個案分析-

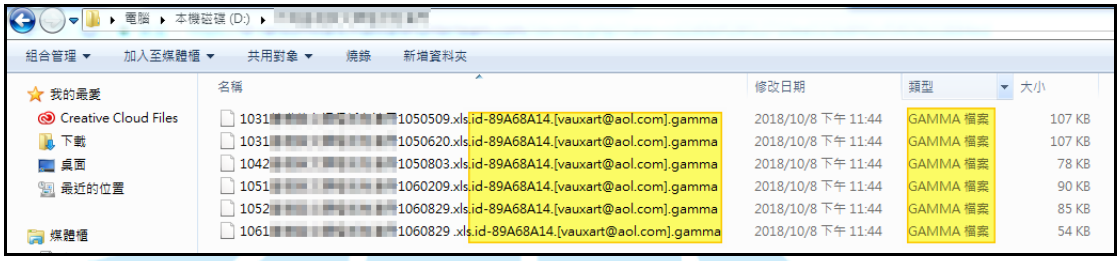
校園勒索恐嚇信與勒索病毒攻擊事件分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

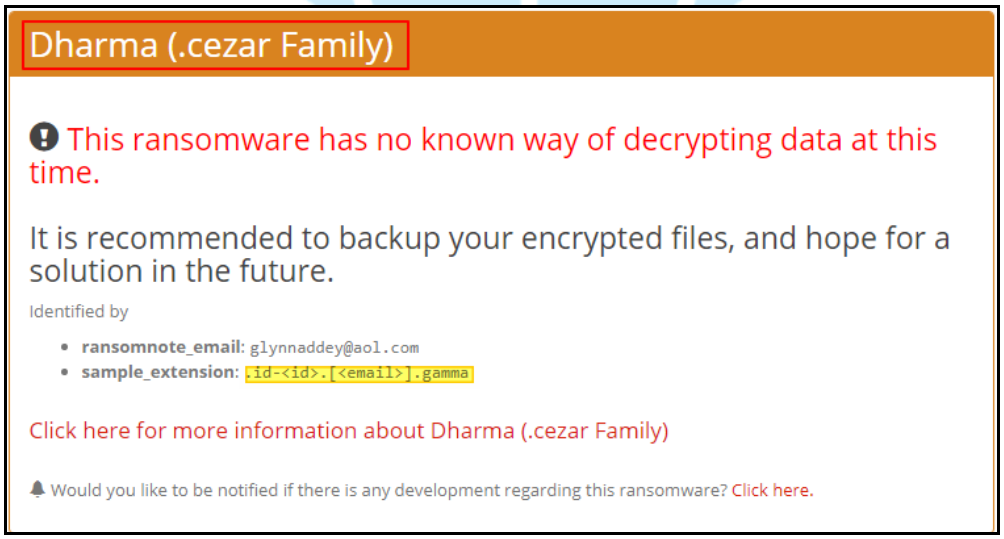
107 年 11 月

I. 事件簡介

1. 在 107 年 9-10 月學術網路中發生勒索恐嚇信事件與副檔名 Gamma 勒索病毒攻擊事件，而本中心同仁在 10 月底也陸續收到這類型勒索恐嚇信。
2. 某校園主機感染副檔名為 Gamma 的勒索病毒，受害主機內的資料皆已被加密，所幸該主機為工讀生用電腦，平時所用資料皆已有備份，影響不大，又該系統裝設還原卡，在感染病毒後重新開機，已清除病毒。



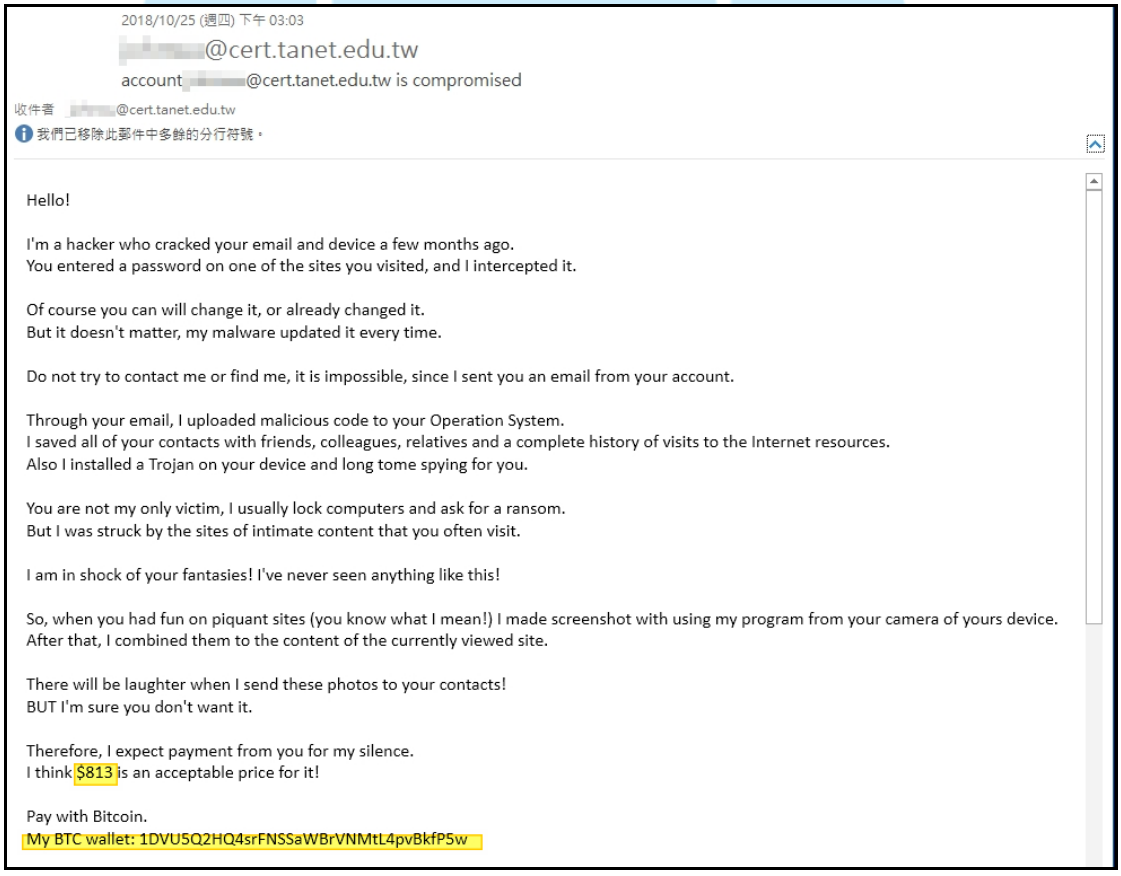
3. 因受害主機系統碟已系統還原，透過 D 槽被加密的檔案與勒索通知信，經查.Gamma 的勒索病毒來自 Dharma(CrySiS)勒索病毒家族，Dharma 病毒為 2018 年前三大勒索病毒家族之一，此類型的勒索病毒每隔幾個星期就會有新變種產生，各變種之間的差異在於副檔名與聯絡用的 E-mail 信箱不同，其他特徵皆相同。



4. 為了解勒索恐嚇信在開啟後對主機是否有任何系統行為與網路行為產生，又為了解 Dharma 勒索病毒在感染主機後之網路行為與系統行為，本中心取得勒索恐嚇信樣本與 Dharma 勒索病毒樣本進行檢測。

II. 事件檢測

1. 首先使用 1 台安裝 Windows 7 系統的 VM 虛擬主機進行隔離環境測試。本中心總共收到四份勒索恐嚇信，將陸續對這四份勒索恐嚇信件進行檢測。
2. 檢測 107 年 10 月 25 日下午 3:03 收到主旨為「account XXXX@cert.tanet.edu.tw is compromised」之恐嚇信，發現在該信開啟後主機並無任何異樣，而使用者所用帳號也無異常。駭客為讓受害者相信已取得受害者的帳號，以受害者的帳號為寄件者寄信給受害者，但檢視信件來源 IP 為來自法國 IP:81.66.24.250。在信件中駭客告訴受害者已掌握帳戶密碼、瀏覽器的歷史紀錄與通聯紀錄等資料，並告訴受害者需於 48 小時內付美金 813 元，否則將會寄受害者瀏覽色情網站的表情照片寄給受害者的親朋好友。



2018/10/25 (週四) 下午 03:03
[redacted]@cert.tanet.edu.tw
account [redacted]@cert.tanet.edu.tw is compromised
收件者 [redacted]@cert.tanet.edu.tw
我們已移除此郵件中多餘的分行符號。

Hello!

I'm a hacker who cracked your email and device a few months ago.
You entered a password on one of the sites you visited, and I intercepted it.

Of course you can will change it, or already changed it.
But it doesn't matter, my malware updated it every time.

Do not try to contact me or find me, it is impossible, since I sent you an email from your account.

Through your email, I uploaded malicious code to your Operation System.
I saved all of your contacts with friends, colleagues, relatives and a complete history of visits to the Internet resources.
Also I installed a Trojan on your device and long tome spying for you.

You are not my only victim, I usually lock computers and ask for a ransom.
But I was struck by the sites of intimate content that you often visit.

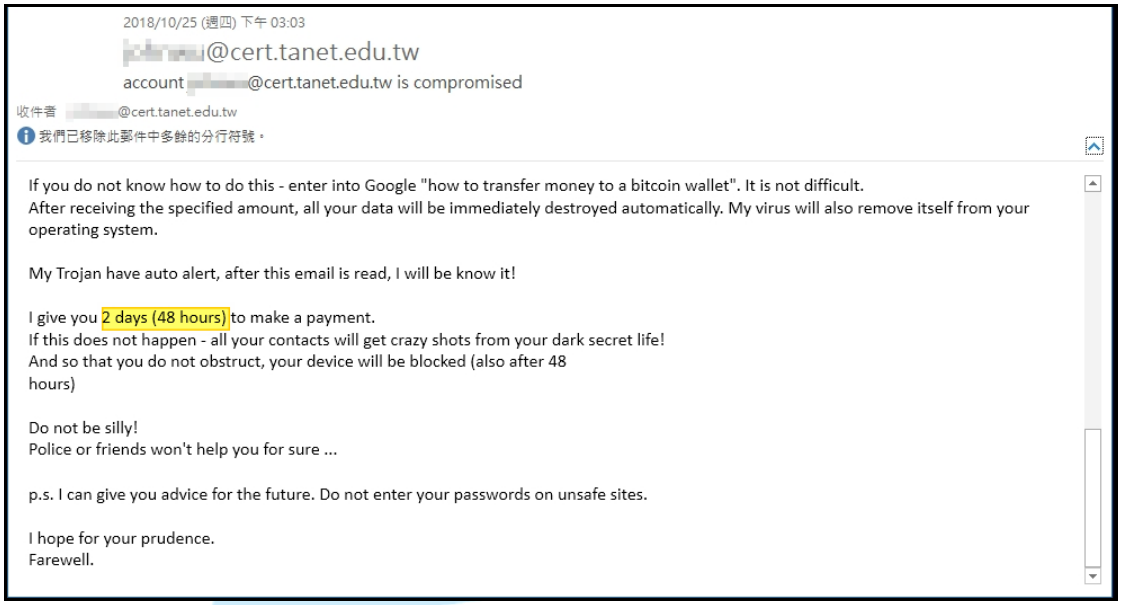
I am in shock of your fantasies! I've never seen anything like this!

So, when you had fun on piquant sites (you know what I mean!) I made screenshot with using my program from your camera of yours device.
After that, I combined them to the content of the currently viewed site.

There will be laughter when I send these photos to your contacts!
BUT I'm sure you don't want it.

Therefore, I expect payment from you for my silence.
I think $813 is an acceptable price for it!

Pay with Bitcoin.
My BTC wallet: 1DVU5Q2HQ4srFNSSaWBrVNMtL4pvBkfP5w


2018/10/25 (週四) 下午 03:03
@cert.tanet.edu.tw
account @cert.tanet.edu.tw is compromised
收件者 @cert.tanet.edu.tw
我們已移除此郵件中多餘的分行符號。

If you do not know how to do this - enter into Google "how to transfer money to a bitcoin wallet". It is not difficult.
After receiving the specified amount, all your data will be immediately destroyed automatically. My virus will also remove itself from your operating system.

My Trojan have auto alert, after this email is read, I will be know it!

I give you 2 days (48 hours) to make a payment.
If this does not happen - all your contacts will get crazy shots from your dark secret life!
And so that you do not obstruct, your device will be blocked (also after 48 hours)

Do not be silly!
Police or friends won't help you for sure ...

p.s. I can give you advice for the future. Do not enter your passwords on unsafe sites.

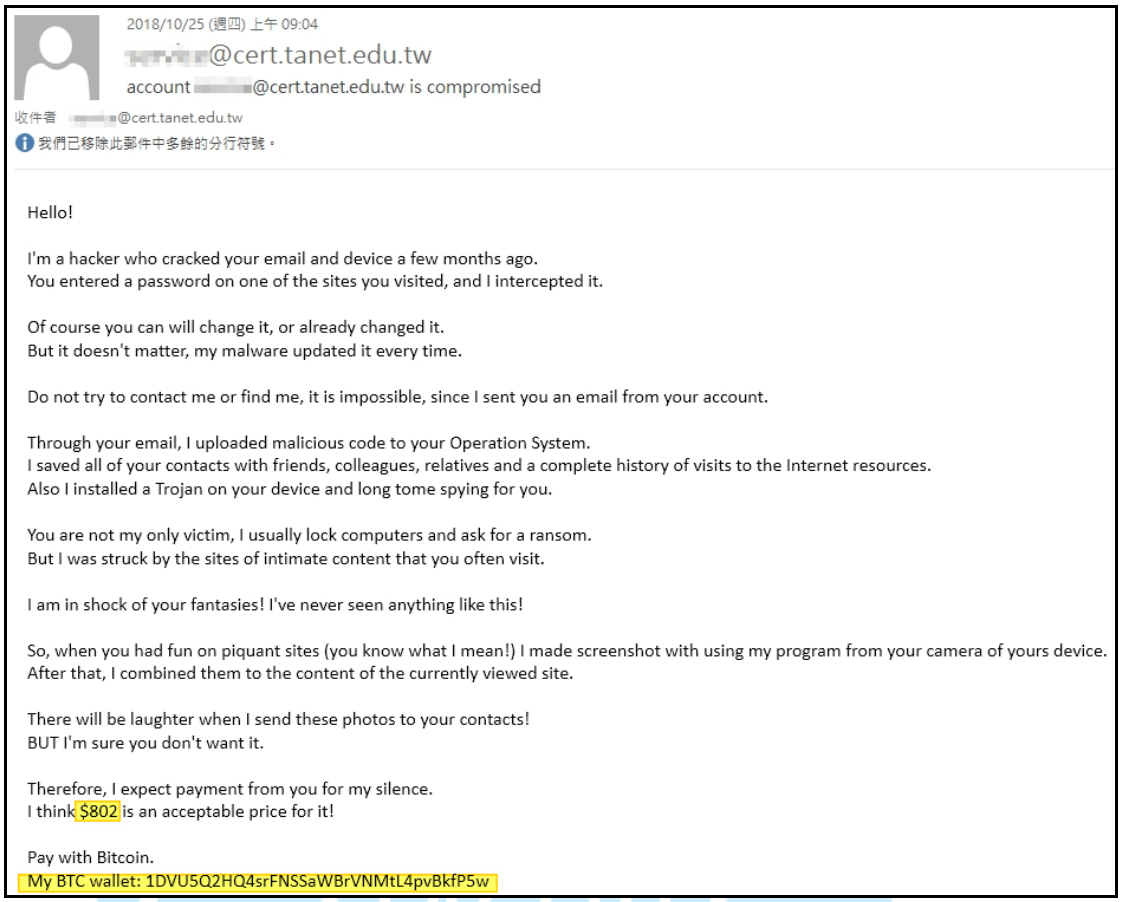
I hope for your prudence.
Farewell.


From: <@cert.tanet.edu.tw>
To: <@cert.tanet.edu.tw>
Subject: account @cert.tanet.edu.tw is compromised
Date: Thu, 25 Oct 2018 15:03:21 +0800
Message-ID: <587F0F47DC283794B3C38B10E4FB587F@29DLUNI29D>
MIME-Version: 1.0


網際網路標題(H)

Received: from 81-66-24-250.rev.numericable.fr (81-66-24-250.rev.numericable.fr [81.66.24.250])
by cert.tanet.edu.tw (Postfix) with ESMTP id 3B41850BB400
for <@cert.tanet.edu.tw>; Thu, 25 Oct 2018 13:24:49 +0800 (CST)
From: <@cert.tanet.edu.tw>

3. 檢測 107 年 10 月 25 日上午 9:04 收到主旨為「account XXXX@cert.tanet.edu.tw is compromised」之恐嚇信，發現在該信開啟後主機並無任何異樣，而使用者所用帳號也無異常。檢視信件來源 IP 為來自智利的 IP:186.156.236.214，而信件內容與前一封檢測之恐嚇信無異，僅索求付款金額不同。



2018/10/25 (週四) 上午 09:04
[redacted]@cert.tanet.edu.tw
account [redacted]@cert.tanet.edu.tw is compromised
收件者 [redacted]@cert.tanet.edu.tw
我們已移除此郵件中多餘的分行符號。

Hello!

I'm a hacker who cracked your email and device a few months ago.
You entered a password on one of the sites you visited, and I intercepted it.

Of course you can will change it, or already changed it.
But it doesn't matter, my malware updated it every time.

Do not try to contact me or find me, it is impossible, since I sent you an email from your account.

Through your email, I uploaded malicious code to your Operation System.
I saved all of your contacts with friends, colleagues, relatives and a complete history of visits to the Internet resources.
Also I installed a Trojan on your device and long tome spying for you.

You are not my only victim, I usually lock computers and ask for a ransom.
But I was struck by the sites of intimate content that you often visit.

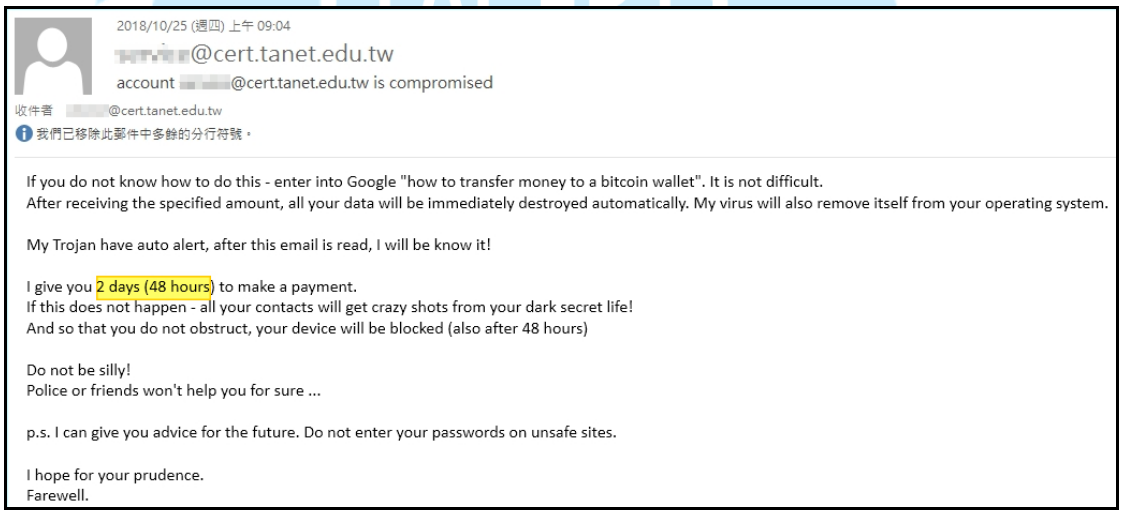
I am in shock of your fantasies! I've never seen anything like this!

So, when you had fun on piquant sites (you know what I mean!) I made screenshot with using my program from your camera of yours device.
After that, I combined them to the content of the currently viewed site.

There will be laughter when I send these photos to your contacts!
BUT I'm sure you don't want it.

Therefore, I expect payment from you for my silence.
I think $802 is an acceptable price for it!

Pay with Bitcoin.
My BTC wallet: 1DVU5Q2HQ4srFNSSaWBrVNMtL4pvBkfP5w



2018/10/25 (週四) 上午 09:04
[redacted]@cert.tanet.edu.tw
account [redacted]@cert.tanet.edu.tw is compromised
收件者 [redacted]@cert.tanet.edu.tw
我們已移除此郵件中多餘的分行符號。

If you do not know how to do this - enter into Google "how to transfer money to a bitcoin wallet". It is not difficult.
After receiving the specified amount, all your data will be immediately destroyed automatically. My virus will also remove itself from your operating system.

My Trojan have auto alert, after this email is read, I will be know it!

I give you 2 days (48 hours) to make a payment.
If this does not happen - all your contacts will get crazy shots from your dark secret life!
And so that you do not obstruct, your device will be blocked (also after 48 hours)

Do not be silly!
Police or friends won't help you for sure ...

p.s. I can give you advice for the future. Do not enter your passwords on unsafe sites.

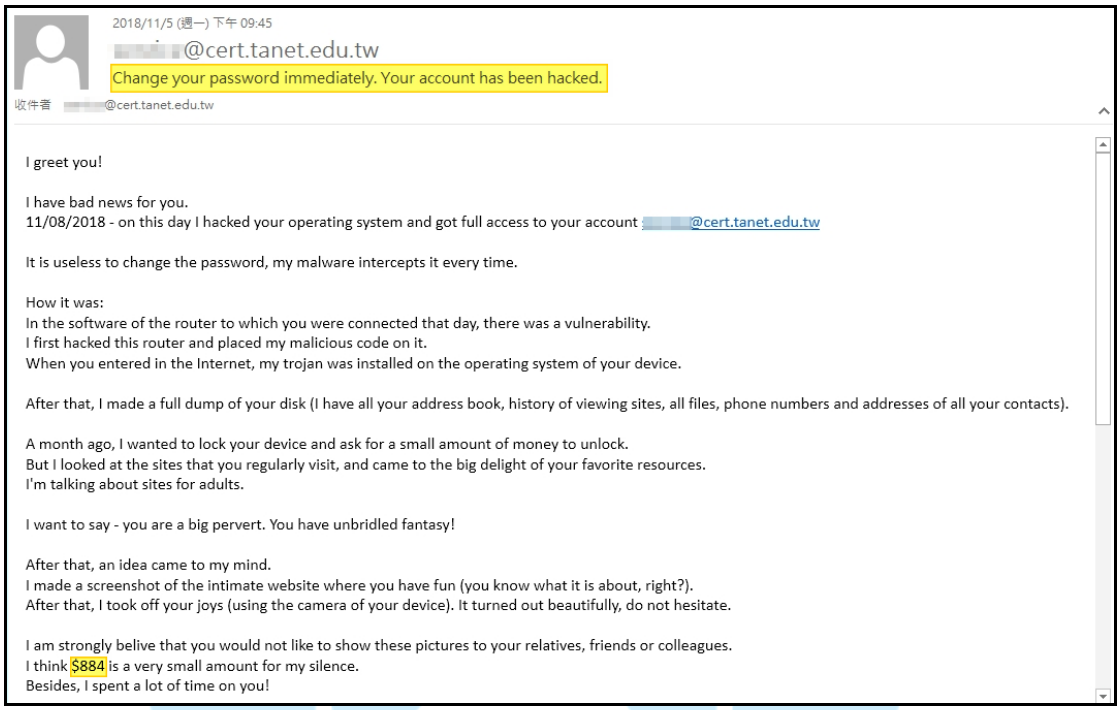
I hope for your prudence.
Farewell.

網際網路標題(H)

Return-Path: <[redacted]@cert.tanet.edu.tw>
X-Original-To: [redacted]@cert.tanet.edu.tw
Delivered-To: [redacted]@cert.tanet.edu.tw
Received: from dvc-214-236-156-186.movil.vtr.net
(dvc-214-236-156-186.movil.vtr.net [186.156.236.214])
by cert.tanet.edu.tw (Postfix) with ESMTP id
F1BFB50BB402

4. 檢測 107 年 11 月 5 日下午 9:45 收到主旨為「Change your password immediately. Your account has been hacked」之恐嚇信，發現在該信開啟後主機並無任何異

樣，而使用者所用帳號也無異常。檢視信件來源 IP 為來自越南的 IP:116.107.191.207，而信件內容提到在 2018 年 8 月 11 日駭客已經駭入受害者主機，並且能完整存取 E-mail 帳號，要求受害者在 50 小時內支付美金 884 元，否則受害主機將會被鎖住，而受害者的親朋好友將會收到受害者瀏覽色情網站的表情照片。



2018/11/5 (週一) 下午 09:45
@cert.tanet.edu.tw
Change your password immediately. Your account has been hacked.
收件者 @cert.tanet.edu.tw

I greet you!

I have bad news for you.
11/08/2018 - on this day I hacked your operating system and got full access to your account @cert.tanet.edu.tw

It is useless to change the password, my malware intercepts it every time.

How it was:
In the software of the router to which you were connected that day, there was a vulnerability.
I first hacked this router and placed my malicious code on it.
When you entered in the Internet, my trojan was installed on the operating system of your device.

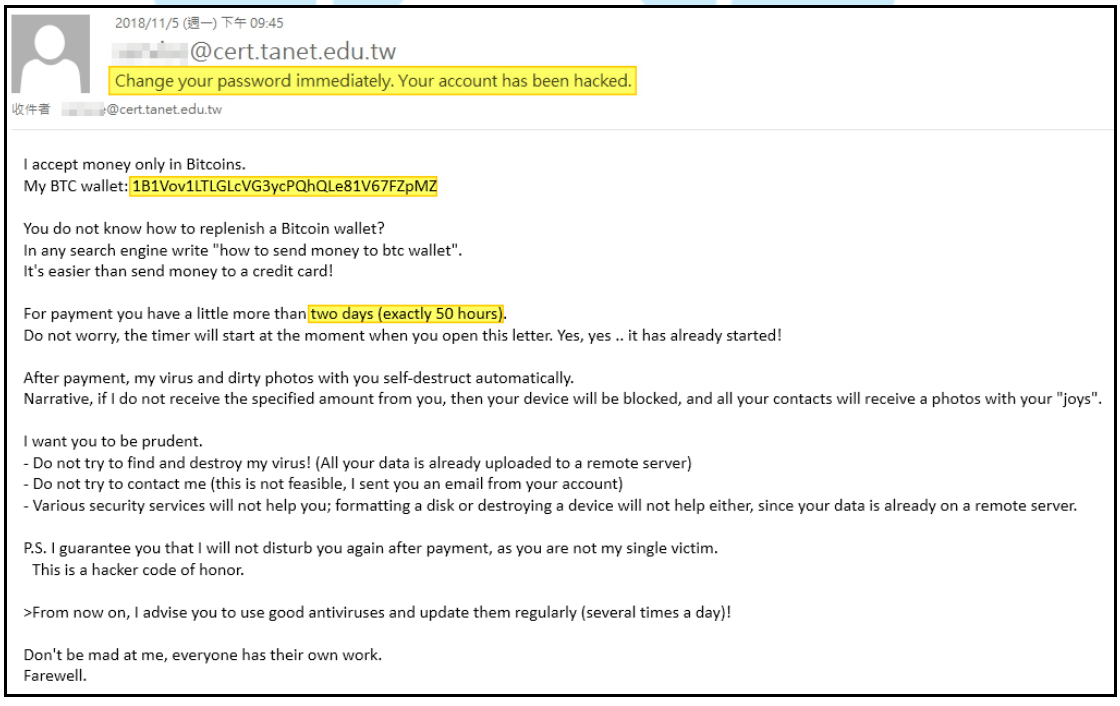
After that, I made a full dump of your disk (I have all your address book, history of viewing sites, all files, phone numbers and addresses of all your contacts).

A month ago, I wanted to lock your device and ask for a small amount of money to unlock.
But I looked at the sites that you regularly visit, and came to the big delight of your favorite resources.
I'm talking about sites for adults.

I want to say - you are a big pervert. You have unbridled fantasy!

After that, an idea came to my mind.
I made a screenshot of the intimate website where you have fun (you know what it is about, right?).
After that, I took off your joys (using the camera of your device). It turned out beautifully, do not hesitate.

I am strongly belive that you would not like to show these pictures to your relatives, friends or colleagues.
I think $884 is a very small amount for my silence.
Besides, I spent a lot of time on you!



2018/11/5 (週一) 下午 09:45
@cert.tanet.edu.tw
Change your password immediately. Your account has been hacked.
收件者 @cert.tanet.edu.tw

I accept money only in Bitcoins.
My BTC wallet: 1B1Vov1LTLGLcVG3ycPQhQLe81V67FZpMZ

You do not know how to replenish a Bitcoin wallet?
In any search engine write "how to send money to btc wallet".
It's easier than send money to a credit card!

For payment you have a little more than two days (exactly 50 hours).
Do not worry, the timer will start at the moment when you open this letter. Yes, yes .. it has already started!

After payment, my virus and dirty photos with you self-destruct automatically.
Narrative, if I do not receive the specified amount from you, then your device will be blocked, and all your contacts will receive a photos with your "joys".

I want you to be prudent.
- Do not try to find and destroy my virus! (All your data is already uploaded to a remote server)
- Do not try to contact me (this is not feasible, I sent you an email from your account)
- Various security services will not help you; formatting a disk or destroying a device will not help either, since your data is already on a remote server.

P.S. I guarantee you that I will not disturb you again after payment, as you are not my single victim.
This is a hacker code of honor.

>From now on, I advise you to use good antiviruses and update them regularly (several times a day)!

Don't be mad at me, everyone has their own work.
Farewell.

5. 檢測 107 年 10 月 31 日上午 4:32 收到主旨為「あなたのパスワードが侵害されました (XXXXX@cert.tanet.edu.tw)」之恐嚇信，發現在該信開啟後主機並無任何異樣，而使用者所用帳號也無異常。檢視信件來源 IP 為來自哥倫比亞的 IP: 201.184.248.210，而信件內容提到在數個月前駭客已經駭入受害者主機，並且破解受害者 E-mail 帳號密碼，要求受害者在 48 小時內支付美金 842 元，否則受害主機將會被鎖住，而受害者的親朋好友將會收到受害者瀏覽色情網站的表情照片。

2018/10/31 (週三) 上午 04:32
[redacted]@cert.tanet.edu.tw
あなたのパスワードが侵害されました ([redacted]@cert.tanet.edu.tw)
收件者 [redacted]@cert.tanet.edu.tw

Bitcoin 経由で支払う。
私の BTC ウォレット：1JDi4GbHUzCrrnT7BCYbnsyLyrFpNK7faP

あなたがこれを行う方法を知らない場合 - Google に「BTC ウォレットに送金する方法」を入力します。難しくない。
指定された金額を受け取ると、妥協しているすべての材料は自動的に破壊されます。私のウイルスはあなた自身のオペレーティングシステムからも削除されます。

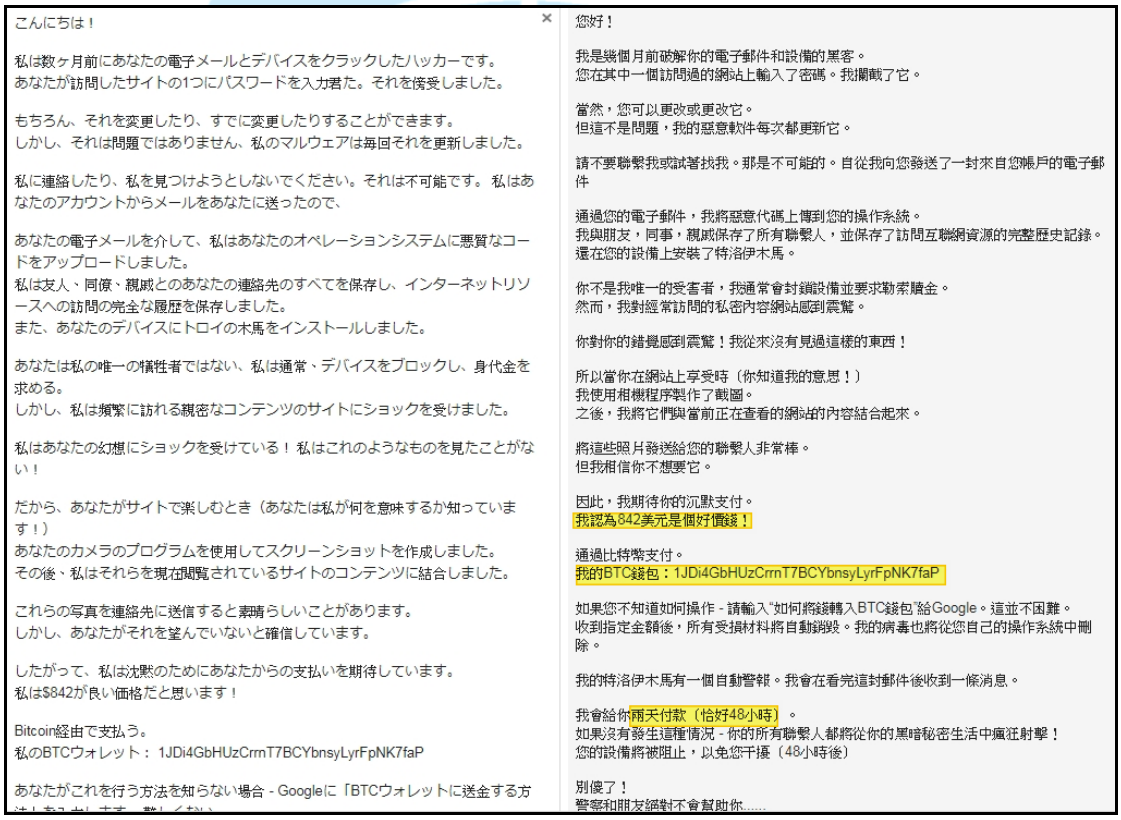
私のトロイの木馬は自動アラートを持っています。私はこのメールを読んだ後でメッセージを受け取ります。

私はあなたに支払いのための2 日間を与える（正確に 48 時間）。
これが起こらない場合 - すべてのあなたの連絡先はあなたの暗い秘密の生活からクレイジーショットを取得します！
あなたが妨害しないように、あなたのデバイスはブロックされます（また、48 時間後）

ばかなことしないで！
警察や友人はあなたを確実に助けません...

p.s. 私はあなたに将来のアドバイスを与えることができます。安全でないサイトにはパスワードを入力しないでください。

私はあなたの慎重さを願っています。
お別れ。



こんにちは！

私は数ヶ月前にあなたの電子メールとデバイスをクラックしたハッカーです。
あなたが訪問したサイトの1つにパスワードを入力君た。それを傍受しました。

もちろん、それを変更したり、すでに変更したりすることができます。
しかし、それは問題ではありません、私のマルウェアは毎回それを更新しました。

私に連絡したり、私を見つけようとしないでください。それは不可能です。 私はあなたのアカウントからメールをあなたに送ったので、

あなたの電子メールを介して、私はあなたのオペレーションシステムに悪質なコードをアップロードしました。
私は友人、同僚、親戚とのあなたの連絡先のすべてを保存し、インターネットリソースへの訪問の完全な履歴を保存しました。
また、あなたのデバイスにトロイの木馬をインストールしました。

あなたは私の唯一の犠牲者ではない、私は通常、デバイスをブロックし、身代金を求める。
しかし、私は頻繁に訪れる親密なコンテンツのサイトにショックを受けました。

私はあなたの幻想にショックを受けている！ 私はこれのようなものを見たことがない！

だから、あなたがサイトで楽しむとき（あなたは私が何を意味するか知っています！）
あなたのカメラのプログラムを使用してスクリーンショットを作成しました。
その後、私はそれらを現在閲覧されているサイトのコンテンツに結合しました。

これらの写真を連絡先に送信すると素晴らしいことがあります。
しかし、あなたがそれを望んでいないと確信しています。

したがって、私は沈黙のためにあなたからの支払いを期待しています。
私は$842が良い価格だと思います！

Bitcoin経由で支払う。
私のBTCウォレット： 1JDi4GbHUzCrrnT7BCYbnsyLyrFpNK7faP

あなたがこれを行う方法を知らない場合 - Googleに「BTCウォレットに送金する方

您好！

我是幾個月前破解你的電子郵件和設備的黑客。
您在其中一個訪問過的網站上輸入了密碼。我攔截了它。

當然，您可以更改或更改它。
但這不是問題，我的惡意軟件每次都更新它。

請不要聯繫我或試著找我。那是不可能的。自從我向您發送了一封來自您帳戶的電子郵件

通過您的電子郵件，我將惡意代碼上傳到您的操作系統。
我與朋友，同事，親戚保存了所有聯繫人，並保存了訪問互聯網資源的完整歷史記錄。
還在您的設備上安裝了特洛伊木馬。

你不是我唯一的受害者，我通常會封鎖設備並要求勒索贖金。
然而，我對經常訪問的私密內容網站感到震驚。

你對你的錯覺感到震驚！我從來沒有見過這樣的東西！

所以當你在網站上享受時（你知道我的意思！）
我使用相機程序製作了截圖。
之後，我將它們與當前正在查看的網站的內容結合起來。

將這些照片發送給您的聯繫人非常棒。
但我相信你不想要它。

因此，我期待你的沉默支付。
我認為842美元是個好價錢！

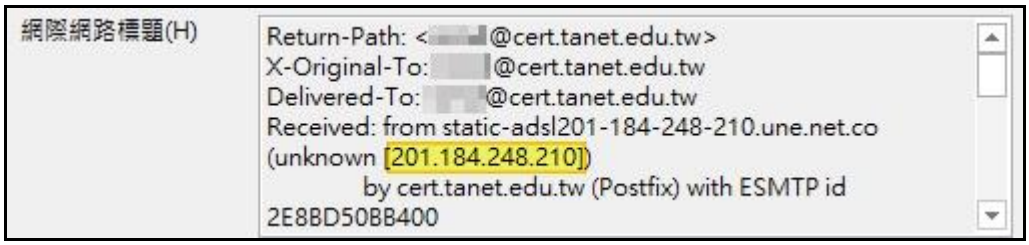
通過比特幣支付。
我的BTC錢包：1JDi4GbHUzCrrnT7BCYbnsyLyrFpNK7faP

如果您不知道如何操作 - 請輸入"如何將錢轉入BTC錢包"給Google。這並不困難。
收到指定金額後，所有受損材料將自動銷毀。我的病毒也將從您自己的操作系統中刪除。

我的特洛伊木馬有一個自動警報。我會在看完這封郵件後收到一條消息。

我會給你兩天付款（恰好48小時）。
如果沒有發生這種情況 - 你的所有聯繫人都將從你的黑暗秘密生活中瘋狂射擊！
您的設備將被阻止，以免您干擾（48小時後）

別傻了！
警察和朋友絕對不會幫助你.....



網際網路標題(H)

Return-Path: <[redacted]@cert.tanet.edu.tw>
X-Original-To: [redacted]@cert.tanet.edu.tw
Delivered-To: [redacted]@cert.tanet.edu.tw
Received: from static-adsl201-184-248-210.une.net.co
(unknown [201.184.248.210])
by cert.tanet.edu.tw (Postfix) with ESMTP id
2E8BD50BB400

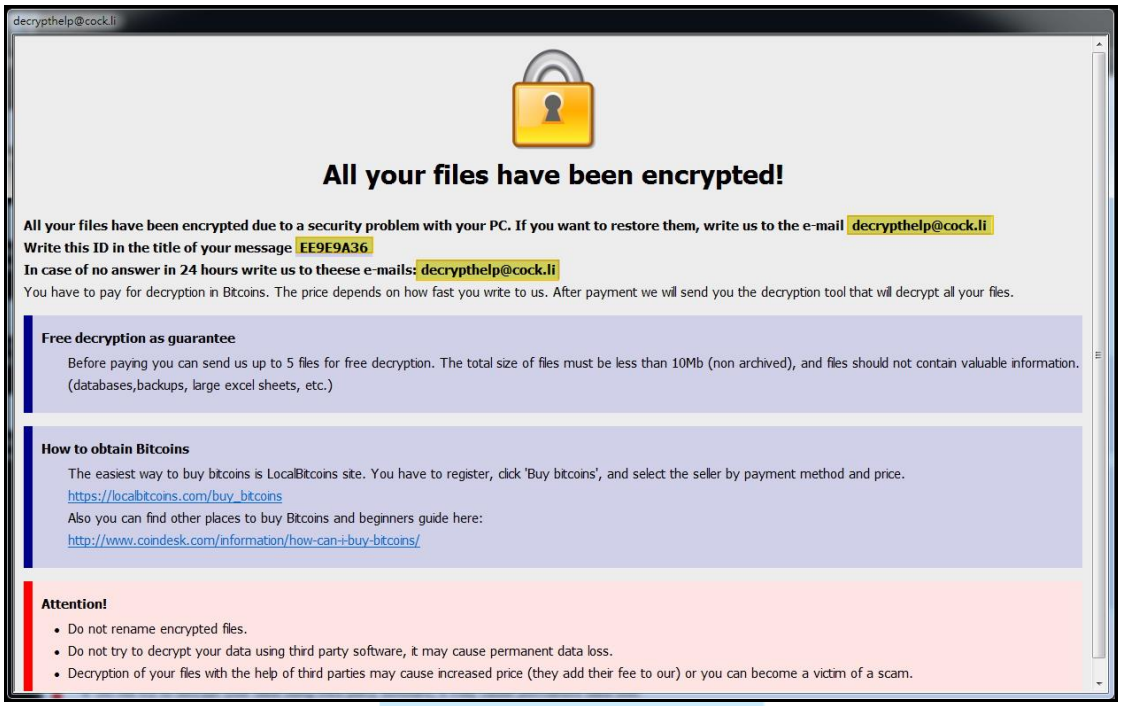
6. 接著檢測 Dharma 勒索病毒，病毒樣本 virus.exe 經 Virutotal 檢測其惡意比例為 58/67，有多家防毒軟體公司使用 CrySiS 或 Dharma 等用字於該病毒命名

上。

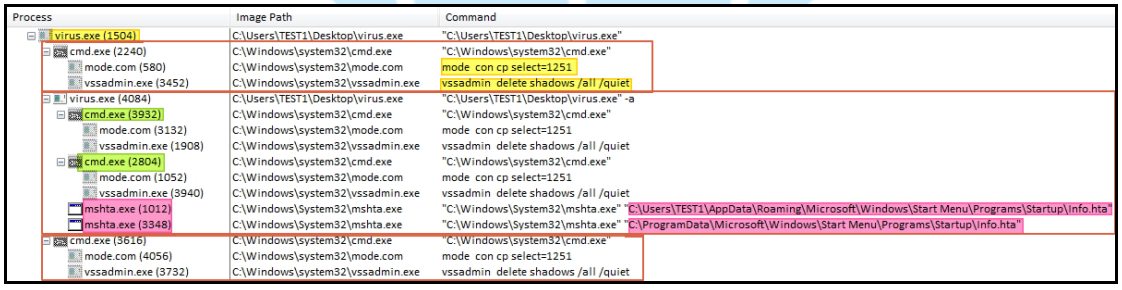
SHA256:	153834ac3c6b67f479548e8069a1de8419764a18df200bd429eb77c062d1b36d
檔案名稱:	virus.exe
偵測率:	58 / 67
分析日期:	2018-10-26 08:09:43 UTC (0 分鐘 前)

防毒	結果	更新
Ad-Aware	Trojan.Ransom.Crysis.E	20181026
ALYac	Trojan.Ransom.Crysis	20181026
Arcabit	Trojan.Ransom.Crysis.E	20181026
BitDefender	Trojan.Ransom.Crysis.E	20181026
ClamAV	Win.Trojan.Dharma-6668198-0	20181026
Emsisoft	Trojan.Ransom.Crysis.E (B)	20181026
ESET-NOD32	a variant of Win32/Filecoder.Crysis.P	20181026
F-Prot	W32/Wadhrama.B	20181026
F-Secure	Trojan.Ransom.Crysis.E	20181026
Fortinet	W32/Crysis.L!tr.ransom	20181026
Ikarus	Trojan-Ransom.Crysis	20181026
Malwarebytes	Ransom.Crysis.Generic	20181026
Microsoft	Ransom:Win32/Wadhrama	20181026
eScan	Trojan.Ransom.Crysis.E	20181026
Rising	Trojan.Ransom.Crysis!1.A6AA (CLOUD)	20181026
SUPERAntiSpyware	Ransom.Crysis/Variant	20181022
Symantec	Ransom.Crysis	20181026
TACHYON	Ransom/W32.crysis.94720	20181026
Tencent	Trojan-Ransom.Win32.Crysis.a	20181026
TheHacker	Trojan/Filecoder.Crysis.I	20181025
TrendMicro	Mal_Crysis	20181026
TrendMicro-HouseCall	Mal_Crysis	20181026

7. 當病毒樣本 virus.exe 執行後，會在受害主機的桌面出現一個「All your files have been encrypted」的視窗，視窗中告訴受害者所有的檔案已被加密，可免費解密 5 個檔案，若想將主機內的檔案解密，需以主旨為受害者 ID (EE9E9A36)寫信至 decrypthelp@cock.li 的 E-Mail 信箱。

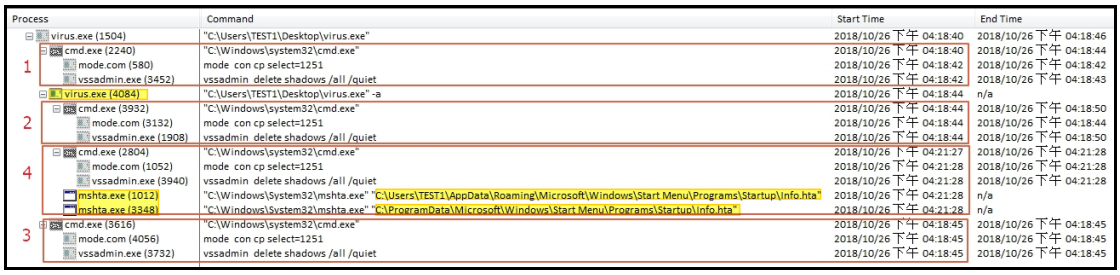


8. 檢視背景程式視運作情形，發現 virus.exe 執行後，除了再次呼叫自己外，也會呼叫 cmd.exe 來執行 mode.com 與 vssadmin.exe 兩個系統執行檔。mode.com 所執行的命令 mode con cp select=1251 為設置代碼頁，顯示西里爾語，而 vssadmin.exe 所執行的命令 vssadmin delete shadows/all/quiet 為刪除主機內所有影子副本。

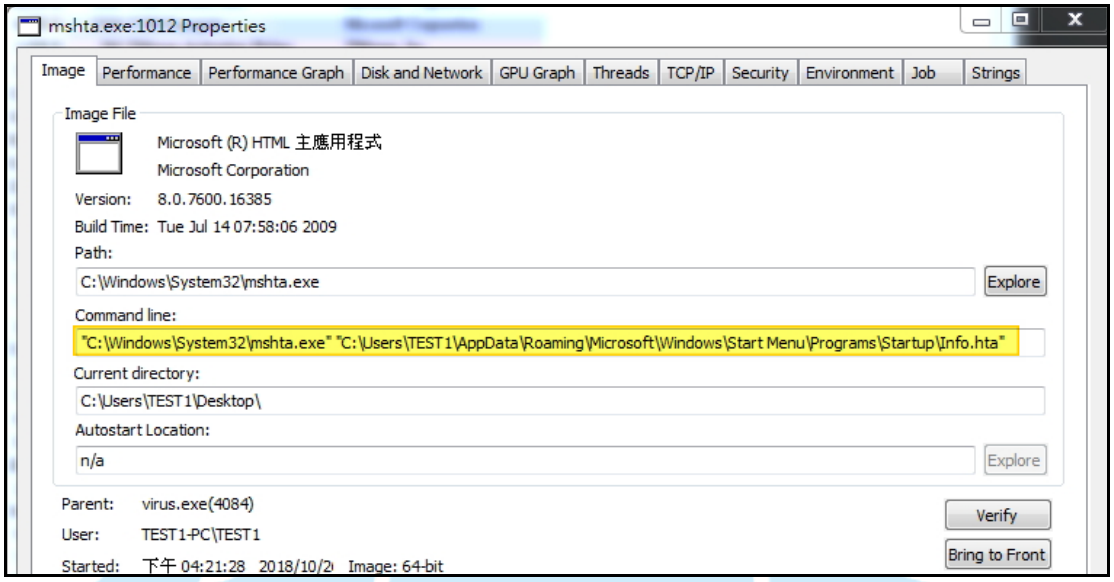


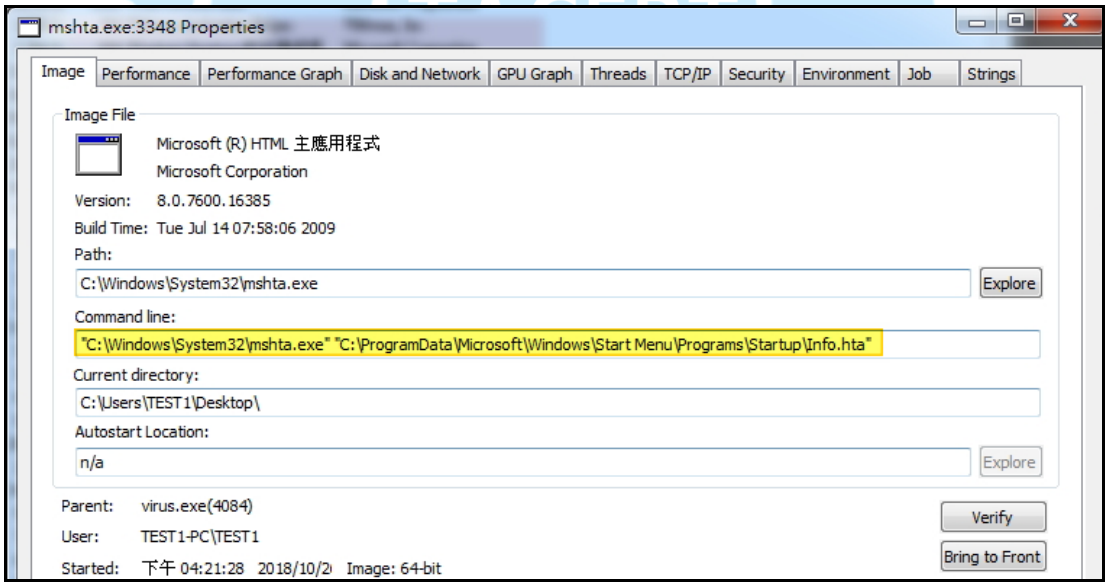
Process	Image Path	Command
virus.exe (1504)	C:\Users\TEST1\Desktop\virus.exe	"C:\Users\TEST1\Desktop\virus.exe"
cmd.exe (2240)	C:\Windows\system32\cmd.exe	"C:\Windows\system32\cmd.exe"
mode.com (580)	C:\Windows\system32\mode.com	mode con cp select=1251
vssadmin.exe (3452)	C:\Windows\system32\vssadmin.exe	vssadmin delete shadows /all /quiet
virus.exe (4084)	C:\Users\TEST1\Desktop\virus.exe	"C:\Users\TEST1\Desktop\virus.exe" -a
cmd.exe (3932)	C:\Windows\system32\cmd.exe	"C:\Windows\system32\cmd.exe"
mode.com (3132)	C:\Windows\system32\mode.com	mode con cp select=1251
vssadmin.exe (1908)	C:\Windows\system32\vssadmin.exe	vssadmin delete shadows /all /quiet
cmd.exe (2804)	C:\Windows\system32\cmd.exe	"C:\Windows\system32\cmd.exe"
mode.com (1052)	C:\Windows\system32\mode.com	mode con cp select=1251
vssadmin.exe (3940)	C:\Windows\system32\vssadmin.exe	vssadmin delete shadows /all /quiet
mshta.exe (1012)	C:\Windows\System32\mshta.exe	"C:\Windows\System32\mshta.exe" "C:\Users\TEST1\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\info.hta"
mshta.exe (3348)	C:\Windows\System32\mshta.exe	"C:\Windows\System32\mshta.exe" "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\info.hta"
cmd.exe (3616)	C:\Windows\system32\cmd.exe	"C:\Windows\system32\cmd.exe"
mode.com (4056)	C:\Windows\system32\mode.com	mode con cp select=1251
vssadmin.exe (3732)	C:\Windows\system32\vssadmin.exe	vssadmin delete shadows /all /quiet

在 virus.exe 再次呼叫自己後，除了執行 cmd.exe、mode.com 與 vssadmin.exe 外，會執行兩次程式 mshta.exe，此兩次程式會分別去呼叫兩個存放於不同處但檔名相同的檔案 info.hta。

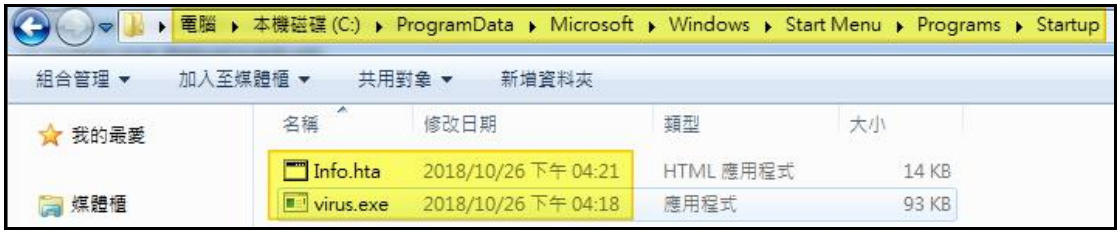


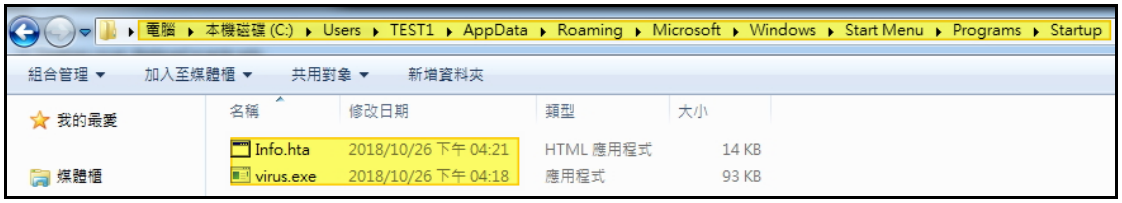
	Process	Command	Start Time	End Time
	virus.exe (1504)	"C:\Users\TEST1\Desktop\virus.exe"	2018/10/26 下午 04:18:40	2018/10/26 下午 04:18:46
1	cmd.exe (2240)	"C:\Windows\system32\cmd.exe"	2018/10/26 下午 04:18:40	2018/10/26 下午 04:18:44
1	mode.com (580)	mode con cp select=1251	2018/10/26 下午 04:18:42	2018/10/26 下午 04:18:42
1	vssadmin.exe (3452)	vssadmin delete shadows /all /quiet	2018/10/26 下午 04:18:42	2018/10/26 下午 04:18:43
	virus.exe (4084)	"C:\Users\TEST1\Desktop\virus.exe" -a	2018/10/26 下午 04:18:44	n/a
2	cmd.exe (3932)	"C:\Windows\system32\cmd.exe"	2018/10/26 下午 04:18:44	2018/10/26 下午 04:18:50
2	mode.com (3132)	mode con cp select=1251	2018/10/26 下午 04:18:44	2018/10/26 下午 04:18:44
2	vssadmin.exe (1908)	vssadmin delete shadows /all /quiet	2018/10/26 下午 04:18:44	2018/10/26 下午 04:18:50
4	cmd.exe (2804)	"C:\Windows\system32\cmd.exe"	2018/10/26 下午 04:21:27	2018/10/26 下午 04:21:28
4	mode.com (1052)	mode con cp select=1251	2018/10/26 下午 04:21:28	2018/10/26 下午 04:21:28
4	vssadmin.exe (3940)	vssadmin delete shadows /all /quiet	2018/10/26 下午 04:21:28	2018/10/26 下午 04:21:28
4	mshta.exe (1012)	"C:\Windows\System32\mshta.exe" "C:\Users\TEST1\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Info.hta"	2018/10/26 下午 04:21:28	n/a
4	mshta.exe (3348)	"C:\Windows\System32\mshta.exe" "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\Info.hta"	2018/10/26 下午 04:21:28	n/a
3	cmd.exe (3616)	"C:\Windows\system32\cmd.exe"	2018/10/26 下午 04:18:45	2018/10/26 下午 04:18:45
3	mode.com (4056)	mode con cp select=1251	2018/10/26 下午 04:18:45	2018/10/26 下午 04:18:45
3	vssadmin.exe (3732)	vssadmin delete shadows /all /quiet	2018/10/26 下午 04:18:45	2018/10/26 下午 04:18:45



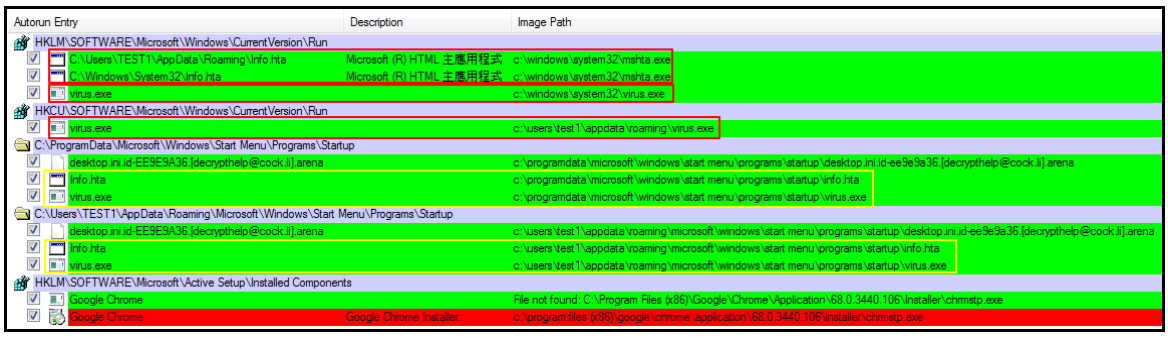


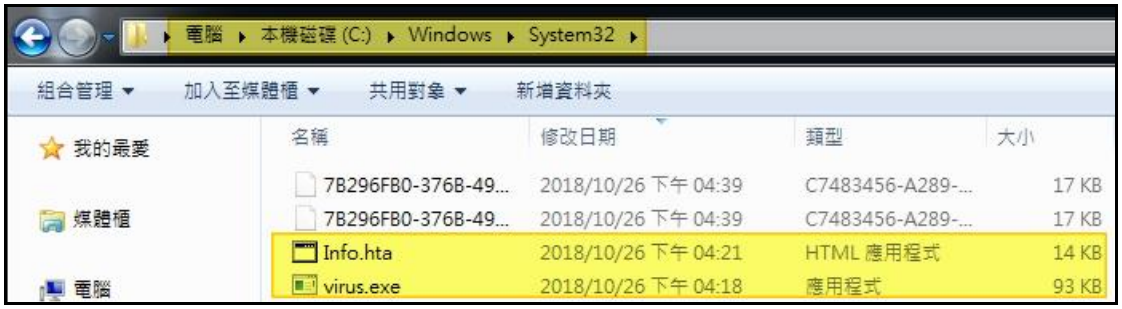
9. 檢視兩個 info.hta 檔案所在位置，發現他們所在的 Startup 資料夾中除了 Info.hta 外，另有病毒 virus.exe，這表示每次開機後皆會執行這兩個檔案，而且 Info.hta 執行後會開啟所有檔案已被加密的通知視窗。





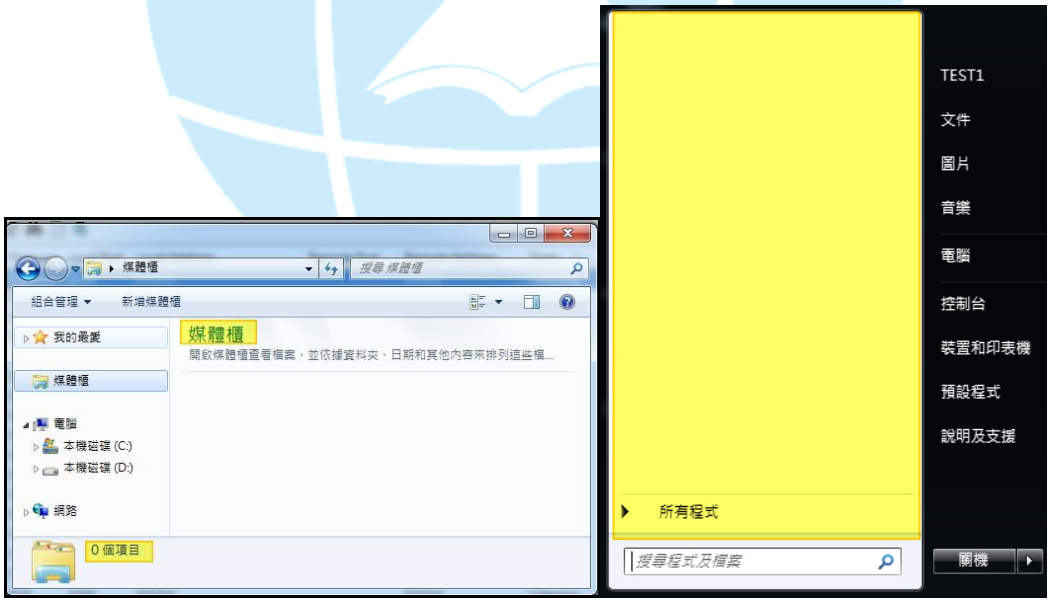
10. 透過 AutoRun 工具，發現 Info.hta 與 virus.exe 所儲存位置不只有前面所提兩處，在 C:\Windows\systme32 資料夾中也有，而 virus.exe 在 C:\users\使用者名稱\appdata\roaming 資料夾中也存在，將病毒本身複製並存放於多處，而且放於 C:\Windows\system32 系統資料夾內之手法於一般勒索病毒之思維不同。





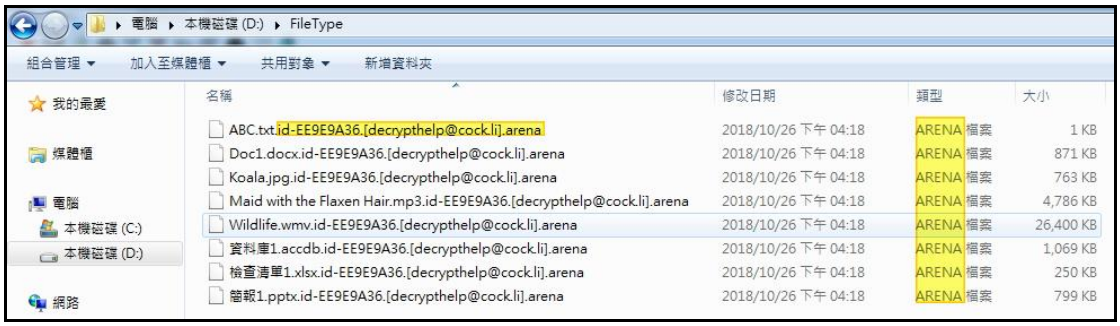
11. 在每個被加密的檔案資料夾中，皆會有一個檔案 FILES ENCRYPTED.txt，檢視其內容得知為駭客告訴受害者所有檔案已被鎖住，如果想要解開檔案，請寫信到電子信箱 decrypthelp@cock.li。

12. 在 virus.exe 執行後，發現原先在媒體櫃中的所有資料皆消失不見，而且在點選「開始」>「程式列表」，發現所有內容皆不見。



13. 檢視被加密的檔案，發現檔案名稱皆使用下面規則命名:「檔案名稱.id-8 位英文數字合成的受害者 ID.[聯絡駭客的 E-mail 信箱].此次變種副檔名 arena」。

例: ABC.txt.id-EE9E9A36.[decrypthelp@cock.li].arena



III. 網路架構圖

1.駭客利用社交工程方式散播 Dharma 病毒。

2.受害者執行 Dharma 病毒。

3.Dharma 病毒呼叫 2 次 cmd.exe 來執行 mode.com 與 vssadmin.exe。

4.再次呼叫 Dharma 病毒執行 2 次 cmd.exe(mode.com 與 vssadmin.exe)。

5.執行 mshta.exe。

6.受害主機重新開機後，執行 Dharma 病毒與 Info.hta。

IV. 建議與總結

1. 當勒索恐嚇信在校園散播時，曾有學校反應有同一位受害者在隔一段時間後再次收到勒索恐嚇信，當時那位受害者在第一次事件發生時已做過密碼變更處理，再次收到這類信件時，十分懷疑自己的密碼是否已被駭客知道。事實上，這是駭客對受害者進行的心理戰，為了讓受害者相信密碼已經被盜，建議遇到此類狀況的受害者第一時間需請校內資安相關人員協

助，切勿相信駭客所言。

2. 針對勒索恐嚇信的資安事件有幾點防護建議，提供使用者參考。
   (1) 定期更換密碼並加強密碼強度，建議使用 8 個字元以上且英文、符號與數字混合的密碼。
   (2) 避免多個服務所用之帳號共用同一組密碼。
   (3) 不隨意開啟不明來源的信件(含附件)或網路連結，以免遭植入惡意程式來竊取資訊。
   (4) 定期更新作業系統、應用程式與病毒碼至最新版本。
   (5) 定期備份重要檔案與執行系統掃毒作業。
3. Dharma 勒索病毒每隔幾個星期就產生新的變種，每個變種主要在變更駭客 E-mail 信箱與被加密檔案的副檔名，目前對於 Dharma 勒索病毒之更版頻繁的變種尚未有解密器產生，因此受害主機內檔案被加密後，無法解密。
4. 針對 Dharma 勒索病毒的防護與處理作業，有幾點建議提供使用者參考。
   (1) 平時定期備份重要檔案與執行系統掃毒作業。
   (2) 定期更新系統與病毒碼至最新版本。
   (3) 不隨意開啟不明來源的信件與網頁連結。
   (4) 若主機感染 Dharma 病毒，可將已被加密的重要檔案留存，等待日後解密器的產生。