

區網網管會議

臺灣大學計資中心

李美雯

mli@ntu.edu.tw

3366-5010

- 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。

[illegible]

虛擬貨幣挖掘

1. 網頁劫持
2. BOTNET 散播
3. 免費共享軟體夾帶

11款免費盜版遊戲暗藏惡意挖礦軟體！全球已有22萬台PC遭感染

2021/06/28 13:40

文 / 紀善新華社



新疆屍大軍形成，Sysrc-hello殭屍網路增強C2伺服器架構使大量受害電腦成為宿主，以擴展感染規模

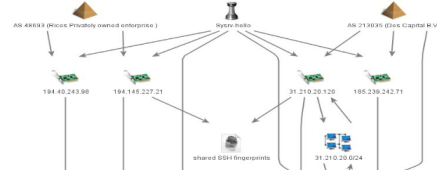
Sysrc-hello利用漏洞欺騙惡意挖礦工具，而資安業者Lackwork發現其基礎架構，多了幾個新的C2伺服器，讓感染的規模擴張。

文 / 莊念恩 | 2021-04-27 發表

讚 9.7 萬

按讚加入iThome粉絲團

讚 2 分享

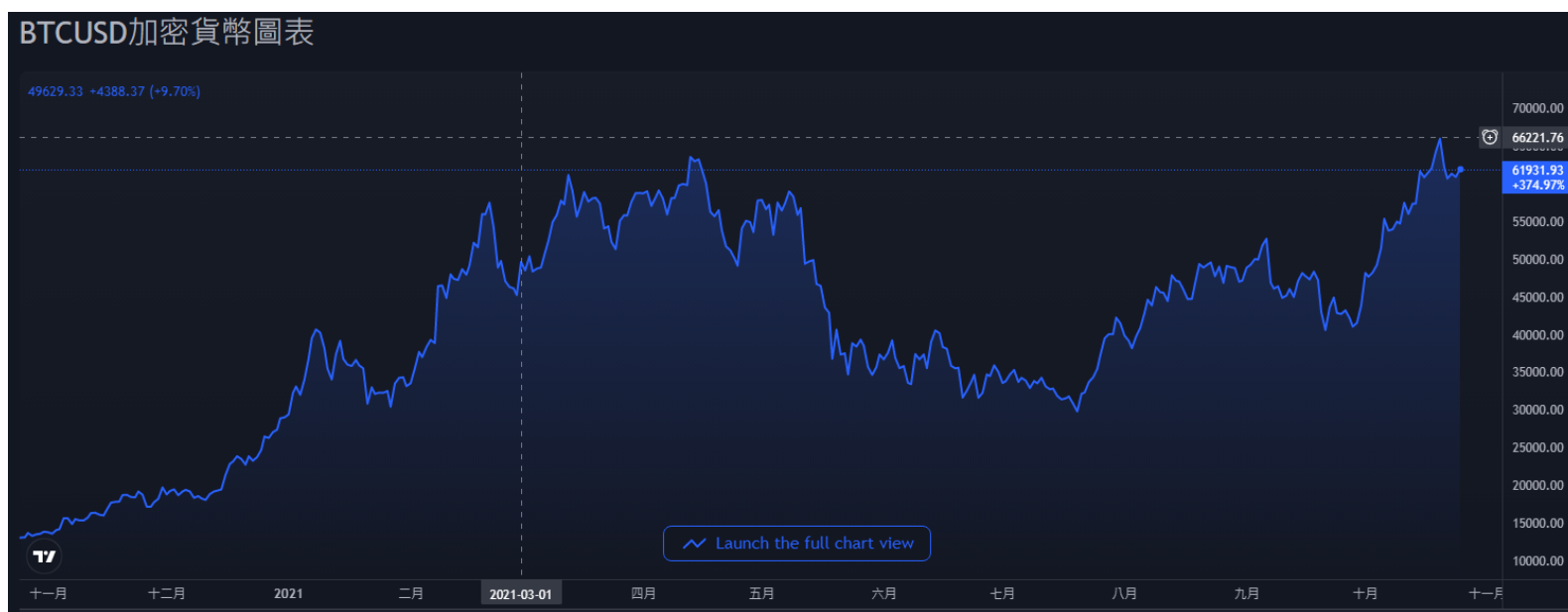


Openfind

揭露企業面臨資安危機
解析 2021 最新威脅攻擊手法

免費報告下載

比特幣 幣值變化



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。

Your network has been infected!



Your documents, photos,
databases and other important files
encrypted



To decrypt your files you need to
buy our special software -
General-Decryptor

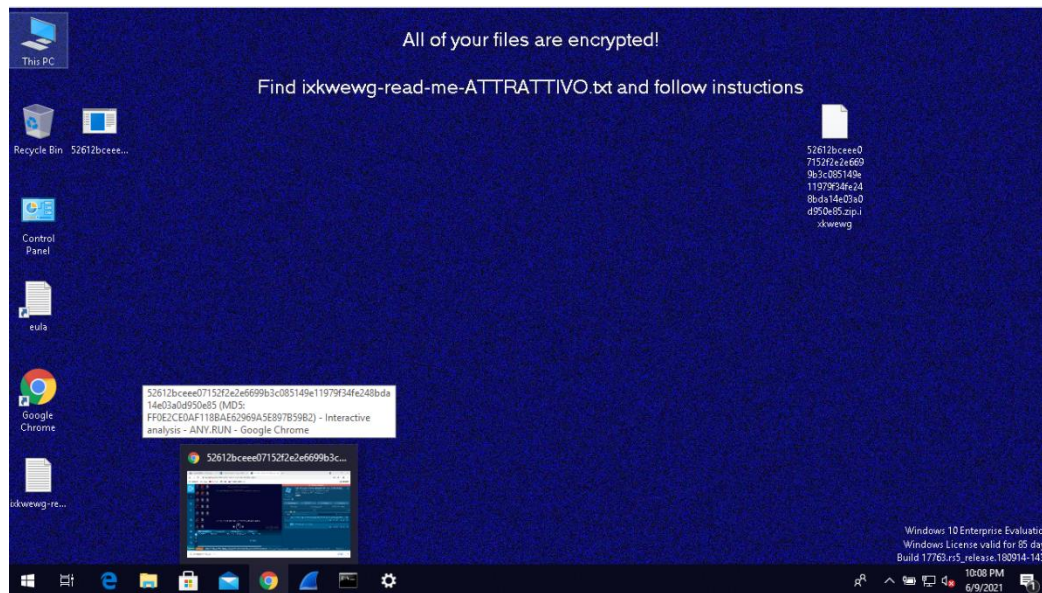


Follow the instructions below.
But remember that you do not
have much time

General-Decryptor price
the price is for all PCs of your infected network

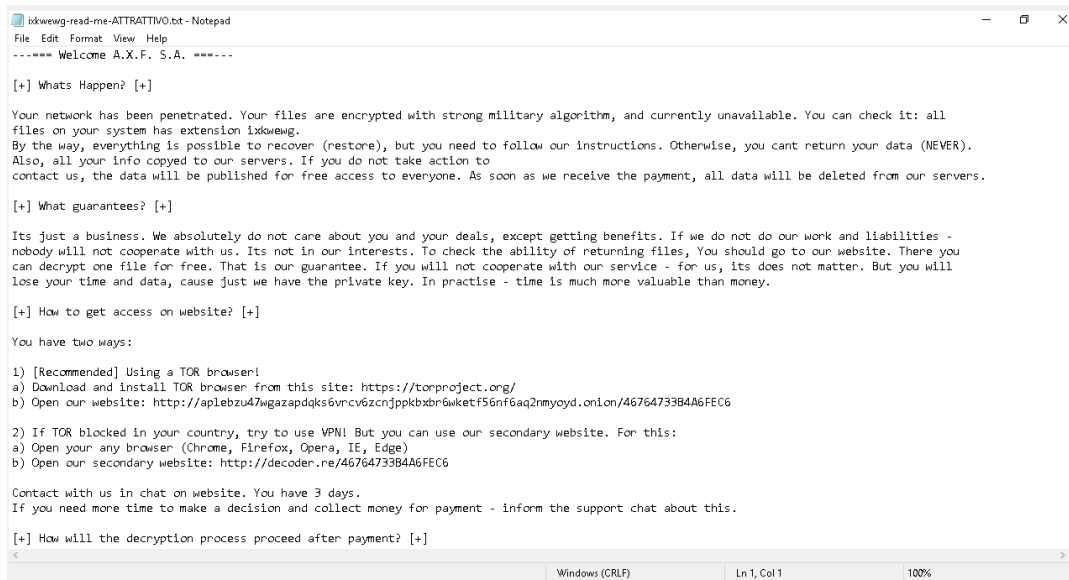
攻擊流程

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。



tkxwewg-read-me-ATTRATTIVO.txt - Notepad

File Edit Format View Help

----- Welcome A.X.F. S.A. -----

[+] Whats Happen? [+]

Your network has been penetrated. Your files are encrypted with strong military algorithm, and currently unavailable. You can check it: all files on your system has extension tkxwewg.

By the way, everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER). Also, all your info copied to our servers. If you do not take action to contact us, the data will be published for free access to everyone. As soon as we receive the payment, all data will be deleted from our servers.

[+] What guarantees? [+]

Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests. To check the ability of returning files, You should go to our website. There you can decrypt one file for free. That is our guarantee. If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data, cause just we have the private key. In practise - time is much more valuable than money.

[+] How to get access on website? [+]

You have two ways:

- 1) [Recommended] Using a TOR browser!
 - a) Download and install TOR browser from this site: <https://torproject.org/>
 - b) Open our website: <http://aplebz47wgazapdqks6vrcv6zcnjppkxbzbr6uketf56nf6aq2nmyoyd.onion/46764733B4A6FEC6>
- 2) If TOR blocked in your country, try to use VPN! But you can use our secondary website. For this:
 - a) Open your any browser (Chrome, Firefox, Opera, IE, Edge)
 - b) Open our secondary website: <http://decoder.re/46764733B4A6FEC6>

Contact with us in chat on website. You have 3 days.

If you need more time to make a decision and collect money for payment - inform the support chat about this.

[+] How will the decryption process proceed after payment? [+]

Windows (CRLF) Ln 1, Col 1 100%

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。



After payment we will send to you our scanner-decoder program and detailed instructions for use. With this program you will be able to decrypt all your encrypted files.

Warning: secondary website can be blocked, thats why first variant much better and more available.

When you open our website, put the following data in the input form:
Key:

```
M3ZrV3PzMuFzLdL1SpYcrFBPTbYqP63wDr355nLKZuXyZ8VFPQbzAd5TZMP  
1r9hWkgs6bTGSX14r68qj7ztj46q7d8CX/jTF8o6DO0sVLsUhsQLeqvjYyF89  
d8kpsuB/r6rc5MarhyX1farpagUXGq(q9q)AahrCQX3j36vUkUnWhuF8pUcJ/W  
GawL47ezC46LWQ2yGJctf4bdeJ1L+ggtB6rPp9of+L8rthE1ka68U9Iphlqns  
yH1L7528R6eBvHbV55zrF8T84A000rG57B5HrBT3h6d18j4FWvWgq/b  
eJelS1wv90u0L2hB1vaSKLDS3zbHCYQg8MwD9p1hA8rzbdluRyfr8ZC0Fr  
1q2bK1YskMeqUvY5ptu3u9gsDekn63vho5AK0BtVtRd434eU3tDReqE2qa3L  
B61zu4Mq2g7Z3kcTxlAGbofv8KodUqWz2YFPBY8G6n607zu6LbEmJ3zh4dJ  
AhtF8pQ8c58rQ4agzjNpnlw5n0z9B3j1y2Af4r9LMbV3QTeRNeY8McK8ZEPAS  
1wLrn53ze2x5rR8Bh6+XAP4yaz5UH5tazqfeL1YCLu7daPecUkVzWQmvoCBbrC  
bagger1X3k8LylpF35354y9yH4X1bzt+11KutNULWbcl1vdapE13UPH5qJmKE  
12uhac4QwKwQ38hJ7T26WuqQ4c36e0h5F7x3H05RqK3+H3XagG8B8qgB7Mg  
Wc99uA8wF8Wq5c8kz3Dn79u38kc92K0EUC7MTU1LW/mw/c5CEHmH7  
B8Q3kx9d8u8nBVL0xwL9g8On43yPp9p0naxFVevrK6EpyLwQ25k83yjn  
2UX7wXnX1ev88Q3J9C25dmKT0aoc1UpeQW6b3hL9q4v53BLz28qW0ZkgcW9  
CUB1359LrP2an8thqF6VLghBTp0zeec3p3c3oUWCKLvLWbV0U7N2h5Q0ezZ  
q9YDLwzOPPPewXFLAclw8C7J0DM8mgKj/JDcfAA9353nYKkapad24uvtvzTgu  
21h885K7bWcGR85puWzE dyap28yH4jzpwzEmDjnkL8HDY8FGQ3w/c3oh95Cz  
xLALFmX50y1BU0y10KcLxNFK38b0uW43P6b0hJ/TFeVLHut23X39yJAA  
5F2K4u802uL2h7hFVQ7/Oacm9QcLxK6g8q8qez2y8Ukdy8PuJ2h3z  
skYm655Cj2h03EfkqJMSLe9ALN27y7mZHvLFPehfajpeS4Sf+a2M66srhp25  
m8mtg==
```

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。

How to decrypt files?

You will not be able to decrypt the files yourself. If you try, you will lose your files forever.

To decrypt your files you need to buy our special software - **General-Decryptor**.

* If you need guarantees, use trial decryption below.

How to buy General-Decryptor?

1. Buy the required amount of XMR (Monero): **I252.7606 XMR**

If you have problems with buying XMR, you can buy BTC (Bitcoin) and exchange it for XMR. See «Exchange BTC for XMR» on the page.

2. Send **I252.7606 XMR** to the following Monero address:

```
86b2gsGeZXYbKg6aJ2SK71Z8WMKU6xLqZ8kXt1KVNZkCKYEprz  
isKPYjUV4qtCQAwifRw7qv8aWf7AYTVqBm2UAKgzLm
```

* This receiving address was created for you, to identify your transactions

3. Wait for **10** confirmations by blockchain

4. Reload current page after, and get a link to download General-Decryptor

Trial decryption

Upload your image file for trial decryption to make sure that **General-Decryptor** works.

* This file should be an encrypted image. Example:

- o your-image.jpg.7zwxixi
- o your-image.png.7zwxixi
- o your-image.gif.7zwxixi

* This file should be an encrypted image.

Browse...

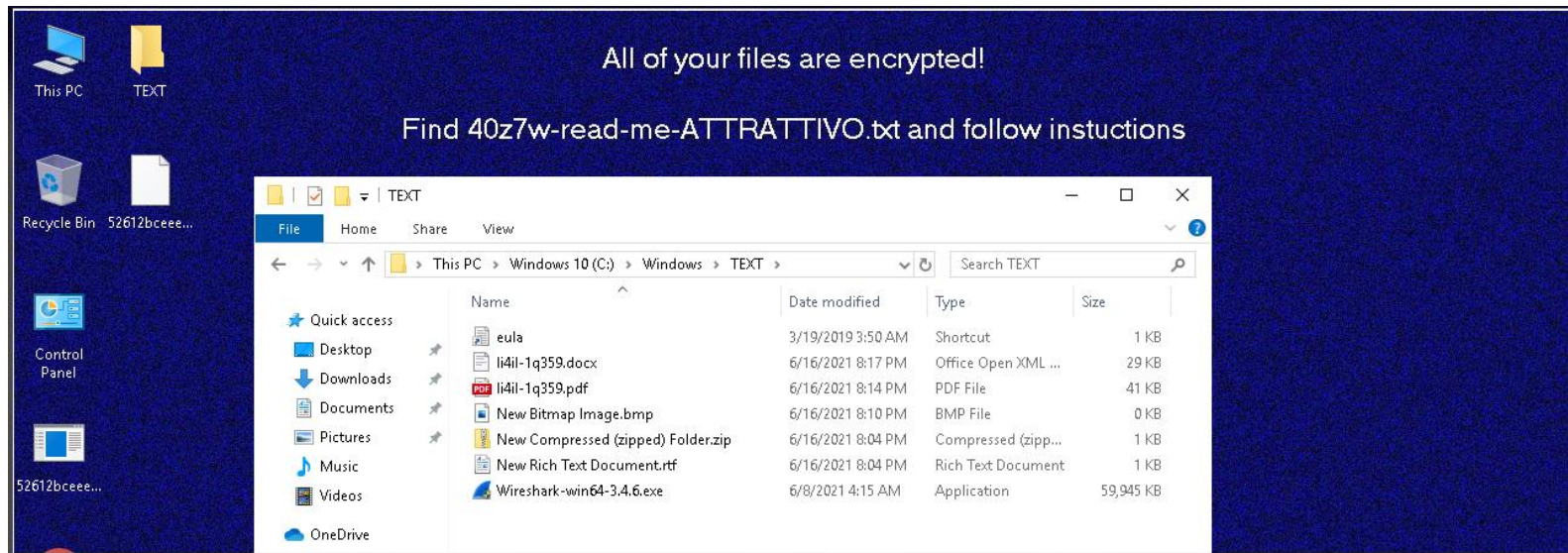
行為分析

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



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。



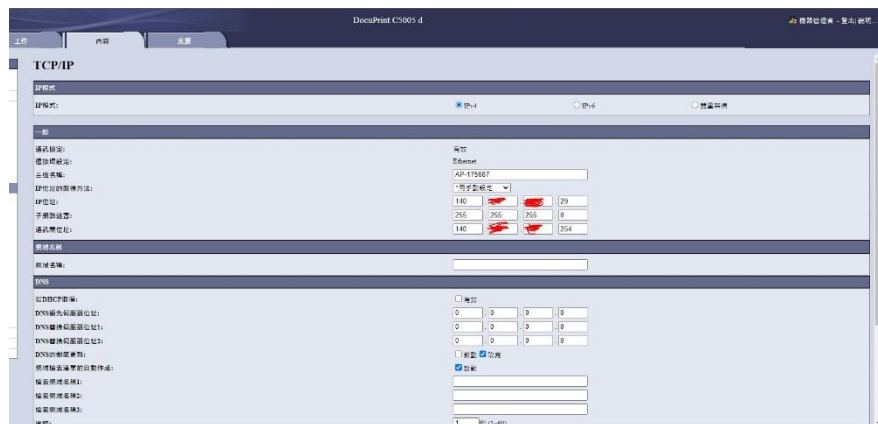
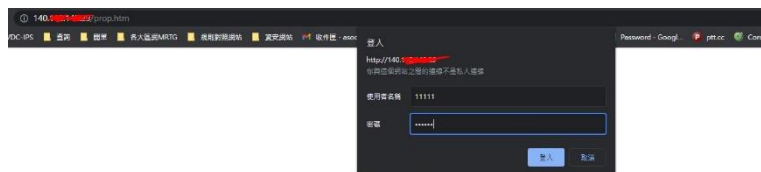
多功能事務機



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