個案分析-

遠端桌面 RDP 入侵與攻擊的殭屍主機事件分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

106 年 2 月

I. 事件簡介

1. 該資安事件為某主機對外部其他主機進行大量的 RDP 暴力破解攻擊，造成網路頻寬壅塞及主機效能降低。

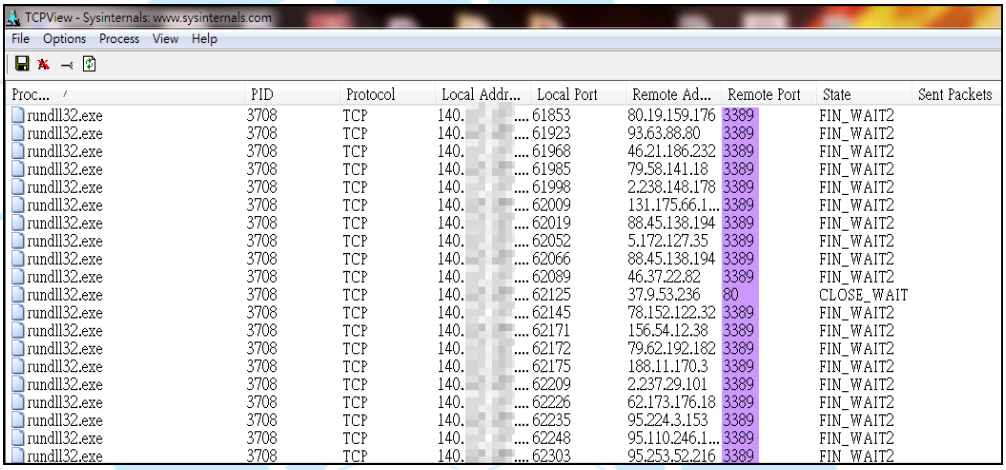
原發布編號	ASOC-INT-201701-7206	原發布時間	2017-01-23 08:21:09
事件類型	對外攻擊	原發現時間	2017-01-23 04:34:05
事件主旨	通報:[國立 [redacted] 大學]140.[redacted].136 MS.RDP.Connection.Brute.Force		
事件描述	ASOC發現貴單位(國立 [redacted] 大學)所屬 140.[redacted].136 疑似對外進行 MS.RDP.Connection.Brute.Force 攻擊		
手法研判	貴單位疑似對外進行非法攻擊行為，遠端攻擊者對Microsoft RDP(Remote Desktop Protocol)進行暴力的密碼猜測攻擊，攻擊者在10秒內進行200次的登入請求，如成功利用將可以連入未經授權的系統，進行非法的存取。		
建議措施	惠請貴單位： 1.檢查防火牆紀錄：查看內部是否有開啟異常或未經許可的連接埠，並查看記錄是否有外界對貴單位內部IP之異常連線。 2.如發現為非授權的連線，建議將該IP於防火牆阻擋。 3.建議針對被攻擊的主機做好相關主機系統服務檢查及弱點修補確認的工作，並關閉不需要的服務。 4.將所使用的密碼複雜度提高。		

2. 該主機為系所研究室學生使用的個人電腦，並且使用 Win7(x64)的作業系統。
3. 經檢測主機並無安裝任何防毒軟體，並且有啟用系統的遠端桌面服務，然而卻無限制來源端網段連入。
4. 該主機所使用的帳號密碼皆為相同，並且為簡易型的三個英文字元作為帳密。

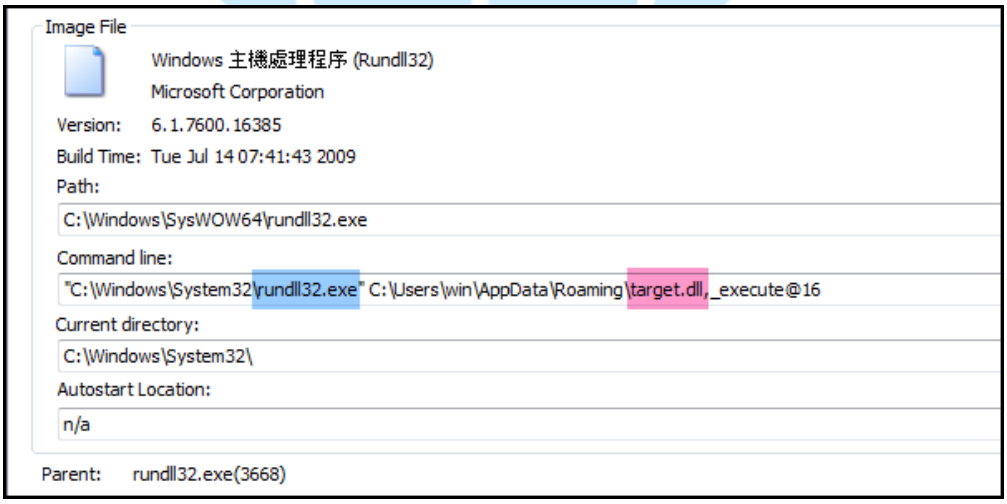
II. 事件檢測

1. 首先將裝有檢測工具的隨身碟插入該主機，並執行工具軟體準備檢測，然而隨身碟資料夾中的執行檔工具卻被開始進行加密，所有檔案名稱都被置換成『檔案名稱.[makedonskiy@india.com].wallet』。
2. 在隨身碟資料尚未被加密完全前，就立刻拔除隨身碟強迫中斷加密動作，加密後的檔名中包含了駭客的 email 位址，可能要透過它來勒索解密贖金。

3. 雖然加密病毒會對隨身碟進行加密，但主機內資料卻不受影響。在系統內執行 TCPview 工具觀察，有一支名為 rundll32.exe 正在大量進行對外 RDP 暴力破解攻擊。

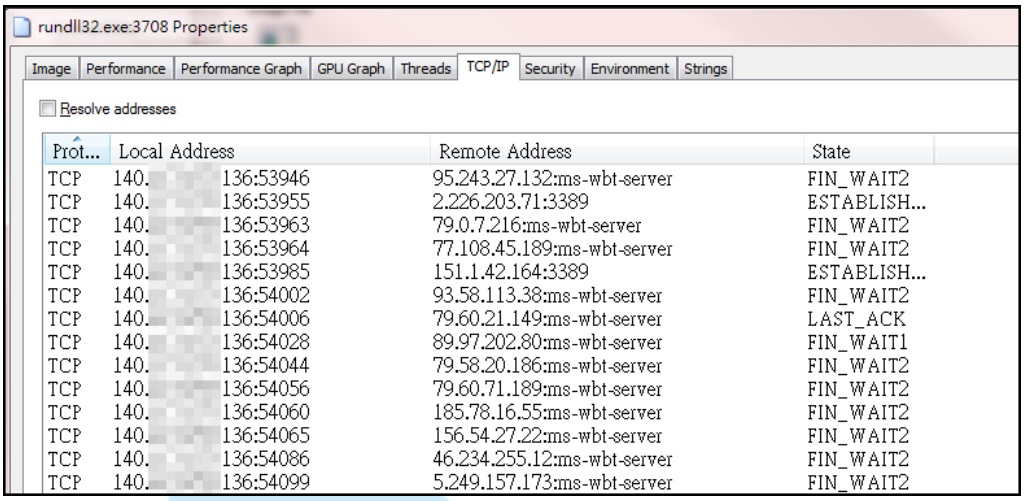


4. 開啟 Procexp 工具檢查系統背景程式狀況，可以清楚看到 rundll32.exe 所執行的惡意程式為 target.dll，此為 RDP 攻擊的主要檔案。

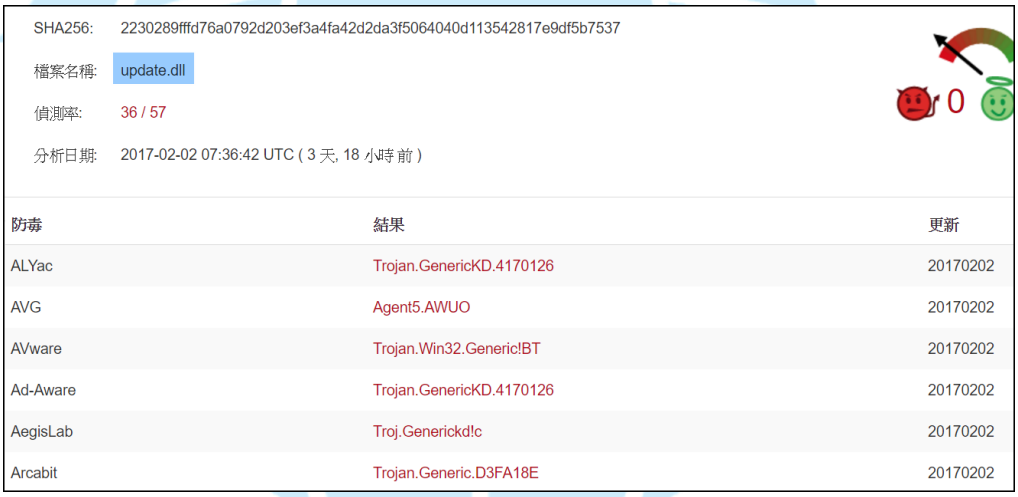


5. 從 rundll32.exe 的連線狀態來看也能確定其網路攻擊為 RDP connection

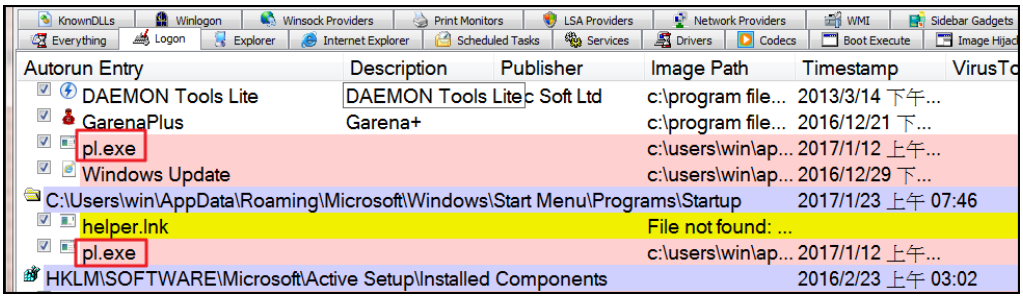
brute force。



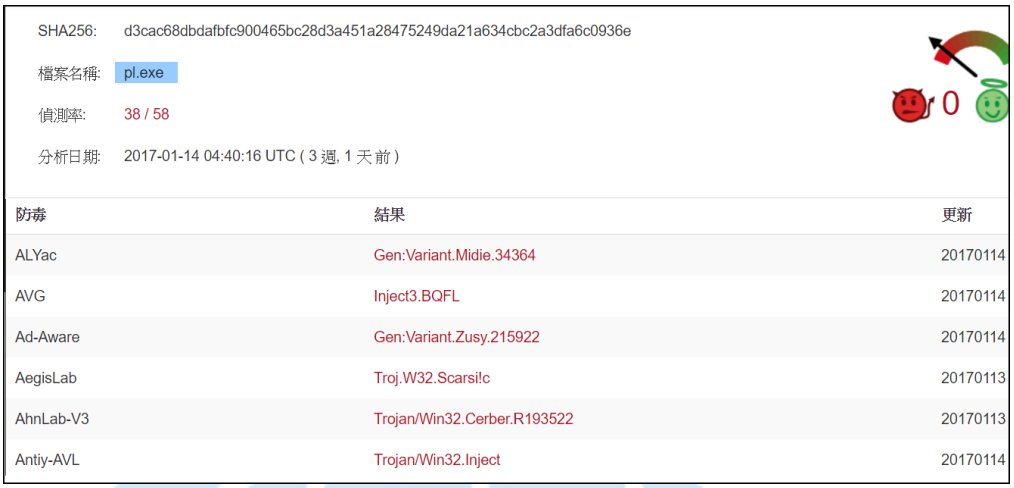
6. 將位於隱藏資料夾中的 \AppData\Roaming\target.dll 透過 Virustotal 進行掃描分析，檢測偵測比例為 36/57 的木馬後門程式，接受駭客指令進行攻擊。



7. 接著透過 autoruns 檢查開機時啟動程序發現，惡意程式 pl.exe 會常駐在開機啟動區，而 pl.exe 與 target.dll 相同都是藏匿於隱藏資料夾 \AppData\Roaming\ 之中。



8. 將 pl.exe 透過 virustotal 掃描得知，該程式的病毒檢測比例為 38/58，判定為啟動 target.dll 做 RDP 攻擊的惡意程式，並且可能帶有對插入的磁碟進行加密動作。



SHA256: d3cac68dbdafbfc900465bc28d3a451a28475249da21a634cbc2a3dfa6c0936e

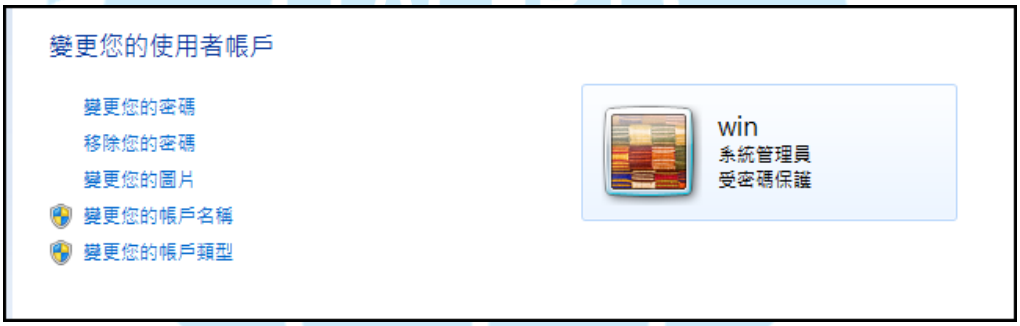
檔案名稱: pl.exe

偵測率: 38 / 58

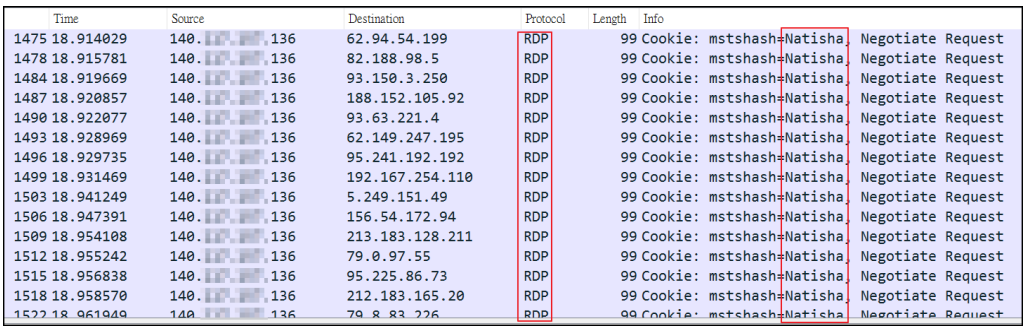
分析日期: 2017-01-14 04:40:16 UTC (3 週, 1 天 前)

防毒	結果	更新
ALYac	Gen:Variant.Midie.34364	20170114
AVG	Inject3.BQFL	20170114
Ad-Aware	Gen:Variant.Zusy.215922	20170114
AegisLab	Troj.W32.Scarsi!c	20170113
AhnLab-V3	Trojan/Win32.Cerber.R193522	20170113
Antiy-AVL	Trojan/Win32.Inject	20170114

9. 該主機最有可能被入侵方式應該就是遠端桌面 RDP 服務，因為使用者常常發現畫面被登出，表示有駭客正在登入使用。且沒有設定防火牆導致外部駭客能夠存取到主機，並且使用密碼與帳號相同的弱密碼。

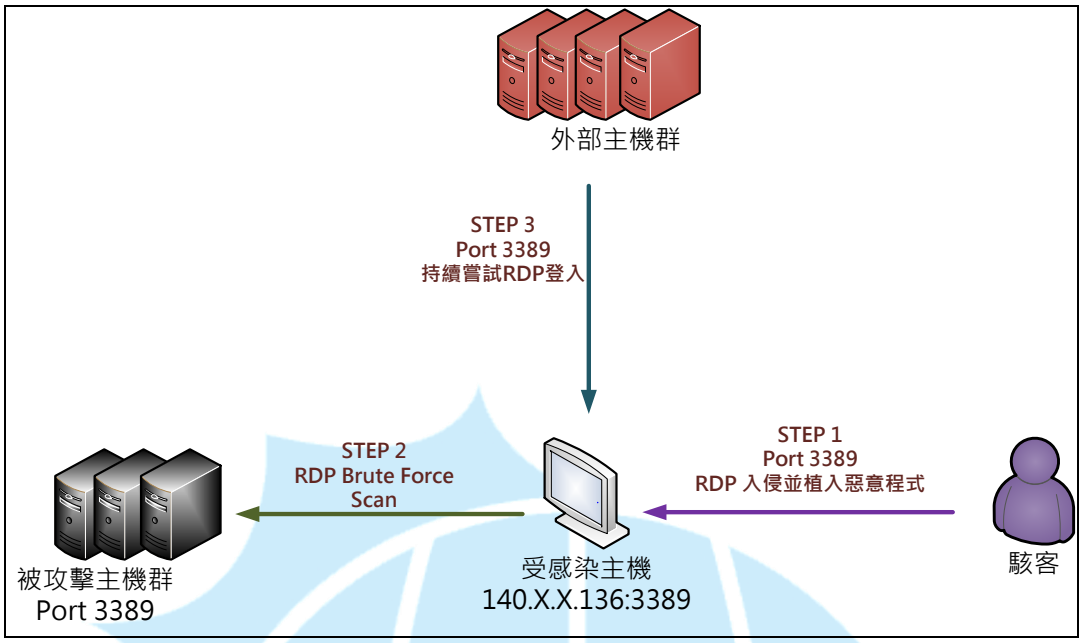


10. 檢查封包連線狀態，可看到主機持續對外做 RDP 登入行為，並且都固定使用帳號 ID 為 Natisha 進行嘗試登入。



Time	Source	Destination	Protocol	Length	Info
1475 18.914029	140.[redacted].136	62.94.54.199	RDP	99	Cookie: mstshash=Natisha Negotiate Request
1478 18.915781	140.[redacted].136	82.188.98.5	RDP	99	Cookie: mstshash=Natisha Negotiate Request
1484 18.919669	140.[redacted].136	93.150.3.250	RDP	99	Cookie: mstshash=Natisha Negotiate Request
1487 18.920857	140.[redacted].136	188.152.105.92	RDP	99	Cookie: mstshash=Natisha Negotiate Request
1490 18.922077	140.[redacted].136	93.63.221.4	RDP	99	Cookie: mstshash=Natisha Negotiate Request
1493 18.928969	140.[redacted].136	62.149.247.195	RDP	99	Cookie: mstshash=Natisha Negotiate Request
1496 18.929735	140.[redacted].136	95.241.192.192	RDP	99	Cookie: mstshash=Natisha Negotiate Request
1499 18.931469	140.[redacted].136	192.167.254.110	RDP	99	Cookie: mstshash=Natisha Negotiate Request
1503 18.941249	140.[redacted].136	5.249.151.49	RDP	99	Cookie: mstshash=Natisha Negotiate Request
1506 18.947391	140.[redacted].136	156.54.172.94	RDP	99	Cookie: mstshash=Natisha Negotiate Request
1509 18.954108	140.[redacted].136	213.183.128.211	RDP	99	Cookie: mstshash=Natisha Negotiate Request
1512 18.955242	140.[redacted].136	79.0.97.55	RDP	99	Cookie: mstshash=Natisha Negotiate Request
1515 18.956838	140.[redacted].136	95.225.86.73	RDP	99	Cookie: mstshash=Natisha Negotiate Request
1518 18.958570	140.[redacted].136	212.183.165.20	RDP	99	Cookie: mstshash=Natisha Negotiate Request
1522 18.961949	140.[redacted].136	79.8.83.226	RDP	99	Cookie: mstshash=Natisha Negotiate Request

III. 網路架構圖



1. 駭客透過 RDP 遠端桌面服務入侵受害者主機。
2. 駭客植入惡意程式 DLL 並持續對外部主機進行 RDP 暴力破解攻擊。
3. 外部其他駭客也可能透過 RDP 破解登入受害者主機。
4. 受害主機同時有可能對外部磁碟進行加密勒索。
5. 因為駭客是 RDP 登入主機，受害者個人資料可能都已經外洩。

IV. 建議與總結

1. 使用者有開啟遠端桌面 RDP 服務，並且都是使用簡易的三個字元的帳號密碼。
2. 因為並無設定防火牆規則限制來源端連入，故駭客輕易透過遠端桌面服務入侵到使用者主機。
3. 使用者經查發現到帳號被登出，卻不知道此時駭客正在登入並植入惡意程式。
4. 駭客植入 target.dll 惡意程式並持續對外部網段進行 RDP Scan 的暴力破解攻擊，嚴重消耗主機的 CPU 和記憶體資源導致電腦變慢。

5. 從 RDP 封包中固定使用 Natisha 作為登入帳號，來判斷該主機應該只是用來探索外部主機 RDP 服務是否可連線。
6. 惡意程式 pl.exe 會再開機時候呼叫 target.dll 執行，並且可能會對 USB 隨身碟內的資料進行加密勒索，並將加密檔名中放入駭客用的 email 位址。
7. 建議電腦務必安裝防毒軟體，並且可用 Teamviewer 方式取代內建的遠端桌面服務避免被駭客入侵。