TLP:WHITE

勒索病毒 DearCry 分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

2021 年 04 月

一、事件簡介

1. 2021/3 初 微軟發出安全公告，指出中國駭客組織 Hafnium 已利用 Microsoft Exchange Server 的 ProxyLogon 漏洞(編號:CVE-2021-26855、CVE-2021-26857、CVE-2021-26858 及 CVE-2021-27065)成功駭入郵件系統。
2. ProxyLogon 是重大的無需驗證的遠端程式碼執行（Pre-Auth Remote Code Execution）零日漏洞，可讓攻擊者得以繞過身份驗證步驟。在駭入後會植入 web shell 程式，來從遠端控制受害的 Exchange Server，包括竊取資訊、執行任意程式碼或在內部網路橫向移動等 RCE 漏洞可能造成的攻擊。
3. 在 ProxyLogon 漏洞被揭露後，陸續發生利用此漏洞的攻擊事件，其中勒索病毒 DearCry 的攻擊事件就此誕生。
4. 勒索軟體識別網站 ID-Ransomware 的建立者 Michael Gillespie 發現，從 2021 年 3 月 9 日開始，有用戶向其系統提交從 Exchange Server 上取得的新勒索通知信和被加密檔案。同時受害人還在 BleepingComputer 論壇中聲明其 Exchange Server 已被使用 ProxyLogon 漏洞進行了入侵，而且遭受 DearCry 勒索軟體攻擊。
5. McAfee 網路調查負責人 John Fokker 表示在美國、盧森堡、印度尼西亞、愛爾蘭、印度和德國等國有看到此類型的受害者。雖然檢測率仍然很低，但 Fokker 指出檢測率仍在繼續增長。

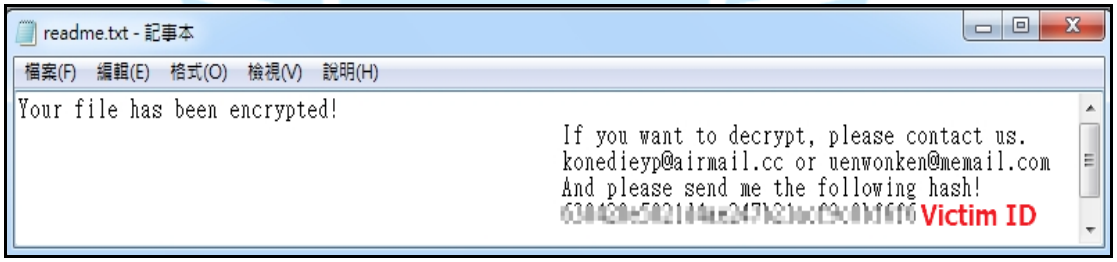
全球感染 DearCry 之受害主機數量分佈圖 (來源:McAfee Insights)

6. 為了瞭解勒索軟體 DearCry 的攻擊行為，本中心取得該類型勒索軟體的樣本後進行檢測。

二、事件檢測

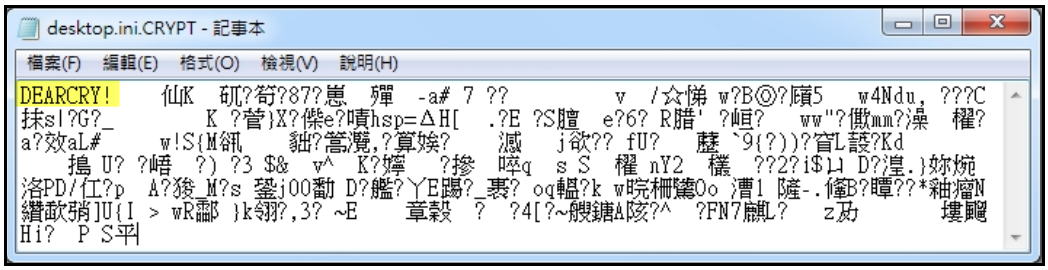
1. 首先，使用一台有掛載網路磁碟機之資料夾的 Windows 7 主機。接著將樣本 2b9838da7.exe 置於主機上執行。執行後不久同資料夾內出現副檔名為 CRYPT 的檔案，而且在桌面出現 readme.txt 的文字檔。2b9838da7.exe 在執行後仍然在原資料夾內，並未消失，可以得知它不是無檔案式的勒索軟體。

2. 開啟 readme.txt 後得知為一封勒索通知信，在信中駭客告訴受害者你的檔案已經被加密，若想解密需與駭客聯絡。隨信附上兩個駭客的 E-mail 信箱與受害主機 ID 的 Hash 值，並且要求受害者需將此 Hash 值放在聯絡的信件中。

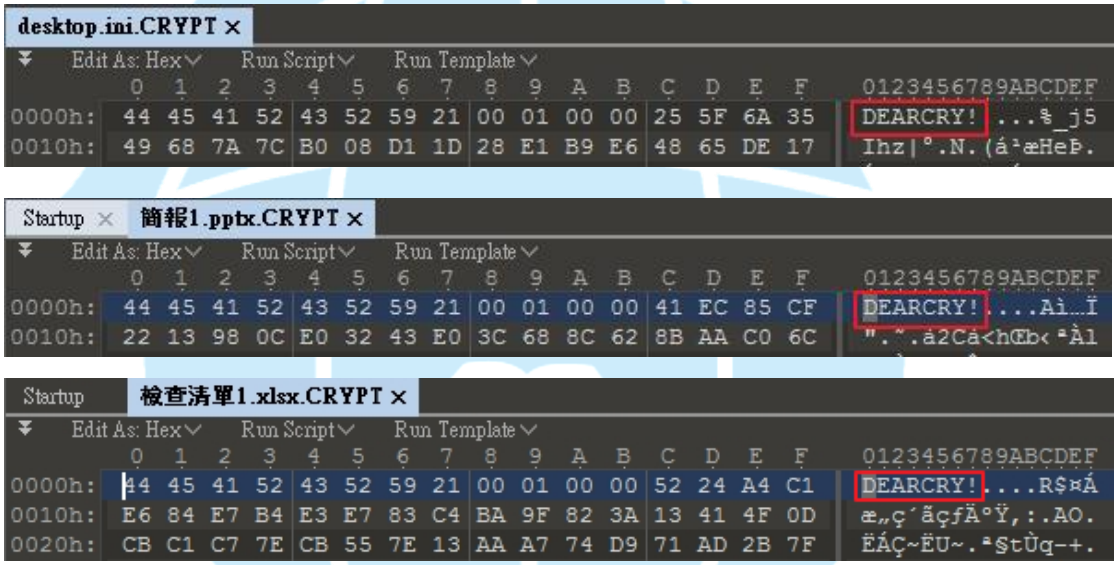


3. 搜尋 readme.txt 在主機內的所在位置，得知該檔案只出現在三個位置，分別在除了作業系統磁碟 C 槽外的兩個磁碟(Z:與 D:)內與桌面上。此特徵與一般勒索軟體會將勒索通知信放在每一個拜訪過的資料夾中之特性不同。

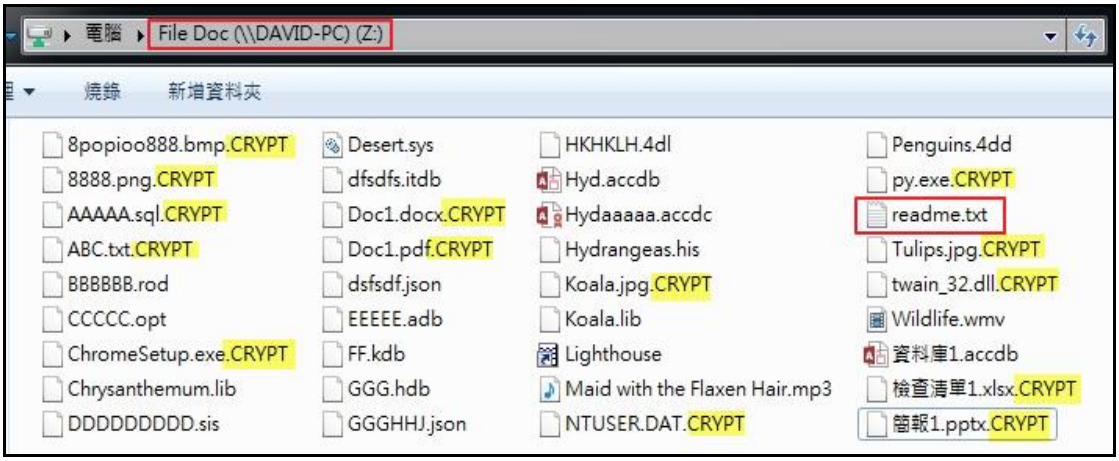
4. 以記事本打開 desktop.ini.CRYPT 後，在內容第一句出現「DEARCRY!」的用字。



5. 檢視多個被加密檔案的 Hex 內容，發現每個檔案開頭第一句都是「DEARCRY!」。此種對被加密檔案進行勒索軟體名稱標示的作法，在一般勒索軟體的攻擊中是不常見的。



6. 從網路磁碟機內檔案被加密的情形發現，並不是所有的檔案都會被加密，推測此勒索軟體只會對於某些類型的檔案進行加密，而且被加密的檔案之副檔名皆為 CRYPT。



7. 檢視 2b9838da7.exe 的程式原始碼內容，得知該勒索軟體會加密的檔案類型有「.TIF .TIFF .PDF .XLS .XLSX .XLTM .PS .PPS .PPT .PPTX .DOC .DOCX .LOG .MSG .RTF .TEX .TXT .CAD .WPS .EML .INI .CSS .HTM .HTML .XHTML .JS .JSP .PHP .KEYCHAIN .PEM .SQL .APK .APP .BAT .CGI .ASPX .CER .CFM .C .CPP .GO .CONFIG .PL .PY .DWG .XML .JPG .BMP .PNG .EXE .DLL .CAD .AVI .H.CSV .DAT .ISO .PST .PGD .7Z .RAR .ZIP .ZIPX .TAR .PDB .BIN .DB .MDB .MDF .BAK .LOG .EDB .STM .DBF .ORA .GPG .EDB .MFS」等 80 種。

```
.data:00536D18 a_tif_tiff_pdf_ db '.TIF .TIFF .PDF .XLS .XLSX .XLTM .PS .PPS .PPT .PPTX .DOC .DOCX .'
.data:00536D18                                         ; DATA XREF: sub_401640+211↑o
.data:00536D18                 db 'LOG .MSG .RTF .TEX .TXT .CAD .WPS .EML .INI .CSS .HTM .HTML  .XHT'
.data:00536D18                 db 'ML .JS .JSP .PHP .KEYCHAIN .PEM .SQL .APK .APP .BAT .CGI .ASPX .C'
.data:00536D18                 db 'ER .CFM .C .CPP .GO .CONFIG .PL .PY .DWG .XML .JPG .BMP .PNG .EXE'
.data:00536D18                 db ' .DLL .CAD .AVI .H.CSV .DAT .ISO .PST .PGD  .7Z .RAR .ZIP .ZIPX .'
.data:00536D18                 db 'TAR .PDB .BIN .DB .MDB .MDF .BAK .LOG .EDB .STM .DBF .ORA .GPG .E'
.data:00536D18                 db 'DB .MFS',0
```

8. 在 2b9838da7.exe 的程式原始碼中，發現該勒索軟體的 RSA 公開金鑰內容。

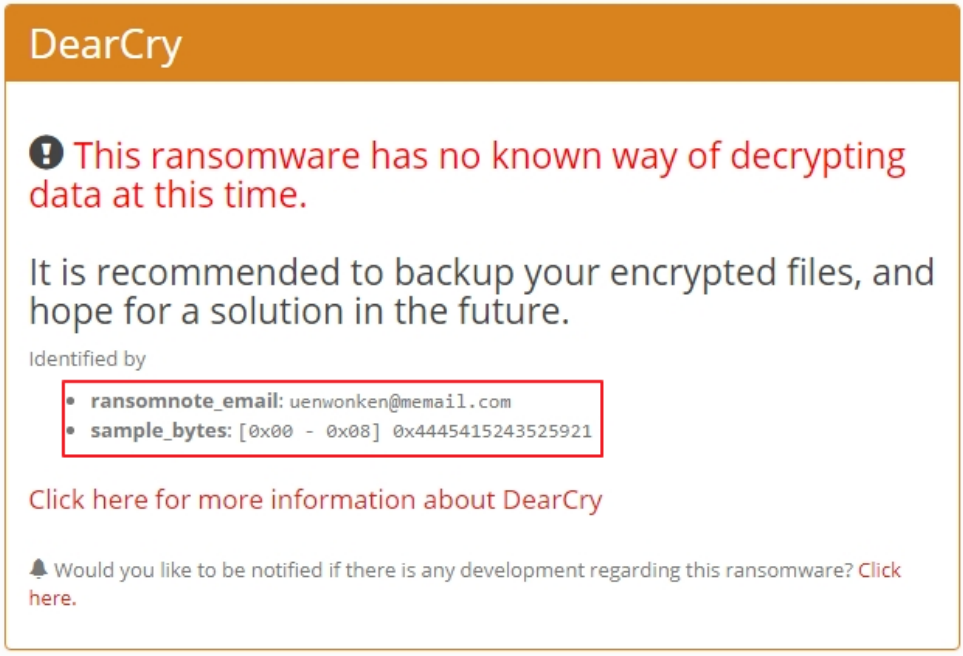
```
.data:00536A9C dword_536A9C    dd 1                    ; DATA XREF: sub_4EF593+1C↑r
.data:00536A9C                                         ; sub_4EF593+4C↑w
.data:00536AA0 aBeginRsaPublic db '-----BEGIN RSA PUBLIC KEY-----',0Ah
.data:00536AA0                                         ; DATA XREF: sub_401000+12↑o
.data:00536AA0                                         ; sub_401000+2C↑o ...
.data:00536AA0                 db 'MIIBCAKCAQEAyLBClz9hsFGRf9Fk3z0zmY2rz2J1qqGfU48DSjPU4lcwnhCi4/5+',0Ah
.data:00536AA0                 db 'C6UsAhk/dI4/5HwbfZBAiMySXNB3DxUB2hOrjDjIeVAkFjQgZ19B+KQFWkSo1ube',0Ah
.data:00536AA0                 db 'VdHjwdv74evE/ur9Lv9HM+89iZdzEpVPO+AjOTtsQgFNtmVecC2vmw9m60dgyR/1',0Ah
.data:00536AA0                 db 'CJQSg6Mob1o2NUF50AK3cIG2/lUh82ebgedXsbUJpjUMc03aTPWU4sNWjTO3o+aX',0Ah
.data:00536AA0                 db '6Z+UGULjuvcpfLDZb3tYppkqZzAHfrCt71U0q047FU8sFC1tuoNiNGKiP084KI7b',0Ah
.data:00536AA0                 db '3XEJepbSJB3UW4o4C4zHFrqmdyOoUlnqcQIBAw==',0Ah
.data:00536AA0                 db '-----END RSA PUBLIC KEY-----',0Ah,0
.data:00536C4B                 align 10h
.data:00536C50 aDear           db 'dear!!!',0
```

9. 分析 2b9838da7.exe 的程式碼，發現在 debug 資訊內存在一個 PDB 路徑資訊「c:\users\john\documents\visual studio 2008\projects\encryptfile

-svcv2\release\encryptfile.exe.pdb」，也得知該程式最後編譯的時間為 2021/3/9 16:08。

property	value
age	1
size	123
format	RSDS
guid	2C2B0CEF-F249-4C09-8C76-2B697F51FAE6
stamp	Tue Mar 09 16:08:39 2021
path	c:\users\john\documents\visual studio 2008\projects\encryptfile -svcv2\release\encryptfile.exe.pdb

10. 將一個被加密的檔案與 readme.txt 送至 ID Ransomware 勒索軟體識別網站 (https://id-ransomware.malwarehunterteam.com) 檢測，檢測結果為 DearCry 勒索軟體。此勒索軟體目前尚未有解密器可將被加密的檔案解密，建議可將被加密的檔案備份，以待未來有解密器產生時進行解密。

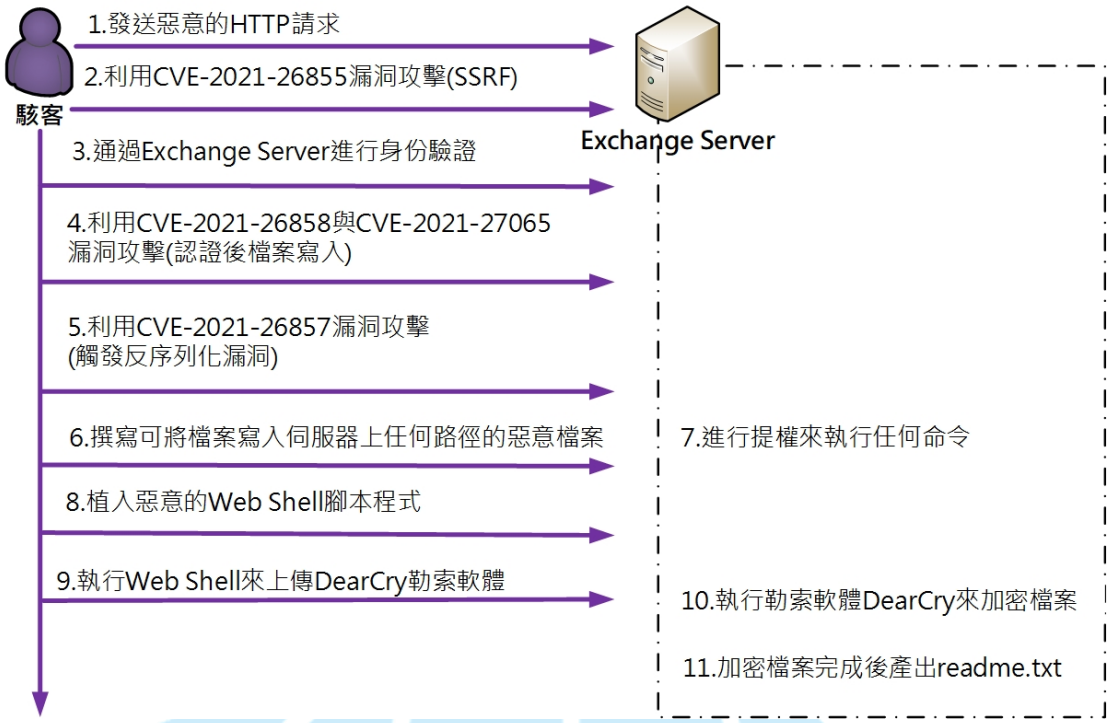


11. 2b9838da7.exe 經 virustotal 檢測其惡意比例為 53/69，多數防毒軟體以 DearCry 或 DoejoCrypt 命名它。

Ad-Aware	Trojan.GenericKD.36477740	AegisLab	Trojan.Win32.Encoder.j!c
AhnLab-V3	Ransomware/Win.DoejoCrypt.R371582	Alibaba	Ransom:Win32/generic.ali2000010
ALYac	Trojan.Ransom.Filecoder	Avast	Win32:RansomX-gen [Ransom]
AVG	Win32:RansomX-gen [Ransom]	Avira (no cloud)	TR/FileCoder.HW
BitDefender	Trojan.GenericKD.36477740	CAT-QuickHeal	Ransom.DearCry.R5
ClamAV	Win.Ransomware.Dearcry-9840778-0	Comodo	Malware@#1tube0f5ifxgx
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cylance	Unsafe
Cynet	Malicious (score: 85)	Cyren	W32/Trojan.FOGJ-5046
DrWeb	Trojan.Encoder.33592	Emsisoft	Trojan.GenericKD.36477740 (B)
eScan	Trojan.GenericKD.36477740	ESET-NOD32	A Variant Of Win32/Filecoder.DearCry.A
FireEye	Trojan.GenericKD.36477740	Fortinet	PossibleThreat.ARN.H
GData	Win32.Trojan-Ransom.DearCry.B	Gridinsoft	Ransom.Win32.Gen.sa
Ikarus	Trojan-Ransom.FileCrypter	Jiangmin	Trojan.Encoder.adj
K7AntiVirus	Trojan (005790de1)	K7GW	Trojan (005790de1)

Kaspersky	HEUR:Trojan-Ransom.Win32.Encoder.gen	Kingsoft	Win32.Troj.Undef.(kcloud)
Malwarebytes	Ransom.DearCry	MAX	Malware (ai Score=100)
MaxSecure	Trojan.Malware.73715490.susgen	McAfee	Ransom-DearCry!0E55EAD3B8FD
McAfee-GW-Edition	BehavesLike.Win32.Generic.th	Microsoft	Ransom:Win32/DoejoCrypt.A
NANO-Antivirus	Trojan.Win32.Encoder.ipilfs	Palo Alto Networks	Generic.ml
Panda	Trj/GdSda.A	Qihoo-360	Win32/Ransom.Encoder.HgIASQcA
Rising	Ransom.DearCry!1.D3C7 (CLOUD)	Sangfor Engine Zero	Ransom.Win32.DoejoCrypt.A
SentinelOne (Static ML)	Static AI - Suspicious PE	Sophos	Troj/Ransom-GFE
TACHYON	Ransom/W32.DearCry.1322496	Tencent	Win32.Trojan.Filecoder.Hfh
TrendMicro	Ransom.Win32.DEARCRY.THCABBA	TrendMicro-HouseCall	Ransom.Win32.DEARCRY.THCABBA
VBA32	TrojanRansom.Encoder	VIPRE	Trojan.Win32.Generic!BT
ViRobot	Trojan.Win32.Z.Agent.1322496.Q	Webroot	W32.Ransomware.Dearcry
Zillya	Trojan.Encoder.Win32.2195	Acronis	Undetected

三、攻擊行為示意圖



1. 駭客以 443port 發送惡意的 HTTP 請求。
2. 利用 CVE-2021-26855 漏洞進行伺服器請求偽造 SSRF 攻擊。
3. 通過 Exchange Server 進行身份驗證。
4. 利用 CVE-2021-26858 與 CVE-2021-27065 漏洞，進行在身份驗證後構造惡意請求，並在系統上寫入任意檔案等攻擊行為。
5. 利用 CVE-2021-26857 漏洞，通過構造惡意請求，觸發反序列化漏洞，在伺服器上執行惡意代碼。
6. 撰寫可將檔案寫入伺服器上任何路徑的惡意檔案。
7. 進行提權來執行任何命令。
8. 植入惡意的 Web Shell 腳本程式。
9. 執行 Web Shell 腳本程式將勒索軟體 DearCry 上傳至 Exchange Server。
10. 執行勒索軟體 DearCry 來加密 Exchange Server 內的檔案。
11. 勒索軟體 DearCry 加密檔案完成後產出 readme.txt 的勒索通知信。

四、總結與建議

1. 由於 ProxyLogon 漏洞被揭露，導致利用漏洞來攻擊的事件頻繁，其中利用勒索病毒 DearCry 來進行攻擊的事件也不少。從分析 DearCry 樣本觀察到 DearCry 具有下列特徵:

   (1) 執行後 DearCry 勒索軟體不會在原地消失，不是無檔案式的勒索病毒。

   (2) 它只會對特定檔案類型的檔案進行加密，而被加密後的檔案之副檔名皆為 CRYPT。

   (3) 每一個被加密檔案的 Hex 內容開頭第一句都是「DEARCRY!」。

   (4) 在加密作業完成後，在主機桌面與其他除 C:外的磁碟機第一層會出現勒索通知信 readme.txt。

   (5) 在程式原始碼中，發現該勒索軟體的 RSA 公開金鑰內容。

   (6) 分析程式原始碼會發現在 debug 資訊內存在一個 PDB 路徑資訊。

   (7) 該勒索軟體的惡意比例高達 53/69。

   (8) 多數防毒軟體公司以 DearCry 或 DoejoCrypt 命名它。

   (9) 該勒索軟體目前尚未有解密器產生。

2. 在預防 DearCry 勒索軟體攻擊 Exchange Server 方面，提供下列建議措施給大家參考。

   (1) 修補 Exchange Server 的漏洞。

   (2) 定期備份使用者 Mail 信箱內的信件與信件聯絡人資訊。

   (3) 定期更新防毒軟體的病毒碼與更新 Exchange Server 的系統。

3. 在 Exchange Server 的資安防護方面，除了修補漏洞外，有下列建議措施提供參考。

   (1)檢視 Exchange Server 是否有駭入跡象或存在 web shell。

   (2)安裝微軟一鍵式工具 EOMT，進行完整的 AV 掃描。

   (3)檢查使用者及使用者群組是否有可疑的新增帳號，可透過查找事件檢視器紀錄內的 Event ID:4720，來確認是否有建立新的帳號。(「Event ID:4720」表示「已建立使用者帳戶」)

(4)變更所有使用者帳號和系統管理員帳號之密碼。

(5)檢查系統 RDP、防火牆、WMI 訂閱以及 Windows 遠程管理（WinRM）是否遭到變更。

(6)檢查系統是否有新增的服務、排程或啟動物件，或是新安裝的影子 IT 工具(如非微軟的 RDP 及遠端存取工具)。

(7)檢查 Exchange 電子郵件轉發設定（ForwardingAddress 和 ForwardingSMTPAddress 屬性）、郵件收件規則以及 Exchange 傳輸規則。

(8)檢視事件檢視器之紀錄，查找是否有 Event ID 為 1102。若有，表示駭客曾經清除系統安全性審核紀錄，來企圖隱藏蹤跡。(「Event ID:1102 」表示「已清除審核記錄」)

4. DearCry IOC: 以下是 DearCry 樣本相關的檔案雜湊碼。

No	SHA256
1	2b9838da7edb0decd32b086e47a31e8f5733b5981ad8247a2f9508e232589bff
2	e044d9f2d0f1260c3f4a543a1e67f33fcac265be114a1b135fd575b860d2b8c6
3	feb3e6d30ba573ba23f3bd1291ca173b7879706d1fe039c34d53a4fdcdf33ede
4	fdec933ca1dd1387d970eeea32ce5d1f87940dfb6a403ab5fc149813726cbd65
5	10bce0ff6597f347c3cca8363b7c81a8bff52d2ff81245cd1e66a6e11aeb25da
6	6834d9f4a9e1888d82c70b72f30ced8aa68c009b55d03efffc94c466fbb3d047
7	17c5161451b5edd31d903fb020afc7f9f2f130fea8fbd9248e069dde7f80efa3

五、參考資料

1. 微軟：修補完 Exchange Server 漏洞還不能掉以輕心
https://www.ithome.com.tw/news/143514

2. Analyzing attacks taking advantage of the Exchange Server vulnerabilities
https://www.microsoft.com/security/blog/2021/03/25/analyzing-attacks-taking-ad

vantage-of-the-exchange-server-vulnerabilities/

3. Guidance for responders: Investigating and remediating on-premises Exchange Server vulnerabilities
https://msrc-blog.microsoft.com/2021/03/16/guidance-for-responders-investigating-and-remediating-on-premises-exchange-server-vulnerabilities/

4. 微軟一鍵式工具 EOMT：
https://msrc-blog.microsoft.com/2021/03/15/one-click-microsoft-exchange-on-premises-mitigation-tool-march-2021/

5. DearCry ransomware attacks Microsoft Exchange with ProxyLogon exploits
https://www.bleepingcomputer.com/news/security/dearcry-ransomware-attacks-microsoft-exchange-with-proxylogon-exploits/