

個案分析-

偽裝成挖礦工具的惡意程式

分析報告

TACERT



TACERT 臺灣學術網路危機處理中心團隊製

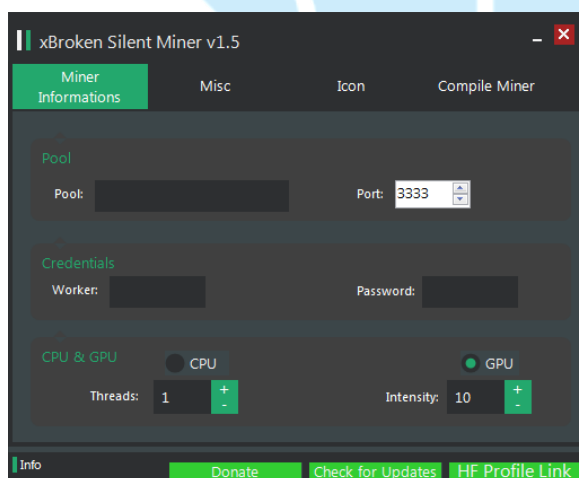
2015/12

## I. 事件簡介

1. 隨著加密數位貨幣的流行，越來越多人開始使用數位貨幣例如比特幣，因此許多駭客提供免費的比特幣挖礦工具讓使用者使用。
2. 網路上很多的免費挖礦工具常見的如 cpuminer 或 gpuminer，分別透過 CPU 和 GPU 處理器進行雜湊運算，以開採運算出新的比特幣。
3. 然而這些工具大多是指令介面，不方便一般人使用，故駭客故意製作出圖形化介面的挖礦工具，實質上卻是惡意程式讓主機成為殭屍電腦。
4. 本事件測試一隻為 Silent Miner Botnet.exe 的惡意程式。

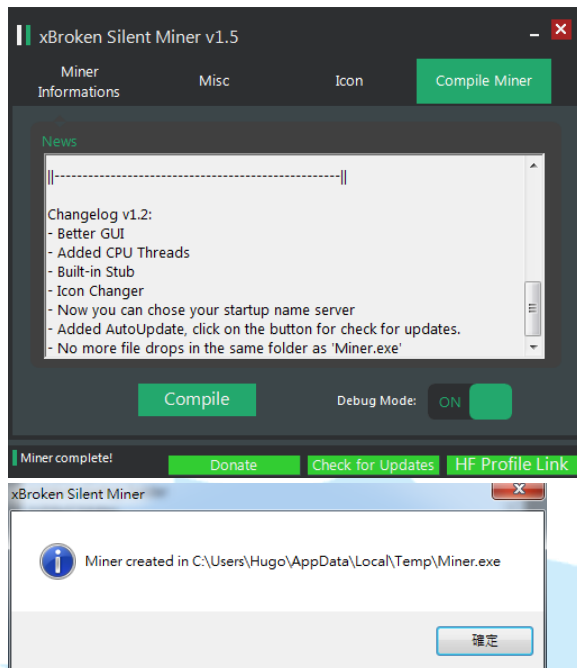
## II. 事件檢測

1. 使用 VM 虛擬主機並且為 Windows 7 (x64)系統進行隔離環境測試。
2. 惡意程式樣本名稱為 Silent Miner Botnet.exe 執行檔，測試過程中會側錄其網路行為進行分析。
3. 該檔案執行後並不會有安裝的動作，而是直接跳出一個軟體視窗，且名為「xBroken Silent Miner v1.5」。
4. 從該軟體視窗來看，看起來是數位貨幣挖礦工具會出現的資訊欄位，例如 pool(礦池 IP)、port(通常是 3333)、worker(礦工名稱)、password(礦工密碼)。



5. 在視窗右側有個頁籤為 Compile Miner，將 Compile 按鍵執行後會產生

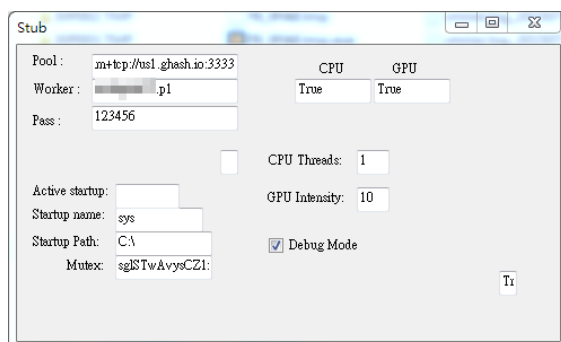
一個惡意程式執行檔 Miner.exe，藏於 C 磁碟的隱藏目錄中。



6. 透過 Virustotal 掃描 Silent Miner Botnet.exe 得到，該程式的偵測比例為 36/55 的木馬程式。




7. 隨後執行惡意程式 Miner.exe，會出現一個視窗並有之前輸入欄位的資訊，似乎是告知使用者挖礦程序已經啟用。



8. 透過 Virustotal 掃描 Miner.exe，得知偵測比例為 29/55 的惡意程式，

主要行為可能是耗用資源進行挖礦。



SHA256: f81bf6bd3d9750552a1460d89e24f2a9ae7315d646f934bf332854f2bc20ca78

File name: Miner.exe

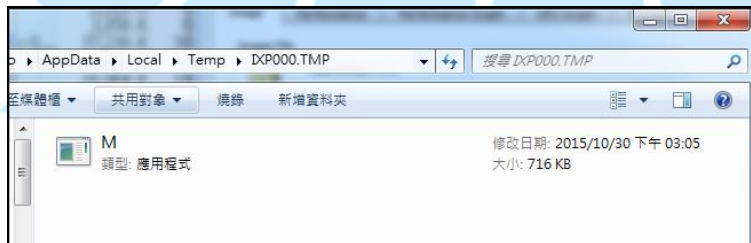
Detection ratio: 29 / 55

Analysis date: 2015-12-07 03:40:48 UTC ( 1 minute ago )

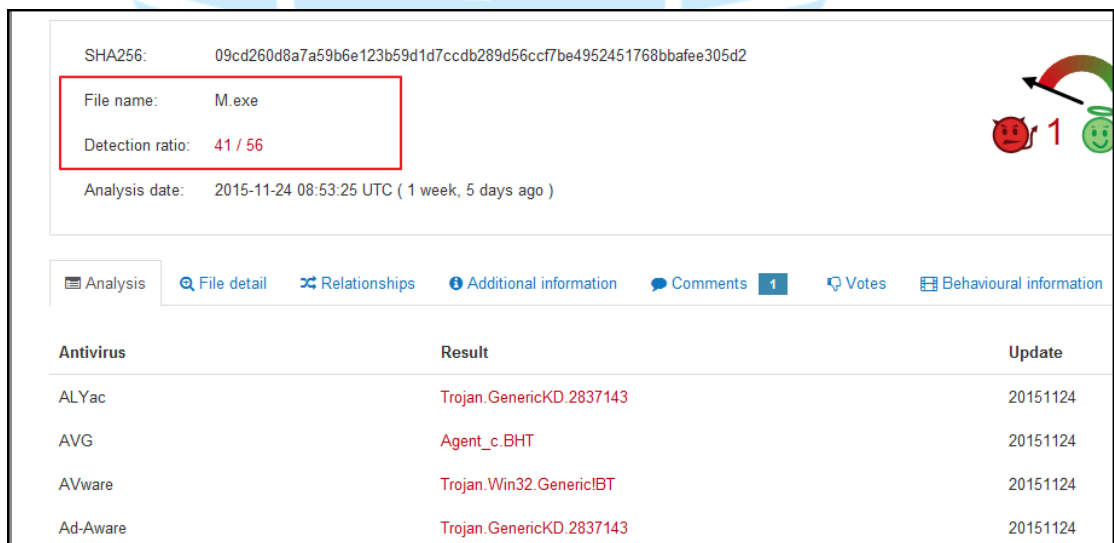
Analysis | File detail | Additional information | Comments | Votes

Antivirus	Result	Update
ALYac	Gen.Variant.Zusy.98981	20151207
AVG	CoinMiner.CEB	20151207
AVware	Trojan.Win32.Generic!BT	20151207

9. 在啟用 Silent Miner Botnet.exe 後會先產生出一隻 M.exe，並藏匿於 C:\ 隱藏目錄下，該 M.exe 程式會在去產生出另一隻監控程式 sysmon.exe 後關閉。



10. 該惡意程式 M.exe 透過 virustotal 掃描確定為 41/56 比例的木馬程式。



SHA256: 09cd260d8a7a59b6e123b59d1d7ccdb289d56ccf7be4952451768bbafee305d2

File name: M.exe

Detection ratio: 41 / 56

Analysis date: 2015-11-24 08:53:25 UTC ( 1 week, 5 days ago )

Analysis | File detail | Relationships | Additional information | Comments | Votes | Behavioural information

Antivirus	Result	Update
ALYac	Trojan.GenericKD.2837143	20151124
AVG	Agent_c.BHT	20151124
AVware	Trojan.Win32.Generic!BT	20151124
Ad-Aware	Trojan.GenericKD.2837143	20151124

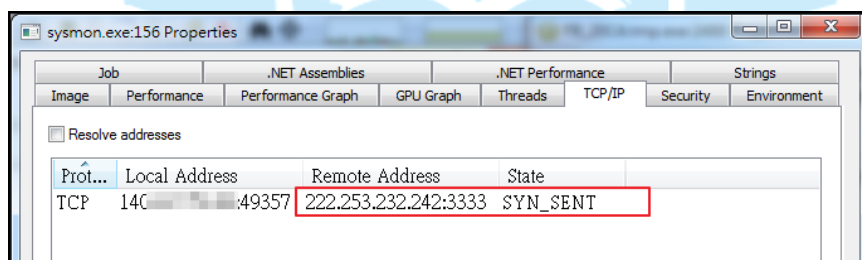
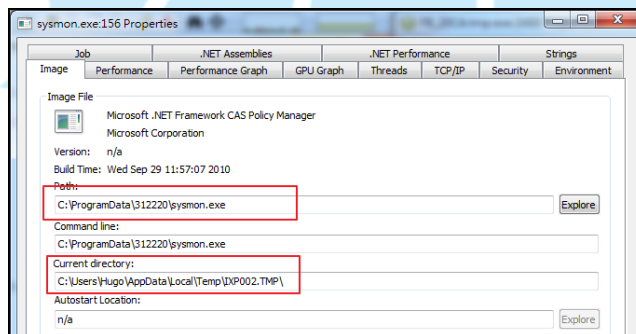
11. 透過 autoruns 檢查開機自動啟用區，可以得知惡意程式主體 sysmon.exe 藏匿於系統的隱藏資料夾中 C:\ProgramData\312220\。

HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components				2010/11/22
Internet Explorer Help	Windows Mail	Microsoft Corporation	c:\program files (x86)\windows mail\w...	2009/7/14
Internet Explorer Setup Tools	Windows Mail	Microsoft Corporation	c:\program files (x86)\windows mail\w...	2009/7/14
Microsoft Windows	Windows Mail	Microsoft Corporation	c:\program files (x86)\windows mail\w...	2009/7/14
Microsoft Windows Script 5.6	Windows Mail	Microsoft Corporation	c:\program files (x86)\windows mail\w...	2009/7/14
System Monitor			c:\programdata\312220\sysmon.exe	2015/10/28

12. 透過 procexp 檢查背景執行程式，發現到一隻隱藏的程式在背景執行，名為 sysmon.exe，並且該程式會持續對外進行連線。

explorer.exe	0.33	57,544 K	76,640 K	2412	Windows 檔案總管	Microsoft Corporati...
vmtoolsd.exe	0.30	11,260 K	23,300 K	2496	VMware Tools Core ...	VMware, Inc.
ports.exe	0.32	2,124 K	11,608 K	2372	CurrPorts	NirSoft
procexp.exe		2,032 K	7,208 K	1904	Sysinternals Process ...	Sysinternals - www...
procexp64.exe	5.69	11,356 K	26,512 K	1508	Sysinternals Process ...	Sysinternals - www...
SnippingTool.exe	1.26	1,824 K	6,096 K	2276	剪取工具	Microsoft Corporati...
FB_20CA.tmp.exe	0.06	53,104 K	54,552 K	2488	SilentMinerv1.2	
FB_3765.tmp.exe	0.09	32,388 K	33,560 K	1868	SilentMinerv1.2	
M.exe	0.05	39,472 K	16,684 K	2548		
sysmon.exe	0.33	45,168 K	18,152 K	156	Microsoft .NET Fram...	Microsoft Corporati...

13. 檢查 sysmon.exe 所在位置以及連線目的 IP，得知該程式會藏匿於系統的隱藏資料夾中 C:\ProgramData\312220\，並且會持續向目的 222.253.232.242:3333 傳送資料。



14. 通常來說 port 3333 的確是一般礦池伺服器所接收用的通訊埠，然而該程式 sysmon 在此所扮演的腳色卻是木馬程式，只是用 port 3333 來掩蓋竊取資料，實質上並無進行挖礦動作，因為挖礦時必然消耗大量 CPU 資源，然而卻只是安靜在背景監控磁碟傳輸資料。

15. 透過 Virustotal 掃描 sysmon.exe 得知，其就是偵測比例 41/56 的惡意程式 M.exe，故 sysmon.exe 由 M.exe 複製產生並藏匿於其他資料中。

SHA256:	09cd260d8a7a59b6e123b59d1d7ccdb289d56ccf7be4952451768bbafee305d2
File name:	M.exe
Detection ratio:	41 / 56
Analysis date:	2015-11-24 08:53:25 UTC ( 1 week, 5 days ago )

Analysis	File detail	Relationships	Additional information	Comments 1	Votes	Behavioural information
----------	-------------	---------------	------------------------	------------	-------	-------------------------

Antivirus	Result	Update
ALYac	Trojan.GenericKD.2837143	20151124
AVG	Agent_c.BHT	20151124
AVware	Trojan.Win32.Generic!BT	20151124
Ad-Aware	Trojan.GenericKD.2837143	20151124

16. 檢查執行惡意程式時產生的網路封包進行分析，初始時 silent miner botnet.exe 會先進行 HTTP GET 到 <http://trainerpatchgta4.altervista.org/News.txt>，也就是德國 88.198.2.208:80，主要內容為此程式的 changelog 內容。

NetWitness Reconstruction for session ID: 1417 ( Source 140.140.140.140 : 50063, Target 88.198.2.208 : 80 )	
Time 11/27/2015 15:41:40 to 11/27/2015 15:42:10 Packet Size 1,622 bytes Payload Size 1,052 bytes	
Protocol: HTTP/1.1 Flags: Keep-Alive, Accept-Range: bytes, Packet Count: 10	
REQUEST	<pre> GET /News.txt HTTP/1.1 Host: trainerpatchgta4.altervista.org Connection: Keep-Alive </pre>
	<pre> HTTP/1.1 200 OK Date: Fri, 27 Nov 2015 07:41:45 GMT Server: Apache Last-Modified: Thu, 10 Jul 2014 00:04:37 GMT ETag: "533e00e-296-4fdb920fc41d" Accept-Ranges: bytes Content-Length: 662 Vary: Accept-Encoding Keep-Alive: timeout=1, max=100 Connection: Keep-Alive Content-Type: text/plain </pre>
	<pre> Changelog v1.5: -Added startup folder -Added Mutex -Added Debug Mode </pre>

17. 接著 sysmon.exe 開始持續向越南的 222.253.232.242:3333 進行 TCP SENT，內容為空資料，從封包紀錄來看該主機似乎已經被關閉，所以封包送出後無回應，研判該主機應為駭客植入的一台殭屍主機。

上午 10:13:13	Added	FB_3765.tmp.exe	TCP	140.	:49351	88.198.2.208:80
上午 10:13:13	Added	FB_20CA.tmp.exe	TCP	140.	:49352	88.198.2.208:80
上午 10:13:13	Removed	System	UDP	0.0.0.0:	58937	*.*
上午 10:13:13	Removed	System	UDP	0.0.0.0:	60903	*.*
上午 10:13:19	Added	sysmon.exe	TCP	140.	:49353	222.253.232.242:3333
上午 10:13:39	Removed	sysmon.exe	TCP	140.	:49353	222.253.232.242:3333
上午 10:13:49	Added	sysmon.exe	TCP	140.	:49354	222.253.232.242:3333
上午 10:14:12	Removed	sysmon.exe	TCP	140.	:49354	222.253.232.242:3333
上午 10:14:22	Added	sysmon.exe	TCP	140.	:49355	222.253.232.242:3333

Source	Destination	Protocol	Length	Info
140.	222.253.232.242	TCP	66	49419-3333 [SYN] Seq=0 win=8192
140.	222.253.232.242	TCP	66	[TCP Retransmission] 49419-3333
140.	222.253.232.242	TCP	62	[TCP Retransmission] 49419-3333

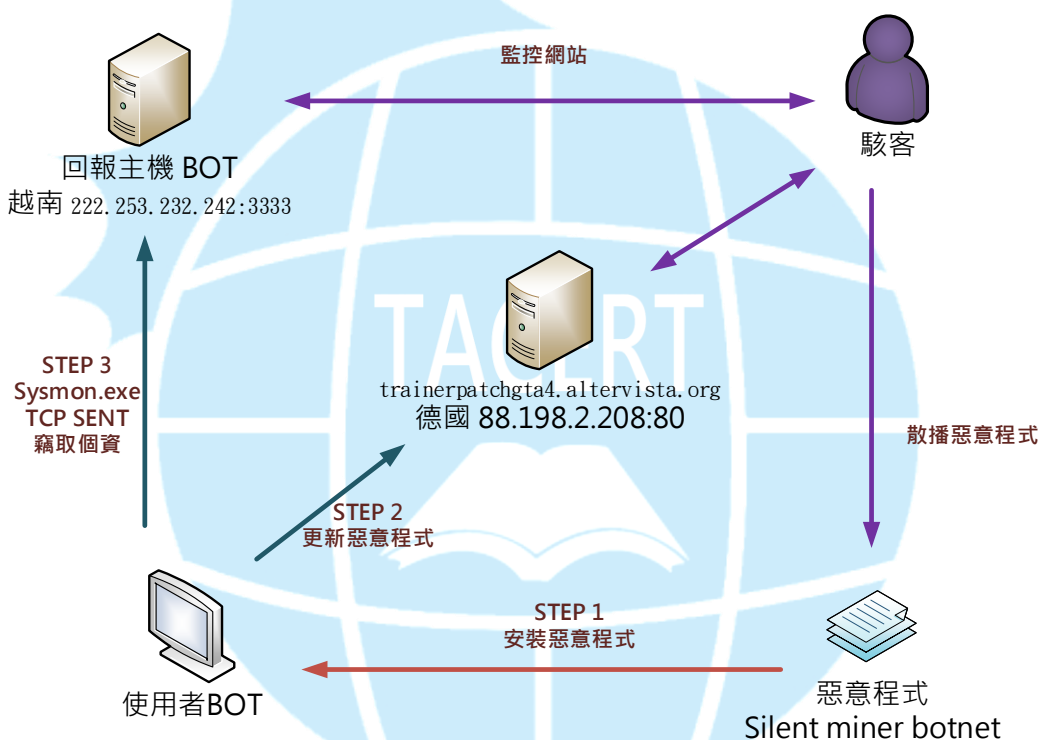
Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)

Ethernet II, Src: Vmware\_e4:38:70 (00:0c:29:e4:38:70), Dst: JuniperN\_d5:dc:81 (80:71:1f:d5:dc:81)

Internet Protocol Version 4, Src: 140. (140.117.72.43), Dst: 222.253.232.242 (222.253.232.242)

Transmission Control Protocol, Src Port: 49419 (49419), Dst Port: 3333 (3333), Seq: 0, Len: 0

### III. 網路架構圖



1. 使用者可能透過地下網站安裝到惡意程式 Silent miner botnet 成為 BOT。
2. 主機安裝惡意程式後向「88.198.2.208:80」報到並更新惡意軟體資訊。
3. Sysmon 惡意程式開始定期向上層 BOT 主機回報。
4. 等待時機駭客可能透過回報主機下達攻擊指令，此時感染主機就會變成活躍的殭屍電腦對外攻擊。

#### IV. 建議與總結

1. 建議使用者不要下載安裝此類的工具軟體，通常都內含木馬程式。
2. 駭客透過人性的弱點製作出一個視窗介面的挖礦工具，引誘用者安裝成為殭屍電腦。
3. 很多殭屍電腦初期並無異狀，大多會等待上層 C&C 主機下達指令時才會發作攻擊其他主機。
4. 網路上很多開源免費的工具軟體，下載使用前最好進行防毒軟體掃描。
5. 一旦安裝到惡意程式，可以透過免費微軟的 sysinternal 套裝工具進行程式和網路連線檢查移除。
6. 定期做好資料備份，若該惡意程式具有加密勒索功能，可能會造成更嚴重的損失。

