附件 5.資安應處事中處理工具說明

1.利用 Msert(微軟掃毒軟體)找出惡意檔案

下載連結 https://docs.microsoft.com/zh-tw/windows/security/threatprotection/intelligence/safety-scanner-download 根據 32 位元或是 64 位元選擇下載,工具使用期限為 10 天,超過 10 天需重新下載。

Microsoft 安全掃描工具

發行項 • 2022/01/25 • 1 位參與者

 $\bigtriangleup \nabla$

Microsoft 安全掃描工具是一種掃描工具,設計來尋找並移除 Windows 電腦中的惡 意程式碼。只要下載,然後執行掃描就可尋找惡意程式碼,並嘗試還原由發現的威 脅所做的變更。

- 下載 Microsoft 安全掃描工具 (32-位元) ☑
- 下載 Microsoft 安全掃描工具 (64-位元) ☑

圖 1 Msert 介紹

下載後在同資料夾開啟 cmd 輸入:MSERT.exe /N /F 參數意義如下:N:僅偵測不刪除;F:完整掃描,掃描完畢後在C:\Windows\debug\msert.log 查看是否有異常,掃描完畢後在

C:\Windows\debug\msert.log 查看是否異常,若 code 代碼非0則為異常。

Results Summary: Found Trojan:Win32/Meterpreter.O, not removed. Microsoft Safety Scanner Finished On Sun Oct 18 17:11:30 2020

Return code: 7 (0x7)

圖 2 Msert log

2.使用 TCPView 查看是否有可疑的程式建立連線

觀察建立的連線發起的程式是否有印象,或是 Port Number >9000 有可能為暗網之洋蔥路由。

TCPView -	Sysinte	rnals: ww	w.sysinternals	s.com							-	٥	\times
File Edit	View	Process	Connection	Options	Help								
CÖ	•••	G	4 TCP v4	6 ТСР v6	4 UDP v4	6 UDP v6 🏴	⇒P Search						
Process Name			Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name		^
💷 tor.exe			17524	TCP	Established	192.168.206.178	4045	193.108.117.103	9001	2022/10/12 下午 03:	tor.exe		
🔳 tor.exe			17524	TCP	Established	192.168.206.178	4047	193.108.117.103	9001	2022/10/12 下午 03:	tor.exe		
🔳 tor.exe			17524	TCP	Established	192.168.206.178	4044	51.77.59.234	9001	2022/10/12 下午 03:	tor.exe		
🔳 tor.exe			17524	TCP	Established	192.168.206.178	4046	51.77.59.234	9001	2022/10/12 下午 03:	tor.exe		
													_

圖 3 TCPView 查看是否有可疑的程式建立連線

3.使用 Process Explorer 查看是否有可疑的程式正在執行

使用 AutoRuns 查看惡意程式是否跟著開機一起被執行,開啟後點 選「Logon」頁籤, Options > Scan Options > 勾選 Verify code signatures、Check VirusTotal(千萬不要勾 Submit Images)。

le	<u>O</u> pt	tions View Process Find Users	<u>H</u> elp						
2		Run At Logon			<filter b<="" td=""><td><i>y name></i></td><td></td><td>A</td><td>م فہ ۔ ۔</td></filter>	<i>y name></i>		A	م فہ ۔ ۔
oce		Verify Image Signatures		CPU 0.56	Private Bytes 0 K	Working Set 0 K	PID Description n/a Hardware Interrupts and DPCs	Company Name	VirusTota
Ē		VirusTotal.com	 Check VirusTotal.com 	94.37	60 K	8 K	0		
		Always On Top	Submit Unknown Executables	0.19	216 K	9,940 K	4		
		Penlace Task Manager		Suspe	188 K	30,744 K	72		
	· ·	Lide Mile as Minimized			1,760 K	4,272 K	96		
		Hide when Minimized			9,548 K	55,332 K	132		
C		Allow Only One Instance			53,164 K	73,632 K	252 Google Chrome	Google LLC	<u>0/72</u>
	~	Confirm Kill			1,072 K	1,000 K	668		
1		- .			6,360 K	8,784 K	724 Intel(R) Local Management Serve	Intel Corporation	<u>0/72</u>
1		I ray Icons			2,020 K	5,928 K	752 Windows Services 的主機處理	. Microsoft Corporation	<u>0/72</u>
				< 0.01	2 104 K	R ORA K	844		

圖 4 Process Explorer 查看疑似惡意程式的方式

4.AutoRuns 識別惡意程式

使用 Process Explorer 查看執行中的程式是否包含惡意程式, Options >Virustotal.com>Check VirusTotal.com(不要 Submit unknown Executables)。

File Search Entry Options Category Help					
☞⊟♡⅊ዖԵ↗៙ ╉	Quick Filter				
C AppInit 🖪 Known DLLs 🍫 Wind	Logon 🛛 🖲 Winsock Provider:	s 🖨 Print Monitors 🕀	LSA Providers 🛛 🖵 Netv	vork Providers 🛛 📩 WM	I 🚺 Office
🔁 Everything 🖺 Logon 🍃 Explorer	🥭 Internet Explorer 🛛 🛅	Scheduled Tasks 🔍 Services	Drivers 🗔 Code	cs o ^o Boot Execute	Image Hijacks
Description	Publisher	Image Path		Timestamp	Virus Total
rrentVersion\Run				Thu Nov 4 14:23:52	
Microsoft Teams	(Verified) Microsoft 3rd P	C:\Users\twnic\AppData\Loca	NMicrosoft\Teams\Updat	Tue Mar 22 10:07	0/72
rrentVersion\Run				Tue Mar 22 10:35:11	_
Bitdefender Vpn App	(Verified) Bitdefender SRL	C:\Program Files\Bitdefender\	Bitdefender VPN\BdVpn	Mon Jan 31 20:2	1/72
HD Audio Background Process	(Verified) Realtek Semico	C:\Program Files\Realtek\Aud	io\HDA\RAVBg64.exe	Mon Oct 15 07:23	0/72
HD Audio Background Process	(Verified) Realtek Semico	C:\Program Files\Realtek\Aud	io\HDA\RAVBg64.exe	Mon Oct 15 07:23	0/72
·········					

圖 5 AutoRuns 查看疑似惡意程式的方法

5.勒索軟體大量讀寫判斷

勒索軟體加密步驟是:讀取資料>加密資料>寫回硬碟,因此勒索 軟體會對硬碟有大量的讀取與寫入。透過開啟系統管理員>詳細資 料>右鍵選取欄位>I/O讀寫位元,若發現 I/O讀寫位元相當大讀取 也差不多,若發現此症狀盡速點選「結束處理程序樹狀目錄」。

選取欄位	\times	₩ 丁作管理員	
選取將出現在表格中的欄位。		檔案(<u>F</u>) 選項(<u>O</u>) 檢視(<u>V</u>)	
 □ 控制代碼 □ 執行緒 	^	處理程序 效能 應用程式歷程記錄 開機 使用者 詳細資料 服	務
□ 使用者物件 □ GDI 物件		名稱	賣取位
│		SmartByteTelemetry eye 917,02 Dsapi,exe 结束工作(F) 788.03	0,582 2.917
☐ 其他 I/O 次數 ✓ I/O 讀取位元組		▶ ■ MsMpEng 結束處理程序樹狀目錄(T) 369,93	5,888
☑ I/O 寫入位元組		■ DDVData(提供意見反應(B) 148,65 □ nessusd e: 109.41	1,209
 ☑ 映像路徑名稱 ☑ 命令列 		■ resource 設定優先順序(P) > 100,111	7,888
□ 作業系統內容	~		8,808
確定 取	(消	■ FortiSSLVI UAC 模擬(V) 17,90	5,878
· · · · · · · · · · · · · · · · · · ·		SupportA: 建立傾印機案(C) 7,85	5,256

圖 6 I/O 讀寫與結束樹狀目錄

6.使用 WireShark 找出 DDoS 的症狀

(1) 檢視連線紀錄封包,是否有收到大量 SYN 封包 tcp.flags.syn
 == 1

1	🛃 *Wi-Fi							-	ø	\times
	<u>File Edit View Go Ca</u>	pture <u>A</u> nalyze <u>S</u> tatistics	Telephony Wireless Tools	<u>H</u> elp						
	📶 📕 🙋 🛞 📕 🛅 🗙	🖸 🍳 🗢 🗢 🚟 🚹 🕹	<u>_</u> 📃 Q. Q. Q. <u>II</u>							
(tcp.flags.syn == 1									+
Γ	No. Time	Source	Destination	Protocol	Length Info					
	35 7.839236	192.168.206.178	34.117.237.239	TCP	66 13468	→ 443	[SYN]	Seq=0	Win	=642
	36 7.842652	34.117.237.239	192.168.206.178	TCP	66 443 →	13468	SYN,	ACK] S	Seq=	0 Ac
	151 41.037830	192.168.206.178	172.217.160.99	TCP	66 13469	→ 443	[SYN]	Seq=0	Win	=642
	152 41.042270	172.217.160.99	192.168.206.178	TCP	66 443 →	13469	SYN,	ACK] S	Seq=	0 Ac
	199 47.536727	192.168.206.178	20.50.80.209	TCP	66 13470	→ 443	[SYN]	Seq=0	Win	=655
	200 47.751885	20.50.80.209	192,168,206,178	TCP	66 443 →	13470	SYN.	ACK1 4	Sea=	a Ac

圖 7 使用 Wireshark 檢查 SYN 封包數量

 (2) 比較 SYN 與 SYN/ACK 是否有大量的差距,不完整的三向 交握透過指令 tcp.flags.syn==1 && tcp.flags.ack==0 找出 SYN 數量; tcp.flags.syn==1 && tcp.flags.ack==0 找出 SYN/ACK 數量。觀察右下角數量差距

=1 && up.mags.ack						
ìme	Source	Destination	Protocol Len	gth Info		
367.850607	34.149.211.227	192.168.206.178	TCP	66 443 →	13670 [SYN,	ACK] Sec
367.896212	34.120.85.253	192.168.206.178	тср	66 443 →	13671 [SYN,	ACK] Sec
367.930282	35.190.56.82	192.168.206.178	TCP	66 443 →	13672 [SYN,	ACK] Sec
368.080620	34.120.85.253	192.168.206.178	TCP	66 443 →	13673 [SYN,	ACK] Sec
368.143764	35.190.56.82	192.168.206.178	TCP	66 443 →	13674 [SYN,	ACK] Sec
386.122095	52.114.16.179	192.168.206.178	TCP	66 443 →	13675 [SYN,	ACK] Sec
392.922963	34.149.211.227	192.168.206.178	тср	66 443 →	13680 [SYN,	ACK] Sec
392.995640	34.149.211.227	192.168.206.178	ТСР	66 443 →	13681 [SYN,	ACK] Sec
392.995979	34.120.85.253	192.168.206.178	TCP	66 443 →	13682 [SYN,	ACK] Sec
392.996400	35.190.56.82	192.168.206.178	ТСР	66 443 →	13683 [SYN,	ACK] Sec
393.065658	34.149.211.227	192.168.206.178	TCP	66 443 →	13684 [SYN,	ACK] Sec
393.132088	34.149.211.227	192.168.206.178	ТСР	66 443 →	13685 [SYN,	ACK] Sec
393.182081	34.120.85.253	192.168.206.178	TCP	66 443 →	13686 [SYN,	ACK] Sec
					COCCE FOUND	10117 0
1d 96 01 17	e2 00 09 0f 09 00 12	08 00 45 00 L····	• • • • • • • • • • • • • • • • • • •			
34 a4 86 00	00 79 06 fd 7d 22 75	ed ef c0 a8 ·4···	$\cdot y \cdot \cdot \cdot u \cdot \cdot \cdot$			
b2 01 bb 34	9c 60 0b cf 36 36 c1	4c 4b 80 12 ····4	·`· ·66 · LK · ·			
Ff e7 6c 00	00 02 04 04 e2 01 01	1 04 02 01 03 ····l·				
38						
hark_Wi-FiN0Z2J1.I	capng		Packets: 155	164 · Displayed	387 (0.2%) · Droppe	d: 0 (0.0%)

圖 8 使用 Wireshark 比較 SYN 與 ACK 數量

(3) 觀察 HTTP Request 與 Response 的數量,一般情況兩者應差 距不大。點選上方「Statistics」→「HTTP」→「Packet Counter」可開啟統計頁面

Го	pic/It	em	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Star
~	Total	HTTP Packets	376				0.0017	100%	0.0800	17.583
Г	0	ther HTTP Packets	0				0.0000	0.00%	-	-
	~ н	TTP Response Packets	188				0.0009	50.00%	0.0400	17.593
		???: broken	0				0.0000	0.00%	-	-
		5xx: Server Error	0				0.0000	0.00%	121	<u></u>
	~	4xx: Client Error	1				0.0000	0.53%	0.0100	74.952
		403 Forbidden	1				0.0000	100.00%	0.0100	74.952
		3xx: Redirection	0				0.0000	0.00%	-	-
	~	2xx: Success	187				0.0009	99.47%	0.0400	17.593
		200 OK	187				0.0009	100.00%	0.0400	17.593
		1vv: Informational	0				0.0000	0.00%	-	-
	· H	TTP Request Packets	188				0.0009	50.00%	0.0400	17.583

圖 9 使用 Wireshark 觀察 Request 與 Response 的數量