奧義智慧科技

AI 資安點線面

MDR 端點偵測與回應、 CTI 威脅情資

2021.05.28 資安分析師 羅煜賢 Wave

關於奧義智慧科技: 本土、實業、正派，世界領先科技

奧義智慧持續厚積台灣能量，以AI驅動的資安自動化服務在國內諸多領域保持第一的市占率，獲得政府機關、金融、高科技等財星500大企業之肯定，2019年獲邀美國 MITRE ATT&CK® 攻擊框架評測計畫，2020年官方公告評測結，奧義智慧在**最高告警能力**、**最少人為介入**、**最低雜訊**，技冠群雄獲全球21家國際大廠之最。

奧義智慧已在日本、新加坡成立據點，策略合作夥伴遍及東協泰國、馬來西亞、印尼、越南及菲律賓等10國，持續積極將台灣能量推向世界舞台。我們以人工智慧提供 MDR，SOC， 情資，資安健診，數位鑑識，資安事件處理IR，以及安全在家工作等相關服務。

- **資安即國安，台灣自主技術**：奧義智慧為台灣國防產業發展協會創始會員廠商暨常務監事
- **世界領先科技水準**：通過美國 MITRE ATT&CK APT29 評測結果為最高告警能力的資安產品
- **在台緊急應變能量獲認證**：國際資安應變聯盟組織 FIRST 認證奧義智慧 CCCSIRT 緊急應變團隊
- **品牌獲國際肯定**：獲頒國際網路安全2020卓越獎 (Cybersecurity Excellence Awards) 28項金獎

TW-DIDA 台灣國防產業發展協會 Taiwan Defense Industry Development Association

資安即國安
國防自主技術

FIRST Improving Security Together

國際企業安全事件
應變認證

MITRE | ATT&CK

2019 MITRE ATT&CK
公開評測最高分

CYBER SECURITY EXCELLENCE AWARDS WINNER 2020

2020 網路安全卓越獎
28 項金獎

Interop BEST 2020

日本Interop
最佳資安產品獎

bsi ISO/IEC 27001 資訊安全管理 CERTIFIED

ISO/IEC
27001

Agenda

- MDR 端點監控與應變服務實例(一)
  - **奧義智慧 獨家數位疫苗發展史**
- MDR 端點監控與應變服務實例(二)
  - **AI 疫調速度之快，絕不發生「校正回歸」**
- 客戶要求其供應鏈都要執行 資安健診 (三)
  - **我國半導體產業技術領先國際，碰到資安問題也得找專家 - 奧義智慧**
- 花了大把時間寫爬蟲，調查起來卻卡卡?
  - **連外國人都搶著用的全球威脅情資平台**
- 人員資安意識訓練永遠流於形式? 有做跟沒做一樣...
  - **透過科技執法，超前部署**

MDR 服務實例(一)

奧義智慧 獨家數位疫苗發展史

疫苗可有效降低風險

英國數據： AZ疫苗第1劑可降8成死亡風險

分享 分享 留言 列印 收藏 A- A+

2021-05-11 12:00 中央社 倫敦10日綜合外電報導 讚 0 分享 + 公共衛生

英格蘭公共衛生署今天表示，英國藥廠阿斯特捷利康（AstraZeneca）疫苗施打結果顯示，打1劑AZ疫苗，可減少80%的2019冠狀病毒疾病（COVID-19）死亡風險。

路透社報導，英格蘭公共衛生署（Public HealthEngland）還說，他們的新分析顯示，美國輝瑞大藥廠（Pfizer）和德國BioNTech合作研發的疫苗，第1劑可預防80%的死亡風險，打完2劑防護力則提升到97%。

Ref : https://money.udn.com/money/story/5599/5448728

單劑AZ疫苗對60歲者保護力達86%

韓國疾病管理廳（Korea Disease Control and Prevention Agency, KDCA）追蹤韓國超過350萬名60歲長者長達2個月，數據顯示長者施打1劑AZ疫苗後，保護力可達86%

KCDA：民眾應根據建議時程完整接種2劑疫苗，保護力會進一步提升。

資料來源：韓國疾病管理廳
https://www.korea.kr/news/pressReleaseView.do?newsId=156450427

中央流行疫情指揮中心 2021/05/06

Ref : https://www.cdc.gov.tw/File/Get/cX0wlALiSWTjbyepSZtaTg

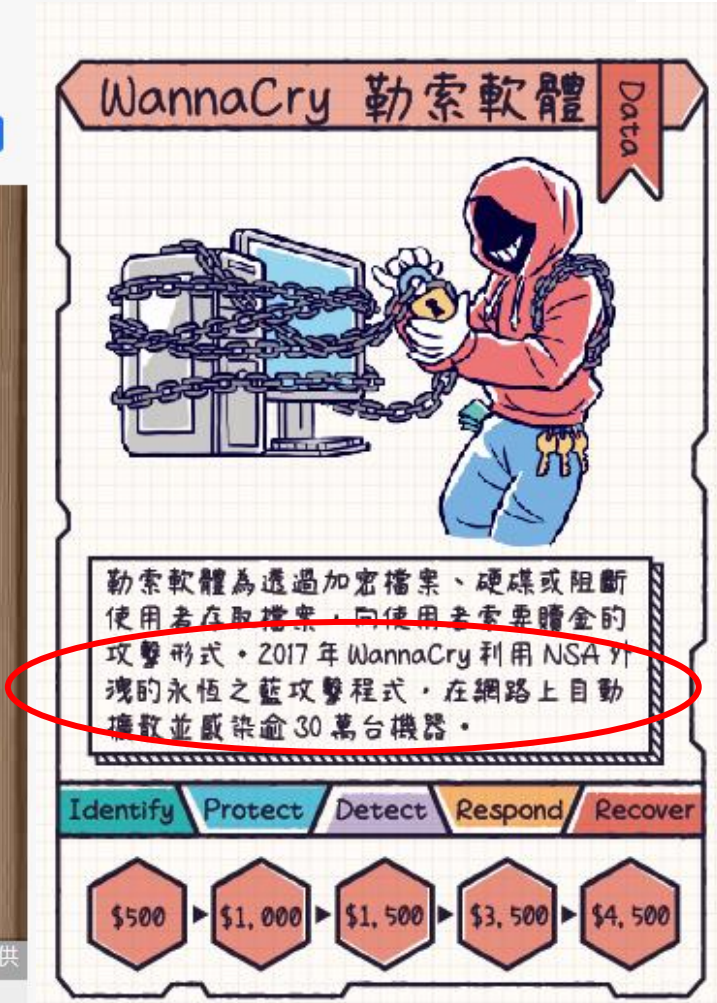
借鑑公共衛生防疫概念，顛覆資安防護既有作法：臺資安公司推勒索軟體數位疫苗

誤導攻擊者的惡意軟體行動，使其無法依照預定行程發動攻勢

文/ 黃彥棻 | 2021-03-25 發表

讚 6.5 萬 按讚加入iThome粉絲團 讚 220 分享

面對這種勒索軟體的威脅，臺灣資安公司奧義智慧共同創辦人叢培侃日前在HITCON Freetalk的研討會中，正式公開該公司與勒索軟體Conti交手過招的過程，以及揭露他們研發的數位疫苗。



Ref : https://www.ithome.com.tw/news/143457

數位疫苗發展故事前言 ~

目標範圍

- 5000+ 台電腦
- 300+ 台伺服器
- 範圍分佈於台灣、中國大陸、美國、歐洲

防護配置

- 有我國知名 SOC 監控商委外服務
- 有防毒軟體(AV)、防火牆(FW)、入侵防禦(IPS)、...
- 有國際知名 APT 產品

發生症狀

- AD 遭增加帳號
- Web 有不知名檔案產生
- 防毒主機遭攻擊
- 天天都有電腦遭加密慘案

接下來，出動奧義

某遭勒索軟體攻擊客戶工作紀錄摘要

2020年 9 月底 防毒廠商進場

- 客戶持續有問題發生

10月初 我國 某 MDR 大廠

- 無發現明確問題

10月中 我國某 知名健診工具廠商

- 該廠 PoC 報告並處置後，問題持續發酵
- 客戶再持續找其他廠商做 PoC

11 月 16 日 奧義開始掃描

- 自動通報出高風險事件
- 客戶隨即將防毒主機下線
- 通報 AD 伺服器問題
- 通報偵測異常 Process

11 月 24 日 PoC 結案報告

- 所有廠商中根因分析最快速且最完整
- 提供最佳整治方案
- 客戶請求進一步協助

11 月 25 日 決定進一步合作

- 轉 IR 服務

11 月 26 日 執行緩解方案

- 數位疫苗施打
- 必要戰場清掃

12 月 9 日 服務完成報告

- 確認戰場概況
- 回報未繼續發生勒索

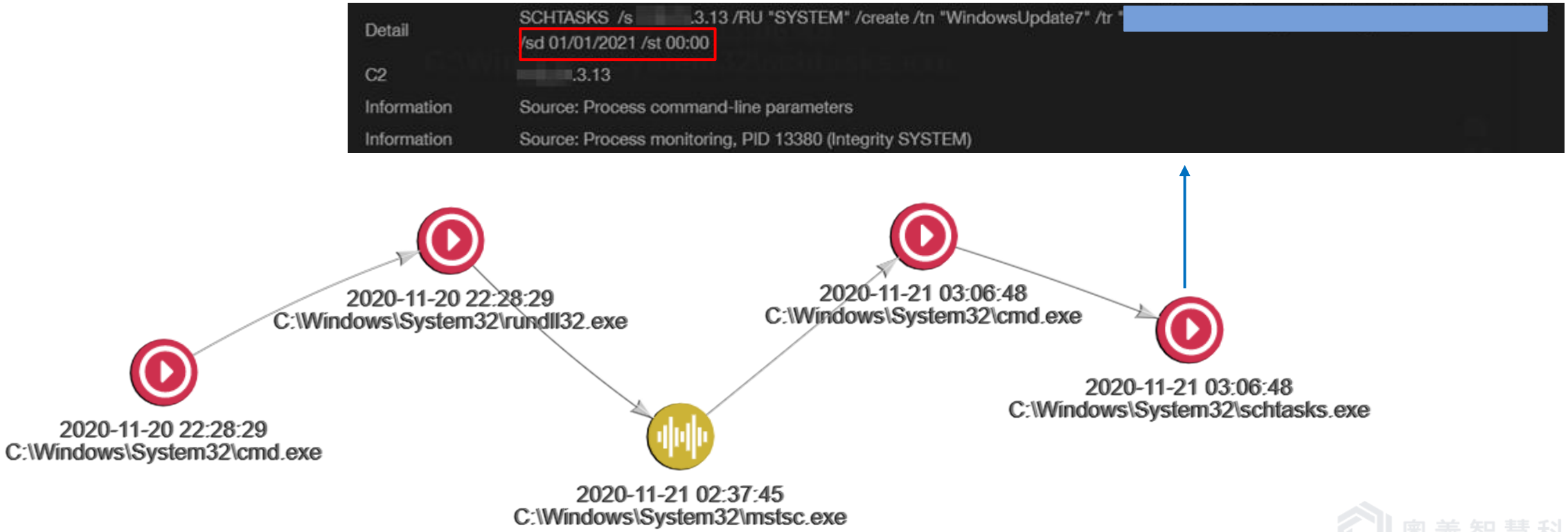
2021年 1 月 1 日 轉正式客戶

- 正式 MDR 客戶

持續監控期

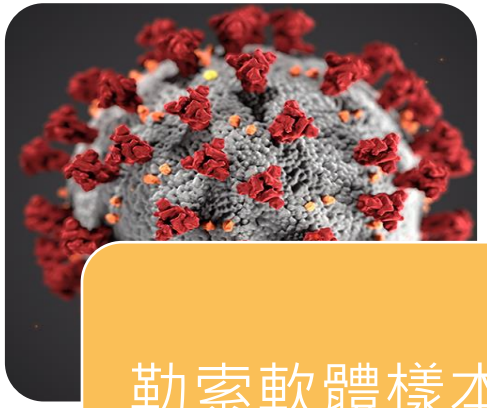
防毒主機發現定時炸彈

- 駭客將在 2021年 01月 01日 0點0分時，執行大規模勒索



數位疫苗首場戰役，有效抑止感染擴散

- 依照勒索病毒特性製作專屬疫苗，再透過 Agent 施打數位疫苗，抑制此波勒索軟體持續感染
- 根據全場域受駭狀況，提供**完善的診治計畫**，包含**後續追蹤事項**



勒索軟體樣本收集及分析

Agent 施打數位疫苗

有效阻止勒索風險

*** 無額外派送新軟體之痛點**

*** 如欲了解數位疫苗更深入的服務與功能，請洽各服務業務**

「數位疫苗」使用契機

5 大優勢讓 奧義 有效整治企業內部資訊問題

- 非單台的檢測結果 → 一次分析上萬台電腦及各電腦間的關聯性
- 非仰賴規則式的檢測方式 → 因無規則，故駭客無法繞過所謂的規則
- 專業顧問團隊 → 奧義匯集各領域專家，以提供最精準的諮詢服務
- 持續性監控，見林又見樹 → 駭客使用原藏匿工具，遭行為分析發現，持續見招拆招
- 數位疫苗誕生 → 台灣原廠程式客製化，針對各場域不同隨時變化整治計畫之策略

MDR 服務實例(二)

AI 疫調速度之快，絕不發生「校正回歸」

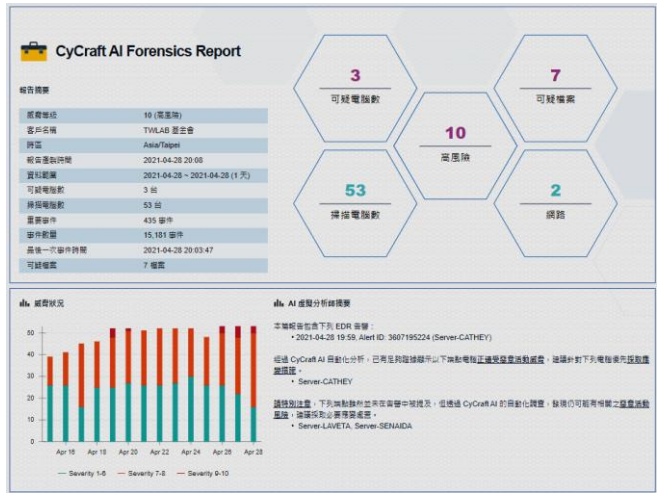
MDR 服務故事前言 ~

目標範圍	防護配置	資安事件
40+ 台端點電腦	有 SOC 監控服務	有勒索軟體事件
20+ 台服務主機	有 Firewall, WAF	對外網站疑似被入侵
300 個內網設備	有 APT 偵測產品	資安設備有零星事件

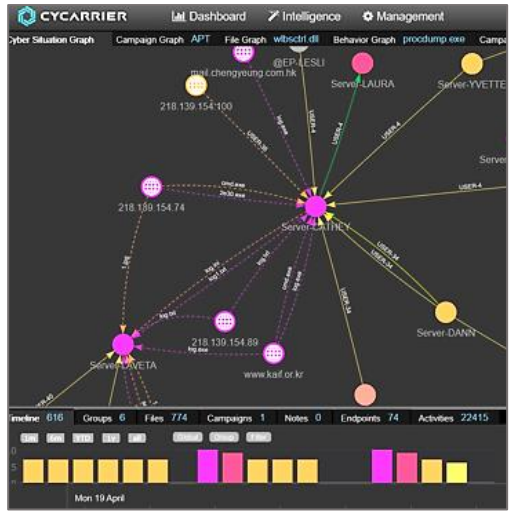
接下來，出動奧義

1

2



3



20:00
XENSOR EDR 威脅告警

20:08
AI 資安威脅鑑識報告

20:55
進行遠端緊急處置

19:57
AGENT 偵測到駭客活動

20:45
分析師完成根因分析

奧義智慧 MDR - 快速應變、強化資安

2021 年 04/27 PoC 執行會議

- 說明產品運作架構
- 了解客戶環境架構
- 分工雙方工作小組職務

04/28 部署建置

- Xensor Agent 部署建置
- 當晚即時偵測駭客活動並發出 EDR Alert
- 10 分鐘內產出全場域 AI Report

04/28 晚上 分析師接手

- 奧義 24/7 SOC 監控分析師接手
- 操作 CyCarrier 完整分析入侵軌跡及手法
- 通知客戶入侵脈絡及回應方式

04/29 早上 大規模部署

- 與客戶討論整體受害狀況
- 啟動更大規模部署作業

04/29 下午 戰場清理

- 確認端點部署率涵概率高
- 整體入侵脈絡及入侵根源掌握
- 啟動 Xensor Remediation 自動清理戰場

05/01 持續監控

- 持續監控客戶環境，啟動遠端移除功能
- 確保客戶於弱點修補前，持續阻止駭客進一步攻城掠地

客戶要求其供應鏈都要執行 資安健診 (三)

我國半導體產業技術領先國際，碰到資安問題也得找專家 - 奧義智慧

我國半導體產業遭大規模竊取

- **攻擊時間：2018 ~ 2019 期間**
- **攻擊對象：半導體產業**
- 目標：竊取晶片相關文件、原始碼...等技術機密

至少達 1年
時間

至少 7 家
半導體

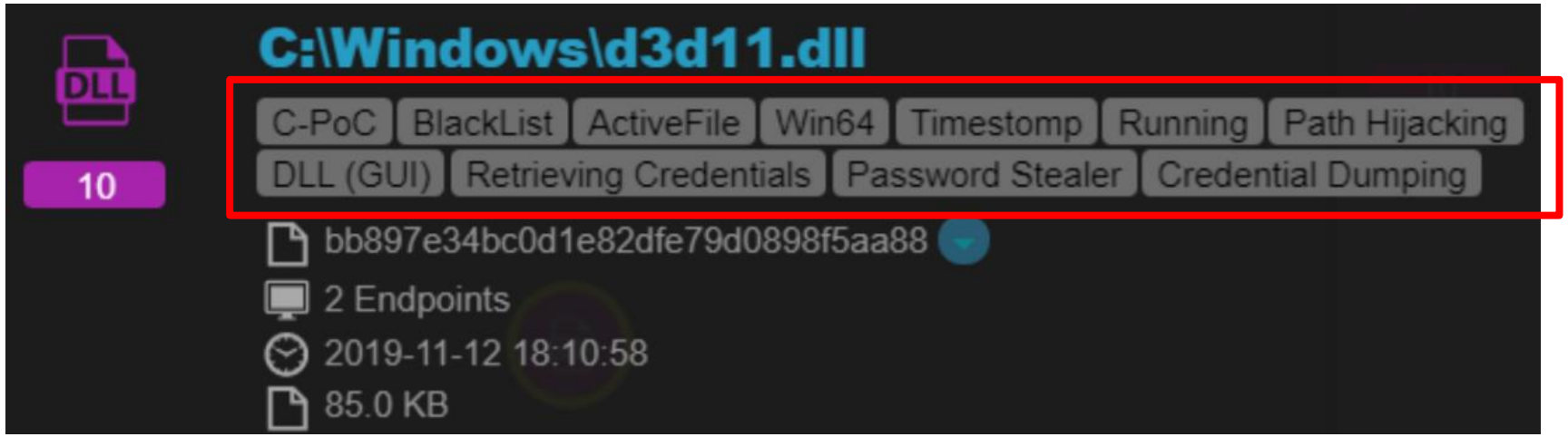
合作夥伴
上下游商

Ref : https://medium.com/cycraft/taiwan-high-tech-ecosystem-targeted-by-foreign-apt-group-5473d2ad8730

再多權限管制也敵不過被插入「萬能金鑰」

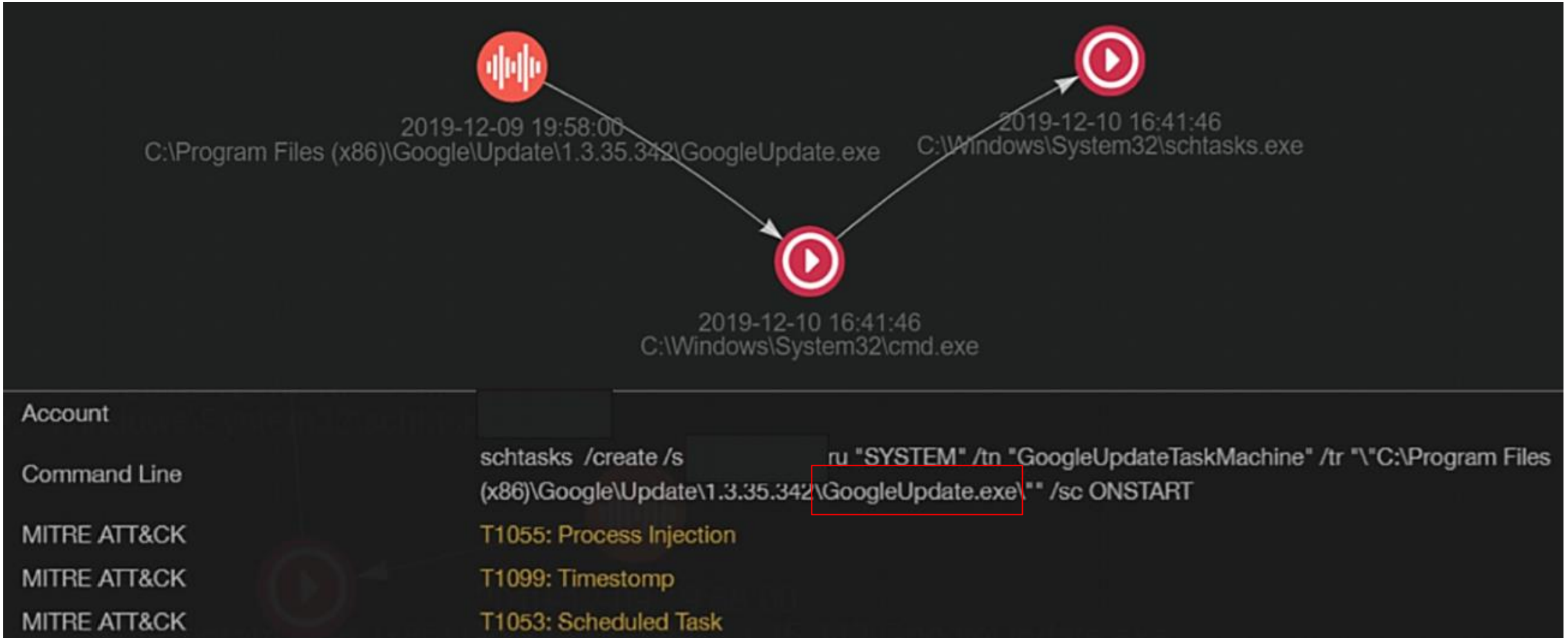
- 發現於數間我國之 IC 設計公司
- 專注於攻擊我國之惡意程式 國際上查無任何資料
- 擁有萬能金鑰，企業內電腦暢行無阻！

萬能金鑰



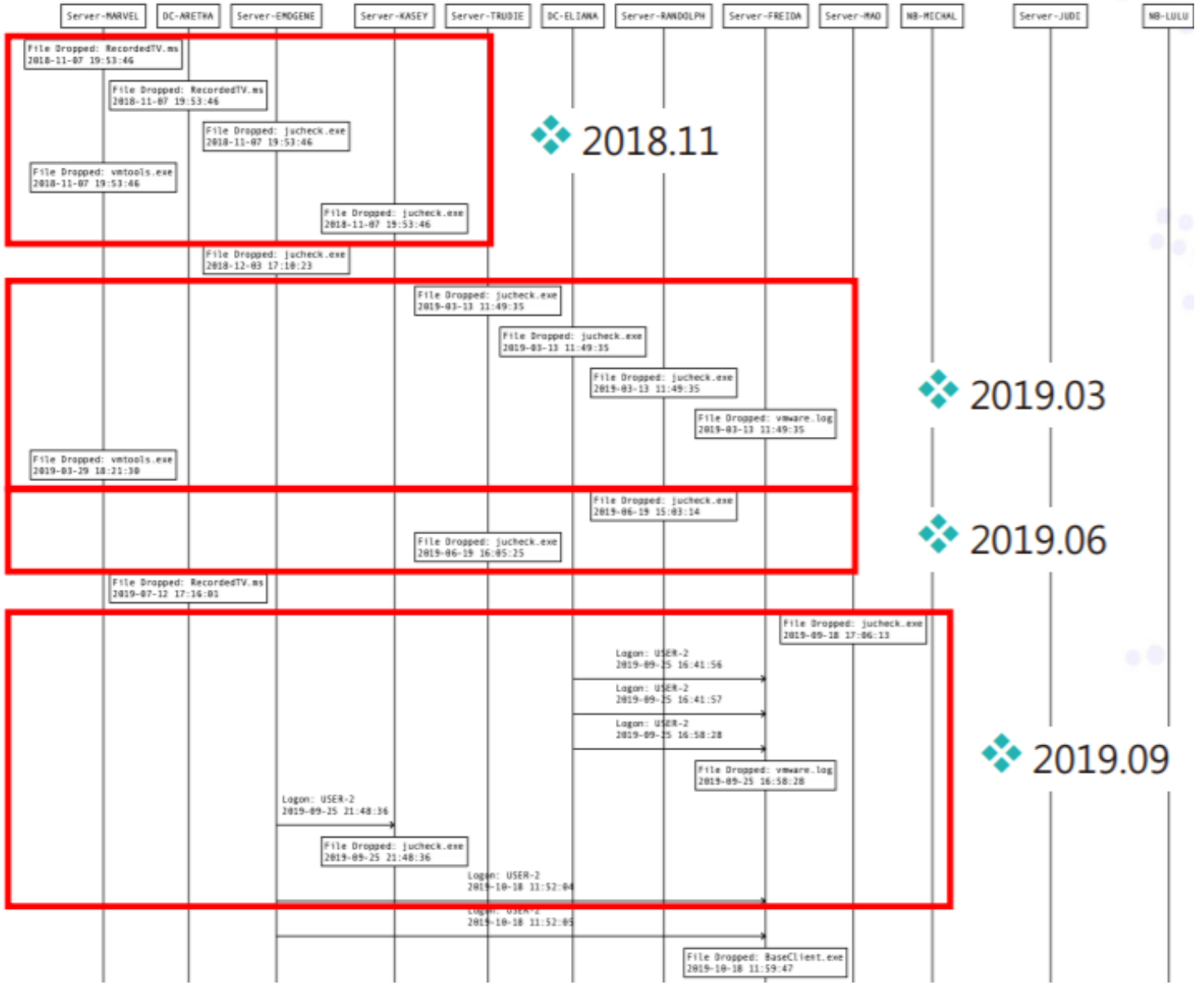
透過檔案結構分析，判別功能

攻擊者隱匿於 Google 的更新程式中



人人羨慕的躺著賺

駭客無痛創造每季績效指標

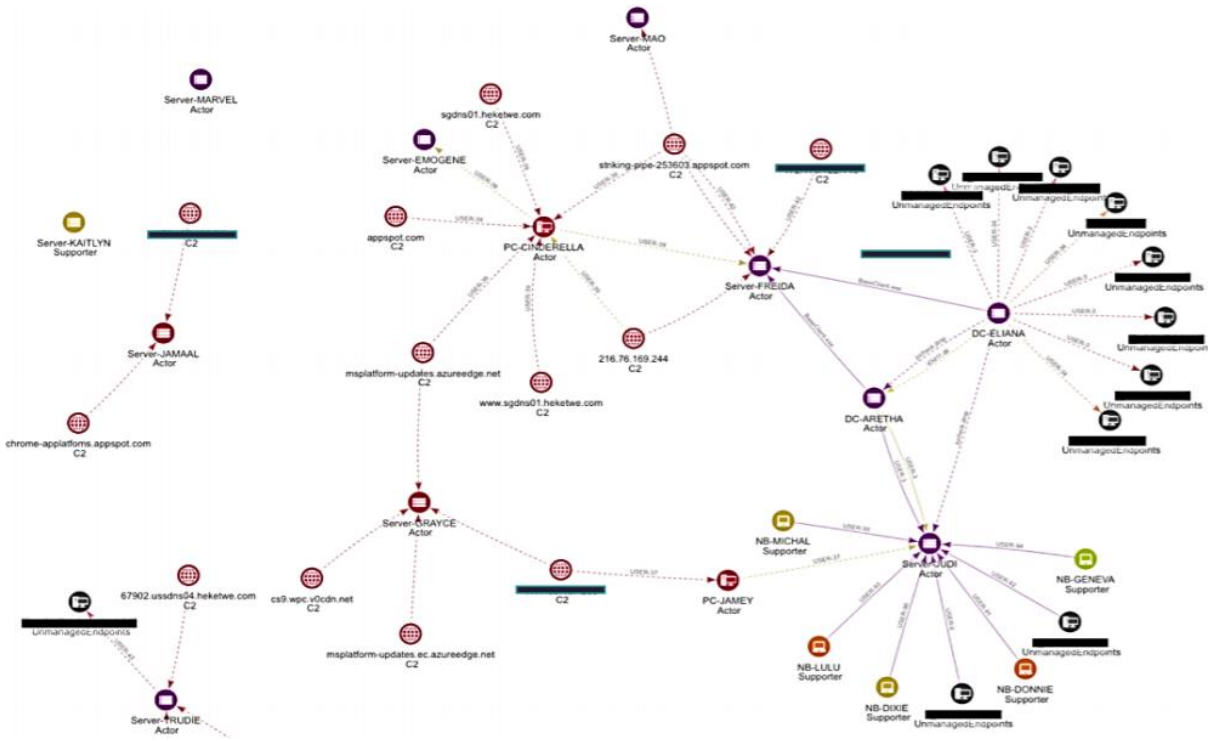


調查最後一哩路 - 清查企業損失

駭客竊取的資料	白話文翻譯	目的
Project\Roadmap	產品未來策略規劃	掌握競爭對手策略
Backup\Workspace	工作區備份	研究競爭對手工作環境
Chip and SDK Setting	(晶片) 設定檔	核心的參數設定
Product SDK	產品開發工具包	用以模仿晶片
Installation Guide	(晶片)使用與安裝手冊	快速掌握核心技術

奧義 MDR 客戶可立即無償盤點攻擊活動

- 一把金鑰在企業內網走透透，無視所有 資安阻擋機制、權限控管機制、偵測機制
- 僅刪除惡意檔案 (友商會用奧義所發布之 IoC 進行刪除) 也無法根除問題
- 透過萬用金鑰進行驗證，於系統上僅留「登入成功」 紀錄，無法被 Rule 判為異常
- **必須透過 AI 進行自動化關聯(有效)，並輔以專業顧問諮詢以根除問題(解決)**



花了大把時間寫爬蟲，調查起來卻卡卡?

連外國人都搶著用的全球威脅情資平台

解決傳統調查痛點 – 時間冗長

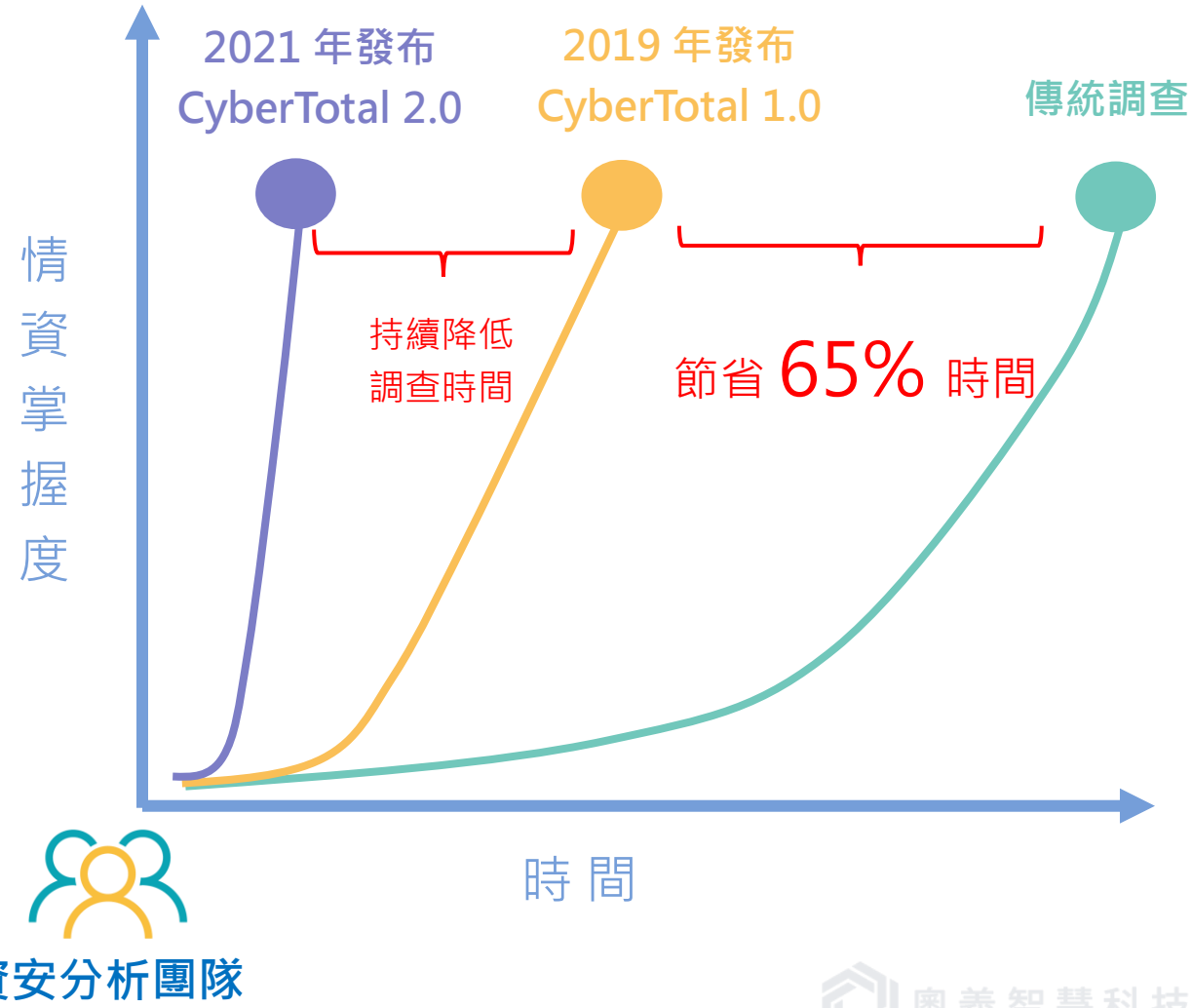
株式会社CYCRAFT JAPAN

2019-06-12

【CSIRT担当＋SOCサービス企業向け 脅威インテリジェンス・プラットフォーム導入事例のご紹介】 アラート調査の時間を約６５％カット、大幅短縮を実現。

株式会社CyCraft Japan（本社：東京都千代田区、代表取締役社長：Benson Wu、以下CyCraft）の主力商品である脅威インテリジェンス・プラットフォーム「CyberTotal」が、ネットワンシステムズ株式会社（本社：東京都千代田区、代表取締役社長：荒井 透、以下 ネットワンシステムズ）において、2019年4月より導入されたことをお知らせいたします。ネットワンシステムズでは、2017年より自社独自のSOCを立ち上げ、MSS (Managed Security Service) やMDR (Managed Detection & Response) サービス等のセキュリティ監視・運用サービスを提供してきました。この中で、セキュリティを監視するアナリストにとって、24時間リアルタイムでアラートに対応する際に、未知の新しいIOC（Indicator of Compromise：脅威の痕跡）の深い調査は負担が多く、効率化の観点でも重要な課題がありました。

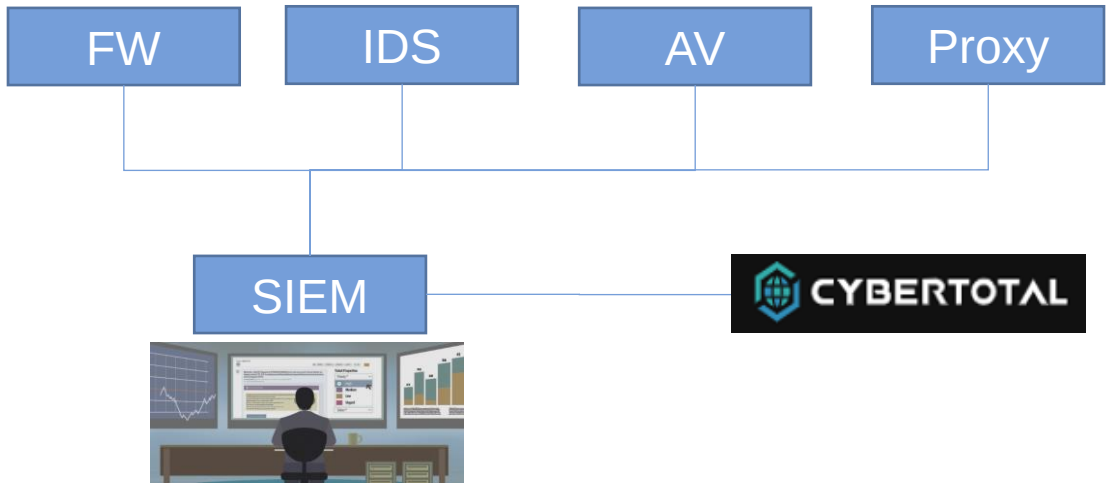
今回、CyberTotalを導入したことで、セキュリティ監視をする際の各種IOC調査に必要な時間を大幅に短縮するとともに、より一層深い分析が可能になり、さらには、独自の指標ガイダンスにより判断速度を速め、業務の効率化を実現しました。



- CyberTotal 2.0 的應用在許多資安場合，包含日本 SOC 廠商、某國軍方、某國電信業者
- 將資安手工業轉變成自動化工業

CyberTotal 還能做什麼?

- 我國金融業者 SIEM 與 CyberTotal 介接
  - 導入前：雪片般地告警，不知從何查起
  - 導入後：自動化產製報表，問題一目了然，精準處置，準時下班！！！



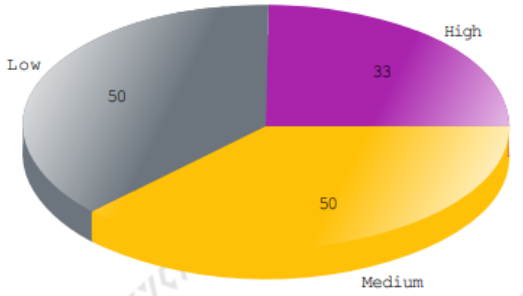
SOC Team

CYBERTOTAL

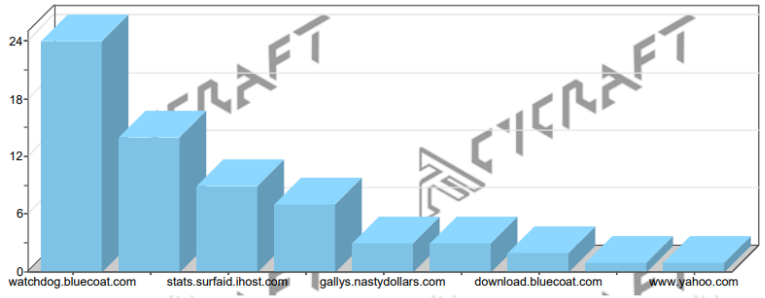
CyberTotal Daily Report :

133 IP/URL(s) in 2020/1/21 has been sent to CyberTotal.
This report contains top 10 high-severity search, top 10 high-risk endpoints and details.

Threat Severity Statistics



Top 10 High-Severity Search



Top 10 High-Severity Search Detail

Severity	Indicator	Reputation	Confidence	Categories	URL	Count	SourceAgentNamt
10	http://www.4whw.com/ct/thumbs/tn6743.jpg	6/9	6	sex, porn, Pornography, adult content	https://10.50.22.66/app/intelligence/a83db69c9cebaldb541917b6	1	bc
10	http://www.4whw.com/ct/thumbs/tn3551.jpg	6/9	6	sex, porn, Pornography, adult content	https://10.50.22.66/app/intelligence/f3f5732a8b6881133baa36f8	1	bc
10	http://www.4whw.com/ct/thumbs/tn6653.jpg	6/9	6	sex, porn, Pornography, adult content	https://10.50.22.66/app/intelligence/419eb76da5390b52d80b56ab	1	bc
10	http://www.4whw.com/ct/thumbs/tn5529.jpg	6/9	6	sex, porn, Pornography, adult content	https://10.50.22.66/app/intelligence/14b4ad664a800a860e31181f5	1	bc

人員資安意識訓練永遠流於形式? 有做跟沒做一樣...

透過科技執法，超前部署

2021春節期間詐騙釣魚簡訊氾濫

iThome 新聞 產品&技術 專題 AI Cloud DevOps 資安 研討會 社群 臺灣資安大會 搜尋

假冒銀行釣魚簡訊詐騙規模擴大，繼國泰世華、台新銀行後，中國信託今日也出現遭冒名的狀況，金融業者與民眾可千萬注意

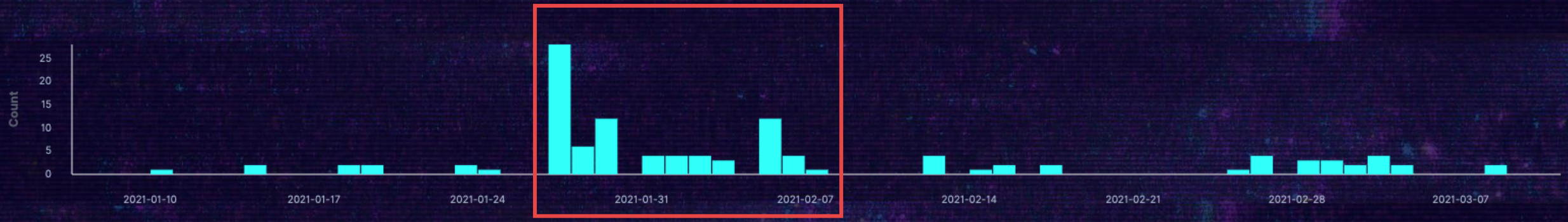
近半個月來，假冒國內金融機關釣魚簡訊詐騙的狀況相當不尋常，不只出現假國泰世華、假台新銀行的釣魚簡訊，已造成30多位民眾上當受害，損失金額超過500萬元，今日（2月9日）再度出現假中國信託的釣魚簡訊。

文/ 羅正漢 | 2021-02-09 發表

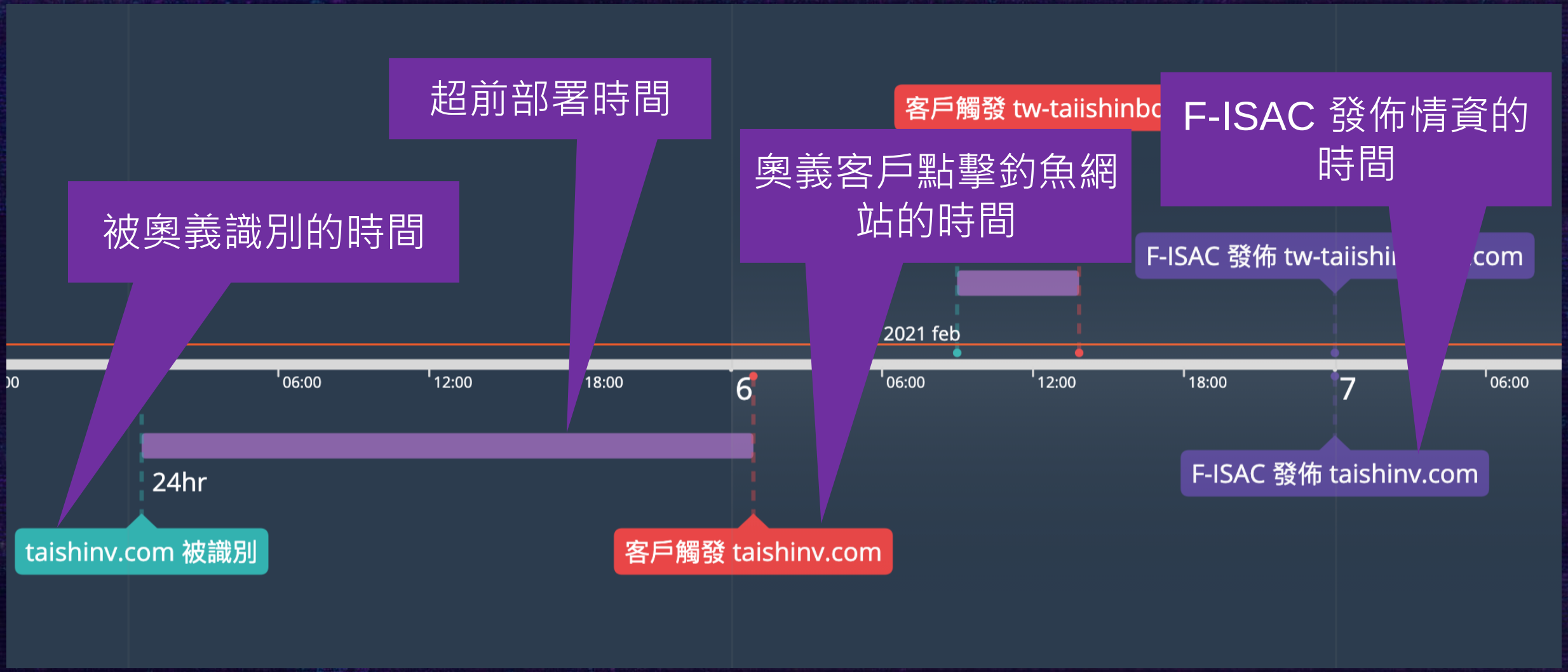
讚 6.5 萬 按讚加入iThome粉絲團 讚 4,484 分享

案例分析 - 金融詐騙

- 金融詐騙在農曆新年 (01/26 ~ 02/08) 達到最高峰



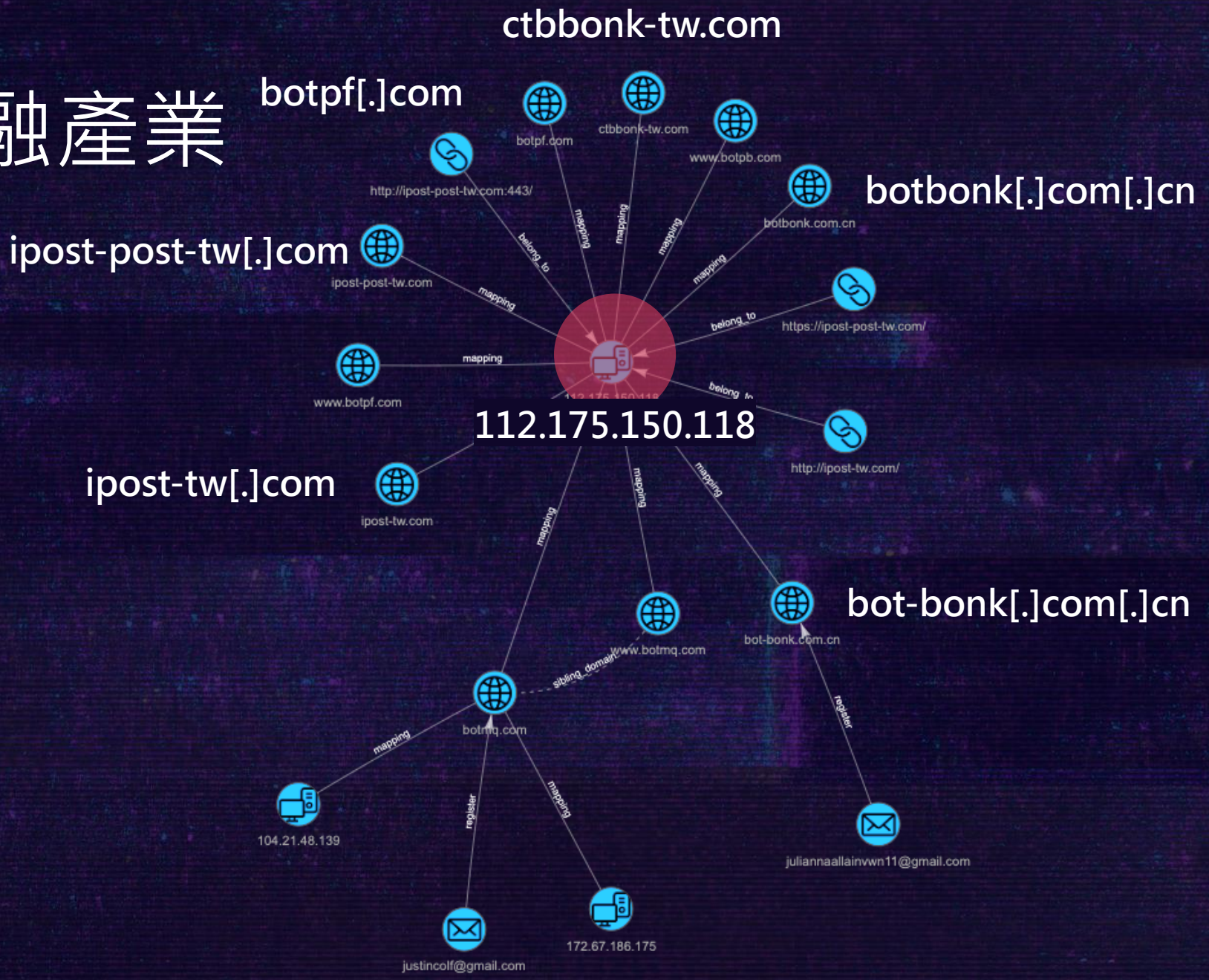
釣魚網域	奧義掌握情資時間	第一位受害者點擊時間	F-ISAC 發佈時間	奧義為企業超前部署
www.cathaydw.com	2021-01-28 22:54	2021-01-29 12:10	01/29	13 h
www.taishinv.com	2021-02-05 00:34	2021-02-06 00:53	02/07	24 h
tw-taiishinbonk.com	2021-02-06 08:59	2021-02-06 13:50	02/07	5 h
...	...	...	...	...



案例分析 - 金融產業

A: 這個 IP 是風水寶地，
銀行們都想要搶

B: 這個 IP 使用者刻意的
在模仿不同的銀行



案例分析 - 金融產業

該 e-mail（Julia）註冊了
兩個可疑的 Domain

A: Julia 是個人才，同時在
amazon 與**台灣銀行（bot）**上班

B: Julia 想釣我！

還在流於形式做人員資安意識訓練?

資安人員：可疑網站不要點
公司同仁：要怎麼分辨「可疑」?
資安人員：....

透過專家的科技執法才是最佳解

接下來行動

奧義粉專

奧義 Medium

鉅立粉絲團

- 下一週：
  - 開啟信箱寄信獲取更詳細解說
  - 奧義: contact@cycarrier.com
  - 鉅立: marketing@jlead.com.tw
- 接下來三個月：
  - 體驗 MDR 資安健診服務
  - 體驗超前部署的威脅情資
- 六個月內應該：
  - 導入 MDR 服務，透過專家為您把關，解決失眠問題
  - 導入 威脅情資 服務，透過科技為您掌握國際最新變化

資安是一種陪伴 奧義一直都在