Day in Life of a Threat Intelligence Researcher

What the heck is threat intel anyways?

Still

TEAMT5

Persistent Cyber Threat Hunters

whoami

Still Hsu / Azaka Sekai 安坂星海

- Threat Intelligence Researcher @ TeamT5

Topic of interest

- .NET
- Windows
- Gaming & malware reverse engineering

Non-binary (they/them)

Story Time!

how did i get here tho

IT ALL BEGAN...

Here at the CTF club back in 2018!

ok not really

文組做資安？

心路歷程

國小

對電腦有興趣

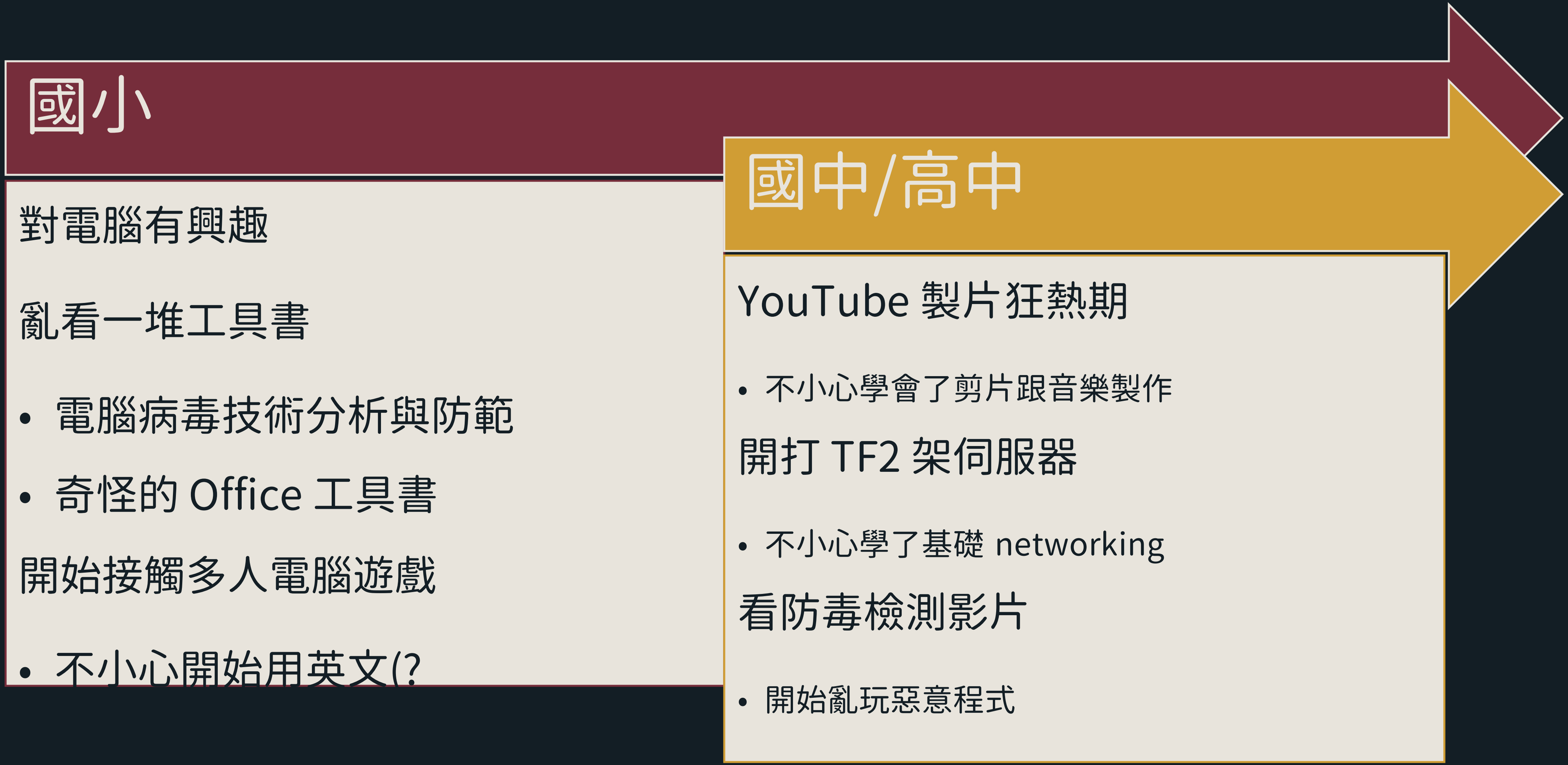
亂看一堆工具書

- 電腦病毒技術分析與防範
- 奇怪的 Office 工具書

開始接觸多人電腦遊戲

- 不小心開始用英文(?

心路歷程



國小

對電腦有興趣

亂看一堆工具書

- 電腦病毒技術分析與防範
- 奇怪的 Office 工具書

開始接觸多人電腦遊戲

- 不小心開始用英文(?

國中/高中

YouTube 製片狂熱期

- 不小心學會了剪片跟音樂製作

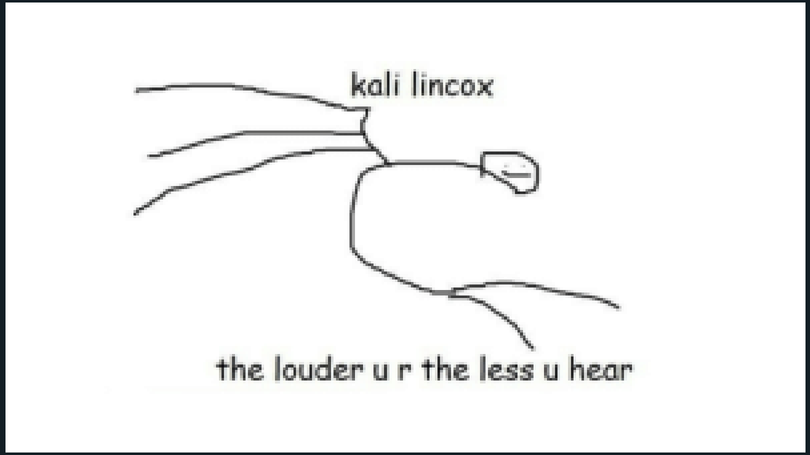
開打 TF2 架伺服器

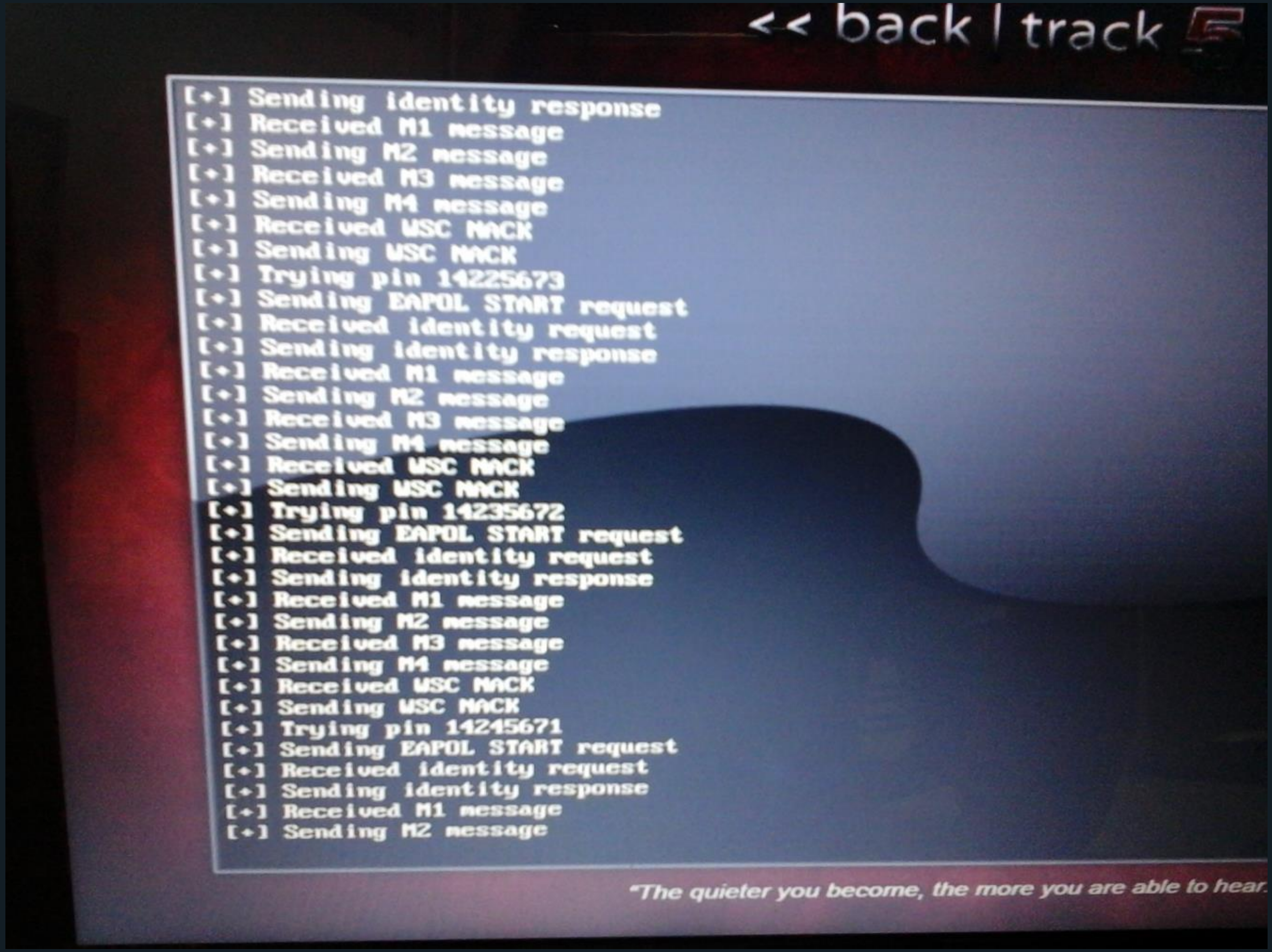
- 不小心學了基礎 networking

看防毒檢測影片

- 開始亂玩惡意程式

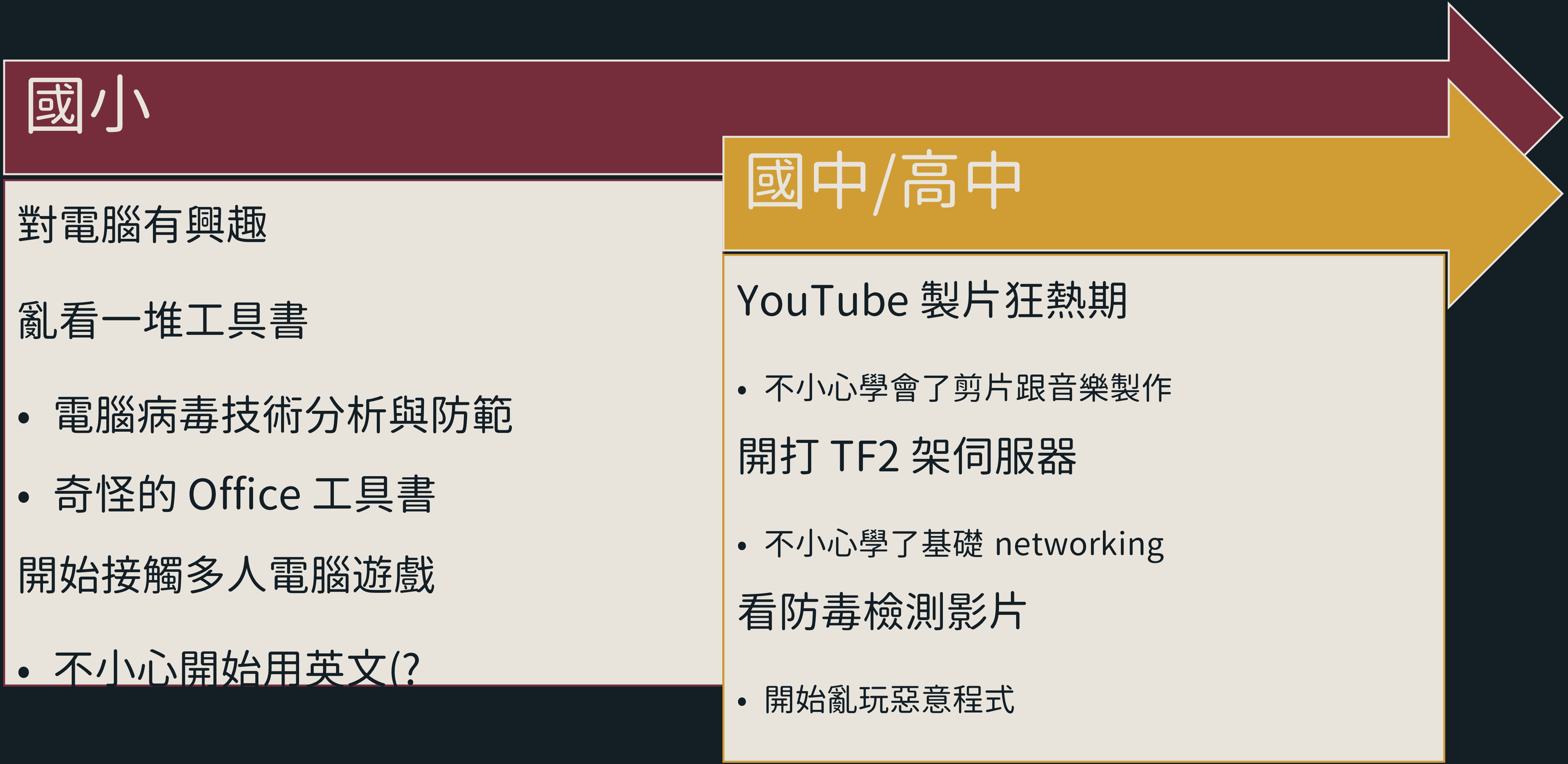
屁孩時期





```
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] Trying pin 14225673
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] Trying pin 14235672
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] Trying pin 14245671
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
```

心路歷程



國小

對電腦有興趣

亂看一堆工具書

- 電腦病毒技術分析與防範
- 奇怪的 Office 工具書

開始接觸多人電腦遊戲

- 不小心開始用英文(?

國中/高中

YouTube 製片狂熱期

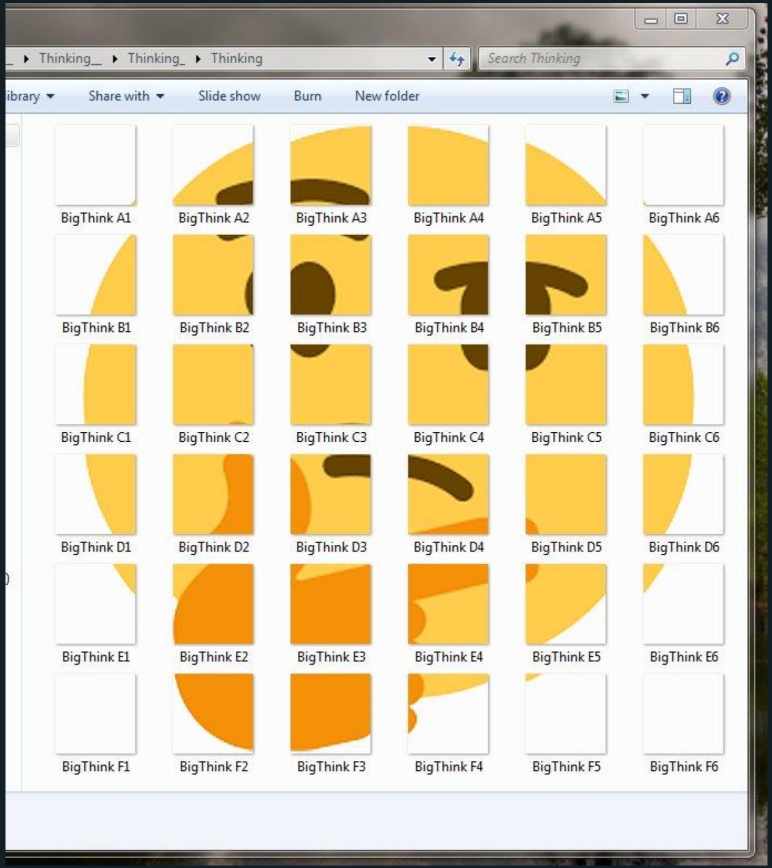
- 不小心學會了剪片跟音樂製作

開打 TF2 架伺服器

- 不小心學了基礎 networking

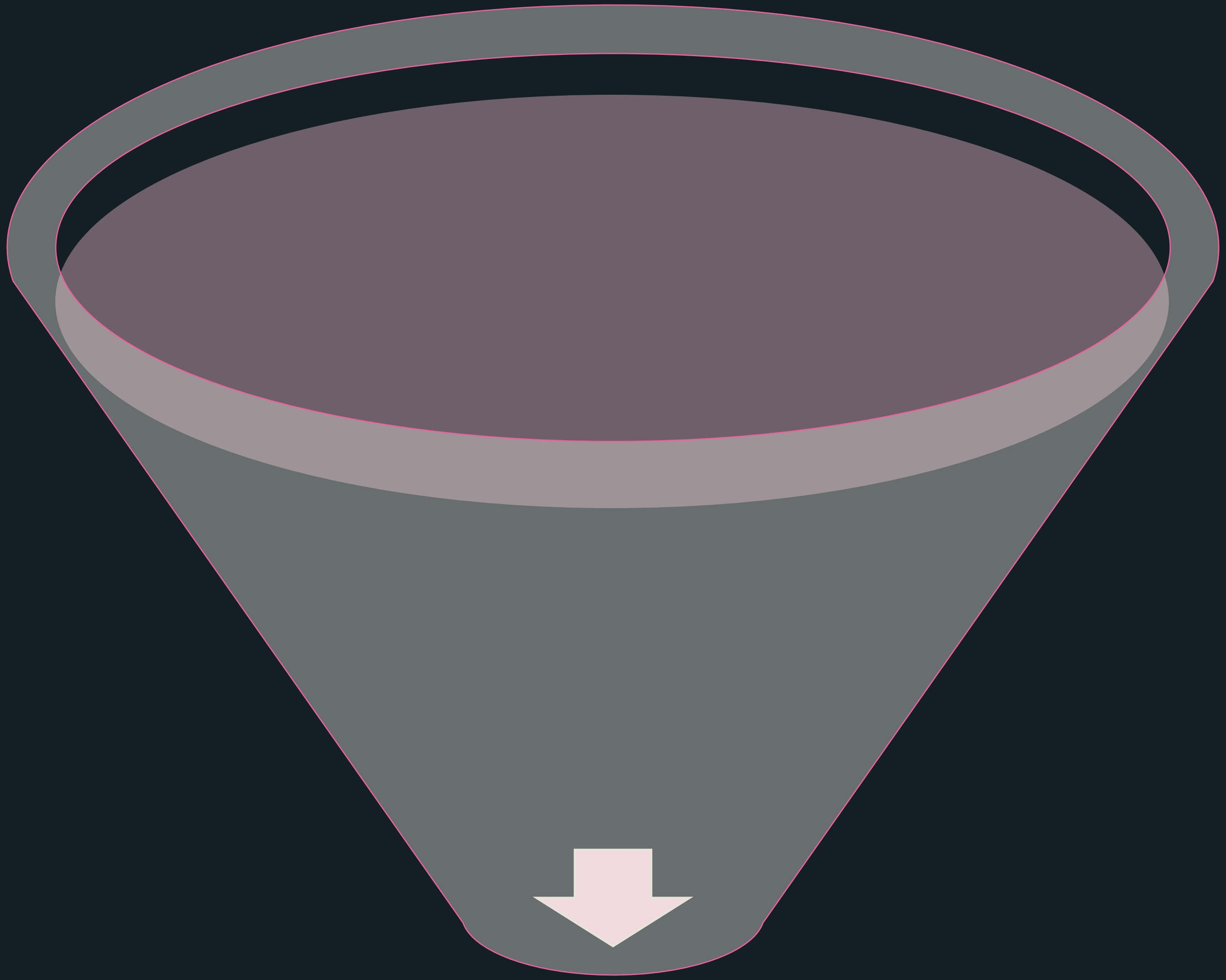
看防毒檢測影片

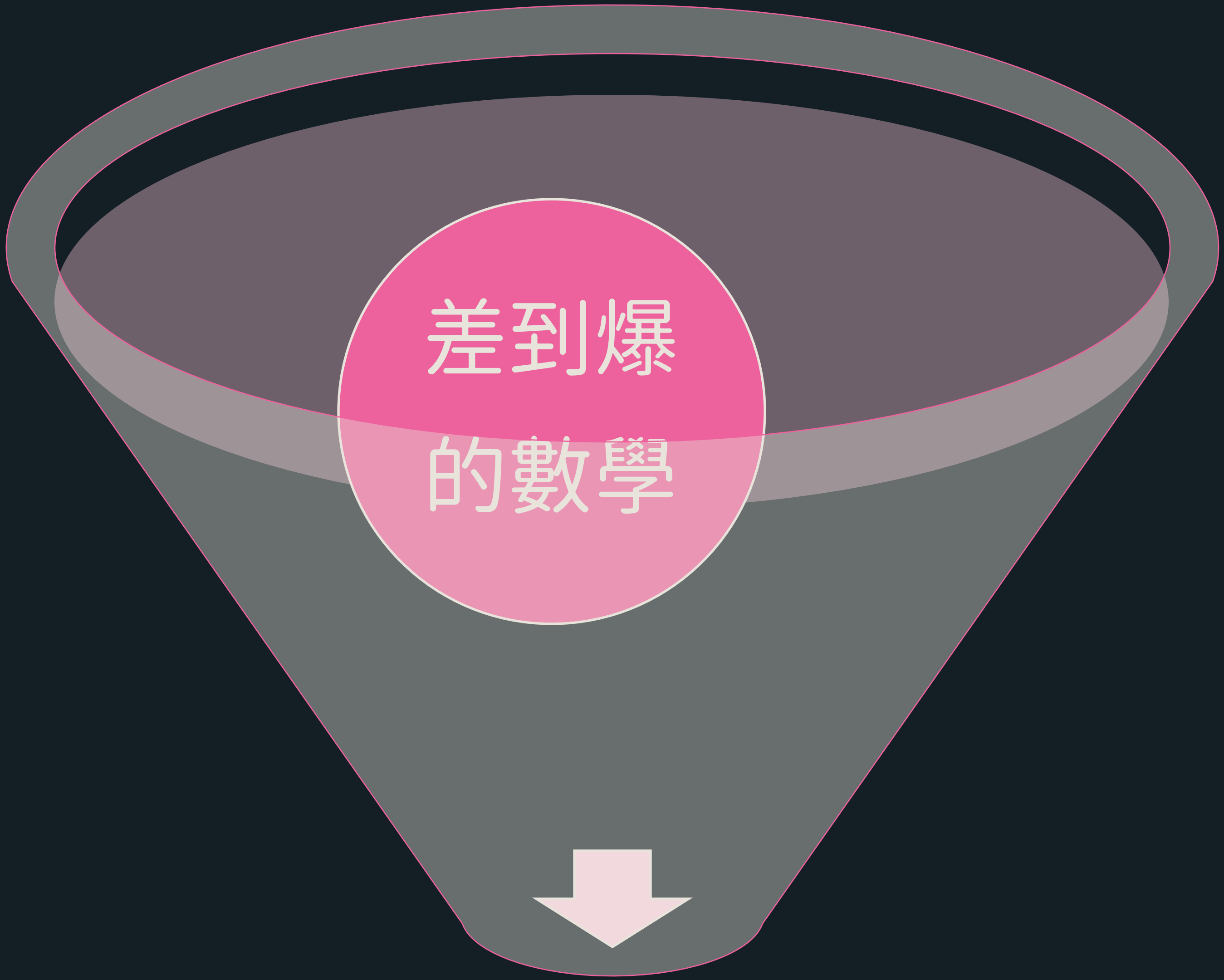
- 開始亂玩惡意程式



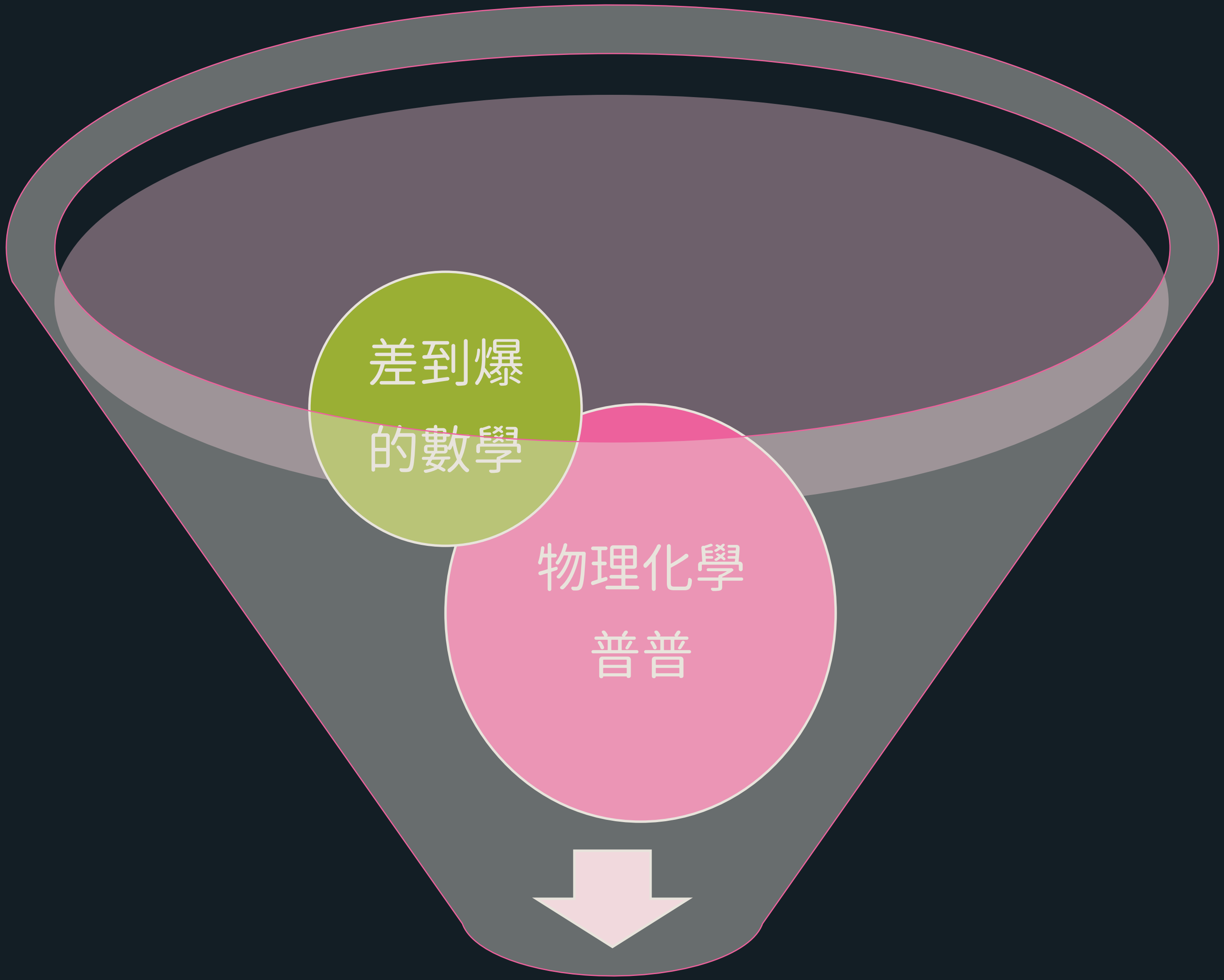
Thinking_ ▸ Thinking_ ▸ Thinking
Search Thinking
ibrary ▾
Share with ▾
Slide show
Burn
New folder
BigThink A1
BigThink A2
BigThink A3
BigThink A4
BigThink A5
BigThink A6
BigThink B1
BigThink B2
BigThink B3
BigThink B4
BigThink B5
BigThink B6
BigThink C1
BigThink C2
BigThink C3
BigThink C4
BigThink C5
BigThink C6
BigThink D1
BigThink D2
BigThink D3
BigThink D4
BigThink D5
BigThink D6
BigThink E1
BigThink E2
BigThink E3
BigThink E4
BigThink E5
BigThink E6
BigThink F1
BigThink F2
BigThink F3
BigThink F4
BigThink F5
BigThink F6

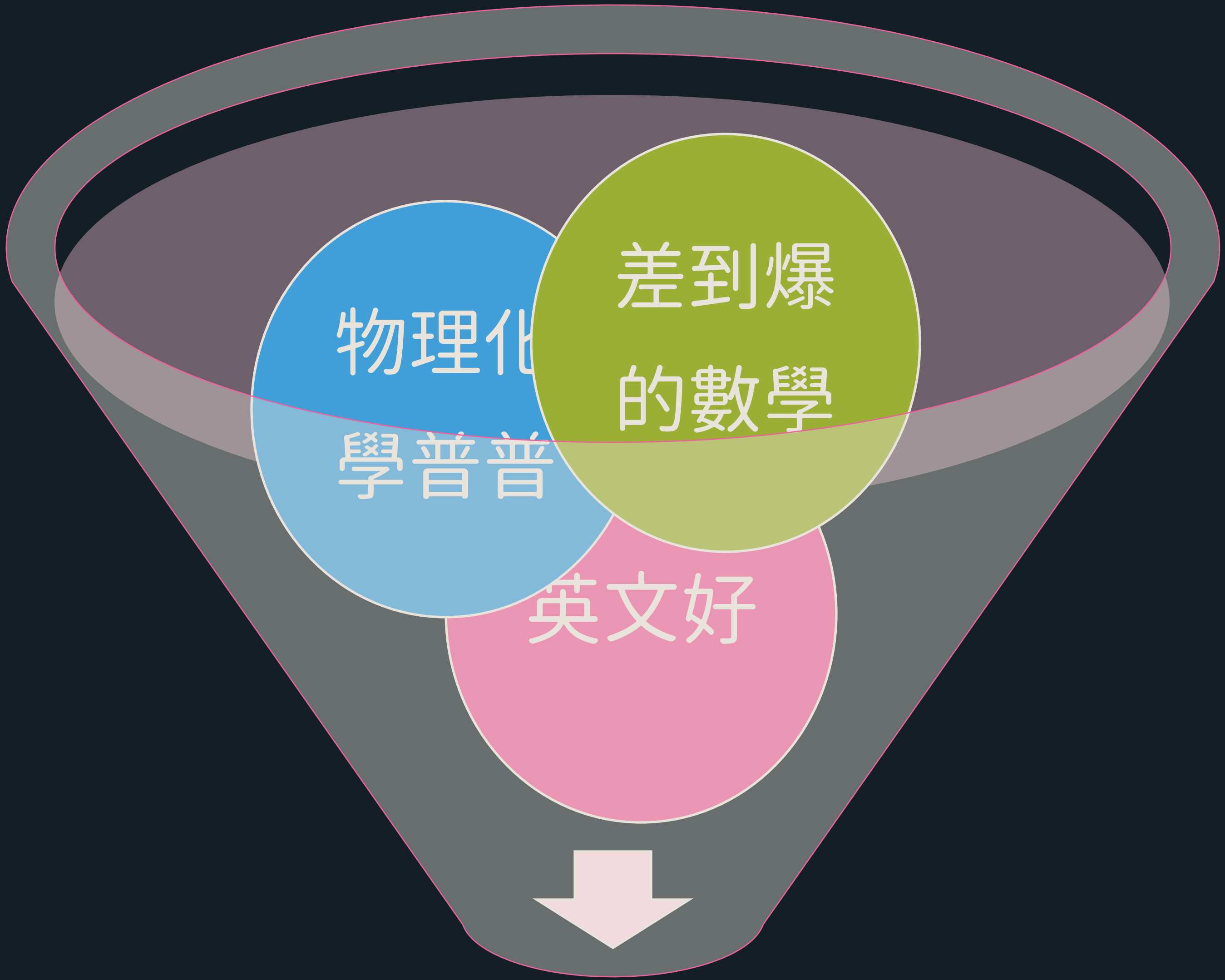
大學要念啥？





差到爆
的數學

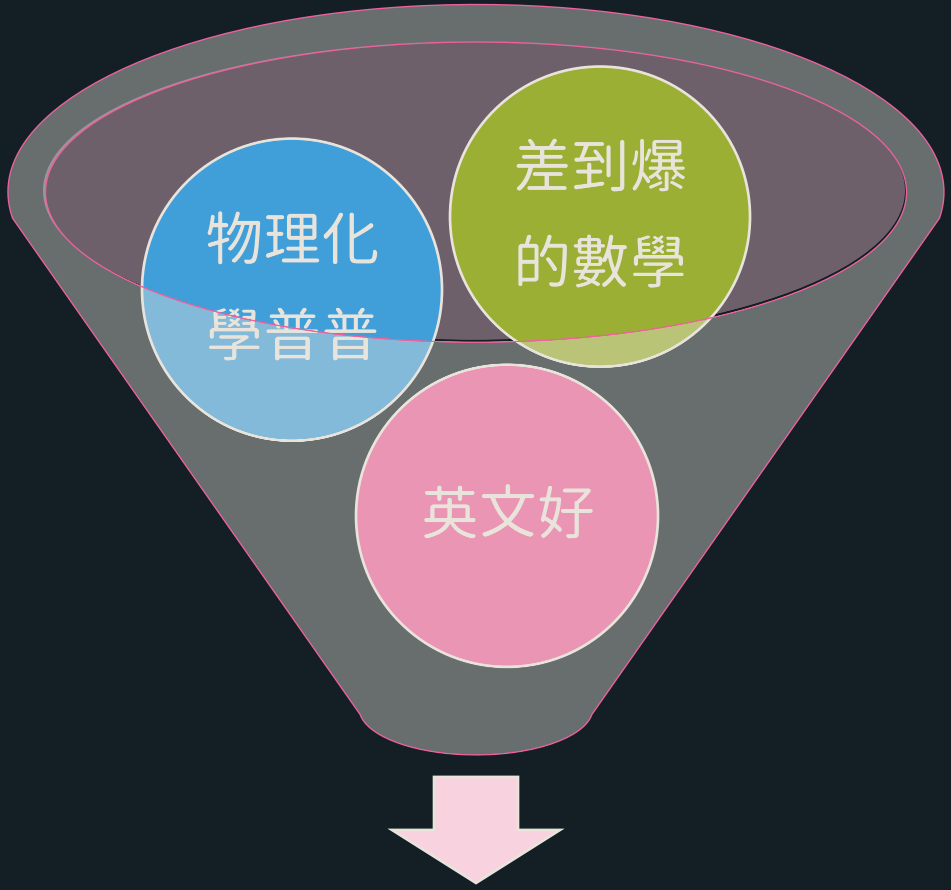

差到爆
的數學
物理化學
普普



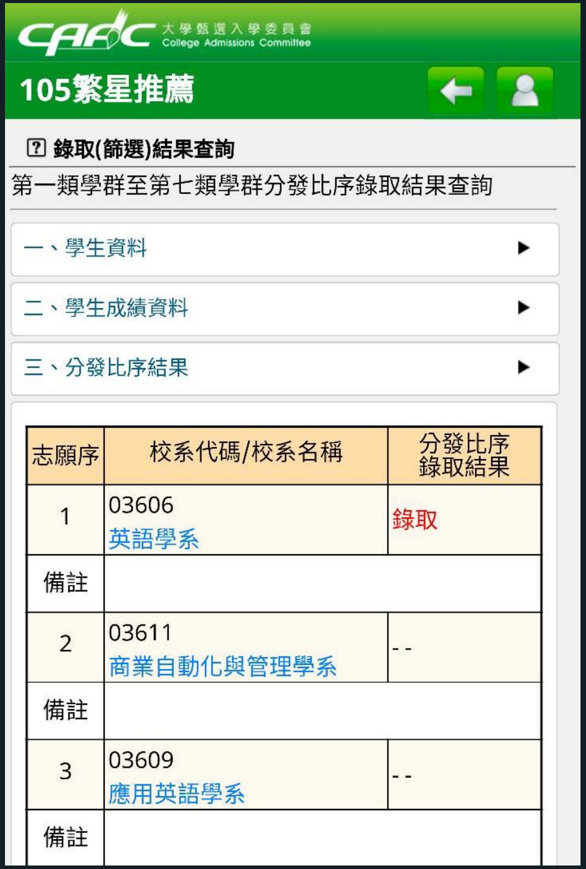
物理化學普普

差到爆的數學

英文好



好ㄅ看來只有英文系了



105繁星推薦

? 錄取(篩選)結果查詢

第一類學群至第七類學群分發比序錄取結果查詢

一、學生資料 ▶

二、學生成績資料 ▶

三、分發比序結果 ▶

志願序	校系代碼/校系名稱	分發比序 錄取結果
1	03606 英語學系	錄取
備註		
2	03611 商業自動化與管理學系	- -
備註		
3	03609 應用英語學系	- -
備註		

然後就這樣惹

心路歷程

TEAMT5

國小 (~2010)

對電腦有興趣

亂看一堆工具書

- 電腦病毒技術分析與防範
- 奇怪的 Office 工具書

開始接觸多人電腦遊戲

- 不小心開始用英文(?

國中/高中 (2010~2016)

開打 TF2 架伺服器

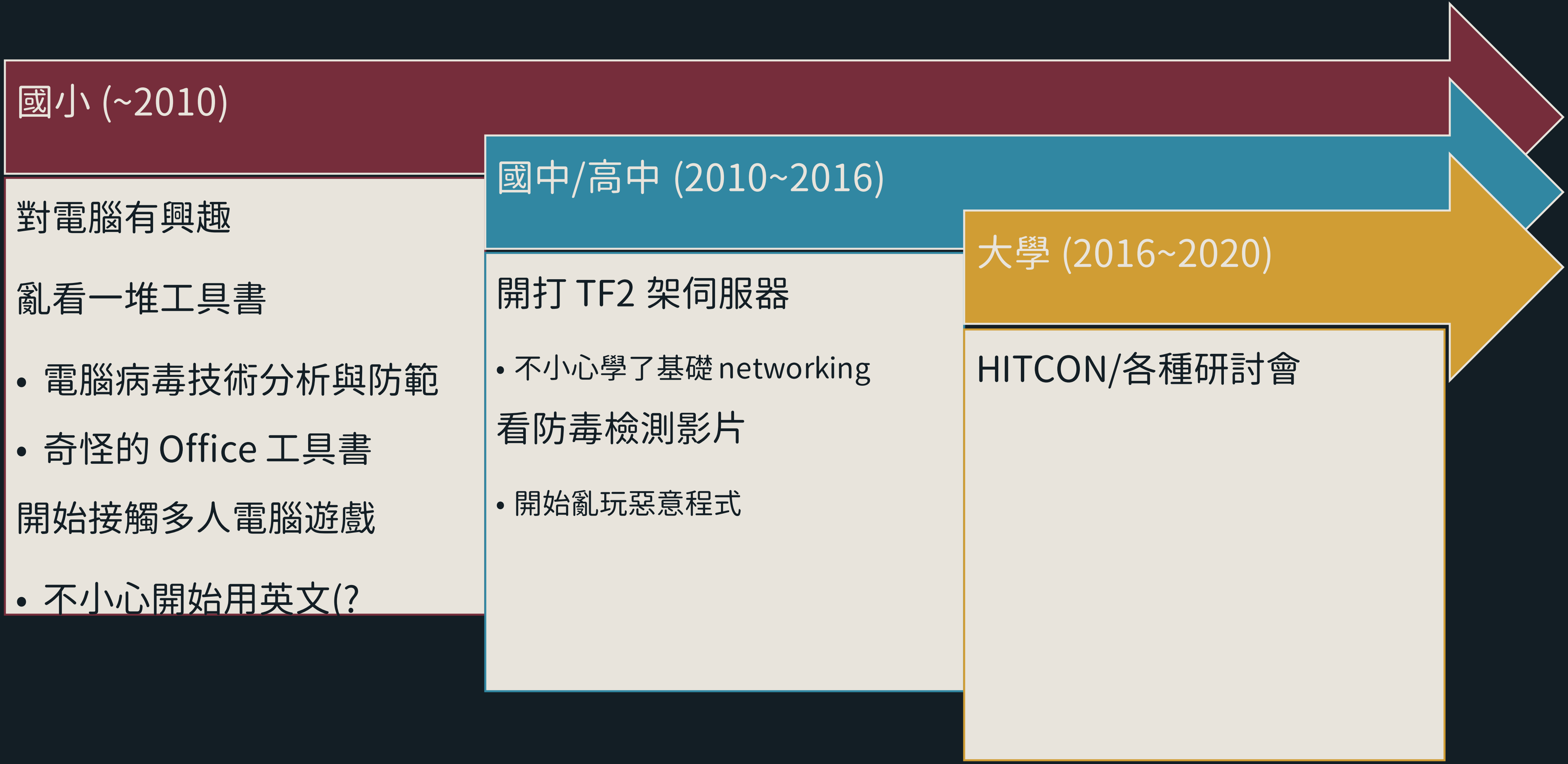
- 不小心學了基礎 networking

看防毒檢測影片

- 開始亂玩惡意程式

心路歷程

TEAMT5



國小 (~2010)

對電腦有興趣

亂看一堆工具書

- 電腦病毒技術分析與防範
- 奇怪的 Office 工具書

開始接觸多人電腦遊戲

- 不小心開始用英文(?

國中/高中 (2010~2016)

開打 TF2 架伺服器

- 不小心學了基礎 networking

看防毒檢測影片

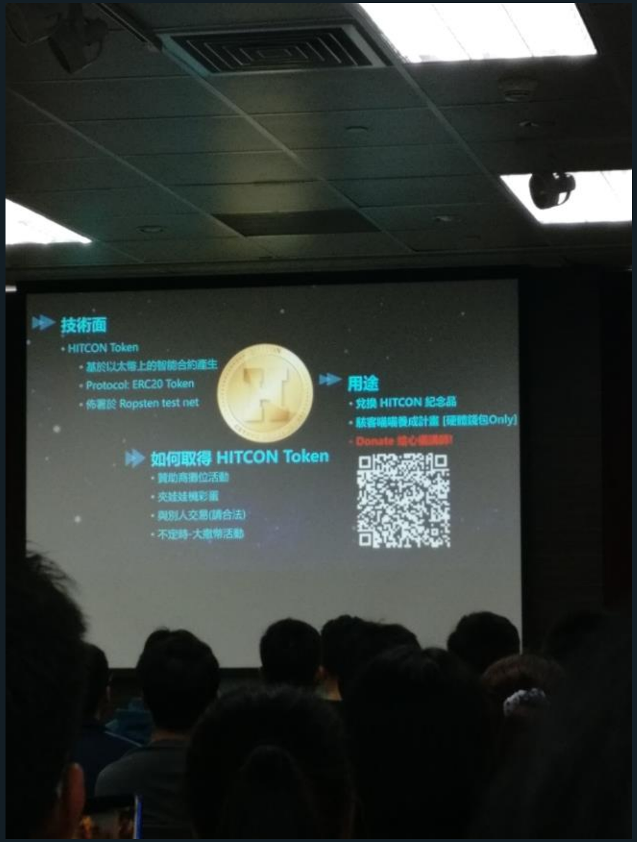
- 開始亂玩惡意程式

大學 (2016~2020)

HITCON/各種研討會

HITCON

HITCON 2018



技術面

- HITCON Token
  - 基於以太幣上的智能合約產生
  - Protocol: ERC20 Token
  - 佈署於 Ropsten test net

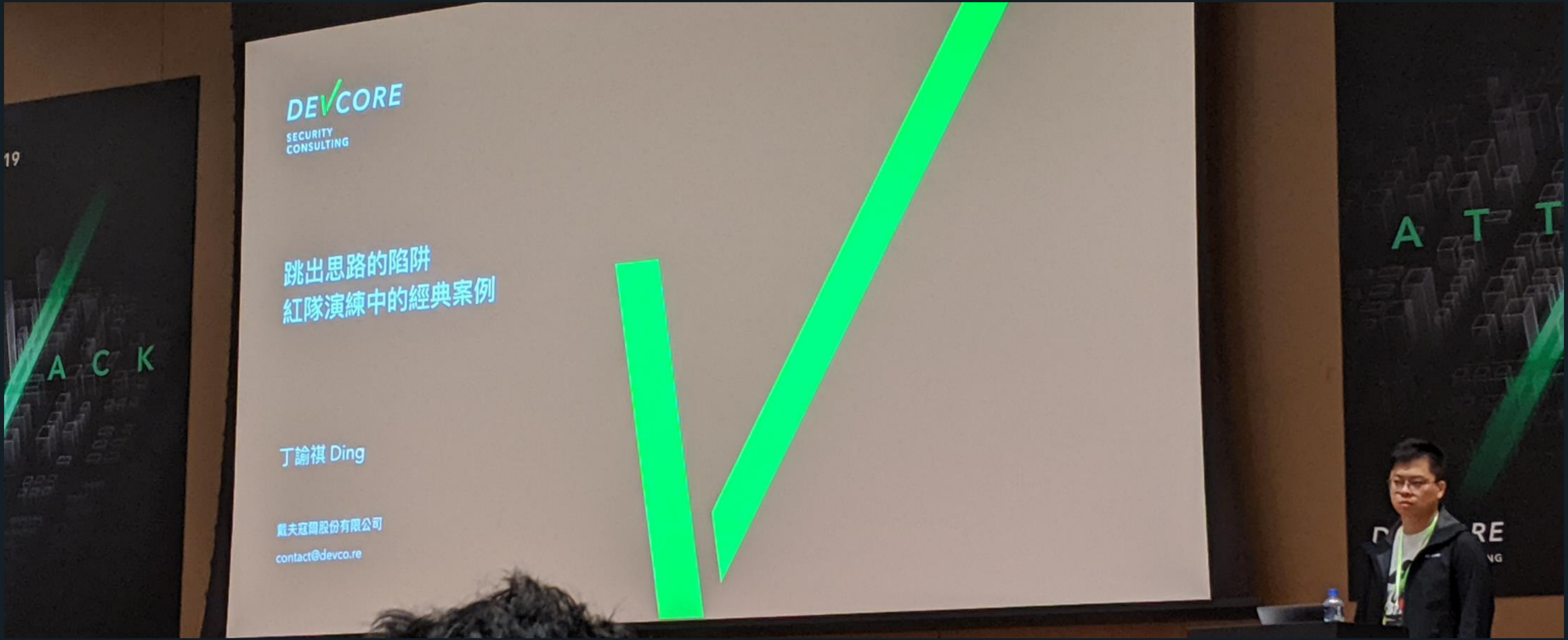
用途

- 兌換 HITCON 紀念品
- 駭客喵喵養成計畫 (硬體錢包Only)
- Donate 愛心捐獻!

如何取得 HITCON Token

- 贊助商攤位活動
- 夾娃娃機彩蛋
- 與別人交易(請合法)
- 不定時-大撒幣活動

HITCON 2019



DEVCORE

SECURITY
CONSULTING

跳出思路的陷阱
紅隊演練中的經典案例

丁諭祺 Ding

戴夫寇爾股份有限公司
contact@devco.re

DEVCORE Conf 2019

心路歷程

國小 (~2010)

對電腦有興趣

亂看一堆工具書

- 電腦病毒技術分析與防範
- 奇怪的 Office 工具書

開始接觸多人電腦遊戲

- 不小心開始用英文(?

國中/高中 (2010~2016)

開打 TF2 架伺服器

不小心學了基礎 networking

- 看防毒檢測影片
  - 開始亂玩惡意程式

大學 (2016~2020)

HITCON/各種研討會

心路歷程

TEAMT5

國小 (~2010)

對電腦有興趣

亂看一堆工具書

- 電腦病毒技術分析與防範
- 奇怪的 Office 工具書

開始接觸多人電腦遊戲

- 不小心開始用英文(?

國中/高中 (2010~2016)

開打 TF2 架伺服器

不小心學了基礎 networking

- 看防毒檢測影片
  - 開始亂玩惡意程式

大學 (2016~2020)

HITCON/各種研討會

CTF???

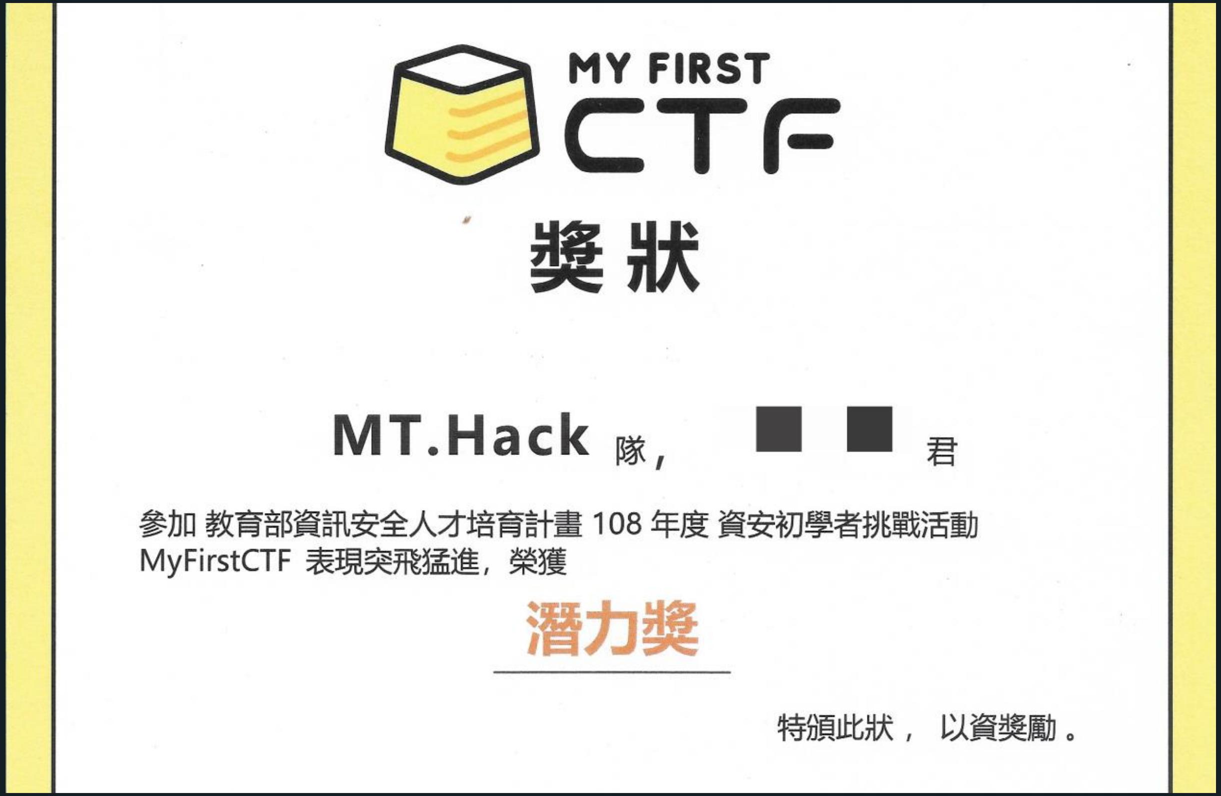
系上大量電腦管理工作

- 不小心學會了 AD 架構跟大量部署

因緣際會接觸了學校資安社

CTF/資安學界

MFCTF 2019



MY FIRST CTF

獎 狀

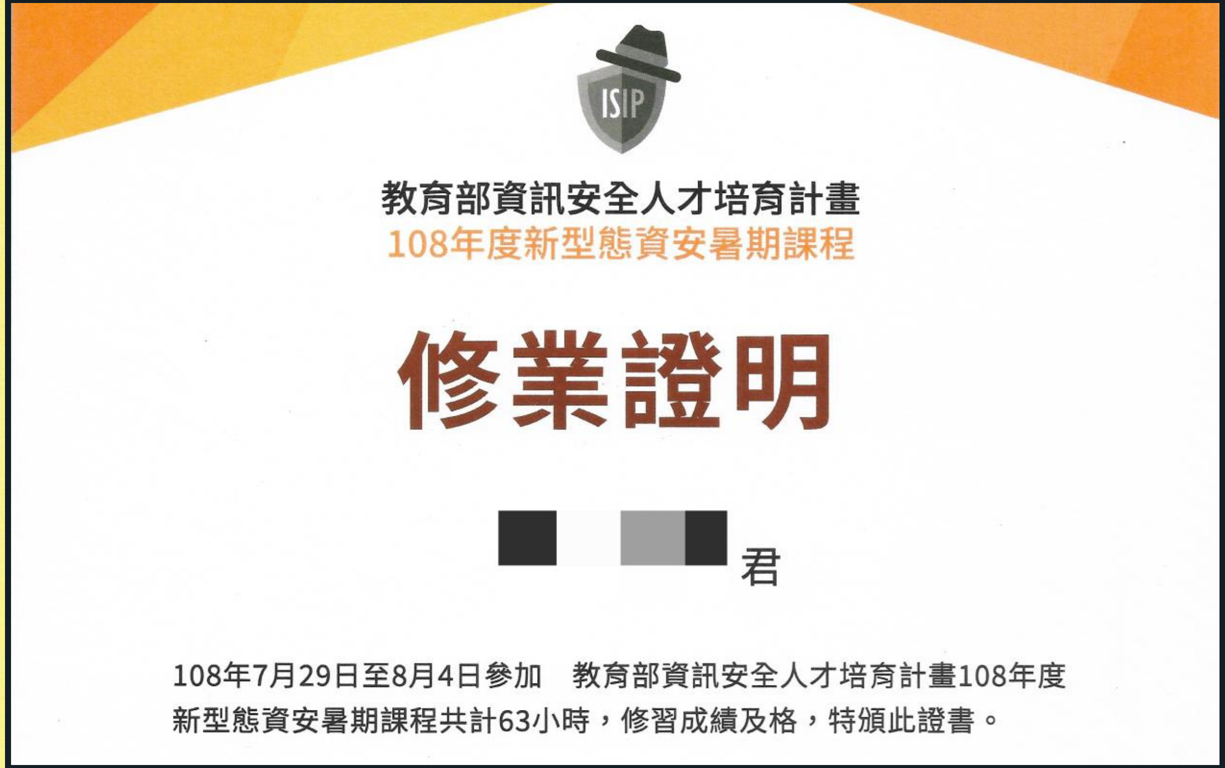
MT.Hack 隊，[redacted] [redacted] 君

參加 教育部資訊安全人才培育計畫 108 年度 資安初學者挑戰活動
MyFirstCTF 表現突飛猛進，榮獲

潛力獎

特頒此狀， 以資獎勵。

AIS3 2019



ISIP

教育部資訊安全人才培育計畫
108年度新型態資安暑期課程

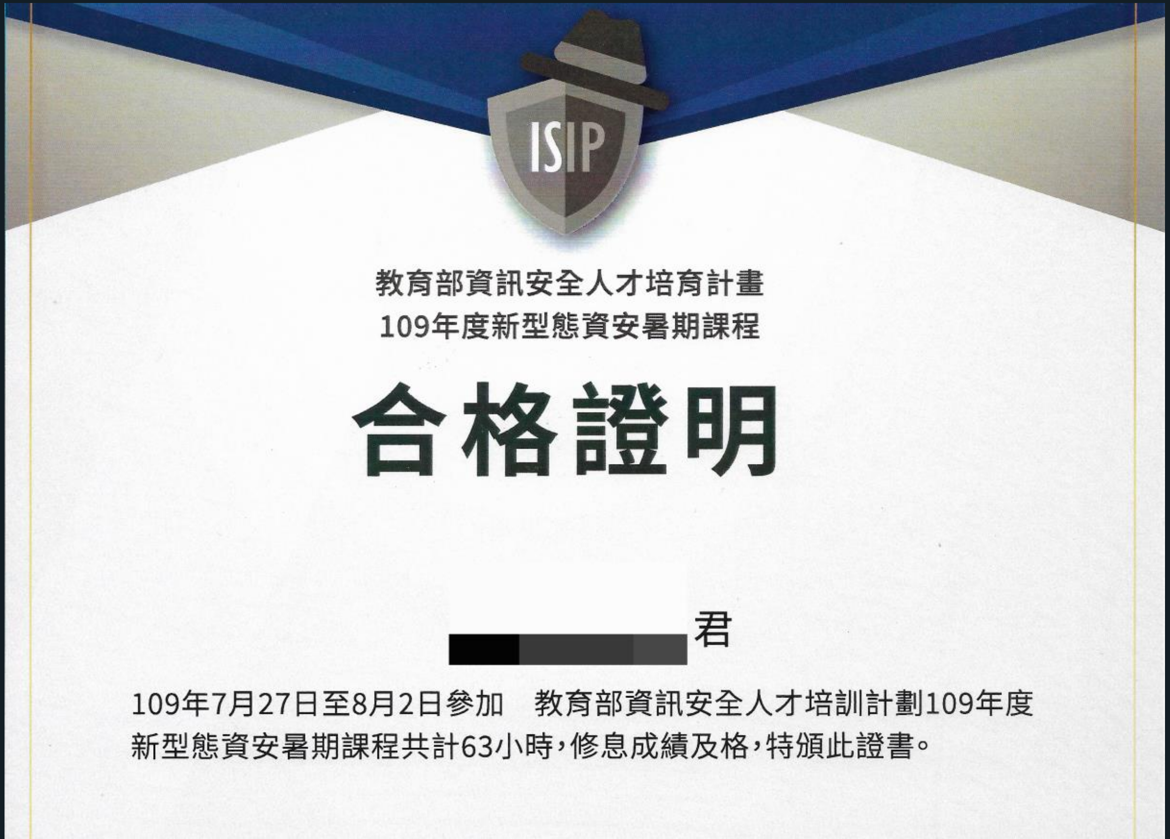
修業證明

[redacted] 君

108年7月29日至8月4日參加　教育部資訊安全人才培育計畫108年度
新型態資安暑期課程共計63小時，修習成績及格，特頒此證書。

CTF/資安學界

AIS3 2020



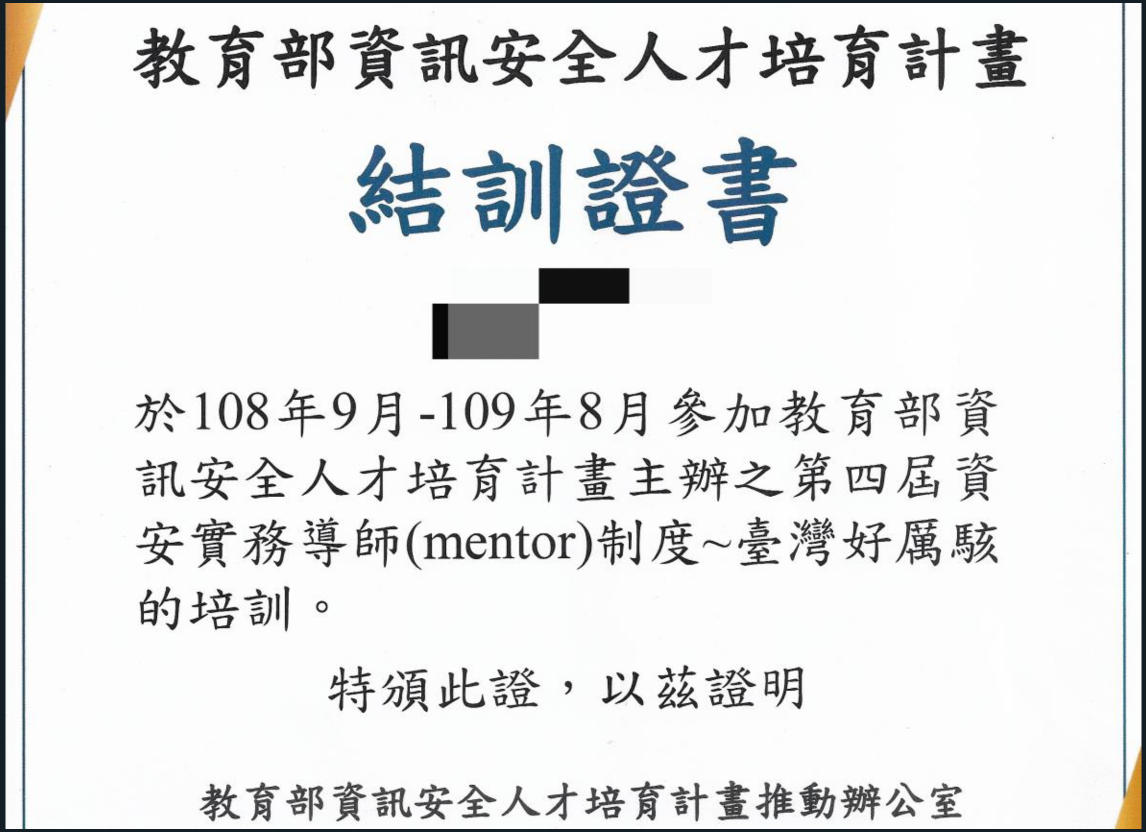
教育部資訊安全人才培育計畫
109年度新型態資安暑期課程

合格證明

[redacted]君

109年7月27日至8月2日參加　教育部資訊安全人才培訓計劃109年度新型態資安暑期課程共計63小時，修息成績及格，特頒此證書。

臺灣好厲駭 2020



教育部資訊安全人才培育計畫

結訓證書

[redacted]

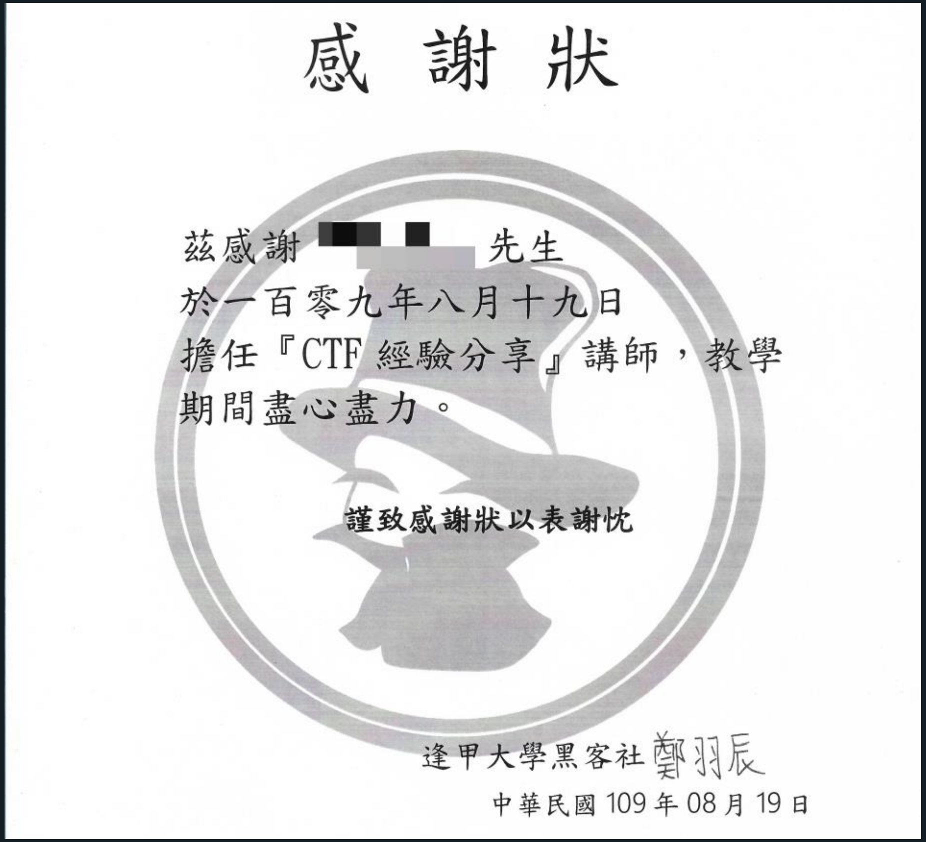
於108年9月-109年8月參加教育部資訊安全人才培育計畫主辦之第四屆資安實務導師(mentor)制度~臺灣好厲駭的培訓。

特頒此證，以茲證明

教育部資訊安全人才培育計畫推動辦公室

到處亂講(

逢甲黑客社2020



感 謝 狀

茲感謝 [redacted] 先生

於一百零九年八月十九日

擔任『CTF 經驗分享』講師，教學

期間盡心盡力。

謹致感謝狀以表謝忱

逢甲大學黑客社 鄭羽辰

中華民國 109 年 08 月 19 日

中山資安社

<沒有證明>

於是乎，大學畢業後找工作

然後就誤打誤撞進了T5

Back in HITCON 2018

Mighty Net
Hacks In Taiwan Conference
Best Partner For Hardware Innovation

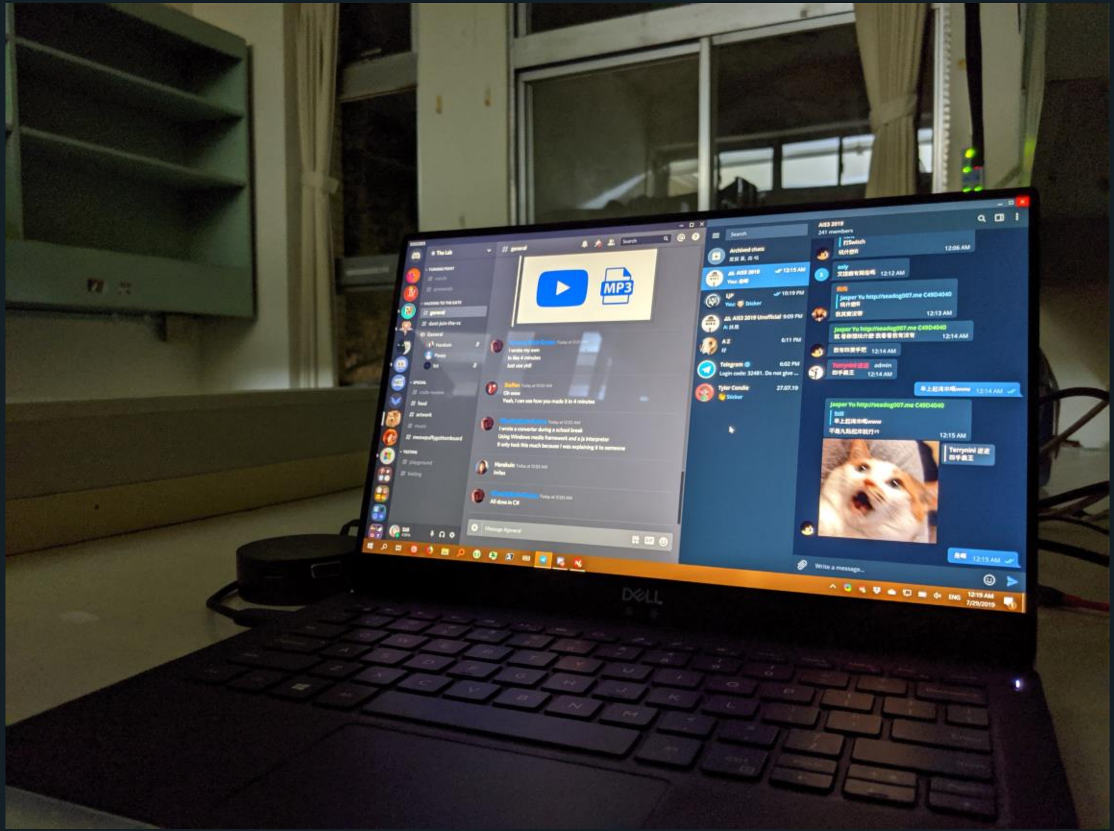
Agenda 7/27
R0
R1
R2
R4
09:00-09:40 總召致詞 & Opening
09:40-10:30 Keynote
10:30-10:40 Break
The rise of Middle East - Blue vs Red
HITCON 101 - Malicious Encrypted Traffic Detection
10:40-11:30
11:30-12:30 Launch
Alphathreat Soup: Burning Threat Actors with Data
12:30-13:20
13:20-13:30 Break
Taipei Ethereum Meetup
13:30-14:20
14:20-14:50 Coffee Break
Panel Discussion
14:50-15:40
15:40-15:50 Break
My story of unlocking the stolen iPhone
How to build your own wireless packet capture rig.
ZeroDay 發表會
16:40-17:00
Agenda 7/28
08:30-09:00 報到時間 Attendant Registration Time
09:00-09:10 Opening
Keynote : Car Infotainment Hacking Methodology and Attack Surface Scenarios
10:00-10:10 Launch
11:00-11:10 Break
12:00-13:00 Lunch
13:05-13:10 HITCON GIRLS
13:30-13:40 Break
14:30-15:00 Coffee Break
15:50-16:50 閉幕 Closing / 花絮與展望 HITCON 2019
16:50-17:20 散場 See You

Then I joined the CTF club

And a bunch of other things just kinda happened

HITCON 2019

AIS3 2019



And a bunch of other things just kinda happened

DEVCORE 2019

ZYXEL 2020

Quick Q&A

Threat Intelligence

Threat Intelligence

「知彼知己者，百戰不殆。」

《孫子．謀攻》

Definition

TEAMT5 杜浦數位安全

Shed light on the **adversaries**

- Understand **WHO** exactly you're dealing with

(CrowdStrike, 2021)

Definition

Shed light on the **adversaries**

- Understand **WHO** exactly you’re dealing with

Understand the motives and TTPs

- Why?
- How?
  - Tactics
  - Techniques
  - Procedures

(CrowdStrike, 2021)

Definition

Shed light on the **adversaries**

- Understand **WHO** exactly you’re dealing with

Understand the motives and TTPs

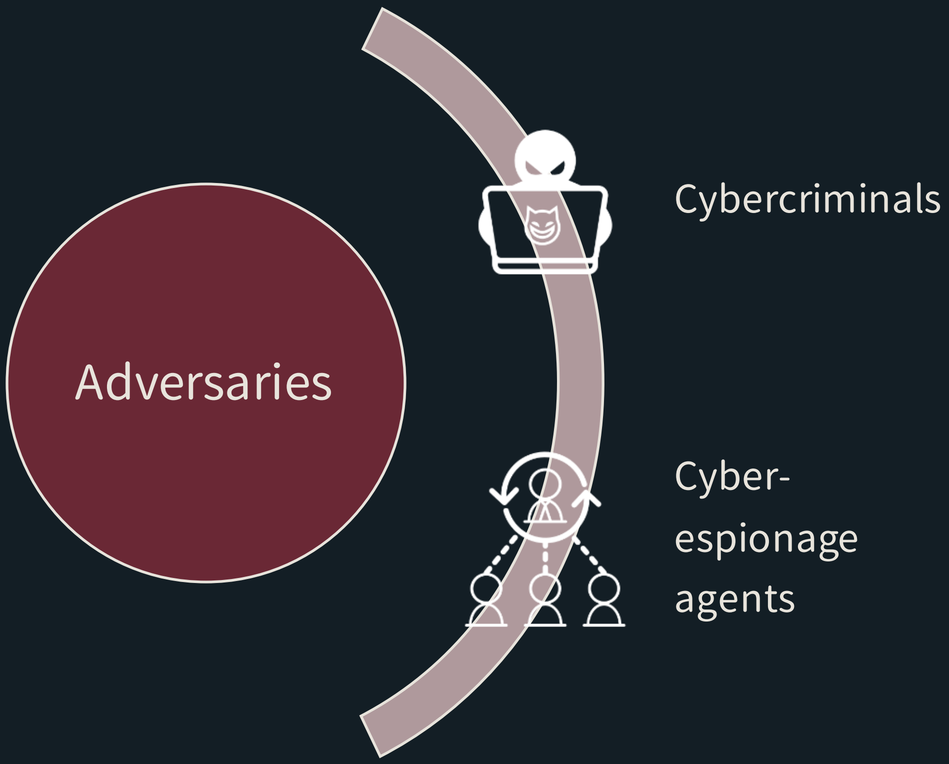
- Why?
- How?
  - Tactics
  - Techniques
  - Procedures

Help mitigate risks and boost efficiency

(CrowdStrike, 2021)

Cyber Attacks

Type of adversaries

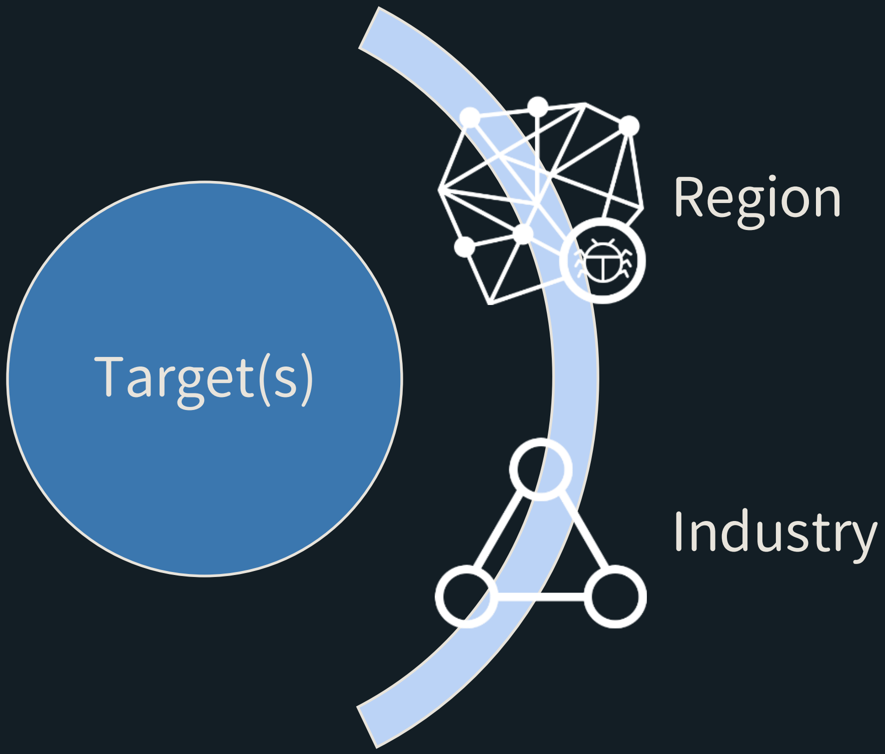


Adversaries

Cybercriminals

Cyber-espionage agents

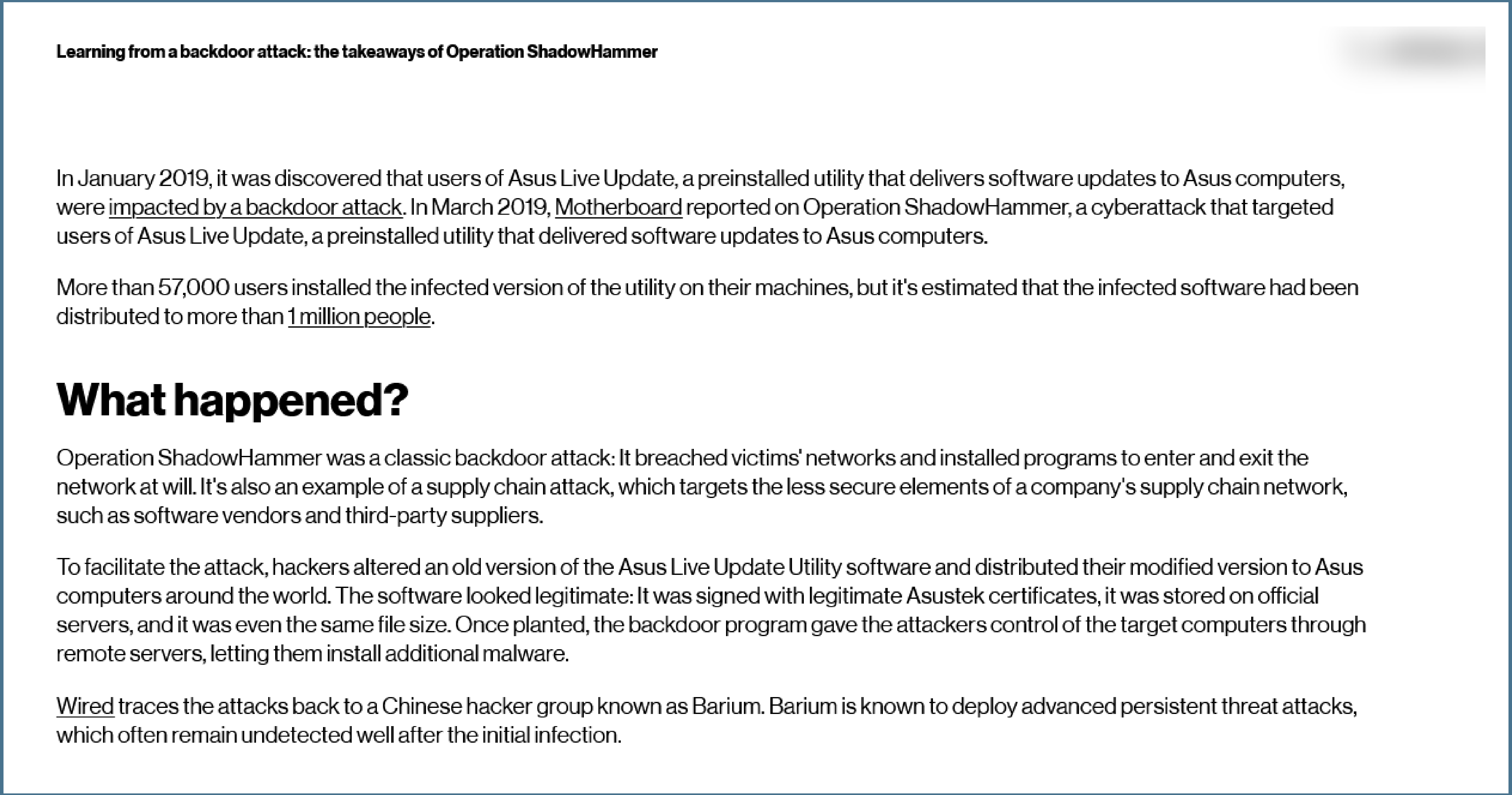
Information about the target(s)



Target(s)

Region

Industry



Learning from a backdoor attack: the takeaways of Operation ShadowHammer

In January 2019, it was discovered that users of Asus Live Update, a preinstalled utility that delivers software updates to Asus computers, were impacted by a backdoor attack. In March 2019, Motherboard reported on Operation ShadowHammer, a cyberattack that targeted users of Asus Live Update, a preinstalled utility that delivered software updates to Asus computers.

More than 57,000 users installed the infected version of the utility on their machines, but it's estimated that the infected software had been distributed to more than 1 million people.

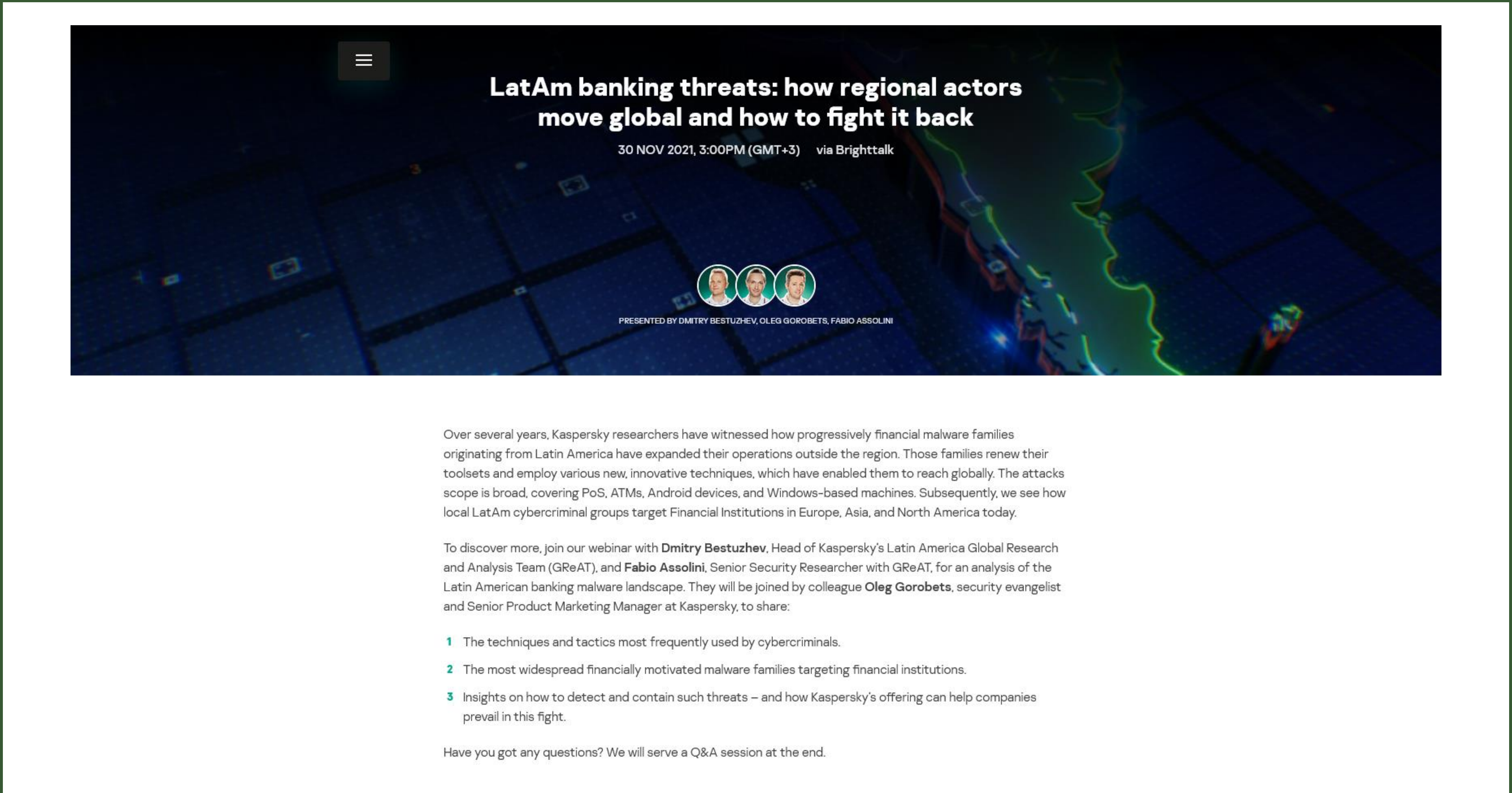
What happened?

Operation ShadowHammer was a classic backdoor attack: It breached victims' networks and installed programs to enter and exit the network at will. It's also an example of a supply chain attack, which targets the less secure elements of a company's supply chain network, such as software vendors and third-party suppliers.

To facilitate the attack, hackers altered an old version of the Asus Live Update Utility software and distributed their modified version to Asus computers around the world. The software looked legitimate: It was signed with legitimate Asustek certificates, it was stored on official servers, and it was even the same file size. Once planted, the backdoor program gave the attackers control of the target computers through remote servers, letting them install additional malware.

Wired traces the attacks back to a Chinese hacker group known as Barium. Barium is known to deploy advanced persistent threat attacks, which often remain undetected well after the initial infection.

(Stone, n.d.)



LatAm banking threats: how regional actors move global and how to fight it back

30 NOV 2021, 3:00PM (GMT+3) via Brighttalk

PRESENTED BY DMITRY BESTUZHEV, OLEG GOROBETS, FABIO ASSOLINI

Over several years, Kaspersky researchers have witnessed how progressively financial malware families originating from Latin America have expanded their operations outside the region. Those families renew their toolsets and employ various new, innovative techniques, which have enabled them to reach globally. The attacks scope is broad, covering PoS, ATMs, Android devices, and Windows-based machines. Subsequently, we see how local LatAm cybercriminal groups target Financial Institutions in Europe, Asia, and North America today.

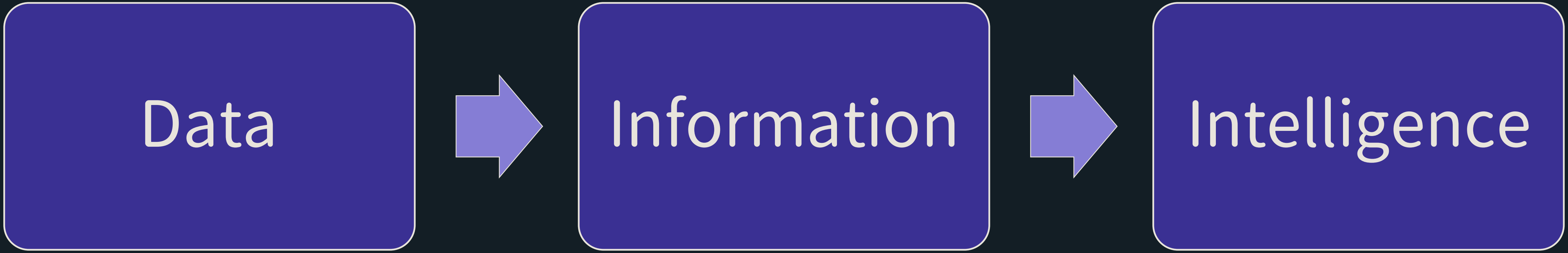
To discover more, join our webinar with **Dmitry Bestuzhev**, Head of Kaspersky's Latin America Global Research and Analysis Team (GReAT), and **Fabio Assolini**, Senior Security Researcher with GReAT, for an analysis of the Latin American banking malware landscape. They will be joined by colleague **Oleg Gorobets**, security evangelist and Senior Product Marketing Manager at Kaspersky, to share:

1. The techniques and tactics most frequently used by cybercriminals.
2. The most widespread financially motivated malware families targeting financial institutions.
3. Insights on how to detect and contain such threats – and how Kaspersky's offering can help companies prevail in this fight.

Have you got any questions? We will serve a Q&A session at the end.

(Bestuzhev et al., 2021)

Collection


Data

Information

Intelligence

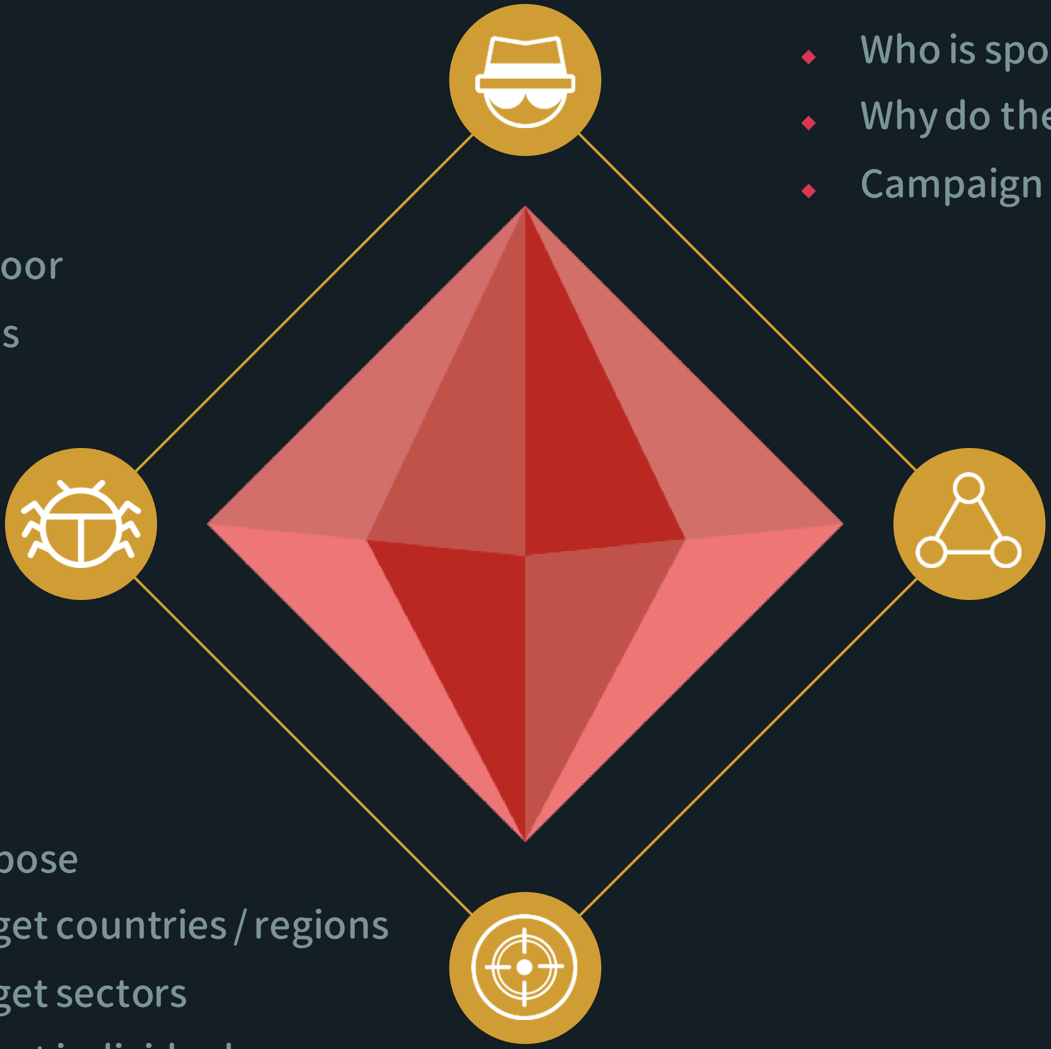
External Source

- Community
- Social Media
- Threat Data Feed
- Open-source Intelligence
- Deep Web
- Dark Web

Internal Source

- SIEM / Sensors
- Incident Response
- Network Visibility
- Endpoint Visibility
- Malware Analysis
- Research Lab

Diamond Model



CAPABILITY

- Reconnaissance techniques
- Delivery methods
- Attacking exploit / vulnerability
- Remote control malware / backdoor
- Lateral movement skills and tools
- Data stealing techniques

ADVERSARY

- Where are they from?
- Who are they?
- Who is sponsoring them?
- Why do they attack?
- Campaign timeline and plan

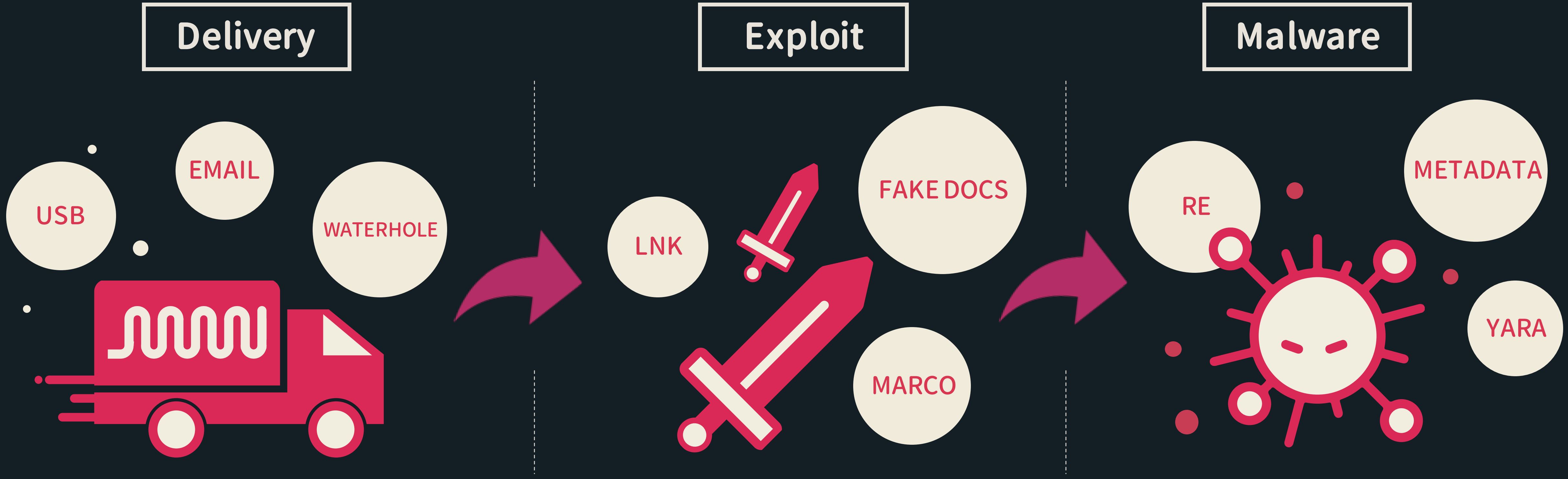
INFRASTRUCTURE

- C2 Domain names
- Location of C2 servers
- Type of C2 servers
- Compromised machines
- C2 management mechanism and structure
- Path of Control and data leakage

TARGET

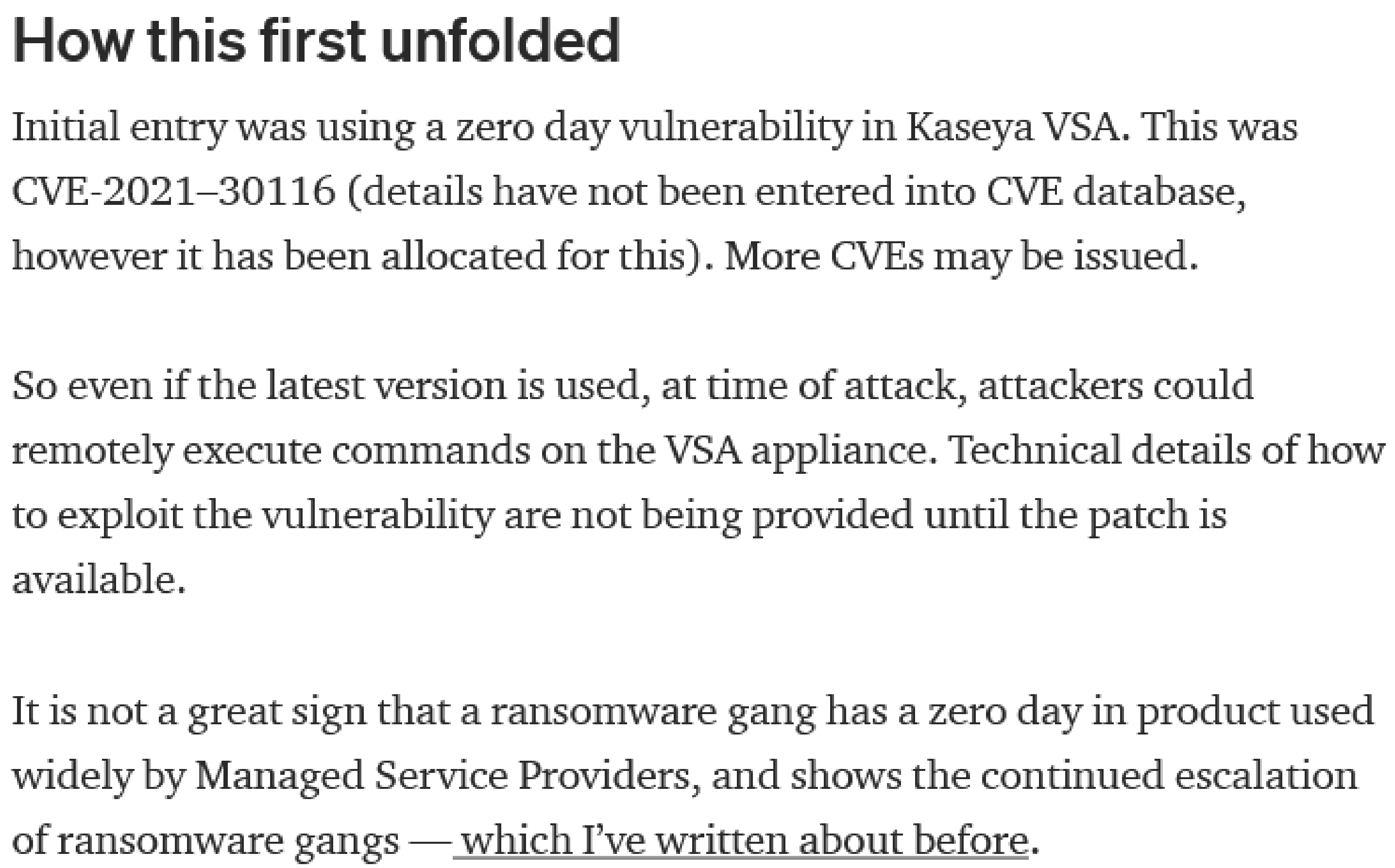
- Purpose
- Target countries / regions
- Target sectors
- Target individuals
- Target data

Capability Analysis


Delivery

Exploit

Malware



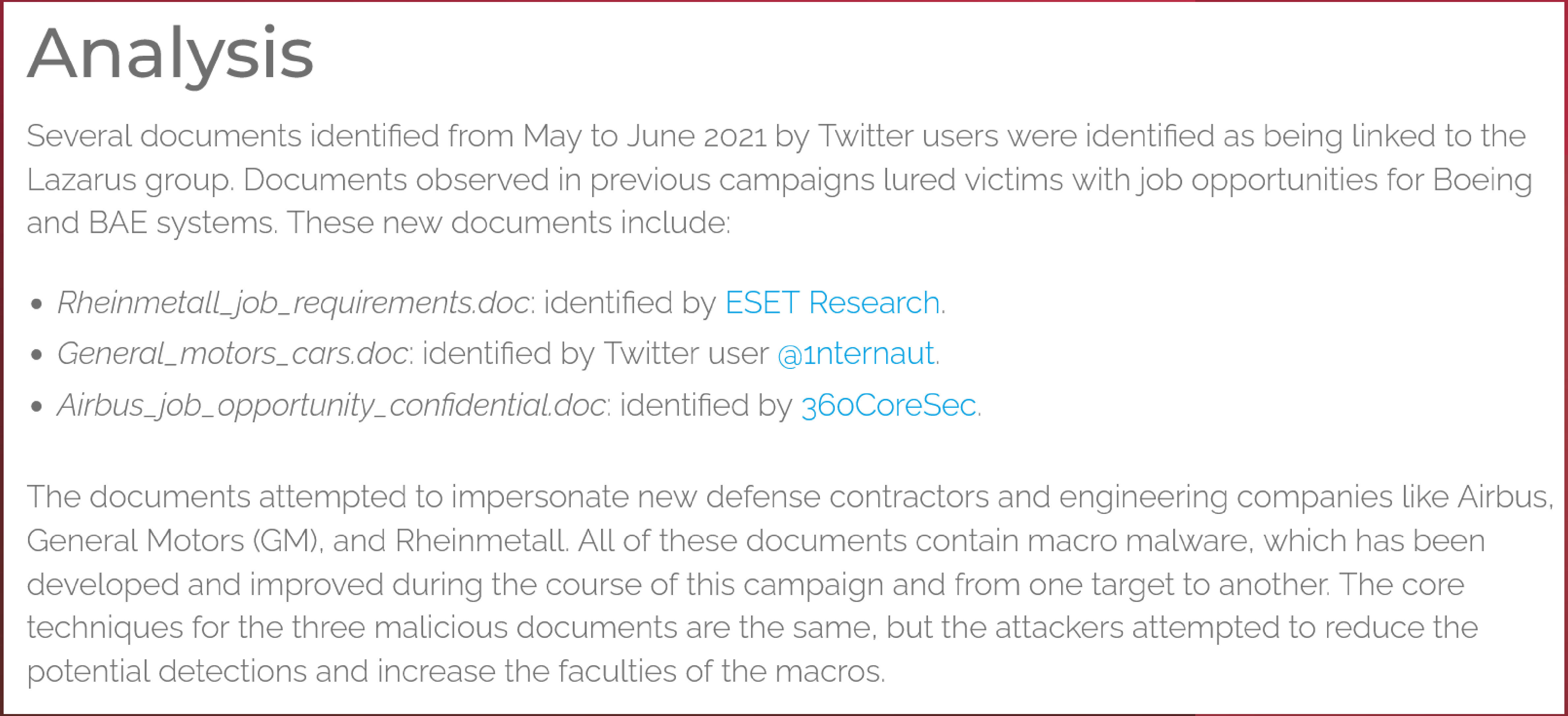
How this first unfolded

Initial entry was using a zero day vulnerability in Kaseya VSA. This was CVE-2021–30116 (details have not been entered into CVE database, however it has been allocated for this). More CVEs may be issued.

So even if the latest version is used, at time of attack, attackers could remotely execute commands on the VSA appliance. Technical details of how to exploit the vulnerability are not being provided until the patch is available.

It is not a great sign that a ransomware gang has a zero day in product used widely by Managed Service Providers, and shows the continued escalation of ransomware gangs — which I've written about before.

(Beaumont, 2021)



Analysis

Several documents identified from May to June 2021 by Twitter users were identified as being linked to the Lazarus group. Documents observed in previous campaigns lured victims with job opportunities for Boeing and BAE systems. These new documents include:

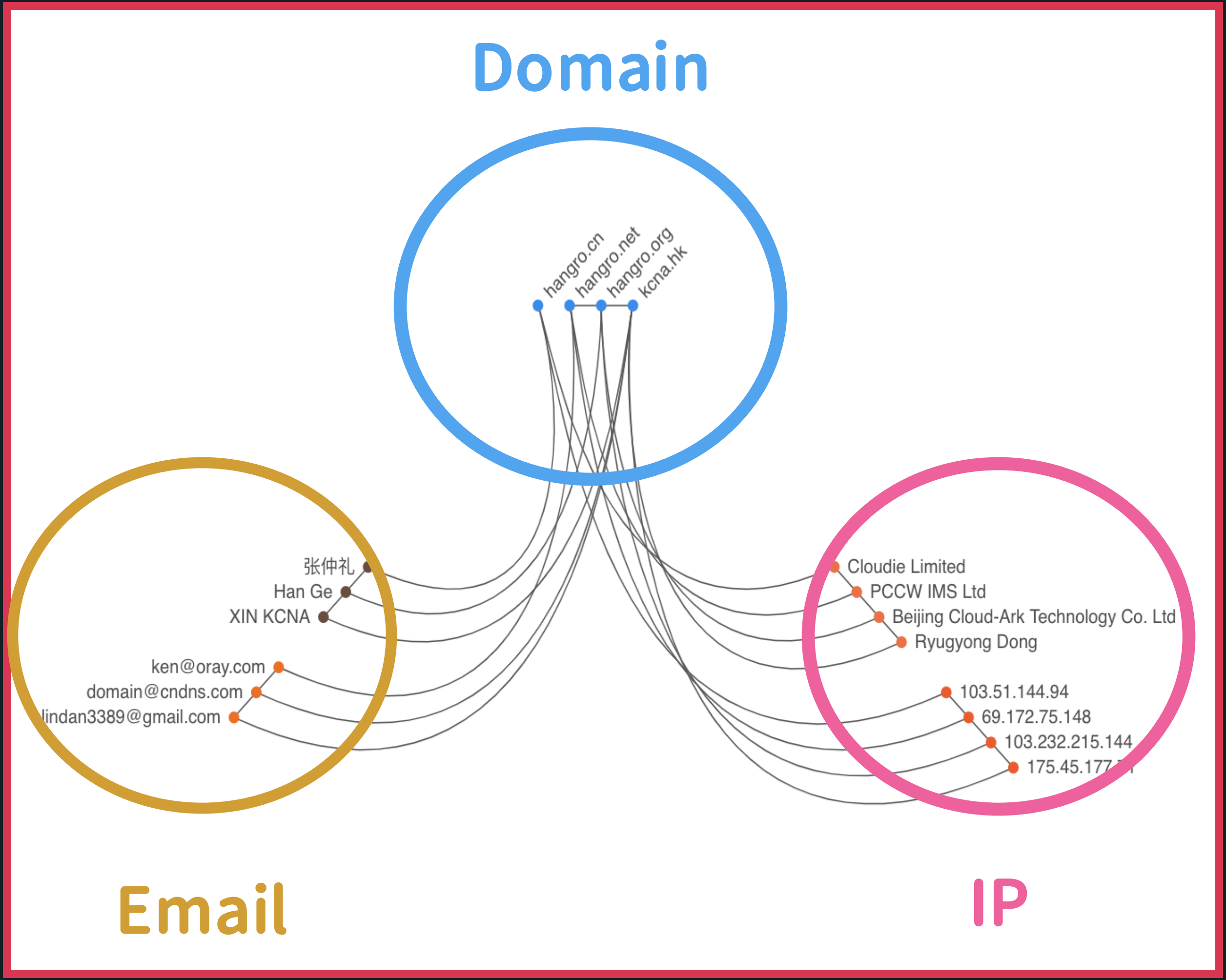
- *Rheinmetall_job_requirements.doc*: identified by ESET Research.
- *General_motors_cars.doc*: identified by Twitter user @1nternaut.
- *Airbus_job_opportunity_confidential.doc*: identified by 360CoreSec.

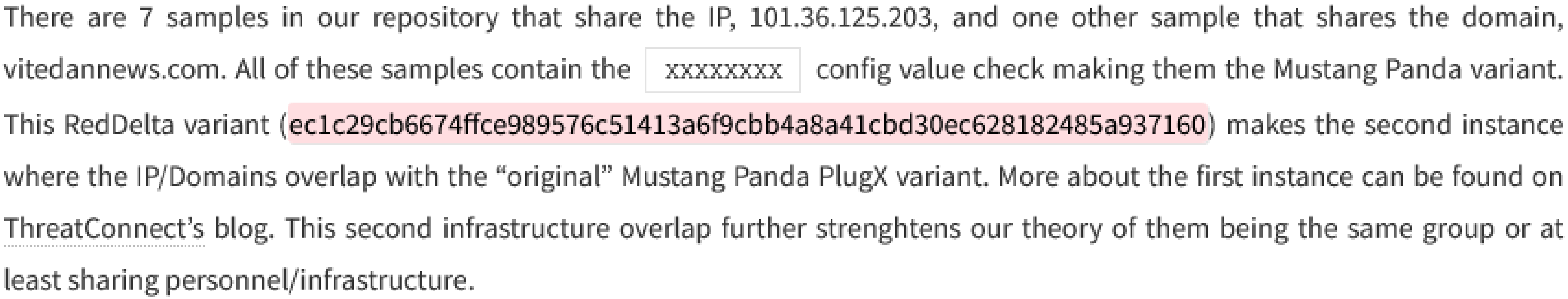
The documents attempted to impersonate new defense contractors and engineering companies like Airbus, General Motors (GM), and Rheinmetall. All of these documents contain macro malware, which has been developed and improved during the course of this campaign and from one target to another. The core techniques for the three malicious documents are the same, but the attackers attempted to reduce the potential detections and increase the faculties of the macros.

(Cloud Consultancy News, 2021)

Infrastructure Analysis

- Domain
  - WHOIS -> Email
  - Passive DNS -> IP
- IP
  - Passive DNS -> Domain
- Email
  - Reverse WHOIS - > Domain





There are 7 samples in our repository that share the IP, 101.36.125.203, and one other sample that shares the domain, vitedannews.com. All of these samples contain the `xxxxxxxx` config value check making them the Mustang Panda variant. This RedDelta variant (ec1c29cb6674ffce989576c51413a6f9cbb4a8a41cbd30ec628182485a937160) makes the second instance where the IP/Domains overlap with the “original” Mustang Panda PlugX variant. More about the first instance can be found on ThreatConnect’s blog. This second infrastructure overlap further strenghtens our theory of them being the same group or at least sharing personnel/infrastructure.

(xorhex, 2021)

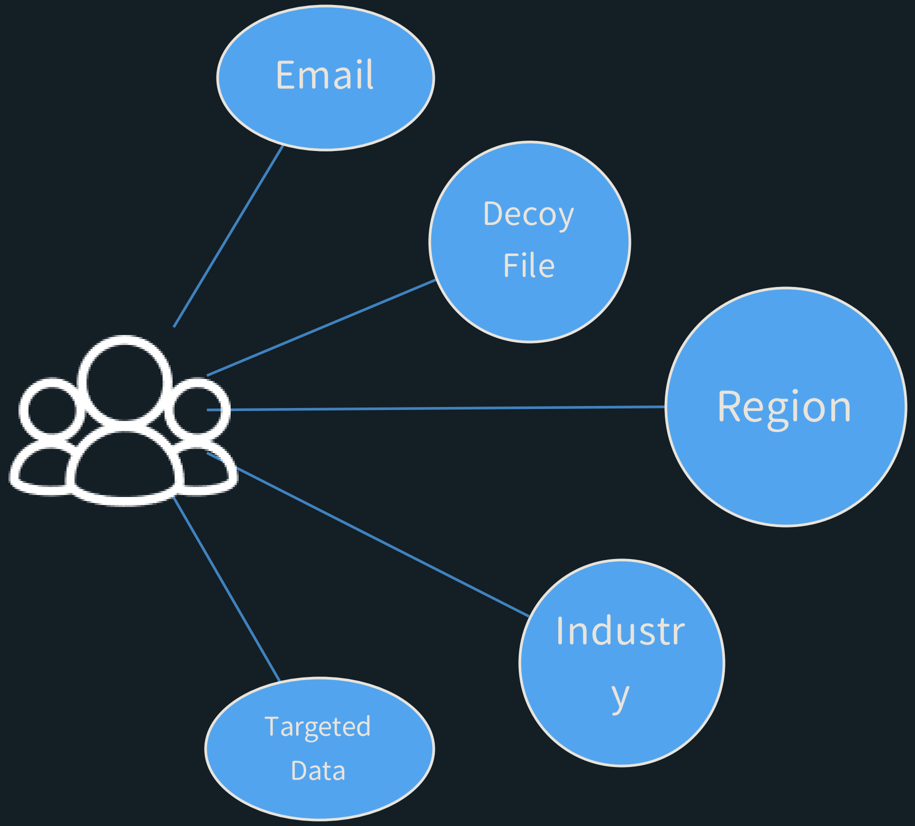
Adversary Analysis

Amoeba
CloudDragon
DarkHotel
DragonOK
GouShe
GuDiao
Higaisa
Huapi
HurricanePanda
KimDragon
Lapis
LuoYu
menuPass
Nian
OceanLotus
Polaris
QiongQi
Sanyo
Sheshnag
SocialNetworkTeam

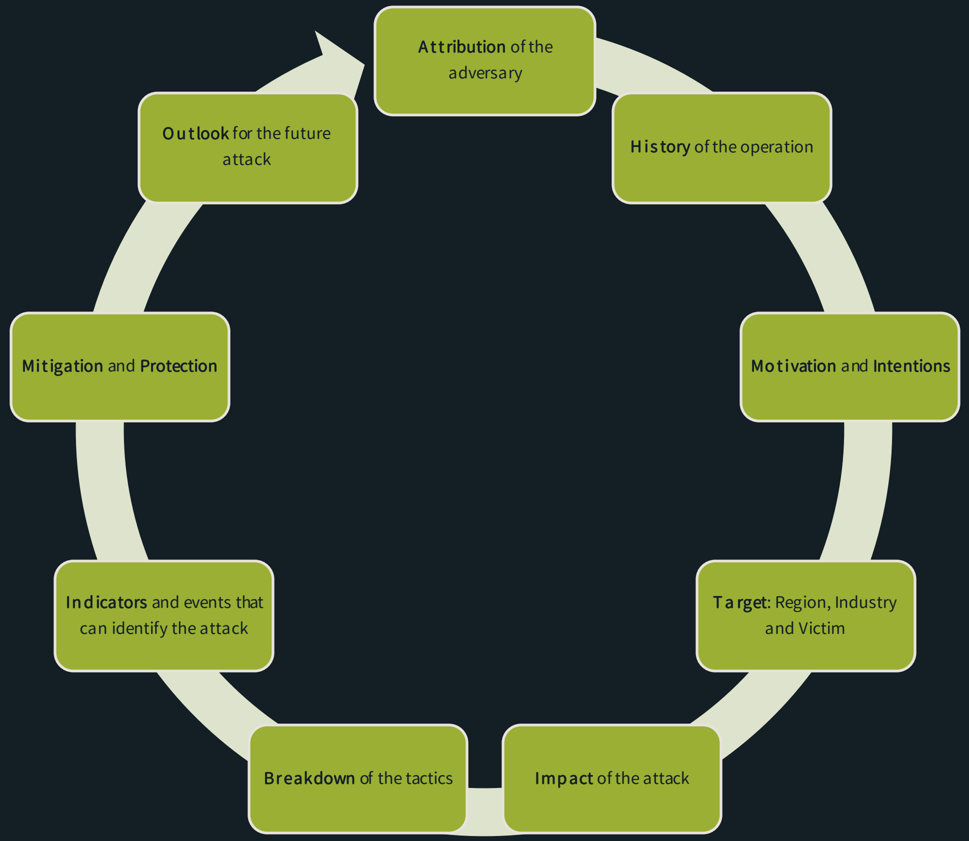
- Actors
  - Language
  - Tools
  - Infrastructure
  - Time zone
- Motivations, intentions
- Cooperation relationship between different groups
  - Shared Tool
  - Shared C2

Target Analysis

Victim Analysis

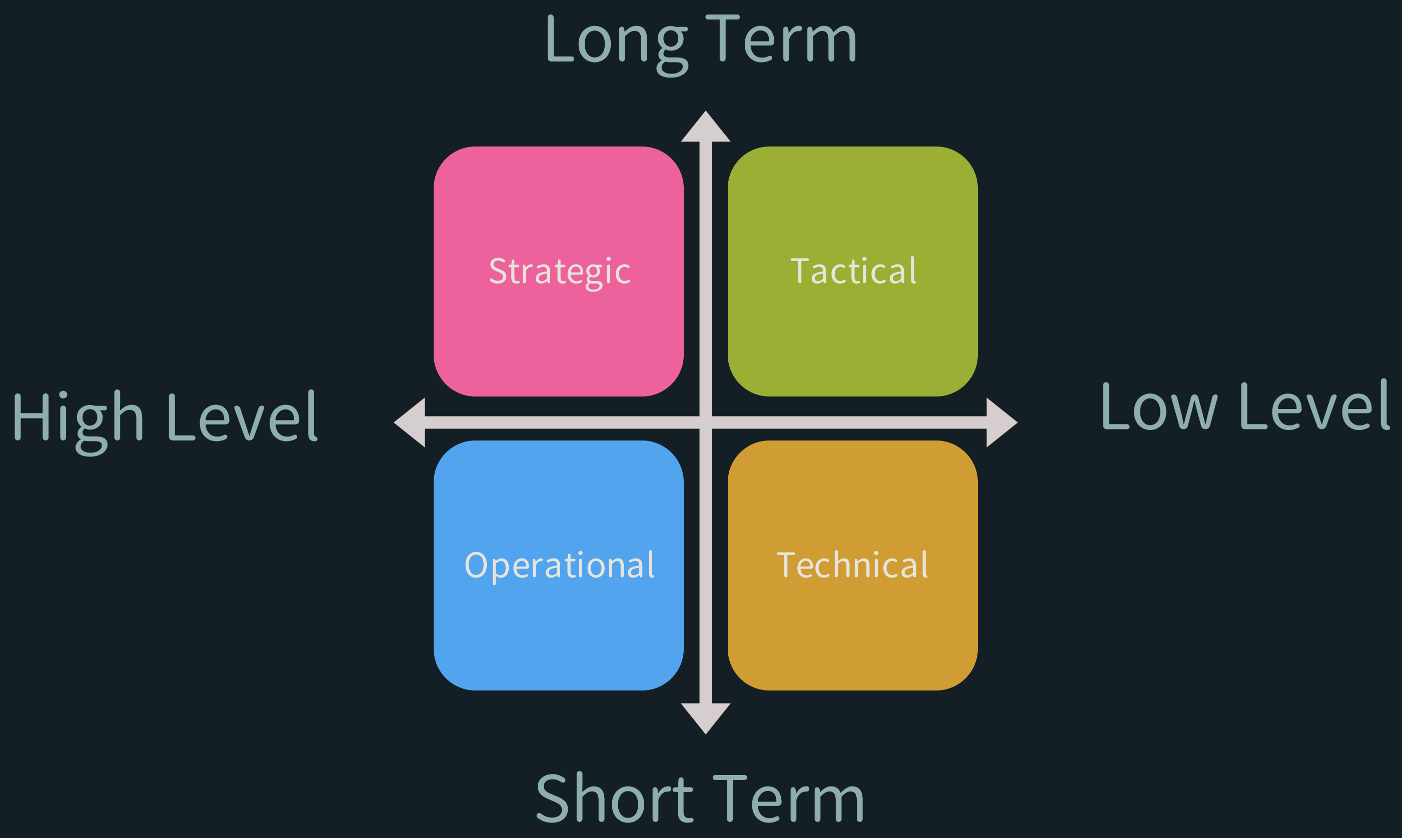


Threat Analysis Report


Attribution of the adversary
History of the operation
Motivation and Intentions
Target: Region, Industry and Victim
Impact of the attack
Breakdown of the tactics
Indicators and events that can identify the attack
Mitigation and Protection
Outlook for the future attack

Dissemination & Integration

- Strategic Planning
- ISCT / CERT Community
- IT Staff CSIRT Team
- Firewall SIEM Triage



Long Term

Strategic

Tactical

High Level

Low Level

Operational

Technical

Short Term

Adversaries Tracked @ T5

GouShe

TEAMT5

- Targets
  - IN, TW, PH, TH, VN
  - Media, Education, Government, IT
- Aliases
  - Tropic Trooper, Pirate Panda, APT23, KeyBoy
- Description
  - GouShe first drew the world's attention with the name Keyboy in 2013, but it became more widely known as Tropic trooper in 2015.
  - The group shows great interest in countries like Taiwan, Vietnam, Philippines, and Australia.
  - GouShe's actors have long been targeting government and military units.

GuDiao

TEAMT5

- Targets
  - HK, MY, PH, VN
  - Dissident, Military, Government
- Description
  - Related to other Chinese APT groups
  - The group mainly aims at governments and military units in Southeast Asia, such as Vietnam and Malaysia.
  - In recent years, it has developed its own malwares and adopted the RoyalRoad exploit, which is popular among Chinese APT groups.

Polaris

- Targets
  - JP, MN, MM, PH, TH, KR, VN
  - Dissident, Government, Media, Telecommunications
- Aliases
  - Mustang Panda, HoneyMyte
- Description
  - The Polaris group has long been a threat to Asian countries, using spear-phishing email to lure their victims.
  - The group was found attacking government departments, media, and journalism-related industries. The group shares common features with other APT groups.

HUAPI

- Targets
  - HK, JP, TW, US, KR
  - Media, Military, Dissidents, Telecommunication, Think tank, IT, Political Party, Heavy Industry, Education & Research Institutions
- Aliases
  - PLEAD, BlackTech, 黑凤梨, Palmerworm
- Description
  - The HUAPI actors have focused on Taiwan, including entities affiliated with Taiwan in other countries, for the first ten years.
  - However, they have started to expand their scope to include Japan since 2017.
  - These actors have the ability to create custom packers to avoid antivirus detection.

CloudDragon

- Targets
  - JP, US, KR
- Aliases
  - Kimsuky, Thallium
- Description
  - Two groups were created, named CloudDragon and KimDragon, as we observed different TTP in the recent years.
  - Main target is South Korea.
  - Recently began to attack United States and Japan as well.

Andariel

- Targets
  - DE, IN, JP, KR
- Description
  - Andariel is a state-sponsored North Korean APT which has been active since at least 2013.
  - According to U.S. Army report, the group is under North Korea’s Cyber Warfare Guidance Unit (commonly known as Bureau 121).
  - Andariel has sniped at critical infrastructure in Asian countries with its propriety malwares.

Getting Started on Threat Intelligence Research

TEAMT5

Threat/Intel Hunting Resources

- Twitter
  - #APT
  - @vxunderground
  - @namazso
  - @Unit42_Intel
  - @ShadowChasing1
  - @h2jazi

- Curated Resources
  - https://start.me/p/rxRbpo/ti
- TLP White Resources
  - Abuse.ch
  - Malpedia
  - vx-underground

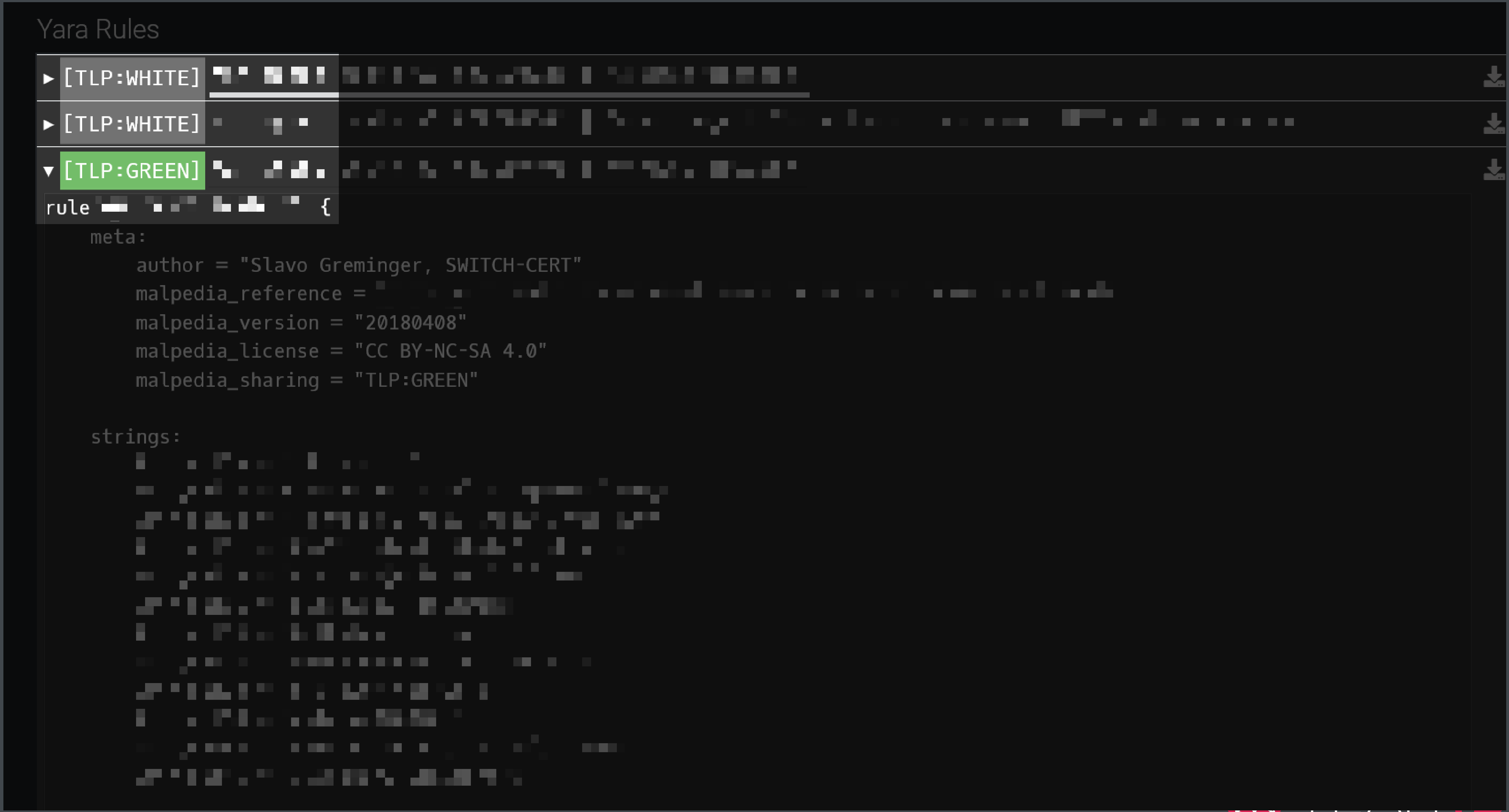
Threat/Intel Hunting Resources

TEAMT5

- Yara rules
  - `Yara-Rules/rules` @ GitHub
  - `InQuest/awesome-yara` @ GitHub
  - `Neo23x0/signature-base` @ GitHub
- CAPA
  - `Mandiant/CAPA` @ GitHub

- Manual analysis
  - Behavior analysis via sandboxes
    - e.g., Triage, CAPEv2, etc.
  - Static analysis via disassemblers
    - e.g., IDA Pro, Ghidra, etc.
  - Dynamic analysis via contained environments
    - e.g., virtual machines, physical bare-bones

Understanding TLP



Yara Rules

▶ [TLP:WHITE] [redacted]

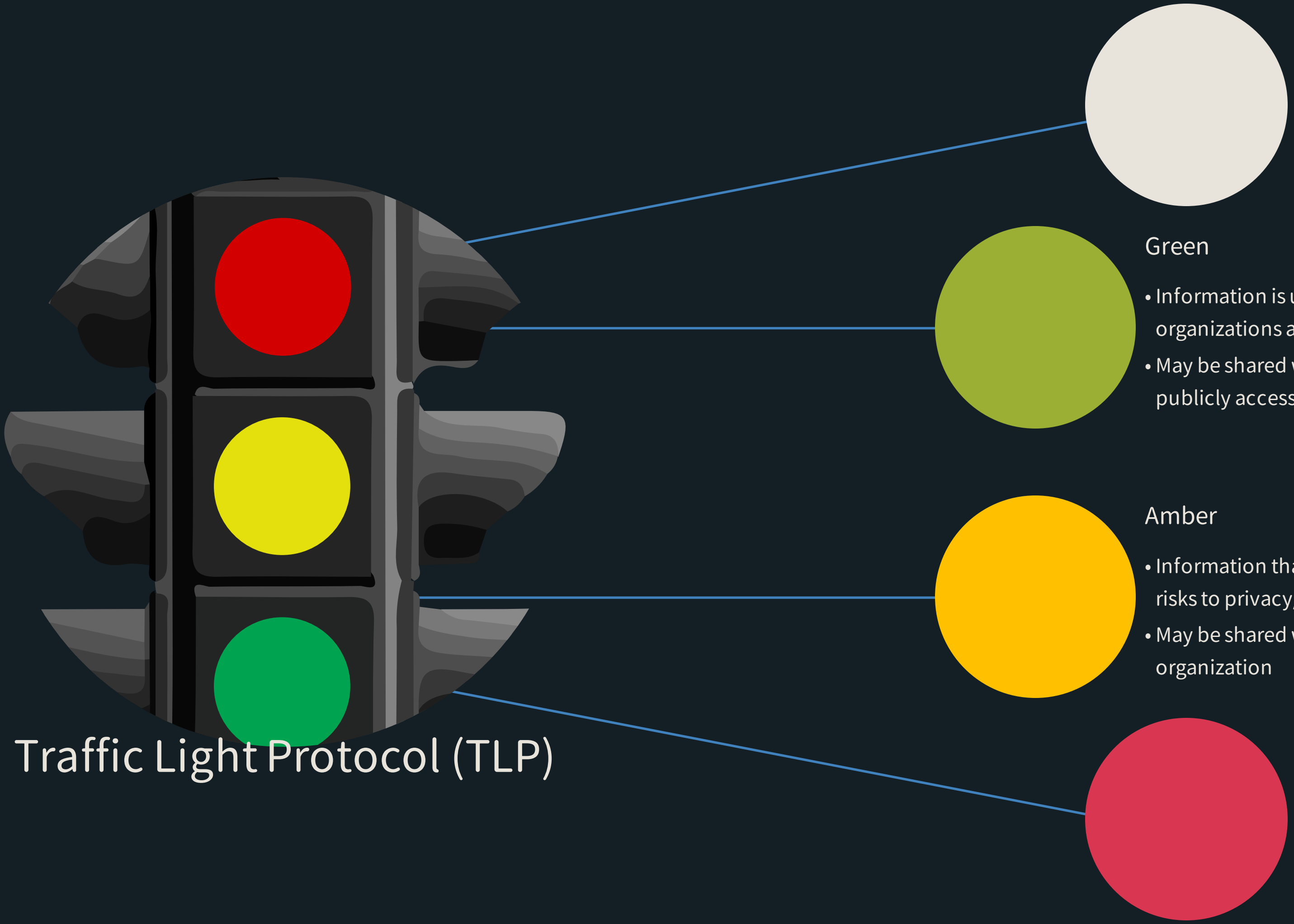
▶ [TLP:WHITE] [redacted]

▼ [TLP:GREEN] [redacted]

```
rule [redacted] {
    meta:
        author = "Slavo Greminger, SWITCH-CERT"
        malpedia_reference = [redacted]
        malpedia_version = "20180408"
        malpedia_license = "CC BY-NC-SA 4.0"
        malpedia_sharing = "TLP:GREEN"

    strings:
        [redacted]
```

What is TLP?



Traffic Light Protocol (TLP)

White

- Information carries minimal risk of misuse
- May be shared without restriction (subject to copyright laws)

Green

- Information is useful for all participating organizations and peers within communities
- May be shared within communities but NOT publicly accessible channels

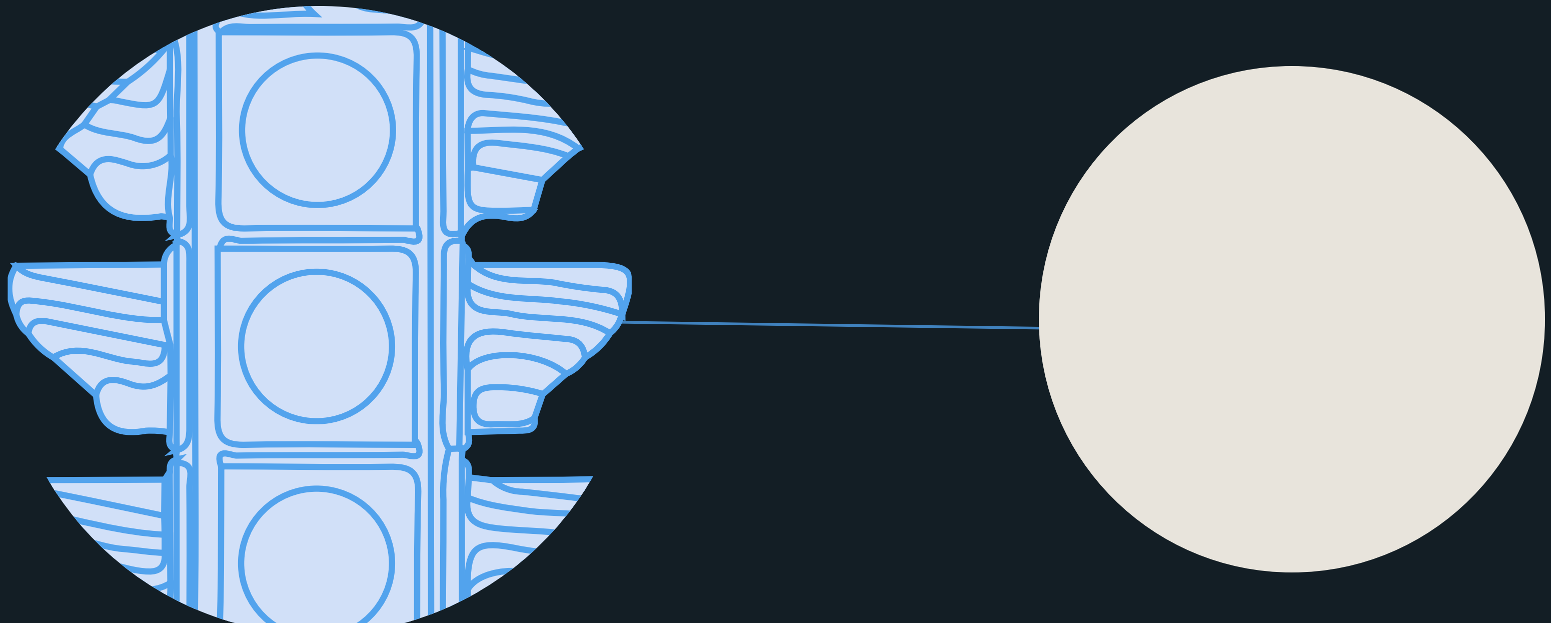
Amber

- Information that is sensitive and may carry risks to privacy/reputation/operations
- May be shared with members of their own organization

Red

- Information that can impact on a party's privacy/reputation/operations
- May NOT be shared outside of private exchange and should be exchanged in-person or verbally.

White



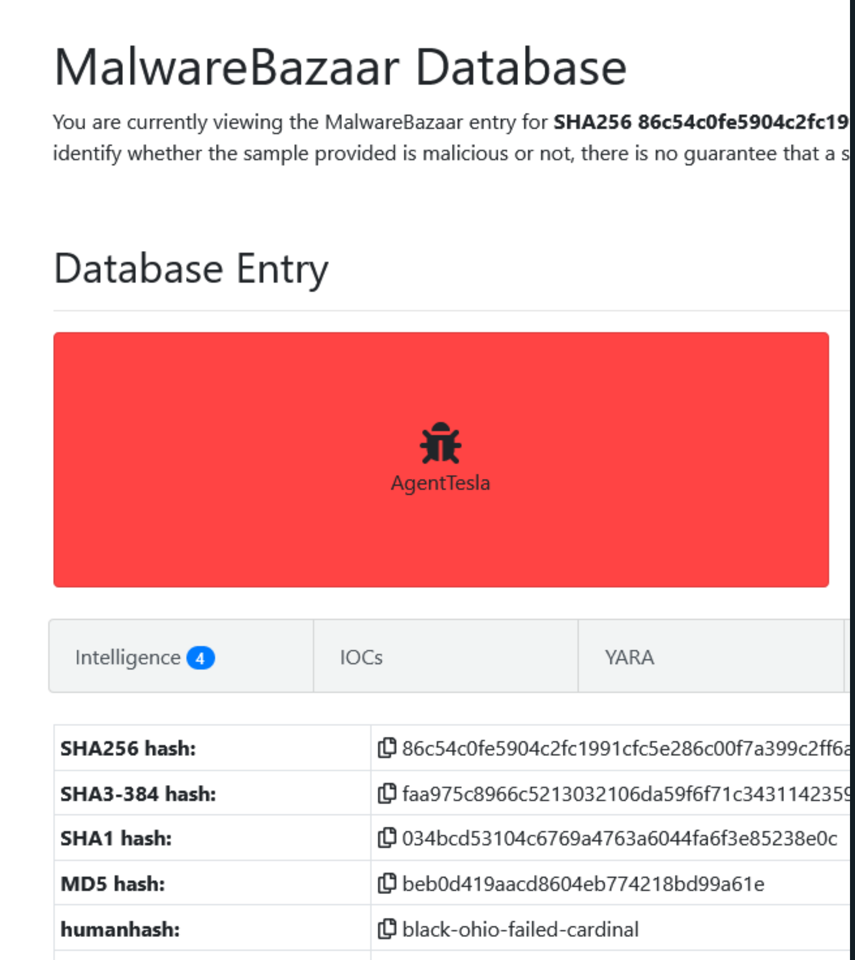
Traffic Light Protocol (TLP)

White

- Information carries minimal risk of misuse
- May be shared without restriction (subject to copyright laws)

Examples of TLP:White

- Malware Bazaar (bazaar.abuse.ch)
- #APT
- @vxunderground
- Malpedia (public)



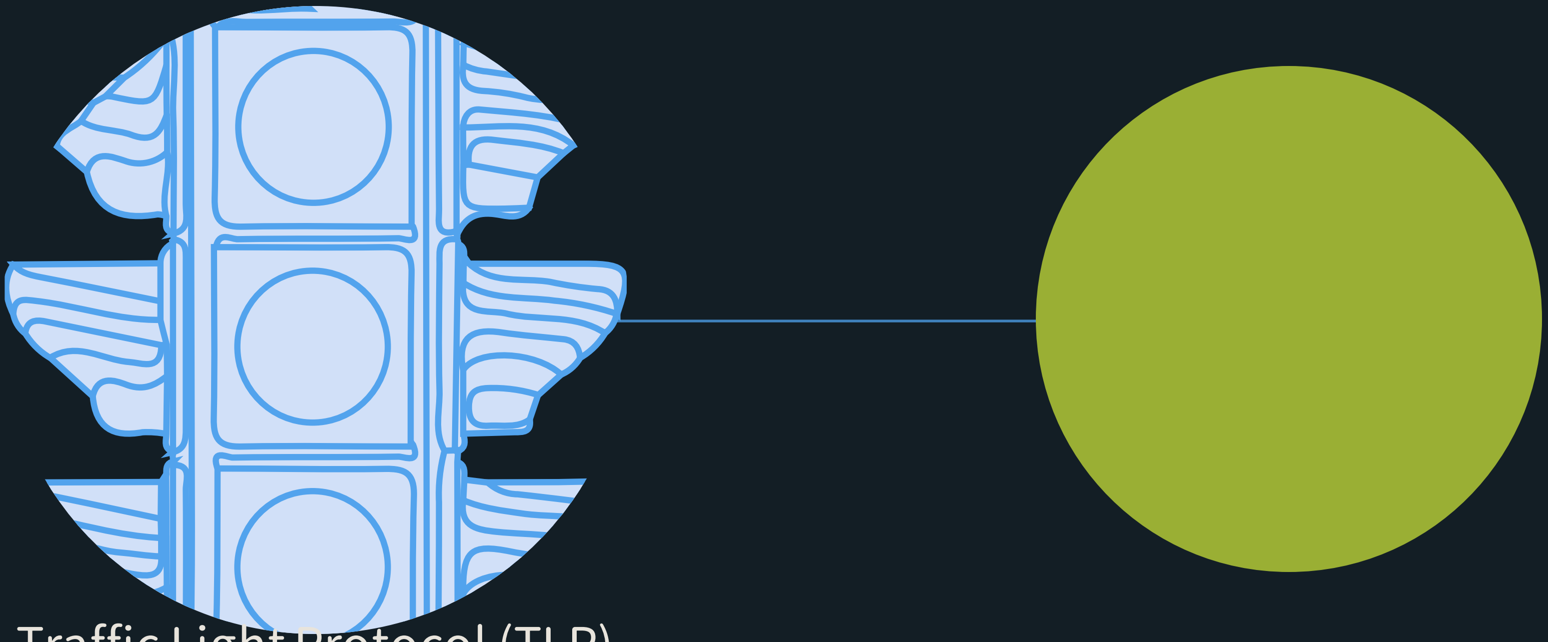
MalwareBazaar Database

You are currently viewing the MalwareBazaar entry for **SHA256 86c54c0fe5904c2fc19**
identify whether the sample provided is malicious or not, there is no guarantee that a s

Database Entry

SHA256 hash:	86c54c0fe5904c2fc1991cfc5e286c00f7a399c2ff6a
SHA3-384 hash:	faa975c8966c5213032106da59f6f71c3431142359
SHA1 hash:	034bcd53104c6769a4763a6044fa6f3e85238e0c
MD5 hash:	beb0d419aacd8604eb774218bd99a61e
humanhash:	black-ohio-failed-cardinal

What is TLP?

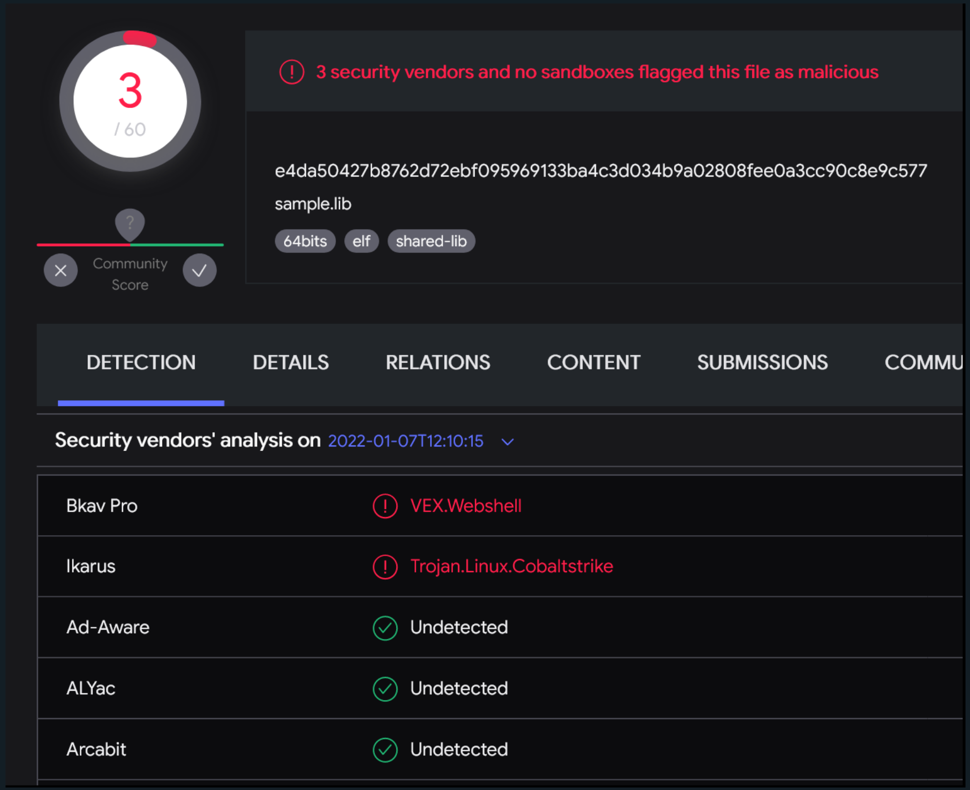


Traffic Light Protocol (TLP)

Green

- Information is useful for all participating organizations and peers within communities
- May be shared within communities but NOT publicly accessible channels

Examples of TLP:Green



3 security vendors and no sandboxes flagged this file as malicious

e4da50427b8762d72ebf095969133ba4c3d034b9a02808fee0a3cc90c8e9c577

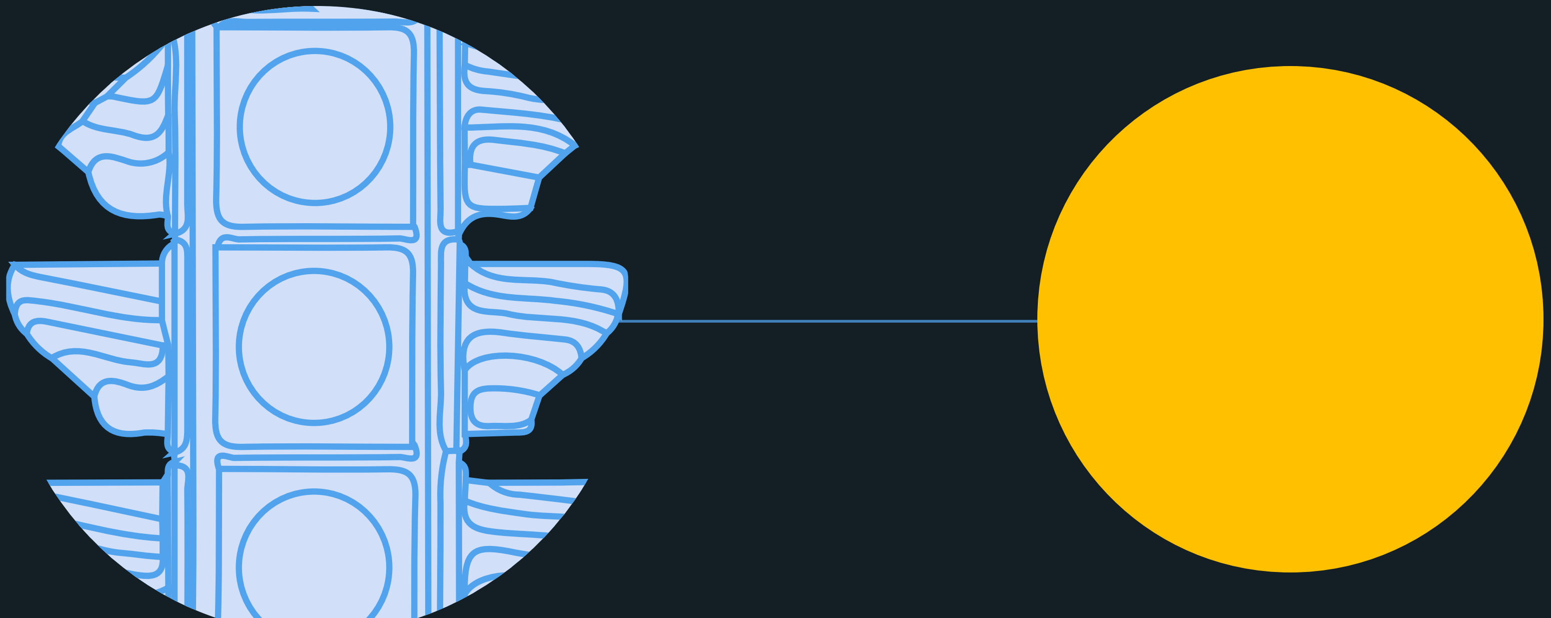
sample.lib

Security vendors' analysis on 2022-01-07T12:10:15

Bkav Pro	VEX.Webshell
Ikarus	Trojan.Linux.Cobaltstrike
Ad-Aware	Undetected
ALYac	Undetected
Arcabit	Undetected

- Samples on public sandbox
  - VirusTotal (Enterprise API)
  - Hybrid-analysis (manual approval)
  - CAPE (manual approval)
- Intelligence from private community
  - Malpedia (manual approval)

What is TLP?



Traffic Light Protocol (TLP)

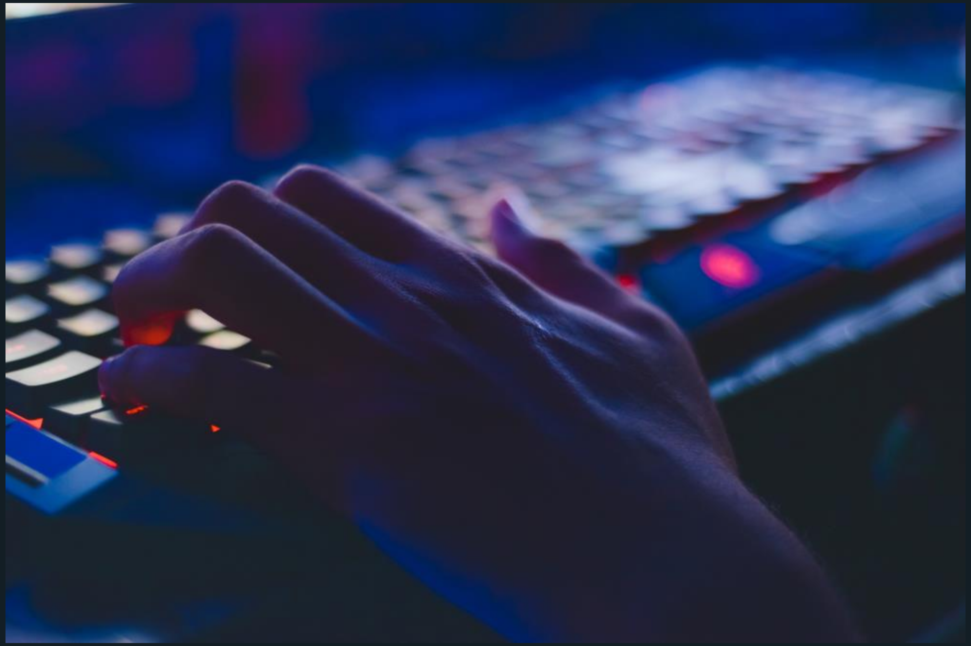
Amber

- Information that is sensitive and may carry risks to privacy/reputation/operations
- May be shared with members of their own organization

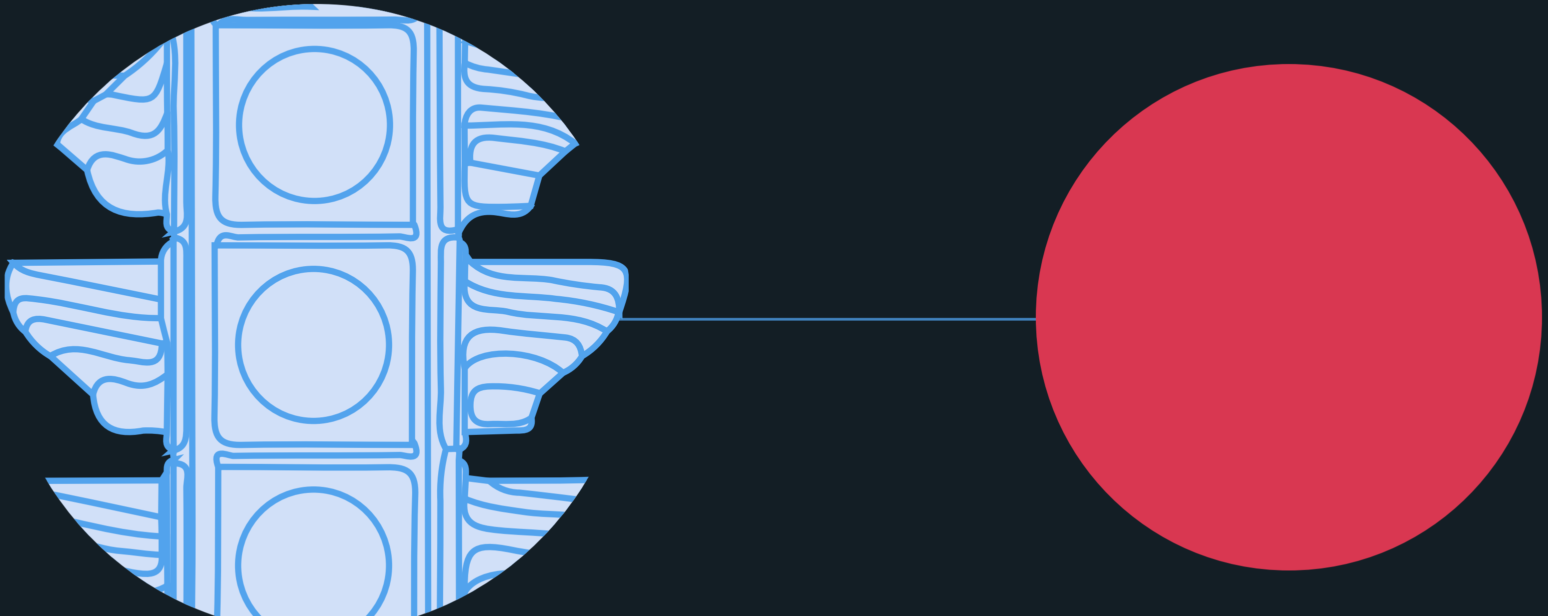
Examples of TLP:Amber

TEAMT5

- Samples passed from private sources
  - Friends
  - Fellow researchers
  - Colleagues
- Customer data



What is TLP?



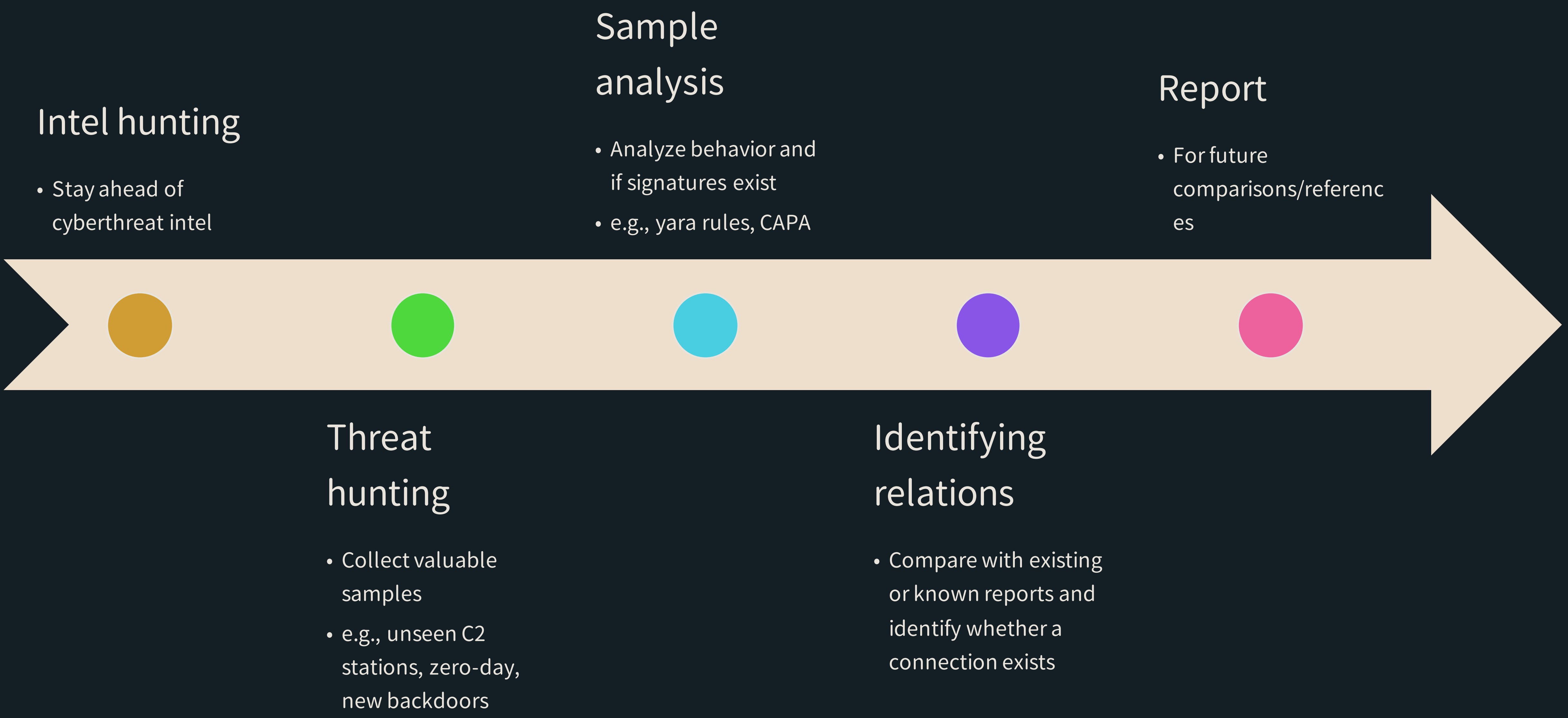
Traffic Light Protocol (TLP)

Red

- Information that can impact on a party’s privacy/reputation/operations
- May NOT be shared outside of private exchange and should be exchanged in-person or verbally.

Writing a CTI Report

Standard Operating Procedures



Intel hunting

- Stay ahead of cyberthreat intel

Threat hunting

- Collect valuable samples
- e.g., unseen C2 stations, zero-day, new backdoors

Sample analysis

- Analyze behavior and if signatures exist
- e.g., yara rules, CAPA

Identifying relations

- Compare with existing or known reports and identify whether a connection exists

Report

- For future comparisons/references

Content of a Report

TEAMT5

How did the incident occur?

- Delivery method(s)
- Phishing method(s)/theme(s)
- Exploitation method(s)

Content of a Report

How did the incident occur?

- Delivery method(s)
- Phishing method(s)/theme(s)
- Exploitation method(s)

What did it cause?

- Summary of the malicious behaviors
- IOC (Indicator of Compromise)

Content of a Report

TEAMT5

How did the incident occur?

- Delivery method(s)
- Phishing method(s)/theme(s)
- Exploitation method(s)

What did it cause?

- Summary of the malicious behaviors
- IOC (Indicator of Compromise)

Who did it?

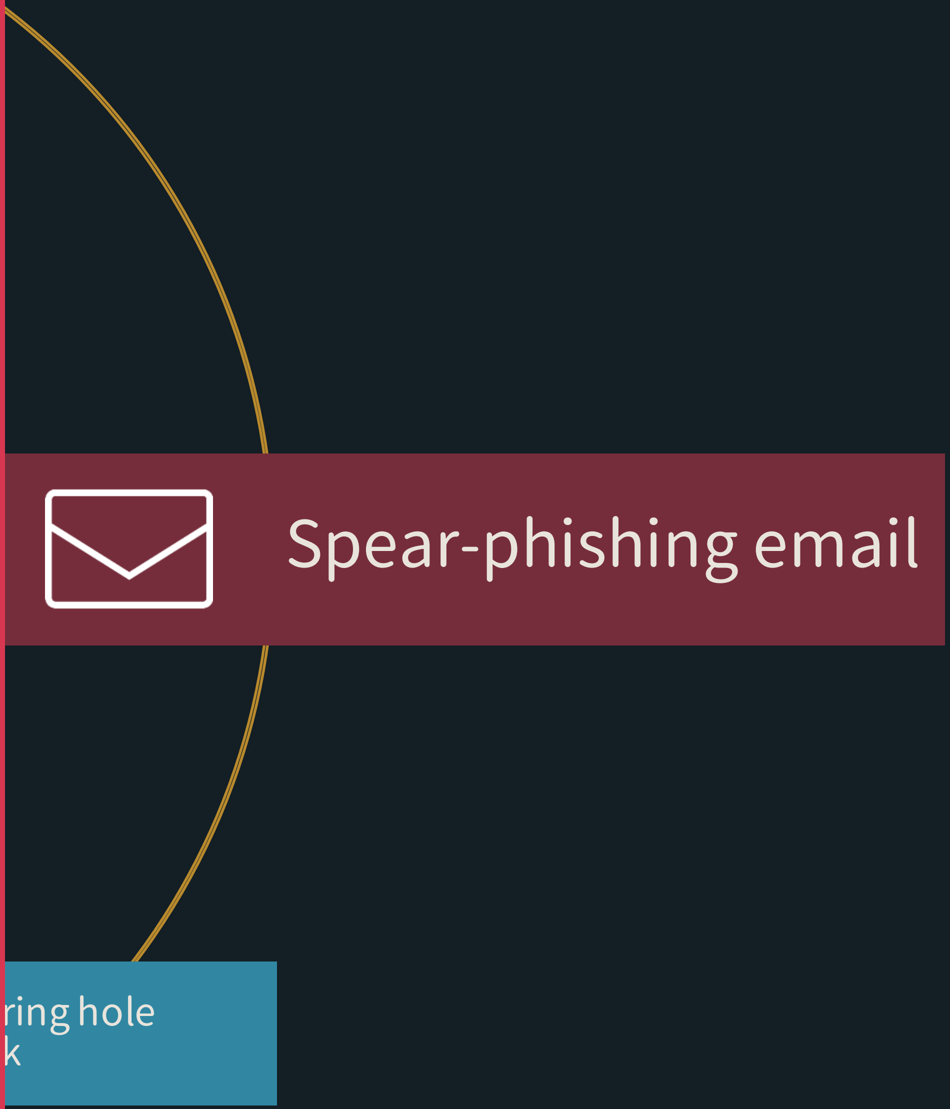
- Source infrastructure analysis
- Piece everything together with existing reports

How did the incident occur?

Delivery Methods

- Spear-phishing email
- Watering hole attack
- Supply chain attack

Delivery Methods

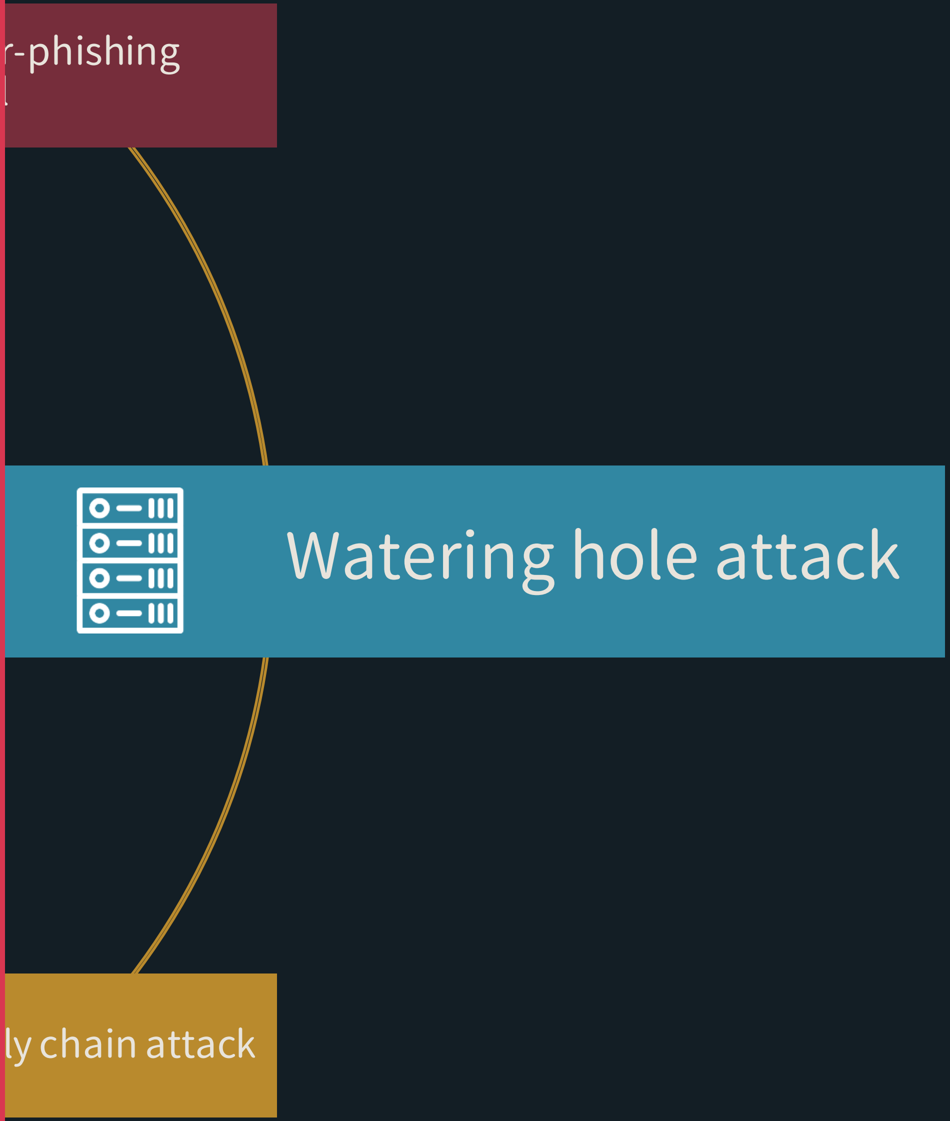


Spear-phishing email

ring hole
k

- Targeted attack
  - Typically used against high-profile individuals or company head
  - e.g., CEO, head of a division, activists
- Social engineering
  - Sensitive subject matter
  - e.g., something that involves sense of urgency
- Disguised as legitimate corporate email
  - Potentially contains malicious attachments or links

Delivery Methods

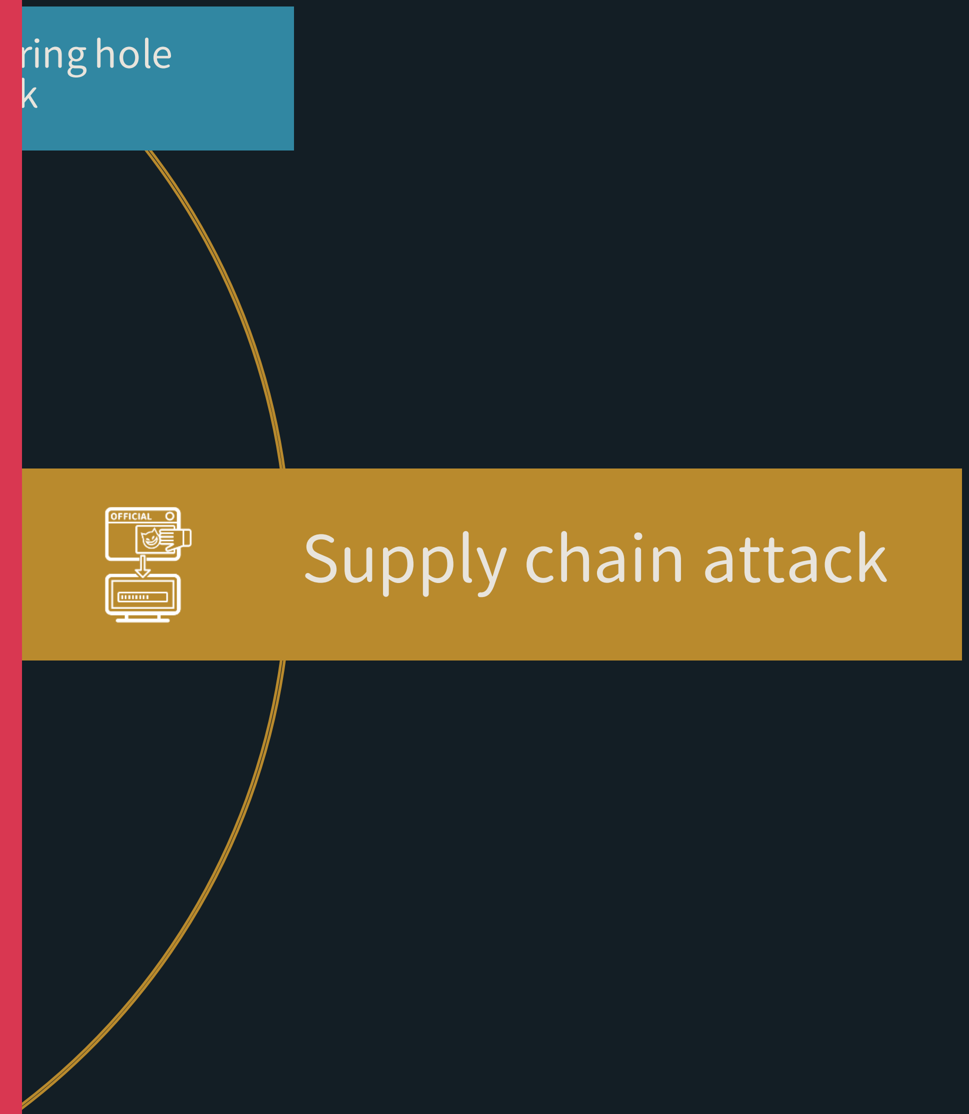


- Compromise sites that victim frequents
- Drive-by via malvertisements or domain redirection
- Example
  - Holy Water campaign in 2020
    - Targeted religious and charity websites

Delivery Methods

- Compromise components from supply chains
  - e.g., software update hosts
- Easily wide-spread as these software components may be mass distributed (i.e., from part of a supply chain)
- Example
  - ASUS ShadowHammer in 2019

Delivery Methods



- Compromise components from supply chains
  - e.g., software update hosts
- Easily wide-spread as these software components may be mass distributed (i.e., from part of a supply chain)
- Example
  - ASUS ShadowHammer in 2019

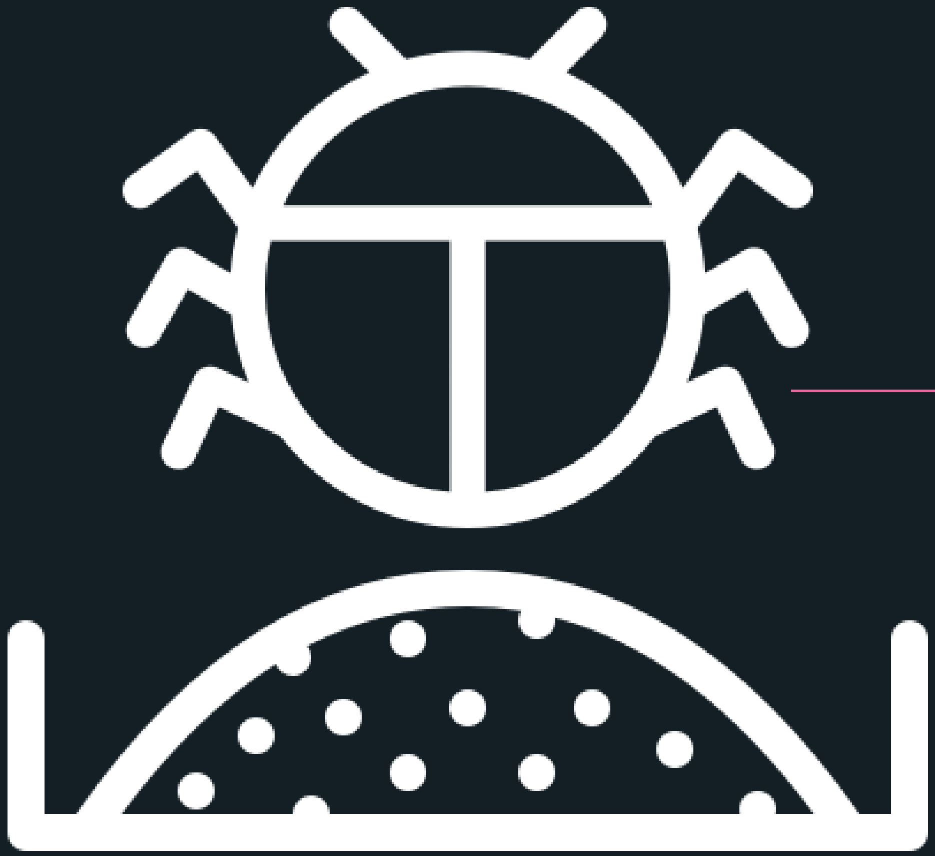
What exactly happened?

Malware Analysis

Containerized environment

- Preferably offline
- Otherwise, connect to a VPN/TOR at host-level

Malware Analysis

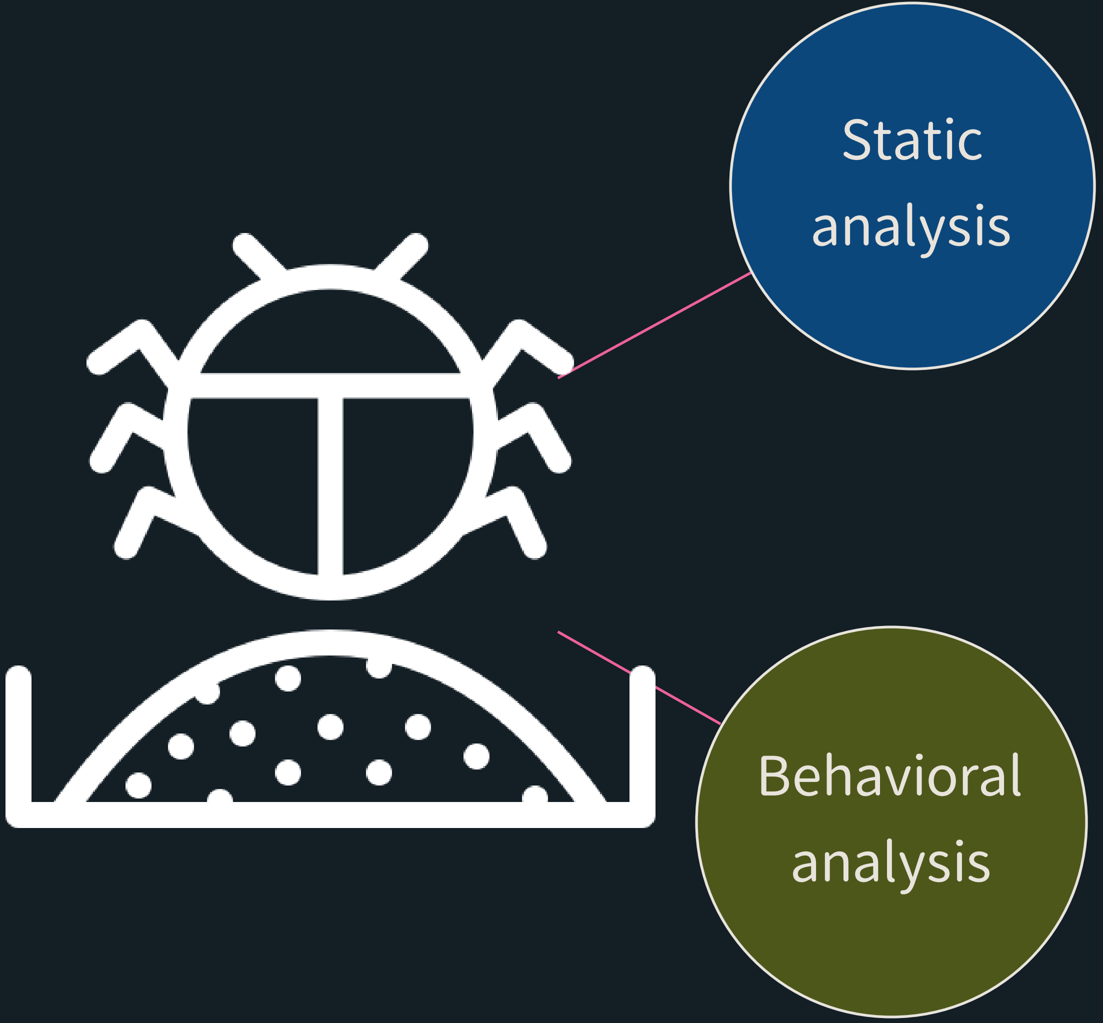


Static analysis

- Disassembler
- Digital signature
  - Stolen cert
- PE header

Malware Analysis

TEAMT5



- Disassembler
- Digital signature
  - Stolen cert
- PE header

- Artifacts
- Persistence
- Exfiltrated data
- Network traffic
- Encryption algorithm
- Backdoor

Who did it?

Infrastructure Analysis

TEAMT5

Virtual Private Server (VPS)

- e.g., Linode, Digital Ocean, Aliyun, AWS, GCP

Web hosting

- e.g., hostinger, Bluehost, SiteGround

Compromised server

- i.e., privately owned by an individual, overtaken by threat actor

Virtual Private Server (VPS)

- Rented or bought by the threat actor
- Usually assigned a fixed and unique IP
- Threat actor has complete control over the server
  - Open certain ports or services for backdoor connection
  - Connect via SSH/RDP

Web Hosting

- Free/paid
- Two or more users may share the same machine
  - More than one domain may resolve to the same IP address or set of addresses
  - Threat actors could only access the frontend
  - Implemented alongside simple backdoors or only used to serve malicious files

Compromised Server

- Unauthorized access via…
  - Web application vulnerabilities
  - Software vulnerabilities
  - Compromised credentials
- Access level highly depends on the method of intrusion
- Backdoors are generally well-hidden to avoid raising suspicion

Compare Findings

- Collect OSINT resources
  - Other analysists' view or thoughts
    - Twitter, Medium, blogs, etc.
  - Existing reports on the sample published by another security firm or researcher
    - FireEye, Kaspersky, CrowdStrike, Malwarebytes, etc.
- Personal or internal documents
  - Look for past records in the archive, if any
  - Cross-compare C2 used, behaviors exhibited, peculiar strings, etc.

工商時間

TeamT5 – 世界級的專業資安團隊

台灣自主研發團隊

TEAMT5
杜 浦 數 位 安 全
Persistent Cyber Threat Hunters

資安顧問服務

Threat Intelligence	網路威脅情資追蹤研究
Incident Response	資安事件處理與調查
Consulting Service	綜合資安諮詢顧問

10年以上網路威脅研究經驗

- 於Black Hat、CODE BLUE等國際頂尖研討會發表多篇研究成果
- 實驗室多位成員參與DEF CON CTF等國際比賽獲獎無數

擅長亞太區網路間諜防護，服務客戶範圍遍及全球

- 台灣：政府單位、金融業、科技業、顧問業、各大SOC
- 日本：電信集團、電機製造商、綜合商社、政府單位
- 美國、歐洲、韓國：結盟知名資安大廠，服務金融業客戶

TEAMT5

TeamT5
台北總部

南京三民站

TEAMT5
杜浦數位安全

TeamT5
高雄辦公室

三多商圈站

公司福利

電玩大賽 吃喝玩樂 國內外員工旅遊 部門聚餐

TEAMT5

休假多多

Work-Life Balance
連七夕也放假

社團多元

羽球、登山
瑜伽，各種社團
歡迎來找同好

遊戲空間

PS4、Switch、
按摩椅、飛鏢機
遊戲空間應有盡有

各種獎金

績效、年終
生日、佳節
各種$$$$$

我也想加入！

TEAMT5

We Want You

Vulnerability Researcher

- 熱愛產品安全研究，熟悉韌體分析相關程序及細節
- 熟悉 IDA、Ghidra、GDB 等逆向分析及動態分析工具

Cyber Threat Intelligence Researcher

- 具備 Python, C 等程式語言撰寫能力
- 熟悉 IDA、x64dbg 等逆向分析及動態分析工具，有 YARA rule 撰寫經驗者佳

Cyber Threat Intelligence Analyst

- 非資工科系背景，關心國際政治局勢變化
- 具備英文報告撰寫能力、批判性思考、邏輯分析能力

THANK YOU!

@AzakaSekai_

@AzakaSekai

still@teamt5.org

@still@infosec.exchange

TEAMT5

Persistent Cyber Threat Hunters

References

- Beaumont, K. (2021, July 5). *Kaseya supply chain attack delivers mass ransomware event to US companies*. Medium. https://doublepulsar.com/kaseya-supply-chain-attack-delivers-mass-ransomware-event-to-us-companies-76e4ec6ec64b
- Bestuzhev, D., Oleg Gorobets, & Assolini, F. (2021, November 30). *LatAm banking threats: How regional actors move global and how to fight it back*. https://securelist.com/webinars/latam-banking-threats-regional-actors-move-global/
- Cloud Consultancy News. (2021, July 14). Lazarus APT was found hitting job seekers in the U.S. and Europe with malicious emails. *The Cloud Consultancy*. https://thecloudconsultancy.co/news/lazarus-campaign-ttps-and-evolution/
- Microsoft Corp. (2021, November 12). *PE Format—Win32 apps*. https://docs.microsoft.com/en-us/windows/win32/debug/pe-format
- Stone, M. (n.d.). *Backdoor Attacks: Learning from Operation ShadowHammer*. Verizon Enterprise. Retrieved January 17, 2022, from https://enterprise.verizon.com/resources/articles/s/learning-from-backdoor-attacks-operation-shadowhammer/
- xorhex. (2021, June 2). *RedDelta PlugX Undergoing Changes and Overlapping Again with Mustang Panda PlugX Infrastructure*. Custom Tools, Reverse Engineering, and Threat Research. https://blog.xorhex.com/blog/reddeltaplugxchangeup/
- Yosifovich, P., Russinovich, M. E., Solomon, D. A., & Ionescu, A. (2017). *Windows Internals: Part 1* (Seventh edition). Microsoft.