區網網管會議

臺灣大學計資中心

李美雯

mli@ntu.edu.tw

3366-5010

大 綱

- ASOC 資安偵測 & 情資分析
- 資安案例分享
  - 資安事件趨勢
  - Revil勒索病毒

資安案例分享

資安事件趨勢

今年度最值得關注的網路資安威脅

- 遠端服務協定攻擊
- 勒索軟體
- 加密貨幣挖掘

遠端服務協定攻擊的資安風險

- Windows 遠端桌面服務(RDP)
- Secure Shell 服務(SSH)
- TELNET 服務

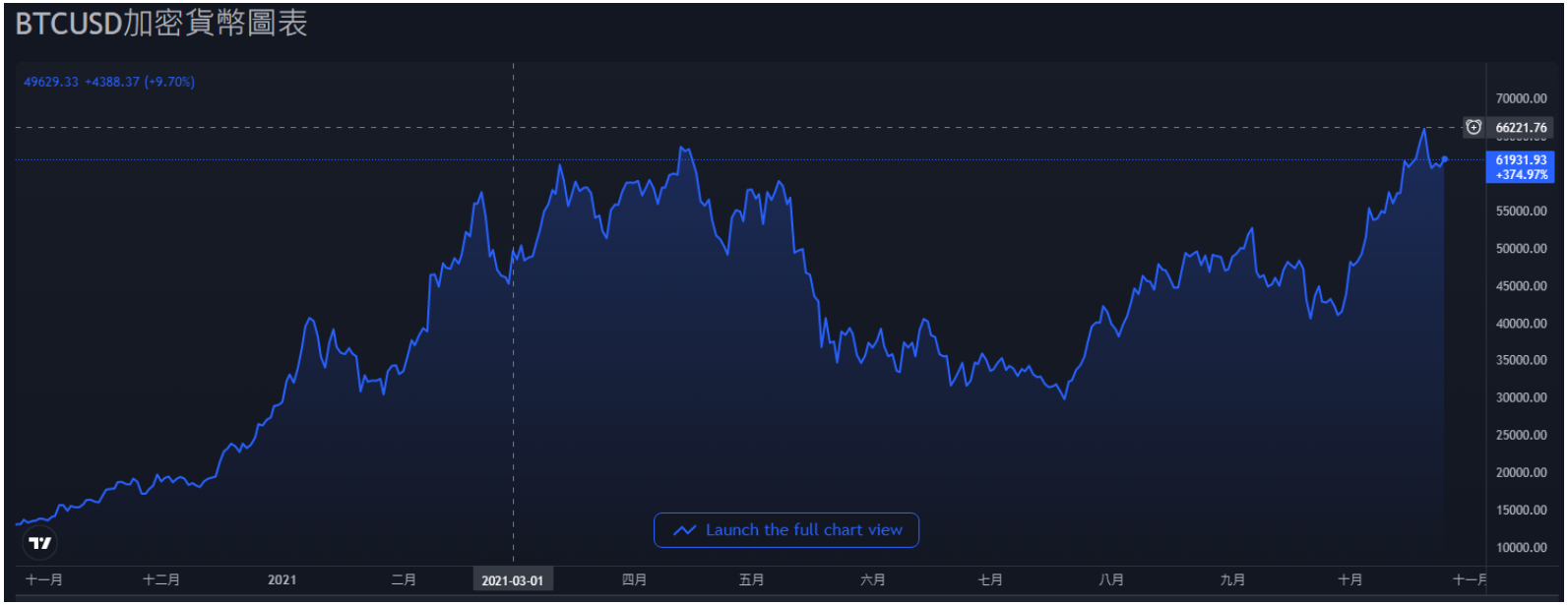
勒索軟體即服務RaaS

2020年~2021年台灣高科技製造業遭受駭客攻擊
2020年分別遭受Evil Corp、DoppelPaymer、Conti等七個不同的勒索病毒集團攻擊
2021年第一季則以REvil (Sodinokibi) 為主。

虛擬貨幣挖掘

1. 網頁劫持
2. BOTNET 散播
3. 免費共享軟體夾帶

比特幣 幣值變化


BTCUSD加密貨幣圖表
49629.33 +4388.37 (+9.70%)
70000.00
66221.76
61931.93
+374.97%
55000.00
50000.00
45000.00
40000.00
35000.00
30000.00
25000.00
20000.00
15000.00
10000.00
Launch the full chart view
十一月
十二月
2021
二月
2021-03-01
四月
五月
六月
七月
八月
九月
十月
十一月

Revil簡介

Revil最早被發現於2019年，又稱Sodinokibi，國內外許多企業都曾受過其攻擊，並被要求支付巨額的贖金，直至今年國內仍有企業受害相關新聞。

Sodinokibi

You probably already know about us. Many publications call us Sodinokibi.

If you've read them, you know that our Ransomware is different in its **technology and reliability.**

We've developed the best data encryption and decryption system available today.

Our competitors allow themselves to lose and destroy their victims' data during the encryption or decryption process, making it impossible to recover the data.

We don't allow ourselves to do that.

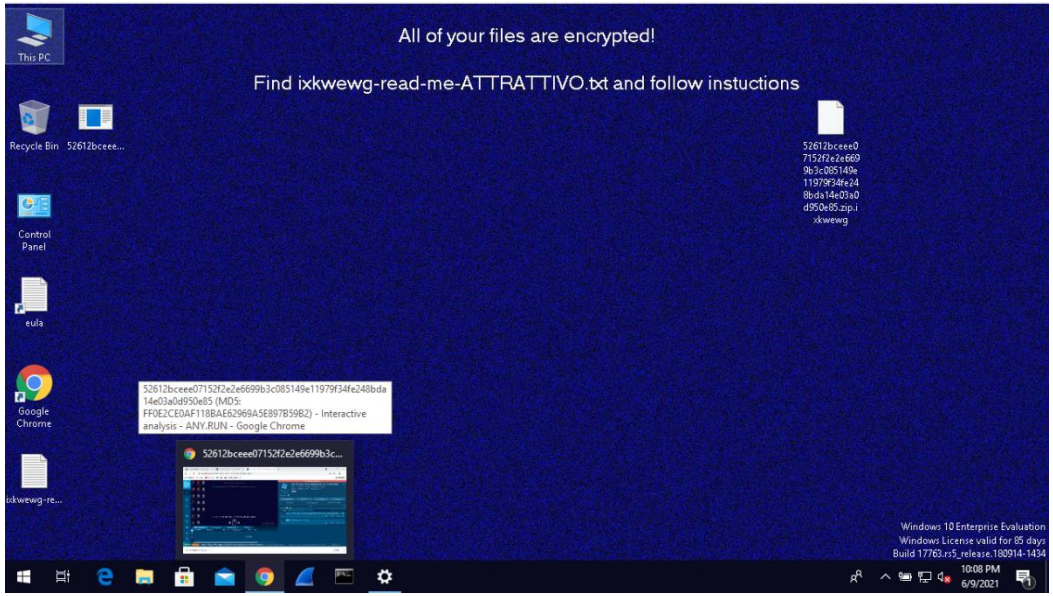
So you should be glad you were infected by our guys, not our competitors. This means that when you pay for the decryption, **you can be sure that all your data will be decrypted.**

Revil散播手法

Revil散佈方式多種，常見手法像封裝在非官方的軟體中，或釣魚手法散佈惡意巨集檔案，除此之外還會針對大型設備的漏洞置入或暴力破解登入後進行攻擊。

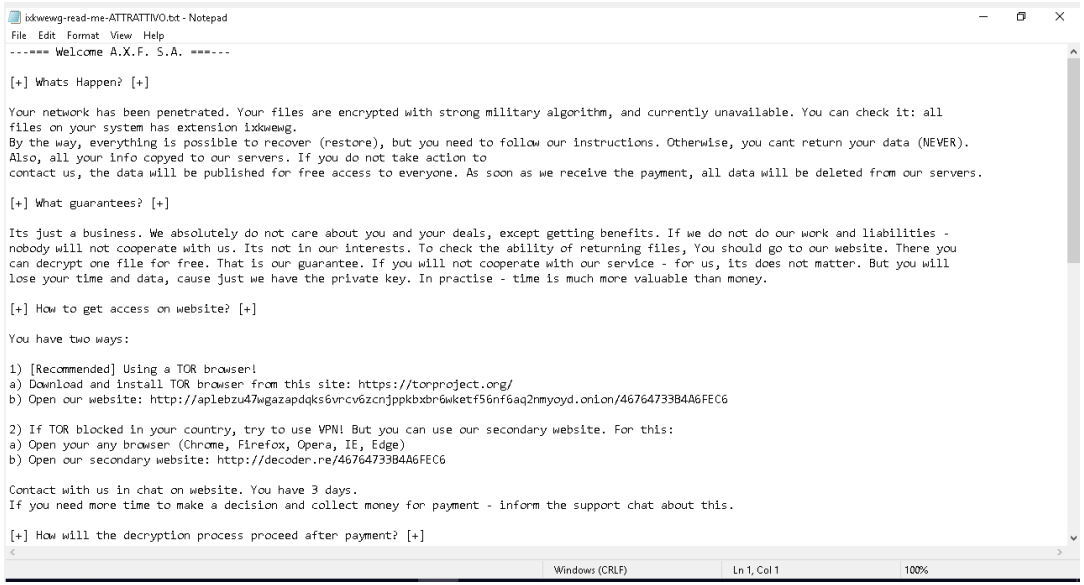
攻擊流程

電腦在感染後會迅速將檔案文件進行加密，並置換桌布告知設備已被加密勒索



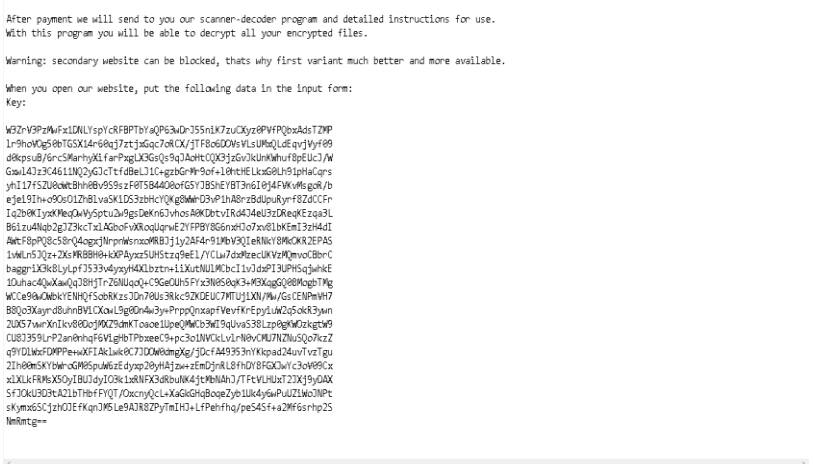
攻擊流程

被加密檔案的同資料夾內都會出現txt檔，內容為駭客的聯絡方式與付款贖金期限。



攻擊流程

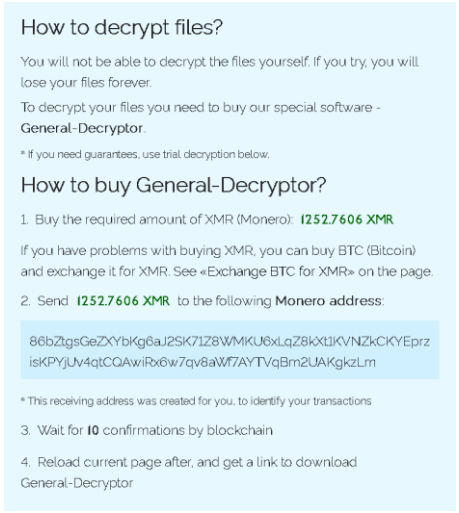
Sodinokibi提供的聯絡方式為透過洋蔥路由，連上指定的網站，再由駭客提供的金鑰登入。

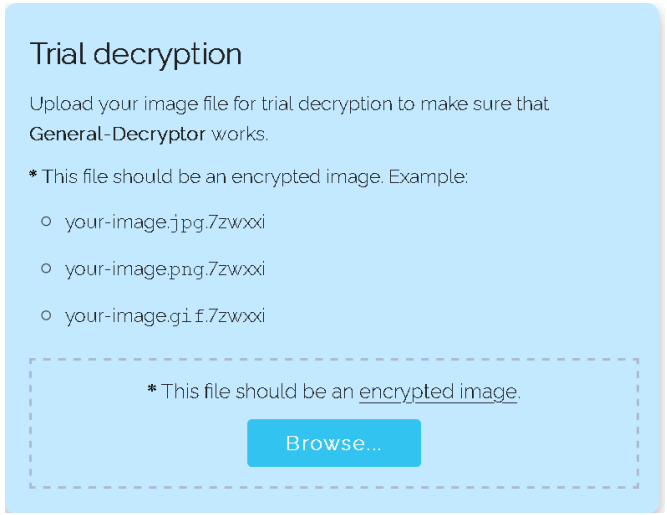


攻擊流程

進入後會告知付款金額、方式。 Sodinokibi要求付款的貨幣為門羅幣。

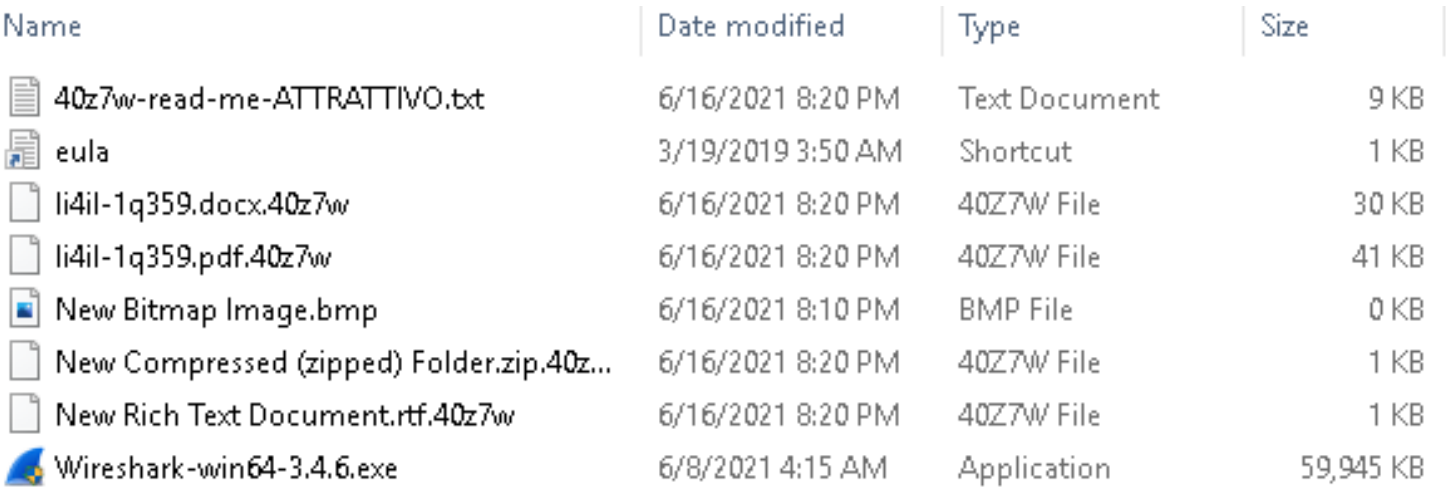
為獲得信任，提供解密測試檔給受害者使用，但限定jpg、png及gif檔。





行為分析

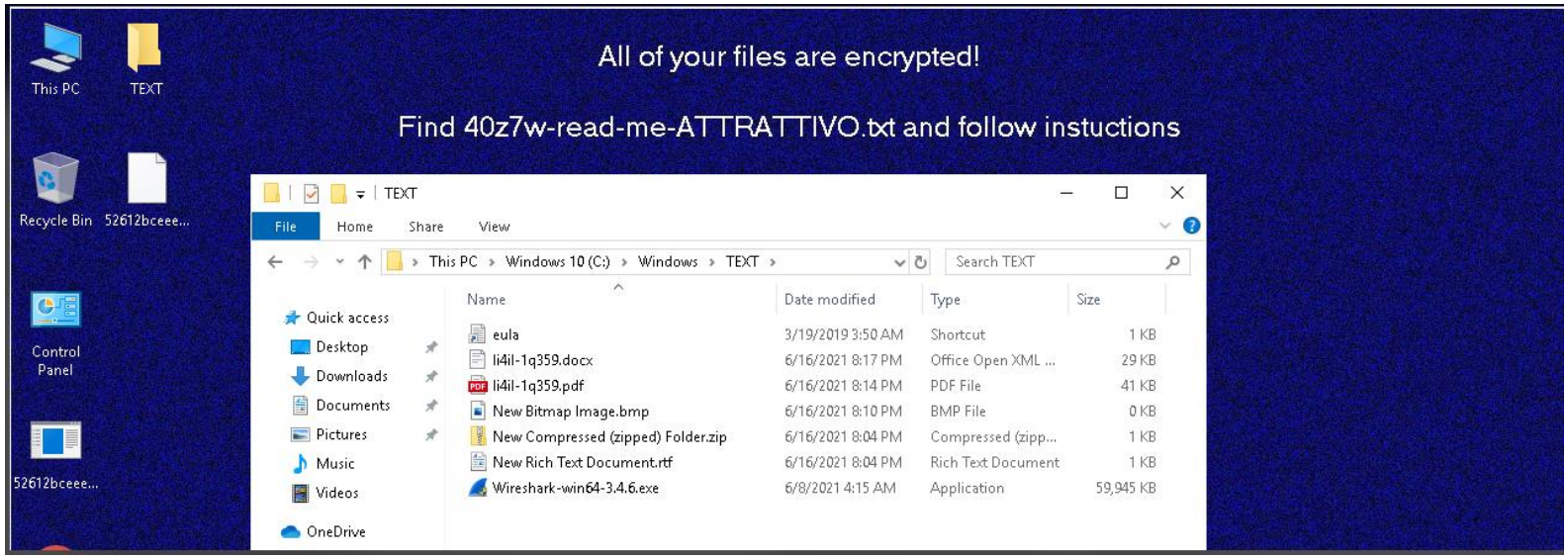
Revil加密類型有範圍，exe、bmp不進行加密，推測只對文件或壓縮檔等類型進行加密，其中文件類型的txt檔不在加密範圍中。



Name	Date modified	Type	Size
40z7w-read-me-ATTRATTIVO.txt	6/16/2021 8:20 PM	Text Document	9 KB
eula	3/19/2019 3:50 AM	Shortcut	1 KB
li4il-1q359.docx.40z7w	6/16/2021 8:20 PM	40Z7W File	30 KB
li4il-1q359.pdf.40z7w	6/16/2021 8:20 PM	40Z7W File	41 KB
New Bitmap Image.bmp	6/16/2021 8:10 PM	BMP File	0 KB
New Compressed (zipped) Folder.zip.40z...	6/16/2021 8:20 PM	40Z7W File	1 KB
New Rich Text Document.rtf.40z7w	6/16/2021 8:20 PM	40Z7W File	1 KB
Wireshark-win64-3.4.6.exe	6/8/2021 4:15 AM	Application	59,945 KB

行為分析

為確保受害者系統正常運作，Windows系統資料夾內的檔案不在病毒的加密範圍內，除此以外的資料夾皆被加密。



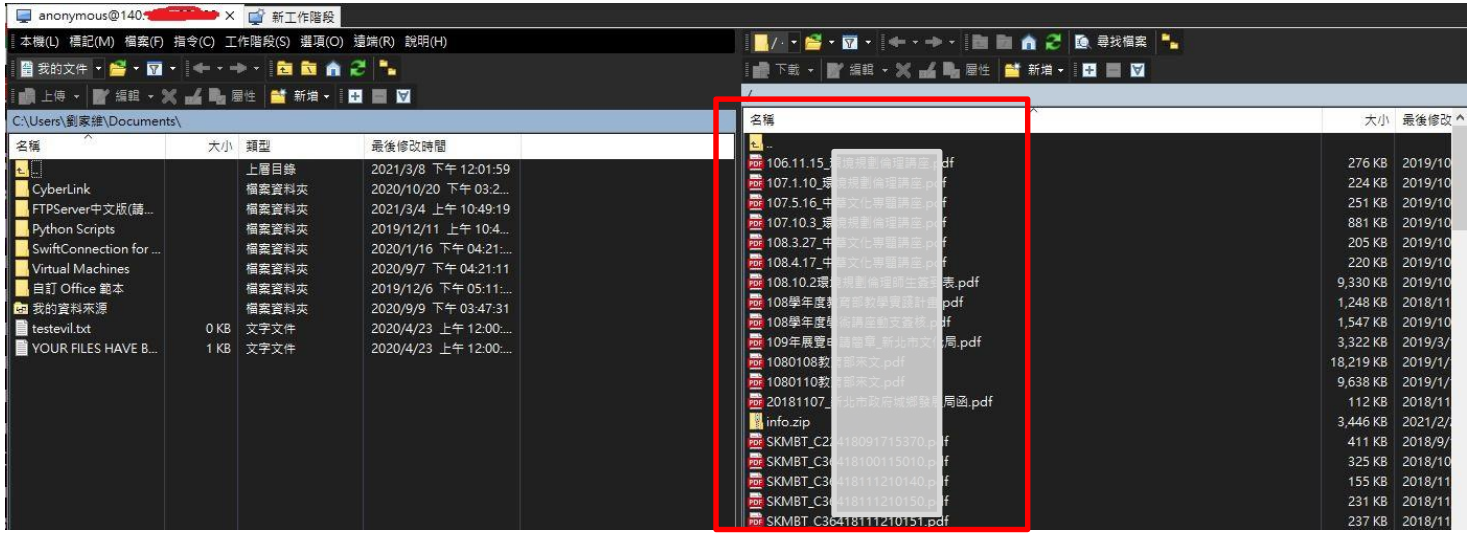
總結

- Revil在執行上相當快，虛擬環境測試約5分鐘即可完成整台電腦的加密作業，因此實際環境中可能更快
- 不只是單純對電腦進行加密勒索，感染後還會出現大量異常連線與組態管理檔案，換句話說感染後，設備會保持在攻擊者的監控管理中。
- 根據過往情資，不少被暴力破解密碼或利用漏洞植入惡意程式的方式進行攻擊。

FTP匿名登入弱點

說明

FTP匿名登入弱點經常發生於多功能事務機的掃描功能共享文件目錄，如未將該功能關閉，有心人士能夠相當輕易的存取辦公室內曾經掃描過的文件檔案，非常容易造成機敏資料外洩。

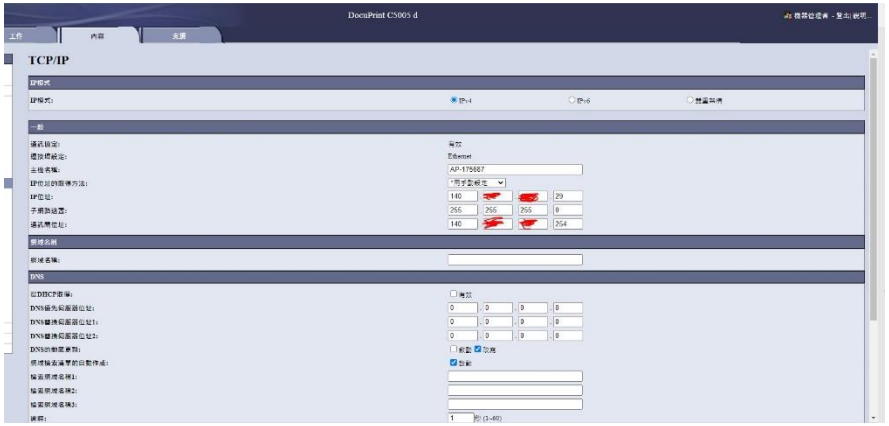


多功能事務機

說明

共享工作空間的上班文化已成為全球趨勢，網路印表機與多功能事務機已然成為辦公室不可或缺的一員

近年來網路攻擊者以漸漸將目標鎖定成這些未經控管的連網裝置。這些多功能事務機經常出現預設帳號密碼未修改的情形，使攻擊者能夠輕易地透過預設帳密接管設備。



Q & A