CYBERSEC 2025
臺灣資安大會
4/15-4/17
臺北南港展覽二館

Offensive 〉
〈 Security
Forum

我打你應該，不打你悲哀

TEAM
CYBERSECURITY

PD Lee
自由資安顧問

Whoami

- Hitcon speaker
- APT Seminar Keynote speaker
- ModernWeb speaker
- Cybersec 2024 speaker

Agenda

- 駭客想得和你不一樣
- 攻擊是最好的防守？

要瞭解駭客思維,才能更有效對抗駭客

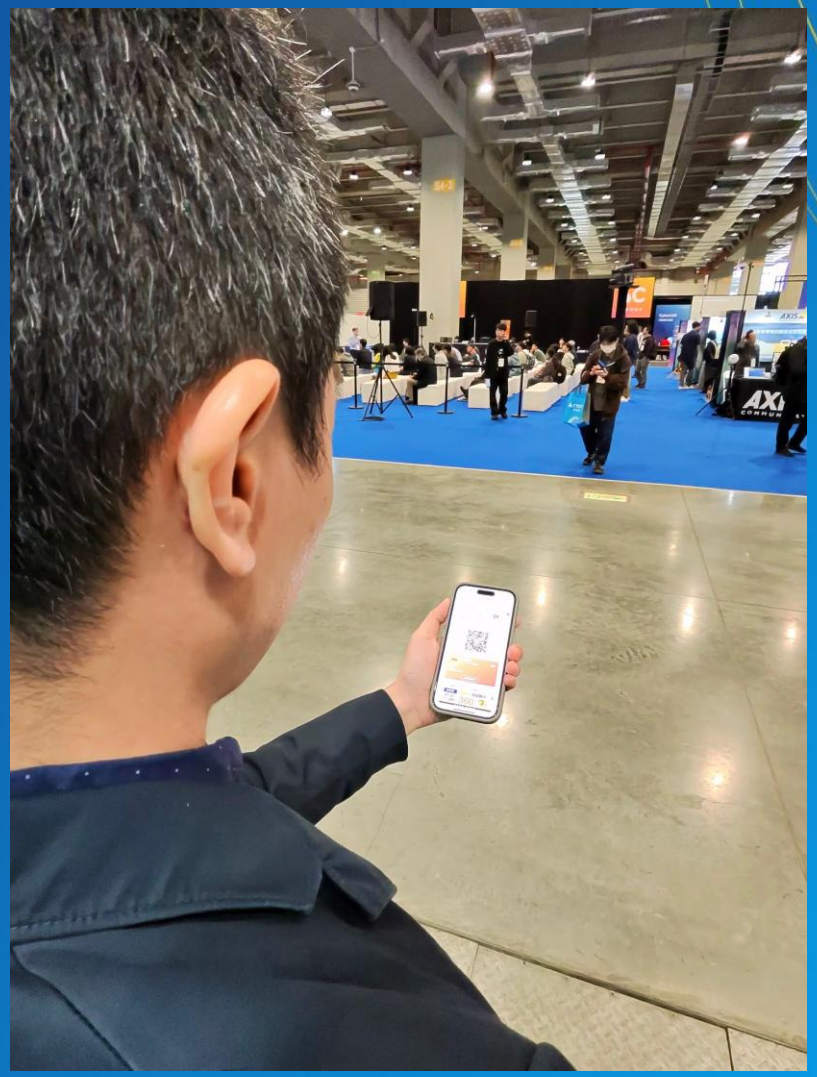
駭客黑，IT要更黑!

了解駭客思路的好處

- 跟上駭客的腳步
  - 法規跟標準必須經過嚴謹的審核機制
  - 因此往往落後攻擊實務好幾年
  - 了解駭客思路可避免拿明朝的劍斬清朝的官
- 避免做出hacker friendly的設計

跟上駭客的腳步

- 新技術可應用在
  - 增進工作效率
  - 增進駭客攻擊效率
- 以智慧型眼鏡為例
  - 側錄的延伸利用
  - 肩窺再進化
  - 防禦規則也必須改變



常見Hacker friendly的設計

- 邏輯漏洞
- 短網址

邏輯漏洞範例

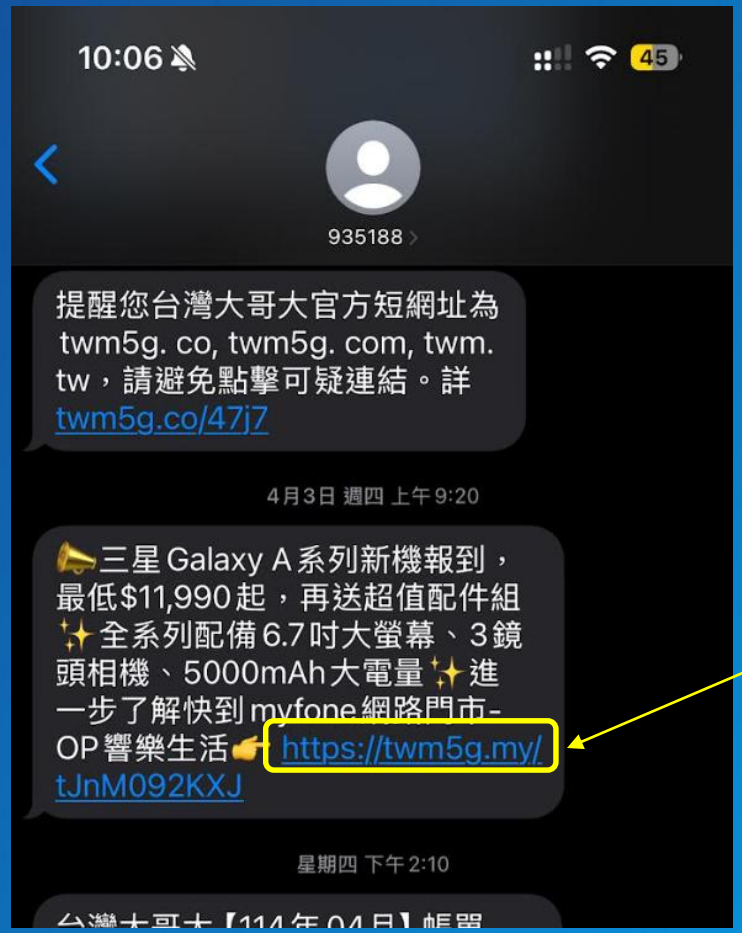

大樹林滯洪池「水の秘密
管理者登入
民眾預約登入
14 林*瑾 268 1
15 羅*年 535 1
16 李*明 023 1
17 陳*法 163 1
18 羅*亮 875 1
19 陳*惠 545 1
20 許* 291 1
21 黃*誠 763 1
22 張*婷 133 1
23 黃*庭 001 1

短網址

- 問題點：
  - 官網都記不住了
  - 還記這麼多域名？

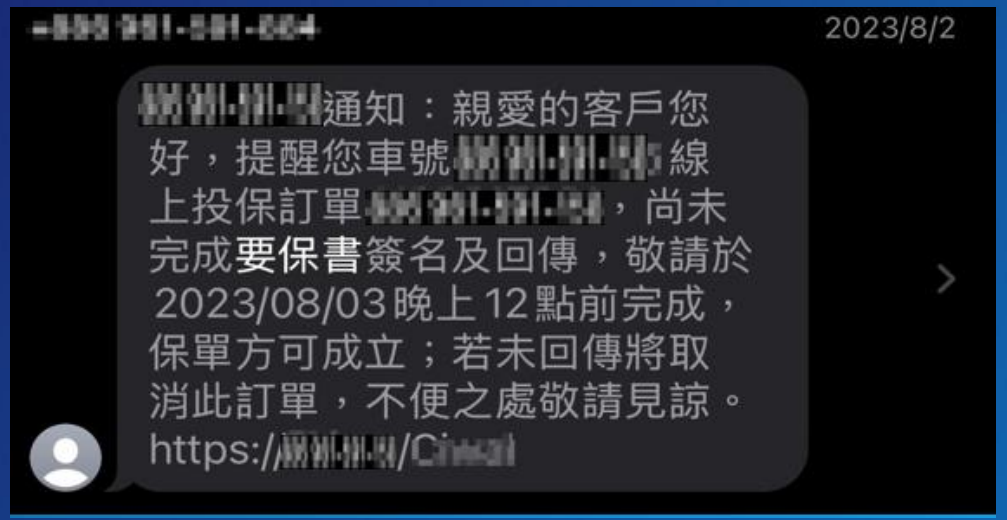
下列哪個是前述企業的官方短網址域名？

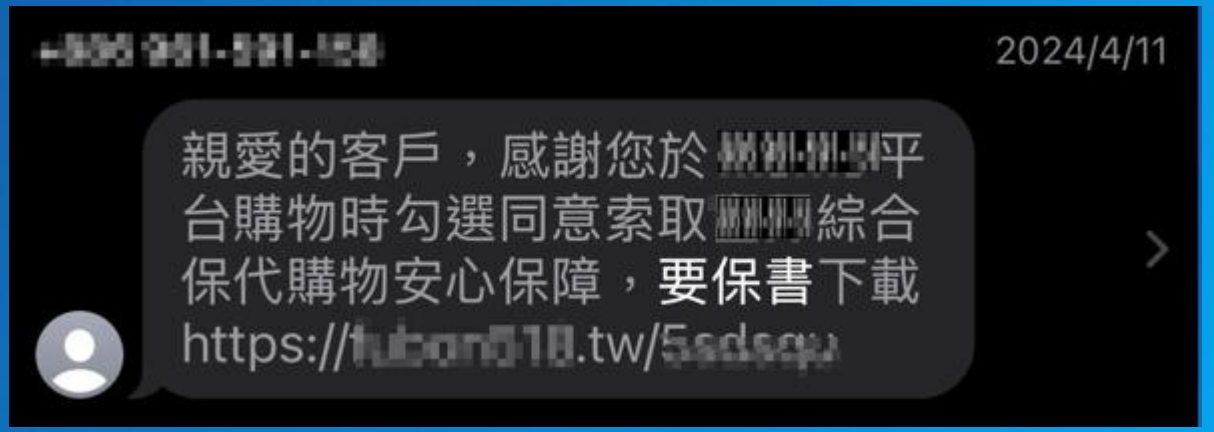
- twm5g.com.tw
- twm5g.net
- twm5g.tw
- twm.com
- twm.co
- twm.com.tw



那這個是?

還有哪些利用方式？

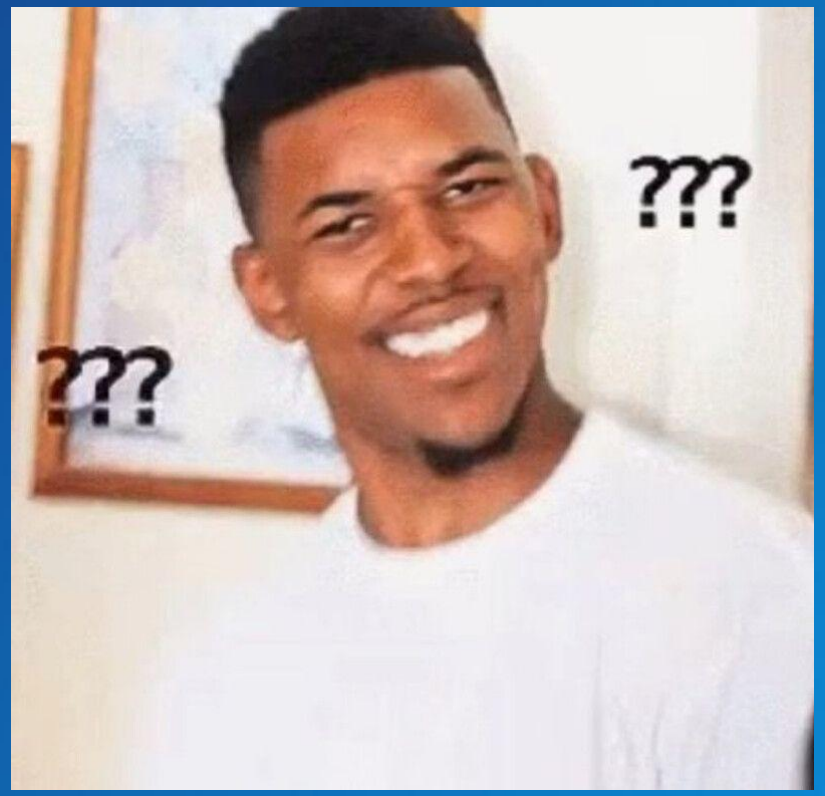

2023/8/2
通知：親愛的客戶您好，提醒您車號 線上投保訂單，尚未完成要保書簽名及回傳，敬請於2023/08/03晚上12點前完成，保單方可成立；若未回傳將取消此訂單，不便之處敬請見諒。
https://


2024/4/11
親愛的客戶，感謝您於 平台購物時勾選同意索取 綜合保代購物安心保障，要保書下載
https://

攻擊方式

- 針對企業專屬短網址路徑Brute force
  - 找出可下載的文件
  - 也常找到會員禮或兌換券等
- 離線用特定格式密碼針對下載的文件再brute force一次
  - Ex：身份證字號

為了不容易被猜測路徑所以加了一堆參數值和UUID等來防止
（避免被預測）
再為了容易存取又把上述路徑存成短網址???
（再讓它變得容易預測）

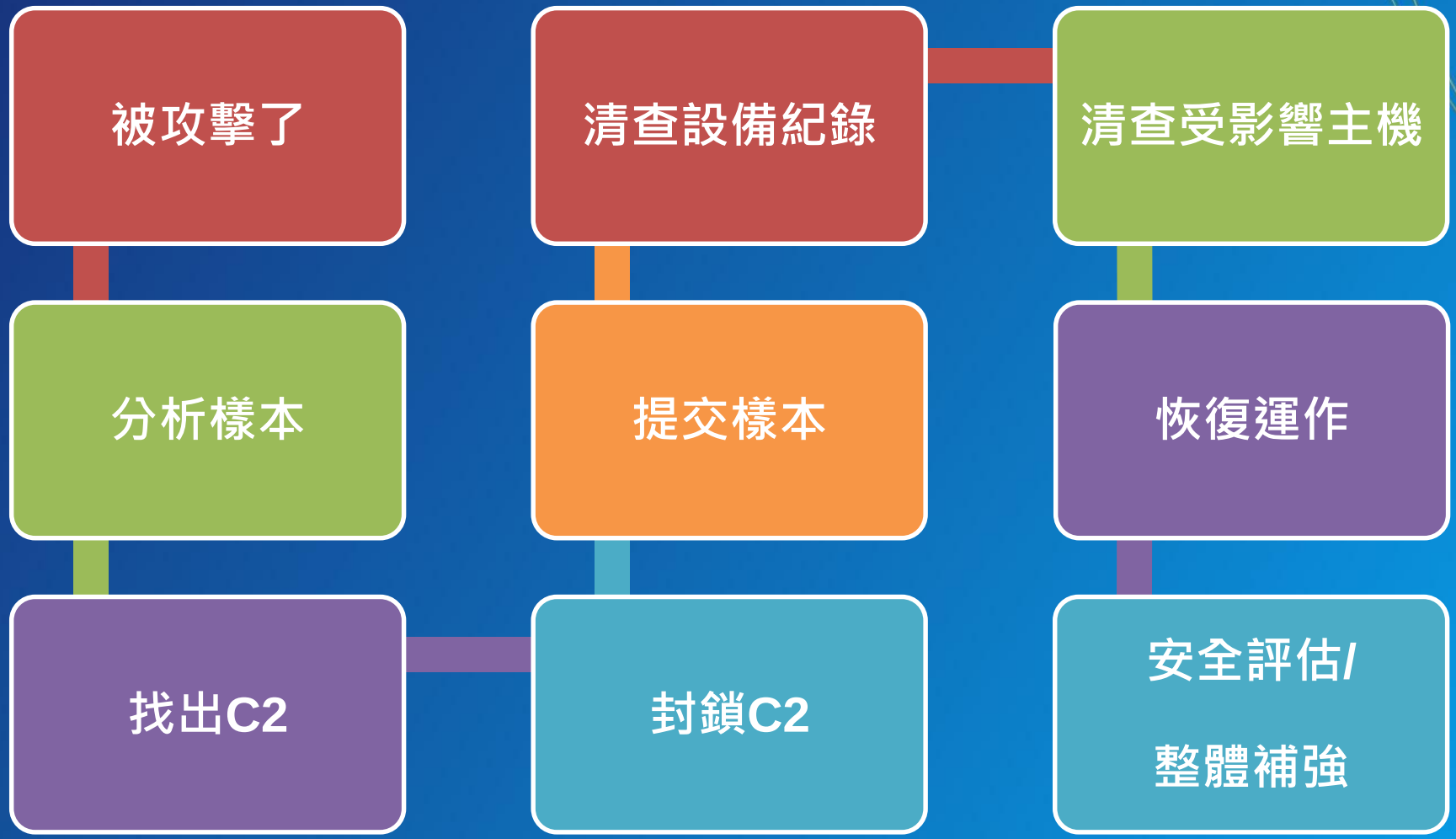


Agenda

- 駭客想得和你不一樣
- 攻擊是最好的防守？

Don't try it in ur office

傳統資安事件處理流程



逆襲中繼站

被攻擊了

分析樣本

找出C2

接管兵器庫

接管C2

打回去

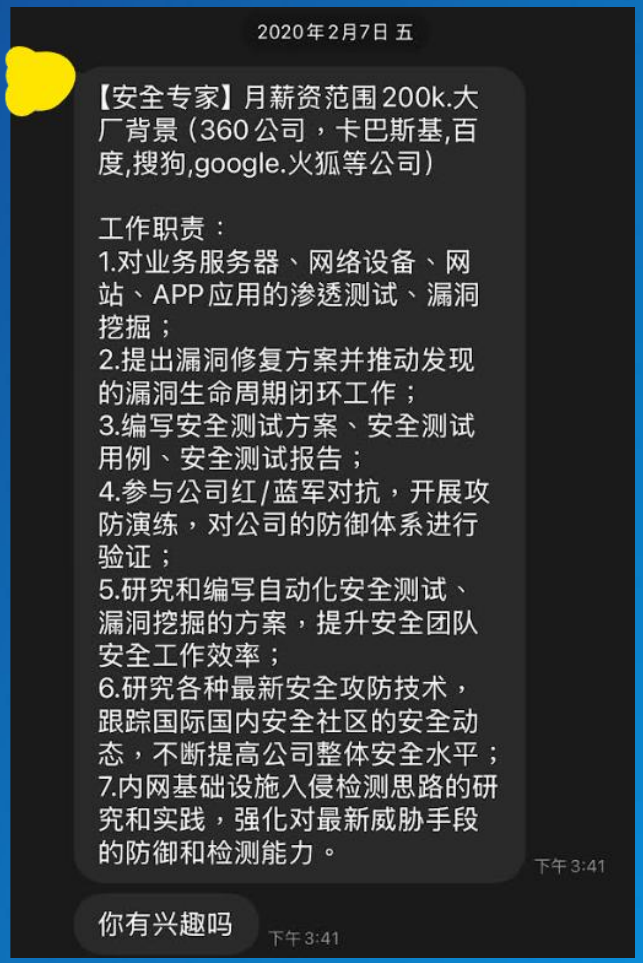
分析每日
上架新品

超前佈署

(抓內鬼)

部分產業(非政府網軍)黑產分工

- Hacker(貴&稀缺)
  - 蒐集&挖掘各種Exploit
  - 客製化後門
- OP(CP值高&易取代)
  - 建置&維護C2環境
  - 發動社交工程等攻擊
  - 或聽話的自己人



反擊中繼站

- 已知漏洞或不當配置
- 未公開漏洞
- 偽造被入侵環境進行反監控
- 社交工程

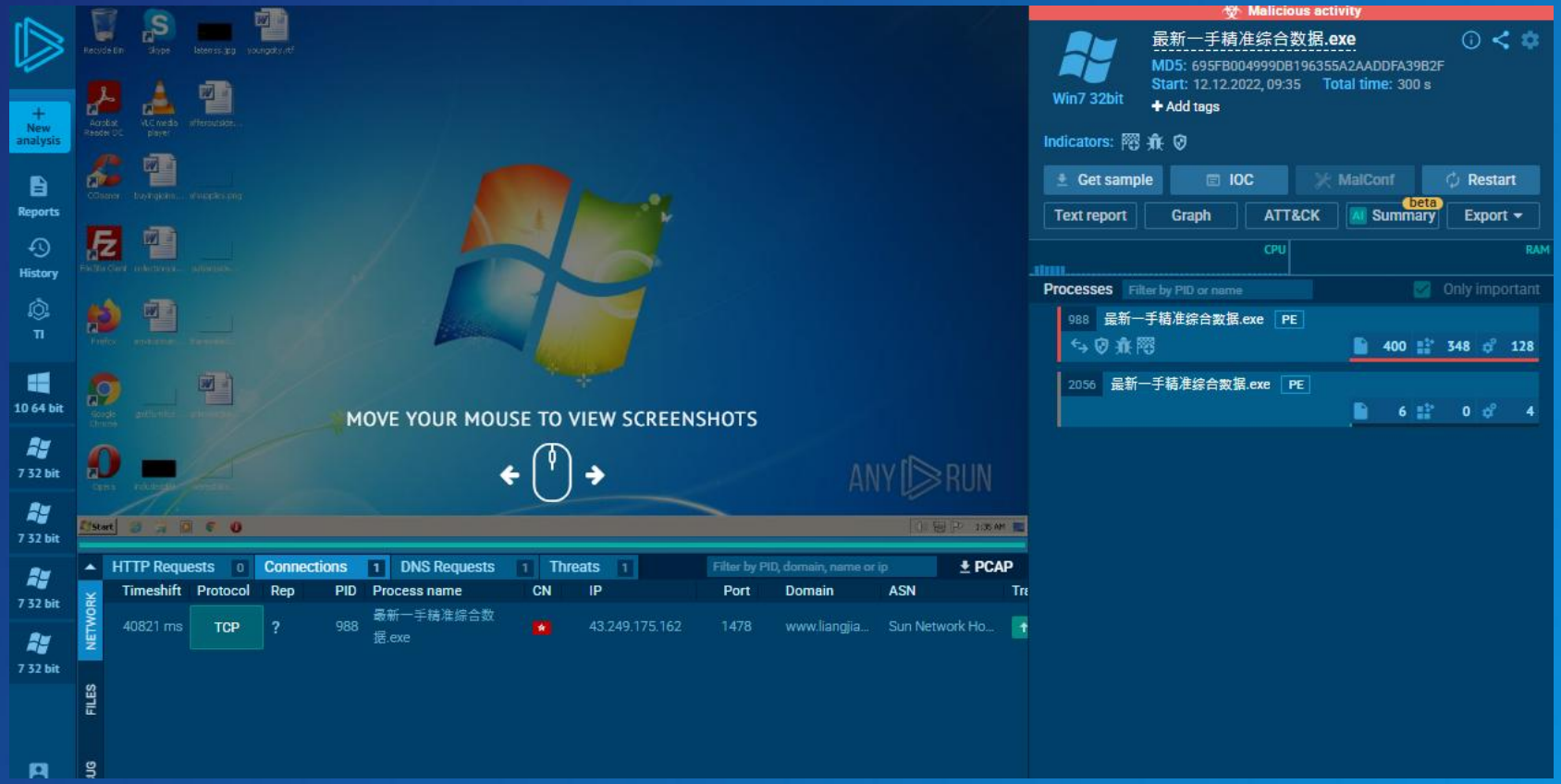
已知漏洞或不當配置

- 分析樣本
  - 找出中繼站
- 已知漏洞
- 常見不當配置
  - 對岸技術教學網站
    - 更改下載源
    - 定製版系統
    - 水坑式攻擊
  - gitleak

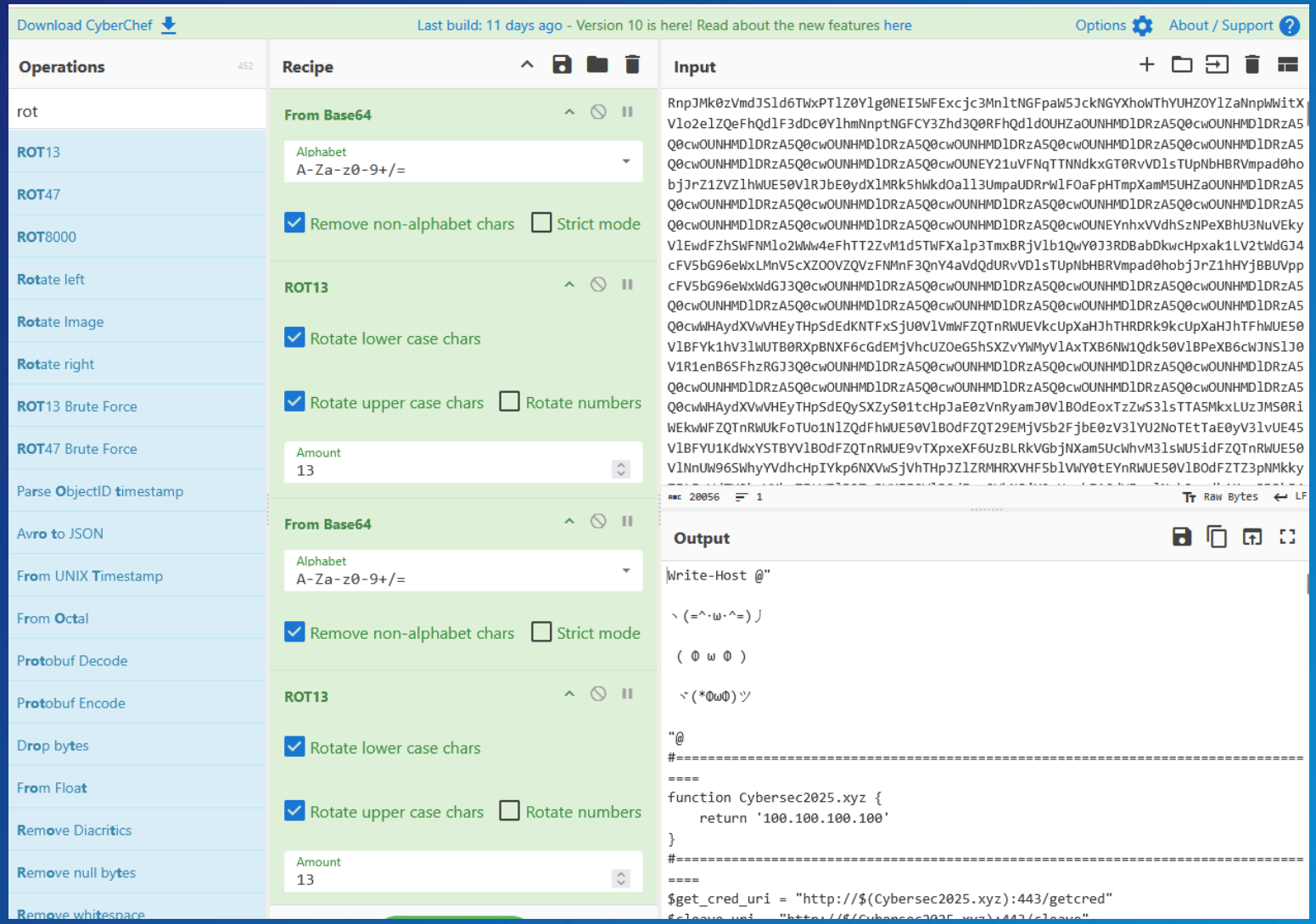
分析樣本找出中繼站

- IR Tools
- Sandbox
  - Virustotal
  - Any.run
  - cuckoo

從樣本找出中繼站


MOVE YOUR MOUSE TO VIEW SCREENSHOTS
ANY RUN
Malicious activity
最新一手精准综合数据.exe
MD5: 695FB004999DB196355A2AADDFA39B2F
Start: 12.12.2022, 09:35 Total time: 300 s
Win7 32bit
Add tags
Indicators:
Get sample
IOC
MalConf
Restart
Text report
Graph
ATT&CK
Summary
beta
Export
CPU
RAM
Processes
Filter by PID or name
Only important
988 最新一手精准综合数据.exe PE
400 348 128
2056 最新一手精准综合数据.exe PE
6 0 4
HTTP Requests 0
Connections 1
DNS Requests 1
Threats 1
Filter by PID, domain, name or ip
PCAP
Timeshift Protocol Rep PID Process name CN IP Port Domain ASN
40821 ms TCP ? 988 最新一手精准綜合数据.exe 43.249.175.162 1478 www.liangjia... Sun Network Ho...
NETWORK
FILES

從樣本找出中繼站


Download CyberChef
Last build: 11 days ago - Version 10 is here! Read about the new features here
Options
About / Support
Operations
rot
ROT13
ROT47
ROT8000
Rotate left
Rotate Image
Rotate right
ROT13 Brute Force
ROT47 Brute Force
Parse ObjectID timestamp
Avro to JSON
From UNIX Timestamp
From Octal
Protobuf Decode
Protobuf Encode
Drop bytes
From Float
Remove Diacritics
Remove null bytes
Remove whitespace
Recipe
From Base64
Alphabet
A-Za-z0-9+/=
Remove non-alphabet chars
Strict mode
ROT13
Rotate lower case chars
Rotate upper case chars
Rotate numbers
Amount
13
From Base64
Alphabet
A-Za-z0-9+/=
Remove non-alphabet chars
Strict mode
ROT13
Rotate lower case chars
Rotate upper case chars
Rotate numbers
Amount
13
Input
RnpJMk0zVmdJSld6TWxPTlZ0Ylg0NEI5WFExcjc3MnltNGFpaW5JckNGYXhoWThYUHZOYlZaNnpWWitX
Vlo2elZQeFhQdlF3dDc0YlhmNnptNGFCY3Zhd3Q0RFhQdldOUHZaOUNHMDlDRzA5Q0cwOUNHMDlDRzA5
Q0cwOUNHMDlDRzA5Q0cwOUNHMDlDRzA5Q0cwOUNHMDlDRzA5Q0cwOUNHMDlDRzA5Q0cwOUNHMDlDRzA5
Q0cwOUNHMDlDRzA5Q0cwOUNHMDlDRzA5Q0cwOUNEY21uVFNqTTNNdkxGT0RvVDlsTUpNbHBRVmpad0ho
bjJrZ1ZVZlhWUE50VlRJbE0ydXlMRk5hWkdOall3UmpaUDRrWlFOaFpHTmpXamM5UHZaOUNHMDlDRzA5
Q0cwOUNHMDlDRzA5Q0cwOUNHMDlDRzA5Q0cwOUNHMDlDRzA5Q0cwOUNHMDlDRzA5Q0cwOUNHMDlDRzA5
Q0cwOUNHMDlDRzA5Q0cwOUNHMDlDRzA5Q0cwOUNEYnhxVVdhSzNPeXBhU3NuVEky
VlEwdFZhSWFNMlo2WWw4eFhTT2ZvM1d5TWFXalp3TmxBRjVlb1QwY0J3RDBabDkwcHpxak1LV2tWdGJ4
cFV5bG96eWxLMnV5cXZOOVZQVzFNMnF3QnY4aVdQdURvVDlsTUpNbHBRVmpad0hobjJrZ1hHYjBBUVpp
cFV5bG96eWxWdGJ3Q0cwOUNHMDlDRzA5Q0cwOUNHMDlDRzA5Q0cwOUNHMDlDRzA5Q0cwOUNHMDlDRzA5
Q0cwOUNHMDlDRzA5Q0cwOUNHMDlDRzA5Q0cwOUNHMDlDRzA5Q0cwOUNHMDlDRzA5Q0cwOUNHMDlDRzA5
Q0cwWHAydXVwVHEyTHpSdEdKNTFxSjU0VlVmWFZQTnRWUEVkcUpXaHJhTHRDRk9kcUpXaHJhTFhWUE50
VlBFYk1hV3lWUTB0RXpBNXF6cGdEMjVhcUZOeG5hSXZvYWMyVlAxTXB6NW1Qdk50VlBPeXB6cWJNSlJ0
V1R1enB6SFhzRGJ3Q0cwOUNHMDlDRzA5Q0cwOUNHMDlDRzA5Q0cwOUNHMDlDRzA5Q0cwOUNHMDlDRzA5
Q0cwOUNHMDlDRzA5Q0cwOUNHMDlDRzA5Q0cwOUNHMDlDRzA5Q0cwOUNHMDlDRzA5Q0cwOUNHMDlDRzA5
Q0cwWHAydXVwVHEyTHpSdEQySXZyS01tcHpJaE0zVnRyamJ0VlBOdEoxTzZwS3lsTTA5MkxLUzJMS0Ri
WEkwWFZQTnRWUkFoTUo1NlZQdFhWUE50VlBOdFZQT29EMjV5b2FjbE0zV3lYU2NoTEtTaE0yV3lvUE45
VlBFYU1KdWxYSTBYVlBOdFZQTnRWUE9vTXpxeXF6UzBLRkVGbjNXam5UcWhvM3lsWU5idFZQTnRWUE50
VlNnUW96SWhyYVdhcHpIYkp6NXVwSjVhTHpJZlZRMHRXVHF5blVWY0tEYnRWUE50VlBOdFZTZ3pNMkky

已知漏洞

- 弱點掃描工具
- 網站弱掃工具
- 搜尋對應的exploit
- 發動攻擊

不當配置

- 參考教學視頻與技術文章，常看到
  - 更改下載源
  - 定製化系統
  - 非官網的下載點
  - 搬磚的過期文章
  - 水坑式攻擊

水坑式攻擊

- Demo

未公開漏洞

偽造被入侵環境進行反監控

- 將受駭主機轉生為客製化honeypot
- 最適用於standalone的環境
  - Ex：行銷部門自行架設的wordpress
- 建立隔離網段
- 複製受駭主機
- 搭配監控工具：
  - 既有監控工具(Ex：IPGuard、iMonitor)
  - Sniffer
  - Keylogger

社交工程

- 偽裝成另一批打進去的黑客
  - 在受駭主機上進行文字檔案留言交談
- 臥底相關群組
  - 收集攻擊相關資訊
  - 提供有問題的套件

接管中繼站

- 開啟服務或設定
  - Web service
    - 如：HFS
  - Directory Listing
- 持續拓展(帶運氣成分)
  - 更多中繼站
  - 兵器庫
  - 儲存區

兵器庫/儲存區

2019/12/16	19:04	836096	-截屏20191618471.jpg.exe
2019/12/17	18:32	1855488	-截屏20191718311.jpg.exe
2019/12/18	15:43	3527680	-截屏20191815401.jpg.exe
2019/12/18	17:53	1059840	-截屏20191817531.jpg.exe
2019/12/18	18:14	837120	-截屏20191818131.jpg.exe

Name .extension	Size	Timestamp	Hits
001	*folder*	2019/12/9 14:01:26	17
002	*folder*	2019/12/7 22:35:11	29
003	*folder*	2019/12/8 12:44:49	1
004	*folder*	2019/12/8 13:11:27	1
005	*folder*	2019/12/17 19:59:59	178
006	*folder*	2019/12/18 13:13:15	127
007	*folder*	2019/12/11 15:19:57	14
008	*folder*	2019/12/17 1:55:06	40
009	*folder*	2019/12/18 12:14:54	16
QQ	*folder*	2019/12/14 22:01:39	9

兵器庫/儲存區

2019/12/21	13:08	1105926	-截屏2019122113083.jpg.exe
2019/12/21	13:33	933897	-截屏2019122113325.jpg.exe

Name .extension	Size	Timestamp	Hits
001	folder	2019/12/20 1:23:33	45
002	folder	2019/12/20 19:55:14	42
003	folder	2019/12/20 20:07:00	6
004	folder	2019/12/20 20:14:02	6
007	folder	2019/12/11 15:19:57	20
008	folder	2019/12/17 1:55:06	75
009	folder	2019/12/18 12:14:54	51
010	folder	2019/12/18 22:10:42	13
QQ	folder	2019/12/14 22:01:39	25

儲存區

- 隨時留意是否有更新
- 比對自家資料確認
- 是否通報其他受害者?

兵器庫

- 攻擊樣本不定期上架
  - 可加入訂閱功能
  - 或設置定期監控回報
- 保持低調，盡量不添加多餘功能

超前佈署

- 在攻擊發生前，先行佈署對應的病毒碼或防禦規則
  - 即使使用者粗心中招，有較高機率讓攻擊失效
- 在攻擊發生前，先行封鎖C2
  - 即使使用者粗心中招，仍無法順利反連回C2

(抓內鬼)

- 在部分攻擊的情境中，單位內部可能存在內鬼
- 透過超前佈署有時會意外抓到內鬼
  - 提前封鎖C2
  - 攻擊失效
  - 檢視防火牆紀錄，發現未接收到惡意程式的人員主動連至C2
  - 調閱CCTV，並比對時間序與該時段行為動作
  - 發現人員異常
  - 人員訪談(建議配合法務人員)

後記

- 反擊駭客絕不是一種最有效的防禦方式
  - 須熟悉攻擊與IR技術
  - 可能有法律風險
  - 打你的通常不會只有一家，但你有餘力打回去的通常只有一兩家
- 但仍有其優點
  - 研究攻擊者的手法
  - 補強自身防禦機制或政策上的疏漏
  - 當作爭取防禦資源的佐證
  - ~~爽度很高~~

Thanks

TEAM CYBERSECURITY