



勒索病毒 Phobos 之變種 eking 分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

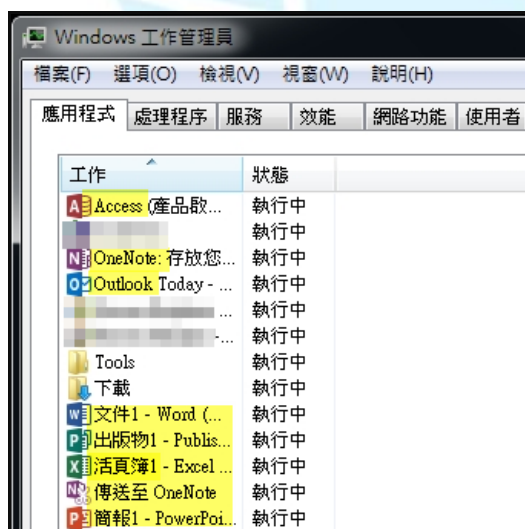
2020 年 11 月

一、事件簡介

1. 2020/10/20 A 國小發生 4 台主機感染勒索病毒事件，而 2020/10/24 B 高中發生 6 台 PC、4 台伺服器與 4 台 NAS 感染勒索病毒事件。經 TACERT 檢測發現這兩間學校皆是感染勒索病毒 Phobos 的新變種病毒 eking。
2. Phobos 的變種病毒 eking 可透過開啟釣魚郵件的附件 Word 檔啟動巨集方式下載到受感染主機內執行。
3. B 高中管理者對所有管理的伺服器皆使用同一組帳號與密碼登入系統，而且該校有使用掛載 NAS 資料夾為網路磁碟機的情形，這些狀況增加了勒索病毒的影響範圍。
4. 為了解該勒索病毒 Phobos 對於受害主機進行何種攻擊行為，TACERT 取得病毒樣本後進行分析。

二、事件檢測

1. 首先，使用一台掛載網路碟機的 Win 7 32 位元主機，並且執行病毒樣本 6e9c9b72.exe (MD5: be13334c44f2e0331a6d1d6460ff9359)。
2. 病毒 6e9c9b72.exe 執行後發現下列現象：
 - (1) 原先執行中的 Office 系列軟體都被關閉。



- (2) 出現光碟機還有檔案等候燒錄的訊息，可能是因為原先隱藏保護的系統檔

案 desktop.ini 變成 .eking 檔後顯示出來的關係。



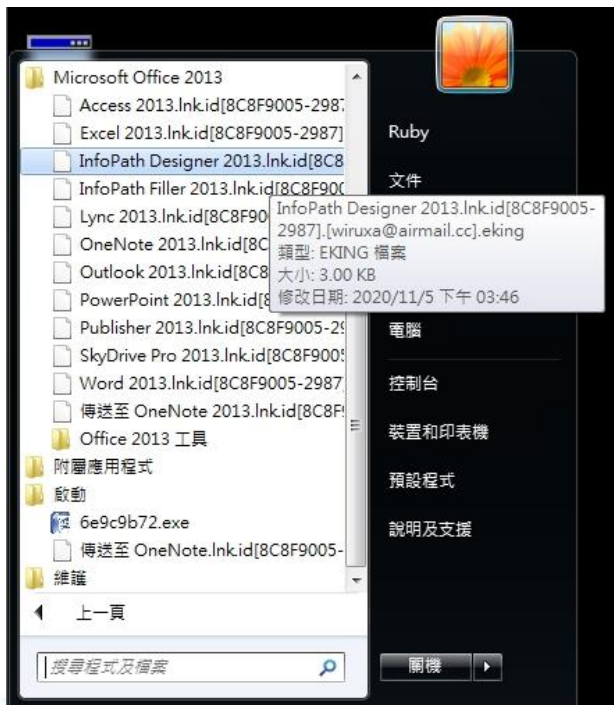
(3) 出現 Windows 防火牆已關閉的訊息。



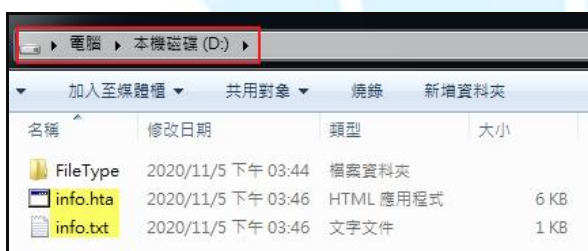
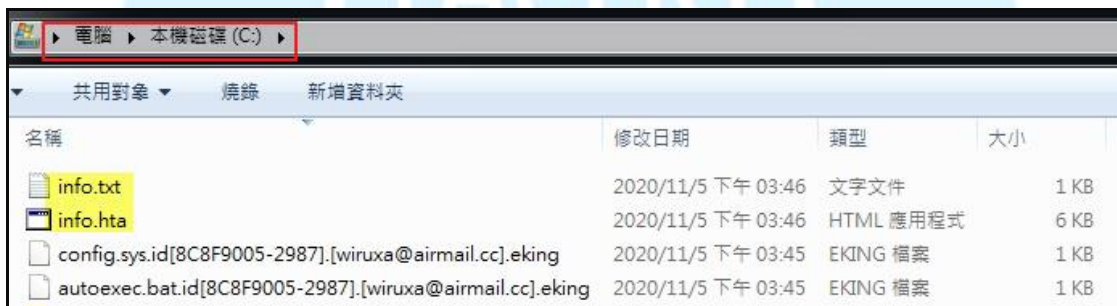
(4) 出現 4 個 encrypted 視窗於桌面。



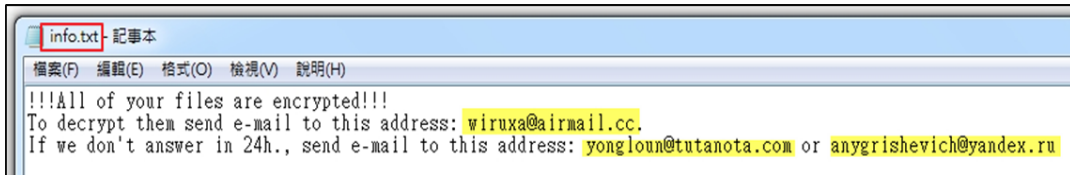
3. 檢視主機內檔案被加密的情形，發現除了 C:\windows 系統資料夾外，所有檔案(包含程式檔案)都被 6e9c9b72.exe 加密。



4. 在 C:\與 D:\內有皆有兩個檔案 info.txt 與 info.hta，而且被加密的檔案副檔名皆為 eking。這些被加密的檔案會從原檔案名稱中延伸出「id[駭客給受害主機的 id].[駭客聯絡的 E-mail].eking」等檔名。



5. 檢視 info.txt 內容，發現駭客告訴受害者你的所有檔案已被加密，想解密檔案需寄信至 wiruxa@airmail.cc 的信箱。如果 24 小時內沒有得到回應，則寄 E-mail 至 yongloun@tutanota.com 或 anygrishovich@yandex.ru。



6. 點選 info.hta 會出現 encrypted 視窗。該視窗除與 info.txt 的內容有重複外，還告訴受害者如何購買比特幣與保證免費協助將 5 個檔案解密，也警告受害者不要做哪些行為。



7. 檢視主機的背景程式內容，發現 6e9c9b72.exe 執行後會陸續執行 3 個 cmd.exe 與 4 個 mshta.exe 來進行除了加密檔案外的一些動作。

Process	Image Path	Command
6e9c9b72.exe (4772)	C:\Users\Ruby\Downloads\6e9c9b72.exe	"C:\Users\Ruby\Downloads\6e9c9b72.exe"
6e9c9b72.exe (4808)	C:\Users\Ruby\Downloads\6e9c9b72.exe	C:\Users\Ruby\Downloads\6e9c9b72.exe
6e9c9b72.exe (5432)	C:\Users\Ruby\Downloads\6e9c9b72.exe	"C:\Users\Ruby\Downloads\6e9c9b72.exe"
1. cmd.exe (5540)	C:\Windows\system32\cmd.exe	"C:\Windows\system32\cmd.exe"
vssadmin.exe (5728)	C:\Windows\system32\vssadmin.exe	vssadmin delete shadows /all /quiet
WMIC.exe (5852)	C:\Windows\System32\Wbem\WMIC.exe	wmic shadowcopy delete
bcddedit.exe (5888)	C:\Windows\system32\bcddedit.exe	bcddedit /set {default} bootstatuspolicy ignoreallfailures
bcddedit.exe (5896)	C:\Windows\system32\bcddedit.exe	bcddedit /set {default} recoveryenabled no
2. wbadm.exe (5908)	C:\Windows\system32\wbadmin.exe	wbadm delete catalog -quiet
3. cmd.exe (5548)	C:\Windows\system32\cmd.exe	"C:\Windows\system32\cmd.exe"
netsh.exe (5720)	C:\Windows\system32\netsh.exe	netsh advfirewall set currentprofile state off
netsh.exe (112)	C:\Windows\system32\netsh.exe	netsh firewall set opmode mode=disable
3. mshta.exe (3748)	C:\Windows\System32\mshta.exe	"C:\Windows\System32\mshta.exe" "C:\Users\Ruby\Desktop\info.hta"
mshta.exe (376)	C:\Windows\System32\mshta.exe	"C:\Windows\System32\mshta.exe" "C:\Users\public\desktop\info.hta"
mshta.exe (3376)	C:\Windows\System32\mshta.exe	"C:\Windows\System32\mshta.exe" "C:\info.hta"
mshta.exe (2944)	C:\Windows\System32\mshta.exe	"C:\Windows\System32\mshta.exe" "D:\info.hta"
4. cmd.exe (220)	C:\Windows\system32\cmd.exe	"C:\Windows\system32\cmd.exe"
vssadmin.exe (3104)	C:\Windows\system32\vssadmin.exe	vssadmin delete shadows /all /quiet
WMIC.exe (1176)	C:\Windows\System32\Wbem\WMIC.exe	wmic shadowcopy delete
bcddedit.exe (4308)	C:\Windows\system32\bcddedit.exe	bcddedit /set {default} bootstatuspolicy ignoreallfailures
bcddedit.exe (4296)	C:\Windows\system32\bcddedit.exe	bcddedit /set {default} recoveryenabled no
wbadm.exe (2700)	C:\Windows\system32\wbadmin.exe	wbadm delete catalog -quiet

- (1) cmd.exe 執行後會呼叫 vssadmin.exe、WMIC.exe、bcdedit.exe 與 wbadmin.exe 來執行下表所列行為。

cmd.exe (5540)	C:\Windows\system32\cmd.exe	"C:\Windows\system32\cmd.exe"
vssadmin.exe (5728)	C:\Windows\system32\vssadmin.exe	vssadmin delete shadows /all /quiet
WMIC.exe (5852)	C:\Windows\System32\Wbem\WMIC.exe	wmic shadowcopy delete
bcdedit.exe (5888)	C:\Windows\system32\bcdedit.exe	bcdedit /set {default} bootstatuspolicy ignoreallfailures
bcdedit.exe (5896)	C:\Windows\system32\bcdedit.exe	bcdedit /set {default} recoveryenabled no
wbadmin.exe (5908)	C:\Windows\system32\wbadmin.exe	wbadmin delete catalog -quiet

指令	行為
vssadmin delete shadows /all /quiet wmic shadowcopy delete	刪除影子副本
bcdedit /set {default} bootstatuspolicy ignoreallfailures bcdedit /set {default} recoveryenabled no	取消「Windows 不正常關機顯示自動修復」的功能
wbadmin delete catalog -quiet	刪除備份目錄

- (2) cmd.exe 執行後呼叫 netsh.exe 來執行下表所列行為。

cmd.exe (5548)	C:\Windows\system32\cmd.exe	"C:\Windows\system32\cmd.exe"
netsh.exe (5720)	C:\Windows\system32\netsh.exe	netsh advfirewall set currentprofile state off
netsh.exe (112)	C:\Windows\system32\netsh.exe	netsh firewall set opmode mode=disable

指令	行為
netsh advfirewall set currentprofile state off	關閉當前使用的防火牆
netsh firewall set opmode mode=disable	關閉防火牆

- (3) 執行 mshta.exe 開啟桌面與 C:\、D:\ 內的 4 個 info.hta 腳本檔案。

mshta.exe (3748)	C:\Windows\System32\mshta.exe	"C:\Windows\System32\mshta.exe" "C:\Users\Ruby\Desktop\info.hta"
mshta.exe (376)	C:\Windows\System32\mshta.exe	"C:\Windows\System32\mshta.exe" "C:\users\public\desktop\info.hta"
mshta.exe (3376)	C:\Windows\System32\mshta.exe	"C:\Windows\System32\mshta.exe" "C:\info.hta"
mshta.exe (2944)	C:\Windows\System32\mshta.exe	"C:\Windows\System32\mshta.exe" "D:\info.hta"

- (4) 再次執行 cmd.exe 呼叫 vssadmin.exe、WMIC.exe、bcdedit.exe 與 wbadmin.exe。

cmd.exe (220)	C:\Windows\system32\cmd.exe	"C:\Windows\system32\cmd.exe"
vssadmin.exe (3104)	C:\Windows\system32\vssadmin.exe	vssadmin delete shadows /all /quiet
WMIC.exe (1176)	C:\Windows\System32\Wbem\WMIC.exe	wmic shadowcopy delete
bcdedit.exe (4308)	C:\Windows\system32\bcdedit.exe	bcdedit /set {default} bootstatuspolicy ignoreallfailures
bcdedit.exe (4296)	C:\Windows\system32\bcdedit.exe	bcdedit /set {default} recoveryenabled no
wbadmin.exe (2700)	C:\Windows\system32\wbadmin.exe	wbadmin delete catalog -quiet

8. 除網路磁碟機的資料夾內檔案被加密外，後來新增於資料夾內的檔案也會馬上被加密。推測 6e9c9b72.exe 加密所有檔案後仍然在背景程式中執行著。

名稱	修改日期	類型	大小
Excel1.xlsx.id[8C8F9005-2987].[wiruxa@airmail.cc].eking	2020/11/5 下午 03:44	EKING 檔案	10 KB
NETWORK.pptx.id[8C8F9005-2987].[wiruxa@airmail.cc].eking	2020/11/5 下午 03:44	EKING 檔案	34 KB
哈囉.docx.id[8C8F9005-2987].[wiruxa@airmail.cc].eking	2020/11/5 下午 03:44	EKING 檔案	12 KB
資料庫1.accdb.id[8C8F9005-2987].[wiruxa@airmail.cc].eking	2020/11/5 下午 03:44	EKING 檔案	433 KB
You.txt.id[8C8F9005-2987].[wiruxa@airmail.cc].eking	2020/11/5 下午 03:44	EKING 檔案	1 KB
This is a test.docx.id[8C8F9005-2987].[wiruxa@airmail.cc].eking	2020/11/5 下午 04:44	EKING 檔案	871 KB

9. 查看運行中的程式會發現有兩個 6e9c9b72.exe 的程序執行著。

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Command Line
6e9c9b72.exe	0.01	4,124 K	7,076 K	4772			"C:\Users\Ruby\Downloads\6e9c9b72.exe"
6e9c9b72.exe	0.07	3,992 K	8,644 K	5432			"C:\Users\Ruby\Downloads\6e9c9b72.exe"

10. 檢視每次開機登入後的程式執行設定，發現有修改登錄檔，而且除了 6e9c9b72.exe 原來所在資料夾外，在主機內另有 3 個資料夾內存有該程式副本。這 4 個勒索病毒的程序會在重新開機後自動執行。

Autorun Entry	Image Path	Timestamp
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run		2020/11/5 下午 03:45
6e9c9b72	c:\users\ruby\appdata\local\6e9c9b72.exe	2020/8/17 上午 03:44
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run		2020/11/5 下午 03:44
6e9c9b72	c:\users\ruby\appdata\local\6e9c9b72.exe	2020/8/17 上午 03:44
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup		2020/11/5 下午 03:46
6e9c9b72.exe	c:\programdata\microsoft\windows\start menu\programs\startup\6e9c9b72.exe	2020/8/17 上午 03:44
desktop.ini.id[8C8F9005-2987].[wiruxa@airmail.cc].eking	c:\programdata\microsoft\windows\start menu\programs\startup\desktop.ini.id[8C8F9005-2987]....	2020/11/5 下午 03:46
C:\Users\Ruby\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup		2020/11/5 下午 03:46
6e9c9b72.exe	c:\users\ruby\appdata\roaming\microsoft\windows\start menu\programs\startup\6e9c9b72.exe	2020/8/17 上午 03:44
desktop.ini.id[8C8F9005-2987].[wiruxa@airmail.cc].eking	c:\users\ruby\appdata\roaming\microsoft\windows\start menu\programs\startup\desktop.ini.id[...	2020/11/5 下午 03:46
System Explorer Auto Start	c:\program files\system explorer\systemexplorer.exe	2015/3/19 下午 03:00
傳送至 OneNote.lnk.id[8C8F9005-2987].[wiruxa@airmail.cc].eking	c:\users\ruby\appdata\roaming\microsoft\windows\start menu\programs\startup\傳送至 oneno...	2020/11/5 下午 03:46
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components		2018/2/13 下午 02:13
Google Chrome	File not found: C:\Program Files\Google\Chrome\Application\86.0.4240.183\installer\chmstp.exe	
Google Chrome	c:\program files\google\chrome\application\76.0.3809.132\installer\chmstp.exe	2019/8/23 下午 01:00

11. 將 info.txt 與一個被加密的 eking 檔案上傳至 ID Ransomware 勒索病毒識別網站(<https://id-ransomware.malwarehunterteam.com>)，經檢測判定為 Phobos，而且該勒索病毒目前尚未有解密器。

Phobos

! This ransomware has no known way of decrypting data at this time.

It is recommended to backup your encrypted files, and hope for a solution in the future.

Identified by

- ransomnote_email: wiruxa@airmail.cc
- sample_extension: .id[<id>].[<email>].eking
- ransomnote_filename: info.txt
- ransomnote_keyword: !!!All of your files are encrypted!!!
- sample_bytes: 0x00 metadata divider
- custom_rule: Padding and metadata offset verified

12.6e9c9b72.exe 經 Virustotal 檢測其惡意比例高達 58/72，而且仍有 14 家防毒軟體公司的防毒軟體無法檢測出它的存在。

58
/ 72

! 58 engines detected this file

6e9c9b72d1bdb993184c7aa05d961e706a57b3becf151ca4f883a80a07fdd955

1.07 MB Size | 2020-11-05 07:22:24 UTC a moment ago

be13334c44f2e0331a6d1d6460ff9359.exe **與6e9c9b72.exe相同hash值**

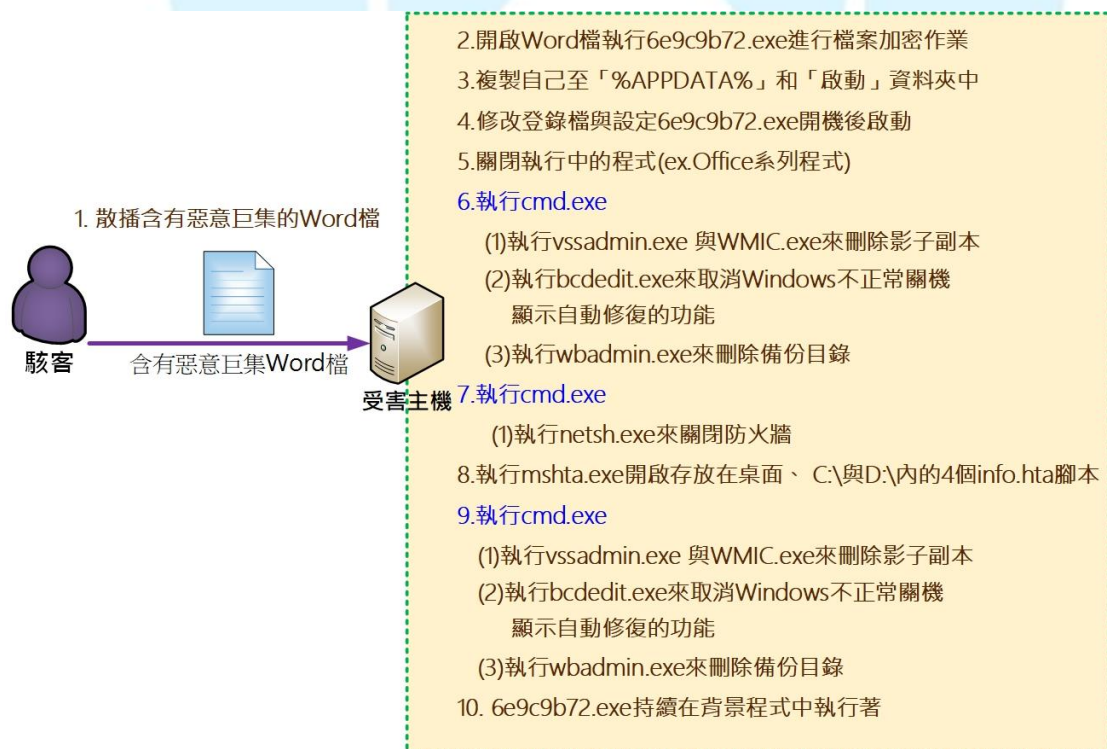
peexe

Ad-Aware	① Trojan.GenericKD.43816596	AegisLab	① Trojan.Win32.Cossta.41c
AhnLab-V3	① Trojan/Win32.Ransomware.C4197397	Alibaba	① Trojan/Win32/Cossta.41e0f057
ALYac	① Trojan.Ransom.Phobos	Antiy-AVL	① Trojan/Win32.Cossta
SecureAge APEX	① Malicious	Arcabit	① Trojan.Generic.D29C9694
Avast	① Win32:Trojan-gen	AVG	① Win32:Trojan-gen
Avira (no cloud)	① HEUR/AGEN.1138446	BitDefender	① Trojan.GenericKD.43816596
BitDefenderTheta	① Gen:NN.ZexaF.34590.evW@amNOD@...	Bkav	① W32.AIDetectVM.malware1
Comodo	① Malware@#18d9518wnlet2	CrowdStrike Falcon	① Win/malicious_confidence_100% (W)
Cybereason	① Malicious.Oa8b59	Cylance	① Unsafe
Cynet	① Malicious (score: 100)	Cyren	① W32/Trojan.SUFF-1742
DrWeb	① Trojan.MulDrop13.64400	Elastic	① Malicious (high Confidence)
Emsisoft	① Trojan.GenericKD.43816596 (B)	eScan	① Trojan.GenericKD.43816596
ESET-NOD32	① A Variant Of Win32/Kryptik.HGMS	F-Secure	① Heuristic.HEUR/AGEN.1138446
FireEye	① Generic.mg.be13334c44f2e033	Fortinet	① W32/Phobos.HGAF!tr.ransom

GData	① Trojan.GenericKD.43816596	Gridinsoft	① Ransom.Win32.Wacatac.oa
Ikarus	① Trojan.SuspectCRC	Jiangmin	① Trojan.Cossta.ahj
K7AntiVirus	① Trojan (0056e3901)	K7GW	① Trojan (0056e3901)
Kaspersky	① Trojan.Win32.Cossta.anci	MAX	① Malware (ai Score=100)
MaxSecure	① Trojan.Malware.106601437.susgen	McAfee	① W32/PinkSbot-HD!BE13334C44F2
McAfee-GW-Edition	① BehavesLike.Win32.Generic.tz	Microsoft	① Ransom:Win32/Phobos!MSR
NANO-Antivirus	① Virus.Win32.Gen.ccmw	Palo Alto Networks	① Generic.ml
Panda	① Trj/CI.A	Qihoo-360	① Generic/HEUR/QVM20.1.DD5B.Malware...
Rising	① Trojan.Generic@ML.87 (RDMK:qus9G0...	Sangfor Engine Zero	① Malware
SentinelOne (Static ML)	① DFI - Malicious PE	Sophos AV	① Mal/EncPk-APW
Sophos ML	① Mal/Generic-R + Mal/EncPk-APW	Symantec	① Trojan Horse
Tencent	① Win32.Trojan.Cossta.Pgcp	TrendMicro	① TROJ_FRS.ONA103IC20
TrendMicro-HouseCall	① TROJ_FRS.ONA103IC20	VBA32	① Trojan.Cossta
VIPRE	① Trojan.Win32.Generic!BT	Webroot	① W32.Malware.Gen

Zillya	① Trojan.Kryptik.Win32.2537744	ZoneAlarm by Check Point	① Trojan.Win32.Cossta.anci
Dr.Web vxCube	① MALWARE	Lastline	① MALWARE RANSOM TROJAN
Yomi Hunter	① MALWARE	Acronis	① Undetected

三、攻擊行為示意圖



1. 駭客散播含有惡意巨集的 Word 檔。
2. 使用者開啟惡意的 Word 檔後執行 6e9c9b72.exe 來進行檔案加密作業。
3. 6e9c9b72.exe 執行後會複製自己至主機內的「%APPDATA%」資料夾和「啟動」資料夾中。
4. 修改登錄檔與設定 6e9c9b72.exe 在主機開機後啟動。
5. 關閉執行中的程式(如:Office 系列程式)。
6. 執行 cmd.exe
 - (1)執行 vssadmin.exe 與 WMIC.exe 來刪除影子副本。
 - (2)執行 bcdedit.exe 來取消 Windows 不正常關機顯示自動修復的功能。
 - (3)執行 wbadmin.exe 來刪除備份目錄。
7. 執行 cmd.exe
 - (1)執行 netsh.exe 來關閉防火牆。
8. 執行 mshta.exe 開啟存放在桌面、C:\與 D:\內的 4 個 info.hta 腳本。
9. 再次執行 cmd.exe
 - (1) 執行 vssadmin.exe 與 WMIC.exe 來刪除影子副本。
 - (2) 執行 bcdedit.exe 來取消 Windows 不正常關機顯示自動修復的功能。
 - (3) 執行 wbadmin.exe 來刪除備份目錄。
- 10.6e9c9b72.exe 持續在背景程式中執行著。

四、總結與建議

1. 勒索病毒 Phobos 是 2019 年初被發現的，之後持續有變種產生，而且經常更改延伸的副檔名與發展新的攻擊方法。
2. 早期該病毒會透過 RDP 連線方式(3389port)散播，近期的攻擊手法改為透過帶有惡意巨集的 Word 文件檔來散播 Phobos 的 eking 變種。
3. 它感染受害主機後會複製自己本身於主機內(在「%APPDATA%」和「啟

動」資料夾中)，故受害主機重新啟動時則該勒索病毒也會啟動。

4. 該 eking 變種程式執行後會關閉防火牆、刪除影子副本、取消 Windows 不正常關機顯示自動修復的功能、刪除備份目錄與開啟勒索通知信的腳本檔案 info.hta 等行為。
5. 該病毒在加密之前會將執行中的程式(例如:Office 系列程式)關閉後才開始加密。
6. 它會產生兩種格式的勒索通知信.txt 與.hta。在完成加密的過程後會彈出.hta 的視窗，此時 Phobos 惡意程式仍然在背景中執行著，等著加密新建立的文件。
7. Phobos 勒索病毒非常有攻擊性，可以重複感染。為了防止重複感染，在處理時建議先將網路線拔除。若開機，需登入後先將該病毒所建立的複本中止執行，並且從受害主機上移除。
8. 對於此勒索病毒的預防除了平時做好資料備份外，建議不要隨意開啟不明來源的檔案。