一探威脅情資

威脅情資到底在幹嘛的？研究人員的一天？

Still Hsu

TEAMT5

Persistent Cyber Threat Hunters

whoami

TEAMT5

Still Hsu

- BEL, English Dep. @ NPTU (屏東大學)
  - Pingtung Hacker TA
- Threat Intel Researcher @ TeamT5
- Interested in...
  - Windows internals
  - .NET
- Non-binary (they/them)

惡意程式？不就只是首頁綁架或勒索軟體那種？

TEAMT5

情資威脅是啥?

APT?????

了解威脅情資

Threat Intelligence

「知彼知己者，百戰不殆。」

《孫子．謀攻》

定義

了解敵人

- 打你的人到底是何方神聖？

(CrowdStrike, 2021)

定義

TEAMT5 杜浦數位安全

了解敵人

- 打你的人到底是何方神聖？

了解動機跟方式 (TTPs)

- 為了什麼？
- 怎麼打的？
  - 戰略 (Tactics)
  - 方式 (Techniques)
  - 步驟 (Procedures)

(CrowdStrike, 2021)

定義

了解敵人

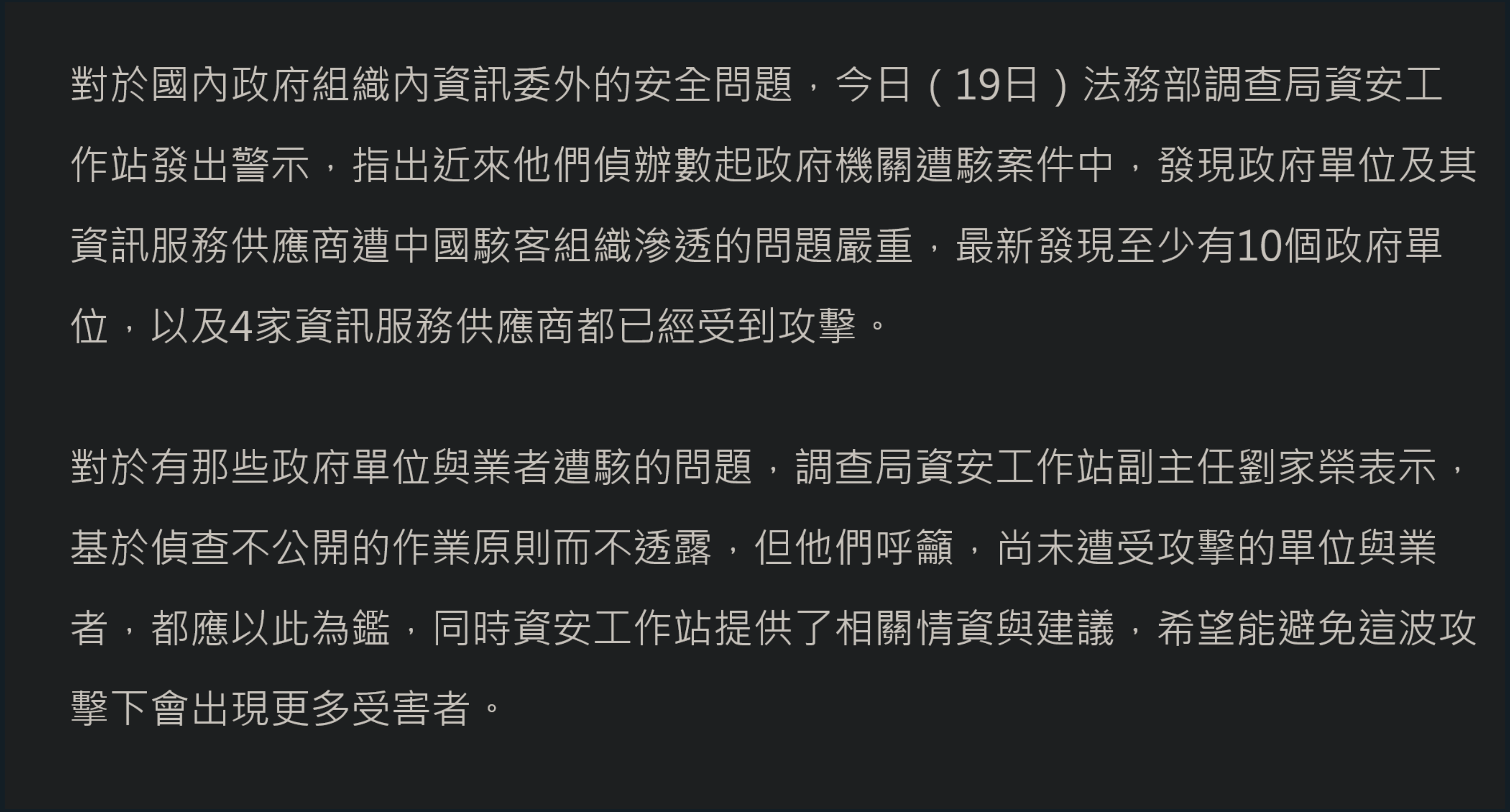
- 打你的人到底是何方神聖？

了解動機跟方式 (TTPs)

- 為了什麼？
- 怎麼打的？
  - 戰略 (Tactics)
  - 方式 (Techniques)
  - 步驟 (Procedures)

幫助降低風險並提升效率

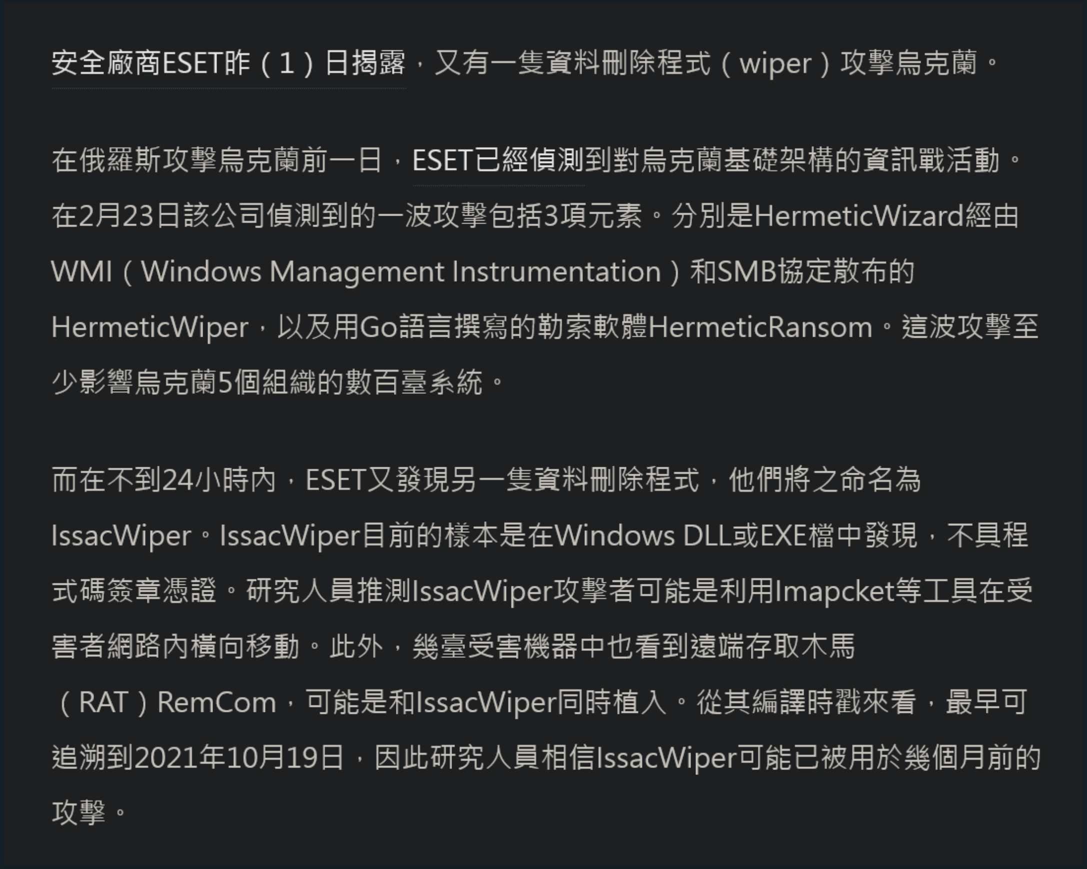
(CrowdStrike, 2021)



對於國內政府組織內資訊委外的安全問題，今日（19日）法務部調查局資安工作站發出警示，指出近來他們偵辦數起政府機關遭駭案件中，發現政府單位及其資訊服務供應商遭中國駭客組織滲透的問題嚴重，最新發現至少有10個政府單位，以及4家資訊服務供應商都已經受到攻擊。

對於有那些政府單位與業者遭駭的問題，調查局資安工作站副主任劉家榮表示，基於偵查不公開的作業原則而不透露，但他們呼籲，尚未遭受攻擊的單位與業者，都應以此為鑑，同時資安工作站提供了相關情資與建議，希望能避免這波攻擊下會出現更多受害者。

「調查局首度揭露國內政府委外廠商成資安破口的現況，近期至少10個公家單位與4家資訊服務供應商遇害」- (iThome, 2020)



安全廠商ESET昨（1）日揭露，又有一隻資料刪除程式（wiper）攻擊烏克蘭。

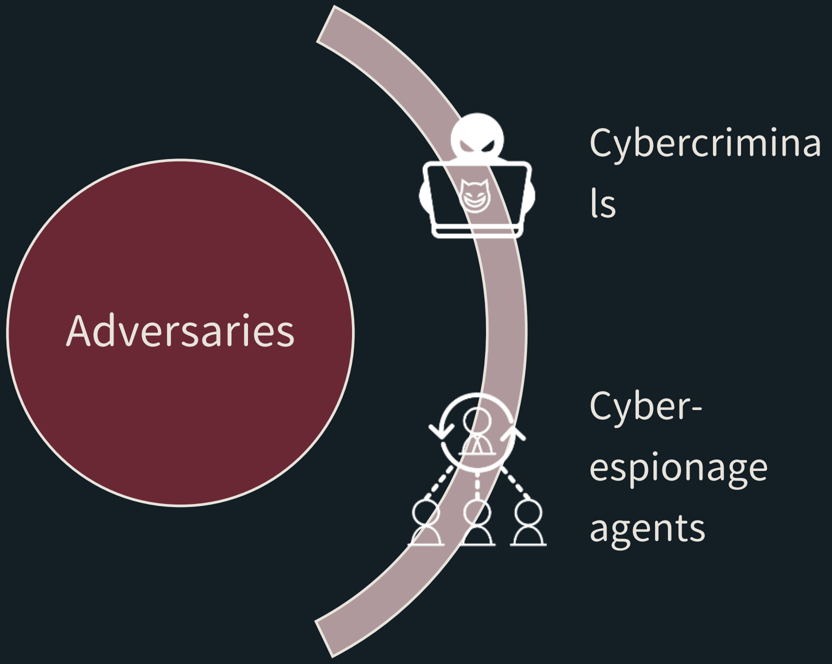
在俄羅斯攻擊烏克蘭前一日，ESET已經偵測到對烏克蘭基礎架構的資訊戰活動。在2月23日該公司偵測到的一波攻擊包括3項元素。分別是HermeticWizard經由WMI（Windows Management Instrumentation）和SMB協定散布的HermeticWiper，以及用Go語言撰寫的勒索軟體HermeticRansom。這波攻擊至少影響烏克蘭5個組織的數百臺系統。

而在不到24小時內，ESET又發現另一隻資料刪除程式，他們將之命名為IssacWiper。IssacWiper目前的樣本是在Windows DLL或EXE檔中發現，不具程式碼簽章憑證。研究人員推測IssacWiper攻擊者可能是利用Imapcket等工具在受害者網路內橫向移動。此外，幾臺受害機器中也看到遠端存取木馬（RAT）RemCom，可能是和IssacWiper同時植入。從其編譯時戳來看，最早可追溯到2021年10月19日，因此研究人員相信IssacWiper可能已被用於幾個月前的攻擊。

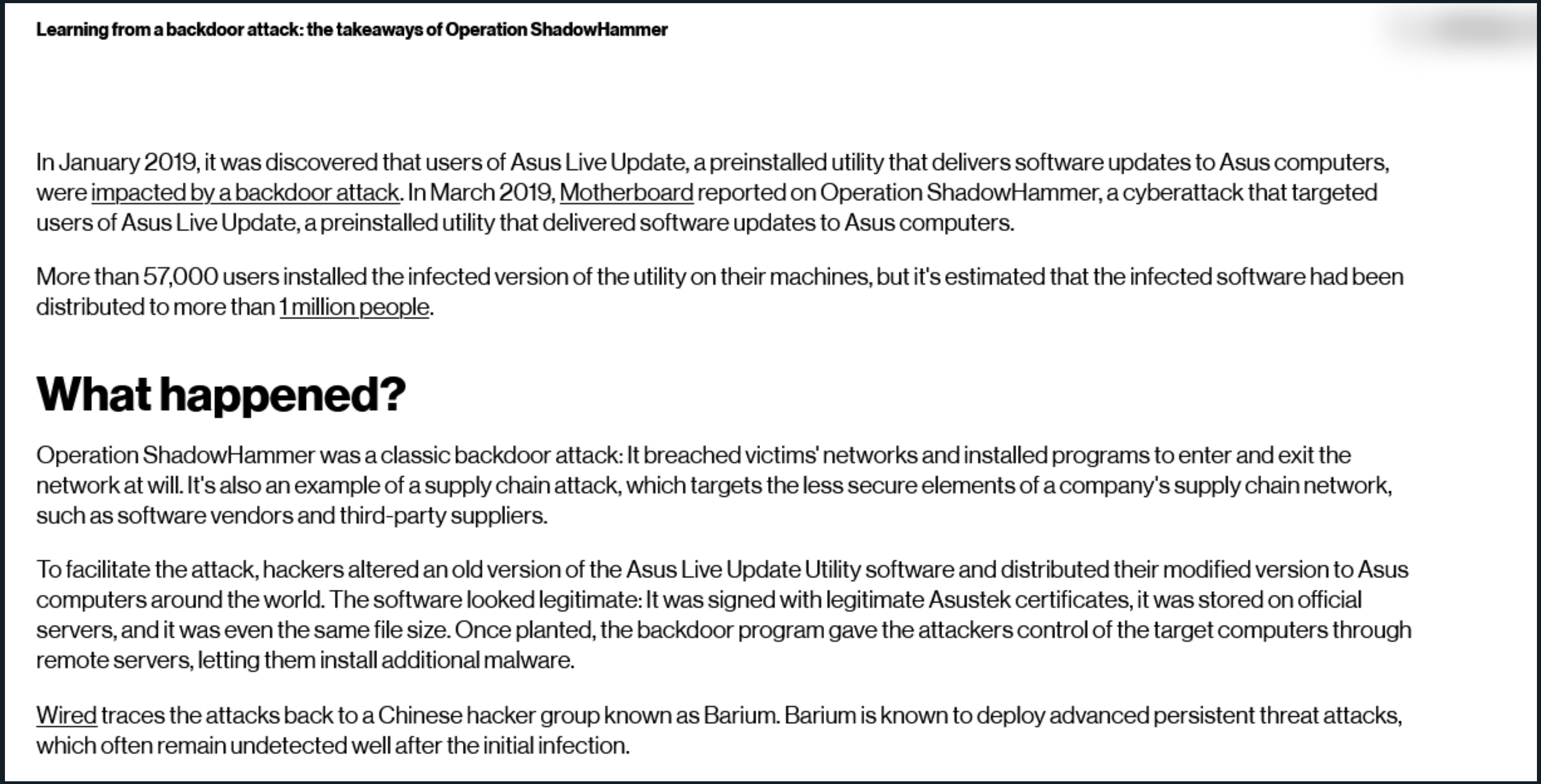
「第3隻資料刪除程式Issac Wiper攻擊烏克蘭」- (iThome, 2022)

敵人種類？

敵人種類



- 犯罪集團 (Cybercriminals)
  - 主要以謀利為主
  - 如使用info stealer, ransomware 等等
- 間諜組織
  - 主要以竊取資訊為主
  - 竊取重要開發資料、設計藍圖、造成經濟損傷等等



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.

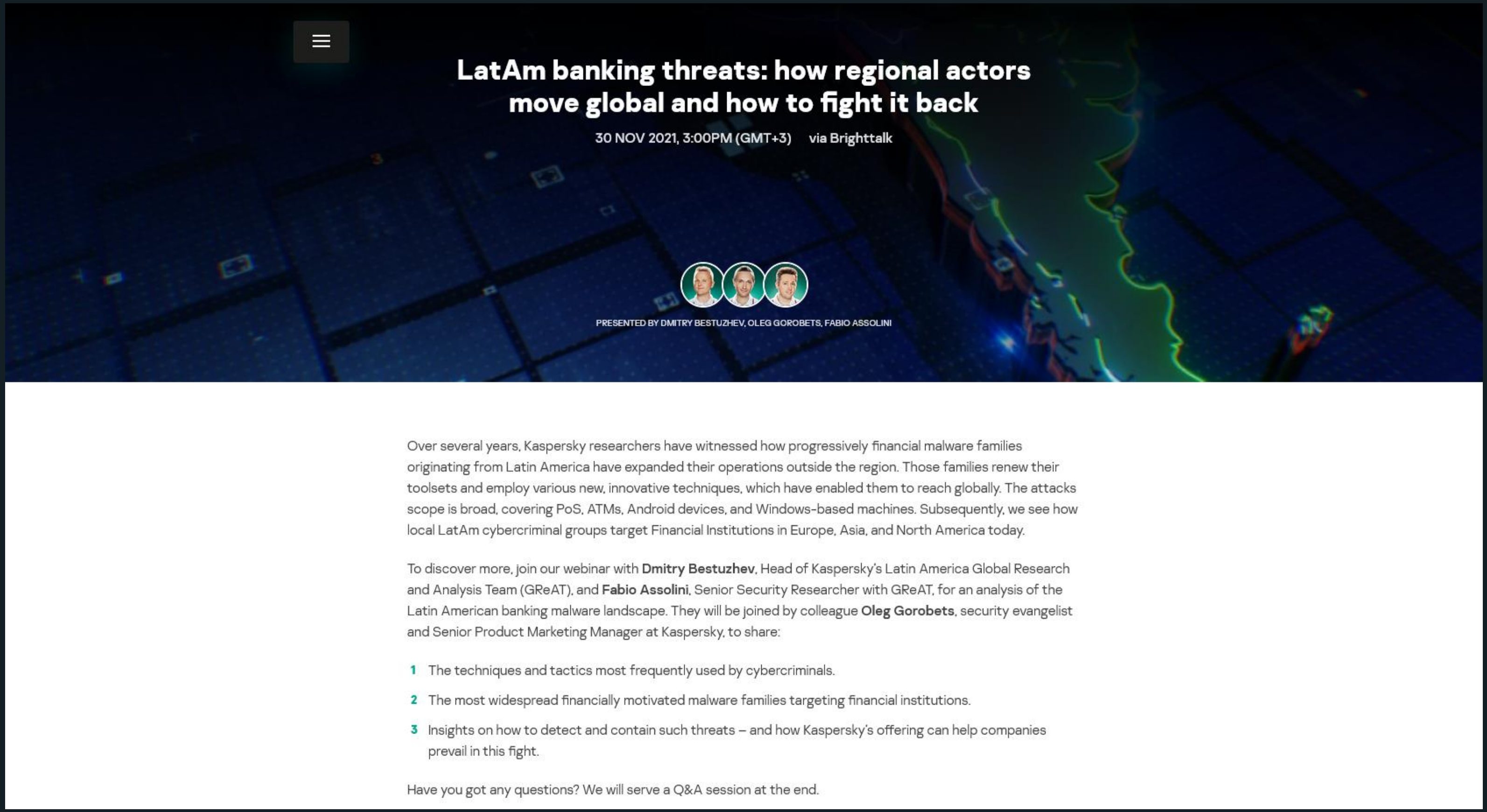
What happened?

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)

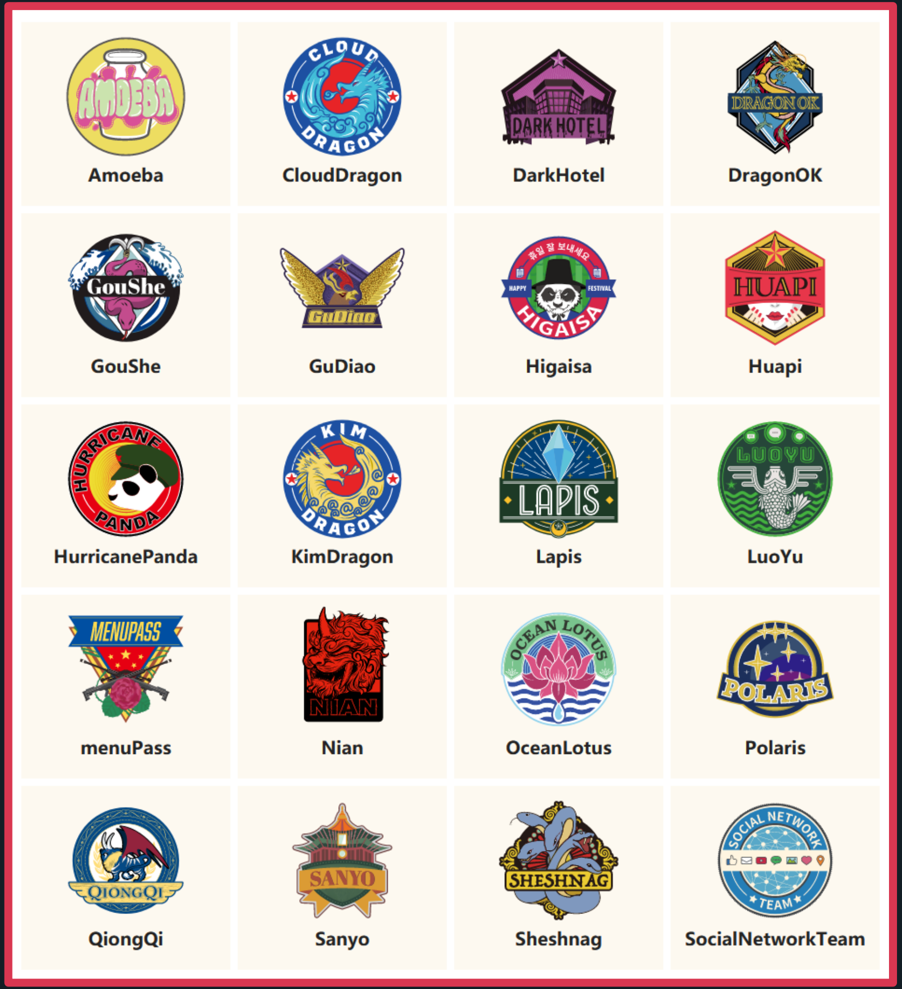
辨認攻擊者

Adversary Analysis

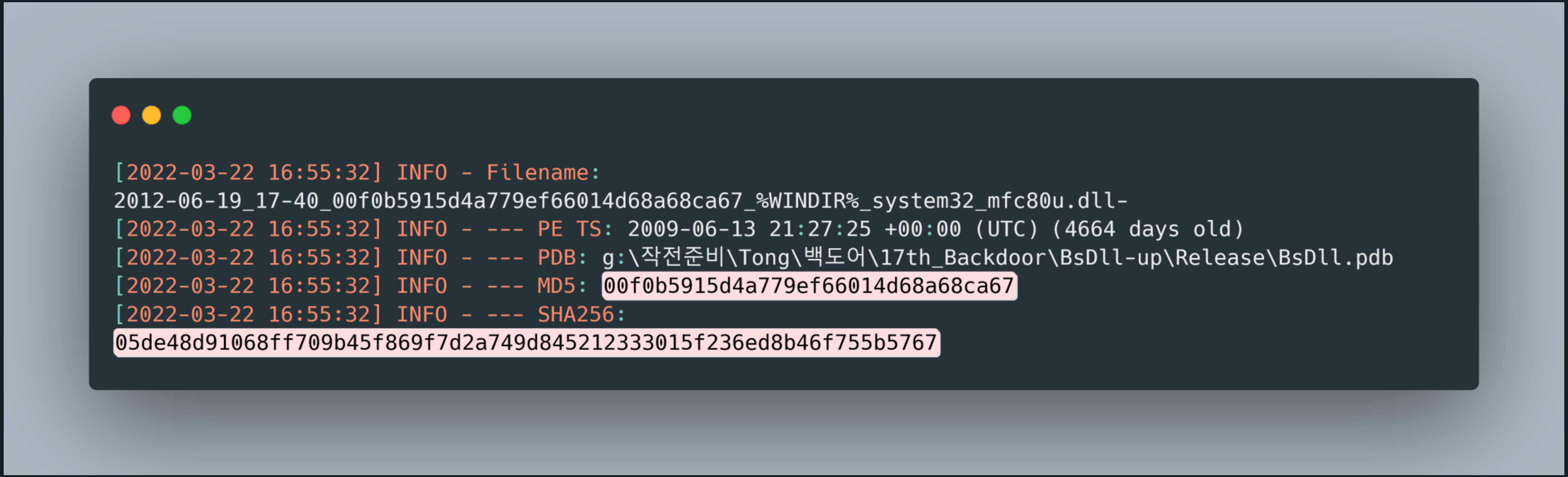
Amoeba
CloudDragon
DarkHotel
DragonOK
GouShe
GuDiao
Higaisa
Huapi
HurricanePanda
KimDragon
Lapis
LuoYu
menuPass
Nian
OceanLotus
Polaris
QiongQi
Sanyo
Sheshnag
SocialNetworkTeam

- 攻擊者/組織

Adversary Analysis



- 攻擊者/組織
    - 語言



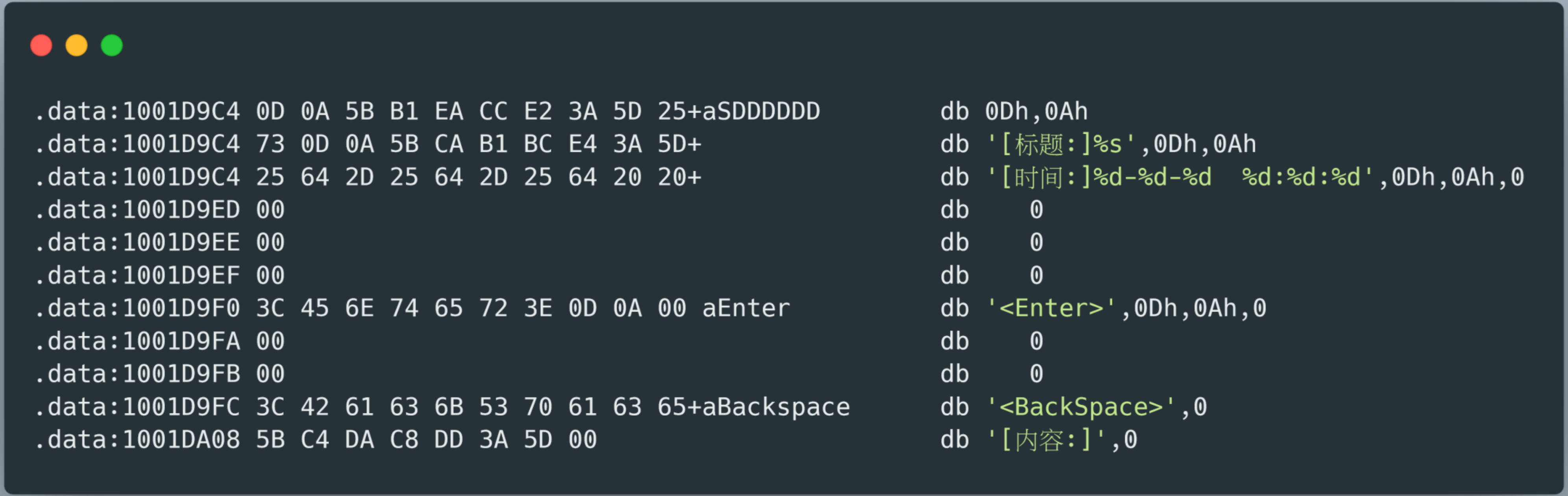
```
[2022-03-22 16:55:32] INFO - Filename:
2012-06-19_17-40_00f0b5915d4a779ef66014d68a68ca67_%WINDIR%_system32_mfc80u.dll-
[2022-03-22 16:55:32] INFO - --- PE TS: 2009-06-13 21:27:25 +00:00 (UTC) (4664 days old)
[2022-03-22 16:55:32] INFO - --- PDB: g:\작전준비\Tong\백도어\17th_Backdoor\BsDll-up\Release\BsDll.pdb
[2022-03-22 16:55:32] INFO - --- MD5: 00f0b5915d4a779ef66014d68a68ca67
[2022-03-22 16:55:32] INFO - --- SHA256:
05de48d91068ff709b45f869f7d2a749d845212333015f236ed8b46f755b5767
```

韓文 PDB 路徑 -> 母語是韓文? -> 北韓或南韓人士？

Adversary Analysis

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

- 攻擊者/組織
  - 語言
  - 工具



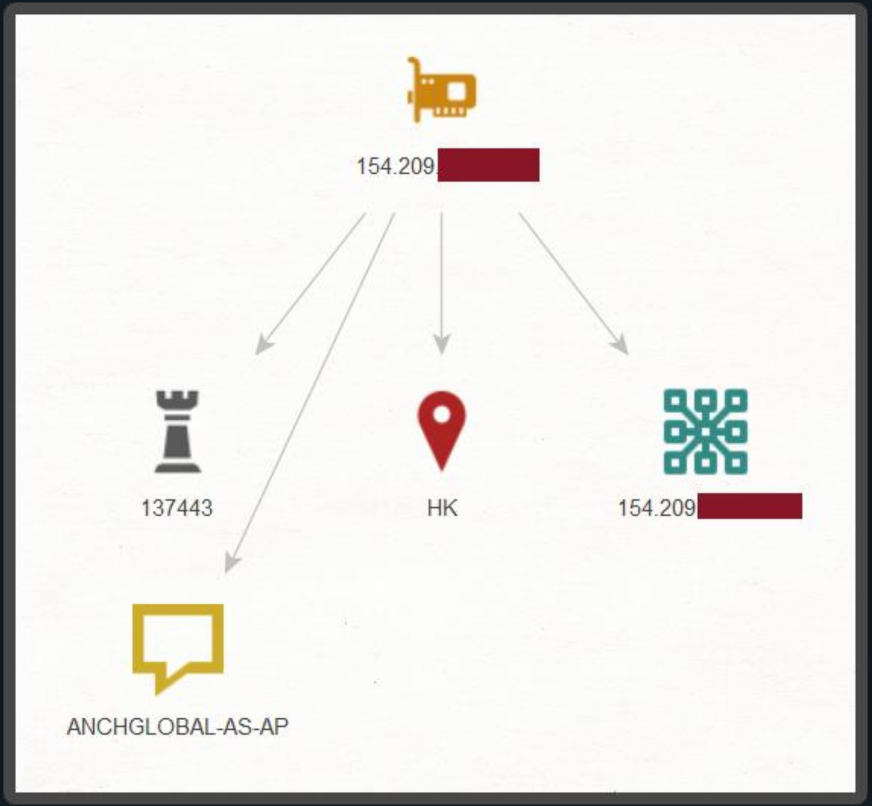
```
.data:1001D9C4 0D 0A 5B B1 EA CC E2 3A 5D 25+aSDDDDDD        db 0Dh,0Ah
.data:1001D9C4 73 0D 0A 5B CA B1 BC E4 3A 5D+                db '[标题:]%s',0Dh,0Ah
.data:1001D9C4 25 64 2D 25 64 2D 25 64 20 20+                db '[时间:]%d-%d-%d  %d:%d:%d',0Dh,0Ah,0
.data:1001D9ED 00                                            db    0
.data:1001D9EE 00                                            db    0
.data:1001D9EF 00                                            db    0
.data:1001D9F0 3C 45 6E 74 65 72 3E 0D 0A 00 aEnter          db '<Enter>',0Dh,0Ah,0
.data:1001D9FA 00                                            db    0
.data:1001D9FB 00                                            db    0
.data:1001D9FC 3C 42 61 63 6B 53 70 61 63 65+aBackspace      db '<BackSpace>',0
.data:1001DA08 5B C4 DA C8 DD 3A 5D 00                       db '[内容:]',0
```

常見 Gh0st 字串 -> 中國開發 -> 中國人?

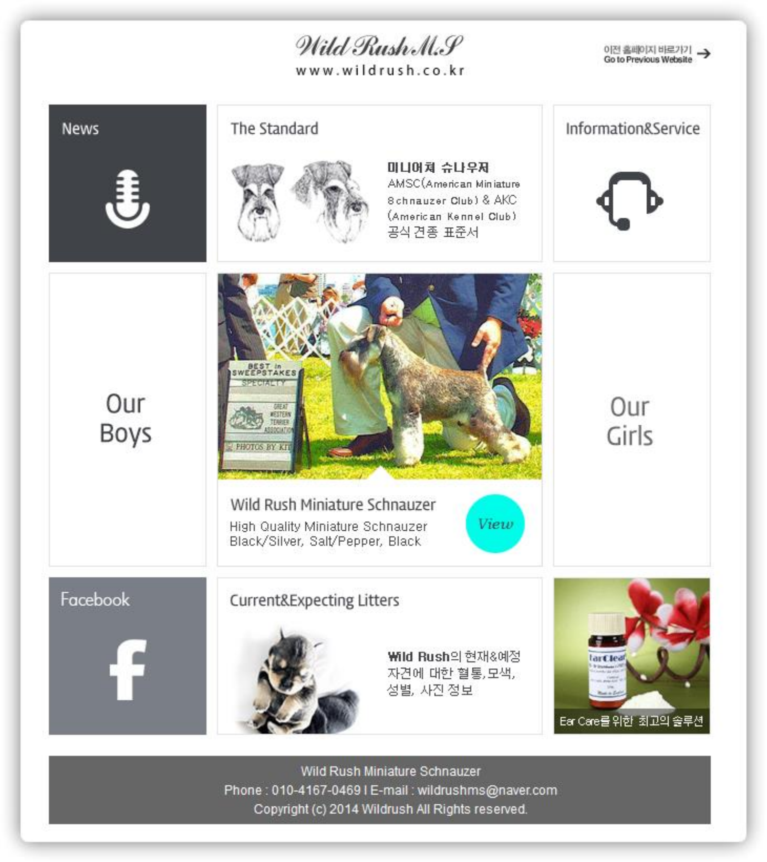
Adversary Analysis

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

- 攻擊者/組織
  - 語言
  - 工具
  - 設施



IP 服務商 -> 安暢 -> 中國 APT 慣用



Wild Rush M.S
www.wildrush.co.kr

이전 홈페이지 바로가기
Go to Previous Website →

News

The Standard

미니어쳐 슈나우저
AMSC(American Miniature Schnauzer Club) & AKC (American Kennel Club) 공식 견종 표준서

Information&Service

Our Boys

Wild Rush Miniature Schnauzer
High Quality Miniature Schnauzer
Black/Silver, Salt/Pepper, Black

View

Our Girls

Facebook

Current&Expecting Litters

Wild Rush의 현재&예정 자견에 대한 혈통,모색, 성별, 사진 정보

Ear Care를 위한 최고의 솔루션

Wild Rush Miniature Schnauzer
Phone : 010-4167-0469 I E-mail : wildrushms@naver.com
Copyright (c) 2014 Wildrush All Rights reserved.

後門連上 www.wildrush[.]co.kr/bbs/data/image/work/webproxy.php

-> 看似正常的網站及持久WHOIS record -> 推斷 compromised -> 北韓族群

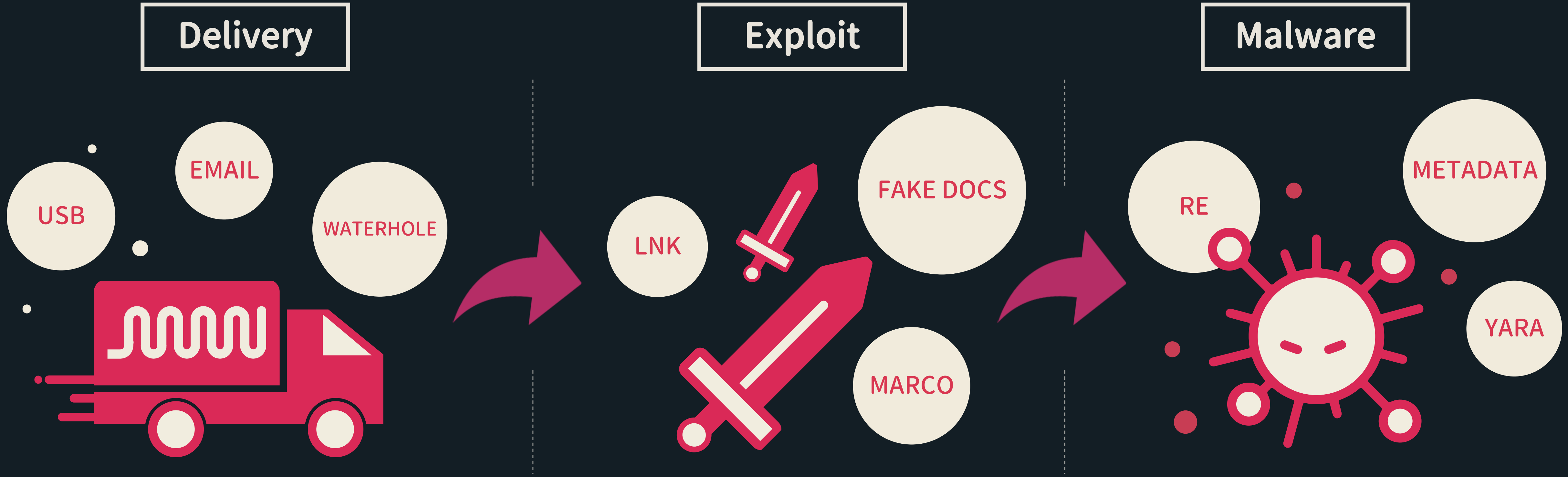
Adversary Analysis

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

- 攻擊者/組織
  - 語言
  - 工具
  - 設施
  - 手法

Capability Analysis

TEAMT5



Delivery

USB

EMAIL

WATERHOLE

Exploit

LNK

FAKE DOCS

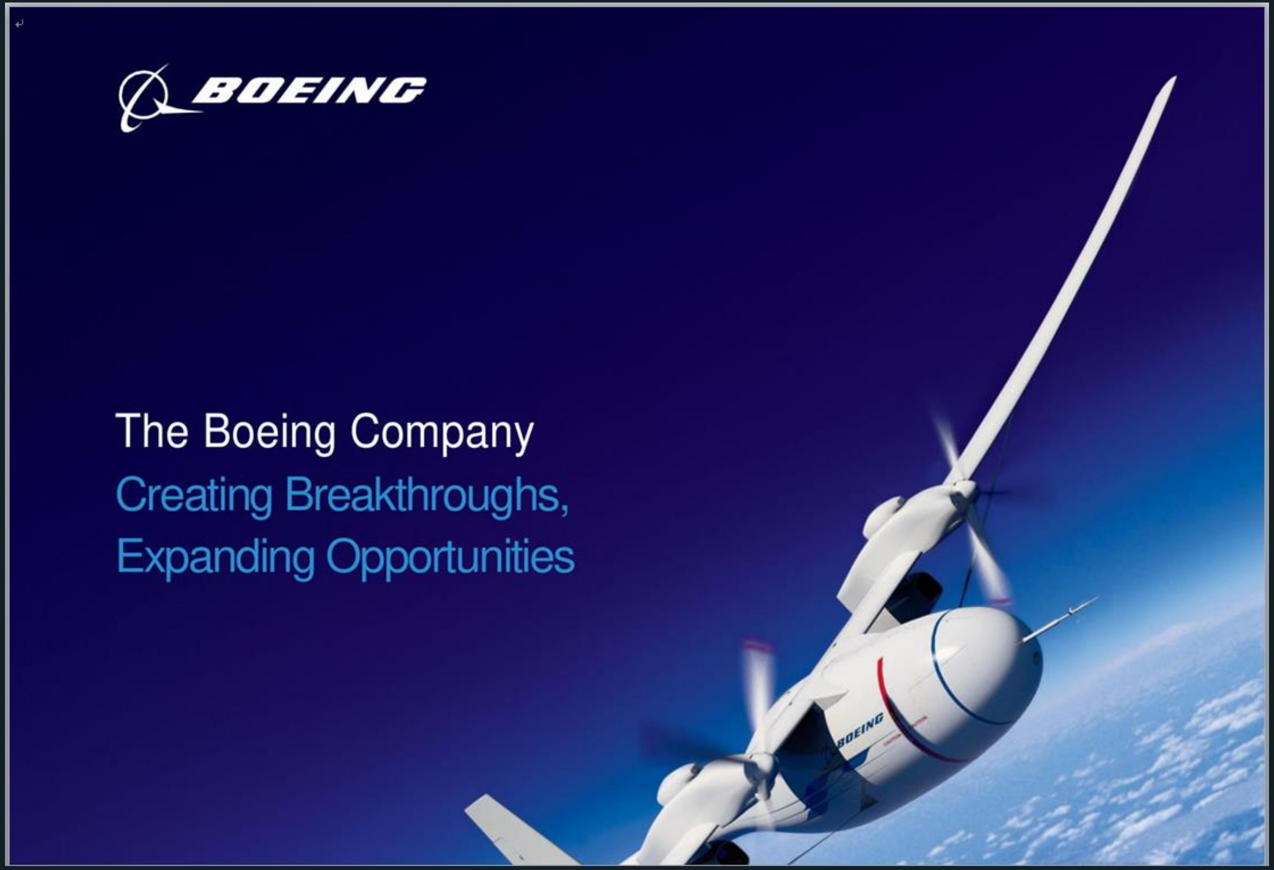
MARCO

Malware

RE

METADATA

YARA

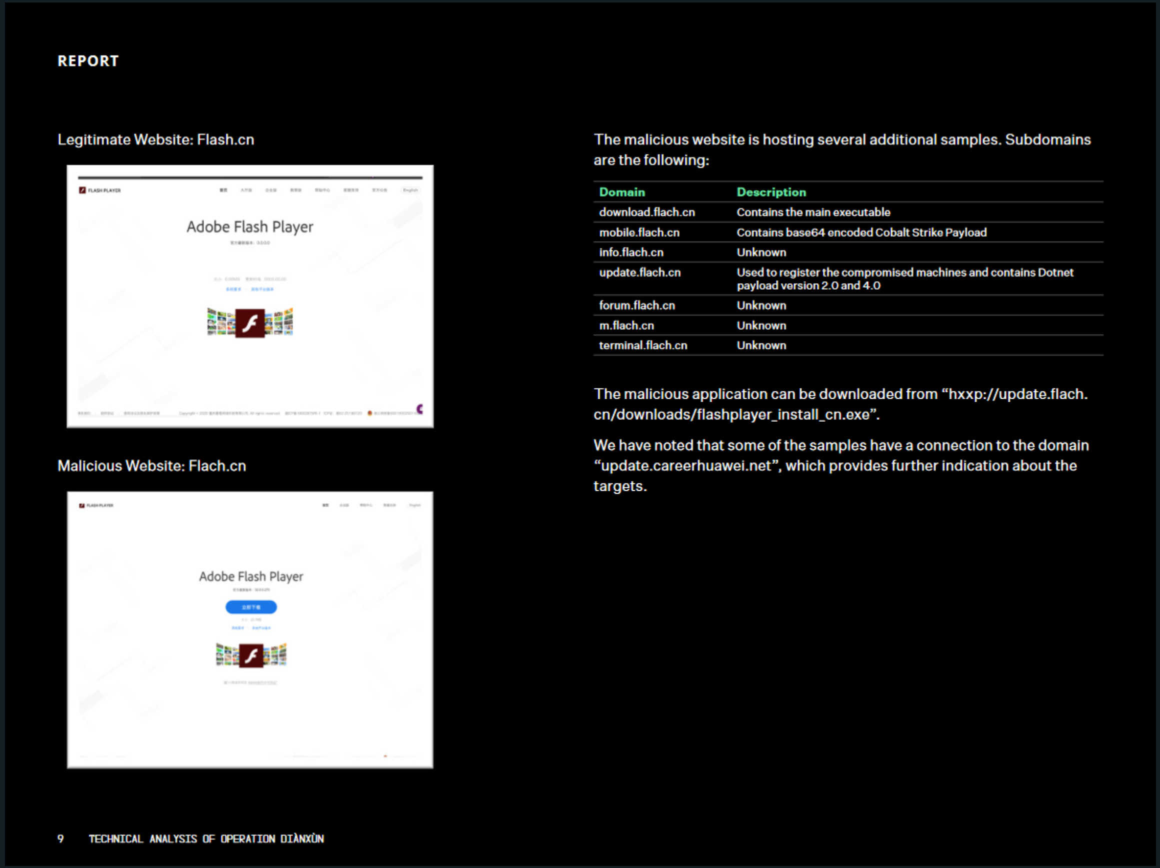


BOEING

The Boeing Company

Creating Breakthroughs,
Expanding Opportunities

Lazarus 慣用巨集文件及明確釣魚主題進行初步攻擊



Legitimate Website: Flash.cn

Malicious Website: Flach.cn

The malicious website is hosting several additional samples. Subdomains are the following:

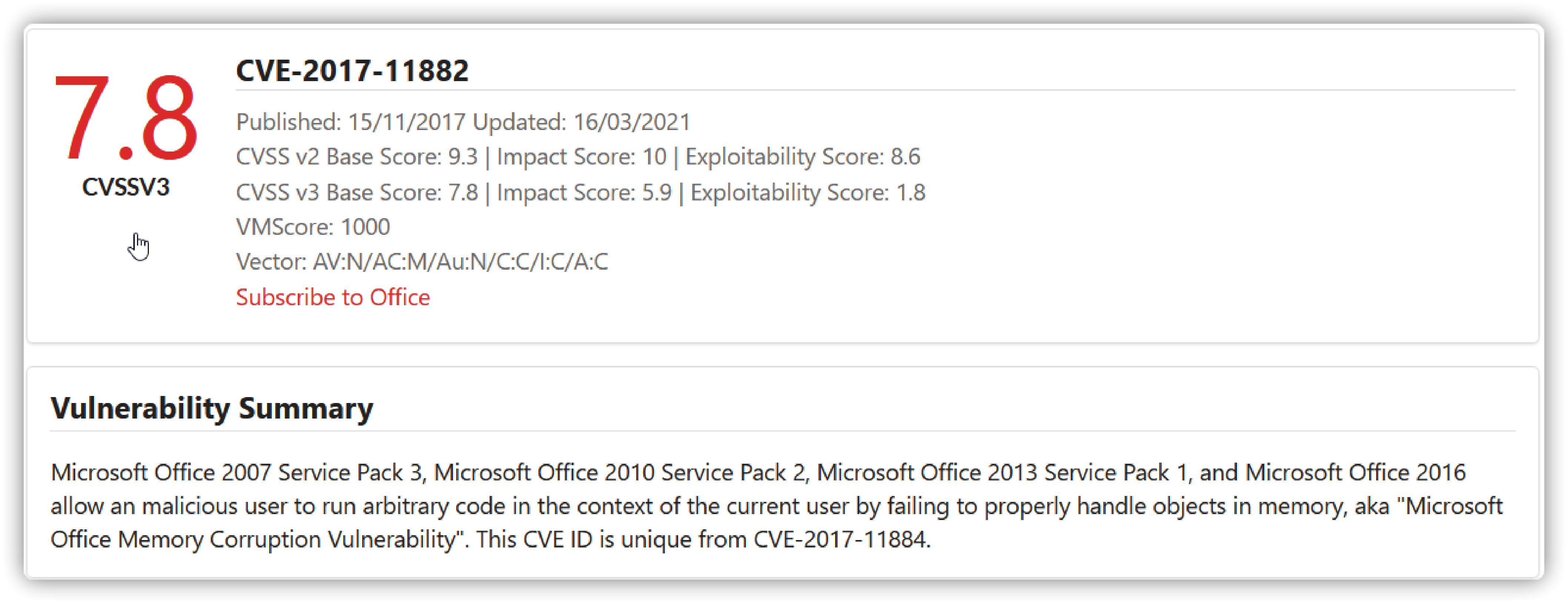
Domain	Description
download.flach.cn	Contains the main executable
mobile.flach.cn	Contains base64 encoded Cobalt Strike Payload
info.flach.cn	Unknown
update.flach.cn	Used to register the compromised machines and contains Dotnet payload version 2.0 and 4.0
forum.flach.cn	Unknown
m.flach.cn	Unknown
terminal.flach.cn	Unknown

The malicious application can be downloaded from “hxxp://update.flach.cn/downloads/flashplayer_install_cn.exe”.

We have noted that some of the samples have a connection to the domain “update.careerhuawei.net”, which provides further indication about the targets.

Polaris/Mustang Panda 一度喜歡用 Flash 當釣魚

(Roccia, T., Seret, T., Fokker J., 2021)



7.8

CVSSV3

CVE-2017-11882

Published: 15/11/2017 Updated: 16/03/2021
CVSS v2 Base Score: 9.3 | Impact Score: 10 | Exploitability Score: 8.6
CVSS v3 Base Score: 7.8 | Impact Score: 5.9 | Exploitability Score: 1.8
VMScore: 1000
Vector: AV:N/AC:M/Au:N/C:C/I:C/A:C
Subscribe to Office

Vulnerability Summary

Microsoft Office 2007 Service Pack 3, Microsoft Office 2010 Service Pack 2, Microsoft Office 2013 Service Pack 1, and Microsoft Office 2016 allow an malicious user to run arbitrary code in the context of the current user by failing to properly handle objects in memory, aka "Microsoft Office Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11884.

印度 Donot 組織慣用 CVE-2017-11882

Adversary Analysis

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

- 攻擊者/組織
  - 語言
  - 工具
  - 設施
  - 手法
- 企圖、為何而打？
- 有沒有可能聯手？
  - 分享的工具
  - 分享的C2

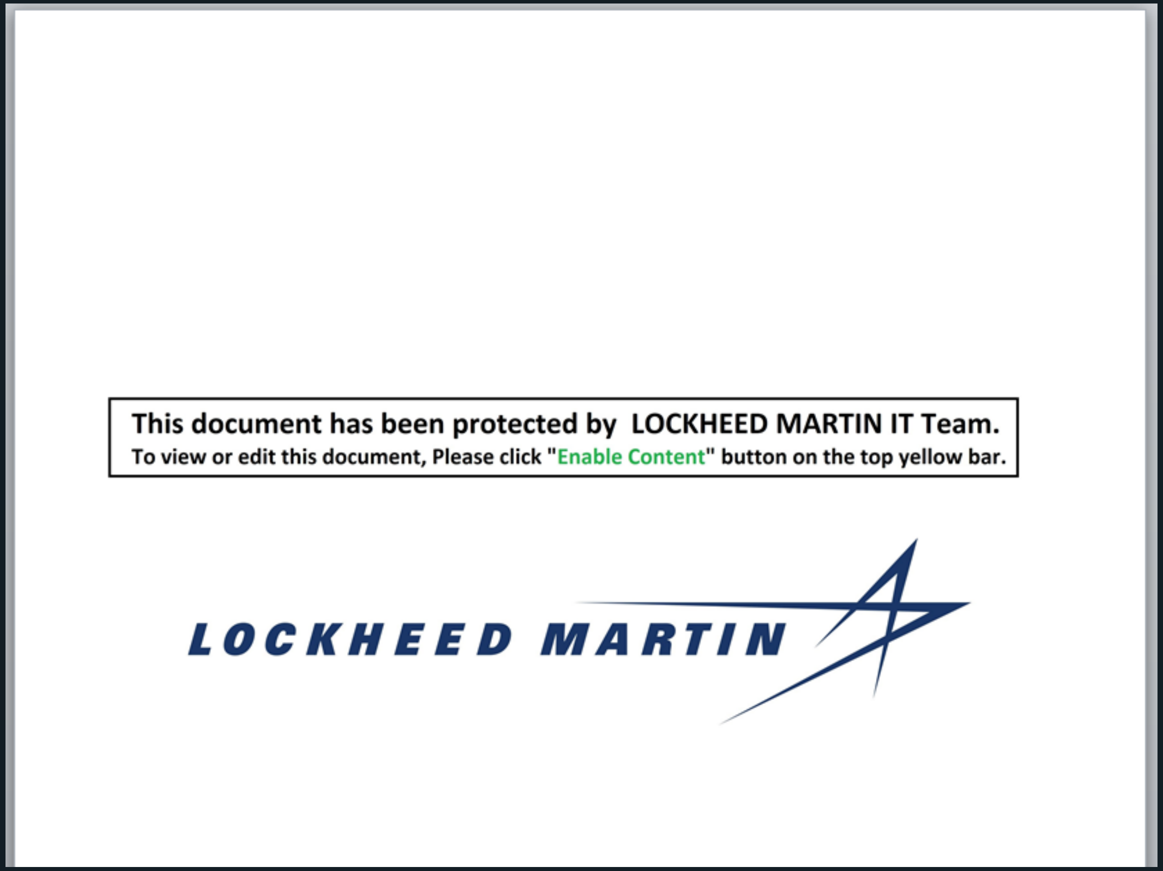
辨認受害者

Identifying victims

- 語言 (Language) / 地區 (Region)
  - 誘餌文件 Decoy document
  - Email
- 所屬業界 (Industry)
  - 誘餌文件 Decoy document
- 目標 (Targeted data)

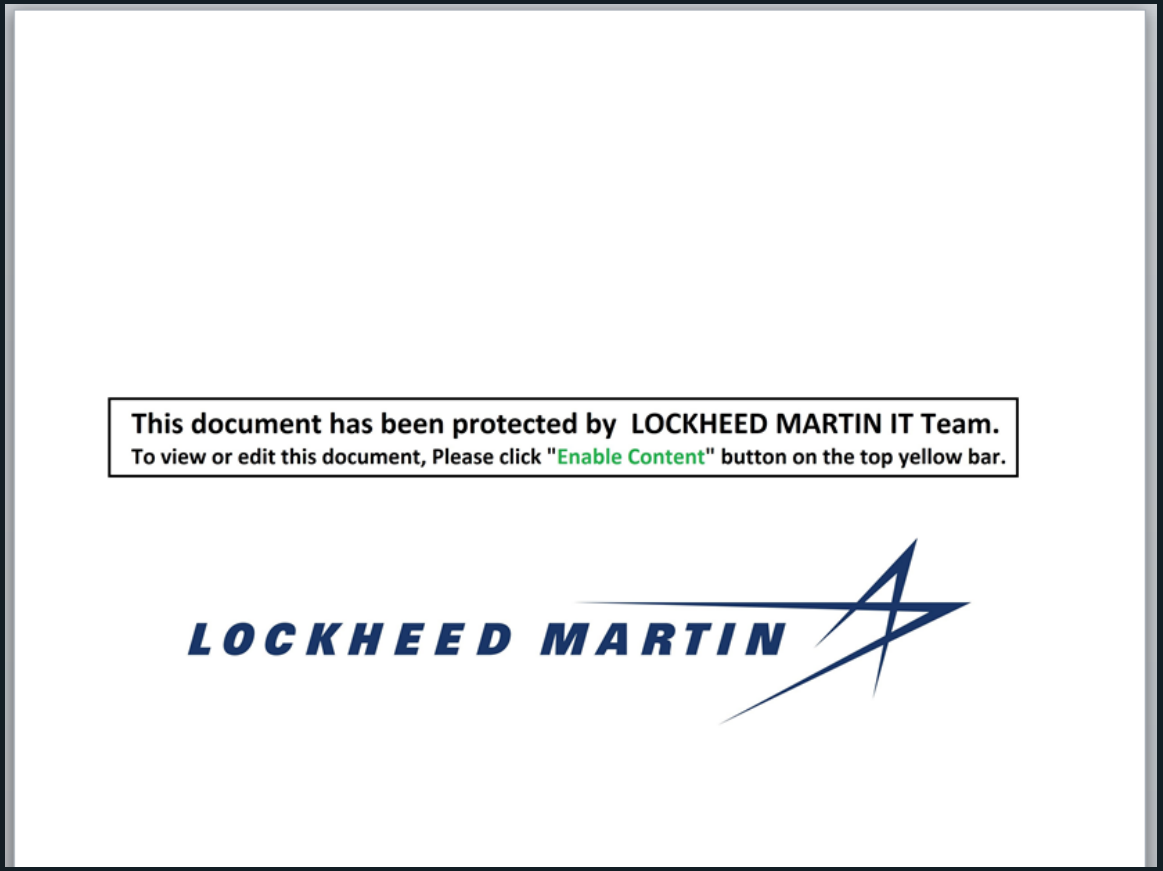
Identifying victims

- 語言 (Language) / 地區 (Region)
  - **誘餌文件 Decoy document**
  - Email
- 所屬業界 (Industry)
  - **誘餌文件 Decoy document**
- 目標 (Targeted data)



This document has been protected by LOCKHEED MARTIN IT Team.
To view or edit this document, Please click "Enable Content" button on the top yellow bar.

Lockheed Martin -> 美國國防/飛航產業



This document has been protected by LOCKHEED MARTIN IT Team.
To view or edit this document, Please click "Enable Content" button on the top yellow bar.

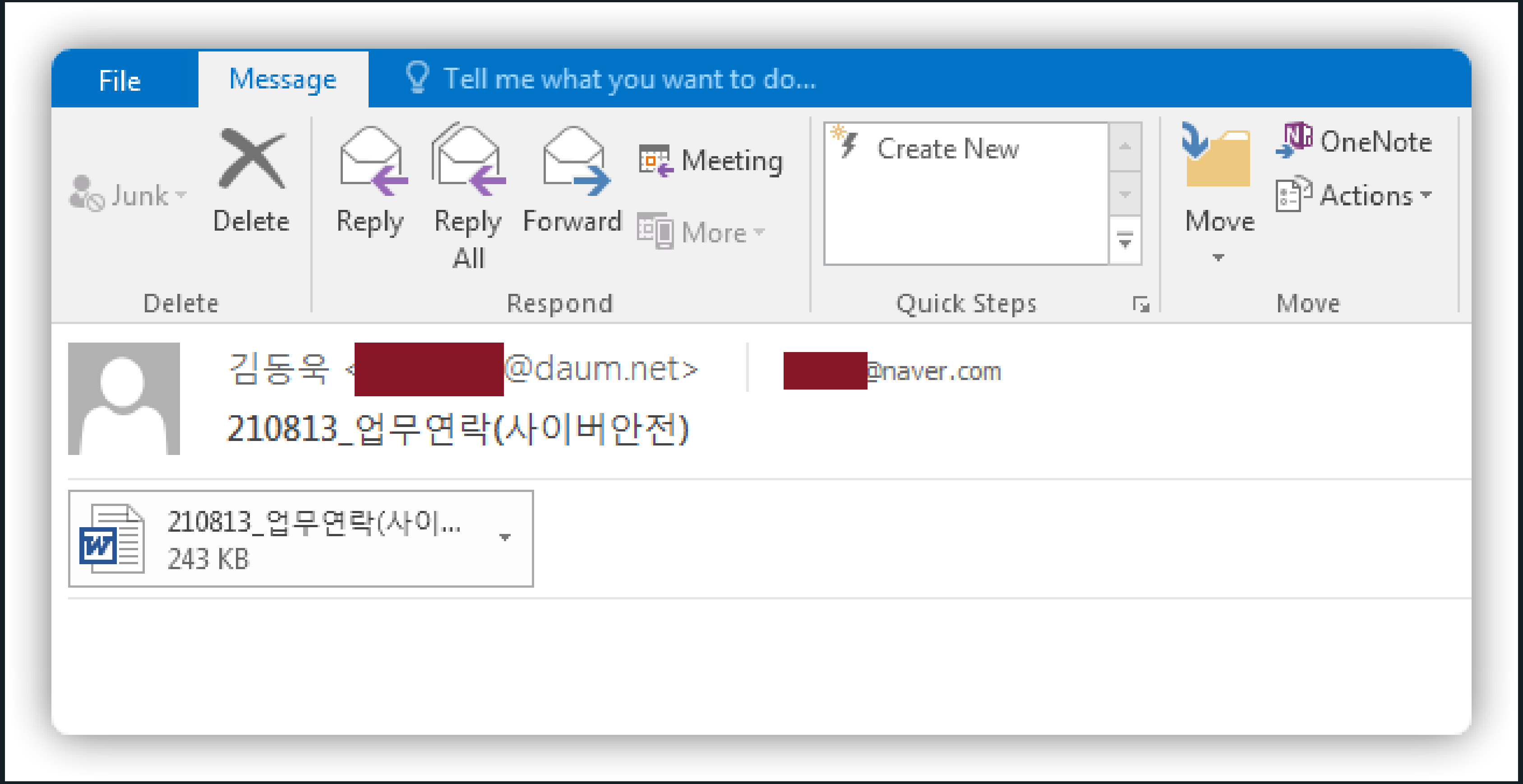
Lockheed Martin -> 美國國防/飛航產業 -> 求職者或公司本身?

Identifying victims

- 語言 (Language) / 地區 (Region)
  - 誘餌文件 Decoy document
  - Email
- 所屬業界 (Industry)
  - 誘餌文件 Decoy document
- 目標 (Targeted data)

Identifying victims

- 語言 (Language) / 地區 (Region)
  - 誘餌文件 Decoy document
  - **Email**
- 所屬業界 (Industry)
  - 誘餌文件 Decoy document
- 目標 (Targeted data)



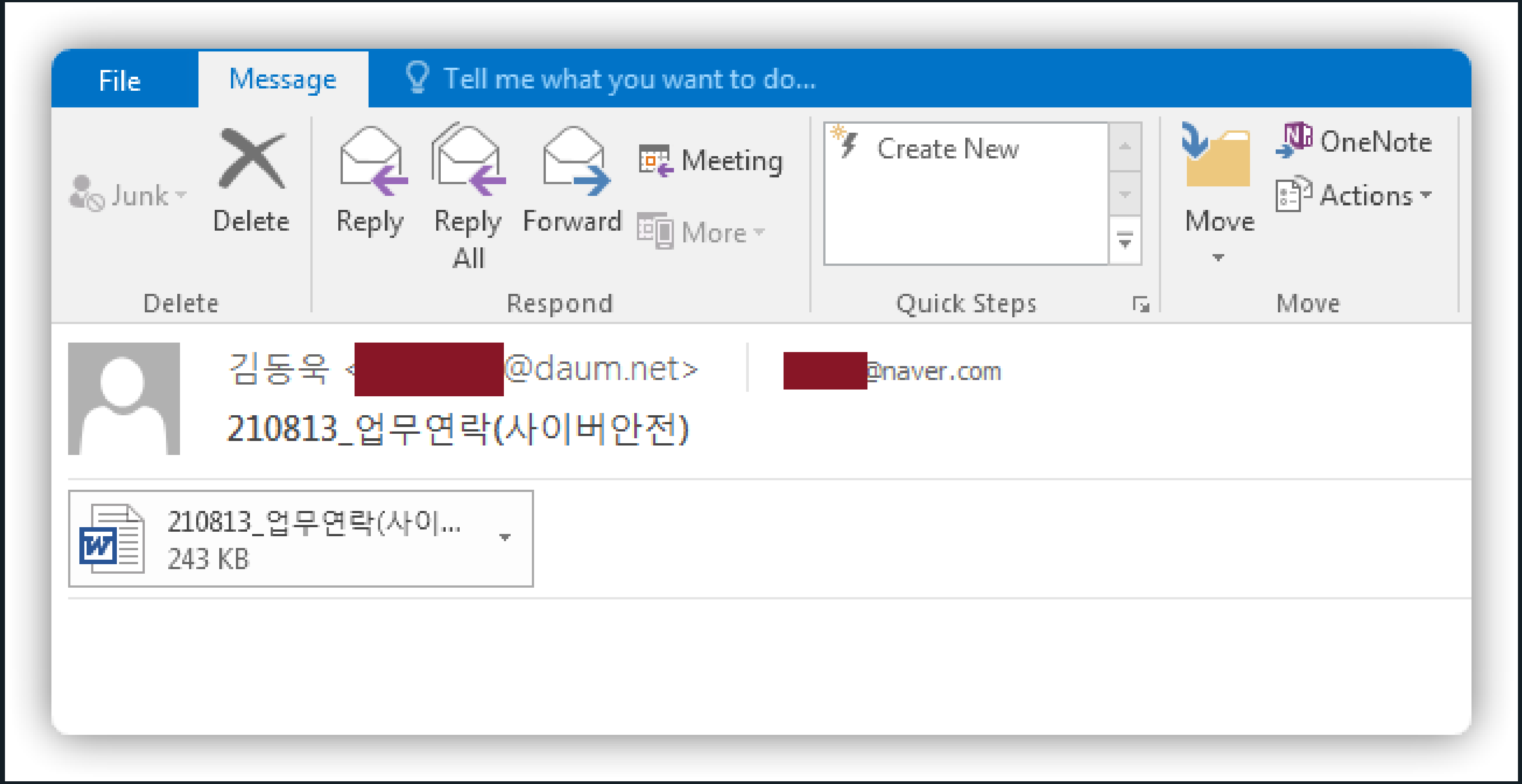
김동욱 <[redacted]@daum.net>

[redacted]@naver.com

210813_업무연락(사이버안전)

210813_업무연락(사이...
243 KB

韓文Email



김동욱 <[redacted]@daum.net> [redacted]@naver.com

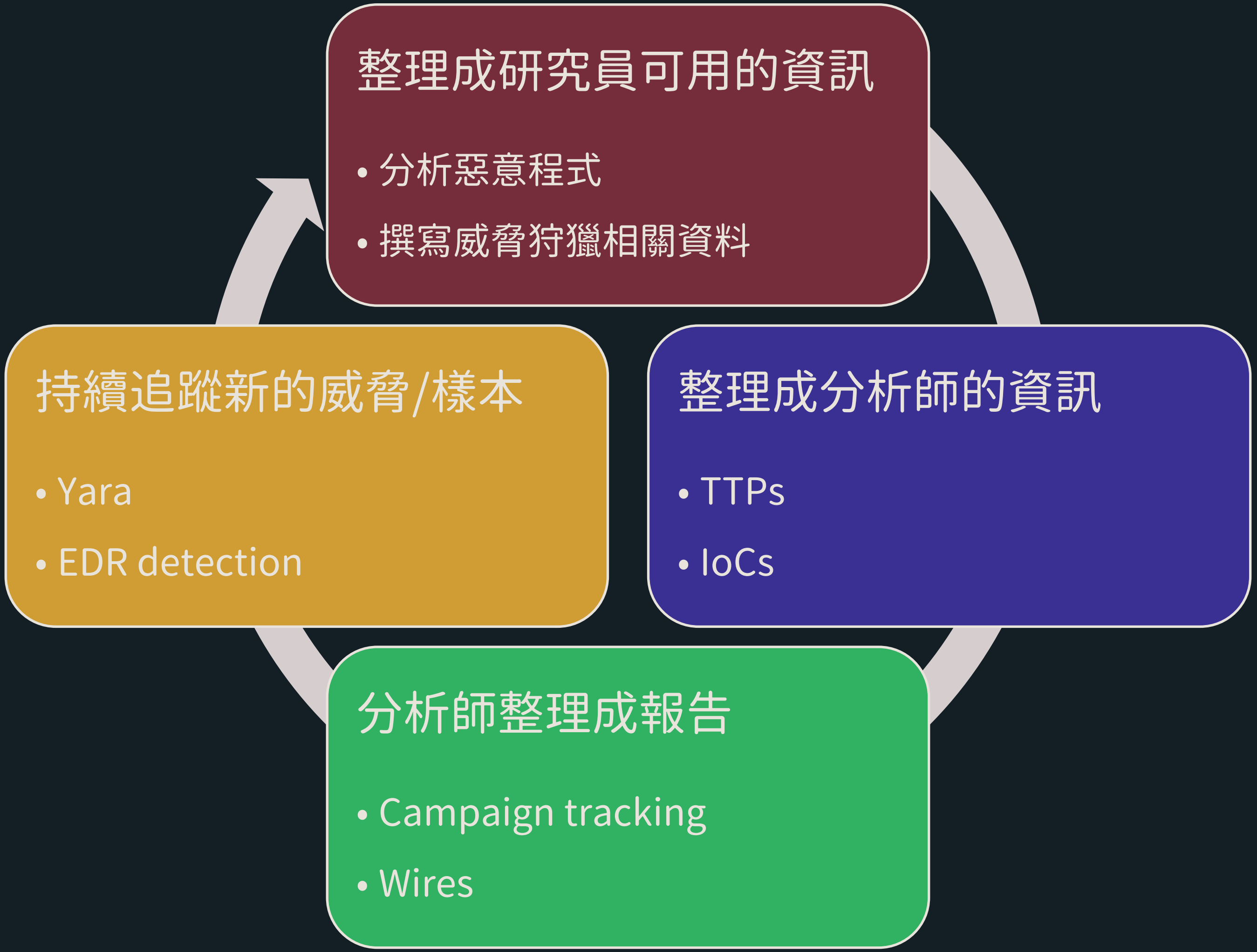
210813_업무연락(사이버안전)

210813_업무연락(사이...
243 KB

韓文Email + 收件者為某報導產業 -> 韓國媒體

情卩

目的



整理成研究員可用的資訊

- 分析惡意程式
- 撰寫威脅狩獵相關資料

整理成分析師的資訊

- TTPs
- IoCs

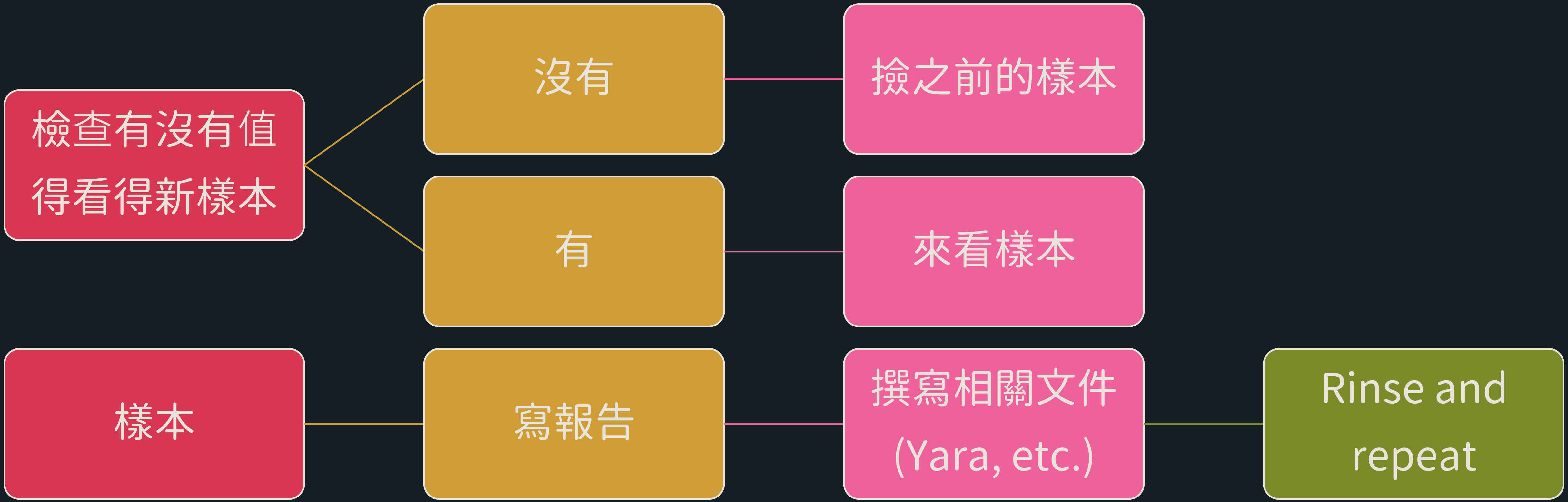
分析師整理成報告

- Campaign tracking
- Wires

持續追蹤新的威脅/樣本

- Yara
- EDR detection

所以每天的行程



檢查有沒有值得看得新樣本

沒有

撿之前的樣本

有

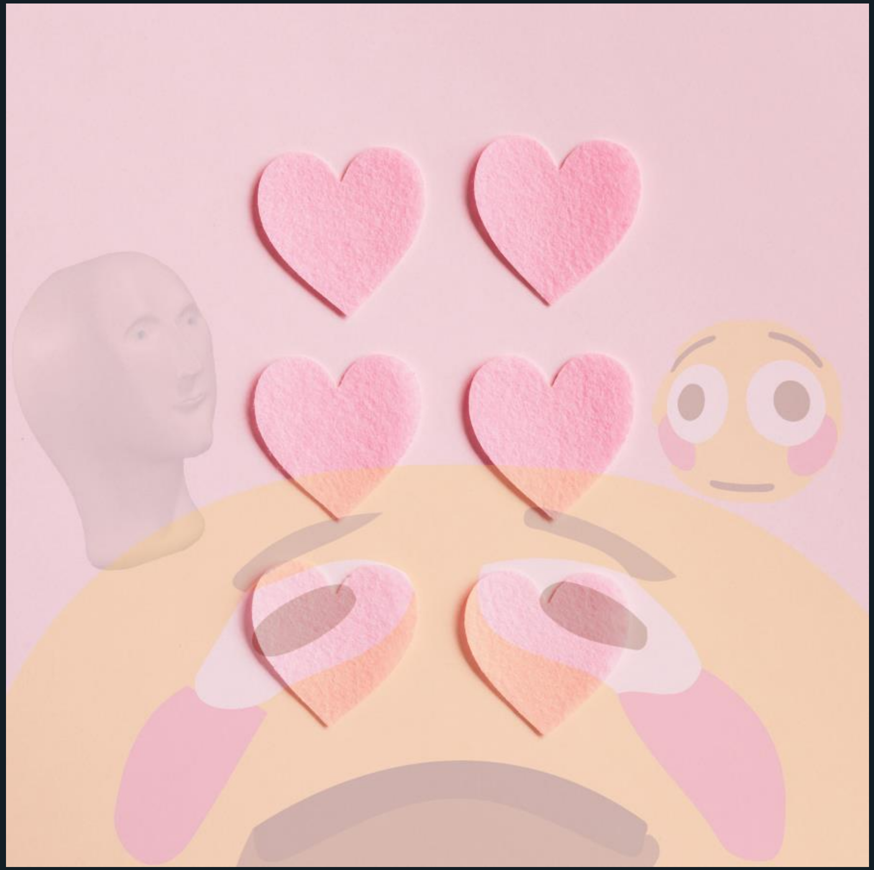
來看樣本

樣本

寫報告

撰寫相關文件 (Yara, etc.)

Rinse and repeat



熱誠

知名網路間諜組織

GouShe

- 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

- 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

TEAMT5

- 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.

THANK YOU!

@AzakaSekai_

✉ still@teamt5.org

TEAMT5

Persistent Cyber Threat Hunters