌握

Shin-Ying Huang (Michelle) 2019.9.4

Outline

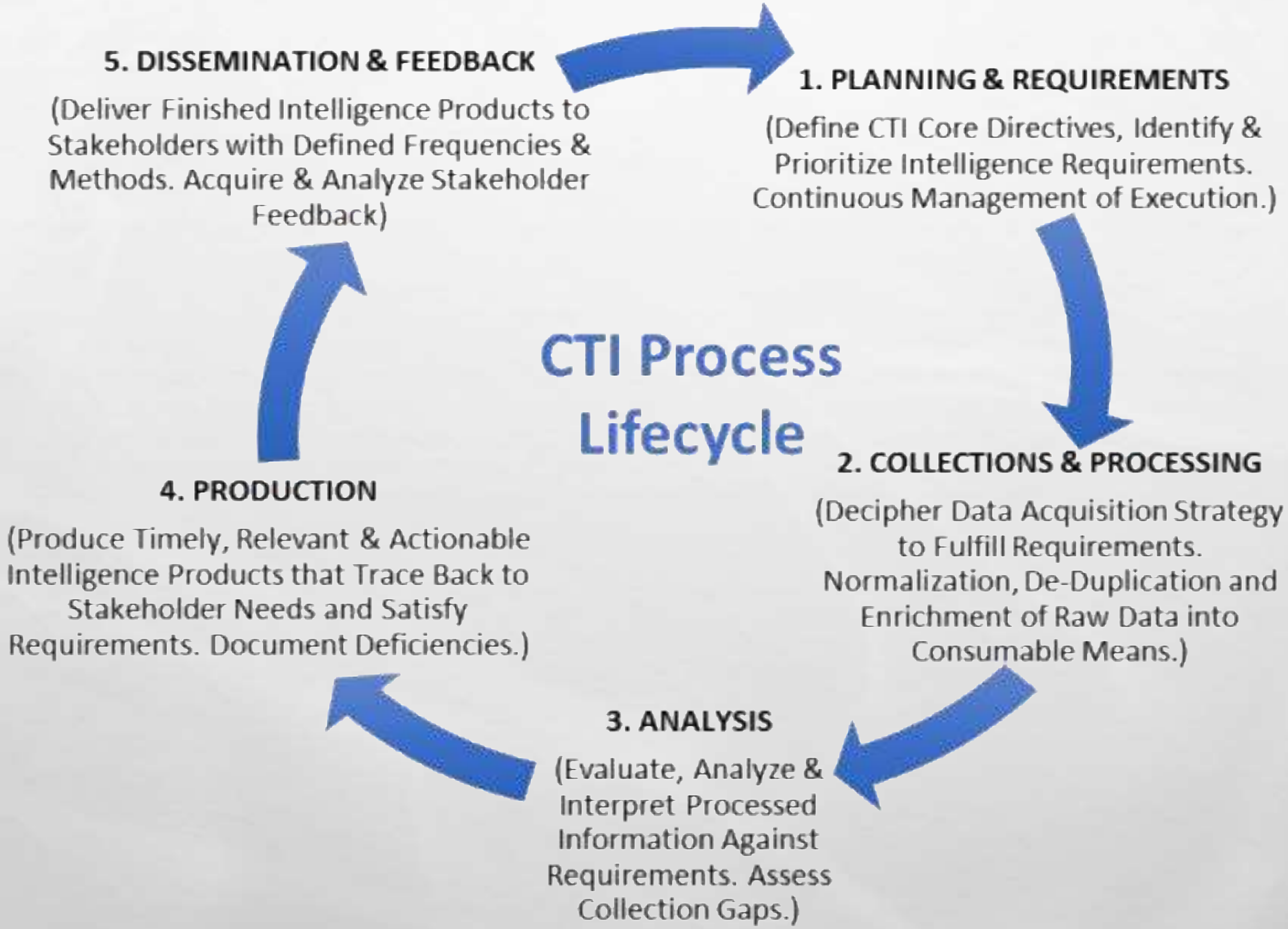
- Part 1: 威脅情資概論
  - 資安威脅情資掌握
  - 威脅情資處理週期
  - OSINT
- Part 2: 資安威脅情資處理
  - 威脅情蒐
  - 資安威脅分析
- Part 3: 資安威脅案例分析
  - 資安威脅事件處理案例導讀
  - 資安威脅通報應變實務

Part 1: 威脅情資概論

Threat Intelligence

- Definition:
  - Threat intelligence provides organized and analyzed information about past, present, and potential attacks that could be a security threat to an enterprise.
  - Threat intelligence delivers in-depth information such as URLs, domain names, files, and IP addresses that were used to execute attacks.
  - **The information helps an organization defend itself from current attacks and respond to security incidents.**

Threat Intelligence Life Cycle



CTI Process Lifecycle

1. PLANNING & REQUIREMENTS

(Define CTI Core Directives, Identify & Prioritize Intelligence Requirements. Continuous Management of Execution.)

2. COLLECTIONS & PROCESSING

(Decipher Data Acquisition Strategy to Fulfill Requirements. Normalization, De-Duplication and Enrichment of Raw Data into Consumable Means.)

3. ANALYSIS

(Evaluate, Analyze & Interpret Processed Information Against Requirements. Assess Collection Gaps.)

4. PRODUCTION

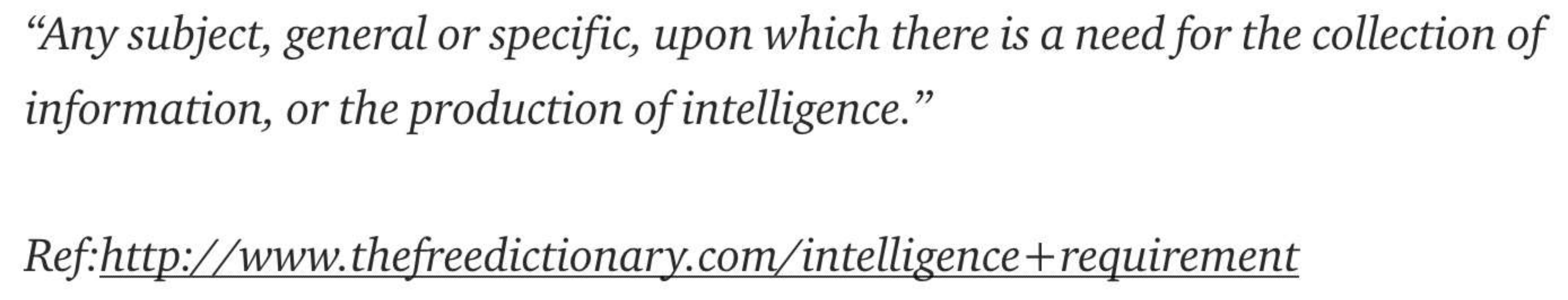
(Produce Timely, Relevant & Actionable Intelligence Products that Trace Back to Stakeholder Needs and Satisfy Requirements. Document Deficiencies.)

5. DISSEMINATION & FEEDBACK

(Deliver Finished Intelligence Products to Stakeholders with Defined Frequencies & Methods. Acquire & Analyze Stakeholder Feedback)

Threat Intelligence Life Cycle

- **Planning and direction**:
  - Set metrics, factors and questions that need to be gathered and answered. These pieces of information are typically called "intelligence requirements (IRs)"

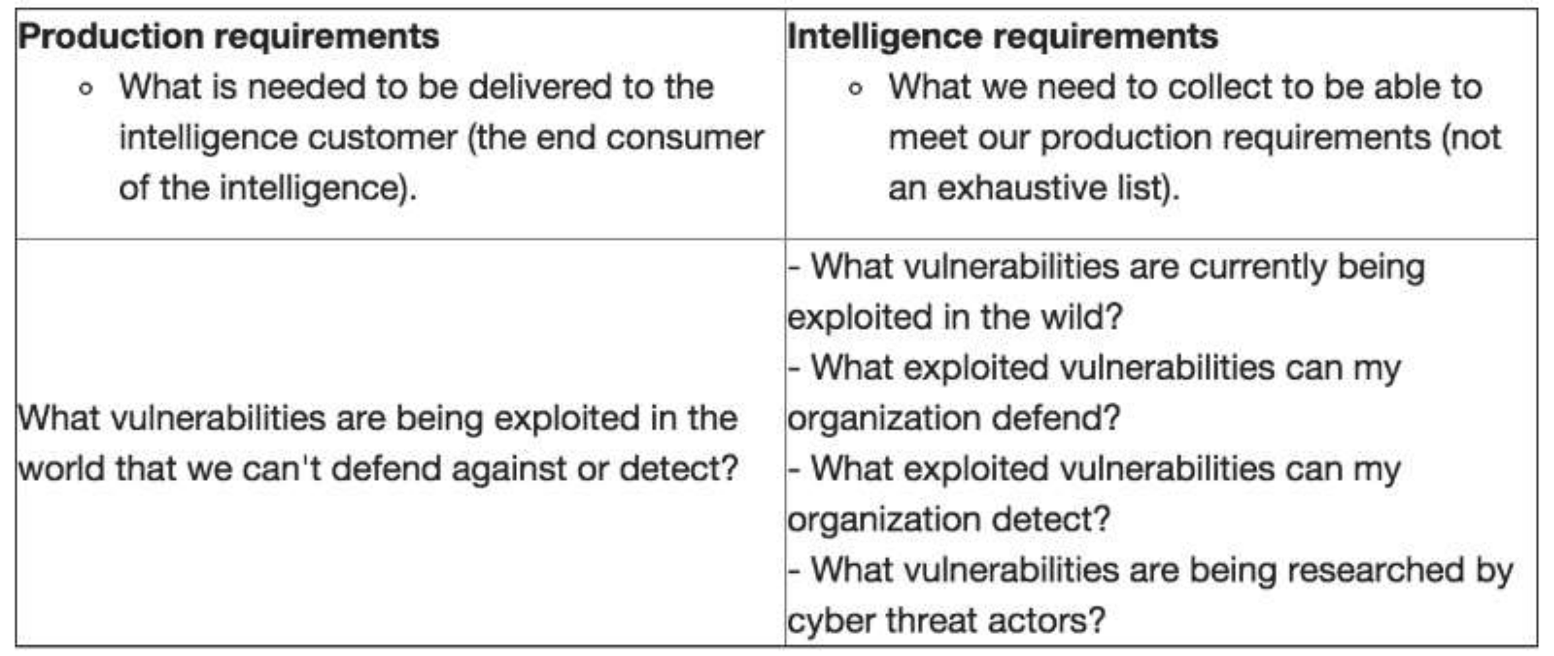


"Any subject, general or specific, upon which there is a need for the collection of information, or the production of intelligence."

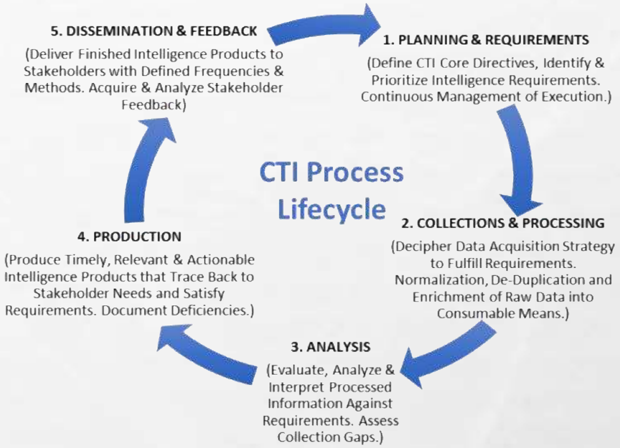
Ref:http://www.thefreedictionary.com/intelligence+requirement

Threat Intelligence Life Cycle

- Intelligence requirements :
  - 命題： The CISO/CSO (Chief Information Security Officer) of your organization wants to know of any vulnerabilities that are being exploited in the wild that your organization can’ t defend against or detect.



Production requirements	**Intelligence requirements**
○ What is needed to be delivered to the intelligence customer (the end consumer of the intelligence).	○ What we need to collect to be able to meet our production requirements (not an exhaustive list).
What vulnerabilities are being exploited in the world that we can't defend against or detect?	- What vulnerabilities are currently being exploited in the wild? - What exploited vulnerabilities can my organization defend? - What exploited vulnerabilities can my organization detect? - What vulnerabilities are being researched by cyber threat actors?



5. DISSEMINATION & FEEDBACK

(Deliver Finished Intelligence Products to Stakeholders with Defined Frequencies & Methods. Acquire & Analyze Stakeholder Feedback)

1. PLANNING & REQUIREMENTS

(Define CTI Core Directives, Identify & Prioritize Intelligence Requirements. Continuous Management of Execution.)

CTI Process Lifecycle

2. COLLECTIONS & PROCESSING

(Decipher Data Acquisition Strategy to Fulfill Requirements. Normalization, De-Duplication and Enrichment of Raw Data into Consumable Means.)

4. PRODUCTION

(Produce Timely, Relevant & Actionable Intelligence Products that Trace Back to Stakeholder Needs and Satisfy Requirements. Document Deficiencies.)

3. ANALYSIS

(Evaluate, Analyze & Interpret Processed Information Against Requirements. Assess Collection Gaps.)

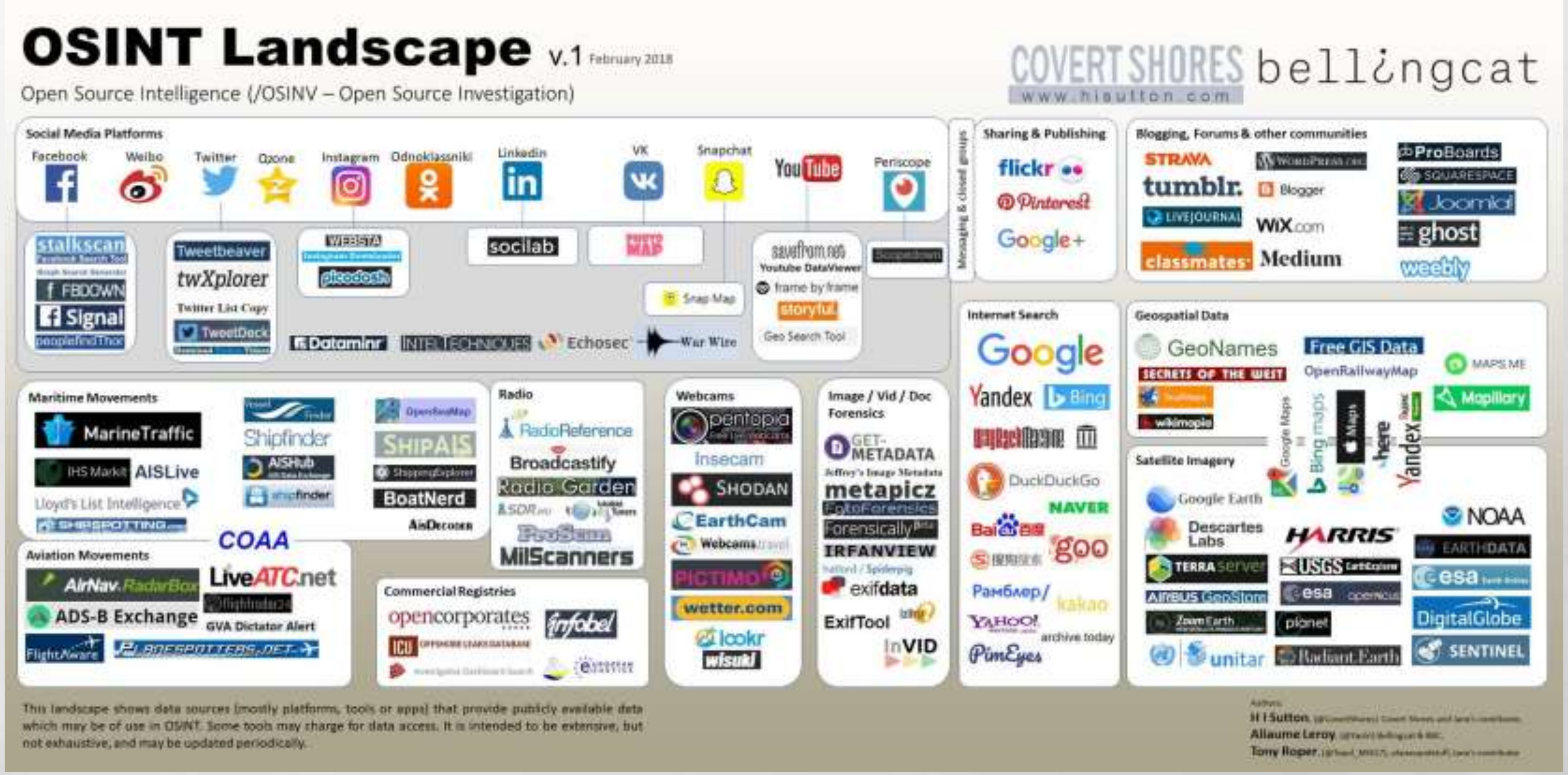
Threat Intelligence Life Cycle

- **Processing**:
  - Those who have gathered the intelligence begin to process and organize the data for the entire team to understand. Processing could be the formation of a report or presentation. Presenting the data gathered must include the ability for the threat intelligence team to analyze it clearly.
- **Analysis and production**:
  - Analysis is the process of the team looking through and recognizing the patterns and key events which lead to both the incident and the vulnerability.
- **Distribution and feedback**:
  - Distribution is the process of getting the created report into the hands of the leadership and key personnel it was created to serve. Once the report is read, feedback is important to improve future reporting.

Open Source Intelligence (OSINT)

- All the publicly available information.

- According to U.S. public law, open source intelligence:
  - Is produced from publicly available information
  - Is collected, analyzed, and disseminated in a timely manner to an appropriate audience
  - Addresses a specific intelligence requirement



OSINT Landscape v.1 February 2018

Open Source Intelligence (/OSINV – Open Source Investigation)

This landscape shows data sources (mostly platforms, tools or apps) that provide publicly available data which may be of use in OSINT. Some tools may charge for data access. It is intended to be extensive, but not exhaustive, and may be updated periodically.

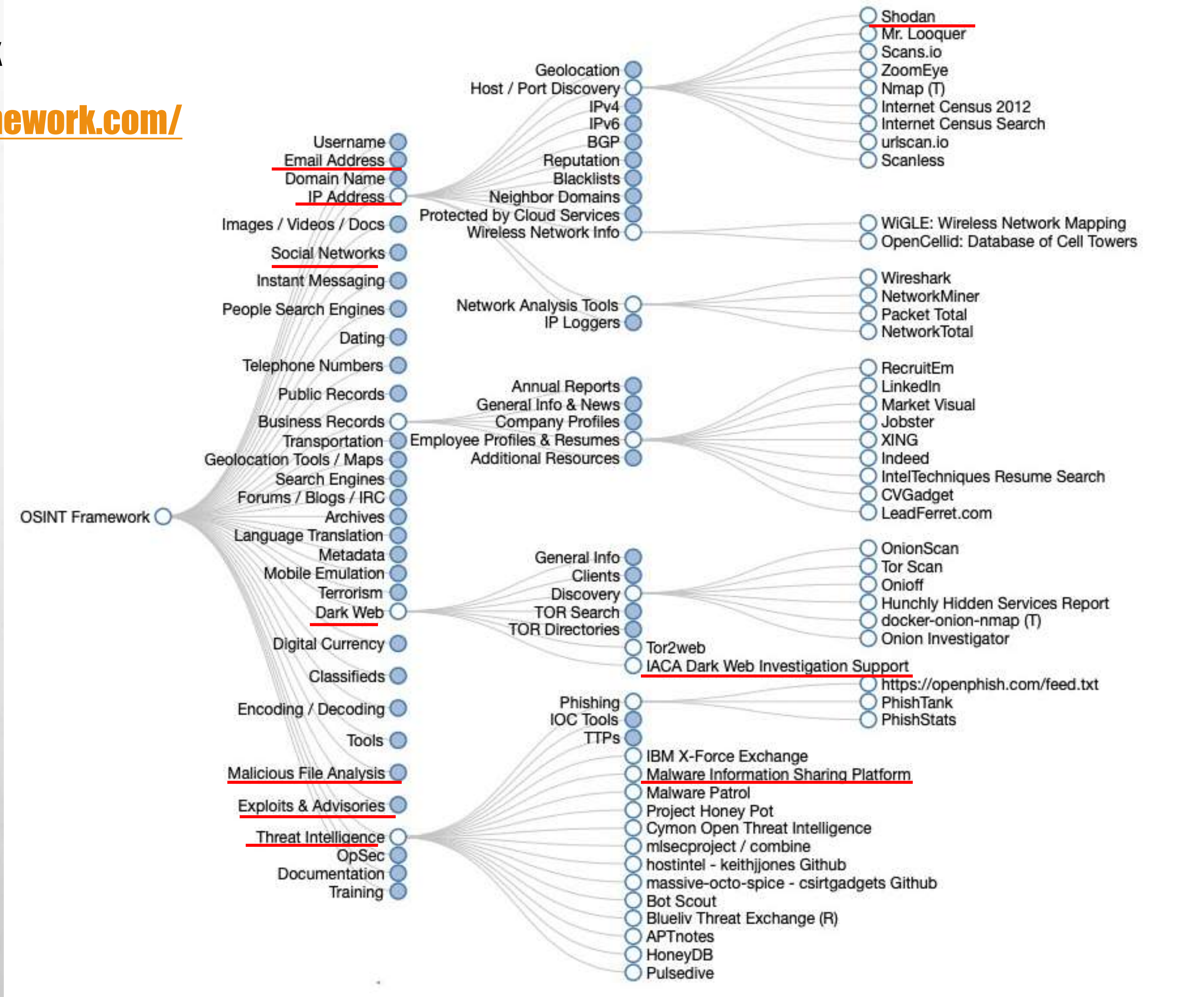
Authors:
H I Sutton
Allaume Leroy
Tony Roper

Open Source Intelligence (OSINT)

- How is open source intelligence used?
  1. Ethical Hacking and Penetration Testing
     - Accidental leaks of sensitive information, like through social media
     - Open ports or unsecured internet-connected devices
     - Unpatched software, such as websites running old versions of common CMS products
     - Leaked or exposed assets, such as proprietary code
  2. Identifying External Threats
     - In most cases, this type of work requires an analyst to identify and correlate multiple data points to validate a threat before action is taken.
     - Intelligence from closed sources such as internal telemetry, closed dark web communities, and external intelligence-sharing communities is regularly used to filter and verify open source intelligence.

OSINT Framework

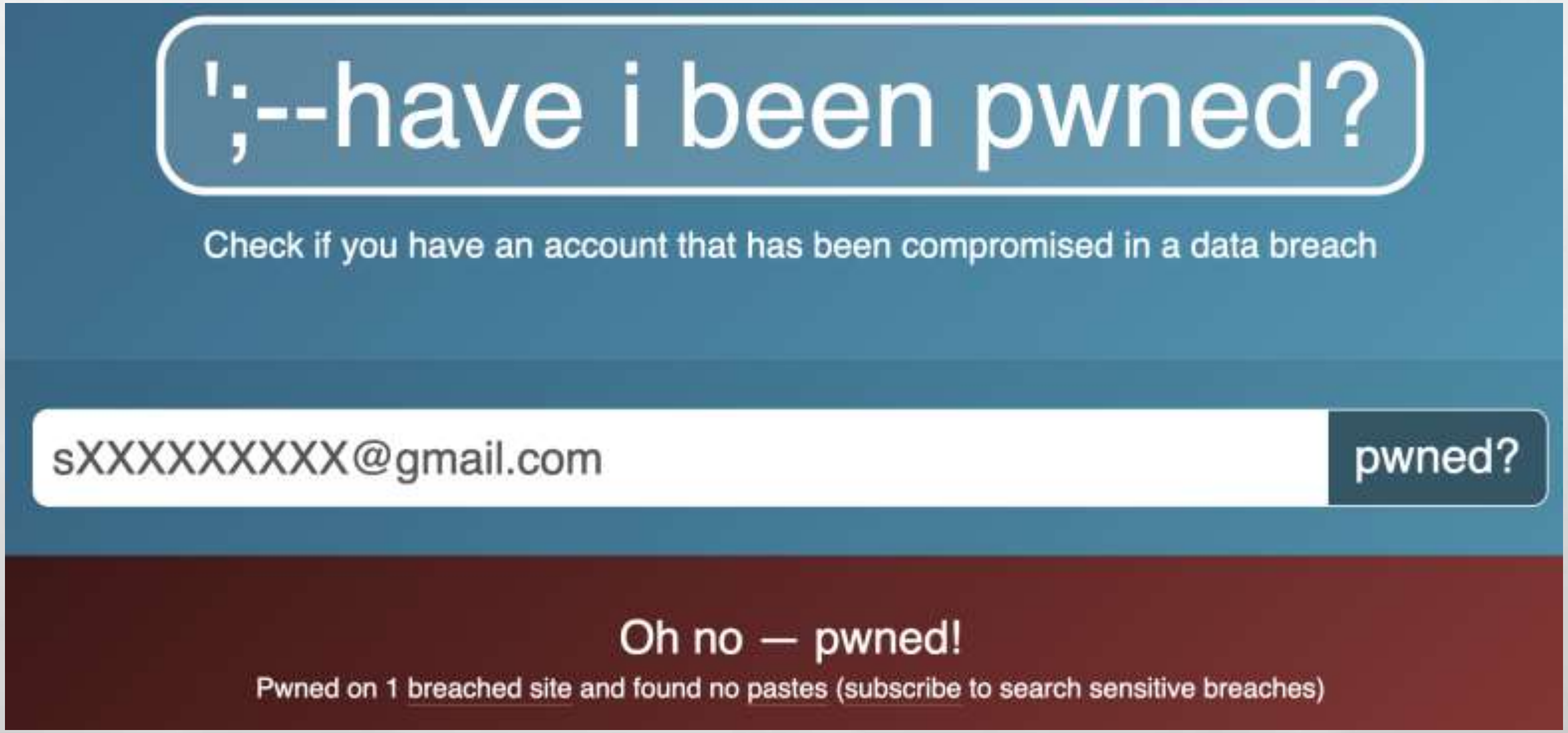
https://osintframework.com/



Part 2: 資安威脅情資處理

Check this website

- have i been pwned (https://haveibeenpwned.com/)
    - Check if you have an account that has been compromised in a data breach.



';--have i been pwned?

Check if you have an account that has been compromised in a data breach

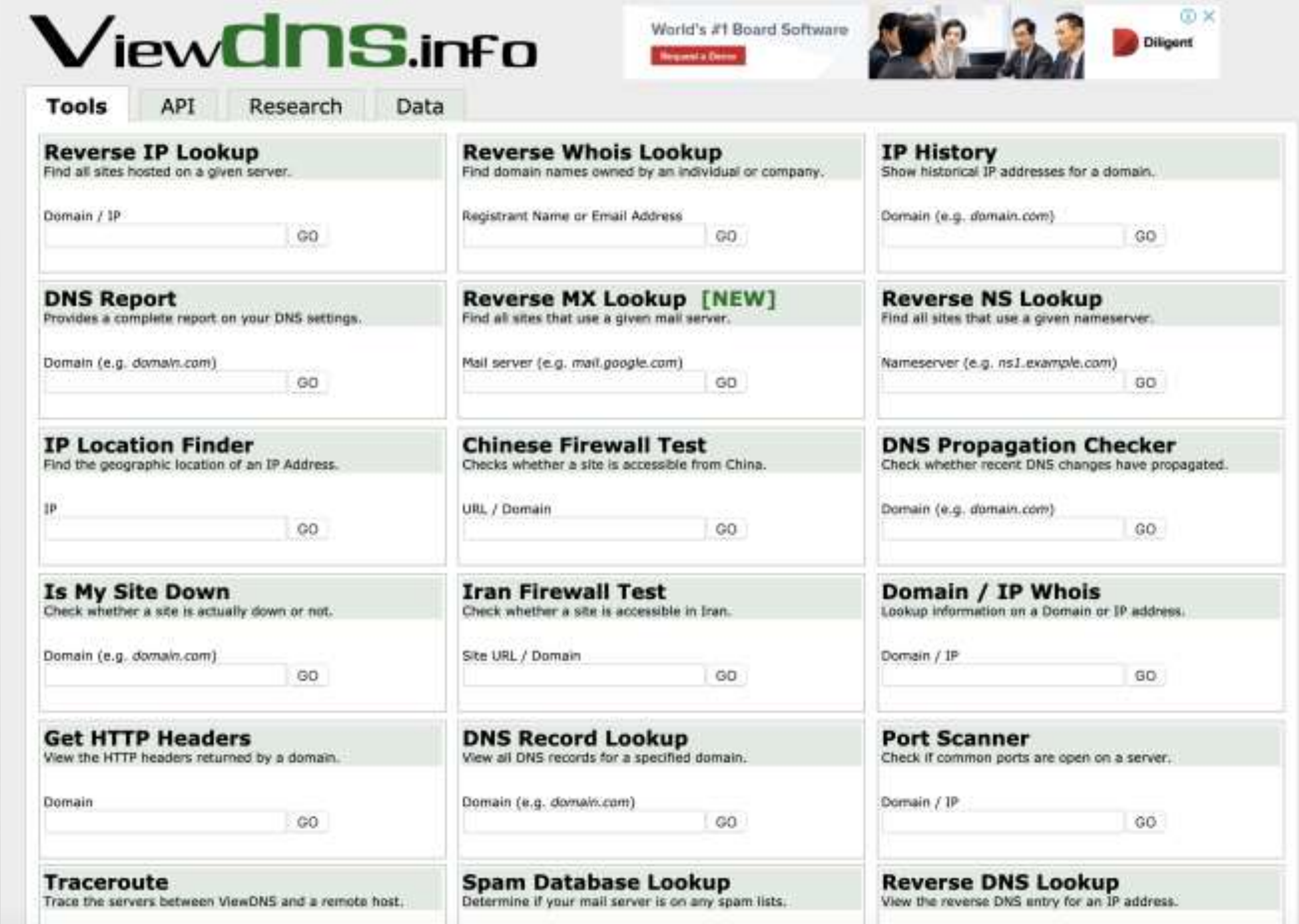
sXXXXXXXXX@gmail.com

Oh no — pwned!

Pwned on 1 breached site and found no pastes (subscribe to search sensitive breaches)

Check this website

- Viewdns (https://viewdns.info/)



ViewDNS.info

Tools | API | Research | Data

Reverse IP Lookup
Find all sites hosted on a given server.
Domain / IP
GO

Reverse Whois Lookup
Find domain names owned by an individual or company.
Registrant Name or Email Address
GO

IP History
Show historical IP addresses for a domain.
Domain (e.g. *domain.com*)
GO

DNS Report
Provides a complete report on your DNS settings.
Domain (e.g. *domain.com*)
GO

Reverse MX Lookup [NEW]
Find all sites that use a given mail server.
Mail server (e.g. *mail.google.com*)
GO

Reverse NS Lookup
Find all sites that use a given nameserver.
Nameserver (e.g. *ns1.example.com*)
GO

IP Location Finder
Find the geographic location of an IP Address.
IP
GO

Chinese Firewall Test
Checks whether a site is accessible from China.
URL / Domain
GO

DNS Propagation Checker
Check whether recent DNS changes have propagated.
Domain (e.g. *domain.com*)
GO

Is My Site Down
Check whether a site is actually down or not.
Domain (e.g. *domain.com*)
GO

Iran Firewall Test
Check whether a site is accessible in Iran.
Site URL / Domain
GO

Domain / IP Whois
Lookup information on a Domain or IP address.
Domain / IP
GO

Get HTTP Headers
View the HTTP headers returned by a domain.
Domain
GO

DNS Record Lookup
View all DNS records for a specified domain.
Domain (e.g. *domain.com*)
GO

Port Scanner
Check if common ports are open on a server.
Domain / IP
GO

Traceroute
Trace the servers between ViewDNS and a remote host.

Spam Database Lookup
Determine if your mail server is on any spam lists.

Reverse DNS Lookup
View the reverse DNS entry for an IP address.

Check this website

- Insecam (https://www.insecam.org/)
  - The world biggest directory of online surveillance security cameras. You can search live web cams around the world. You can find here Axis, Panasonic, Linksys, Sony, TPLink, Foscam and a lot of other network video cams available online without a password. Mozilla Firefox browser is recommended to watch network cameras..

Watch DLink-DCS-932 camera in Ireland,Moycullen

Watch Mobotix camera in Italy,Rome

Watch DLink-DCS-932 camera in United States,Worcester

Watch DLink camera in Singapore,Singapore

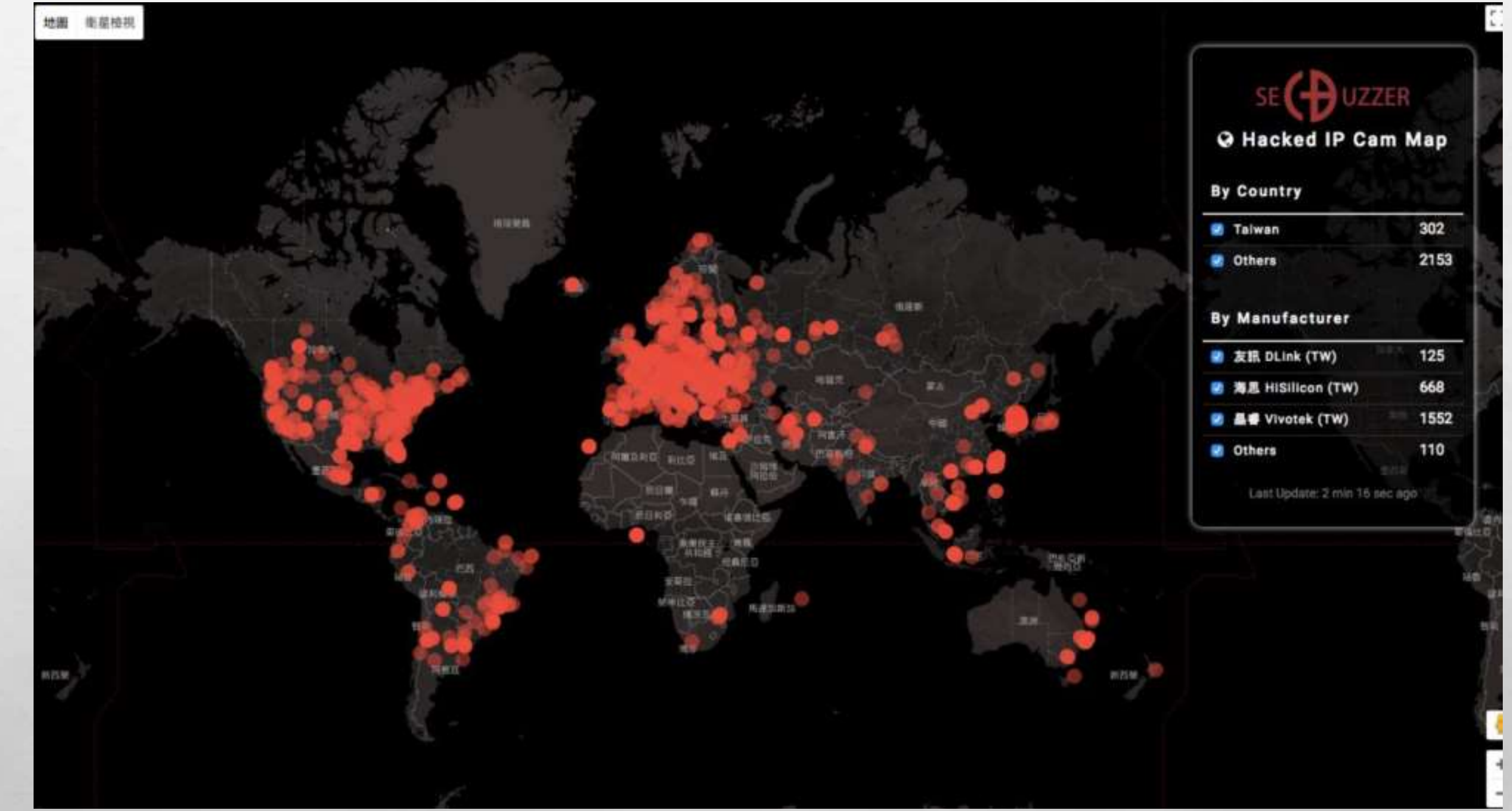
Watch Hi3516 camera in Taiwan, Province Of ,Taipei

Watch Vivotek camera in Slovakia,Tlmace

Watch DLink camera in United States,Cambridge

Watch Axis camera in United Kingdom,Lindley

Hacked IP Cam Map



Hacked IP Cam Map

By Country

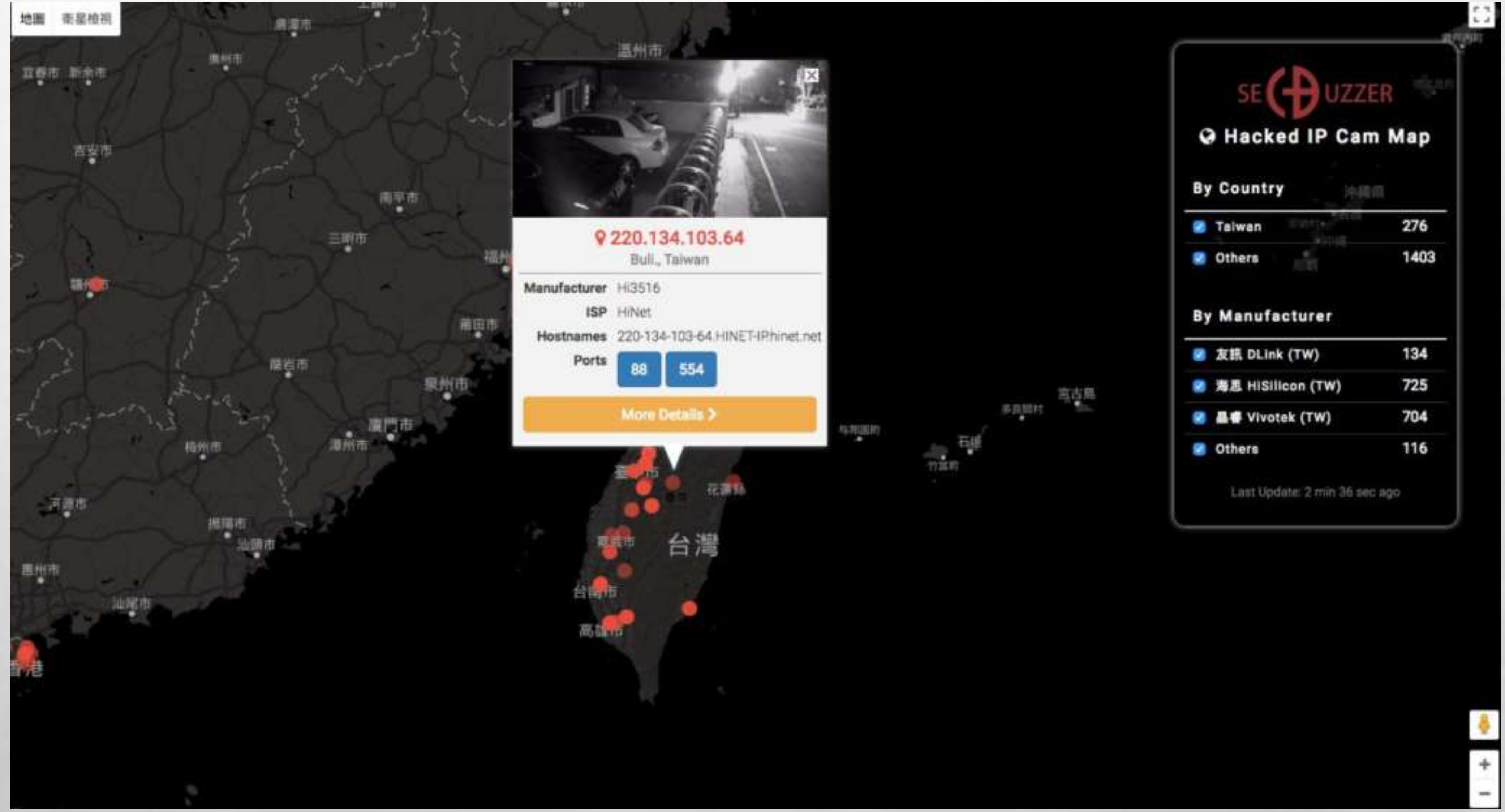
☑ Taiwan	302
☑ Others	2153

By Manufacturer

☑ 友訊 DLink (TW)	125
☑ 海思 HiSilicon (TW)	668
☑ 晶睿 Vivotek (TW)	1552
☑ Others	110

Last Update: 2 min 16 sec ago

Hacked IP Cam Map



220.134.103.64
Buli., Taiwan

Manufacturer	Hi3516
ISP	HiNet
Hostnames	220-134-103-64.HINET-IP.hinet.net
Ports	88 554

More Details >

SECFUZZER

Hacked IP Cam Map

By Country

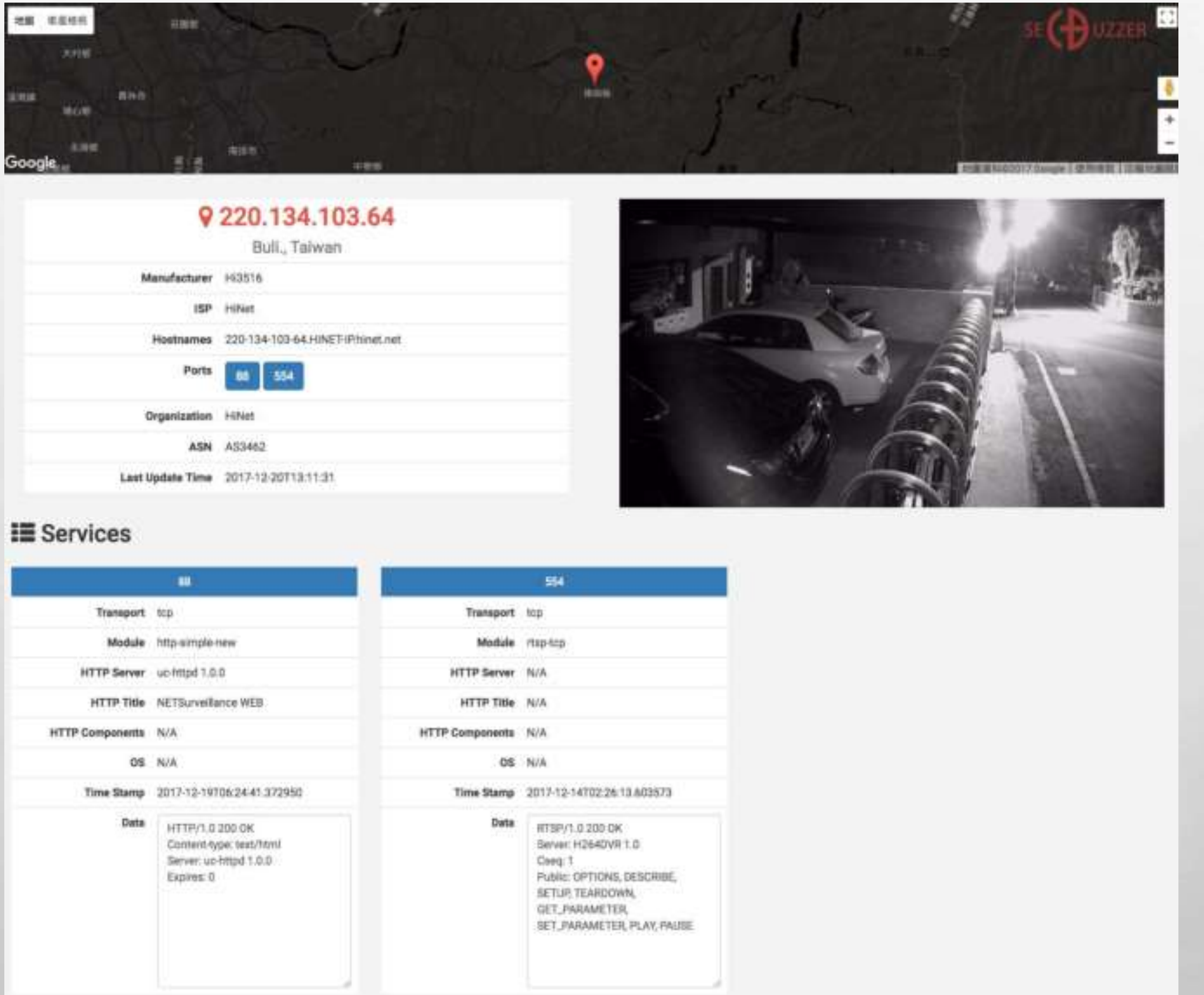
☑ Taiwan	276
☑ Others	1403

By Manufacturer

☑ 友訊 DLink (TW)	134
☑ 海思 HiSilicon (TW)	725
☑ 晶睿 Vivotek (TW)	704
☑ Others	116

Last Update: 2 min 36 sec ago

Hacked IP Cam Map



220.134.103.64

Buli., Taiwan

Manufacturer	Hi3516
ISP	HiNet
Hostnames	220-134-103-64.HINET-IP.hinet.net
Ports	88 554
Organization	HiNet
ASN	AS3462
Last Update Time	2017-12-20T13:11:31

Services

88	
Transport	tcp
Module	http-simple-new
HTTP Server	uc-httpd 1.0.0
HTTP Title	NETSurveillance WEB
HTTP Components	N/A
OS	N/A
Time Stamp	2017-12-19T06:24:41.372950

Data

```
HTTP/1.0 200 OK
Content-type: text/html
Server: uc-httpd 1.0.0
Expires: 0
```

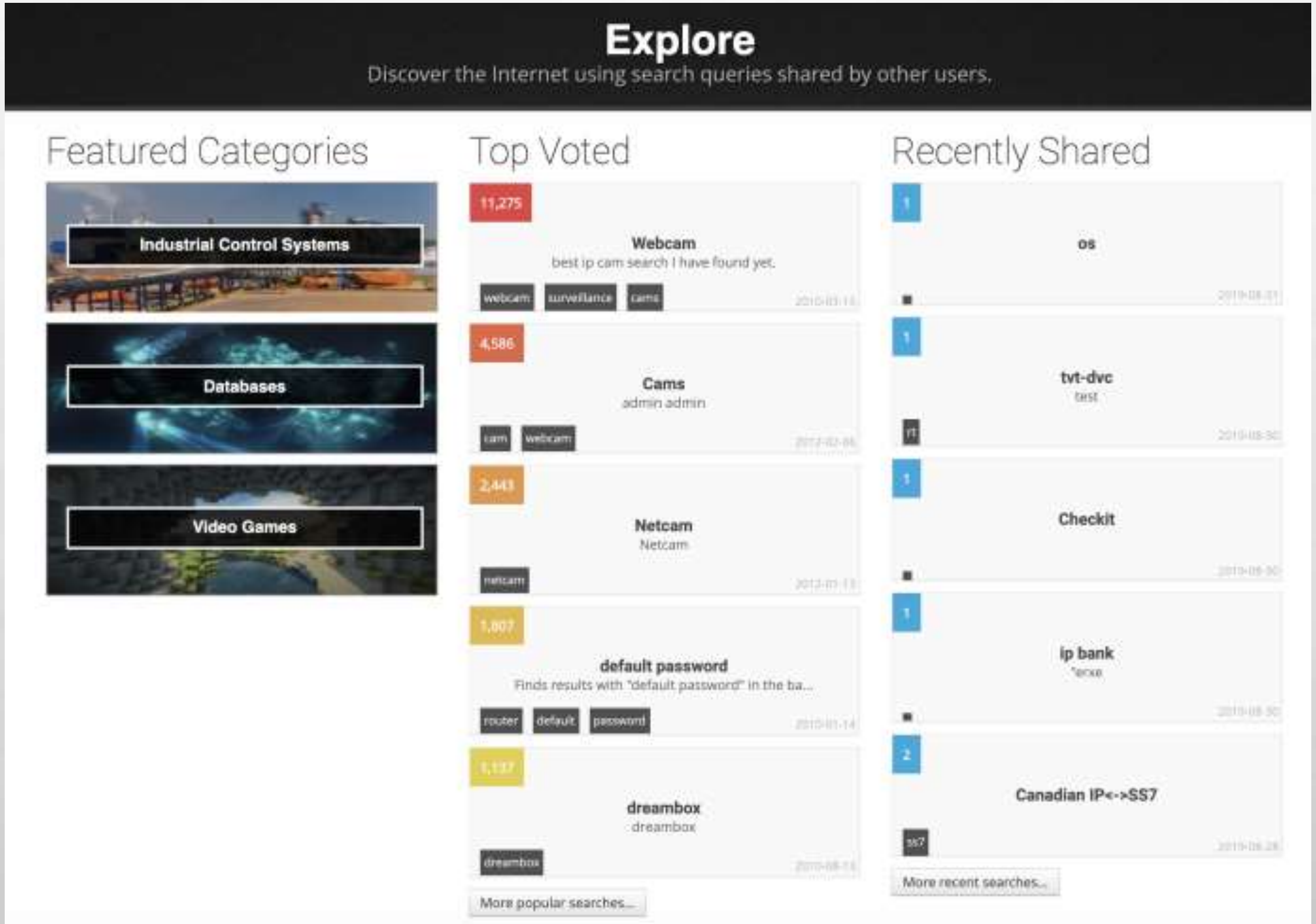
554	
Transport	tcp
Module	rtsp-tcp
HTTP Server	N/A
HTTP Title	N/A
HTTP Components	N/A
OS	N/A
Time Stamp	2017-12-14T02:26:13.603573

Data

```
RTSP/1.0 200 OK
Server: H264DVR 1.0
Cseq: 1
Public: OPTIONS, DESCRIBE,
SETUP, TEARDOWN,
GET_PARAMETER,
SET_PARAMETER, PLAY, PAUSE
```

Shodan https://www.shodan.io/

- Shodan is the world's first search engine for Internet-connected device.



Explore

Discover the Internet using search queries shared by other users.

Featured Categories

- Industrial Control Systems
- Databases
- Video Games

Top Voted

11,275
Webcam
best ip cam search I have found yet.
webcam surveillance cams
2010-03-14

4,586
Cams
admin admin
cam webcam
2012-02-06

2,443
Netcam
Netcam
netcam
2012-01-13

1,807
default password
Finds results with "default password" in the ba...
router default password
2010-01-14

1,137
dreambox
dreambox
dreambox
2010-08-14

More popular searches...

Recently Shared

1
os
2019-08-31

1
tvt-dvc
test
rt
2019-08-30

1
Checkit
2019-08-30

1
ip bank
*erxe
2019-08-30

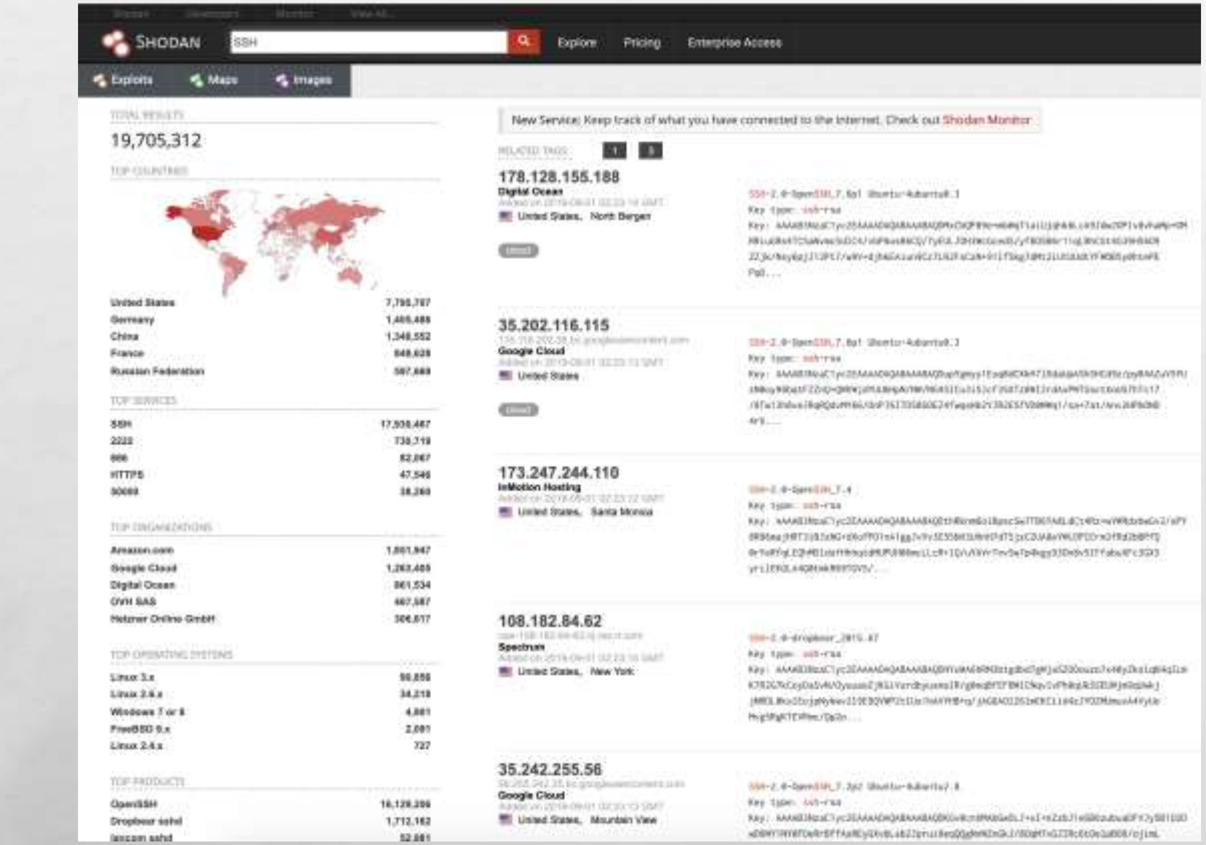
2
Canadian IP<->SS7
ss7
2019-08-28

More recent searches...

Part 2: 資安威脅情資處理 -威脅情蒐

Shodan https://www.shodan.io/

- Query example: SSH



SHODAN SSH Explore Pricing Enterprise Access

Exploits Maps Images

TOTAL RESULTS

19,705,312

TOP COUNTRIES

United States	7,795,767
Germany	1,405,488
China	1,348,552
France	848,628
Russian Federation	587,889

TOP SERVICES

SSH	17,508,467
2222	738,719
666	82,067
HTTPS	47,546
30069	38,260

TOP ORGANIZATIONS

Amazon.com	1,861,947
Google Cloud	1,263,405
Digital Ocean	861,534
OVH SAS	467,587
Hetzner Online GmbH	306,617

TOP OPERATING SYSTEMS

Linux 3.x	96,856
Linux 2.6.x	34,218
Windows 7 or 8	4,881
FreeBSD 9.x	2,081
Linux 2.4.x	727

TOP PRODUCTS

OpenSSH	16,129,206
Dropbear sshd	1,712,162
lancom sshd	52,881

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

RELATED TAGS:

178.128.155.188
Digital Ocean
Added on 2019-09-01 02:23:14 GMT
United States, North Bergen

```
SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3
Key type: ssh-rsa
Key: [illegible]
```

35.202.116.115
Google Cloud
Added on 2019-09-01 02:23:13 GMT
United States

```
SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3
Key type: ssh-rsa
Key: [illegible]
```

173.247.244.110
InMotion Hosting
Added on 2019-09-01 02:23:12 GMT
United States, Santa Monica

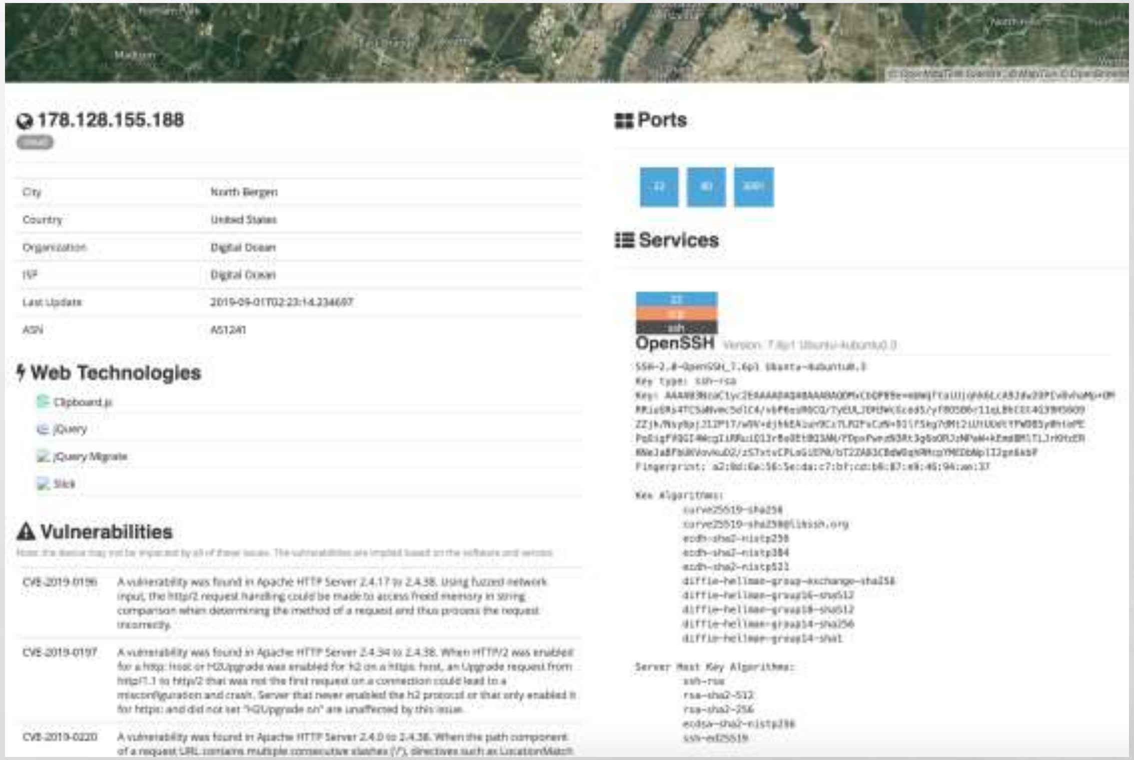
```
SSH-2.0-OpenSSH_7.4
Key type: ssh-rsa
Key: [illegible]
```

108.182.84.62
Spectrum
Added on 2019-09-01 02:23:10 GMT
United States, New York

```
SSH-2.0-dropbear_2015.67
Key type: ssh-rsa
Key: [illegible]
```

35.242.255.56
Google Cloud
Added on 2019-09-01 02:23:13 GMT
United States, Mountain View

```
SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.8
Key type: ssh-rsa
Key: [illegible]
```



178.128.155.188

City	North Bergen
Country	United States
Organization	Digital Ocean
ISP	Digital Ocean
Last Update	2019-09-01T02:23:14.234697
ASN	AS1241

Web Technologies

- Clipboard.js
- jQuery
- jQuery Migrate
- Slick

Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2019-0196	A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38. Using fuzzed network input, the http/2 request handling could be made to access freed memory in string comparison when determining the method of a request and thus process the request incorrectly.
CVE-2019-0197	A vulnerability was found in Apache HTTP Server 2.4.34 to 2.4.38. When HTTP/2 was enabled for a http: host or H2Upgrade was enabled for h2 on a https: host, an Upgrade request from http/1.1 to http/2 that was not the first request on a connection could lead to a misconfiguration and crash. Server that never enabled the h2 protocol or that only enabled it for https: and did not set "H2Upgrade on" are unaffected by this issue.
CVE-2019-0220	A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch

Ports

22 80 [illegible]

Services

22
tcp
ssh

OpenSSH Version: 7.6p1 Ubuntu-4ubuntu0.3

```
SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3
Key type: ssh-rsa
Key: [illegible]
Fingerprint: a2:8d:6a:56:5e:da:c7:bf:cd:b6:87:e9:46:94:ae:37

Kex Algorithms:
	curve25519-sha256
	curve25519-sha256@libssh.org
	ecdh-sha2-nistp256
	ecdh-sha2-nistp384
	ecdh-sha2-nistp521
	diffie-hellman-group-exchange-sha256
	diffie-hellman-group16-sha512
	diffie-hellman-group18-sha512
	diffie-hellman-group14-sha256
	diffie-hellman-group14-sha1

Server Host Key Algorithms:
	ssh-rsa
	rsa-sha2-512
	rsa-sha2-256
	ecdsa-sha2-nistp256
	ssh-ed25519
```

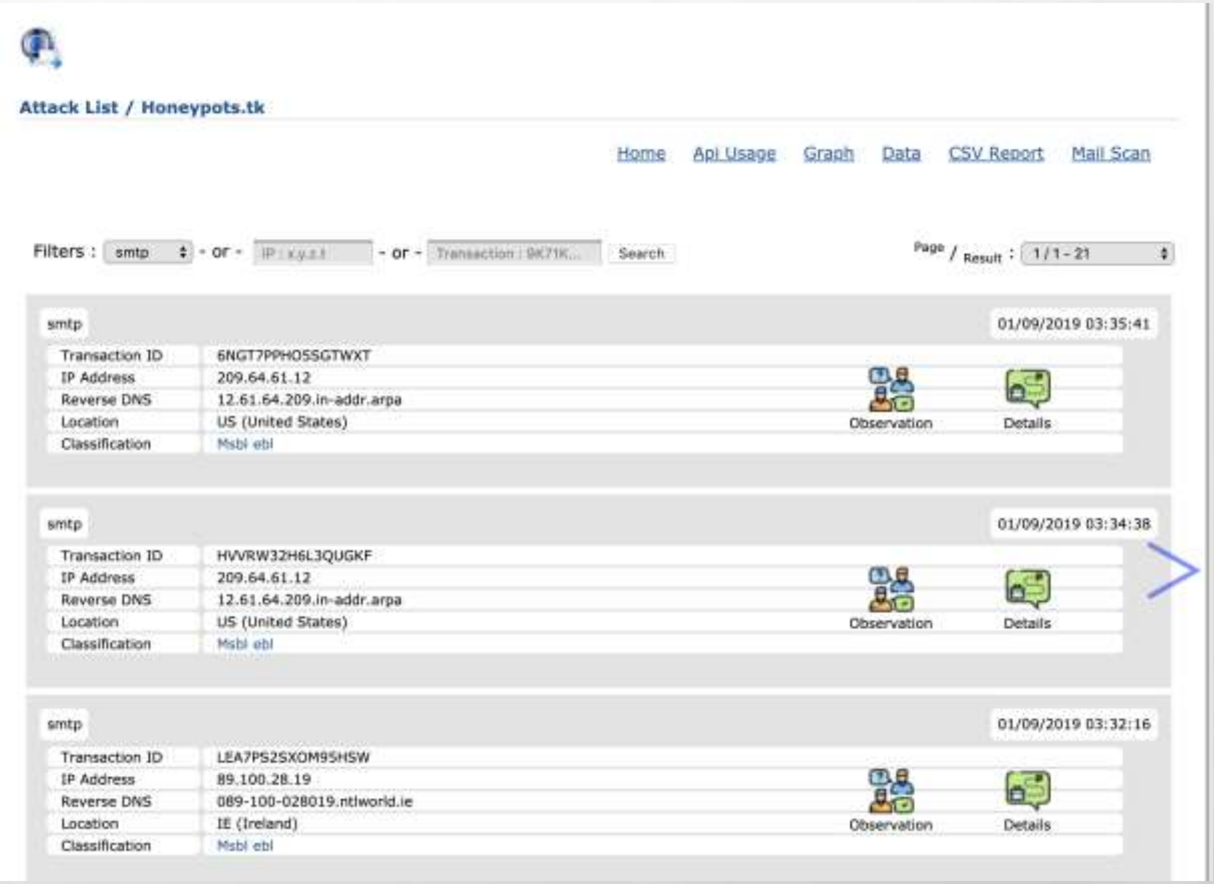
Shodan https://www.shodan.io/

- Other query example:
  - nginx country:"TW”
  - apache city:"Taipei”
  - "Server: gws" hostname:"google”
  - Server: uc-httpd 1.0.0 200 OK Country: “TW” (NetSureveillance Web弱密碼漏洞)
  - IoT Camera CYB671
- Exploit
  - EEC
  - Modbus
  - Medtronic
- Click “map” and “images” based on the searching result

Honeypot intelligence

https://www.honeypots.tk/data?service=smtp

- Attacker attempting to connect will implementing system information gathering and remote code execution.
- Therefore we wrote our own services to collect all attacker informations. These services collect the ip address, executed codes, queries and requested URLs and the header information that they leave.
- Finally they will forward this information from honeypots to our central server



Attack List / Honeypots.tk

Filters : smtp - or - IP : x.y.z.t - or - Transaction : 9K71K... Page / Result : 1 / 1 - 21

smtp 01/09/2019 03:35:41

Transaction ID	6NGT7PPHOSSGTWXT
IP Address	209.64.61.12
Reverse DNS	12.61.64.209.in-addr.arpa
Location	US (United States)
Classification	Msbl ebl

smtp 01/09/2019 03:34:38

Transaction ID	HVVRW32H6L3QUGKF
IP Address	209.64.61.12
Reverse DNS	12.61.64.209.in-addr.arpa
Location	US (United States)
Classification	Msbl ebl

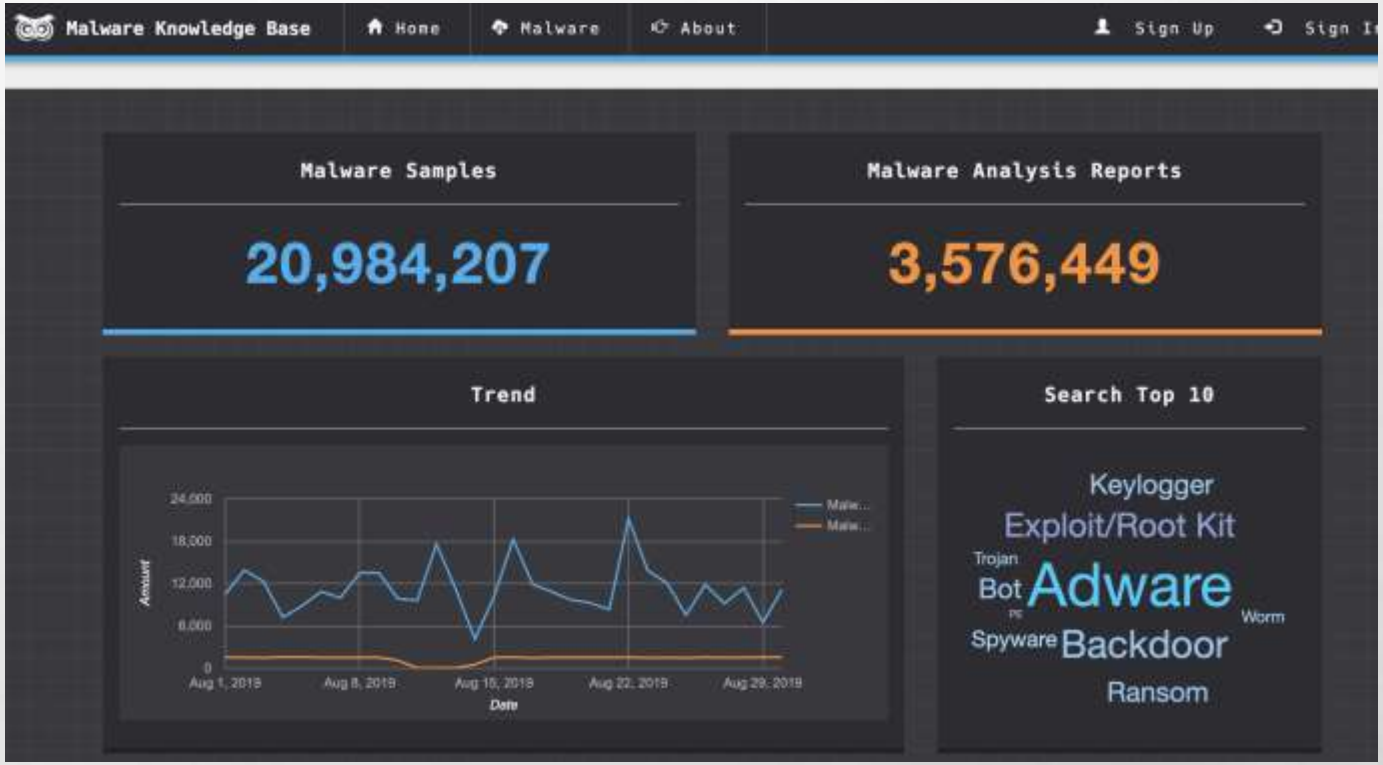
smtp 01/09/2019 03:32:16

Transaction ID	LEA7PS2SXOM9SHSW
IP Address	89.100.28.19
Reverse DNS	089-100-028019.ntlworld.ie
Location	IE (Ireland)
Classification	Msbl ebl

Malware Knowledge Base

https://owl.nchc.org.tw/

- Malware Knowledge Base, hosted by the National Center for High-performance Computing(NCHC) and Taiwan Computer Security Incident Response Team(TWCSIRT), is a malware analysis platform that observes and records system behaviors conducted by analysis objects in a controlled environment with various types of dynamic analysis tools.

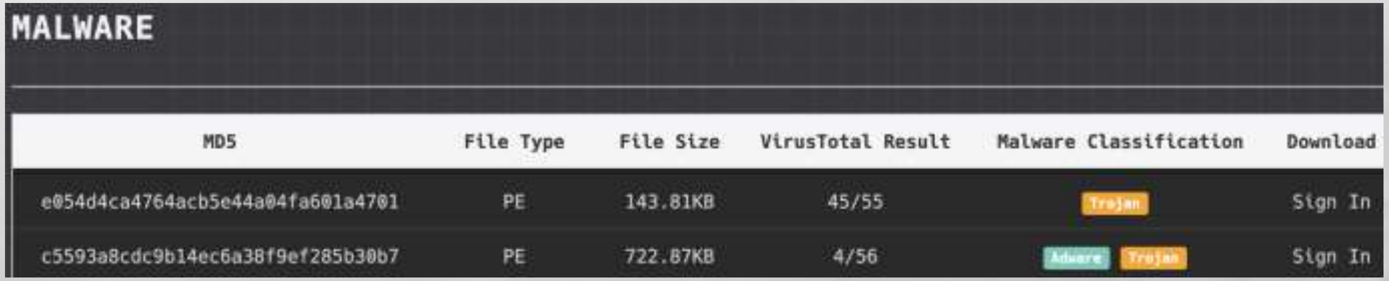


Malware Samples

20,984,207

Malware Analysis Reports

3,576,449



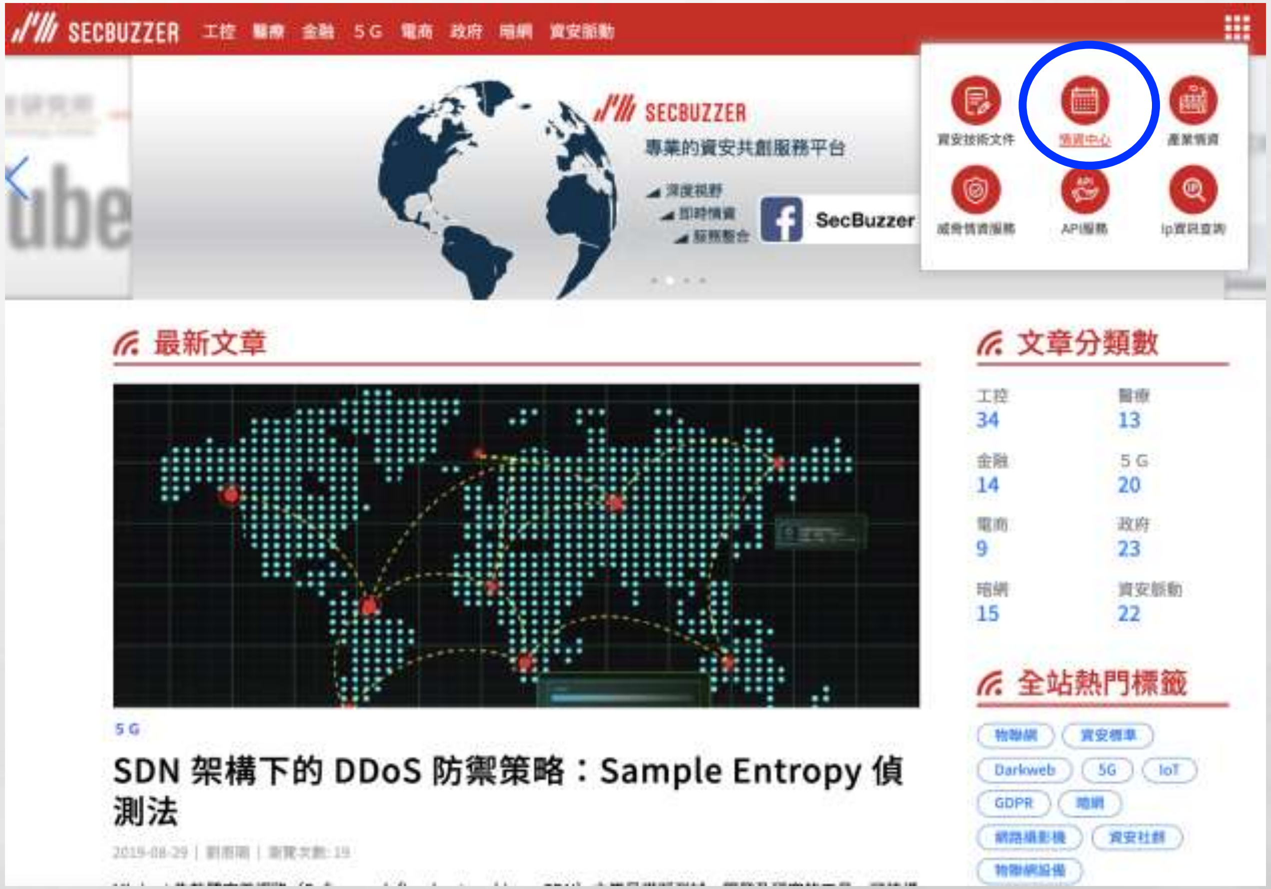
MALWARE

MD5	File Type	File Size	VirusTotal Result	Malware Classification	Download
e054d4ca4764acb5e44a04fa601a4701	PE	143.81KB	45/55	Trojan	Sign In
c5593a8cdc9b14ec6a38f9ef285b30b7	PE	722.87KB	4/56	Adware Trojan	Sign In

SecBuzzer https://secbuzzer.co/

- SecBuzzer is a cybersecurity threat intelligence collection and analytic platform. The intelligence sources include: vulnerability advisories, social media, CERT news, honeypot malware samples, and dark web.

- SecBuzzer can systematically collect, organizing and correlate different intelligence sources.



最新文章

5G

SDN 架構下的 DDoS 防禦策略：Sample Entropy 偵測法

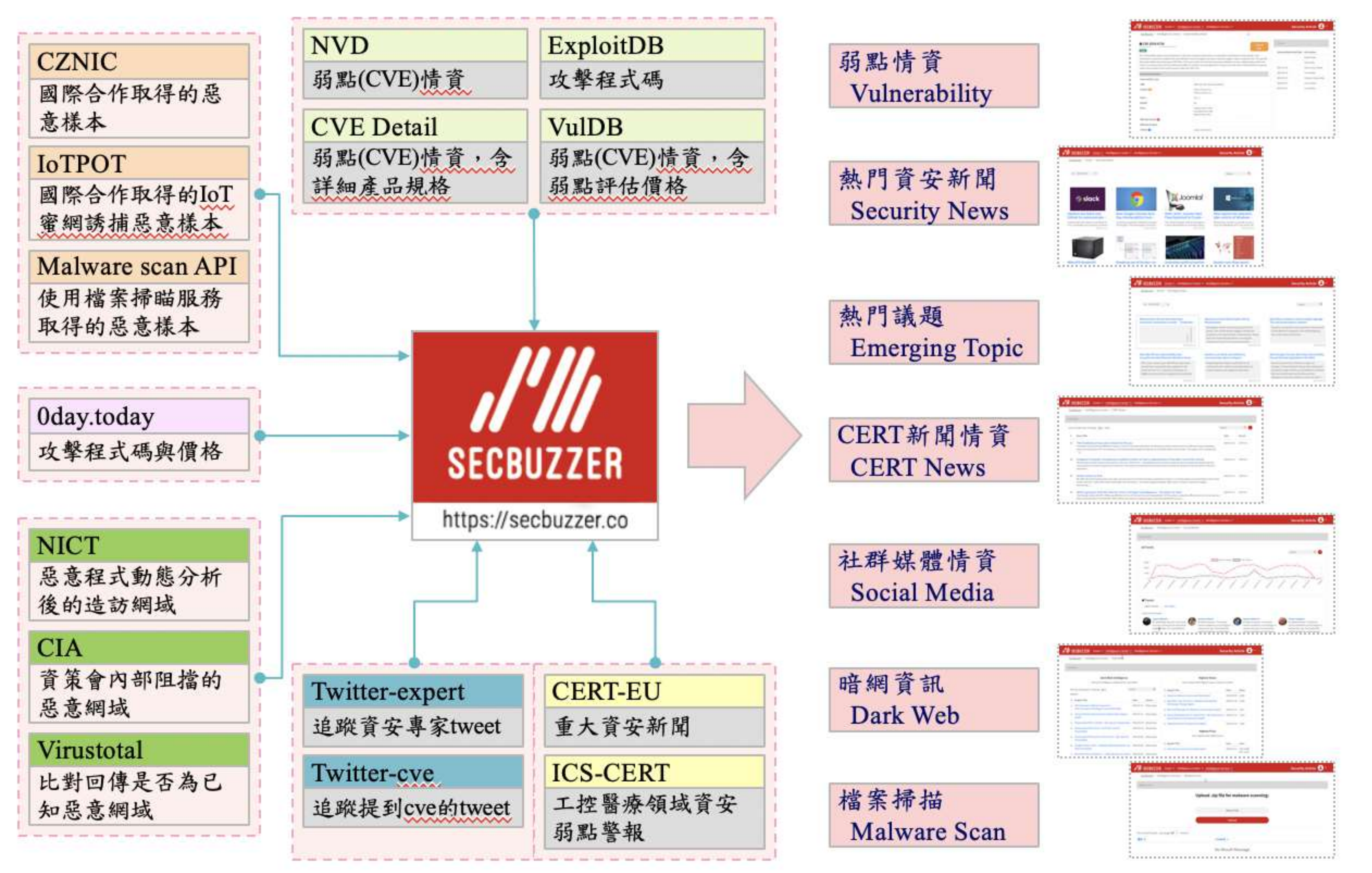
2019-08-29

文章分類數

工控 34	醫療 13
金融 14	5G 20
電商 9	政府 23
暗網 15	資安脈動 22

全站熱門標籤

SecBuzzer intelligence sources and functions



CZNIC
國際合作取得的惡意樣本

IoTPOT
國際合作取得的IoT蜜網誘捕惡意樣本

Malware scan API
使用檔案掃瞄服務取得的惡意樣本

0day.today
攻擊程式碼與價格

NICT
惡意程式動態分析後的造訪網域

CIA
資策會內部阻擋的惡意網域

Virustotal
比對回傳是否為已知惡意網域

NVD
弱點(CVE)情資

ExploitDB
攻擊程式碼

CVE Detail
弱點(CVE)情資，含詳細產品規格

VulDB
弱點(CVE)情資，含弱點評估價格

SECBUZZER
https://secbuzzer.co

Twitter-expert
追蹤資安專家tweet

Twitter-cve
追蹤提到cve的tweet

CERT-EU
重大資安新聞

ICS-CERT
工控醫療領域資安弱點警報

弱點情資
Vulnerability

熱門資安新聞
Security News

熱門議題
Emerging Topic

CERT新聞情資
CERT News

社群媒體情資
Social Media

暗網資訊
Dark Web

檔案掃描
Malware Scan

https://secbuzzer.co/

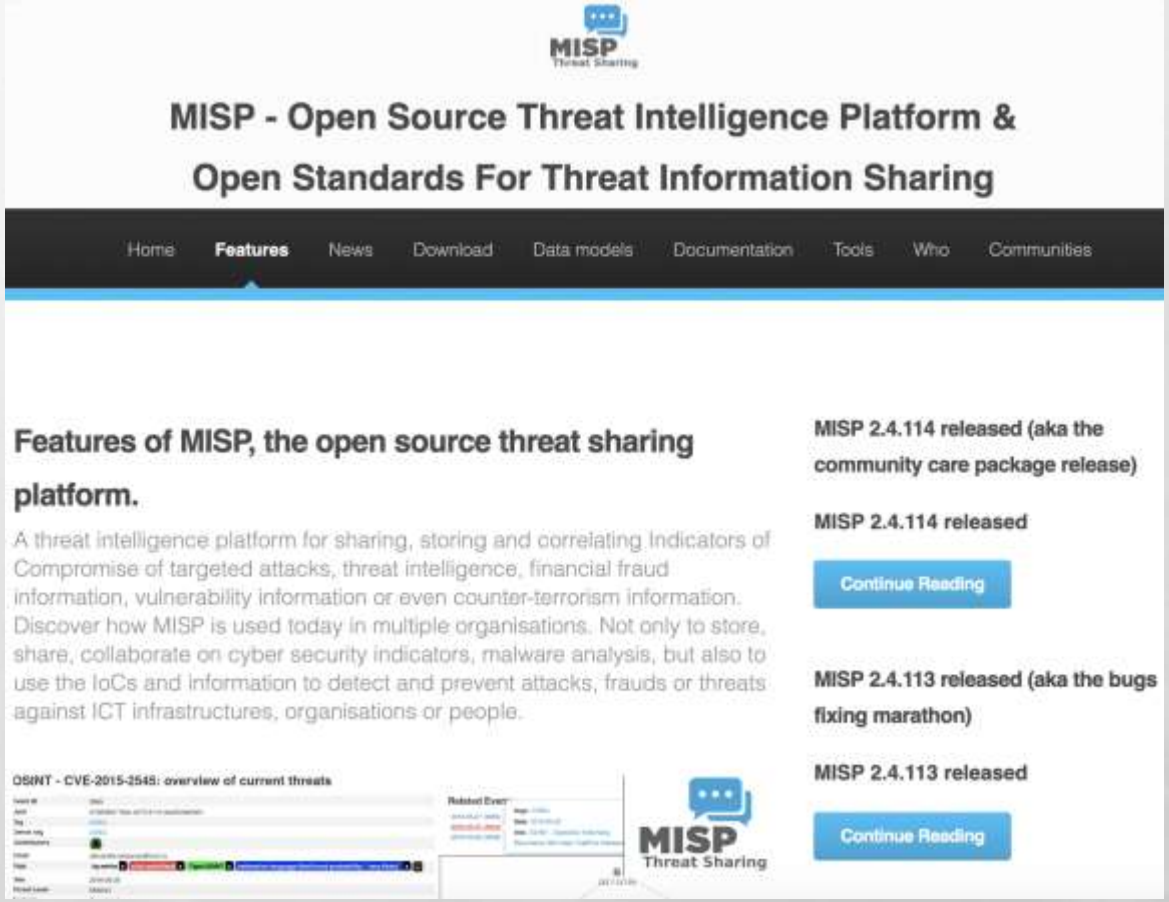
MISP

https://www.misp-project.org/features.html

- Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing

MISP is a threat information sharing free & open source software.

- MISP has a host of functionalities that assist users in creating, collaborating & sharing threat information - e.g. flexible sharing groups, automatic correlation, free-text import helper, event distribution & proposals.
- Many export formats which support IDSes / IPSes (e.g. Suricata, Bro, Snort), SIEMs (eg CEF), Host scanners (e.g. OpenIOC, STIX, CSV, yara), analysis tools (e.g. Maltego), DNS policies (e.g. RPZ).
- A rich set of MISP modules to add expansion, import and export functionalities.



MISP - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing

Features of MISP, the open source threat sharing platform.

A threat intelligence platform for sharing, storing and correlating Indicators of Compromise of targeted attacks, threat intelligence, financial fraud information, vulnerability information or even counter-terrorism information. Discover how MISP is used today in multiple organisations. Not only to store, share, collaborate on cyber security indicators, malware analysis, but also to use the IoCs and information to detect and prevent attacks, frauds or threats against ICT infrastructures, organisations or people.

OSINT - CVE-2015-2545: overview of current threats

MISP 2.4.114 released (aka the community care package release)

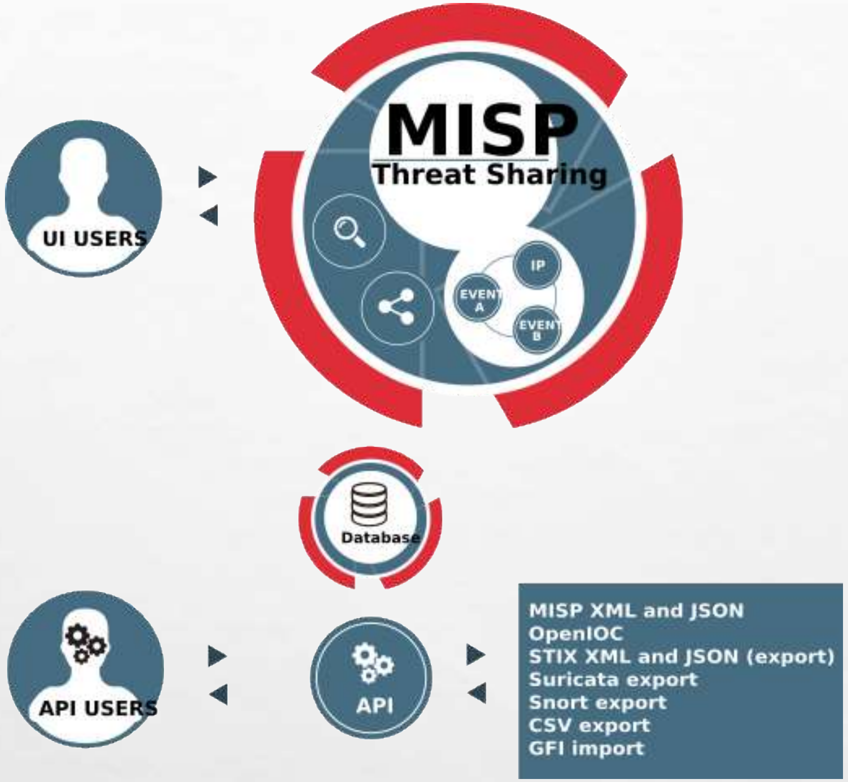
MISP 2.4.114 released

MISP 2.4.113 released (aka the bugs fixing marathon)

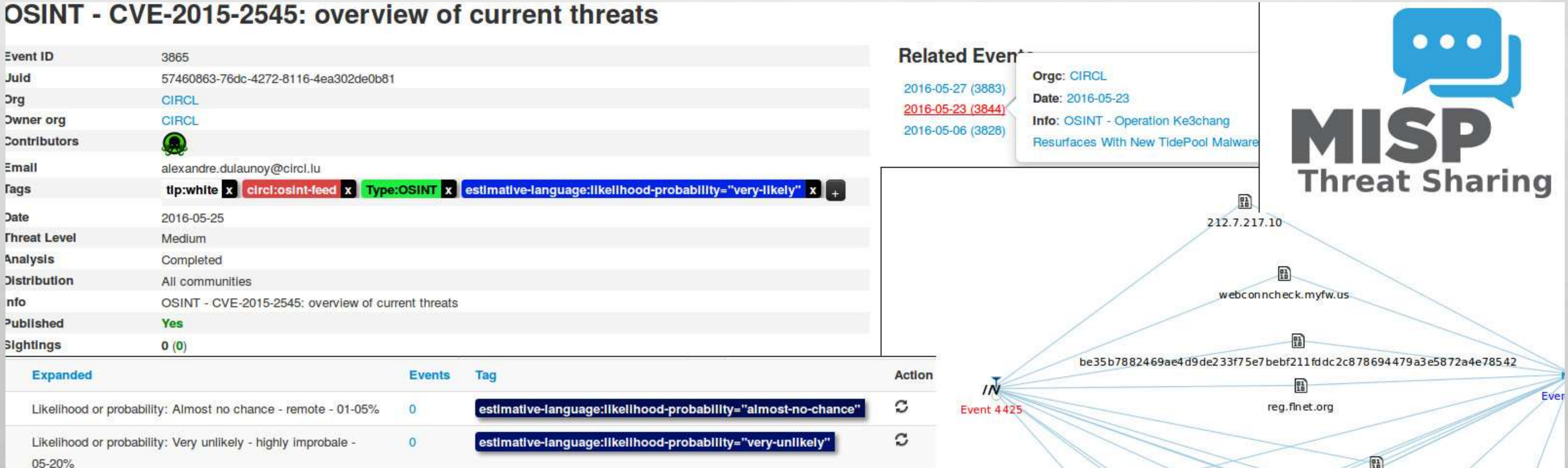
MISP 2.4.113 released

https://www.misp-project.org/features.html

MISP



MISP XML and JSON
OpenIOC
STIX XML and JSON (export)
Suricata export
Snort export
CSV export
GFI import



OSINT - CVE-2015-2545: overview of current threats

Event ID	3865
Juid	57460863-76dc-4272-8116-4ea302de0b81
Org	CIRCL
Owner org	CIRCL
Contributors	
Email	alexandre.dulaunoy@circl.lu
Tags	tlp:white x circl:osint-feed x Type:OSINT x estimative-language:likelihood-probability="very-likely" x +
Date	2016-05-25
Threat Level	Medium
Analysis	Completed
Distribution	All communities
nfo	OSINT - CVE-2015-2545: overview of current threats
Published	Yes
Sightings	0 (0)

Related Even

2016-05-27 (3883)
2016-05-23 (3844)
2016-05-06 (3828)

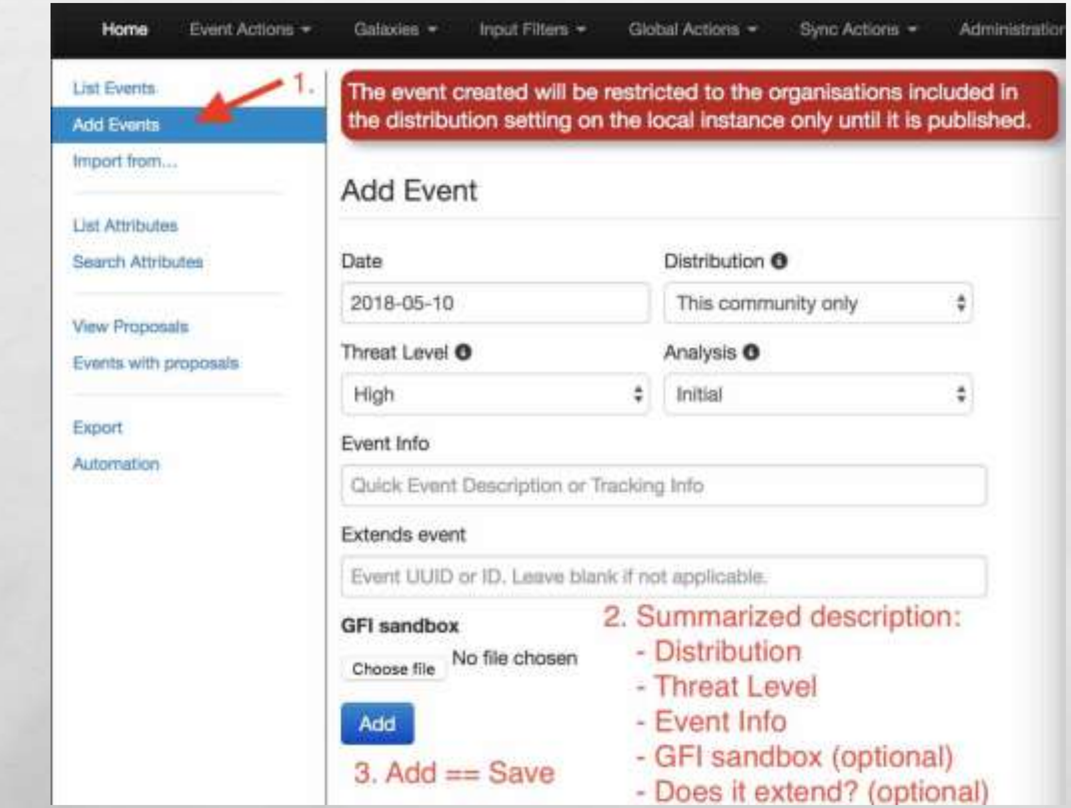
Orgc: CIRCL
Date: 2016-05-23
Info: OSINT - Operation Ke3chang Resurfaces With New TidePool Malware

Expanded	Events	Tag	Action
Likelihood or probability: Almost no chance - remote - 01-05%	0	estimative-language:likelihood-probability="almost-no-chance"	
Likelihood or probability: Very unlikely - highly improbale - 05-20%	0	estimative-language:likelihood-probability="very-unlikely"	

MISP

https://www.circl.lu/doc/misp/quick-start/

- Add event



The event created will be restricted to the organisations included in the distribution setting on the local instance only until it is published.

Date: 2018-05-10

Distribution: This community only

Threat Level: High

Analysis: Initial

Event Info: Quick Event Description or Tracking Info

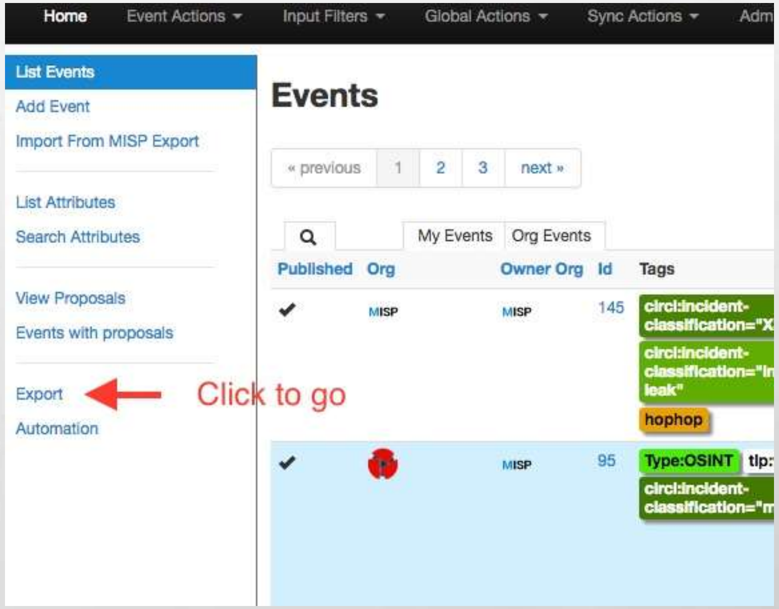
Extends event: Event UUID or ID. Leave blank if not applicable.

GFI sandbox

2. Summarized description:
- Distribution
- Threat Level
- Event Info
- GFI sandbox (optional)
- Does it extend? (optional)

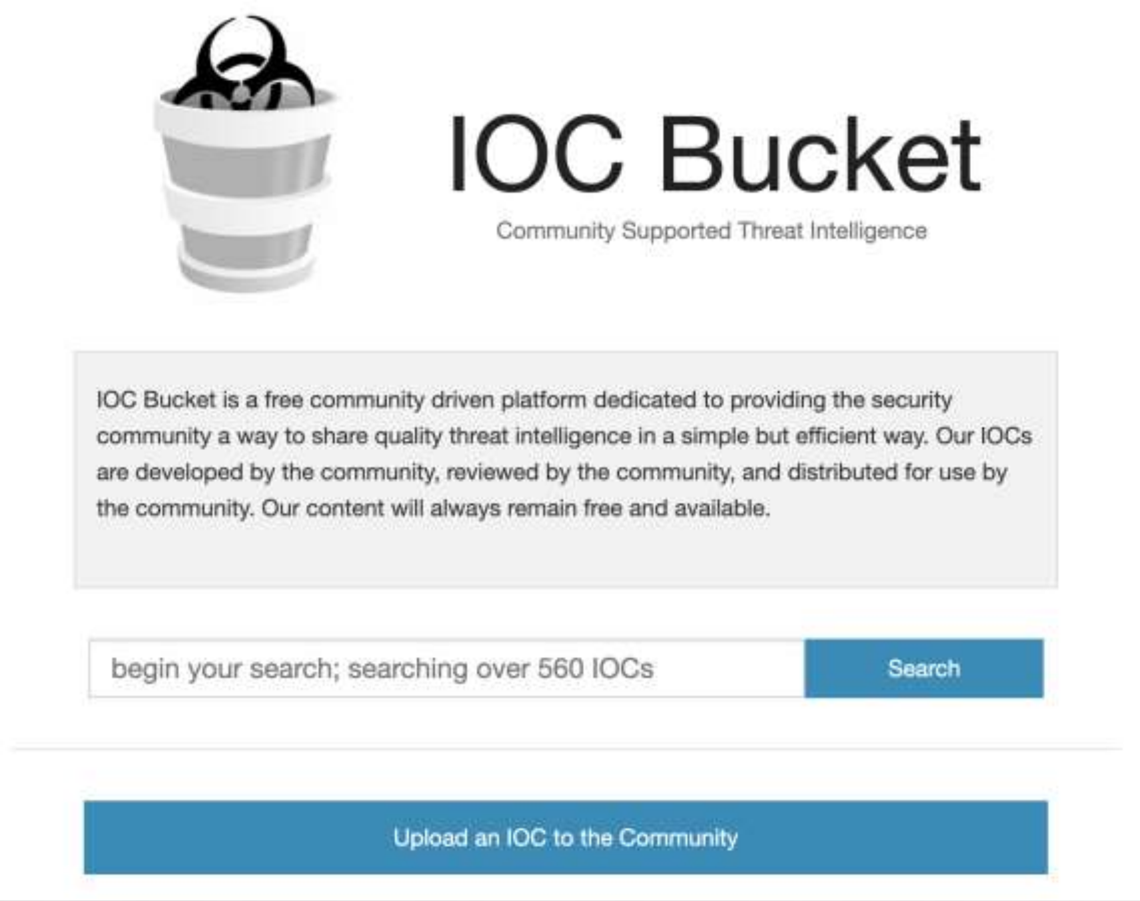
3. Add == Save

- Export Events for Log Search.
  - Export functionality is designed to automatically generate signatures for intrusion detection system.



Published	Org	Owner Org	Id	Tags
✓	MISP	MISP	145	circl:incident-classification="X circl:incident-classification="In leak" hophop
✓		MISP	95	Type:OSINT tlp: circl:incident-classification="m

IOC Bucket https://www.iocbucket.com/



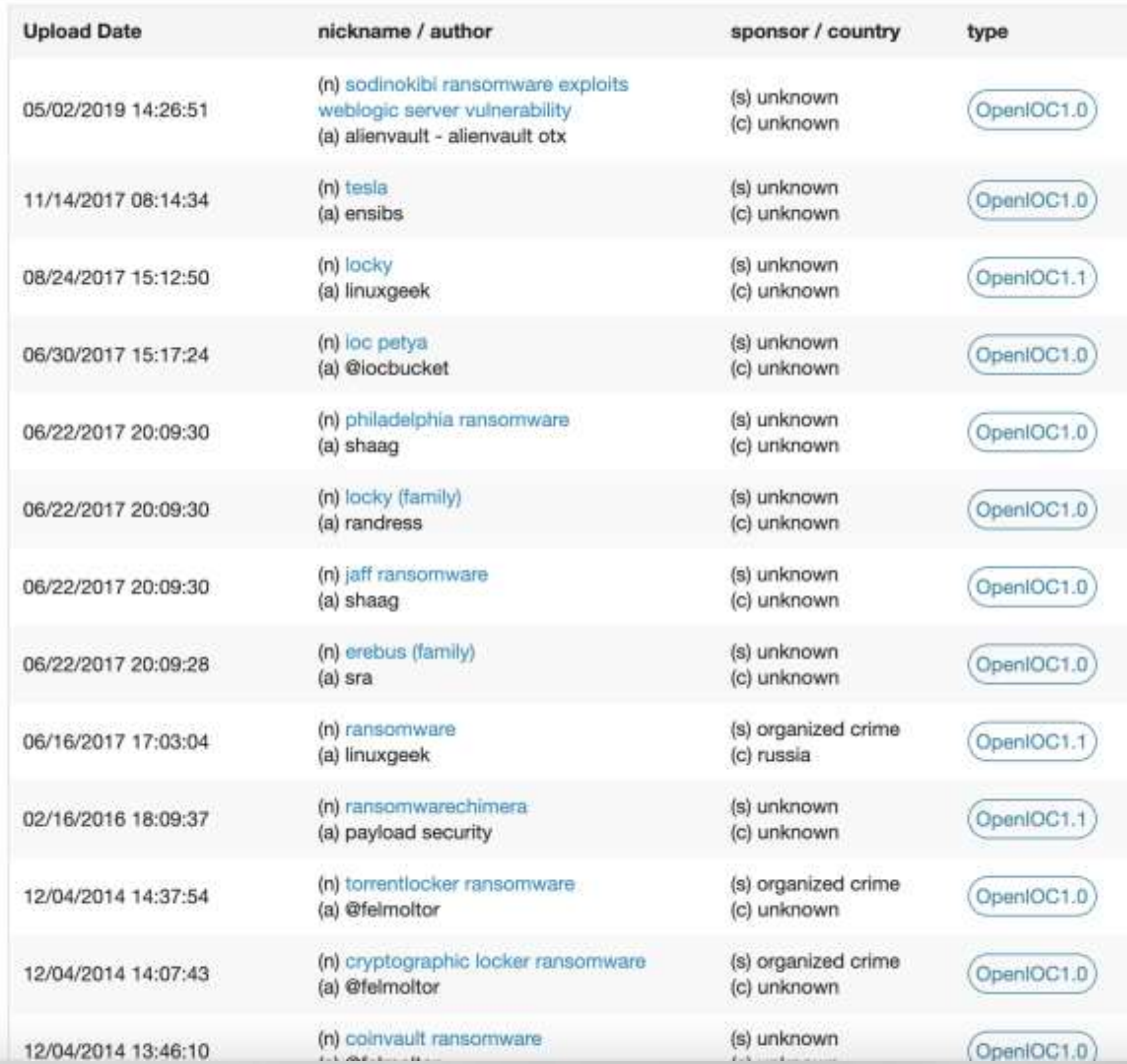
IOC Bucket

Community Supported Threat Intelligence

IOC Bucket is a free community driven platform dedicated to providing the security community a way to share quality threat intelligence in a simple but efficient way. Our IOCs are developed by the community, reviewed by the community, and distributed for use by the community. Our content will always remain free and available.

begin your search; searching over 560 IOCs
Search
Upload an IOC to the Community

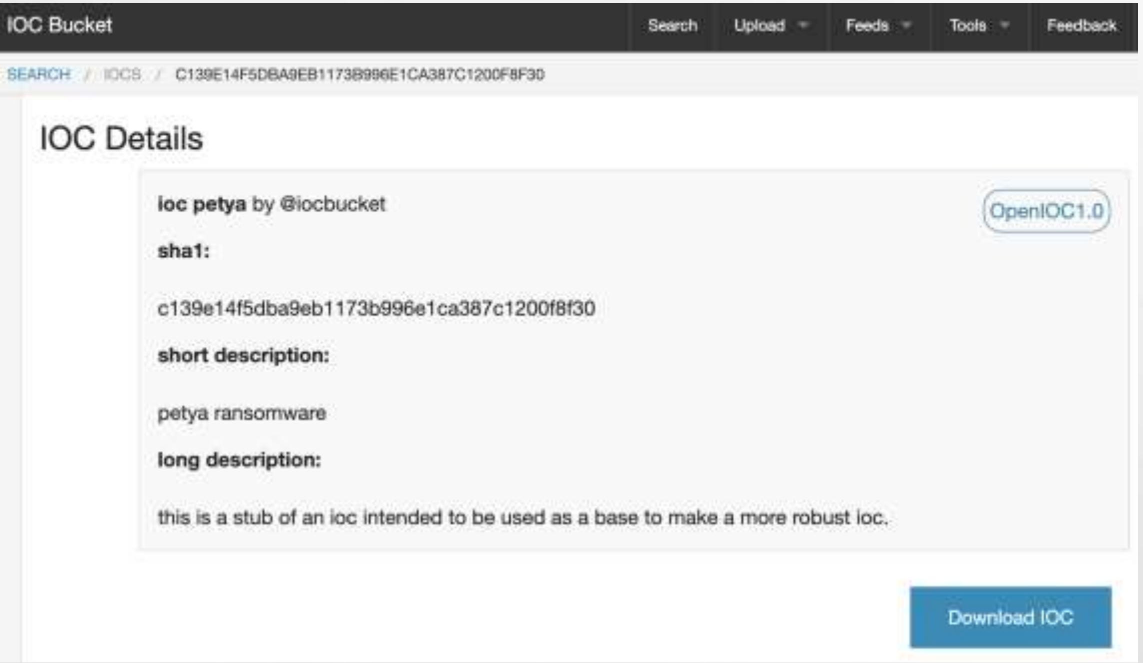
- Example: ransomware



Upload Date	nickname / author	sponsor / country	type
05/02/2019 14:26:51	(n) sodinokibi ransomware exploits weblogic server vulnerability (a) alienvault - alienvault otx	(s) unknown (c) unknown	OpenIOC1.0
11/14/2017 08:14:34	(n) tesla (a) ensibs	(s) unknown (c) unknown	OpenIOC1.0
08/24/2017 15:12:50	(n) locky (a) linuxgeek	(s) unknown (c) unknown	OpenIOC1.1
06/30/2017 15:17:24	(n) ioc petya (a) @iocbucket	(s) unknown (c) unknown	OpenIOC1.0
06/22/2017 20:09:30	(n) philadelphia ransomware (a) shaag	(s) unknown (c) unknown	OpenIOC1.0
06/22/2017 20:09:30	(n) locky (family) (a) randress	(s) unknown (c) unknown	OpenIOC1.0
06/22/2017 20:09:30	(n) jaff ransomware (a) shaag	(s) unknown (c) unknown	OpenIOC1.0
06/22/2017 20:09:28	(n) erebus (family) (a) sra	(s) unknown (c) unknown	OpenIOC1.0
06/16/2017 17:03:04	(n) ransomware (a) linuxgeek	(s) organized crime (c) russia	OpenIOC1.1
02/16/2016 18:09:37	(n) ransomwarechimera (a) payload security	(s) unknown (c) unknown	OpenIOC1.1
12/04/2014 14:37:54	(n) torrentlocker ransomware (a) @felmoltor	(s) organized crime (c) unknown	OpenIOC1.0
12/04/2014 14:07:43	(n) cryptographic locker ransomware (a) @felmoltor	(s) organized crime (c) unknown	OpenIOC1.0
12/04/2014 13:46:10	(n) coinvault ransomware	(s) unknown	OpenIOC1.0

Part 2: 資安威脅情資處理 -威脅情蒐

IOC Bucket https://www.iocbucket.com/



IOC Details

ioc petya by @iocbucket

sha1:

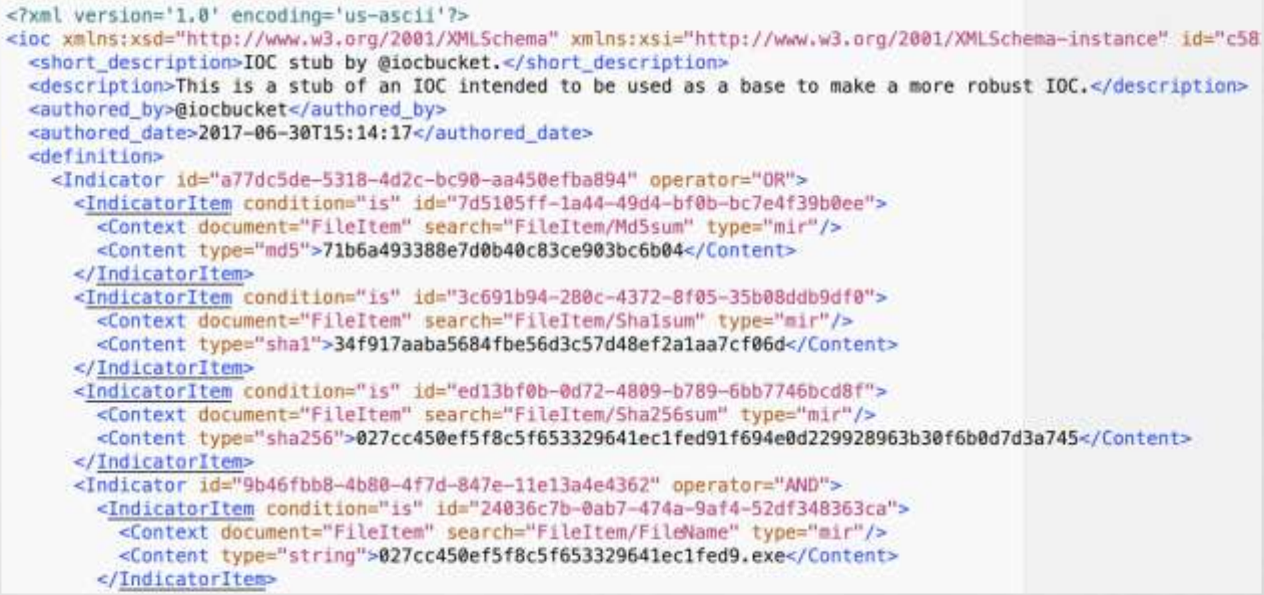
c139e14f5dba9eb1173b996e1ca387c1200f8f30

short description:

petya ransomware

long description:

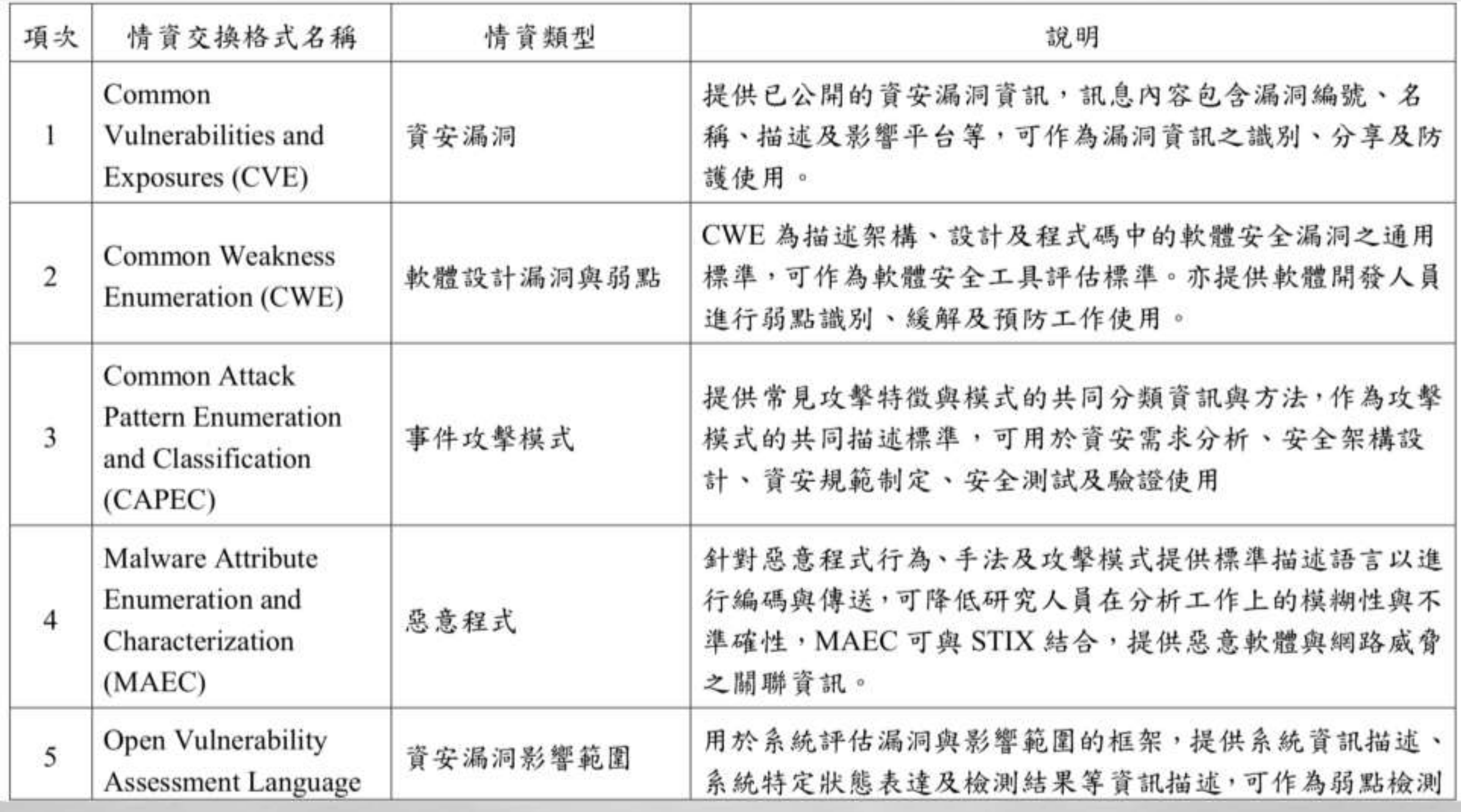
this is a stub of an ioc intended to be used as a base to make a more robust ioc.



```
<?xml version='1.0' encoding='us-ascii'?>
<ioc xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" id="c58
  <short_description>IOC stub by @iocbucket.</short_description>
  <description>This is a stub of an IOC intended to be used as a base to make a more robust IOC.</description>
  <authored_by>@iocbucket</authored_by>
  <authored_date>2017-06-30T15:14:17</authored_date>
  <definition>
    <Indicator id="a77dc5de-5318-4d2c-bc90-aa450efba894" operator="OR">
      <IndicatorItem condition="is" id="7d5105ff-1a44-49d4-bf0b-bc7e4f39b0ee">
        <Context document="FileItem" search="FileItem/Md5sum" type="mir"/>
        <Content type="md5">71b6a493388e7d0b40c83ce903bc6b04</Content>
      </IndicatorItem>
      <IndicatorItem condition="is" id="3c691b94-280c-4372-8f05-35b08ddb9df0">
        <Context document="FileItem" search="FileItem/Sha1sum" type="mir"/>
        <Content type="sha1">34f917aaba5684fbe56d3c57d48ef2a1aa7cf06d</Content>
      </IndicatorItem>
      <IndicatorItem condition="is" id="ed13bf0b-0d72-4809-b789-6bb7746bcd8f">
        <Context document="FileItem" search="FileItem/Sha256sum" type="mir"/>
        <Content type="sha256">027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745</Content>
      </IndicatorItem>
      <Indicator id="9b46fbb8-4b80-4f7d-847e-11e13a4e4362" operator="AND">
        <IndicatorItem condition="is" id="24036c7b-0ab7-474a-9af4-52df348363ca">
          <Context document="FileItem" search="FileItem/FileName" type="mir"/>
          <Content type="string">027cc450ef5f8c5f653329641ec1fed9.exe</Content>
        </IndicatorItem>
```

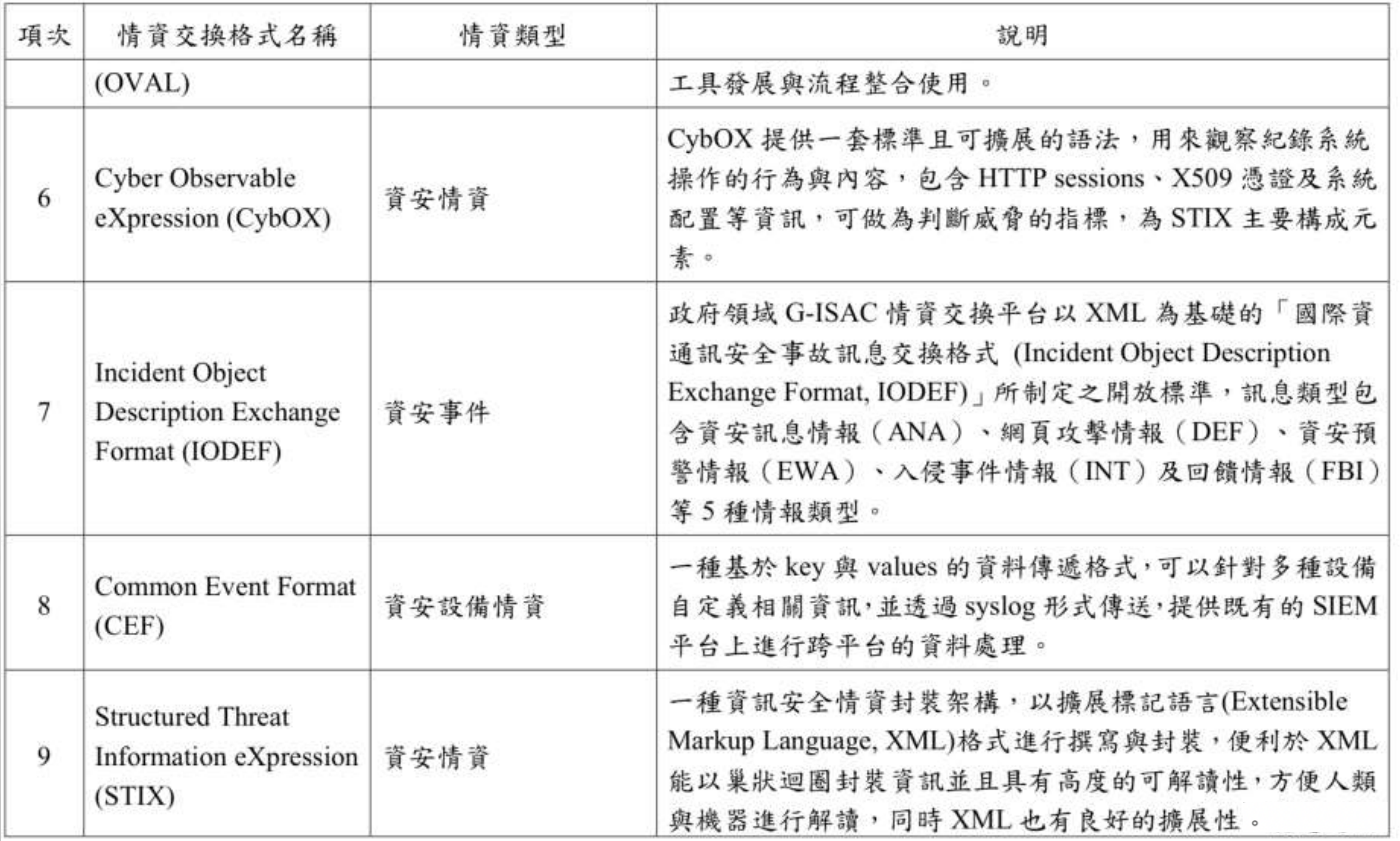
Other tools:
ioc-explorer
https://github.com/lion-gu/ioc-explorer
Awesome-osint
https://github.com/jivoi/awesome-osint

行政院資通安全處通用之情資交換格式



項次	情資交換格式名稱	情資類型	說明
1	Common Vulnerabilities and Exposures (CVE)	資安漏洞	提供已公開的資安漏洞資訊，訊息內容包含漏洞編號、名稱、描述及影響平台等，可作為漏洞資訊之識別、分享及防護使用。
2	Common Weakness Enumeration (CWE)	軟體設計漏洞與弱點	CWE 為描述架構、設計及程式碼中的軟體安全漏洞之通用標準，可作為軟體安全工具評估標準。亦提供軟體開發人員進行弱點識別、緩解及預防工作使用。
3	Common Attack Pattern Enumeration and Classification (CAPEC)	事件攻擊模式	提供常見攻擊特徵與模式的共同分類資訊與方法，作為攻擊模式的共同描述標準，可用於資安需求分析、安全架構設計、資安規範制定、安全測試及驗證使用
4	Malware Attribute Enumeration and Characterization (MAEC)	惡意程式	針對惡意程式行為、手法及攻擊模式提供標準描述語言以進行編碼與傳送，可降低研究人員在分析工作上的模糊性與不準確性，MAEC 可與 STIX 結合，提供惡意軟體與網路威脅之關聯資訊。
5	Open Vulnerability Assessment Language	資安漏洞影響範圍	用於系統評估漏洞與影響範圍的框架，提供系統資訊描述、系統特定狀態表達及檢測結果等資訊描述，可作為弱點檢測

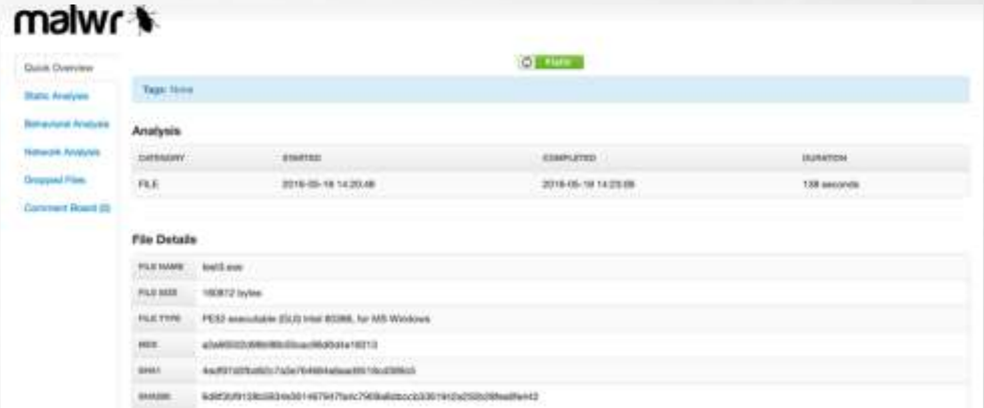
行政院資通安全處通用之情資交換格式



項次	情資交換格式名稱	情資類型	說明
	(OVAL)		工具發展與流程整合使用。
6	Cyber Observable eXpression (CybOX)	資安情資	CybOX 提供一套標準且可擴展的語法，用來觀察紀錄系統操作的行為與內容，包含 HTTP sessions、X509 憑證及系統配置等資訊，可做為判斷威脅的指標，為 STIX 主要構成元素。
7	Incident Object Description Exchange Format (IODEF)	資安事件	政府領域 G-ISAC 情資交換平台以 XML 為基礎的「國際資通訊安全事故訊息交換格式 (Incident Object Description Exchange Format, IODEF)」所制定之開放標準，訊息類型包含資安訊息情報（ANA）、網頁攻擊情報（DEF）、資安預警情報（EWA）、入侵事件情報（INT）及回饋情報（FBI）等 5 種情報類型。
8	Common Event Format (CEF)	資安設備情資	一種基於 key 與 values 的資料傳遞格式，可以針對多種設備自定義相關資訊，並透過 syslog 形式傳送，提供既有的 SIEM 平台上進行跨平台的資料處理。
9	Structured Threat Information eXpression (STIX)	資安情資	一種資訊安全情資封裝架構，以擴展標記語言(Extensible Markup Language, XML)格式進行撰寫與封裝，便利於 XML 能以巢狀迴圈封裝資訊並且具有高度的可解讀性，方便人類與機器進行解讀，同時 XML 也有良好的擴展性。

Part 2: 資安威脅情資處理 -威脅情蒐

- VirusTotal (https://www.virustotal.com)，線上檔案/IP/domain掃瞄
- Malwr (https://malwr.com/)，線上沙箱
- AlienVault Open Threat Exchange (https://www.alienvault.com/open-threat-exchange) 安全專家會分享發現的APT攻擊軌跡IOC or YARA等



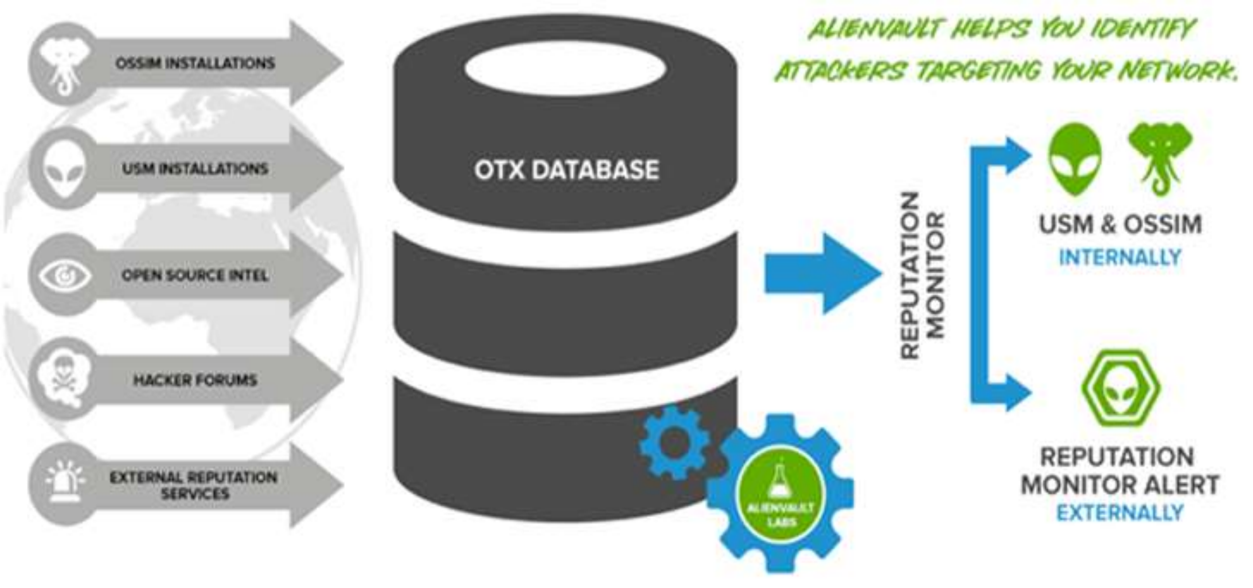
Tags: None

Analysis

CATEGORY	STARTED	COMPLETED	DURATION
FILE	2016-05-18 14:20:48	2016-05-18 14:23:06	138 seconds

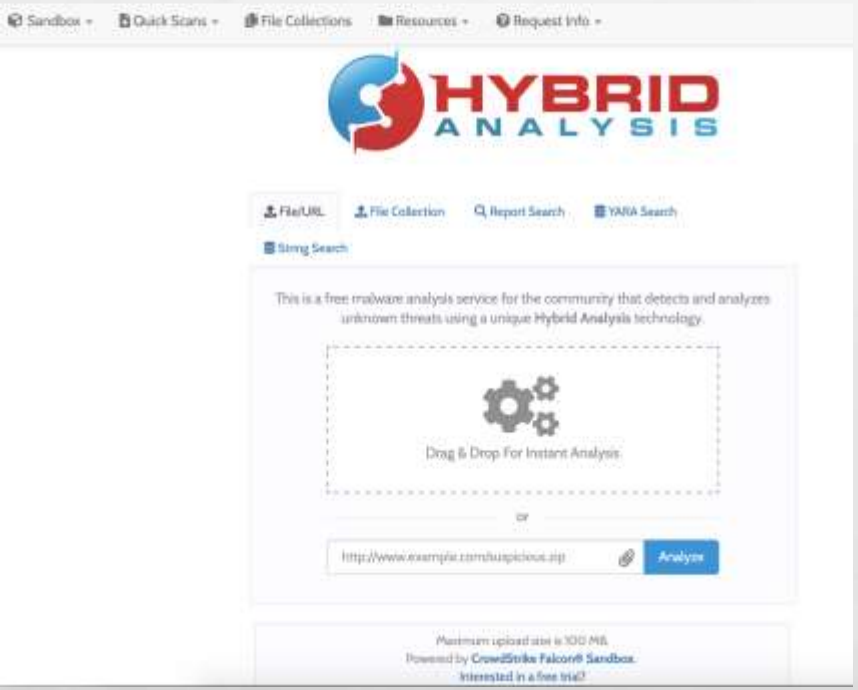
File Details

FILE NAME	[illegible]
FILE SIZE	180872 bytes
FILE TYPE	PE32 executable (DLL) Intel 80386, for MS Windows
MD5	[illegible]
SHA1	[illegible]
SHA256	[illegible]



Part 2: 資安威脅情資處理 -威脅情蒐

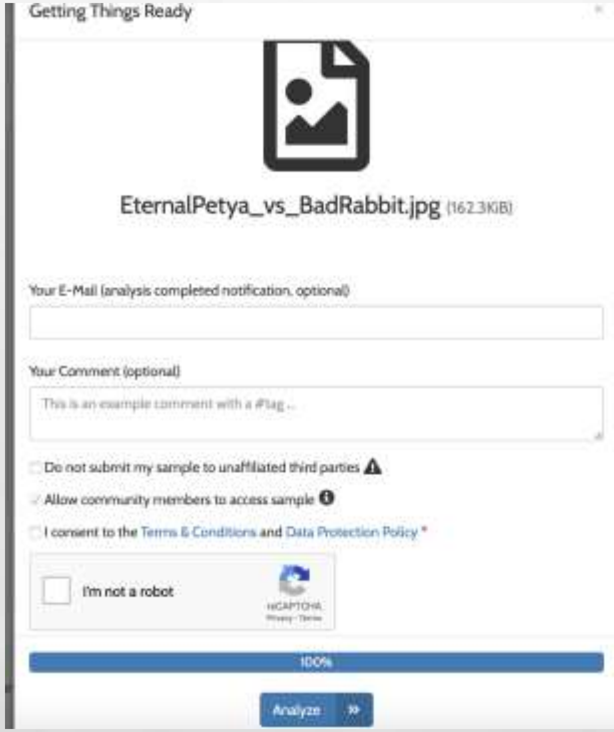
- Hybrid-Analysis (https://www.hybrid-analysis.com)，線上檔案/IP/domain掃瞄



This is a free malware analysis service for the community that detects and analyzes unknown threats using a unique **Hybrid Analysis** technology.

Drag & Drop For Instant Analysis
or
http://www.example.com/suspicious.zip
Analyze

Maximum upload size is 100 MiB.
Powered by CrowdStrike Falcon® Sandbox.
Interested in a free trial?


Getting Things Ready

EternalPetya_vs_BadRabbit.jpg (162.3KiB)

Your E-Mail (analysis completed notification, optional)

Your Comment (optional)

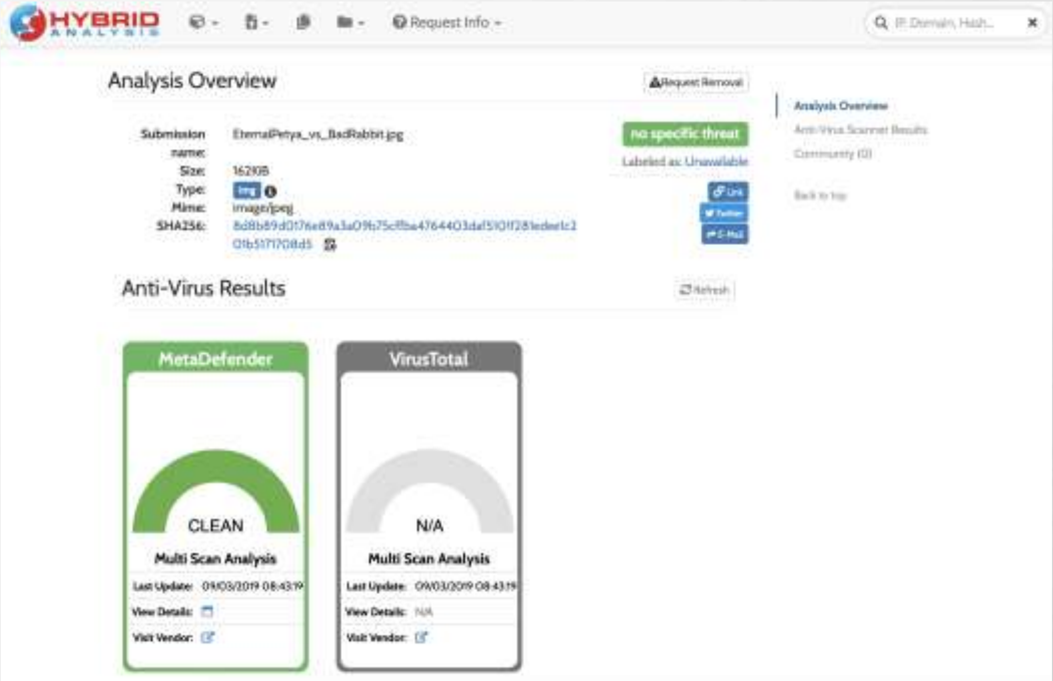
This is an example comment with a #tag ...

□ Do not submit my sample to unaffiliated third parties

✓ Allow community members to access sample

□ I consent to the Terms & Conditions and Data Protection Policy *

□ I'm not a robot



Analysis Overview

Submission name: EternalPetya_vs_BadRabbit.jpg
Size: 162KiB
Type: img
Mime: image/jpeg
SHA256: 8d8b89d0176e89a3a09fb75cf8ba4764403daf5101f28ledeelc3 01b5171708d5

no specific threat
Labeled as: Unavailable

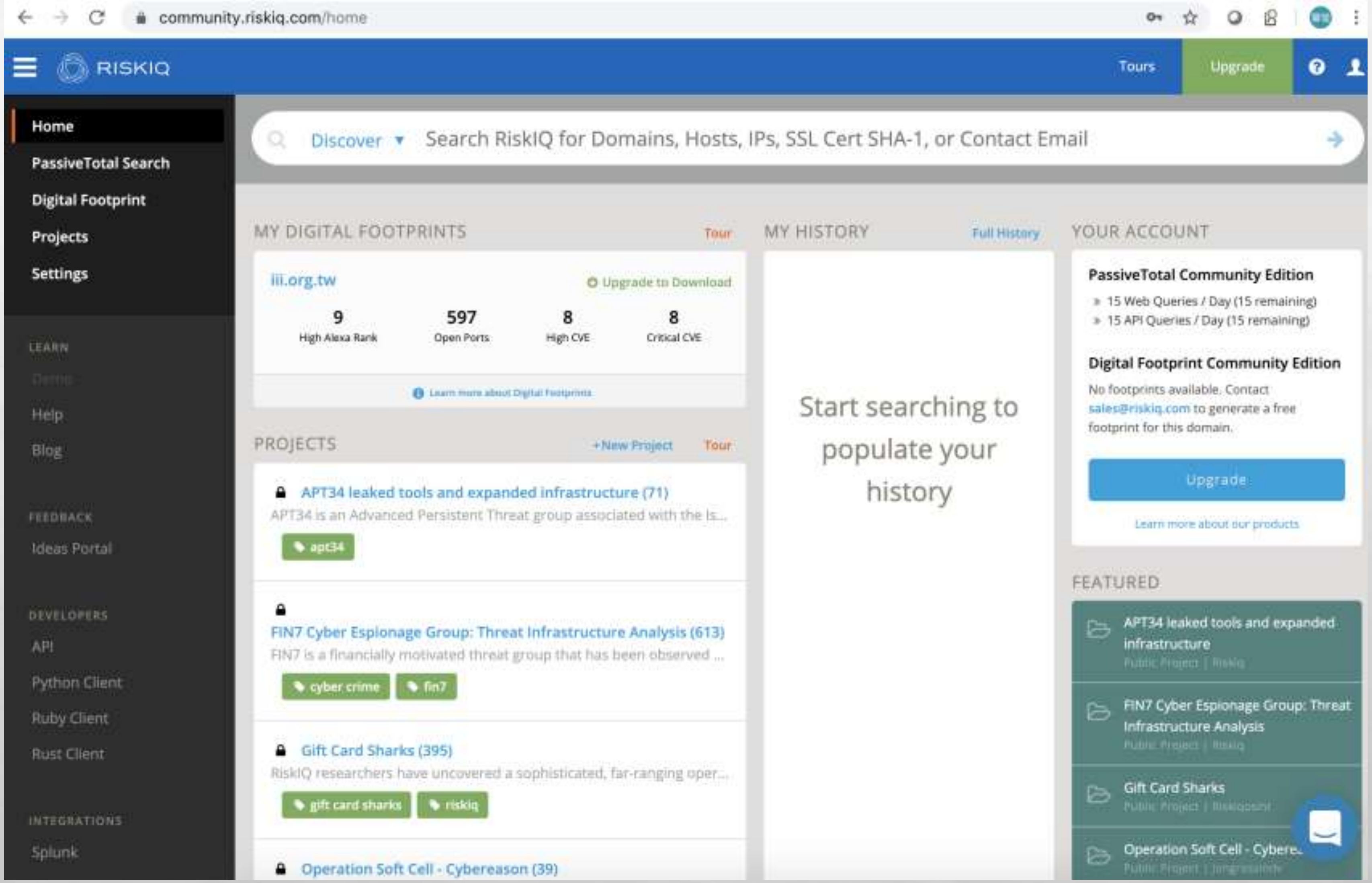
Anti-Virus Results

MetaDefender
CLEAN
Multi Scan Analysis
Last Update: 09/03/2019 08:43:19
View Details:
Visit Vendor:

VirusTotal
N/A
Multi Scan Analysis
Last Update: 09/03/2019 08:43:19
View Details: N/A
Visit Vendor:

Part 2: 資安威脅情資處理 -威脅情蒐

- RiskIQ (https://community.riskiq.com/search)



community.riskiq.com/home

RISKIQ

Search RiskIQ for Domains, Hosts, IPs, SSL Cert SHA-1, or Contact Email

MY DIGITAL FOOTPRINTS

iii.org.tw

Upgrade to Download

9	597	8	8
High Alexa Rank	Open Ports	High CVE	Critical CVE

Learn more about Digital Footprints

PROJECTS

APT34 leaked tools and expanded infrastructure (71)

APT34 is an Advanced Persistent Threat group associated with the Is...

apt34

FIN7 Cyber Espionage Group: Threat Infrastructure Analysis (613)

FIN7 is a financially motivated threat group that has been observed ...

cyber crime | fin7

Gift Card Sharks (395)

RiskIQ researchers have uncovered a sophisticated, far-ranging oper...

gift card sharks | riskiq

Operation Soft Cell - Cybereason (39)

MY HISTORY

Start searching to populate your history

YOUR ACCOUNT

PassiveTotal Community Edition

- 15 Web Queries / Day (15 remaining)
- 15 API Queries / Day (15 remaining)

Digital Footprint Community Edition

No footprints available. Contact sales@riskiq.com to generate a free footprint for this domain.

Learn more about our products

FEATURED

APT34 leaked tools and expanded infrastructure
Public Project | RiskIQ

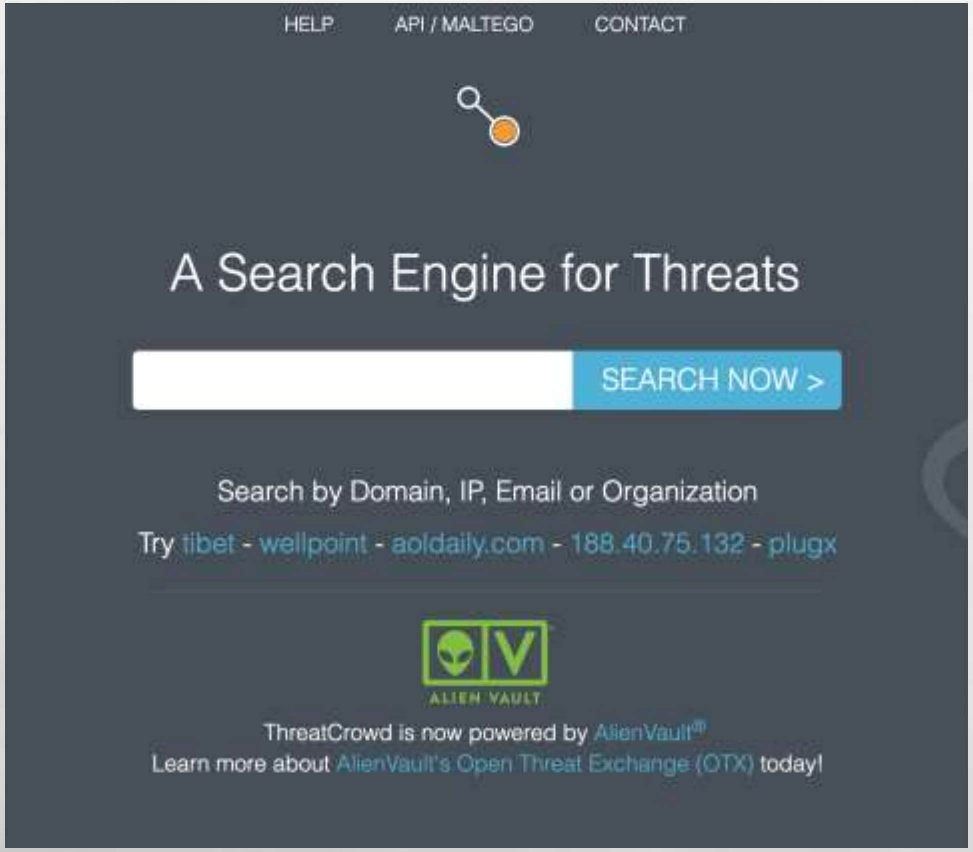
FIN7 Cyber Espionage Group: Threat Infrastructure Analysis
Public Project | RiskIQ

Gift Card Sharks
Public Project | RiskIQOSINT

Operation Soft Cell - Cyberea
Public Project | [illegible]

Part 2: 資安威脅情資處理 -威脅情蒐

- ThreatCrowd (https://www.threatcrowd.org/)

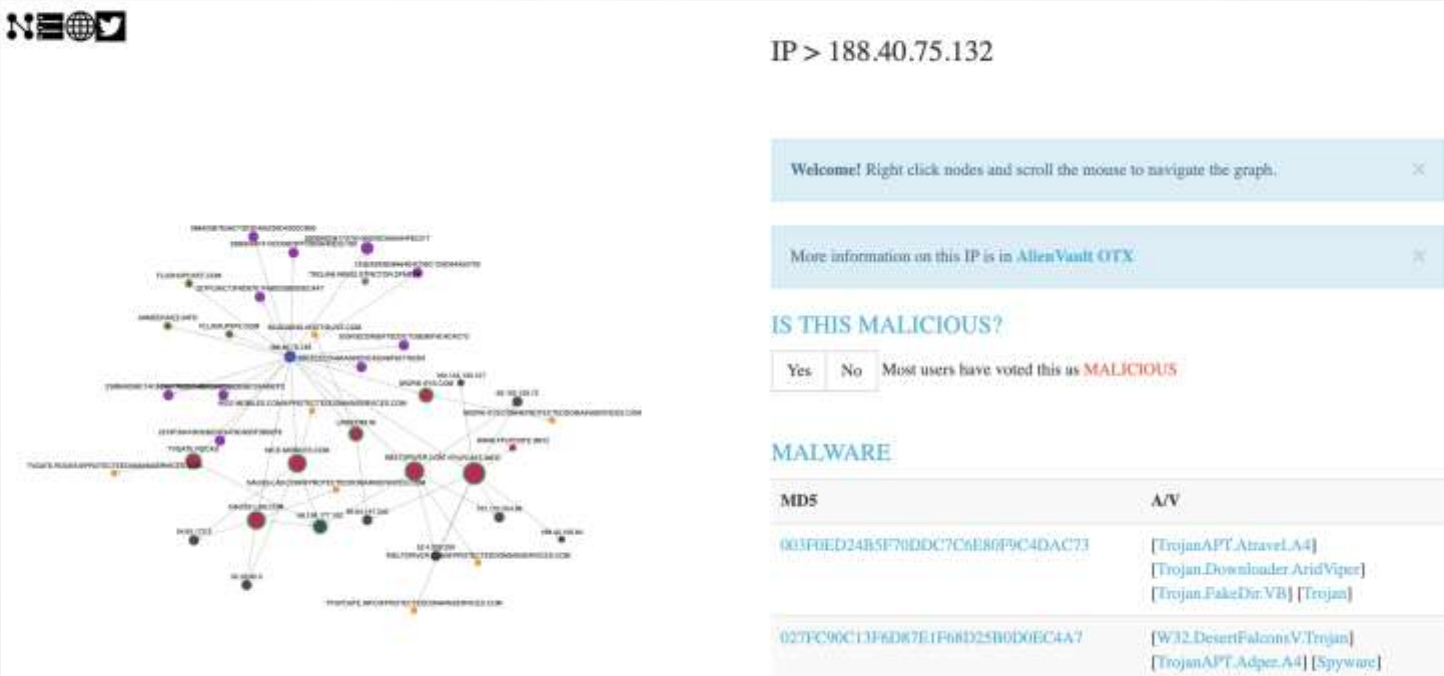


A Search Engine for Threats

Search by Domain, IP, Email or Organization

Try tibet - wellpoint - aoldaily.com - 188.40.75.132 - plugx

ThreatCrowd is now powered by AlienVault®
Learn more about AlienVault's Open Threat Exchange (OTX) today!



IP > 188.40.75.132

Welcome! Right click nodes and scroll the mouse to navigate the graph.

More information on this IP is in AlienVault OTX

IS THIS MALICIOUS?

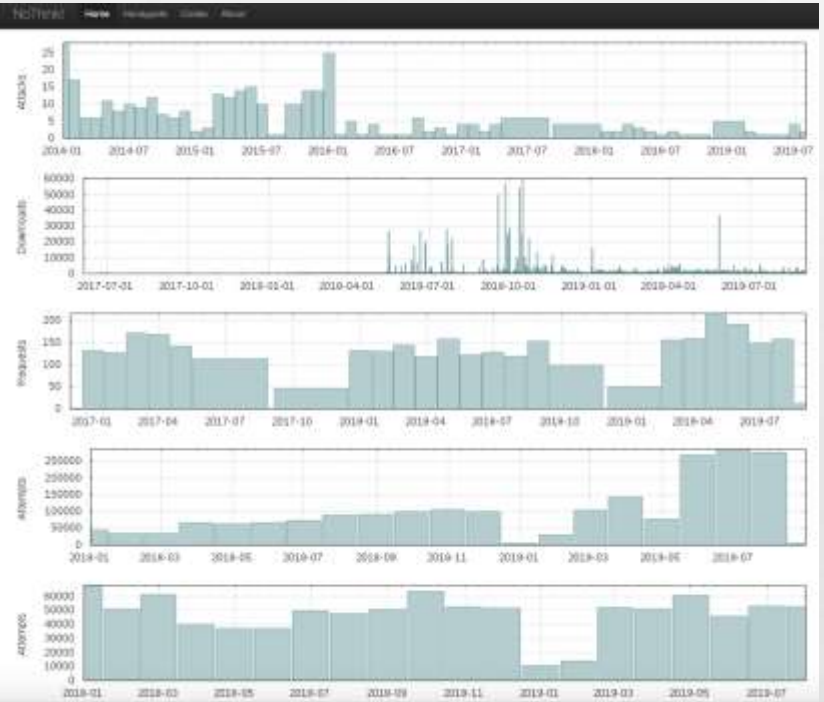
Yes No Most users have voted this us MALICIOUS

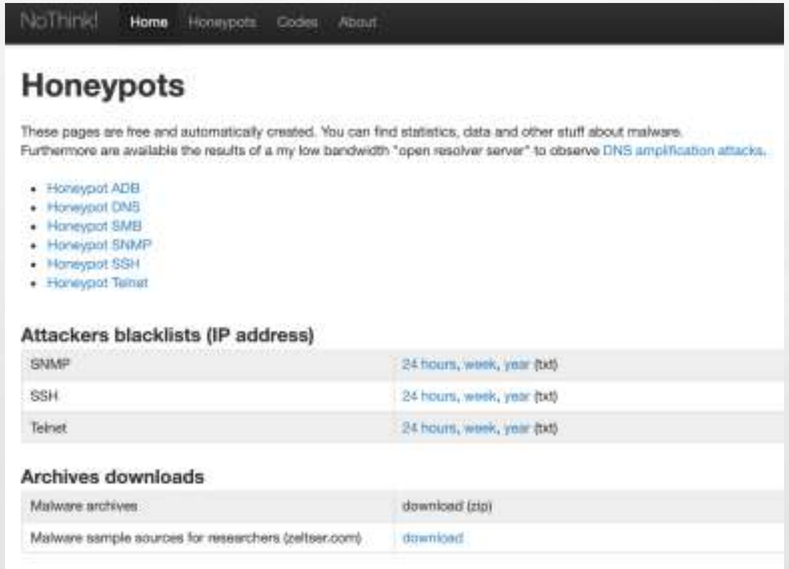
MALWARE

MD5	A/V
003F0ED24B5F70DDC7C6E80F9C4DAC73	[TrojanAPT.Atravel.A4] [Trojan.Downloader.AridViper] [Trojan.FakeDir.VB] [Trojan]
027FC90C13F6D87E1F68D25B0D0EC4A7	[W32.DesertFalconsV.Trojan] [TrojanAPT.Adpez.A4] [Spyware]

Part 2: 資安威脅情資處理 -威脅情蒐

- NoThink! (http://www.nothink.org/index.php)





Honeypots

These pages are free and automatically created. You can find statistics, data and other stuff about malware.
Furthermore are available the results of a my low bandwidth "open resolver server" to observe DNS amplification attacks.

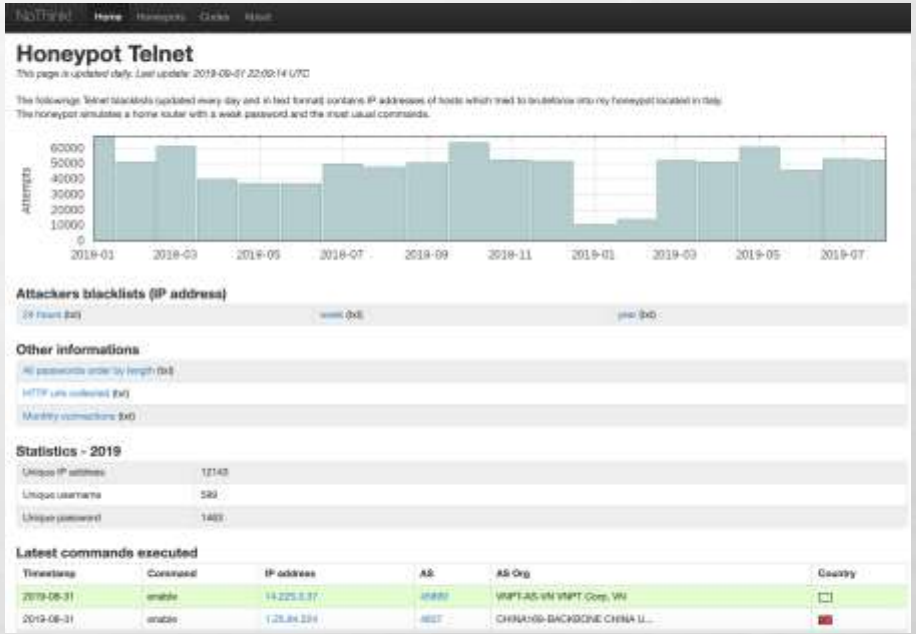
- Honeypot ADB
- Honeypot DNS
- Honeypot SMB
- Honeypot SNMP
- Honeypot SSH
- Honeypot Telnet

Attackers blacklists (IP address)

SNMP	24 hours, week, year (txt)
SSH	24 hours, week, year (txt)
Telnet	24 hours, week, year (txt)

Archives downloads

Malware archives	download (zip)
Malware sample sources for researchers (zeltser.com)	download



Honeypot Telnet

This page is updated daily. Last update: 2019-09-01 22:09:14 UTC

The following Telnet blacklists (updated every day and in text format) contains IP addresses of hosts which tried to bruteforce into my honeypot located in Italy.
The honeypot simulates a home router with a weak password and the most usual commands.

Attackers blacklists (IP address)

24 hours (txt)	week (txt)	year (txt)

Other informations

All passwords order by length (txt)
HTTP urls collected (txt)
Monthly connections (txt)

Statistics - 2019

Unique IP address	12143
Unique username	589
Unique password	1483

Latest commands executed

Timestamp	Command	IP address	AS	AS Org	Country
2019-08-31	enable	14.225.3.37	45899	VNPT-AS-VN VNPT Corp, VN	□
2019-08-31	enable	1.25.84.224	4837	CHINA169-BACKBONE CHINA U...	■

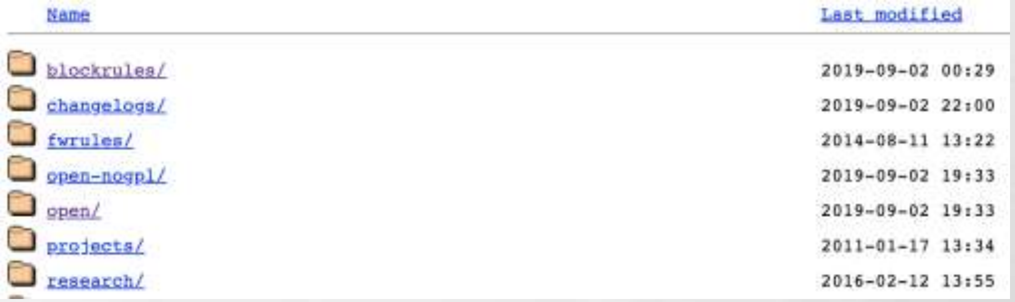
黑名單相關

- Vxvault (http://vxvault.net/ViriList.php)
- Emergingthreats (https://rules.emergingthreats.net/)
- feodotracker.abuse.ch (https://feodotracker.abuse.ch)
- The SSL Blacklist (https://sslbl.abuse.ch/)
- Spamhaus (https://www.spamhaus.org/)

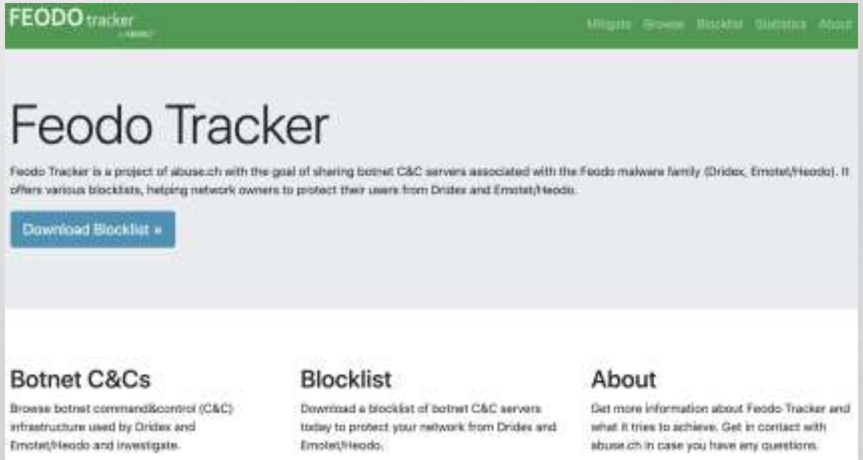
釣魚網站

- Openphish (https://openphish.com)
- PhiskTank (https://www.phishtank.com/phish_archive.php)

Date	URL	MD5	IP	Tools
09-03	[D] 5.56.133.111/[illegible].exe	[illegible]	5.56.133.111	[illegible]
09-03	[D] [illegible]	[illegible]	208.115.234.234	[illegible]
09-03	[D] [illegible]	[illegible]	208.115.234.234	[illegible]
09-03	[D] background.pl/[illegible].exe	[illegible]	[illegible]	[illegible]
09-02	[D] 5.182.39.203/setup.exe	[illegible]	5.182.39.203	[illegible]
09-02	[D] [illegible]	[illegible]	208.115.234.234	[illegible]



Name	Last modified
blockrules/	2019-09-02 00:29
changelogs/	2019-09-02 22:00
fwrules/	2014-08-11 13:22
open-nogpl/	2019-09-02 19:33
open/	2019-09-02 19:33
projects/	2011-01-17 13:34
research/	2016-02-12 13:55



Feodo Tracker

Feodo Tracker is a project of abuse.ch with the goal of sharing botnet C&C servers associated with the Feodo malware family (Dridex, Emotet/Heodo). It offers various blocklists, helping network owners to protect their users from Dridex and Emotet/Heodo.

Botnet C&Cs

Browse botnet command&control (C&C) infrastructure used by Dridex and Emotet/Heodo and investigate.

Blocklist

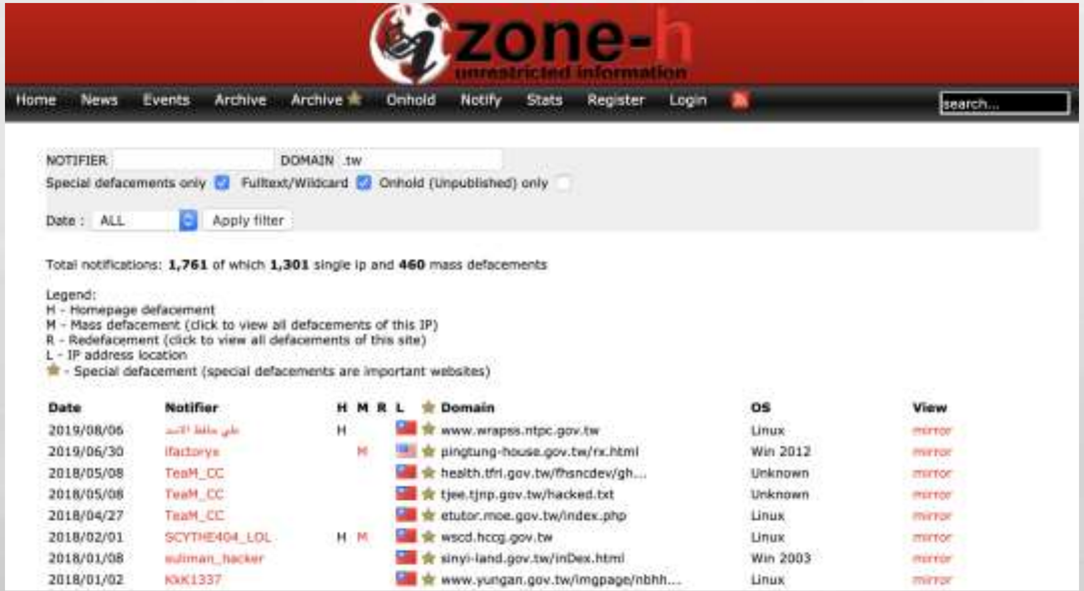
Download a blocklist of botnet C&C servers today to protect your network from Dridex and Emotet/Heodo.

About

Get more information about Feodo Tracker and what it tries to achieve. Get in contact with abuse.ch in case you have any questions.

黑名單相關

- MXToolbox (https://mxtoolbox.com/blacklists.aspx)
- DNSBL (https://www.dnsbl.info/)
- Online Mail Server Blacklist Checker (http://mail-blacklist-checker.online-domain-tools.com/)
- Zone-h (http://www.zone-h.org/archive?hz=1)



NOTIFIER DOMAIN .tw
Special defacements only ☑ Fulltext/Wildcard ☑ Onhold (Unpublished) only □

Date : ALL Apply filter

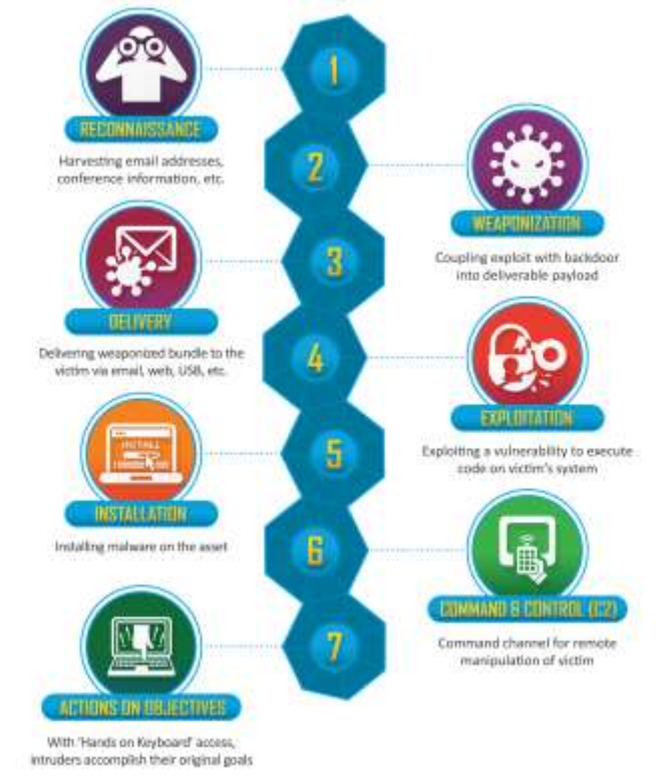
Total notifications: **1,761** of which **1,301** single ip and **460** mass defacements

Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
L - IP address location
★ - Special defacement (special defacements are important websites)

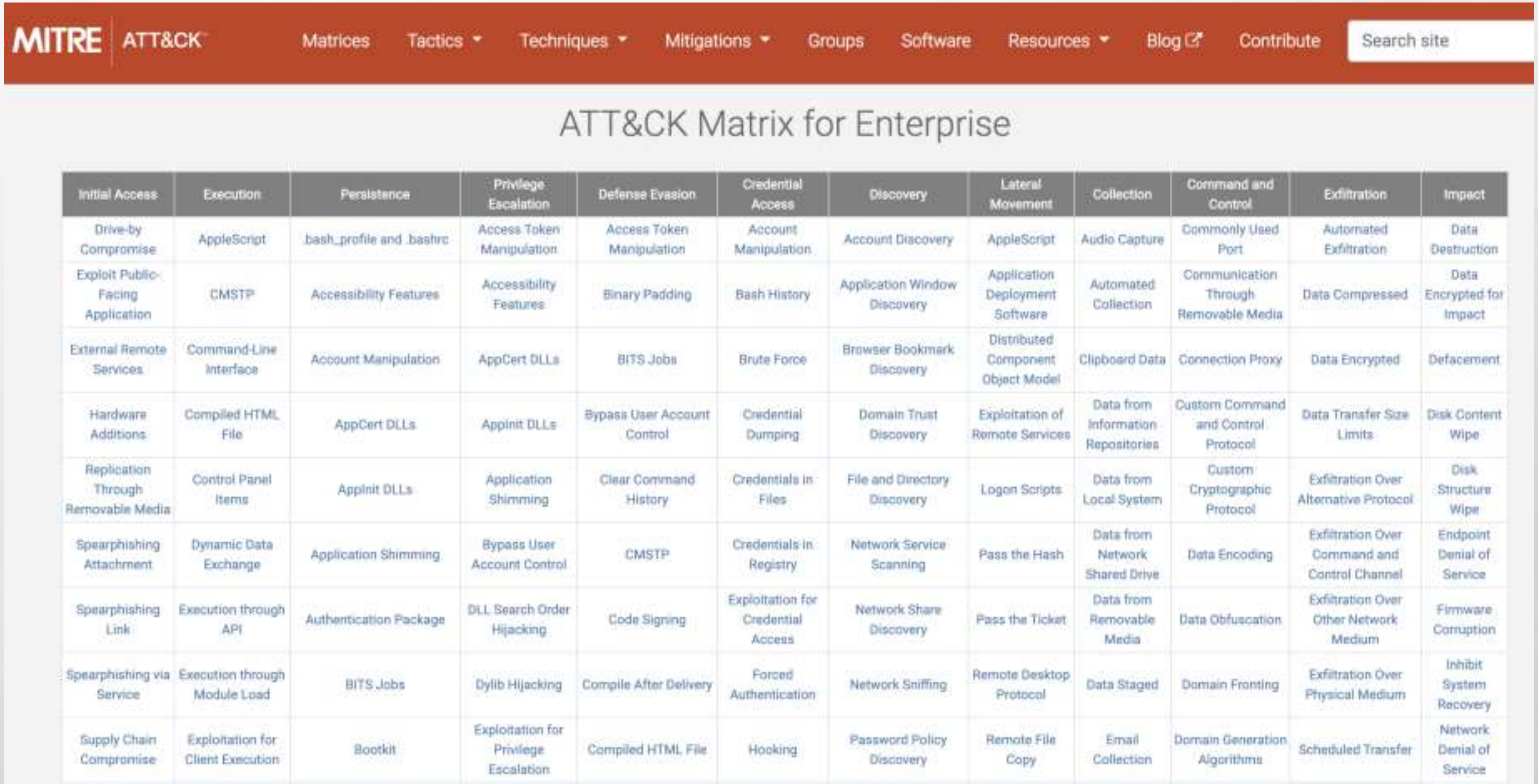
Date	Notifier	H	M	R	L	★ Domain	OS	View
2019/08/06	علي حافظ الاسد	H				★ www.wrapss.ntpc.gov.tw	Linux	mirror
2019/06/30	ifactorye		M			★ pingtung-house.gov.tw/rx.html	Win 2012	mirror
2018/05/08	TeaM_CC					★ health.tfri.gov.tw/fhsncdev/gh...	Unknown	mirror
2018/05/08	TeaM_CC					★ tjee.tjnp.gov.tw/hacked.txt	Unknown	mirror
2018/04/27	TeaM_CC					★ etutor.moe.gov.tw/index.php	Linux	mirror
2018/02/01	SCYTHE404_LOL	H	M			★ wscd.hccg.gov.tw	Linux	mirror
2018/01/08	suliman_hacker					★ sinyi-land.gov.tw/inDex.html	Win 2003	mirror
2018/01/02	KkK1337					★ www.yungan.gov.tw/imgpage/nbhh...	Linux	mirror

ATT&CK

https://attack.mitre.org/


1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

The cyber kill chain



ATT&CK Matrix for Enterprise

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

用MITRE ATT&CK框架識別攻擊鏈，讓入侵手法描述有一致標準
https://www.ithome.com.tw/news/129054

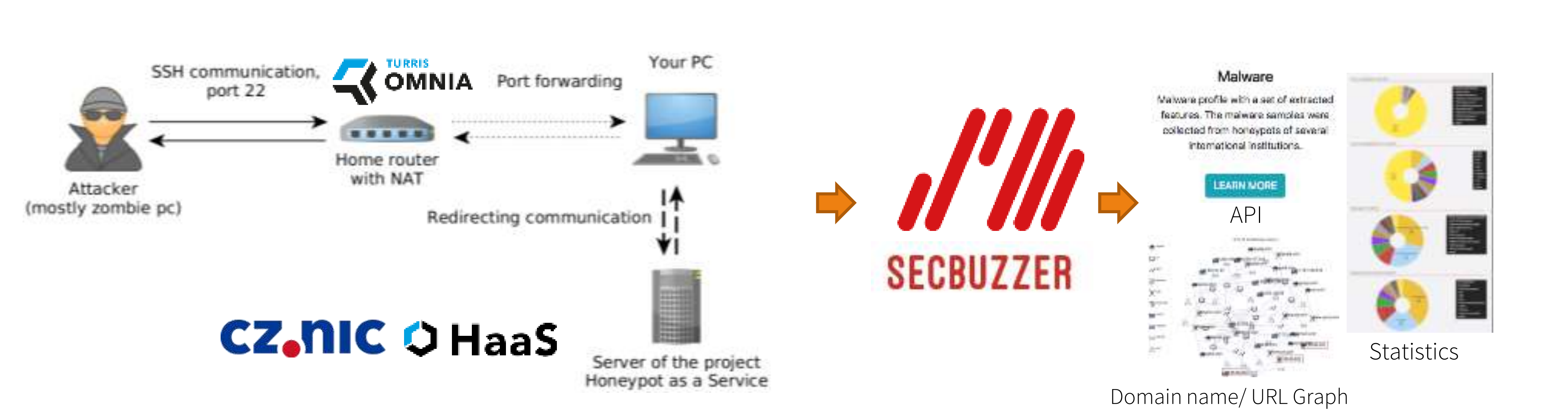
【駭客戰略定義更廣、偵測類別定義更細】快速認識ATT＆CK框架的最新變化
https://www.ithome.com.tw/news/131275

Threat Intelligence Analysis

- Malware analysis using machine analysis
  - Malware family
  - IoT
- Social media analysis
  - Emerging Topic Detection
  - Black market vendor analysis
- CVE-to-exploit prediction
- Other interesting topics

CZ.NIC HaaS (Honeypot as a Service) Project

- CZ.NIC provides malware samples from Turris home routers.
- III analyzed the malware samples through static analysis and dynamic analysis



Malware profile with a set of extracted features. The malware samples were collected from honeypots of several international institutions.

Dionaea: 6071 (~ 13. Feb. 2018)
Cowrie: 8220 (~ 13. Feb. 2018)

補充：
誘捕網路路(Honeynet)為**一個真實網路系統，是由**Honeypot所組成，主要給駭客進行攻擊，藉此學習駭客的攻擊行為，以及所用的工具與手法， 甚至於駭客的攻擊的動機

Malware features

Hash information

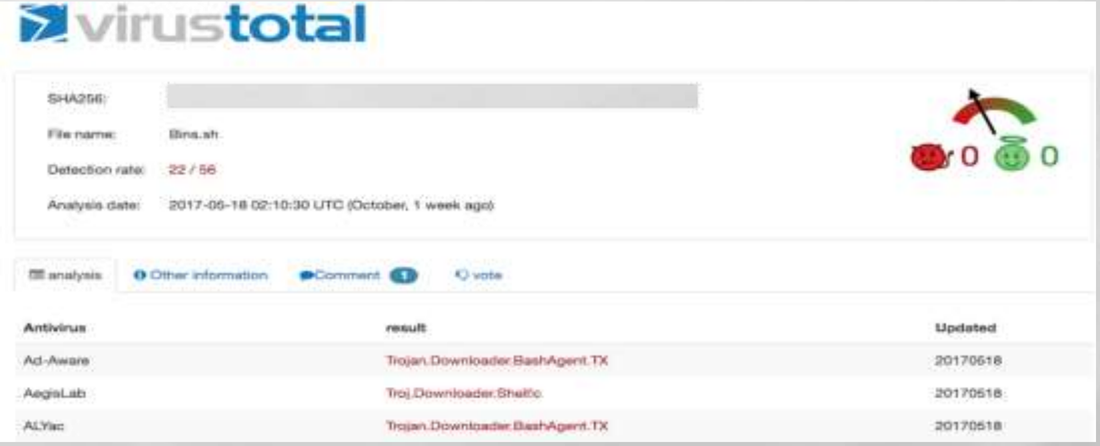
sha1	Well known hash
sha256	Well known hash
ssdeep	Well known hash. The name for the hash is CTPH, calculated by the program named ssdeep
md5	Well known hash

Virus information

vt_virus_name	result of virus names scanned by VirusTotal
vt_token	top 10 virus tokens sorted by their frequencies. tokens are terms appeared in the virus names but containing no blanks or punctuations
vt_detect	the detect ratio, calculated by the number of antivirus software that detect the malware divided by the number of all the antivirus software

Other information

import_file	list of files imported by the malware
import_lib	list of libraries imported by the malware
cpu_etc	the processor by which the malware is compiled
type	other compiler related informations of the malware
packer	the packers used in the malware
IP	the IPs contained in the malware binaries
entropy	we divide the malware into 4 segments (0-20%-50%-80%-100%) and calculate their entropies



SHA256: [redacted]

File name: Bins.sh

Detection rate: 22 / 56

Analysis date: 2017-06-18 02:10:30 UTC (October, 1 week ago)

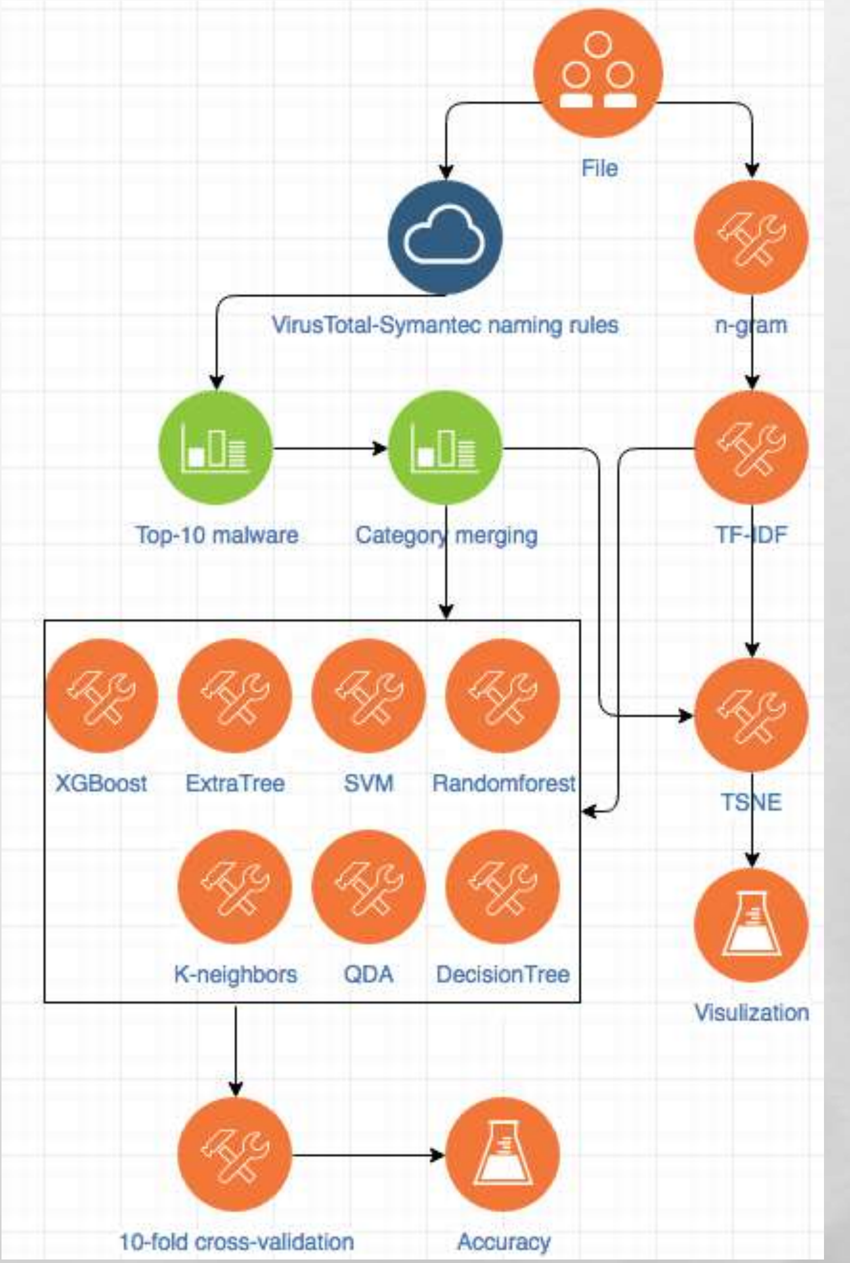
Antivirus	result	Updated
Ad-Aware	Trojan.Downloader.BashAgent.TX	20170518
AegisLab	Troj.Downloader.Shellc	20170518
ALYac	Trojan.Downloader.BashAgent.TX	20170518

Analysis tools:
Virustotal
https://www.virustotal.com/gui/home/upload
Cuckoo
https://cuckoosandbox.org/

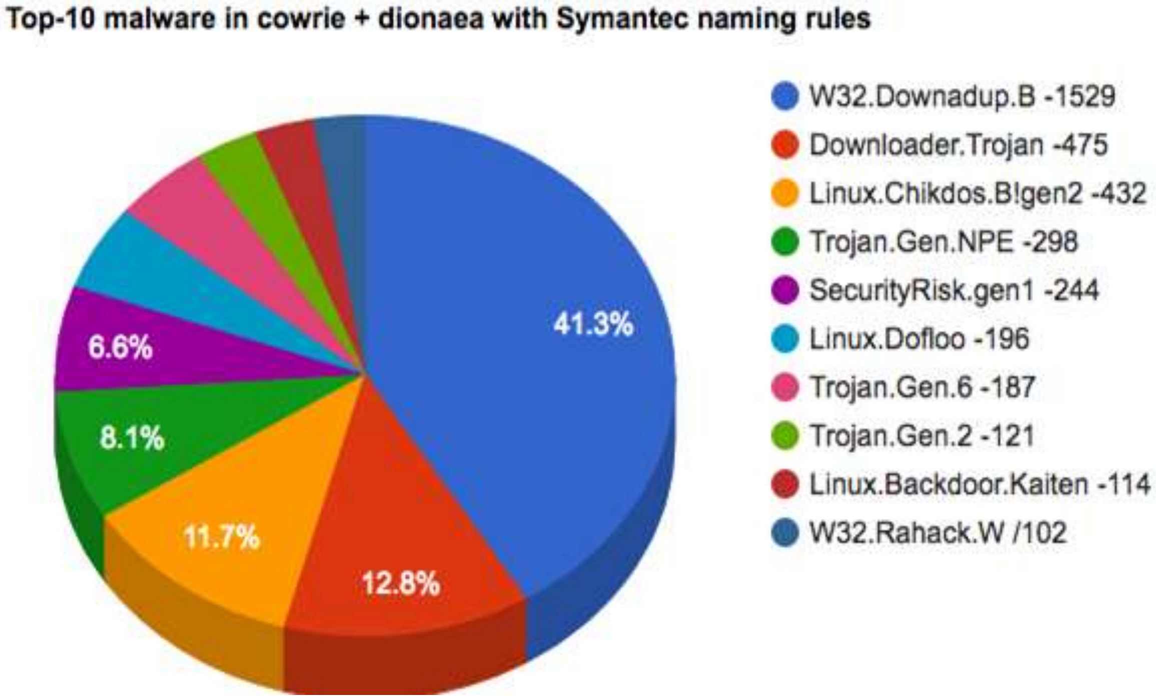
Malware features

- Extract n-gram of binaries and transform them to computed features via TF-IDF.
- Choose a AV’ s naming rules as malware families label (here we use Symantec).
- Use TSNE to visualize sample similarity.
- Apply classification method and represent the accuracy.

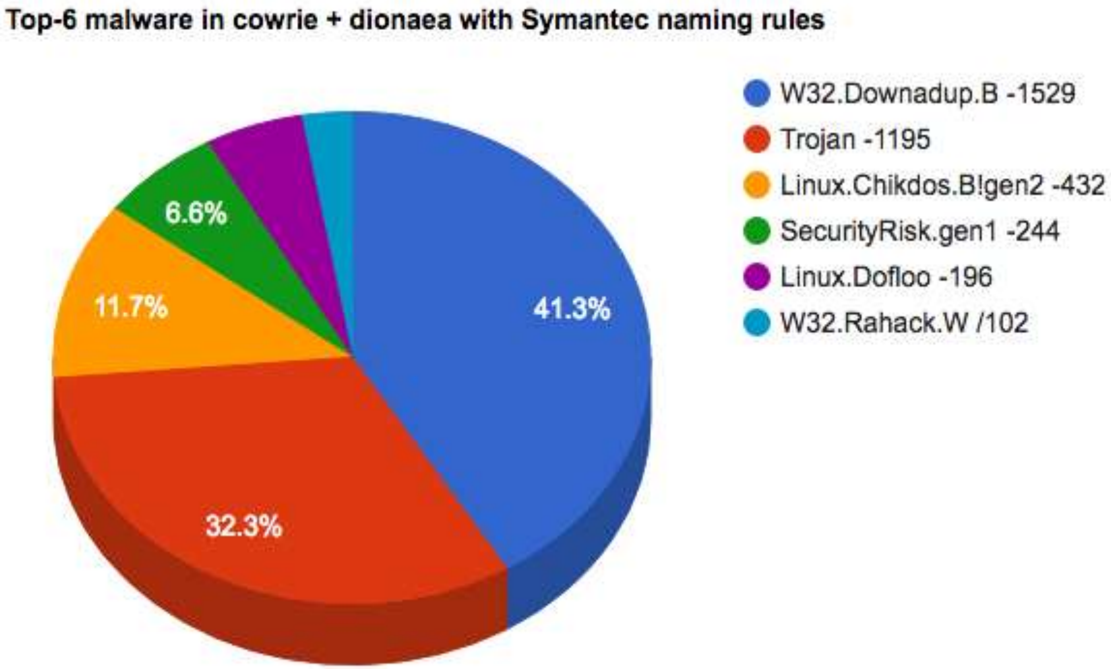
t-Distributed Stochastic Neighbor Embedding (tSNE)
tSNE 是一種降維方式，主要是將高維的數據用高斯分佈的機率密度函數近似，而低維數據的部分使用 t 分佈的方式來近似，在使用 KL(Kullback-Leibler) 距離計算相似度，最後再以梯度下降求最佳解



Get malware labels

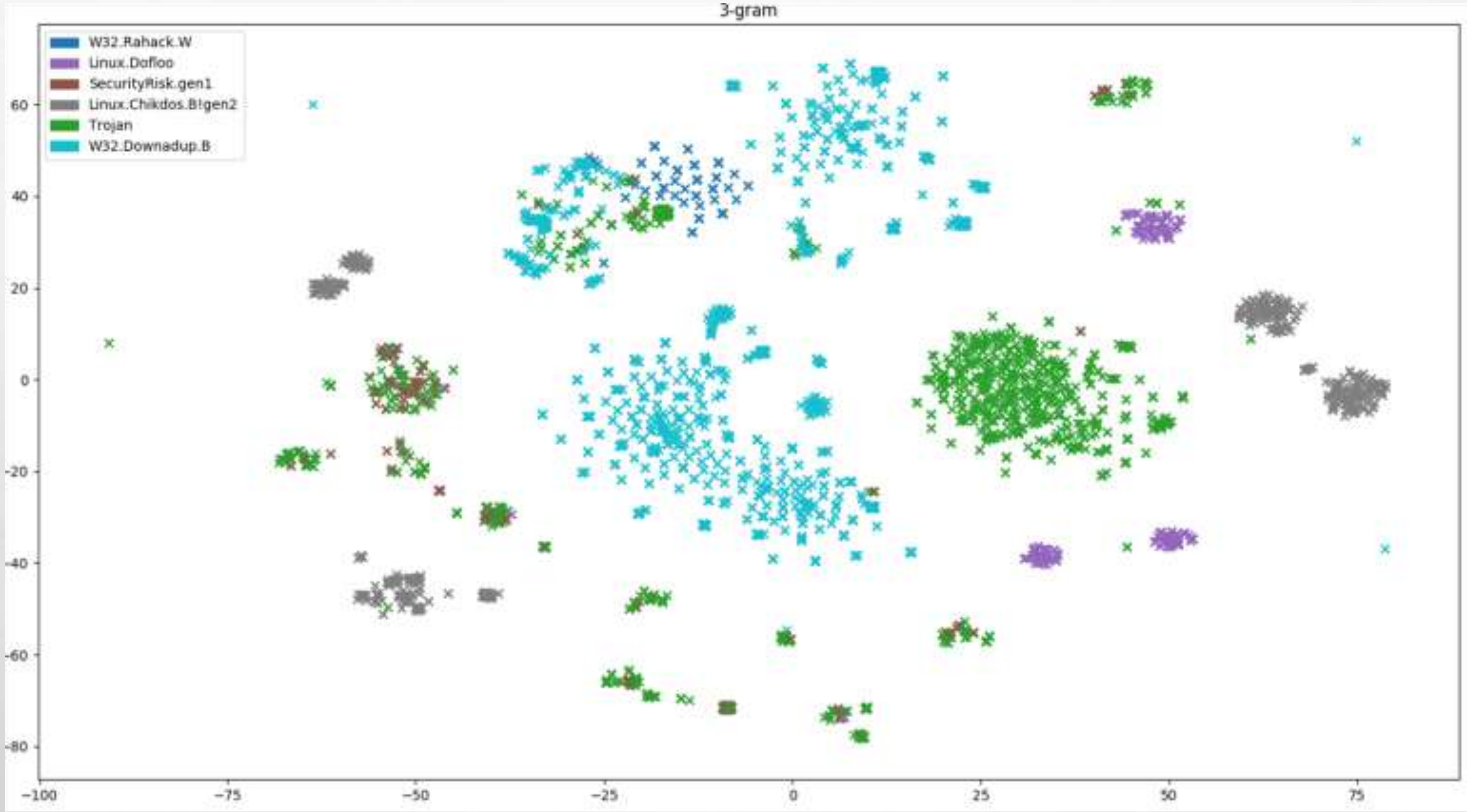


Top-10 malware in cowrie + dionaea with Symantec naming rules

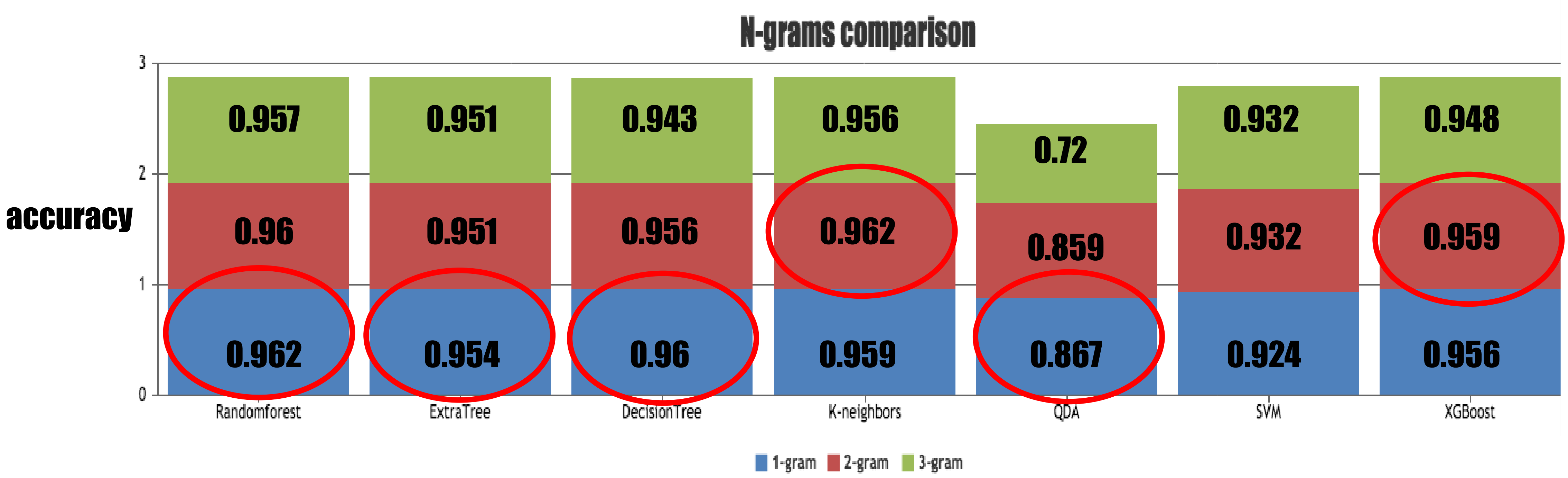


Top-6 malware in cowrie + dionaea with Symantec naming rules

tSNE projection

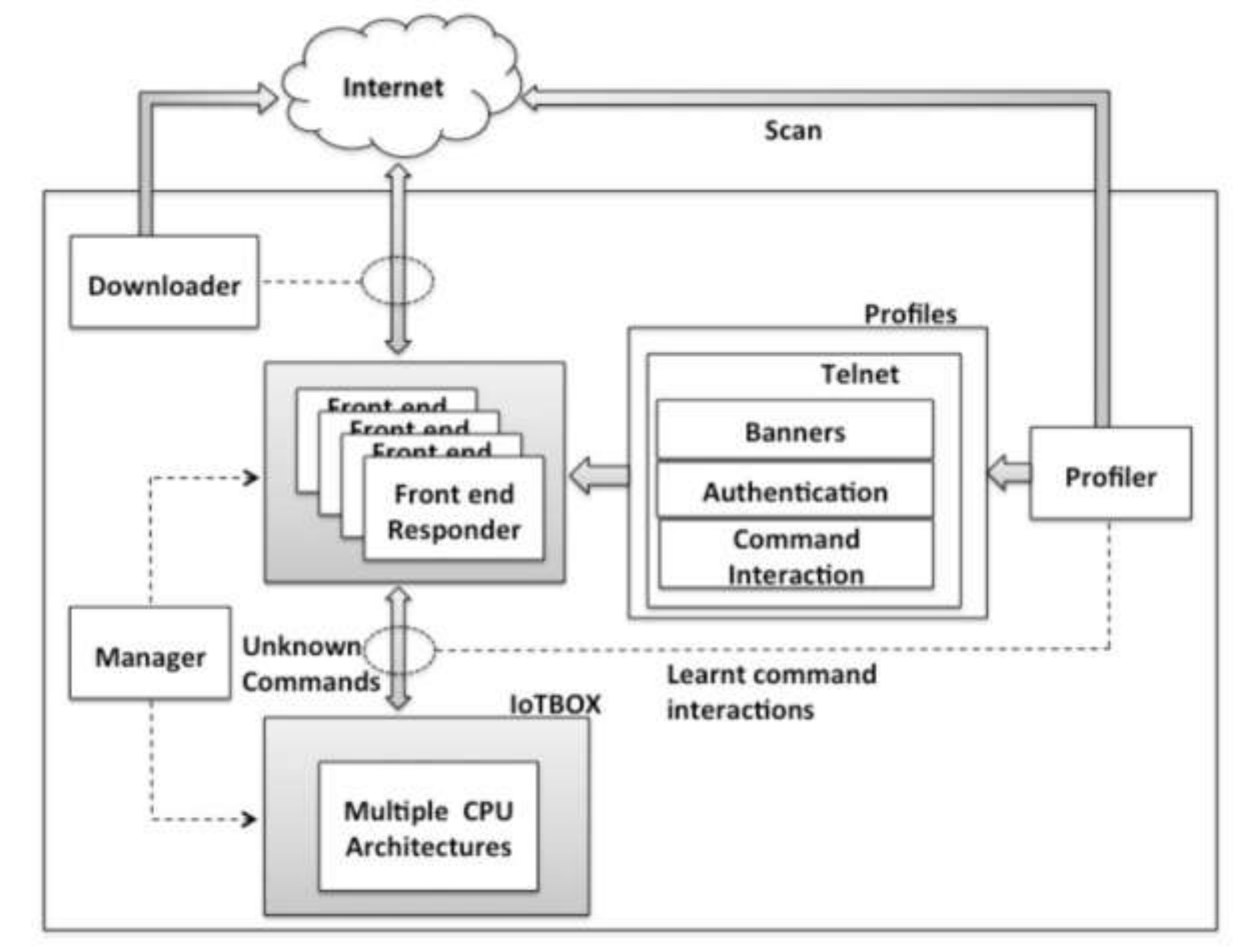


Classifiers comparison



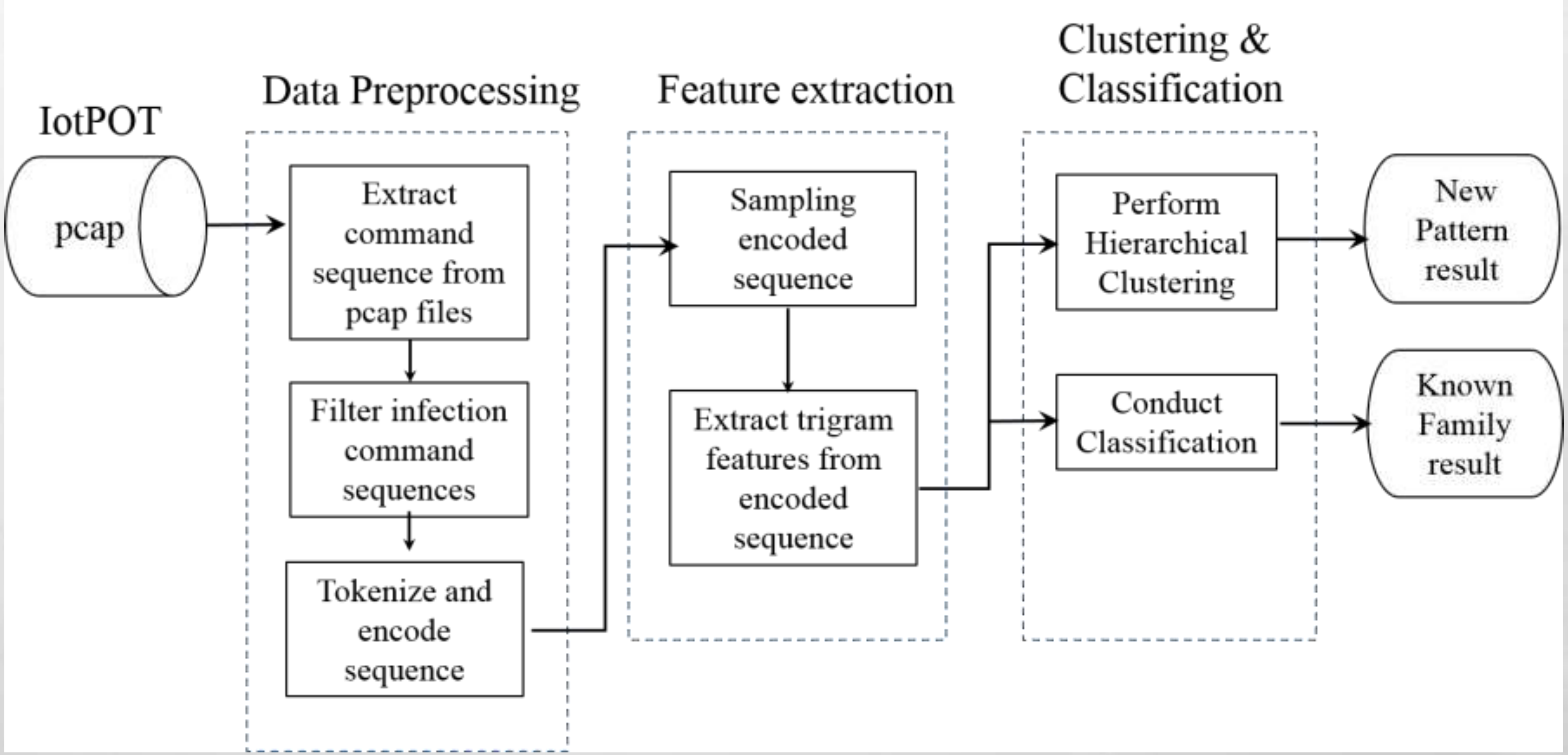
IOT malware classification

- IOTPOT acts as different IoT devices by handling incoming TCP connection requests, banner interactions, authentication, and command interactions with a set of device profiles.



IOT malware classification

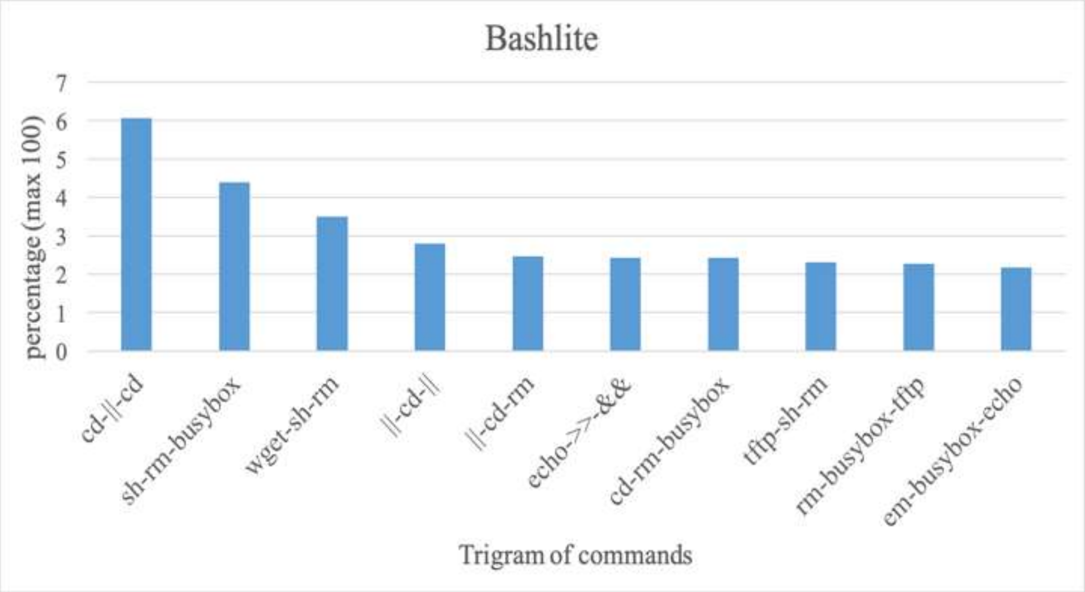
- Data analysis flow


IotPOT
pcap
Data Preprocessing
Extract command sequence from pcap files
Filter infection command sequences
Tokenize and encode sequence
Feature extraction
Sampling encoded sequence
Extract trigram features from encoded sequence
Clustering & Classification
Perform Hierarchical Clustering
Conduct Classification
New Pattern result
Known Family result

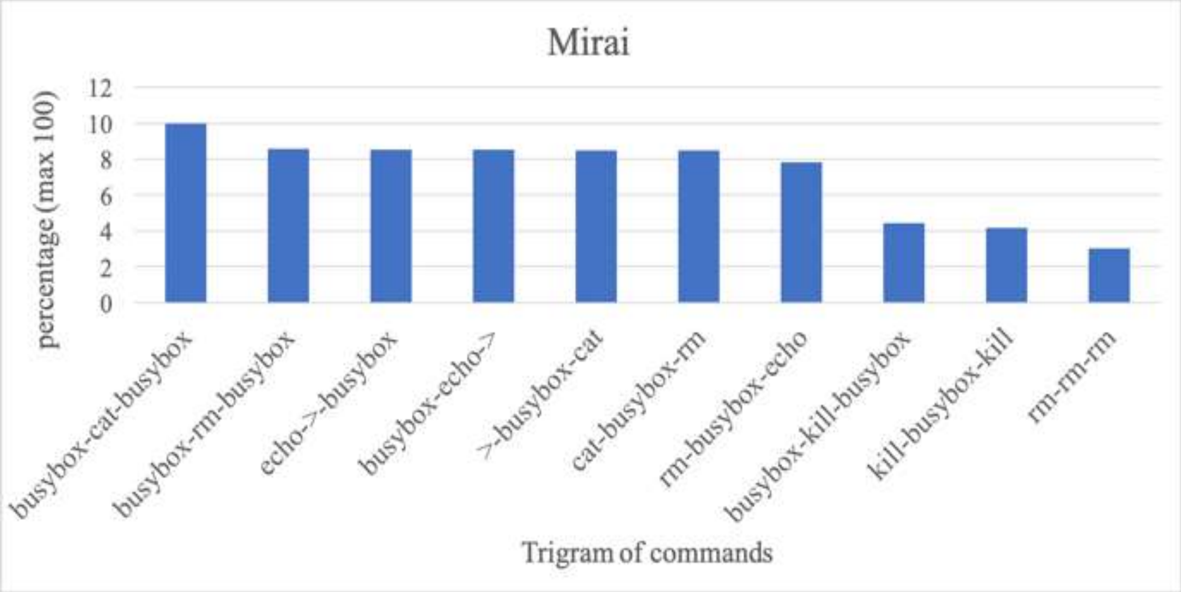
IOT malware classification

- Trigram of commands statistics

Bashlite IoT malware



Mirai IoT malware

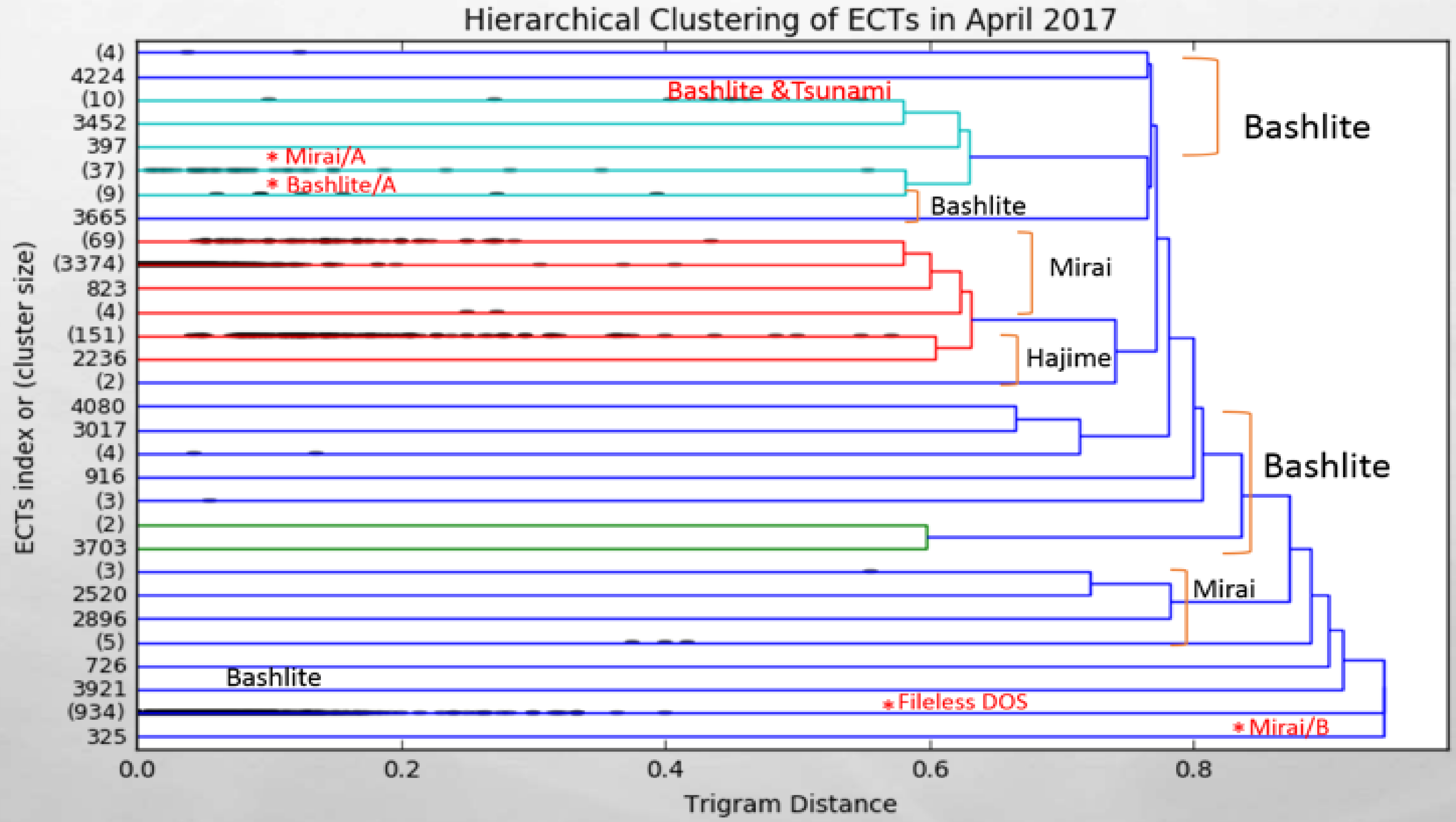


IOT malware classification

- Dataset for analysis

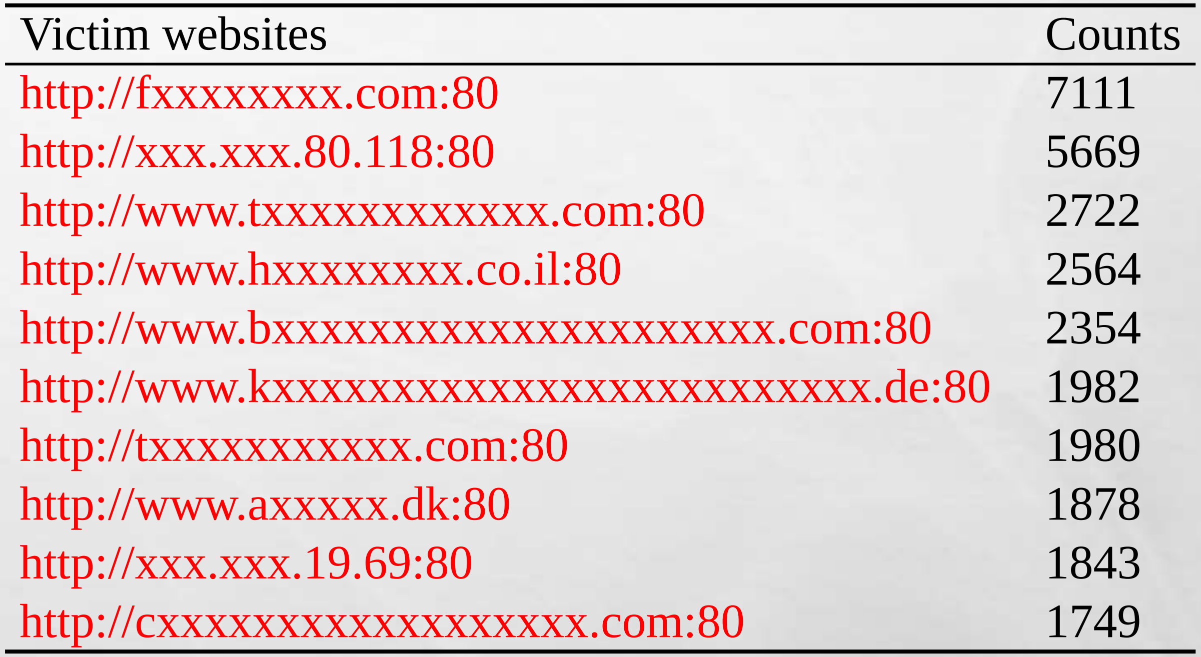
Dataset	Number of infection command sequence	Rearranged command sequence	Number of unique extracted command tokens	Time interval	Analysis
1	2,756,231	44,843*	2,925	2016/12/07~ 2017/09/16	NB, SVM
2	422,591	95,448**	4,626	2017/04/01~ 2017/04/30	Hierarchical clustering

Hierarchical clustering results



Fireless threat

- Fileless DoS is a shell script that employs an infinite while loop and multiple wget commands to mount a DoS attack. Downloaded web contents are sent to /dev/null, and thus no binaries are stored in devices. A total of 934 Fileless DoS ECTs were discovered in April 2017.



Victim websites	Counts
http://fxxxxxxxx.com:80	7111
http://xxx.xxx.80.118:80	5669
http://www.txxxxxxxxxxxx.com:80	2722
http://www.hxxxxxxxx.co.il:80	2564
http://www.bxxxxxxxxxxxxxxxxxxxxx.com:80	2354
http://www.kxxxxxxxxxxxxxxxxxxxxxxxxx.de:80	1982
http://txxxxxxxxxxx.com:80	1980
http://www.axxxxx.dk:80	1878
http://xxx.xxx.19.69:80	1843
http://cxxxxxxxxxxxxxxxxxx.com:80	1749

Classification performance

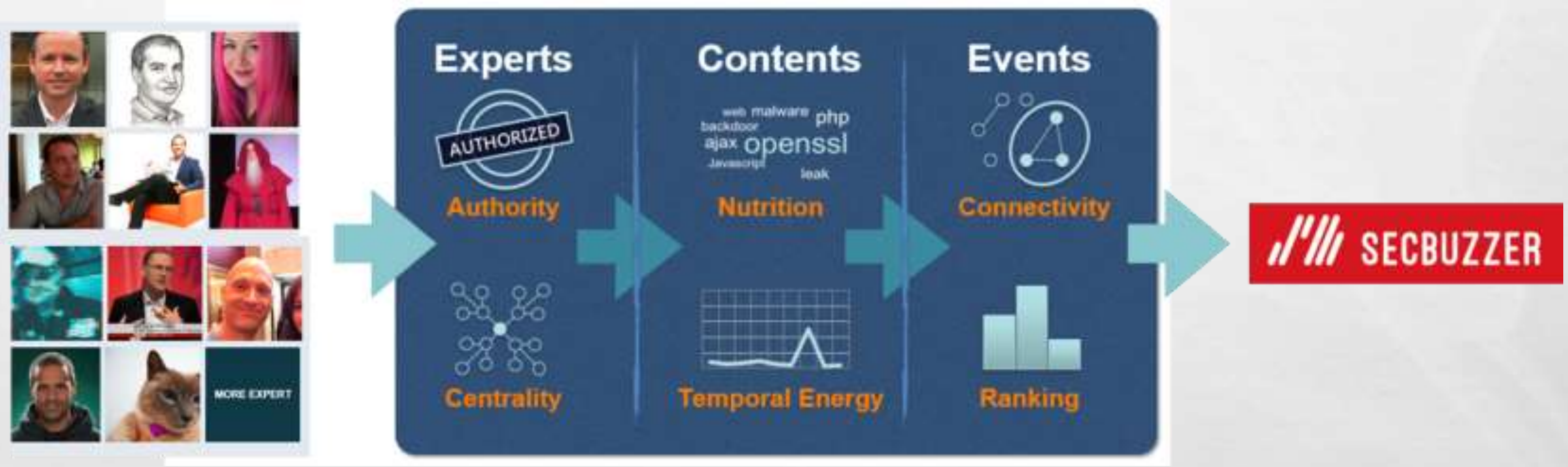
- The precision of Tsunami classification improved because its file sample metadata differed from that of Bashlite. Using additional features can thus help to prevent misidentifying classes that share the same command line pattern, without requiring static and dynamic analyses and simply by looking at the command line and file meta-information.

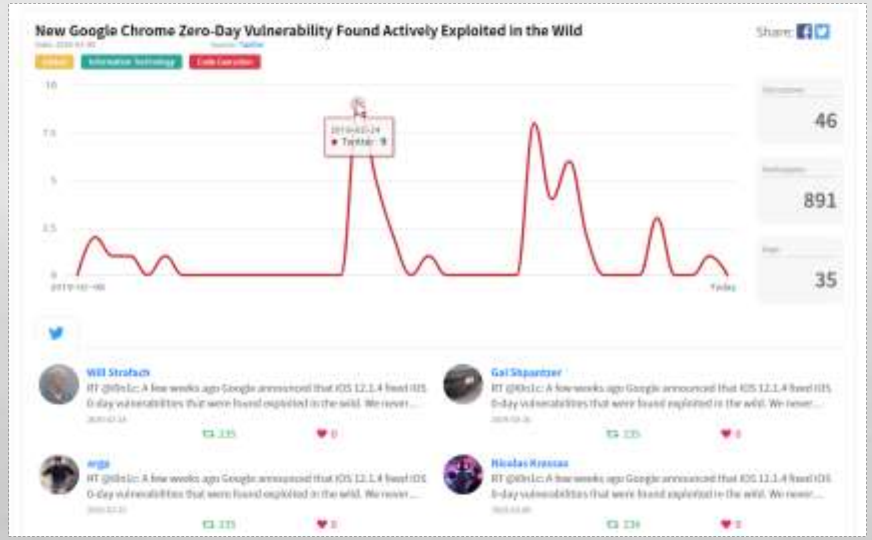
Precision/recall of SVM

	precision	recall	f1-score	support
Bashlite	0.99	0.99	0.99	155
Mirai	0.98	1.00	0.99	1225
Hajime	1.0	1.0	1.00	60
Tsunami	0.90	0.86	0.88	24
Avg / total	0.96	0.98	0.97	1464

Emerging Topic Detection

- Follow top cybersecurity experts' tweets in order to get the first-hand cyber threat topic worldwide.




New Google Chrome Zero-Day Vulnerability Found Actively Exploited in the Wild

Will Strafach
RT @i0n1c: A few weeks ago Google announced that iOS 12.1.4 fixed iOS 0-day vulnerabilities that were found exploited in the wild. We never…
235 0

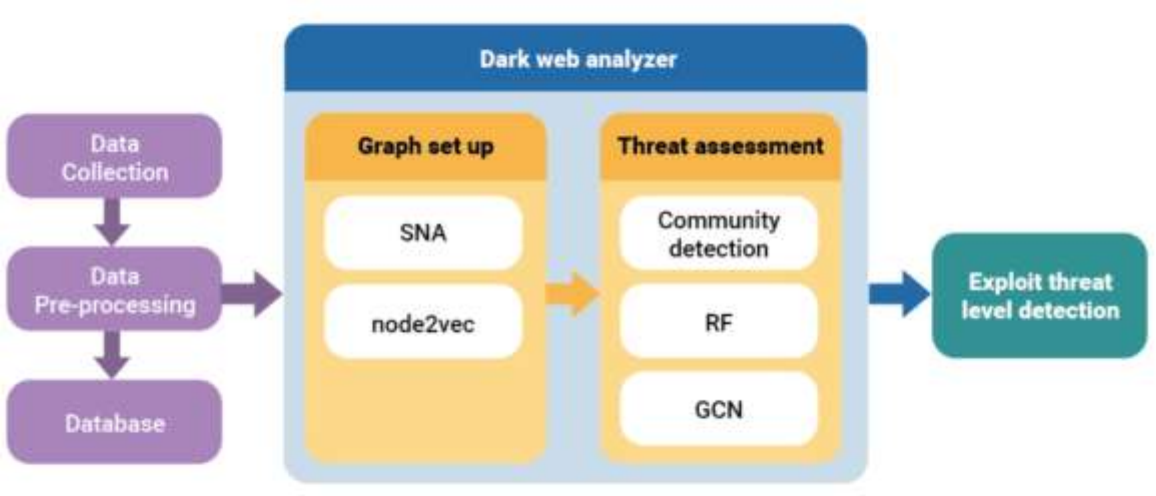
Gal Shpantzer
RT @i0n1c: A few weeks ago Google announced that iOS 12.1.4 fixed iOS 0-day vulnerabilities that were found exploited in the wild. We never…
235 0

argp
RT @i0n1c: A few weeks ago Google announced that iOS 12.1.4 fixed iOS 0-day vulnerabilities that were found exploited in the wild. We never…
235 0

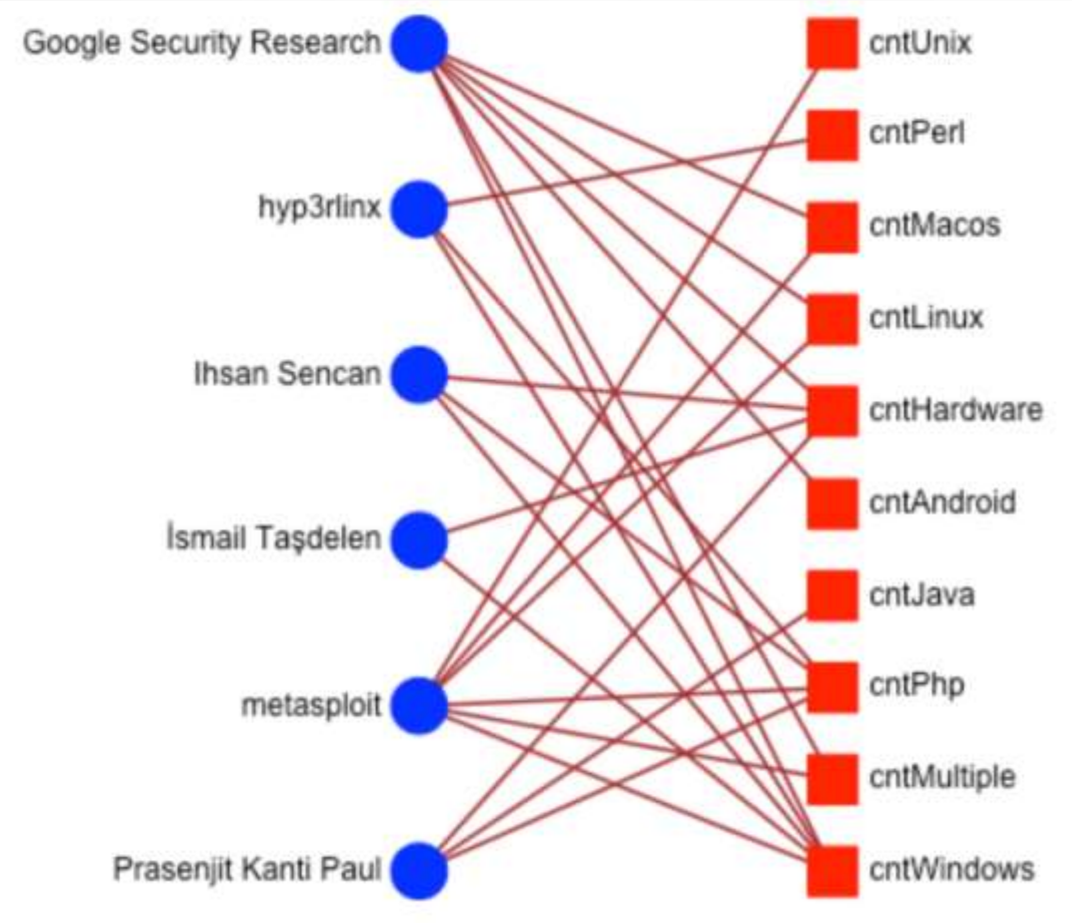
Nicolas Krassas
RT @i0n1c: A few weeks ago Google announced that iOS 12.1.4 fixed iOS 0-day vulnerabilities that were found exploited in the wild. We never…
234 0

Exploit threat analysis

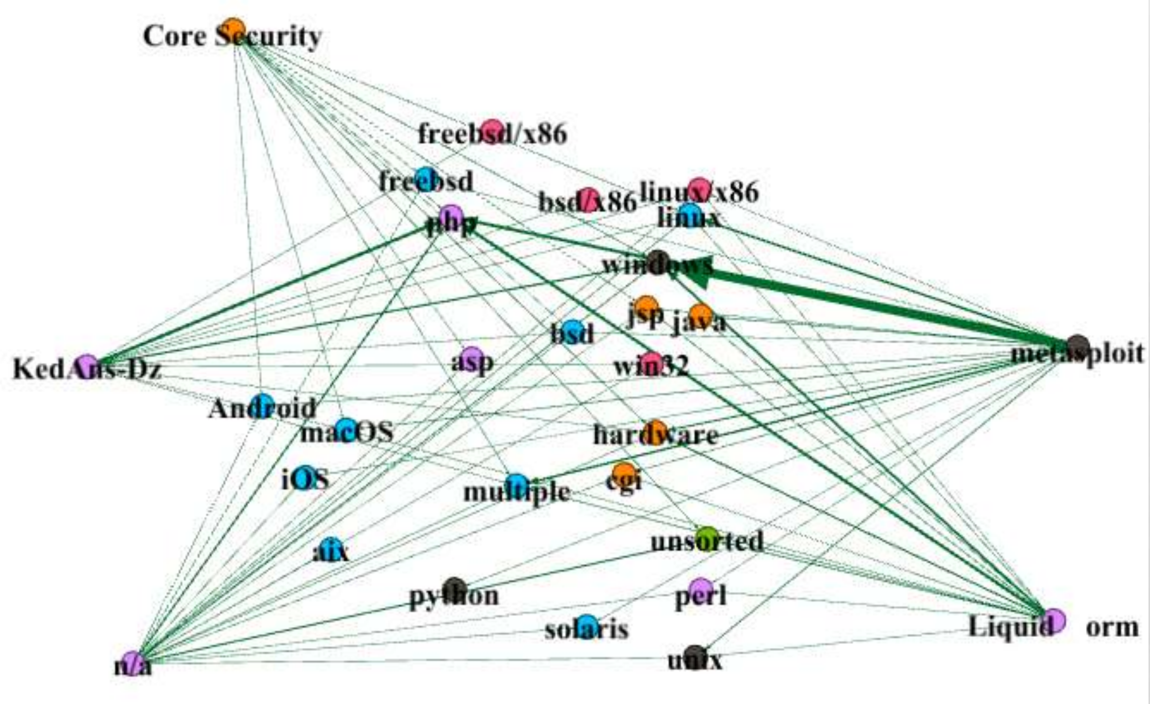
- Analysis step:
  1. Graph modeling: Select two features (author, platform) to set up graph component: node and link file, and then visualize the relationship network between author and platform
  2. Community detection: Perform community detection based on the graph
  3. Network embedding: Use link file to develop node2vec network embedding
  4. Set up classification model (Random Forest) based on the network embedding and the given labels
  5. Set up GCN (Graph Convolutional Network) model based on the network embedding and the given labels



Exploit threat analysis



author vs. platform



Community detection

RF: 89.5% accuracy
GCN: 92.47% accuracy

Black market vendor analysis

- Baidu forums is one of the major online underground marketplaces for the stolen credit cards.
  - Keywords: “four pieces” , “interception” , “intercept” , “black card” , “internal materials” , and “cvv” .
    Four pieces mean account name, Social Security Number (SSN), credit card number, and passwords.
  - Forums retrieved based on the keywords: 21 Baidu forums.
  - Time period: January 2006 – March 2016
  - Total members: 2,129
  - Threads: 5,131
  - Threads including replies: 53,963

1. cvvvvv posts： 6,565
2. cvvvvvvvvp posts： 3,586
3. 四大吧 (four) posts： 4,215
4. 内储吧 (innersave) posts： 1,459
6. 银行唯一的秘密吧 (bank) posts： 2,745
15. 料主吧 (materialOwner) posts： 655
21. 四大件吧 (Four pieces) posts： 12,419

7. 采集器吧 (collectMachine) posts： 796
10. 采集吧 (collect) posts： 2,310
11. 外机吧 (outsideMachine) posts： 1,015

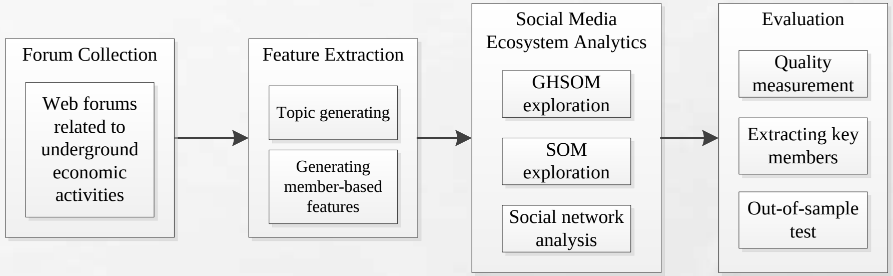
12. 原轨原密吧 (originalChannel) posts： 977
14. 轨道吧 (track) posts： 1,952
18. 拦截料吧 (interceptMaterial) posts： 151
20. 洗拦截吧 (washIntercept) posts： 92

5. 大胆吧 (brave) posts： 3,082
8. 路子非常野 (wild) posts： 7,236
13. 黑产吧 (blackProduct) posts： 736
17. 取钱吧 (pickMoney) posts： 254

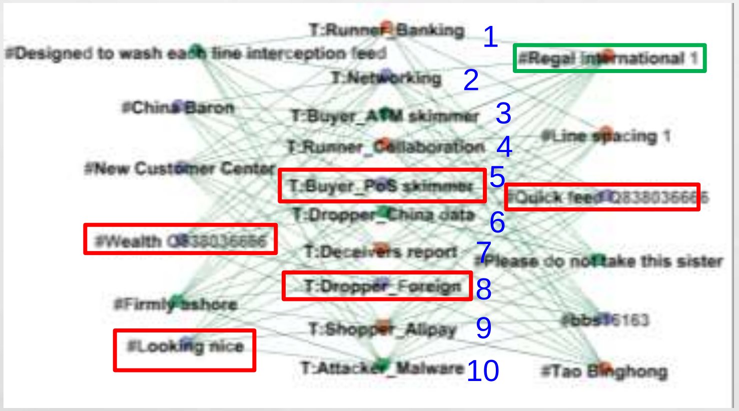
9. 外卡吧 (card) posts： 3,068
16. jp刷货吧 (jp) posts： 168
19. 外币外卡吧 (outsideCard) posts： 111

Black market vendor analysis

- Mapping 12 key members extracted from the topic-based SNA with their belonged clusters in GHSOM.



SNA



T: topic.
#: member name

Key members mapping

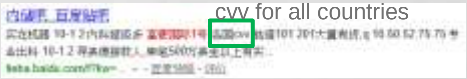
Rank	Member	GHSOM cluster index [map index--unit index]
1	#Wealth Q838036666	**3—3**, 3--4
2	#Line spacing 1	3—2, 3--4
3	#Quick feed Q838036666	**3—3**, 3—4, 9--4
4	#Please do not take this sister	3—2, 3--4
5	#Looking nice	**3—1**, 3—2, 3--4
6	#Firmly ashore	3—1
7	#Regal International 1	**3—3**, 3—4, 6—4
8	#bbs16163	6—4, 6—5, **9—1**
9	#Tao Binghong	2--4
0	#Designed to wash each line interception feed	9--4
11	#China Baron	6—1, 6—2
12	#New Customer Center	6—1, 6—2

light purple: Topic 5- Buyer

bold purple: Topic 8- Dropper

#Wealth Q838036666 profile

The evidence related to selling foreign data



cvv for all countries

We highlight the topics and other key members related to *#Wealth Q838036666* in SNA and GHSOM.

The related key members are interested in topic 5 (PoS skimmer) and topic 8 (Foreign data). The most similar key members are *#Quick feed Q838036666* and *#Looking nice*.

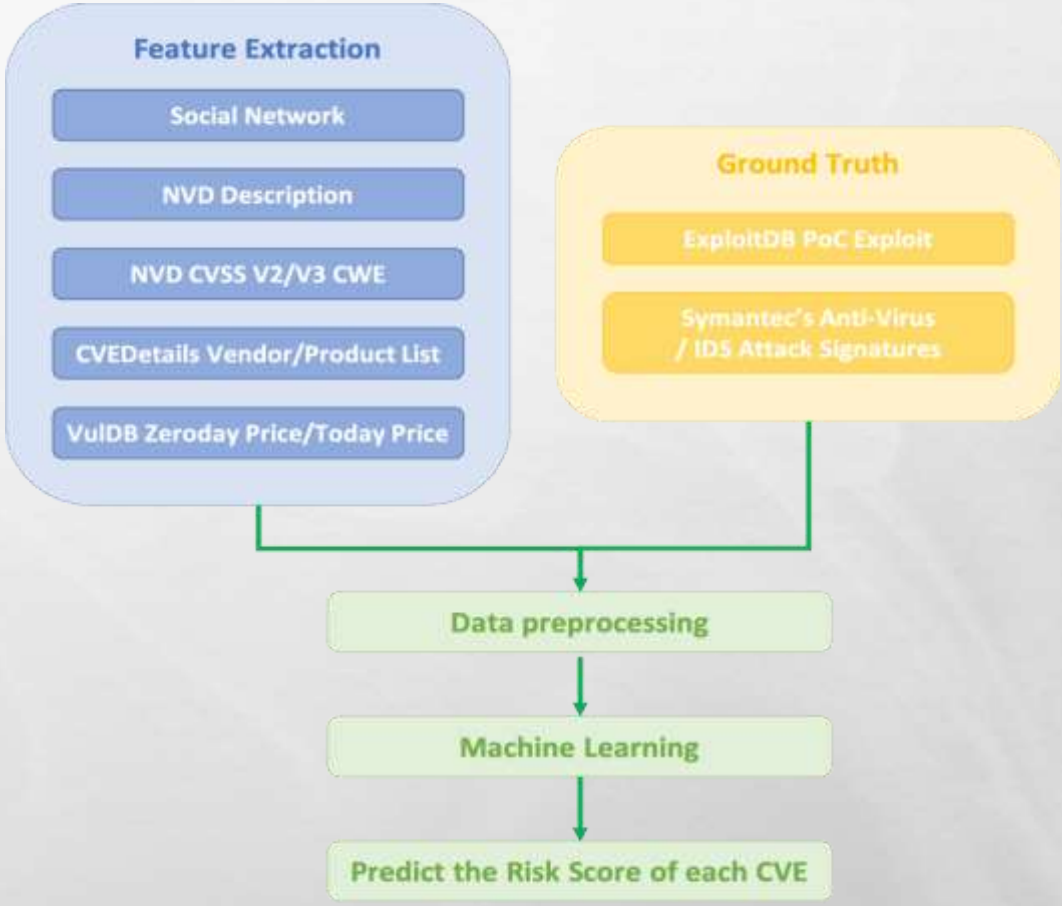
Note that GHSOM indicates that *#Regal International 1* (marked with green square) are also very similar with *#Wealth Q838036666*.

Therefore, GHSOM can help to generate clusters with distinctive characteristics and the topology layout is helpful to measure the similarity.

CVE-to-exploit prediction

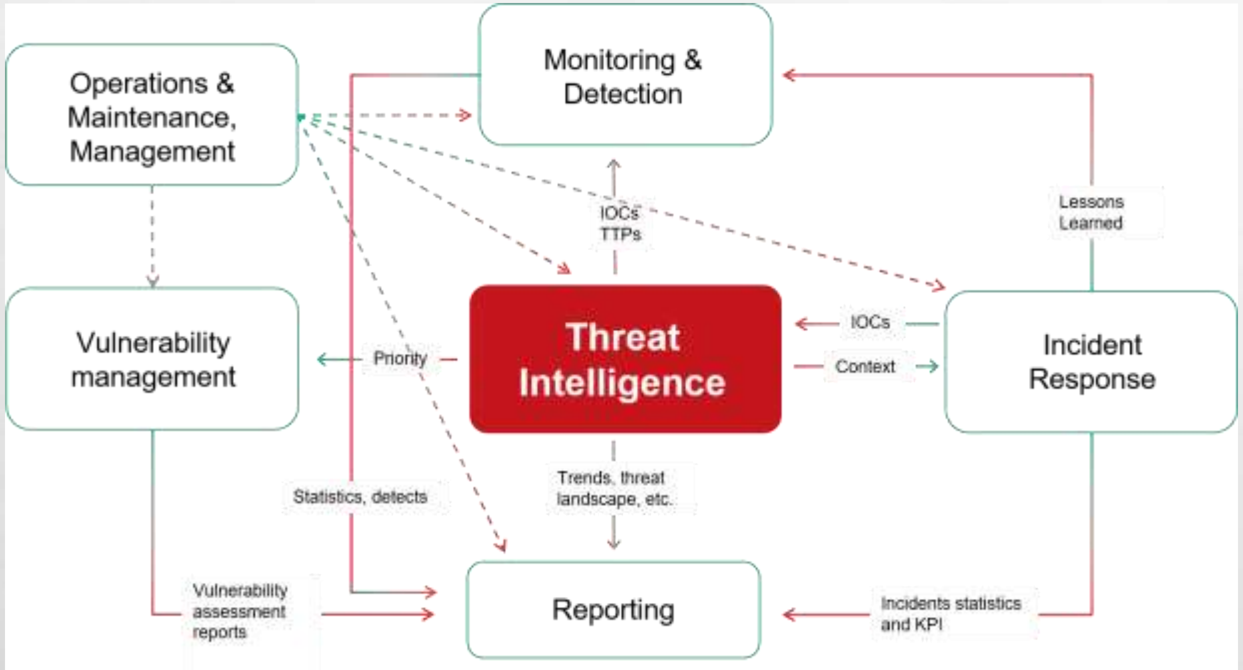
- 近年來越來越多的軟硬體漏洞正在不停地被揭露，從弱點被公布到廠商提供Patch期間，都是網絡犯罪分子攻擊的機會，然而，衡量弱點嚴重性的僅有美國國家標準技術研究所（National Institute of Standards and Technology, NIST）的國家弱點資料庫（National Vulnerability Database, NVD）提供的資料，無法直覺且快速的找出高風險漏洞。

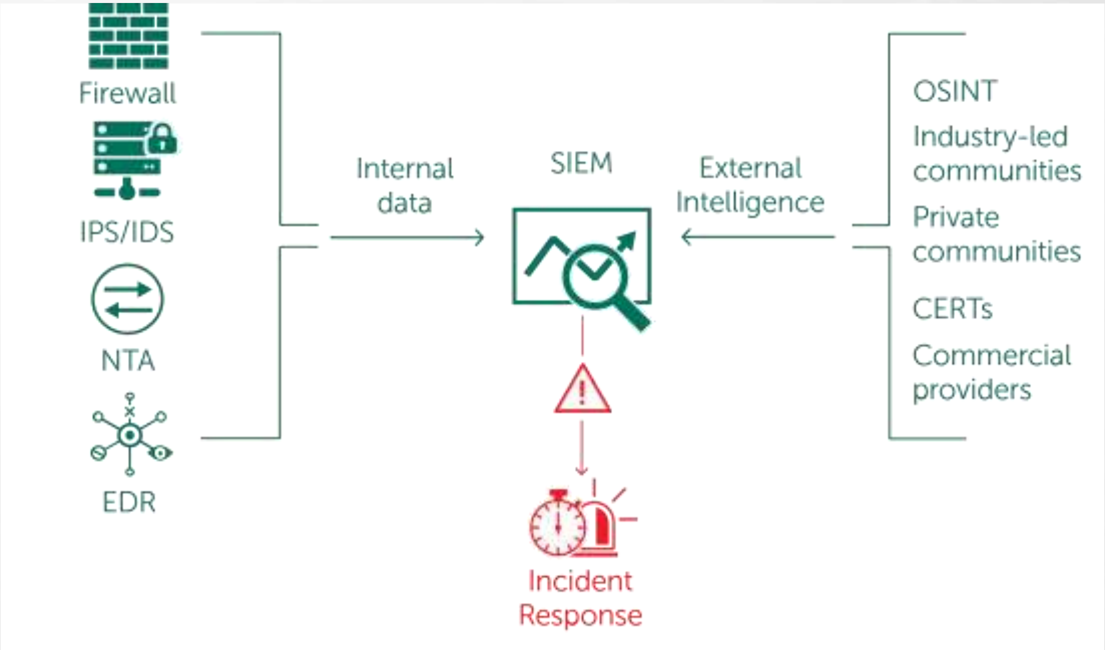
- 因此我們提出除了該弱點之基本屬性外，額外再加上Twitter平台上與該漏洞相關的資訊，並利用Machine Learning的方式，且以動態風險評估的方式來預測該漏洞於現實世界中被利用的可能性與風險，以達到於威脅爆發前之事前預警，進而提供給企業作為防禦之參考、廠商開發補丁之依據。


Feature Extraction
Social Network
NVD Description
NVD CVSS V2/V3 CWE
CVEDetails Vendor/Product List
VulDB Zeroday Price/Today Price
Ground Truth
ExploitDB PoC Exploit
Symantec's Anti-Virus / IDS Attack Signatures
Data preprocessing
Machine Learning
Predict the Risk Score of each CVE

【自己的風險自己估】CVSS 參考價值有限，所以我們開發了一套風險預測模型
https://secbuzzer.co/post/106

How to operate threat intelligence?





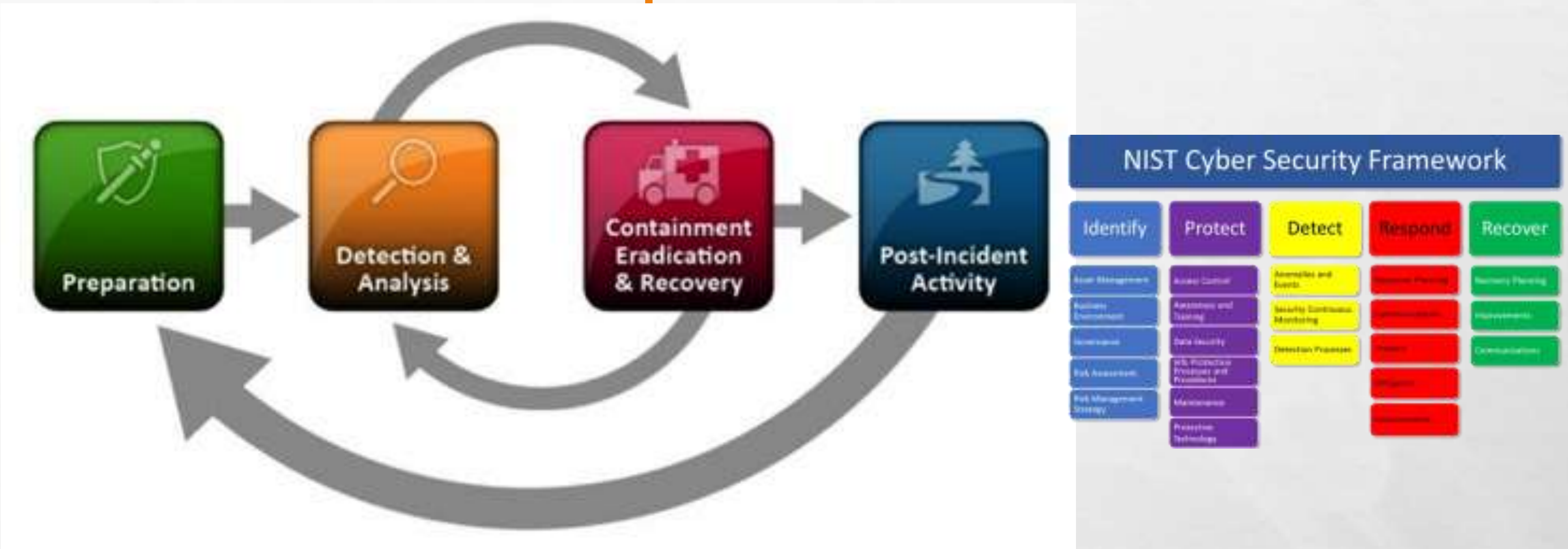
Source: Kaspersky

https://www.kaspersky.com/blog/evaluating-threat-intelligence/26952/

Part 3: 資安威脅案例分析

NIST definition of incident response

Preparation:
1. 人員挑選與培訓
2. 軟體與硬體備妥
3. 確立通報管道
   - 其中軟體包含蒐集資料與分析所需使用的工具軟體
   - 也需建立資安事故應變與處理的通報準則，與通報人員的連絡方式



Detection & Analysis:

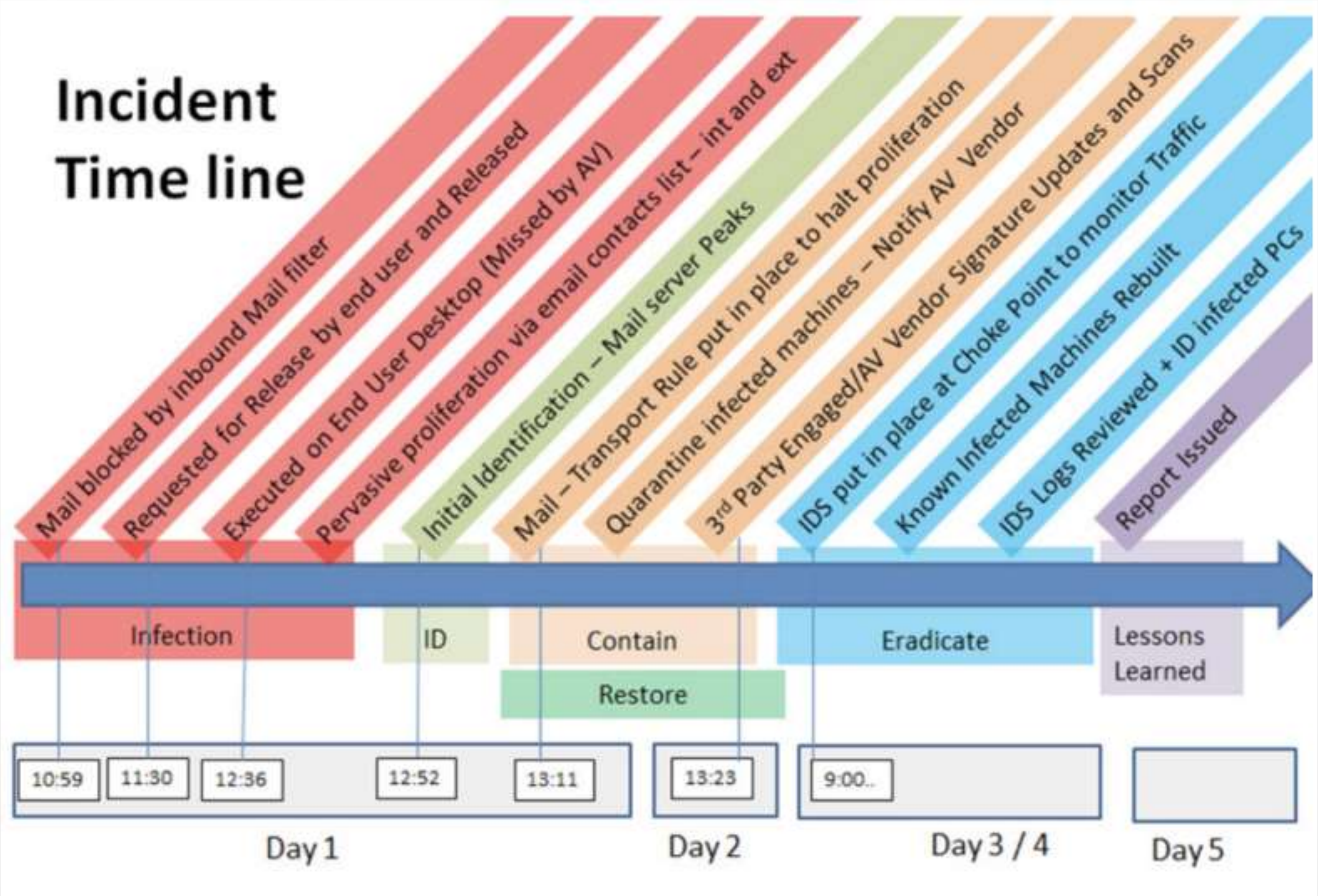
當確定為駭客入侵事件後，應蒐集受害電腦中下列資訊：
1. 防毒軟體偵測記錄
2. 系統資訊，例如作業系統版本、網路設定、執行程序、開機啟動設定
3. 可疑程式或檔案
4. 同時檢視網路防護設備記錄檔，進行網路封包側錄

Containment, Eradication & Recover:
- 啟用備用主機，將受害主機斷線
- 阻擋駭客連線C&C的IP或Domain
- 利用防火牆等設備隔離受害主機
- 停用異常帳號
- 重設帳號與密碼

Post-Incident Activity:
- 除修補駭客入侵途徑外，應持續監控是否有其它潛伏主機的活動跡像，確保無其它潛伏受害電腦

NIST: 美國國家標準技術機構(National Institute of Standards and Technology)

IR timeline

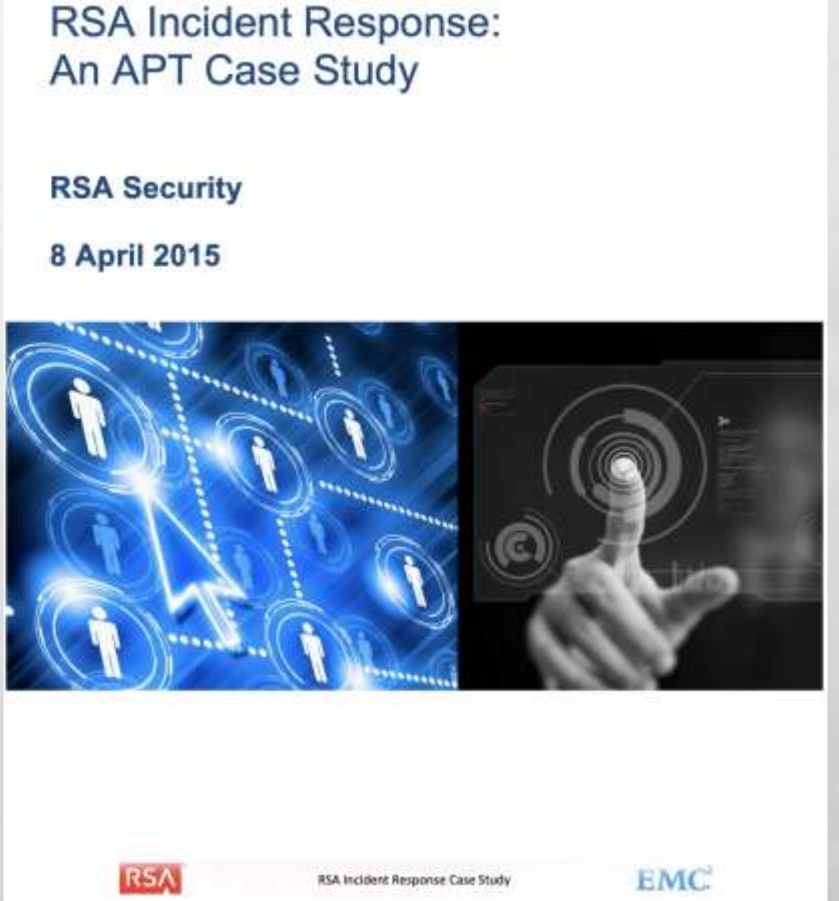

Incident
Time line
Mail blocked by inbound Mail filter
Requested for Release by end user and Released
Executed on End User Desktop (Missed by AV)
Pervasive proliferation via email contacts list – int and ext
Initial Identification – Mail server Peaks
Mail – Transport Rule put in place to halt proliferation
Quarantine infected machines – Notify AV Vendor
3rd Party Engaged/AV Vendor Signature Updates and Scans
IDS put in place at Choke Point to monitor Traffic
Known Infected Machines Rebuilt
IDS Logs Reviewed + ID infected PCs
Report Issued
Infection
ID
Contain
Restore
Eradicate
Lessons
Learned
10:59
11:30
12:36
12:52
13:11
13:23
9:00..
Day 1
Day 2
Day 3 / 4
Day 5

RSA Incident Response: An APT Case Study

https://autoblog.postblue.info/autoblogs/lamaredugoffrblog_a1de86d064e376dc283723997fd86bde6ba2d492/media/9d981698.RSA-IR-Case-Study.pdf

Case study conclusion

- Only with full network and endpoint visibility can investigators ensure they’ ve identified all malware deployed or C2 channels used by an adversary.
- Additionally, this visibility is critical after remediation of the intrusion, as APT adversaries will try to reenter the environment
- By having proper visibility over the network you will be able to proactively identify new infections and more rapidly remediate them.



RSA Incident Response:
An APT Case Study

RSA Security

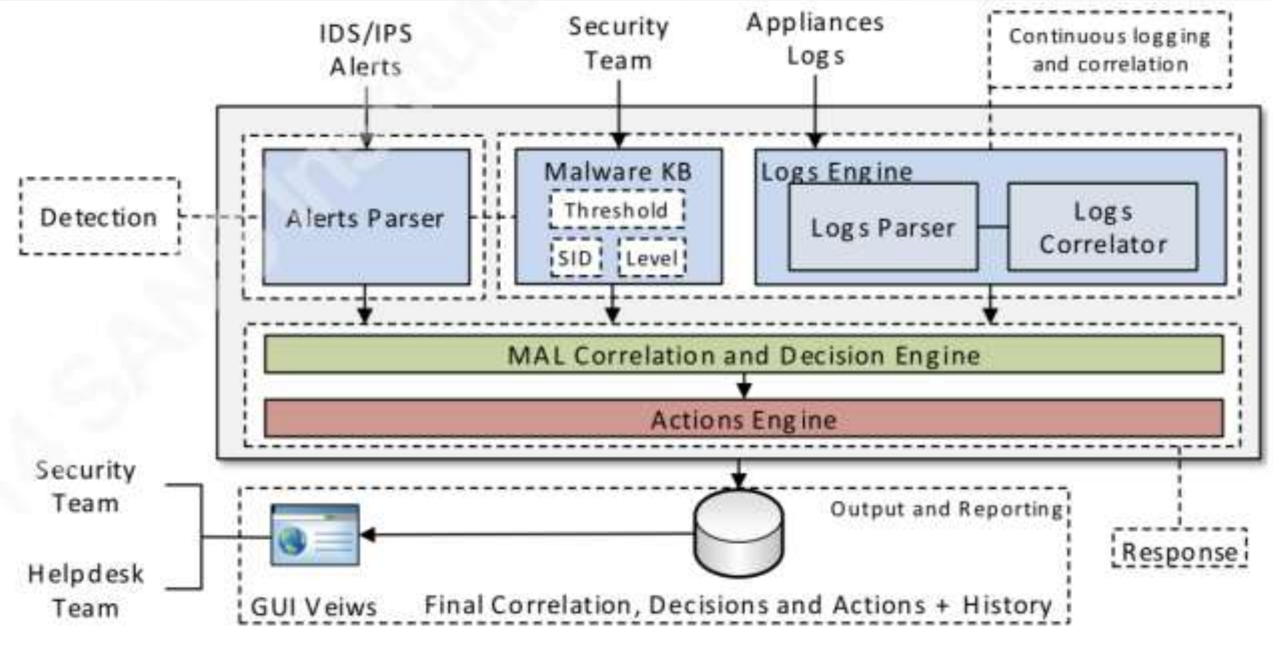
8 April 2015

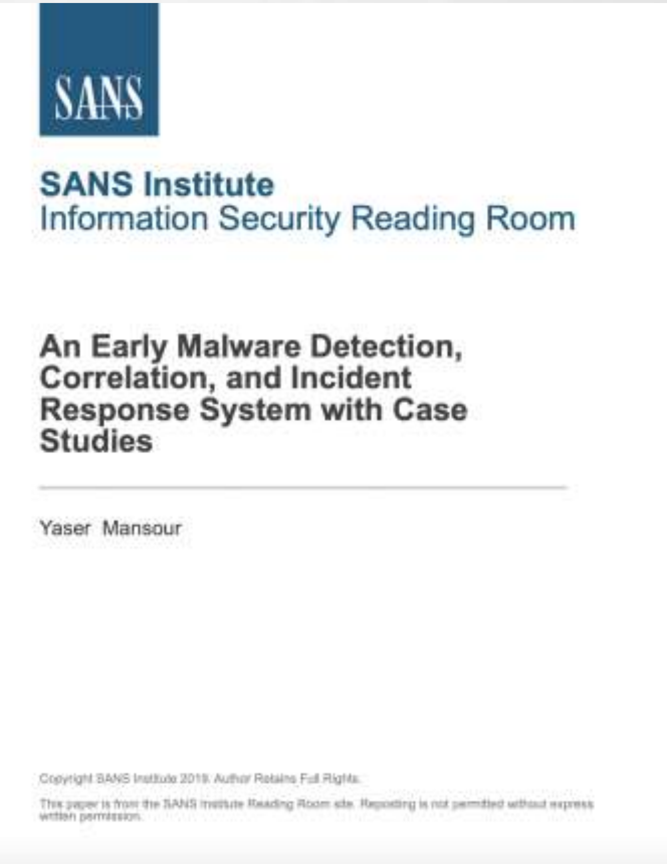
RSA Incident Response Case Study

SANS: An Early Malware Detection, Correlation, and Incident Response System with Case Studies

https://www.sans.org/reading-room/whitepapers/detection/early-malware-detection-correlation-incident-response-system-case-studies-34485

The proposed framework consists of four key components; Logging and Correlation, Detection, Response, and Reporting.




SANS

SANS Institute
Information Security Reading Room

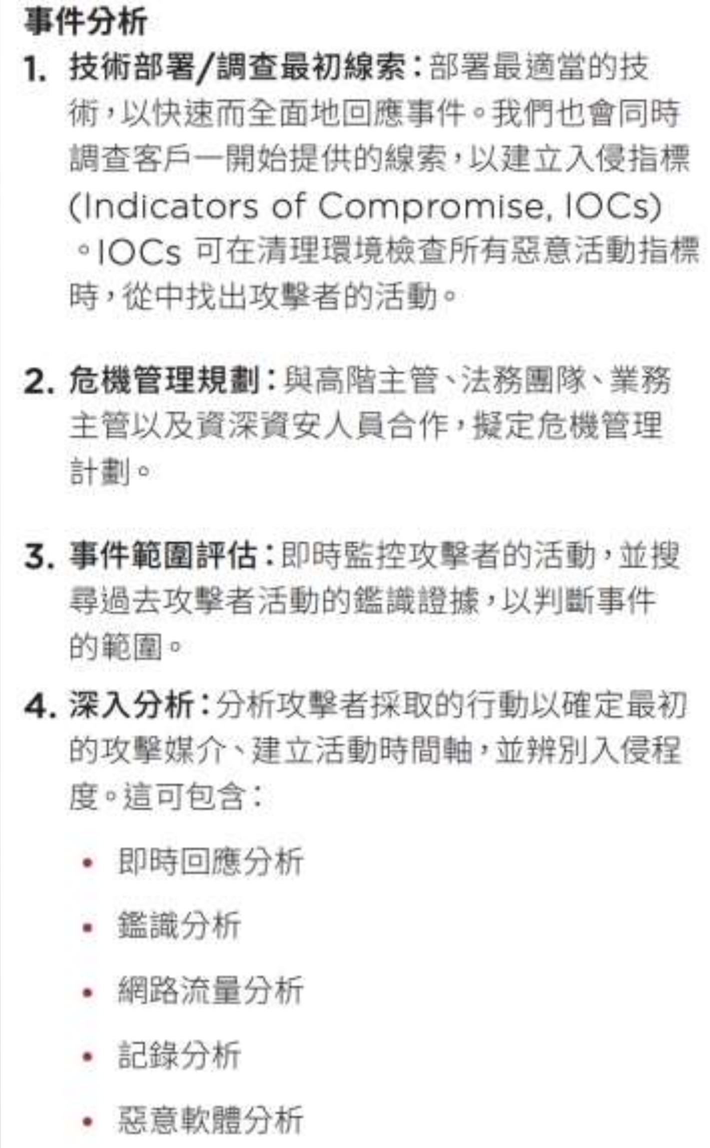
An Early Malware Detection, Correlation, and Incident Response System with Case Studies

Yaser Mansour

IR service

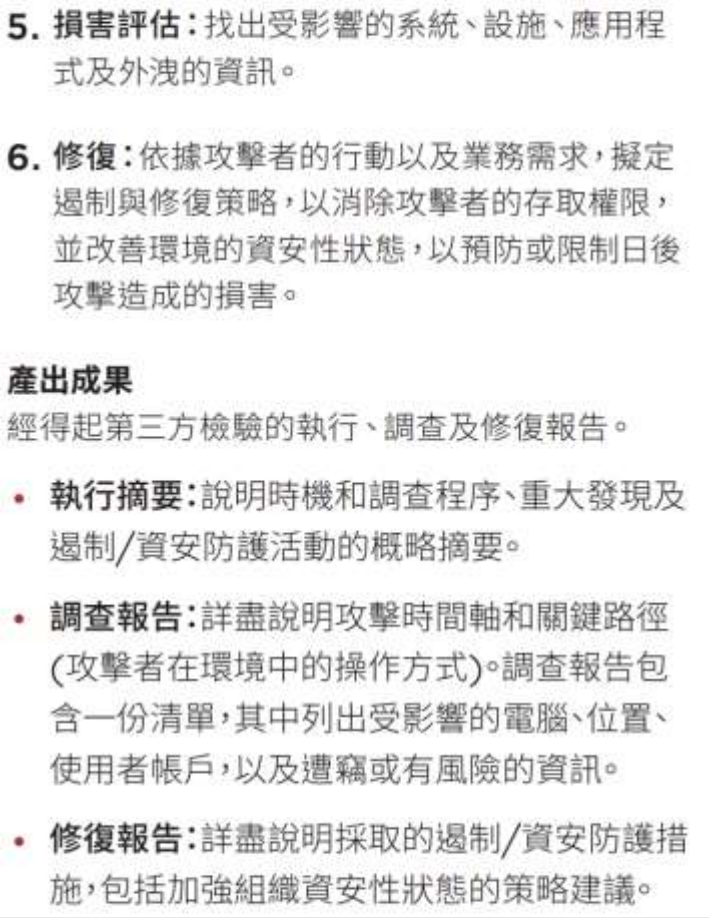
- FireEye
  - MANDIANT

    https://www.fireeye.com/content/dam/fireeye-www/regional/zh_TW/services/pdfs/ds-mandiant-incident-response-services.pdf



事件分析

1. **技術部署/調查最初線索：**部署最適當的技術，以快速而全面地回應事件。我們也會同時調查客戶一開始提供的線索，以建立入侵指標(Indicators of Compromise, IOCs)。IOCs 可在清理環境檢查所有惡意活動指標時，從中找出攻擊者的活動。
2. **危機管理規劃：**與高階主管、法務團隊、業務主管以及資深資安人員合作，擬定危機管理計劃。
3. **事件範圍評估：**即時監控攻擊者的活動，並搜尋過去攻擊者活動的鑑識證據，以判斷事件的範圍。
4. **深入分析：**分析攻擊者採取的行動以確定最初的攻擊媒介、建立活動時間軸，並辨別入侵程度。這可包含：
   - 即時回應分析
   - 鑑識分析
   - 網路流量分析
   - 記錄分析
   - 惡意軟體分析



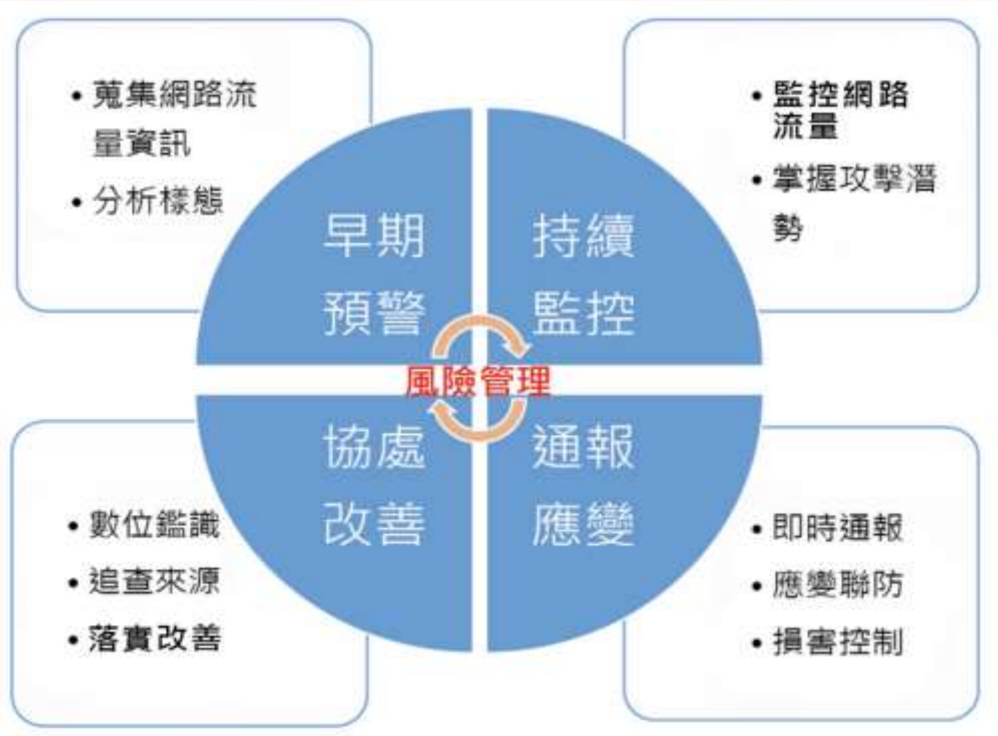
5. **損害評估：**找出受影響的系統、設施、應用程式及外洩的資訊。
6. **修復：**依據攻擊者的行動以及業務需求，擬定遏制與修復策略，以消除攻擊者的存取權限，並改善環境的資安性狀態，以預防或限制日後攻擊造成的損害。

產出成果

經得起第三方檢驗的執行、調查及修復報告。

- **執行摘要：**說明時機和調查程序、重大發現及遏制/資安防護活動的概略摘要。
- **調查報告：**詳盡說明攻擊時間軸和關鍵路徑(攻擊者在環境中的操作方式)。調查報告包含一份清單，其中列出受影響的電腦、位置、使用者帳戶，以及遭竊或有風險的資訊。
- **修復報告：**詳盡說明採取的遏制/資安防護措施，包括加強組織資安性狀態的策略建議。

Cybersecurity Strategy of Department of Cyber Security



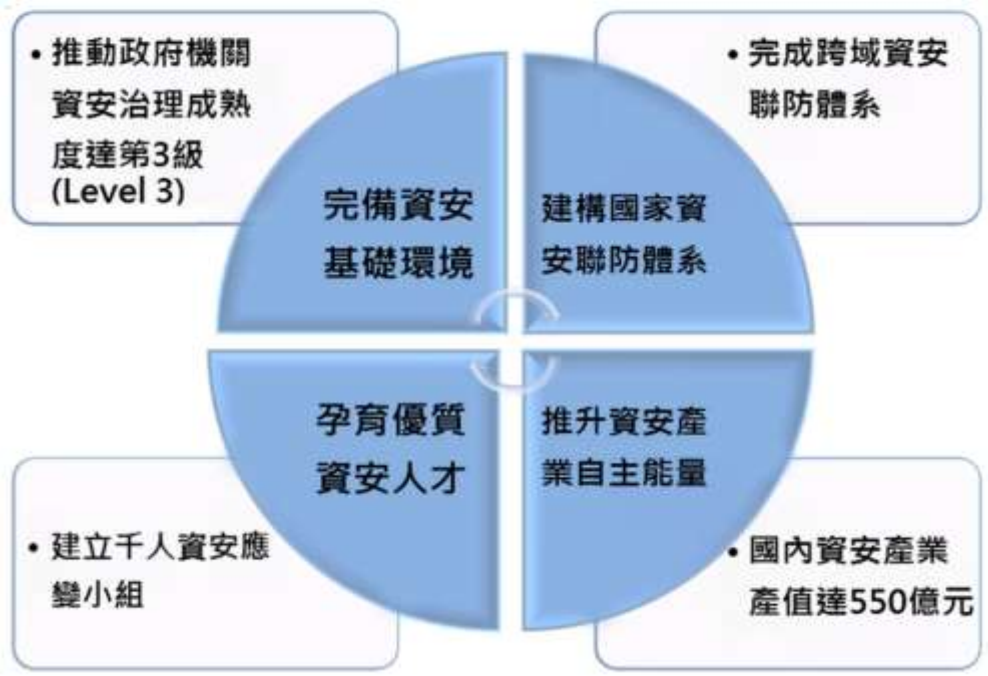
風險管理

早期預警
- 蒐集網路流量資訊
- 分析樣態

持續監控
- 監控網路流量
- 掌握攻擊潛勢

協處改善
- 數位鑑識
- 追查來源
- 落實改善

通報應變
- 即時通報
- 應變聯防
- 損害控制



完備資安基礎環境
- 推動政府機關資安治理成熟度達第3級(Level 3)

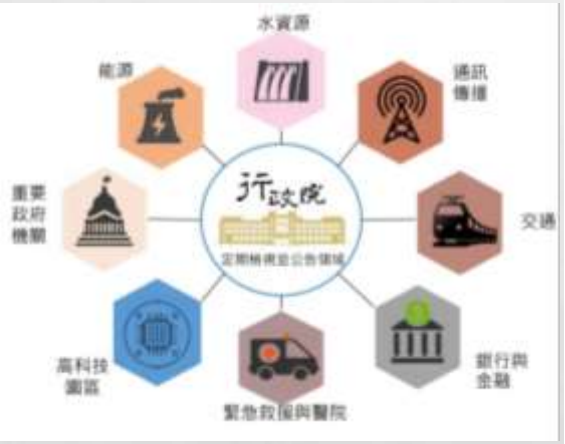
建構國家資安聯防體系
- 完成跨域資安聯防體系

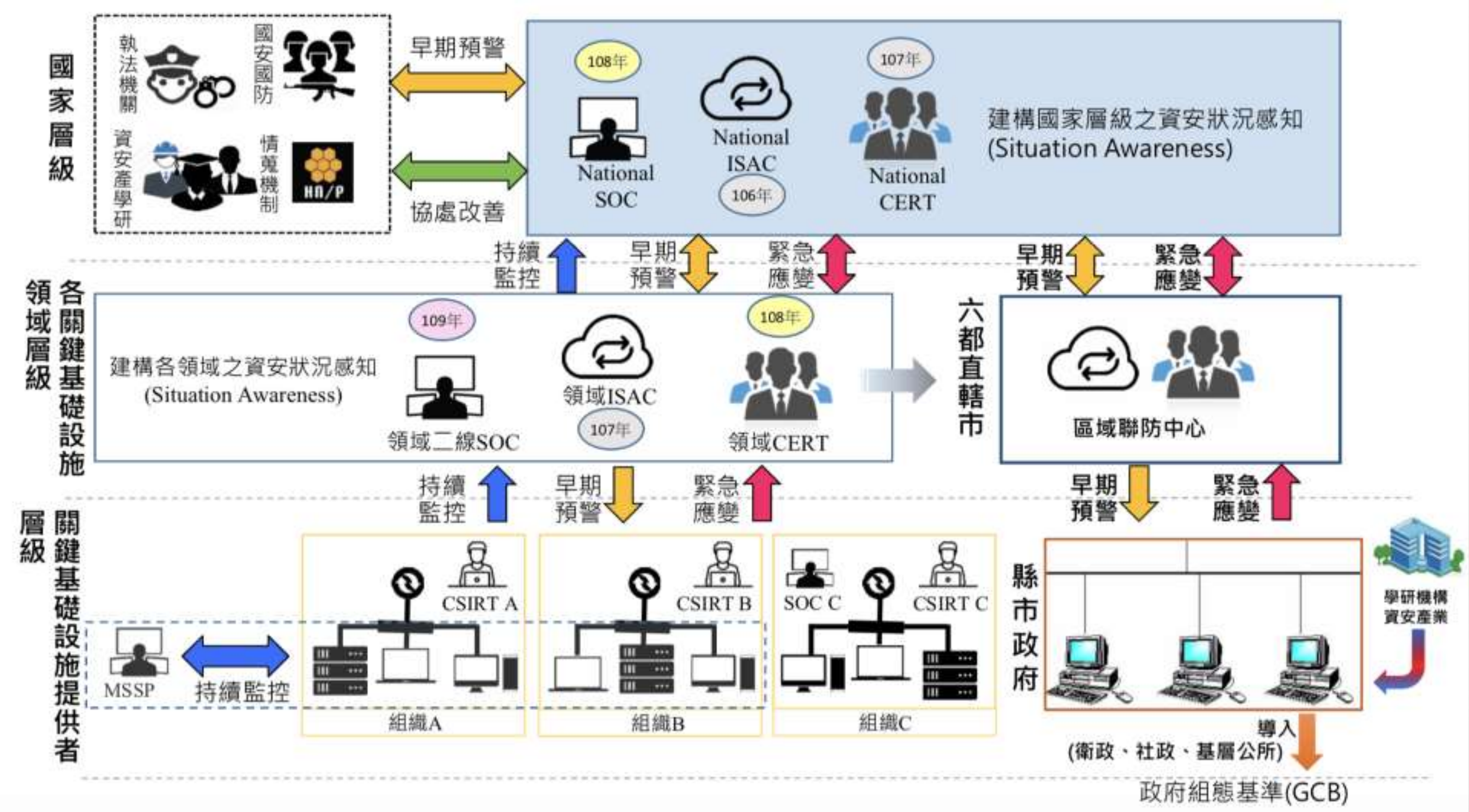
孕育優質資安人才
- 建立千人資安應變小組

推升資安產業自主能量
- 國內資安產業產值達550億元

Source: 行政院資安處

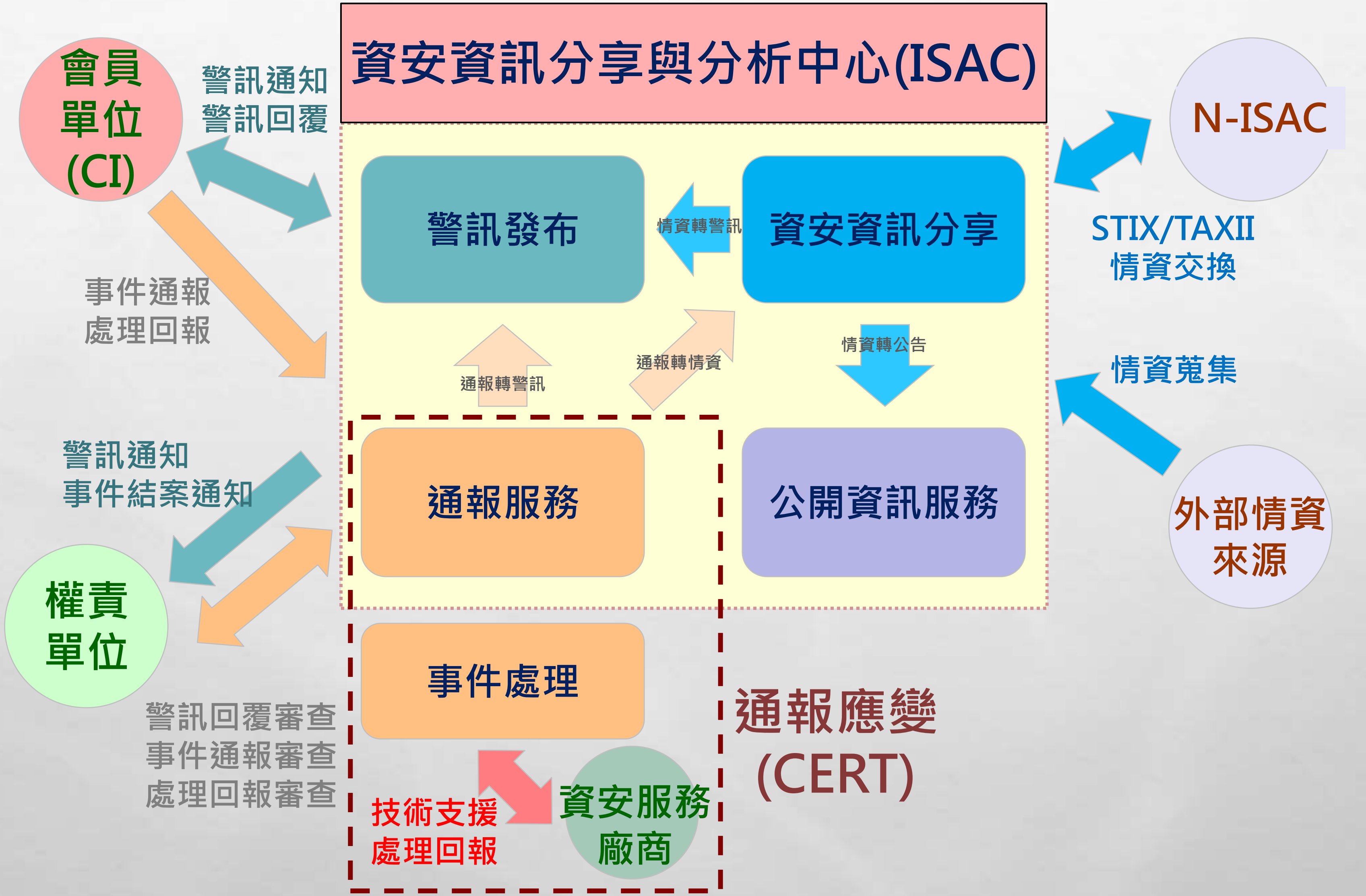
Automatic intelligence sharing





Source: 行政院資安處

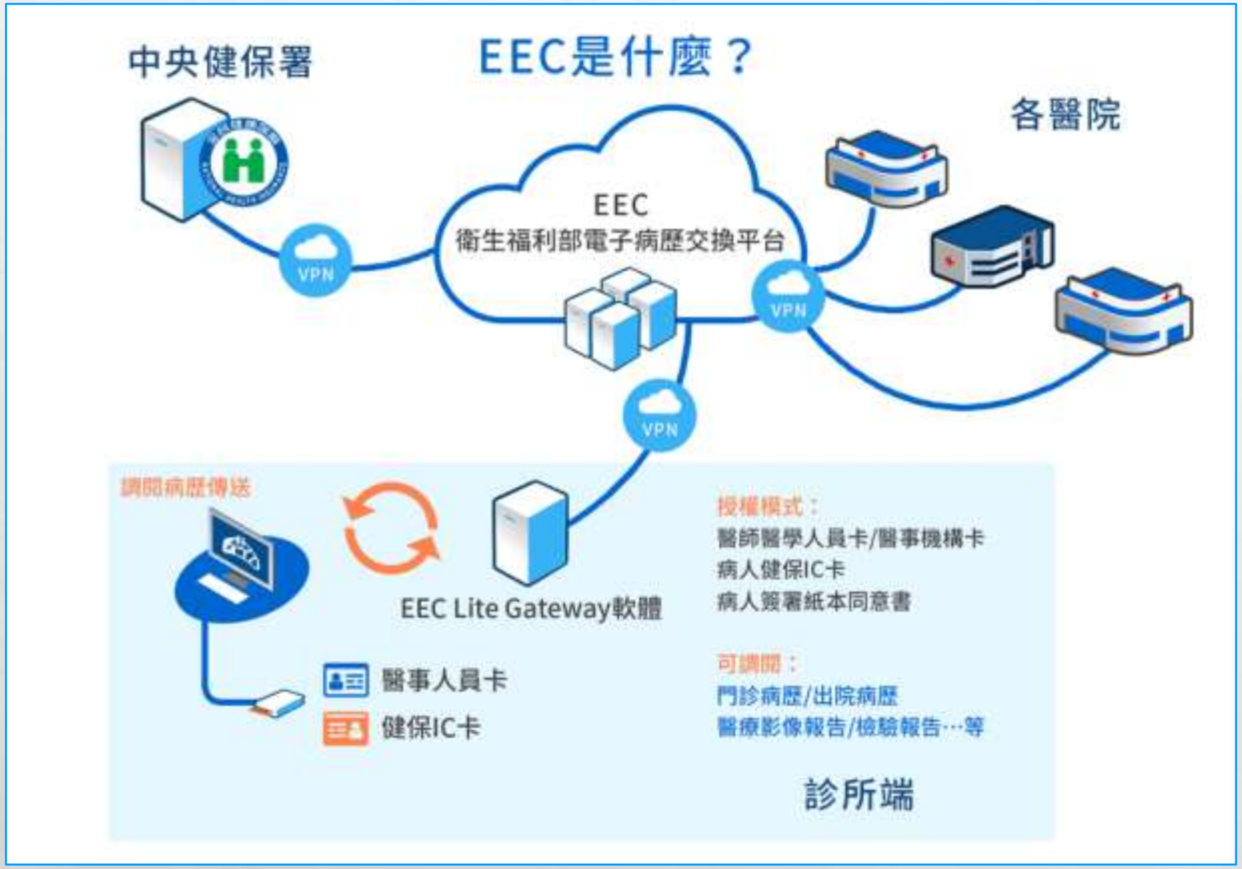
Threat Intelligence Sharing and Response Framework



醫院勒索軟體事件

- EEC Gateway
- GlobeImposter ransomware
- 感染擴散途徑推測

Electronic Medical Record Exchange Center
電子病歷交換中心



EEC是什麼？

中央健保署

各醫院

EEC
衛生福利部電子病歷交換平台

VPN

調閱病歷傳送

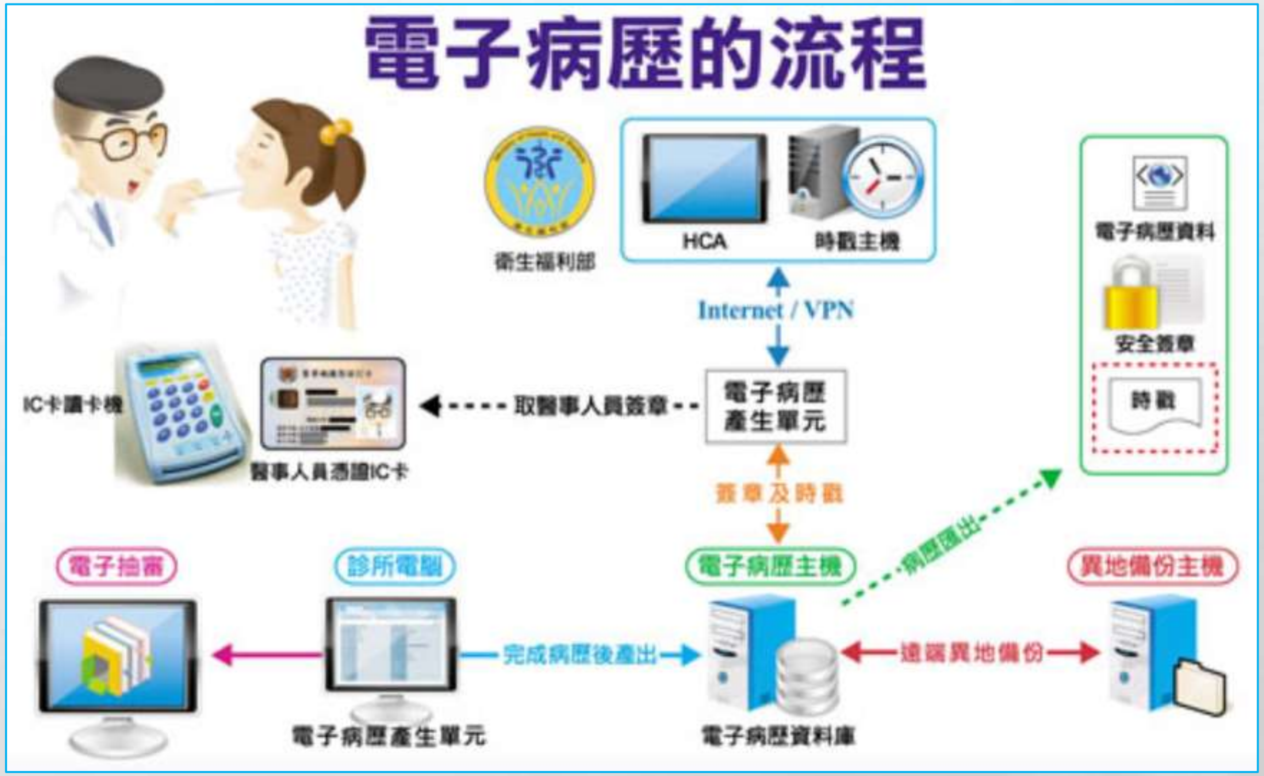
EEC Lite Gateway軟體

醫事人員卡
健保IC卡

授權模式：
醫師醫學人員卡/醫事機構卡
病人健保IC卡
病人簽署紙本同意書

可調閱：
門診病歷/出院病歷
醫療影像報告/檢驗報告…等

診所端

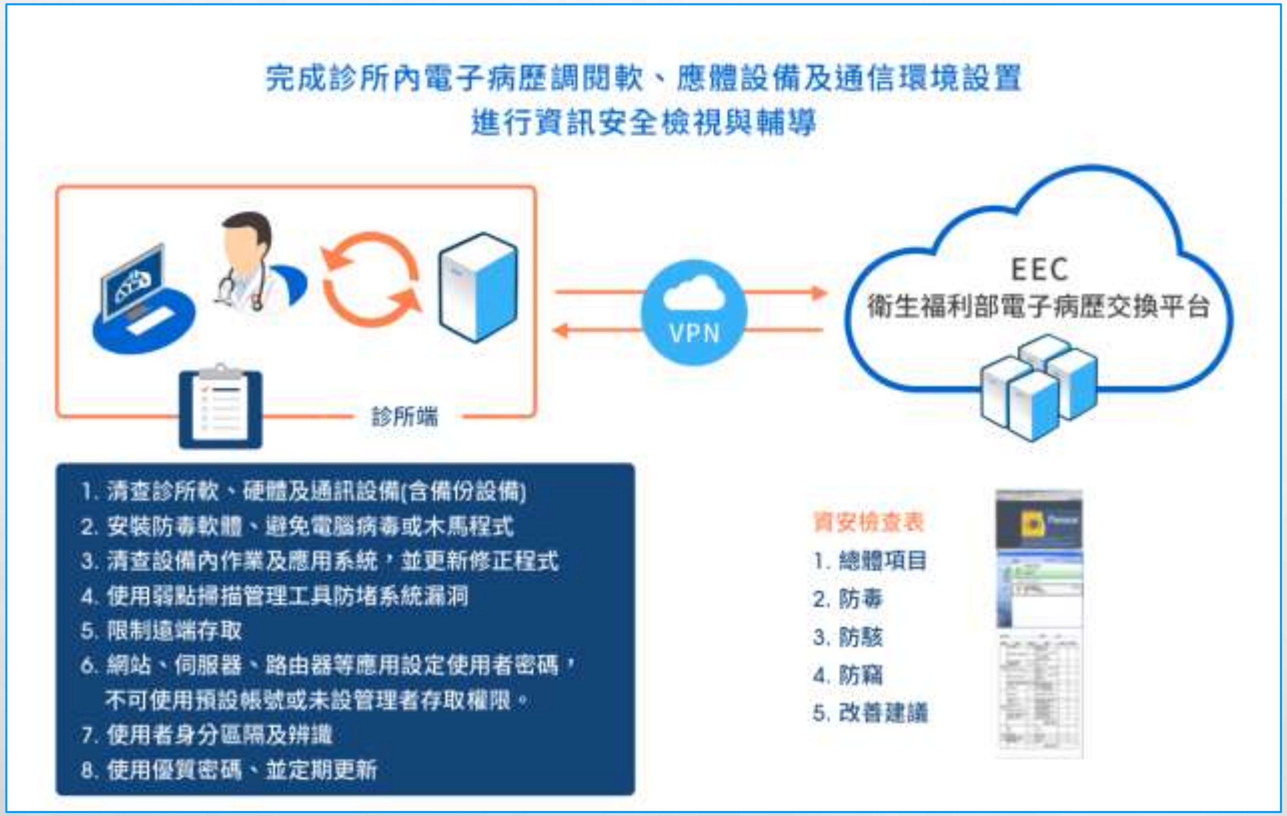


電子病歷的流程

衛生福利部
HCA
時戳主機
Internet / VPN
IC卡讀卡機
醫事人員憑證IC卡
取醫事人員簽章
電子病歷產生單元
簽章及時戳
電子病歷資料
安全簽章
時戳
病歷匯出
電子抽審
診所電腦
電子病歷主機
異地備份主機
完成病歷後產出
遠端異地備份
電子病歷產生單元
電子病歷資料庫

EEC gateway：電子病歷交換閘道器
資料來源： http://www.vision.com.tw/EMR.html

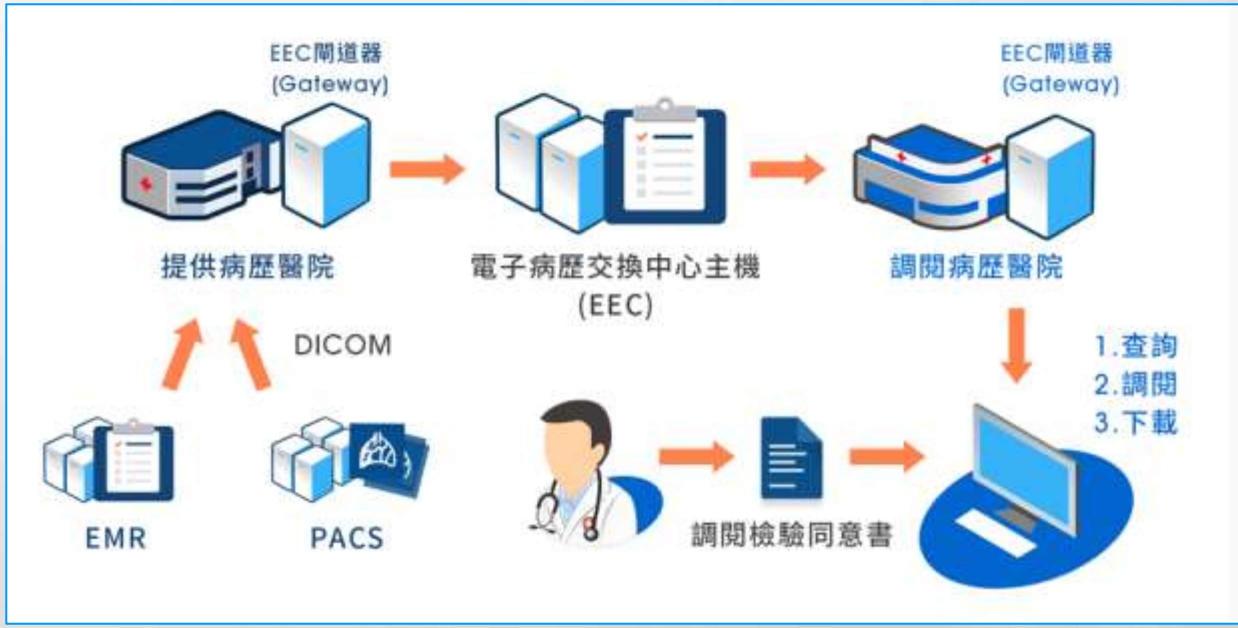
Electronic Medical Record Exchange Center
電子病歷交換中心



完成診所內電子病歷調閱軟、應體設備及通信環境設置
進行資訊安全檢視與輔導

1. 清查診所軟、硬體及通訊設備(含備份設備)
2. 安裝防毒軟體、避免電腦病毒或木馬程式
3. 清查設備內作業及應用系統，並更新修正程式
4. 使用弱點掃描管理工具防堵系統漏洞
5. 限制遠端存取
6. 網站、伺服器、路由器等應用設定使用者密碼，不可使用預設帳號或未設管理者存取權限。
7. 使用者身分區隔及辨識
8. 使用優質密碼、並定期更新

資安檢查表
1. 總體項目
2. 防毒
3. 防駭
4. 防竊
5. 改善建議



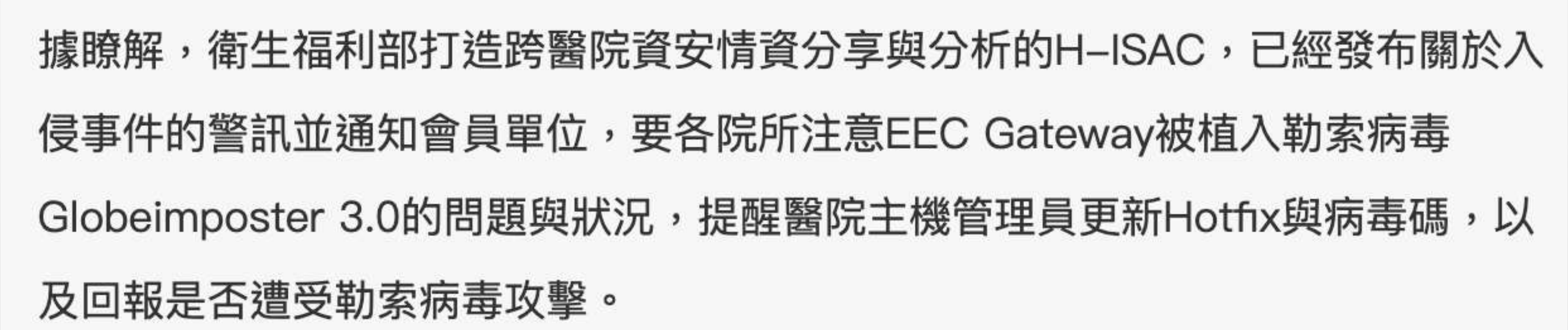
EMR：Electronic Medical Record 電子病歷
PACS：Picture archiving and communication system
醫療影像儲傳系統
資料來源：http://www.vision.com.tw/EMR.html

DICOM： Digital Imaging and Communications in Medicine 醫療數位影像傳輸協定

新聞報導

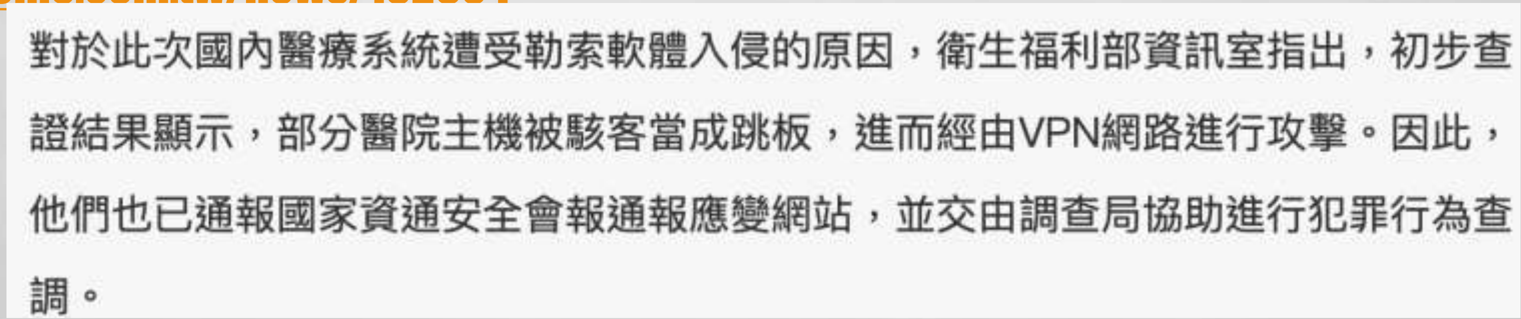
8/31[iThome] 兩家衛福部所屬醫院遭勒索軟體襲擊，確認臺灣已有10多間醫院遇害
https://www.ithome.com.tw/news/132781

8/31[中央通訊社] 全台10餘家醫院中勒索病毒 密碼管理成漏洞
https://www.cna.com.tw/news/firstnews/201908310101.aspx



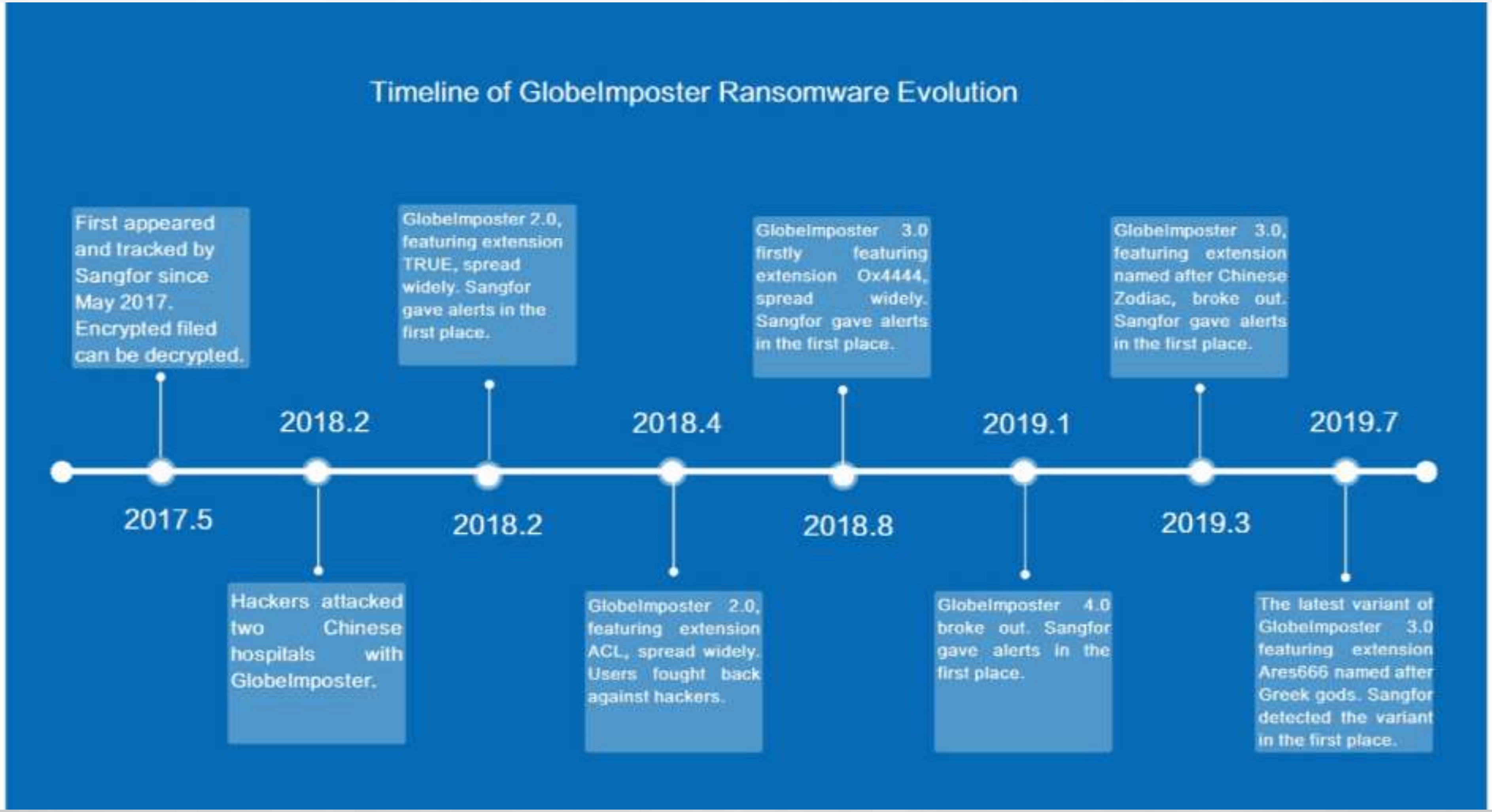
據瞭解，衛生福利部打造跨醫院資安情資分享與分析的H–ISAC，已經發布關於入侵事件的警訊並通知會員單位，要各院所注意EEC Gateway被植入勒索病毒Globeimposter 3.0的問題與狀況，提醒醫院主機管理員更新Hotfix與病毒碼，以及回報是否遭受勒索病毒攻擊。

9/2[iThome] 衛福部晚間公布臺灣醫療院所受勒索軟體攻擊現況，已有22家遇害
https://ithome.com.tw/news/132804



對於此次國內醫療系統遭受勒索軟體入侵的原因，衛生福利部資訊室指出，初步查證結果顯示，部分醫院主機被駭客當成跳板，進而經由VPN網路進行攻擊。因此，他們也已通報國家資通安全會報通報應變網站，並交由調查局協助進行犯罪行為查調。

GlobeImposter Evolution



Timeline of GlobeImposter Ransomware Evolution

2017.5 — First appeared and tracked by Sangfor since May 2017. Encrypted filed can be decrypted.

2018.2 — Hackers attacked two Chinese hospitals with GlobeImposter.

2018.2 — GlobeImposter 2.0, featuring extension TRUE, spread widely. Sangfor gave alerts in the first place.

2018.4 — GlobeImposter 2.0, featuring extension ACL, spread widely. Users fought back against hackers.

2018.8 — GlobeImposter 3.0 firstly featuring extension Ox4444, spread widely. Sangfor gave alerts in the first place.

2019.1 — GlobeImposter 4.0 broke out. Sangfor gave alerts in the first place.

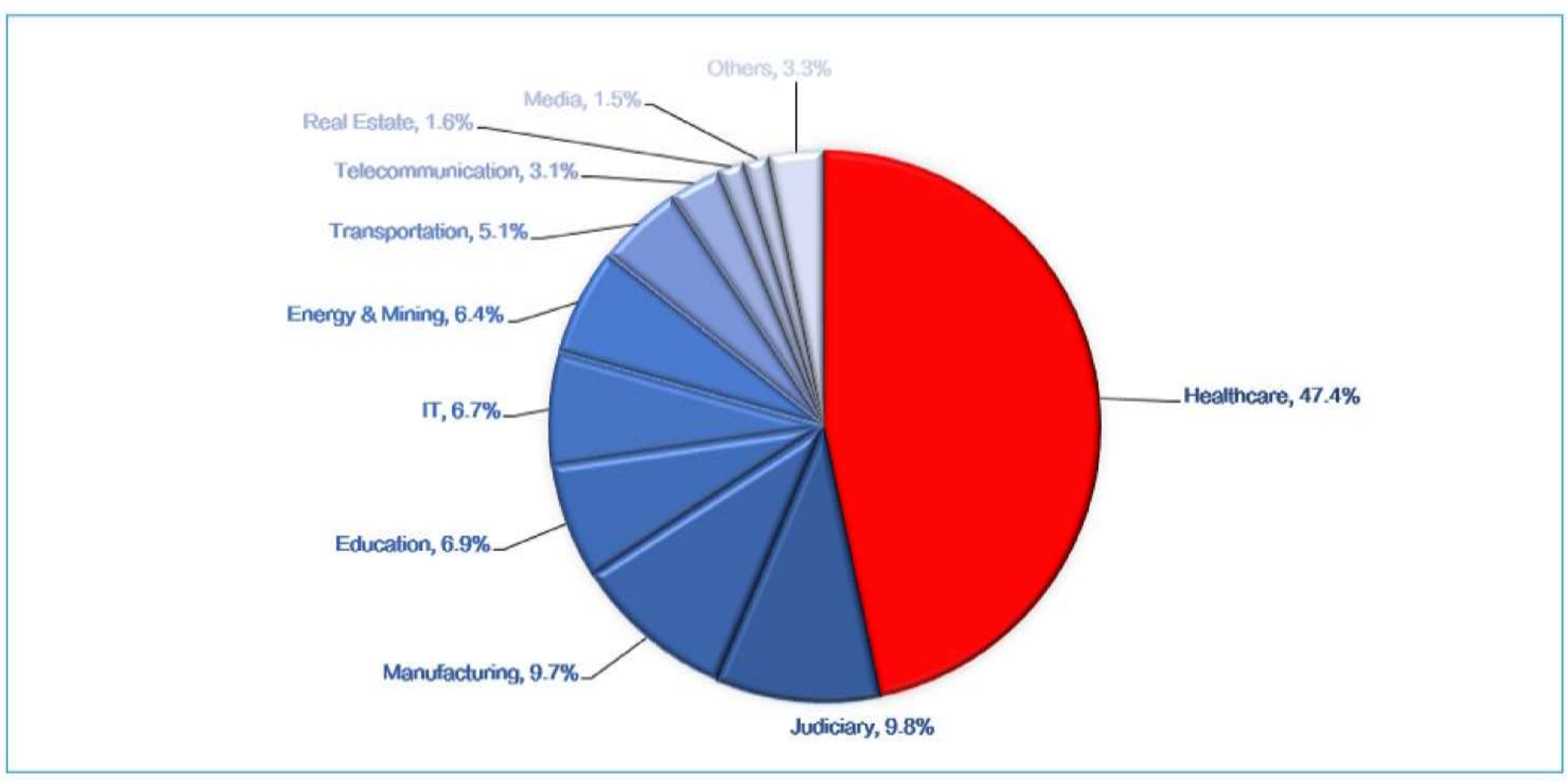
2019.3 — GlobeImposter 3.0, featuring extension named after Chinese Zodiac, broke out. Sangfor gave alerts in the first place.

2019.7 — The latest variant of GlobeImposter 3.0 featuring extension Ares666 named after Greek gods. Sangfor detected the variant in the first place.

[Alert] New GlobeImposter Ransomware Variant in Healthcare Industry (2019/7/9)

https://www.sangfor.com/source/blog-network-security/1311.html

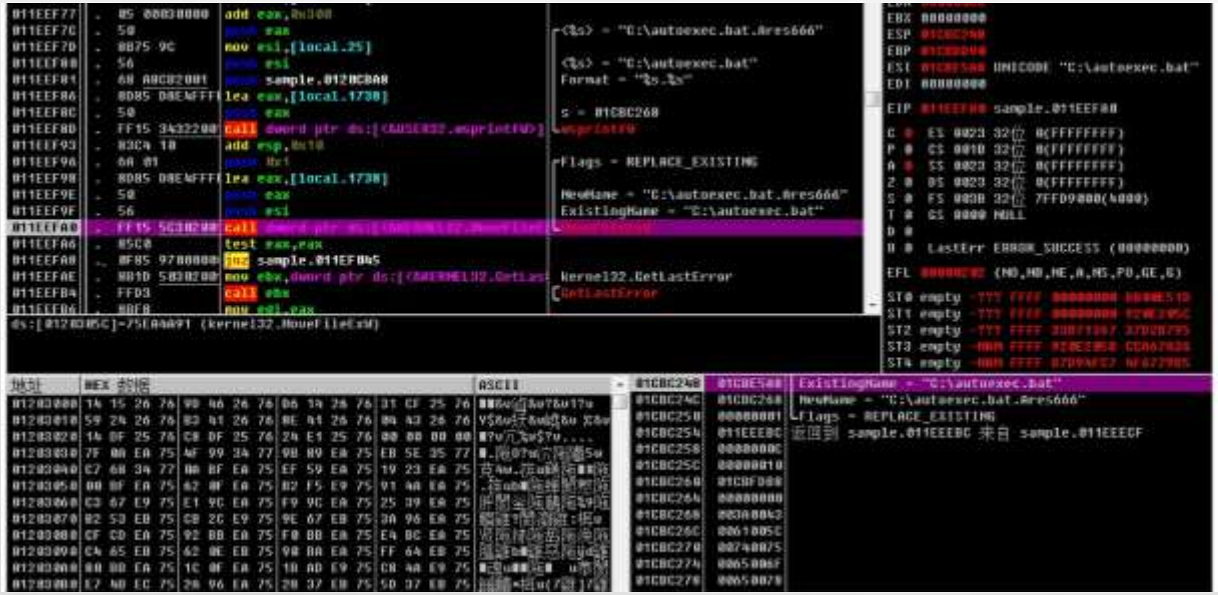
Affected Industry



[Alert] New GlobeImposter Ransomware Variant in Healthcare Industry (2019/7/9)
https://www.sangfor.com/source/blog-network-security/1311.html

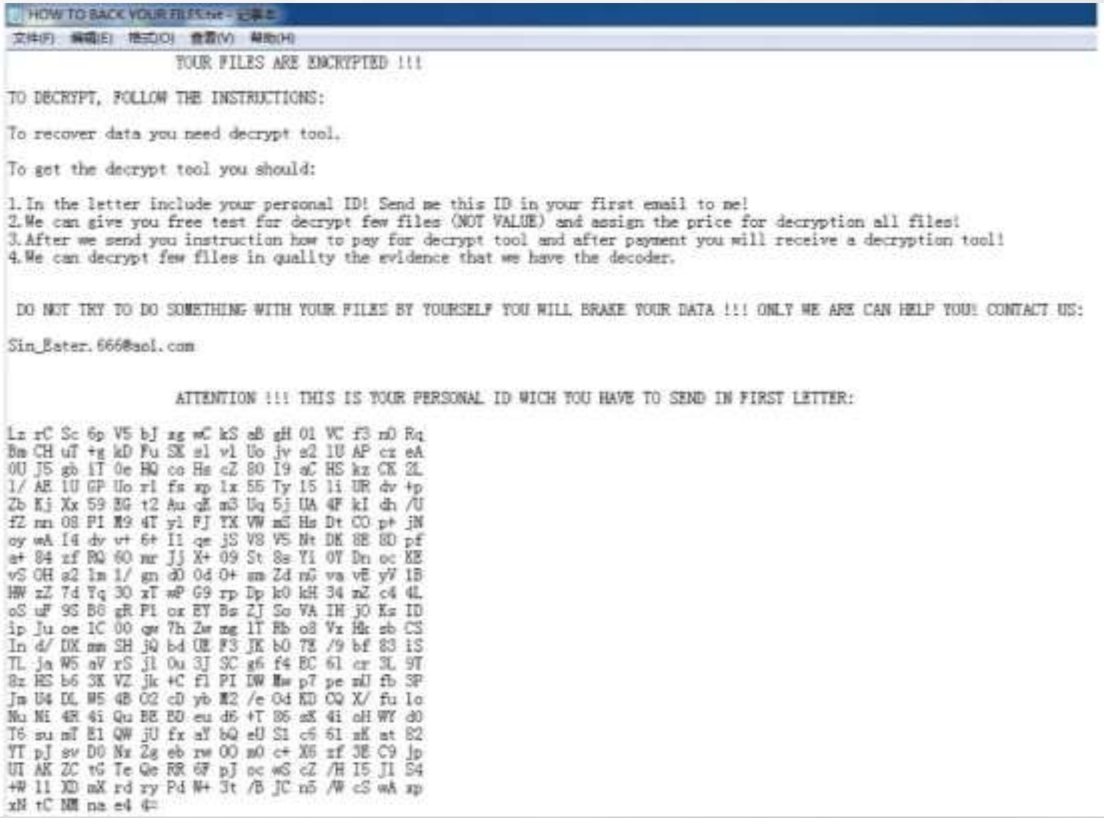
GlobeImposter 3.0

Other files are encrypted and appended with Ares666



```
011EEF77  .  05 00030000   add eax,0x300
011EEF7C  .  50            push eax                                   ┌<%s> = "C:\autoexec.bat.Ares666"
011EEF7D  .  8B75 9C       mov esi,[local.25]                         │
011EEF80  .  56            push esi                                   │<%s> = "C:\autoexec.bat"
011EEF81  .  68 A8CB2001   push sample.0120CBA8                       │Format = "%s.%s"
011EEF86  .  8D85 D0EAFFFF lea eax,[local.1738]                       │
011EEF8C  .  50            push eax                                   │s = 01CBC268
011EEF8D  .  FF15 34322001 call dword ptr ds:[<&USER32.wsprintfW>]    └wsprintfW
011EEF93  .  83C4 10       add esp,0x10
011EEF96  .  6A 01         push 0x1                                   ┌Flags = REPLACE_EXISTING
011EEF98  .  8D85 D0EAFFFF lea eax,[local.1738]                       │
011EEF9E  .  50            push eax                                   │NewName = "C:\autoexec.bat.Ares666"
011EEF9F  .  56            push esi                                   │ExistingName = "C:\autoexec.bat"
011EEFA0  .  FF15 5C302001 call dword ptr ds:[<&KERNEL32.MoveFileExW>] └MoveFileExW
011EEFA6  .  85C0          test eax,eax
011EEFA8  .  0F85 97000000 jnz sample.011EF045
011EEFAE  .  8B1D 58302001 mov ebx,dword ptr ds:[<&KERNEL32.GetLas    kernel32.GetLastError
011EEFB4  .  FFD3          call ebx                                   [GetLastError
011EEFB6  .  8BF8          mov edi,eax
ds:[0120305C]=75EA4A91 (kernel32.MoveFileExW)

EBX 00000000
ESP [illegible]
EBP [illegible]
ESI [illegible] UNICODE "C:\autoexec.bat"
EDI 00000000

EIP [illegible] sample.011EEFA0

C 0  ES 0023 32位 0(FFFFFFFF)
P 0  CS 001B 32位 0(FFFFFFFF)
A 0  SS 0023 32位 0(FFFFFFFF)
Z 0  DS 0023 32位 0(FFFFFFFF)
S 0  FS 003B 32位 7FFD9000(4000)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL [illegible] (NO,NB,NE,A,NS,PO,GE,G)

ST0 empty [illegible]
ST1 empty [illegible]
ST2 empty [illegible]
ST3 empty [illegible]
ST4 empty [illegible]

地址      HEX 数据                                      ASCII
01203000  14 15 26 76 90 46 26 76 06 14 26 76 31 CF 25 76
01203010  59 24 26 76 83 41 26 76 8E 41 26 76 84 43 26 76
01203020  14 DF 25 76 C8 DF 25 76 24 E1 25 76 00 00 00 00
01203030  7F AA EA 75 4F 99 34 77 98 A9 EA 75 EB 5E 35 77
01203040  C7 68 34 77 AA BF EA 75 EF 59 EA 75 19 23 EA 75
01203050  00 BF EA 75 62 AF EA 75 B2 F5 E9 75 91 4A EA 75
01203060  C3 67 E9 75 E1 9C EA 75 F9 9C EA 75 25 39 EA 75
01203070  B2 53 EB 75 CB 2C E9 75 9E 67 EB 75 3A 96 EA 75
01203080  CF CD EA 75 92 BB EA 75 F0 BB EA 75 E4 BC EA 75
01203090  C4 65 EB 75 62 0E EB 75 90 BA EA 75 FF 64 EB 75
012030A0  AA BB EA 75 1C AF EA 75 1A AD E9 75 CA 4A E9 75
012030B0  E7 4B EC 75 2B 96 EA 75 2B 37 EB 75 5D 37 EB 75

01CBC248  01CBE540  ┌ExistingName = "C:\autoexec.bat"
01CBC24C  01CBC268  │NewName = "C:\autoexec.bat.Ares666"
01CBC250  00000001  └Flags = REPLACE_EXISTING
01CBC254  011EEEBC  返回到 sample.011EEEBC 来自 sample.011EEECF
01CBC258  0000000C
01CBC25C  00000010
01CBC260  01CBF000
01CBC264  00000000
01CBC268  003A0043
01CBC26C  0061005C
01CBC270  00740075
01CBC274  0065006F
01CBC278  00650078
```

The ransom note file (HOW TO BACK YOUR FILES.txt)


HOW TO BACK YOUR FILES.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
                    YOUR FILES ARE ENCRYPTED !!!

TO DECRYPT, FOLLOW THE INSTRUCTIONS:

To recover data you need decrypt tool.

To get the decrypt tool you should:

1.In the letter include your personal ID! Send me this ID in your first email to me!
2.We can give you free test for decrypt few files (NOT VALUE) and assign the price for decryption all files!
3.After we send you instruction how to pay for decrypt tool and after payment you will receive a decryption tool!
4.We can decrypt few files in quality the evidence that we have the decoder.


 DO NOT TRY TO DO SOMETHING WITH YOUR FILES BY YOURSELF YOU WILL BRAKE YOUR DATA !!! ONLY WE ARE CAN HELP YOU! CONTACT US:

Sin_Eater.666@aol.com


                    ATTENTION !!! THIS IS YOUR PERSONAL ID WICH YOU HAVE TO SEND IN FIRST LETTER:

Lz rC Sc 6p V5 bJ zg wC kS aB gH 01 VC f3 m0 Rq
Bm CH uT +g kD Fu SX sl vl Uo jv s2 1U AP cz eA
0U J5 gb iT 0e HQ co Hs cZ 80 I9 aC HS kz CK 2L
1/ AE 1U GP Uo rl fs xp 1x 55 Ty 15 1i UR dv +p
Zb Kj Xx 59 EG t2 Au qE m3 Uq 5j UA 4F kI dh /U
fZ mn 08 PI M9 4T yl FJ TX VW mS Hs Dt CO p+ jN
oy wA I4 dv v+ 6+ I1 qe jS V8 V5 Nt DK 8E 8D pf
a+ 84 zf RQ 60 mr JJ X+ 09 St 8s Yi 0Y Dn oc KE
vS OH a2 Im 1/ gn d0 0d O+ sm Zd nG va vE yV 1B
HW zZ 7d Yq 30 xT wP G9 rp Dp k0 kH 34 mZ c4 4L
oS uF 9S B0 gR P1 ox EY Bs ZJ So VA IH j0 Ks ID
ip Ju oe 1C 00 qw 7h Zw mg 1T Rb o8 Vx Hk sb CS
In d/ DX mm SH jQ bd UE F3 JK b0 7E /9 bf 83 iS
TL ja W5 aV rS jl Ou 3J SC g6 f4 BC 61 cr 3L 9T
8z HS b6 3K VZ jk +C f1 PI DW Mw p7 pe mU fb SP
Jm U4 DL W5 4B O2 cD yb M2 /e Od KD CQ X/ fu lo
Nu Ni 4R 4i Qu BE BD eu d6 +T B6 sK 4i oH WY d0
T6 su mT E1 QW jU fx aY bQ eU S1 c6 61 sK at 82
YT pJ sv D0 Nx Zg eb rw 00 m0 c+ X6 zf 3E C9 jp
UI AK ZC tG Te Qe RR 6F pJ oc wS cZ /H I5 JI S4
+W 11 XD mX rd ry Pd N+ 3t /B JC n5 /W cS wA xp
xN tC NM na e4 4=
```

[Alert] New GlobeImposter Ransomware Variant in Healthcare Industry (2019/7/9)

https://www.sangfor.com/source/blog-network-security/1311.html

GlobeImposter versions

版本 項目	1.0	2.0	3.0	4.0
較大規模爆發時間	2017年9月	2018年3月	2018年8月	2019年
加密後副檔名	.CHAK	.TRUE、.doc	.*4444	. Appollon865 . fuck
加密方法	AES + RSA(RSA2048)			
加密目標	各磁碟 (外接、固定、網路) (3.0版不限檔案類型，全部加密)			
加密後特徵	於被加密目錄下會有 HOW_TO_BACK_FILES.txt 文字檔			
感染途徑	社交工程郵件、遠端桌面協定 1. 利用遠端桌面弱密碼暴力破解，植入病毒 2. 利用社交工程郵件，內含密碼抓取工具或病毒 (js、vbs、exe、scr、bat)			
相關埠號	135、139、445、3389 (遠端桌面 + 網路芳鄰 + 遠程程序呼叫)			

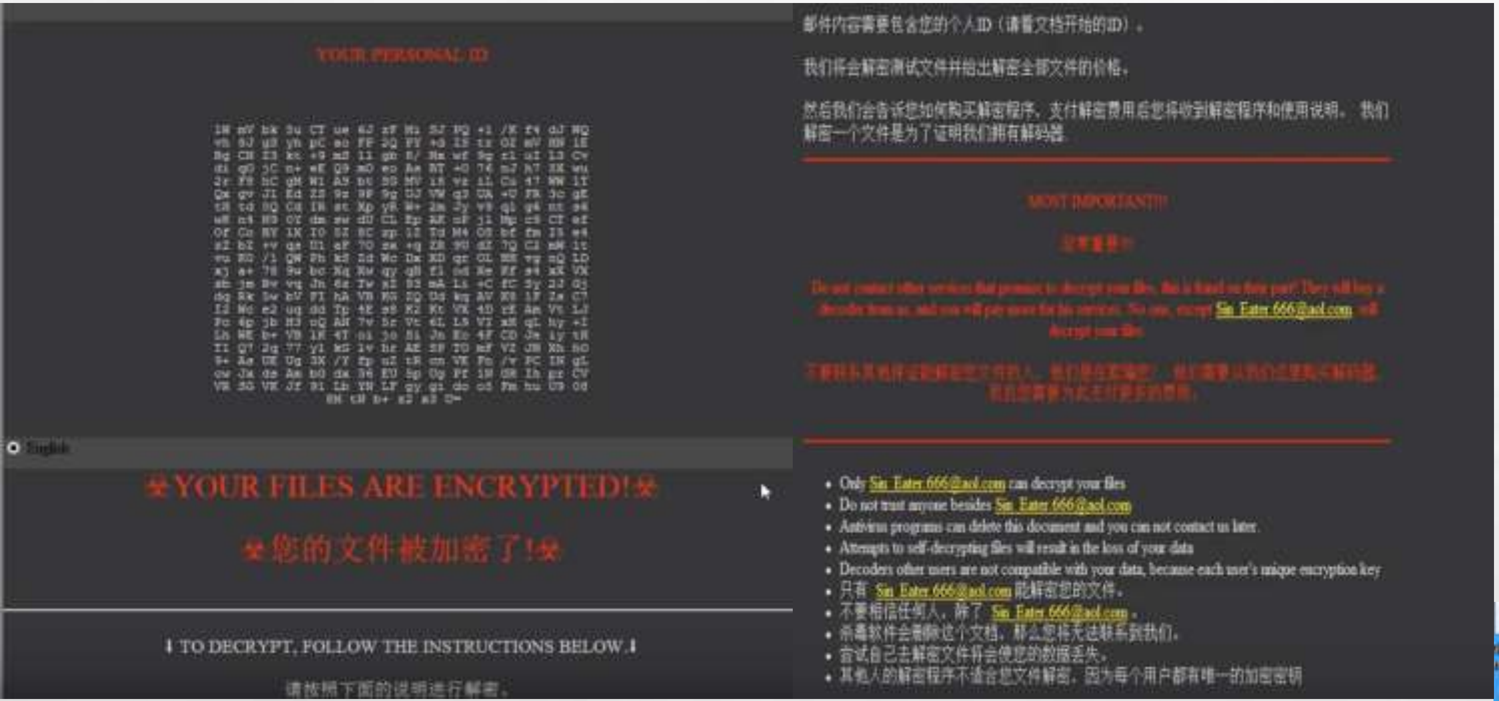
資料來源：http://www.sangfor.com.cn/about/source-news-company-news/1089.html
https://isecurity.huawei.com/sec/web/viewAlert.do?id=2098

GlobeImposter變種

- GlobeImposter勒索病毒首次出現是在2017年5月份，主要通過釣魚郵件進行傳播，2018年2月國內各大醫院爆發GlobeImposter變種樣本2.0版本，通過溯源分析發現此勒索病毒可能是通過RDP爆破、社會工程等方式進行傳播，此勒索病毒採用RSA2048加密算法，導致加密後的文件無法解密。
- GlobeImposter3.0採用了十二生肖英文名+4444的加密後綴
- GlobeImposter4.0，此勒索病毒加密後綴為fuck等，生成的勒索信息超文本文件README_BACK_FILES.htm

GlobeImposter勒索病毒變種家族史，看這篇就夠了
https://kknews.cc/tech/5r29o98.html

New #GlobeImposter Ransomware extension .Apollon865!



YOUR PERSONAL ID

1W mV bk 5u CT ue 6J zF M1 SJ PQ +1 /K f4 dJ WQ
vh BJ g5 yh pC ao FP 2Q PY +d IS tr OZ mV HN 1E
Bg CN Z3 kt +9 m5 11 gb 8/ Nx wf 9g r1 uI L3 Cv
d1 qO jC n+ eE Q9 mO eo As BT +O 76 nJ h7 5X wu
2r F8 hC gM W1 A9 bt SG MV 18 vz 1L Cu 47 WW 1T
Qx gv J1 Ed ZS 9z 9P 9g UJ VW q3 UA +U FR 3c gE
tH td 0Q Cd IR st Xp yR W+ 2m Jy v9 q1 g6 nt s6
wK n4 N9 0Y dm sw dU CL Ep AK oP j1 Mp c9 CT ef
Of Co 8Y 1X I0 5Z 8C zp 1Z Td M4 OS bf fm IS e4
zZ bZ +v qs U1 aF 7O sx +q ZR 9U dZ 7Q C2 mW 1t
vu K0 /1 QW Ph k5 Zd Wc Dx XD qr OL HH vg nQ LD
xj a+ 78 9w bc Xq Xw qy qB f1 od Xe Kf s4 xX VX
sb jm Rv vq Jn 6z Tw zZ 93 mA L1 +C fC 5y 2J Gj
dq Rk 5w bV FI hA VB KG 2Q Ud kq AV KB 1F Zs C7
I2 Wc e2 uq dd Tp 4E s8 K2 Kt VX 4D rE Am Vt LJ
Pc 6p jb H3 oQ AN 7v 5r Vt 6L L9 VI xH qL hy +I
Lh WE b+ VB 1K 4T oi jo 5i Jn Eo 4F CD Je iy tH
T1 Q7 2q 77 y1 kG 1v hr AE SP TO mF V2 JN Xh hO
9+ As UE Ug 3X /Y fp uZ tR cn VE Fn /v PC IN gL
ow Jx ds Am bG dx 36 EU 5p Ug Pf 1N GH In pr CV
VR SG VK Jf 91 Lb YN LF gy g1 do o5 Fm hu U9 08
8M tN b+ z2 x3 U=

○ English

☣YOUR FILES ARE ENCRYPTED!☣

☣您的文件被加密了!☣

⬇ TO DECRYPT, FOLLOW THE INSTRUCTIONS BELOW.⬇

请按照下面的说明进行解密。

邮件内容需要包含您的个人ID（请看文档开始的ID）。

我们将会解密测试文件并给出解密全部文件的价格。

然后我们会告诉您如何购买解密程序，支付解密费用后您将收到解密程序和使用说明。 我们解密一个文件是为了证明我们拥有解码器.

MOST IMPORTANT!!!

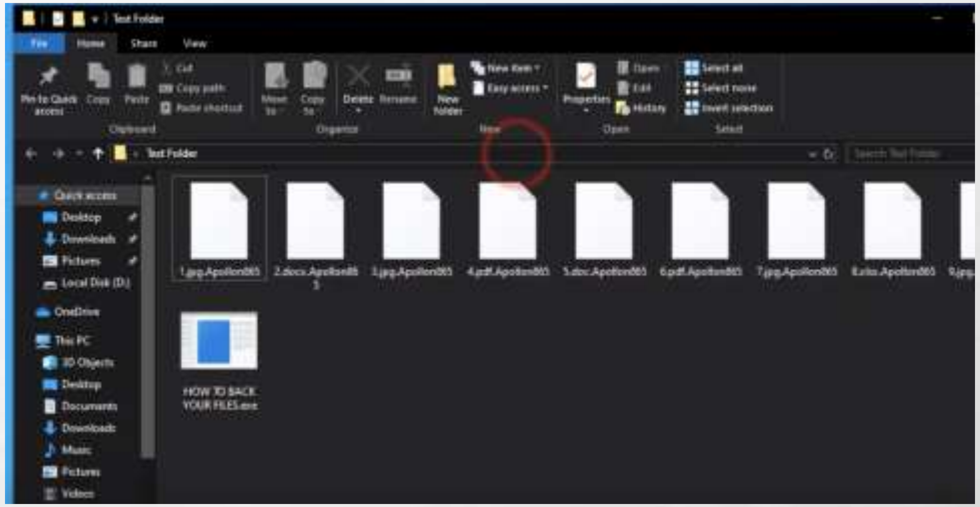
[illegible]

Do not contact other services that promise to decrypt your files, this is fraud on their part! They will buy a decoder from us, and you will pay more for his services. No one, except Sin_Eater 666@aol.com, will decrypt your files.

[illegible]

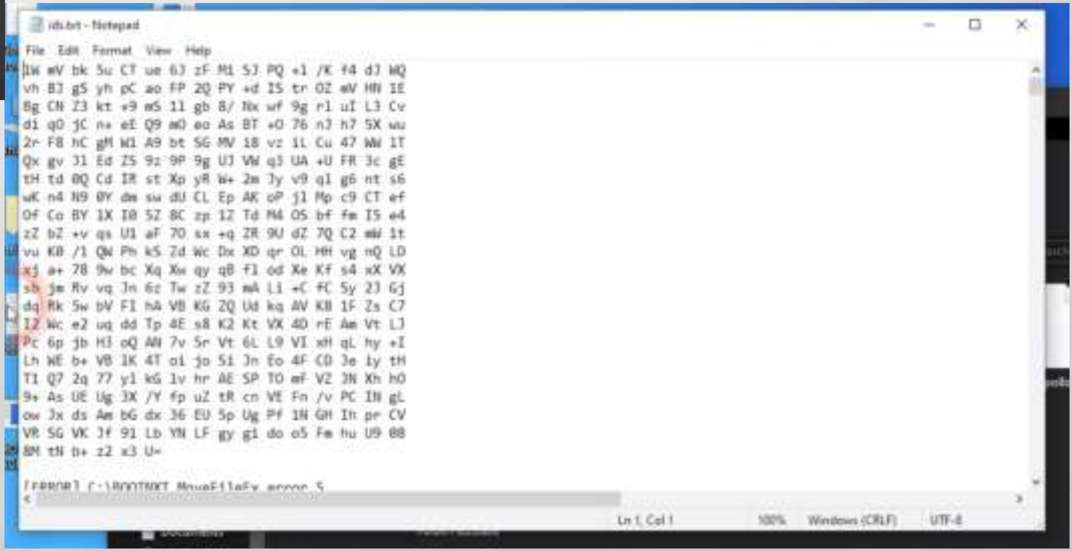
- Only Sin_Eater 666@aol.com can decrypt your files
- Do not trust anyone besides Sin_Eater 666@aol.com
- Antivirus programs can delete this document and you can not contact us later.
- Attempts to self-decrypting files will result in the loss of your data
- Decoders other users are not compatible with your data, because each user's unique encryption key
- 只有 Sin_Eater 666@aol.com 能解密您的文件。
- 不要相信任何人，除了 Sin_Eater 666@aol.com 。
- 杀毒软件会删除这个文档，那么您将无法联系到我们。
- 尝试自己去解密文件将会使您的数据丢失。
- 其他人的解密程序不适合您文件解密，因为每个用户都有唯一的加密密钥

Ransom note



1.jpg.Apollon865
2.docx.Apollon865
3.jpg.Apollon865
4.pdf.Apollon865
5.doc.Apollon865
6.pdf.Apollon865
7.jpg.Apollon865
8.xlsx.Apollon865
9.jpg
HOW TO BACK YOUR FILES.exe

Generated files

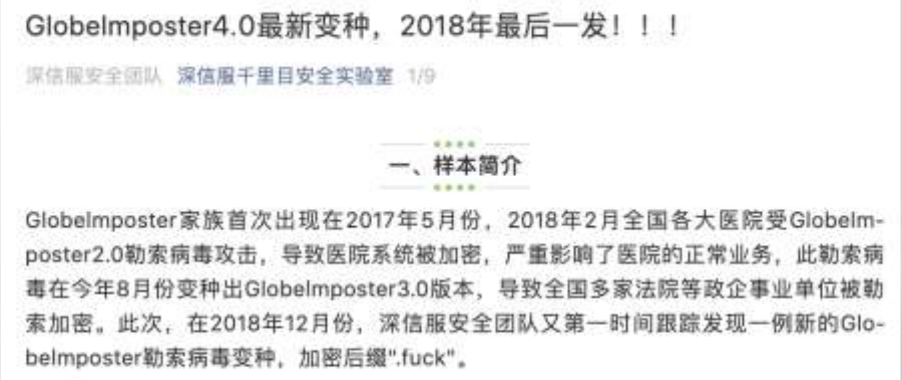


```
1W mV bk 5u CT ue 6J zF M1 SJ PQ +1 /K f4 dJ WQ
vh BJ g5 yh pC ao FP 2Q PY +d IS tr OZ mV HN 1E
Bg CN Z3 kt +9 m5 11 gb 8/ Nx wf 9g r1 uI L3 Cv
d1 qO jC n+ eE Q9 mO eo As BT +O 76 nJ h7 5X wu
2r F8 hC gM W1 A9 bt SG MV 18 vz 1L Cu 47 WW 1T
Qx gv J1 Ed ZS 9z 9P 9g UJ VW q3 UA +U FR 3c gE
tH td 0Q Cd IR st Xp yR W+ 2m Jy v9 q1 g6 nt s6
wK n4 N9 0Y dm sw dU CL Ep AK oP j1 Mp c9 CT ef
Of Co 8Y 1X I0 5Z 8C zp 1Z Td M4 OS bf fm IS e4
zZ bZ +v qs U1 aF 7O sx +q ZR 9U dZ 7Q C2 mW 1t
vu K0 /1 QW Ph k5 Zd Wc Dx XD qr OL HH vg nQ LD
xj a+ 78 9w bc Xq Xw qy qB f1 od Xe Kf s4 xX VX
sb jm Rv vq Jn 6z Tw zZ 93 mA L1 +C fC 5y 2J Gj
dq Rk 5w bV FI hA VB KG 2Q Ud kq AV KB 1F Zs C7
I2 Wc e2 uq dd Tp 4E s8 K2 Kt VX 4D rE Am Vt LJ
Pc 6p jb H3 oQ AN 7v 5r Vt 6L L9 VI xH qL hy +I
Lh WE b+ VB 1K 4T oi jo 5i Jn Eo 4F CD Je iy tH
T1 Q7 2q 77 y1 kG 1v hr AE SP TO mF V2 JN Xh hO
9+ As UE Ug 3X /Y fp uZ tR cn VE Fn /v PC IN gL
ow Jx ds Am bG dx 36 EU 5p Ug Pf 1N GH In pr CV
VR SG VK Jf 91 Lb YN LF gy g1 do o5 Fm hu U9 08
8M tN b+ z2 x3 U=

[ERROR] C:\BOOTNXT MoveFileEx error 5
```

https://www.youtube.com/watch?v=qkSKOSffTH4

感染擴散途徑與威脅推測

- 部分醫院主機被駭客當成跳板，進而經由VPN網路進行攻擊。
- 最初被感染的主機，可能是因社交網路email中毒 (仍待查證)。
- 事件發生時間有可能是8/29
- 大量事件同時發生的時間8/30
- 2018年12月，大陸資安公司有發佈GlobeImposter4.0報告
  - GlobeImposter4.0最新变种，2018年最后一发！！！
- 2019年感染的GlobeImposter有可能是4.0的變種



GlobeImposter4.0最新变种，2018年最后一发！！！

深信服安全团队 深信服千里目安全实验室 1/9

一、样本簡介

GlobeImposter家族首次出现在2017年5月份，2018年2月全国各大医院受GlobeImposter2.0勒索病毒攻击，导致医院系统被加密，严重影响了医院的正常业务，此勒索病毒在今年8月份变种出GlobeImposter3.0版本，导致全国多家法院等政企事业单位被勒索加密。此次，在2018年12月份，深信服安全团队又第一时间跟踪发现一例新的GlobeImposter勒索病毒变种，加密后缀".fuck"。

Conclusion

- Future challenge lies on source verification, event timeline summarizing, label normalization and response mechanism.
- Honeypot sources plays an important part because of its location uniqueness.
- Monitoring global cyberthreat event is crucial to prevent future attack activities.
- Information Sharing and Analysis Center (ISAC) can leverage social media, honeypot, dark web, and other hacking-related websites to mapping potential threat and leaked data.
- Good cyber threat defense alliance relies on: first-hand information broadcasting+ selected cyberthreat news articles+ actionable threat intelligence + vulnerability adversary + beware of other CII threat events + consider human risk factors

Thank you for your listening

- Feel free to contact me:
  - Shin-Ying Huang (Michelle)
  - shinyinghuang@iii.org.tw
- SecBuzzer website:
  - https://secbuzzer.co/