

個案分析-

利用 DDE 散播 Locky 病毒
的 Word 文檔事件分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

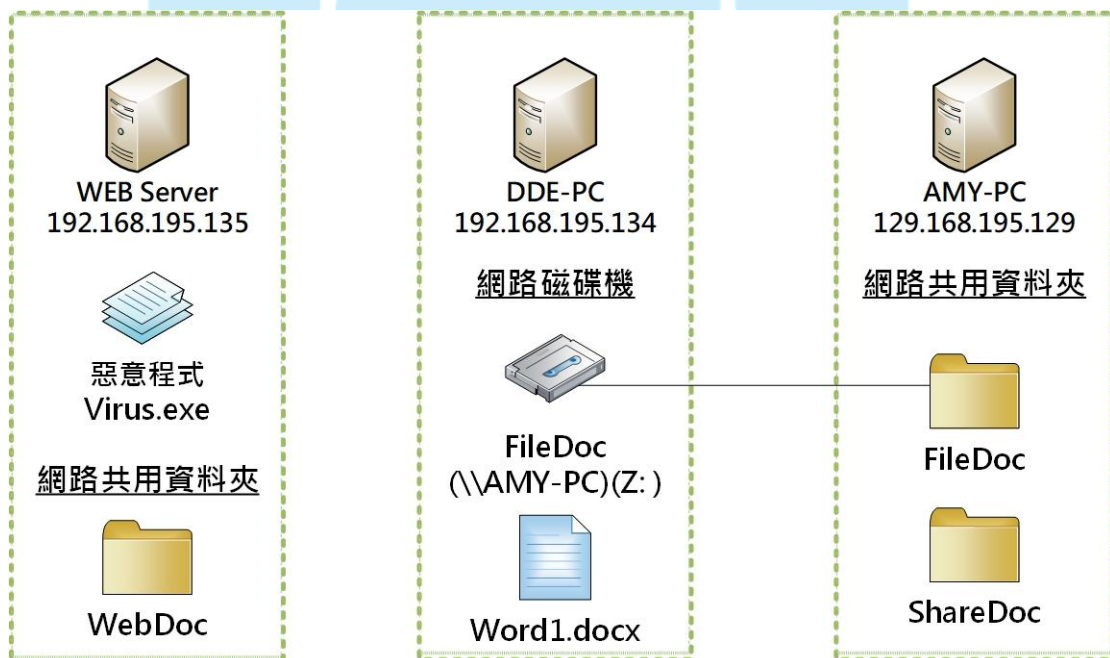
106 年 12 月

I. 事件簡介

1. 在 2017 年 10 月有愈來愈多的駭客濫用微軟 Windows 中的動態資料交換 (Dynamic Data Exchange, DDE) 協定來散布惡意程式。
2. DDE 協定是微軟 Windows 與 Office 中用來於不同程式中交換資料的協定之一，它可在共享資料的程式間傳遞訊息，並藉由共享記憶體交換資料。
3. 勒索病毒的家族繁多，其中一個著名勒索病毒家族 Locky 勒索病毒，在 2017 年 9 月產生一個新的以「.YKCOL」為副檔名的 Locky 變種病毒。
4. 在 2017 年 10 月發生 Locky 變種病毒透過 DDE 協定散播的事件，為了瞭解其攻擊與感染過程，本中心在取得樣本後進行分析。

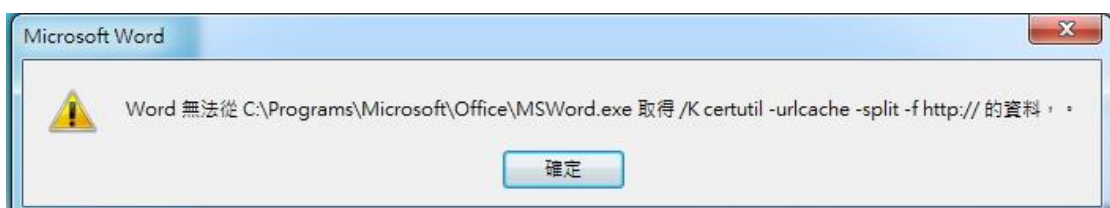
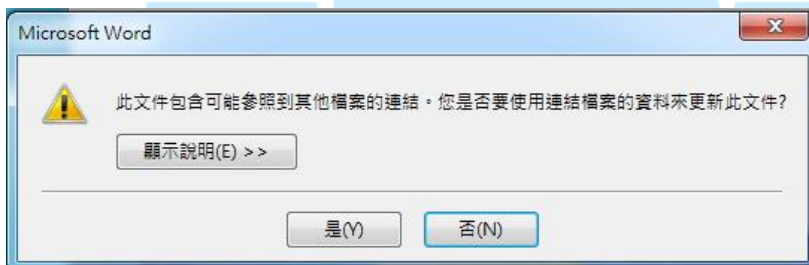
II. 事件檢測

1. 使用 3 台 Windows 7 的 VM 虛擬主機進行隔離環境測試，並且設定一些網路共用資料夾與網路磁碟機，詳細內容如下圖所示。



本案檢測的三個主機所代表的角色分別敘述如下：

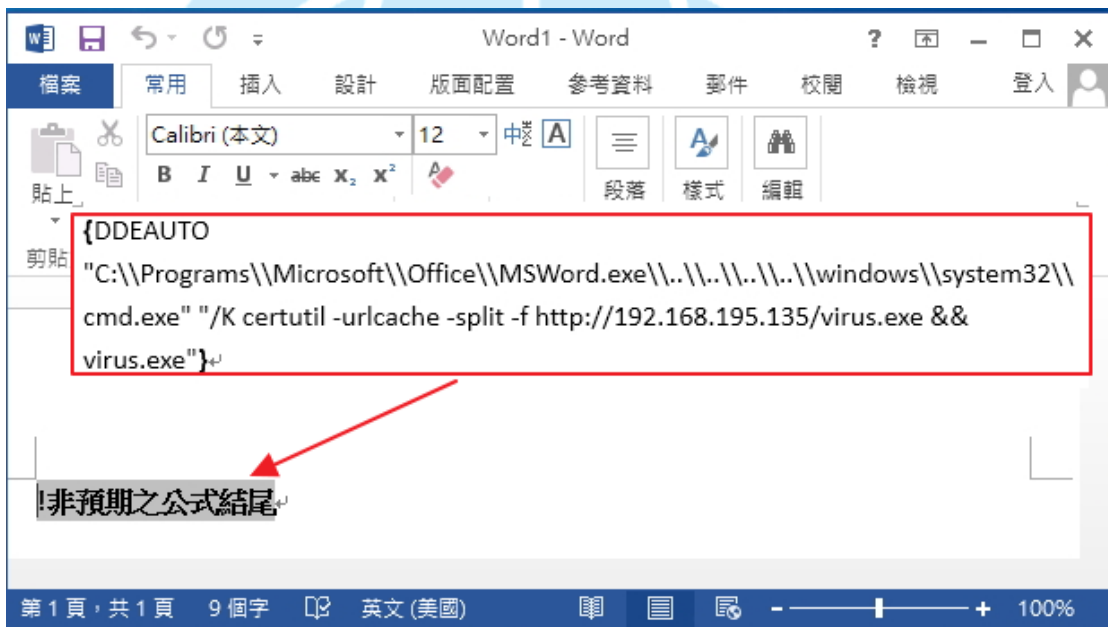
- (1)WEB Server：為含有惡意程式 Virus.exe 的網站伺服器，觀察受害主機是否會連至網站伺服器下載惡意程式。另外，因為它與受害主機是同一個網域，我們也安排一個網路共用資料夾 WebDoc，觀察看看受害主機中毒後是否會感染它。
 - (2)DDE-PC：為受害主機，會收到含有 Word1.docx 的郵件，設定一個從同一區域網路連過來的 AMY-PC 下的 FileDoc 網路共用資料夾為網路磁碟機 Z，並觀察在有設定網路磁碟機的狀況下病毒擴散之情形。
 - (3)AMY-PC：與 DDE-PC 為同一個區域網路的主機，此主機上有兩個網路共享資料夾，其中一個 FileDoc 為 DDE-PC 的網路磁碟機資料夾，另一個 ShareDoc 為一般網路共用資料夾。
2. 開啟含有 DDE 的 Word1.docx 檔案後，依序出現三個訊息視窗，在點選 2 次「是」與「確定」後即關閉視窗，並且看到 Word 檔的內文，同時在桌面上出現一個 virus.exe 執行檔。



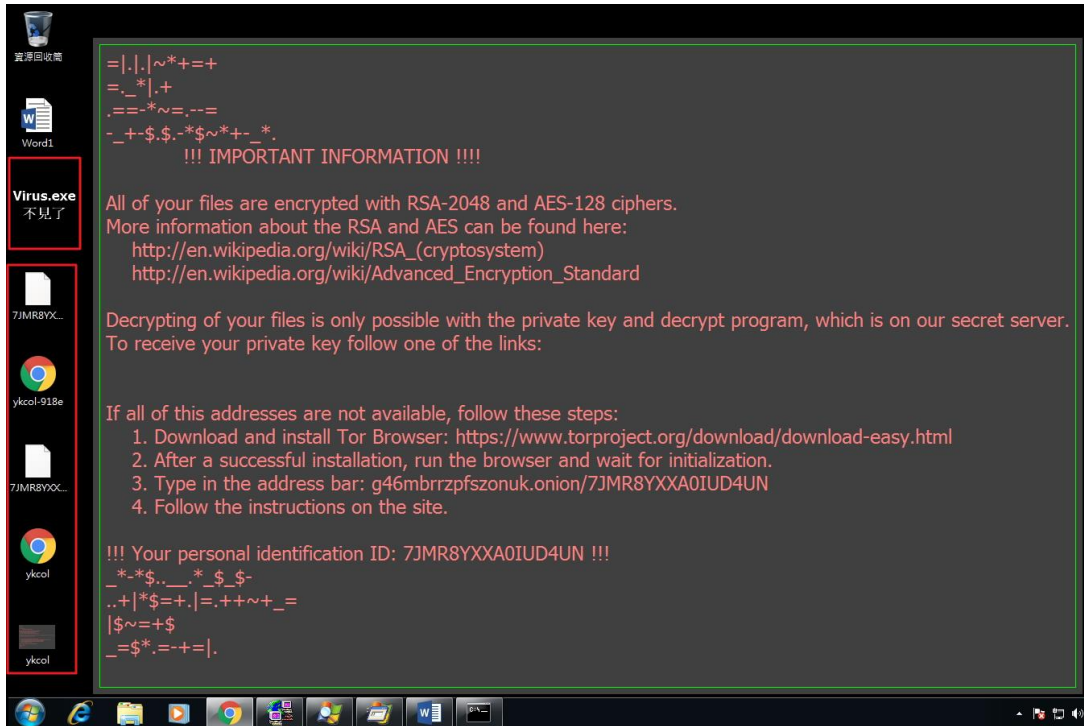
下面表格為針對三個訊息視窗的按鈕選擇所可能產生的程式執行結果。

No	第一個訊息	第二個訊息	第三個訊息	結果
1	否	-	-	看到 Word 內文
2	是	否	確定	看到 Word 內文
3	是	是 (下載惡意程式)	確定	下載惡意程式與 看到 Word 內文

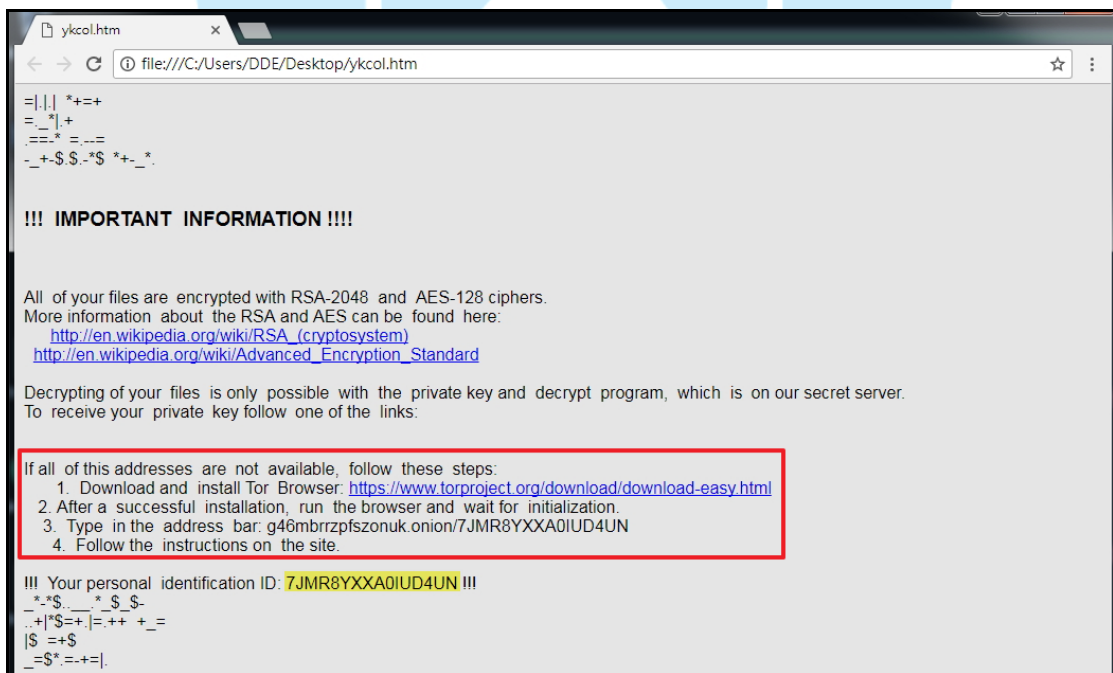
3. 檢視 Word1.docx 內文，發現 Word 的功能變數 (Field) 設定有嵌入 DDE，而且會在文件開啟時自動執行，駭客可用它來開啟命令提示，並且連至某網站下載與執行惡意程式。



4. 在 Word1.docx 開啟後不久，出現一些加密檔案，會開啟一個 ykcol.htm 網頁與一個 ykcol.bmp 圖檔，並且 ykcol.bmp 圖檔也變成電腦桌布，最後原先桌面 virus.exe 檔案消失，可見程式 virus.exe 具有自我毀滅機制，能讓受害者找不到它的存在。

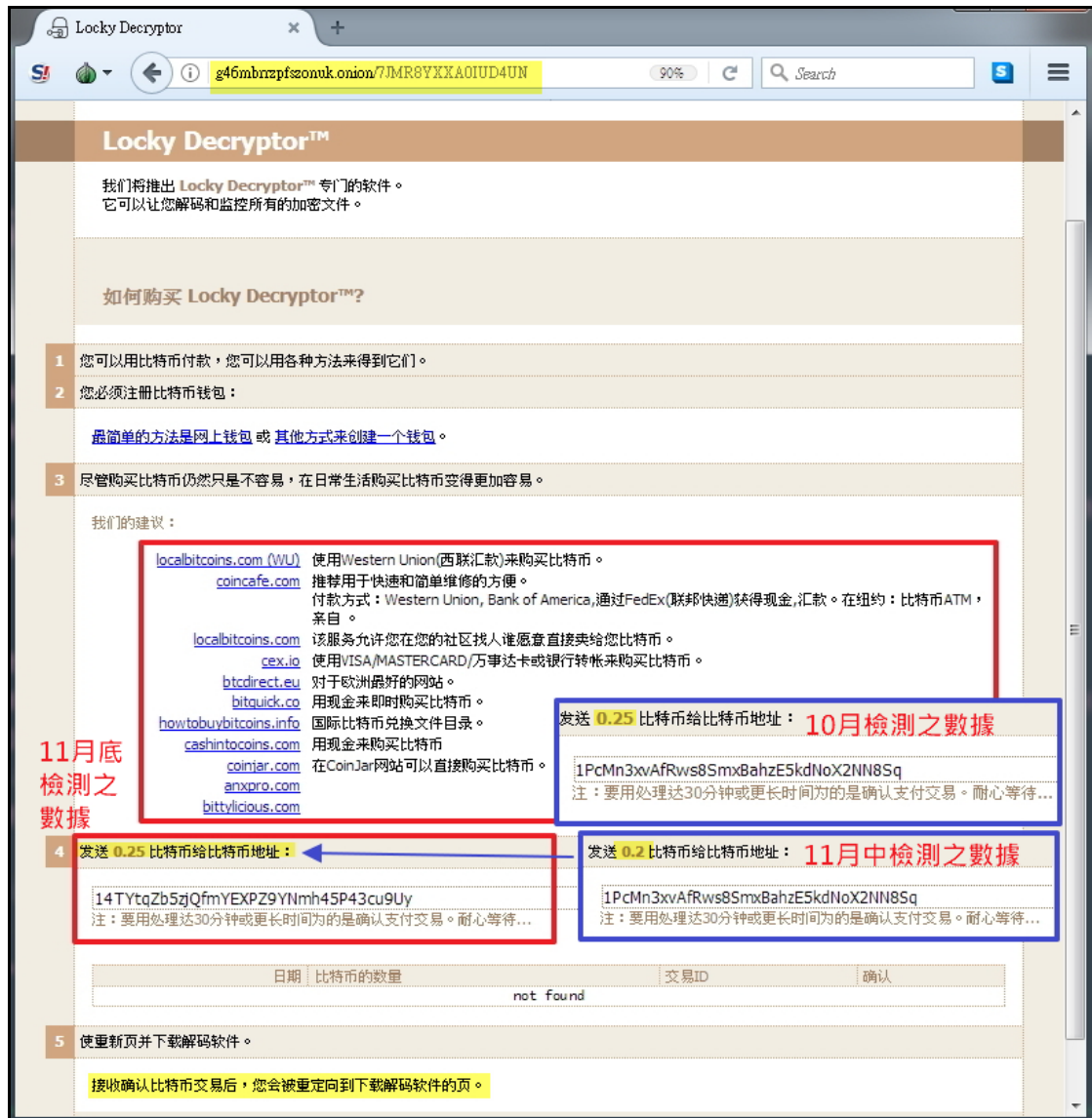


5. 查看 ykcol.htm 內容，發現內容為告訴受害者如何取得解密金鑰的資訊，駭客提供受害者一個個人識別 ID:7JMR8YXXA0IUD4UN，請受害者下載並安裝 Tor 瀏覽器，之後在瀏覽器上打網址：g46mbrrzpfsonuk.onion/7JMR8YXXA0IUD4UN 即可看到訊息。

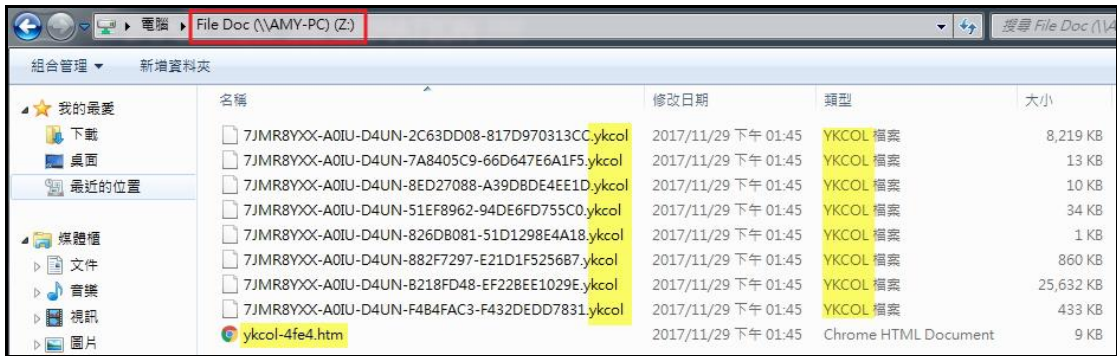


6. 透過 Tor 瀏覽器，我們可以得知駭客告訴受害者購買比特幣的管道有哪些，受害者需支付 0.25 個比特幣到駭客所提供的比特幣地址內，經比特幣交易被

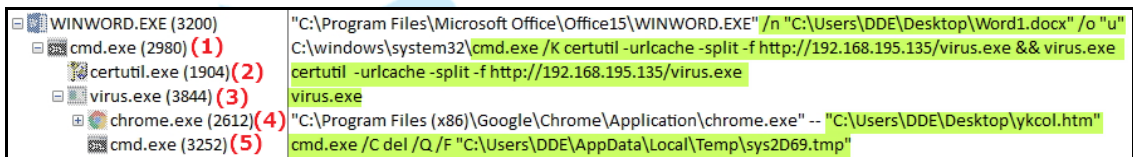
確認後，受害者會被重新導向解密金鑰下載頁面。另外，比較 10 月、11 月中旬與 11 月底三次檢測發現，駭客要求受害者支付的比特幣從原先的 0.25 個降為 0.2 個，又在半個月後升回 0.25 個比特幣，可見駭客隨時會調整要求受害者給付的比特幣數量。



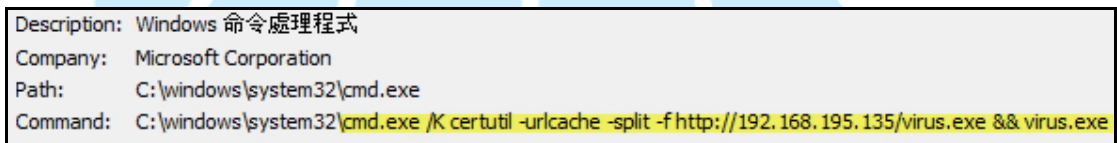
7. 查看檔案被加密的情形，發現在每個被加密的檔案資料夾中會有一個以「ykcol-4 位英文字母與數字混合.htm」命名的網頁檔，而被加密的檔案名稱皆為「受害者識別 ID-8 位英文字母與數字混合-12 位英文字母與數字混合.ykcol」，也發現在網路磁碟機 Z 內的檔案都被加密，但 C:\windows 與 C:\program files 內檔案沒有被加密的情形。



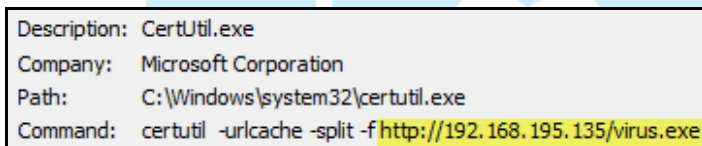
8. 檢視背景程式運作情形，發現在開啟 Word1.docx 檔案後，陸續呼叫 cmd.exe、certutil.exe、virus.exe、chrome.exe 與 cmd.exe 等程式。



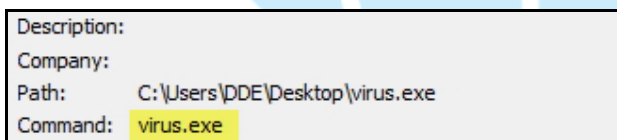
- (1) 當 cmd.exe 執行後，會呼叫 certutil.exe。



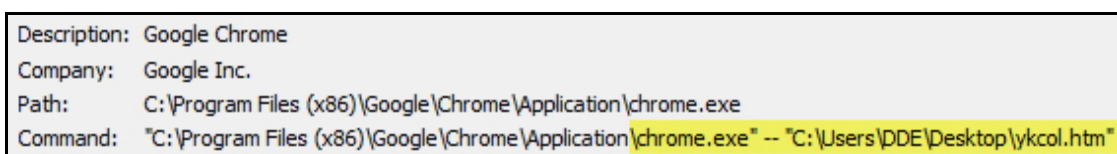
- (2) 當 certutil.exe 執行後，會連至網站下載惡意程式 virus.exe。



- (3) 當執行 virus.exe 後，受害主機內的檔案開始被加密。



- (4) 當 Chrome.exe 執行時，表示已完成受害主機內檔案的加密作業，接者會開啟 ykcol.htm 來告訴受害者檔案已被加密與如何下載安裝 Tor 瀏覽器來取得付款資訊。



(5)最後當執行 cmd.exe 時，表示此時惡意程式在完成檔案加密作業後會刪除自己本身，並且刪除 temp 資料夾內的 tmp 檔資訊。

```
Description: Windows 命令處理程式  
Company: Microsoft Corporation  
Path: C:\Windows\SysWOW64\cmd.exe  
Command: cmd.exe /C del /Q /F "C:\Users\DDE\AppData\Local\Temp\sys2D69.tmp"
```

9. 透過 Virustotal 網站檢測 Word1.docx，偵測率為 19/60，可見其不容易被大多數的防毒軟體檢測出來，而且有多家防毒軟體公司判定它為 DDE 的 Downloader(下載器)。



virustotal

SHA256: 73a0cc2d1d78ada54bfaaff34855476e588eb2d3ba9f5f8f9471e1643f9793b1e

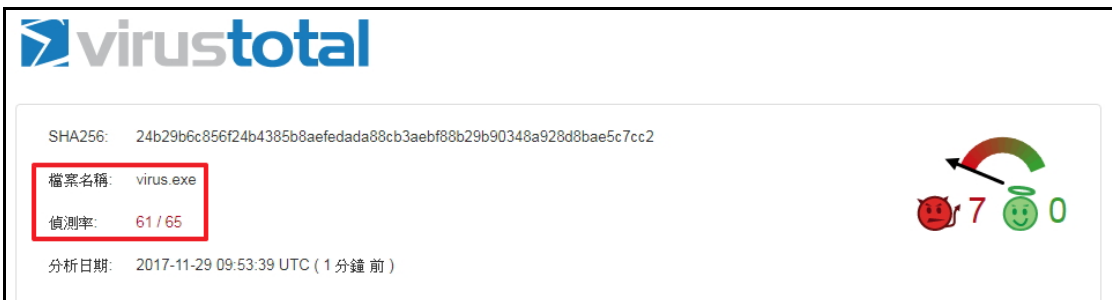
檔案名稱: Word1.docx
偵測率: 19 / 60

分析日期: 2017-11-29 06:56:07 UTC (0 分鐘前)



防毒	結果	更新
Ad-Aware	Trojan.Downloader.DDE.Gen.1	20171129
Arcabit	Trojan.Downloader.DDE.Gen.1	20171129
Avira (no cloud)	HEUR/Downloader.DDE	20171128
Baidu	MSWord.Trojan.Agent.h	20171129
BitDefender	Trojan.Downloader.DDE.Gen.1	20171129
ClamAV	Win.Downloader.CertutilURLCache-6335697-0	20171129
Emsisoft	Trojan.Downloader.DDE.Gen.1 (B)	20171129
ESET-NOD32	VBA/DDE.A	20171129
F-Secure	Trojan.Downloader.DDE.Gen.1	20171129
GData	Trojan.Downloader.DDE.Gen.1	20171129

10. 將 virus.exe 送至 Virustotal 網站檢測，偵測率為 61/65，可見其惡意比例相當高，而且多家知名防毒軟體公司判定它為 Locky 勒索病毒的變種。




virustotal

SHA256: 24b29b6c856f24b4385b8aefedada88cb3aebf88b29b90348a928d8bae5c7cc2

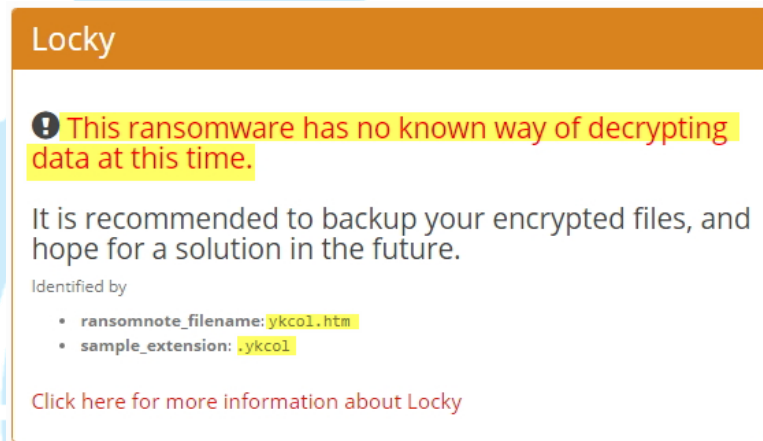
檔案名稱: virus.exe
偵測率: 61 / 65

分析日期: 2017-11-29 09:53:39 UTC (1 分鐘前)



SUPERAntiSpyware	Ransom.Locky/Variant	20171129
Symantec	Ransom.Locky.B	20171129
Tencent	Suspicious.Heuristic.Gen.b.0	20171129
TheHacker	Trojan/Kryptik.fwst	20171126
TrendMicro	Ransom_LOCKY.TH918	20171129
TrendMicro-HouseCall	Ransom_LOCKY.TH918	20171129

11. 將 ykcol.htm 與被加密的檔案上傳至勒索病毒辨別網站 (https://id-ransomware.malwarehunterteam.com)，檢測結果為 Locky 勒索病毒，目前此病毒沒有解密檔案的方式，只能將被加密的檔案備份，等未來有解密方式時才解密。



12. 從封包內容檢視，觀察到惡意程式執行後會對內部網路進行 139 port 與 445 port 的掃描，並嘗試針對能夠存取的共享資料夾進行加密，若有連接網路磁碟機或 NAS 就有可能所儲存的檔案遭受到破壞。

Time	Service	Size	Events	Displaying 1 - 4 of 4
2017-Nov-29 13:36:12	IP / TCP / SMB	3.33 KB	192.168.195.134 -> 192.168.195.129	49546 -> 139 (netbios-ssn)
2017-Nov-29 13:44:56	IP / TCP / SMB	3.32 KB	192.168.195.134 -> 192.168.195.129	49551 -> 139 (netbios-ssn)
2017-Nov-29 13:48:18	IP / TCP / SMB	3.33 KB	192.168.195.134 -> 192.168.195.129	49556 -> 139 (netbios-ssn)
2017-Nov-29 14:00:23	IP / TCP / SMB	3.33 KB	192.168.195.134 -> 192.168.195.129	49568 -> 139 (netbios-ssn)

Time	Service	Size	Events	Displaying 1 - 25 of 25
2017-Nov-29 13:36:08	IP / TCP / SMB	2.41 KB	192.168.195.134 -> 192.168.195.129	49545 -> 445 (cifs)
2017-Nov-29 13:44:57	IP / TCP / SMB	2.37 KB	192.168.195.134 -> 192.168.195.135	49552 -> 445 (cifs)
2017-Nov-29 13:44:57	IP / TCP / SMB	1.94 KB	192.168.195.134 -> 192.168.195.135	49553 -> 445 (cifs)
2017-Nov-29 13:44:57	IP / TCP / SMB	1.94 KB	192.168.195.134 -> 192.168.195.135	49554 -> 445 (cifs)
2017-Nov-29 13:32:59	IP / TCP / SMB	8.00 MB	192.168.195.134 -> 192.168.195.129	49540 -> 445 (cifs)
2017-Nov-29 13:44:59	IP / TCP / SMB	8.00 MB	192.168.195.134 -> 192.168.195.129	49540 -> 445 (cifs)
2017-Nov-29 13:44:59	IP / TCP / SMB	8.00 MB	192.168.195.134 -> 192.168.195.129	49540 -> 445 (cifs)
2017-Nov-29 13:44:59	IP / TCP / SMB	8.00 MB	192.168.195.134 -> 192.168.195.129	49540 -> 445 (cifs)
2017-Nov-29 13:45:00	IP / TCP / SMB	8.00 MB	192.168.195.134 -> 192.168.195.129	49540 -> 445 (cifs)

13. 檢視封包內容，發現受害主機連到網站下載 virus.exe 的資訊。

```

RSA Security Analytics Reconstruction for session ID: 2 (Source 192.168.195.134 : 49548, Target 192.168.195.135 : 80)
Time 11/29/2017 13:43:55 to 11/29/2017 13:43:55 Packet Size 490,198 bytes Payload Size 483,750 bytes
Protocol 2048/5/80 - Flags Keep-Alive Partial-Assembled AppMeta-NoneNetMeta-None Packet Count 113

R E Q U E S T
  GET /virus.exe HTTP/1.1
  Cache-Control: no-cache
  Connection: Keep-Alive
  Pragma: no-cache
  Accept: */*
  User-Agent: Microsoft-CryptoAPI/6.1
  Host: 192.168.195.135

R E S P O N S E
  HTTP/1.1 200 OK
  Content-Type: application/octet-stream
  Last-Modified: Tue, 19 Sep 2017 04:33:44 GMT
  Accept-Ranges: bytes
  ETag: "04f979031d31:0"
  Server: Microsoft-IIS/7.5
  Date: Wed, 29 Nov 2017 05:43:55 GMT
  Content-Length: 660480

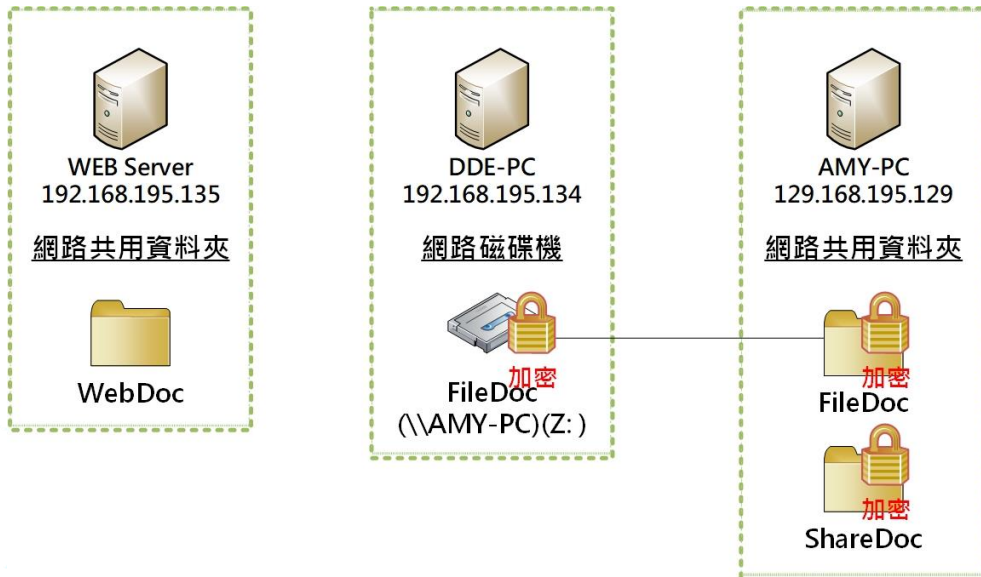
MZ  曙 煽 碌 !This program cannot be run in DOS mode.
$PELOB V'突@
-
  慮 伊 確 .textV劃 `..rdata46韞@.data z喚 .rsrcP n@ABDEGHJKMN@ACDFG IJLMO@BCEFH
  HIKLNOABDEGHJKMN@ACDFG IJLMO@BCEFH IKLNOABDEGHJKMN@ACDFG IJLMO@BCEFH IKLNOABDEGHJKMN@
  ACDFG IJLMO@BCEFH IKLNOABDEGHJKMN@ACDFG IJLMO@BCEFH IKLNOABDEGHJKMN@ACDFG IJLMO@BCEFH I
  KLNOABDEGHJKMN@ACDFG IJLMO@BCEFH IKLNOABDEGHJKMN@ACDFG IJLMO@BCEFH IKLNOABDEGHJKMN@AC
  DFG IJLMO@BCEFH IKLNOABDEGHJKMN@ACDFG IJLMO@BCEFH IKLNOABDEGHJKMN@ACDFG IJLMO@BCEFH I
  NOABDEGHJKMN@ACDFG IJLMO@BCEFH IKLNOABDEGHJKMN@ACDFG IJLMO@BCEFH IKLNOABDEGHJKMN@ACDF
  G IJLMO@BCEFH IKLNOABDEGHJKMN@ACDFG IJLMO@BCEFH IKLNOABDEGHJKMN@ACDFG IJLMO@BCEFH I
  ABDEGHJKMN@ACDFG IJLMO@BCEFH IKLNOABDEGHJKMN@ACDFG IJLMO@BCEFH IKLNOABDEGHJKMN@ACDFG
  IJLMO@BCEFH IKLNOABDEGHJKMN@ACDFG IJLMO@BCEFH IKLNOABDEGHJKMN@ACDFG IJLMO@BCEFH IKLNOA
  BDEGHJKMN@ACDFG IJLMO@BCEFH IKLNOABDEGHJKMN@ACDFG IJLMO@BCEFH IKLNOABDEGHJKMN@ACDFG I
  NO@BCEFH IKLNOABDEGHJKMN@ACDFG IJLMO@BCEFH IKLNOABDEGHJKMN@ACDFG IJLMO@BCEFH IKLNOAB
  DEGHJKMN@ACDFG IJLMO@BCEFH IKLNOABDEGHJKMN@ACDFG IJLMO@BCEFH IKLNOABDEGHJKMN@ACDFG I
  NO@BCEFH IKLNOABDEGHJKMN@ACDFG IJLMO@BCEFH IKLNOABDEGHJKMN@ACDFG IJLMO@BCEFH IKLNOAB
  DEGHJKMN@ACDFG IJLMO@BCEFH IKLNOABDEGHJKMN@ACDFG IJLMO@BCEFH IKLNOABDEGHJKMN@ACDFG I
  NO@BCEFH IKLNOABDEGHJKMN@ACDFG IJLMO@BCEFH IKLNOABDEGHJKMN@ACDFG IJLMO@BCEFH IKLNOA
  BDEGHJKMN@ACDFG IJLMO@BCEFH IKLNOABDEGHJKMN@ACDFG IJLMO@BCEFH IKLNOABDEGHJKMN@ACDFG
  JKMN@ACDFG IJLMO@BCEFH IKLNOY
  DS#A亦孺哇 P  -!綫 綫 綫 綫 綫 突 P  綫 綫
  
```

14. 檢視封包內容，發現惡意程式將網路磁碟機 Z 內檔案加密後更改檔案名稱的資訊。

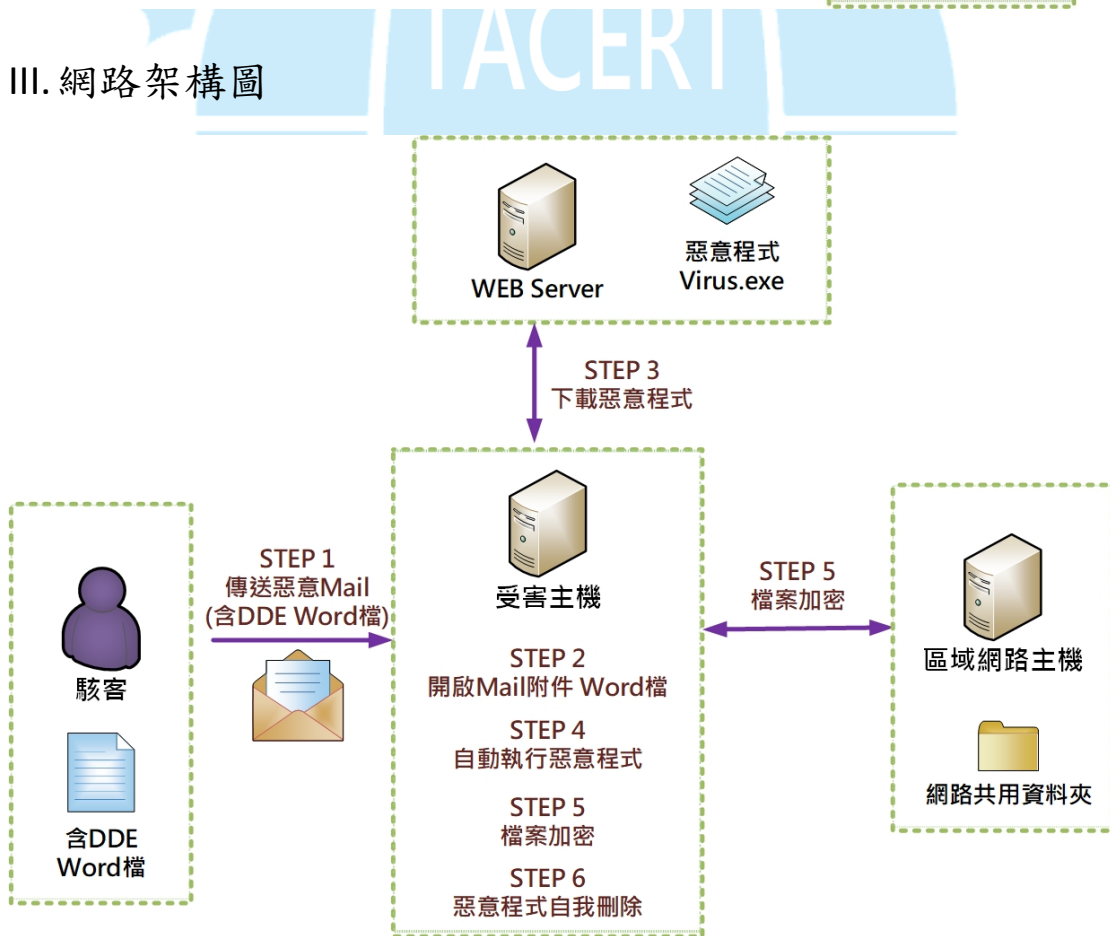
```

> Frame 336: 270 bytes on wire (2160 bits), 270 bytes captured (2160 bits)
> Ethernet II, Src: Vmware_55:3a:87 (00:0c:29:55:3a:87), Dst: Vmware_05:fb:dc (00:0c:29:05:fb:dc)
> Internet Protocol Version 4, Src: 192.168.195.134, Dst: 192.168.195.129
> Transmission Control Protocol, Src Port: 49540, Dst Port: 445, Seq: 22684, Ack: 27972, Len: 216
> NetBIOS Session Service
< SMB2 (Server Message Block Protocol version 2)
  < SMB2 Header
  < SetInfo Request (0x11)
    < StructureSize: 0x0021
    < Class: FILE_INFO (0x01)
    InfoLevel: SMB2_FILE_RENAME_INFO (0x0a)
    Setinfo Size: 116
    Setinfo Offset: 0x0060
    Unknown: 000000000000
  < GUID handle File: Excel1.xlsx
    File Id: 000001a5-0010-0000-3d00-2000ffffffffff
    [Frame handle opened: 312]
    [Frame handle closed: 340]
  < SMB2_FILE_RENAME_INFO
    0000 0001 = Replace If: Replace the target if it exists
    Reserved (Random): 0000000000000000
    Root Dir Handle (MBZ): 0000000000000000
    Filename Length: 92
    Filename: 7JMR8YXX-A0IU-D4UN-8ED27088-A39DBDE4EE1D.ykcol
  
```

15. 查看 Web Sever 與 AMY-PC 內的網路共享資料夾，發現 Web Sever 沒有任何感染情形，但是 AMY-PC 內的兩個網路共用資料夾內檔案皆都被加密，可見只要受害主機有存在網路磁碟機的連線，則惡意程式會透過此連線加密連線另一方電腦內共用資料夾內的檔案。



III. 網路架構圖



1. 駭客傳送惡意 Mail(含 DDE Word 檔)給受害者。
2. 受害者開啟 Mail 附件 Word 檔。
3. 受害主機連至含有惡意程式的 Web 伺服器下載惡意程式。
4. 受害主機自動執行惡意程式。
5. 受害主機進行檔案加密。
6. 惡意程式執行完畢後自我刪除。

IV. 建議與總結

1. 惡意程式透過 DDE 協定來散播的途徑非常容易，只要開啟一個 Word 檔將 DDEAUTO 的語法打入後存檔即完成含惡意程式的 Word 檔，之後再以 E-mail 方式寄出即可。
2. 利用 DDEAUTO 的語法，駭客可以隨時更換惡意程式的下載路徑與更改惡意程式的內容，惡意程式可以為其他的勒索病毒或者為一個挖礦程式。
3. 含有 DDE 的 Word 檔在開啟後所出現的訊息視窗內容，如同系統本身訊息提示，讓使用者不易察覺有異。
4. 起先微軟公司雖了解此風險的存在，但認為 DDE 的問題在技術上並不代表一個錯誤，而是一個程式本身的功能。隨著利用 DDE 技術被大肆濫用，微軟的安全團隊慢慢開始改變主意。目前微軟在 10 月中旬與 12 月中旬陸續發表了 4053440 安全通報 (Security Advisory) 與 Office 防禦深度更新 ADV170021，以協助使用者減輕 DDE 攻擊所帶來的威脅。

(1) 微軟安全通報 4053440

告訴使用者如何安全地打開包含動態數據交換 (DDE) 字段的 Microsoft Office 文檔，通過 GUI 選項或 Windows 註冊表修改禁用 DDE 支持的方法。

<https://technet.microsoft.com/en-us/library/security/4053440>

(2) Office 防禦深度更新 ADV170021

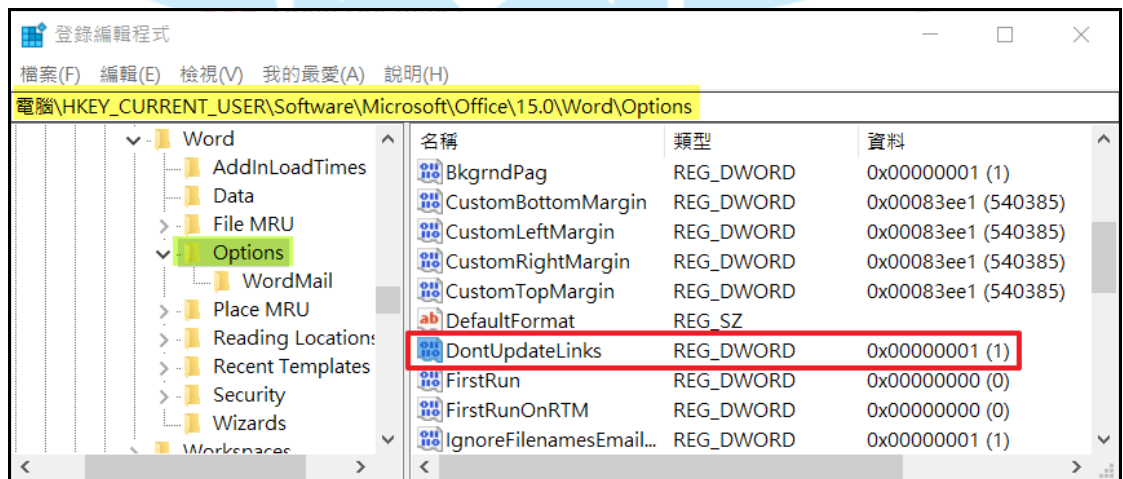
針對微軟 Office 的更新，提供了增強的安全性作為一種縱深防禦措施。
此更新禁用 Microsoft Word 的所有受支持版本中的動態更新交換協議
(DDE)。

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV170021>

5. 為了有效預防此類型攻擊事件，建議使用者不要開啟來路不明的郵件附加檔案。
6. 使用者可以利用「Word 選項>進階>一般>不勾選「開啟舊檔時自動更新連結」選項」來關閉每次 Word 檔開啟時出現的 DDE 訊息視窗。



7. 使用者可利用登錄編輯程式手動關閉各種 Office 版本與程式的 DDE 功能。

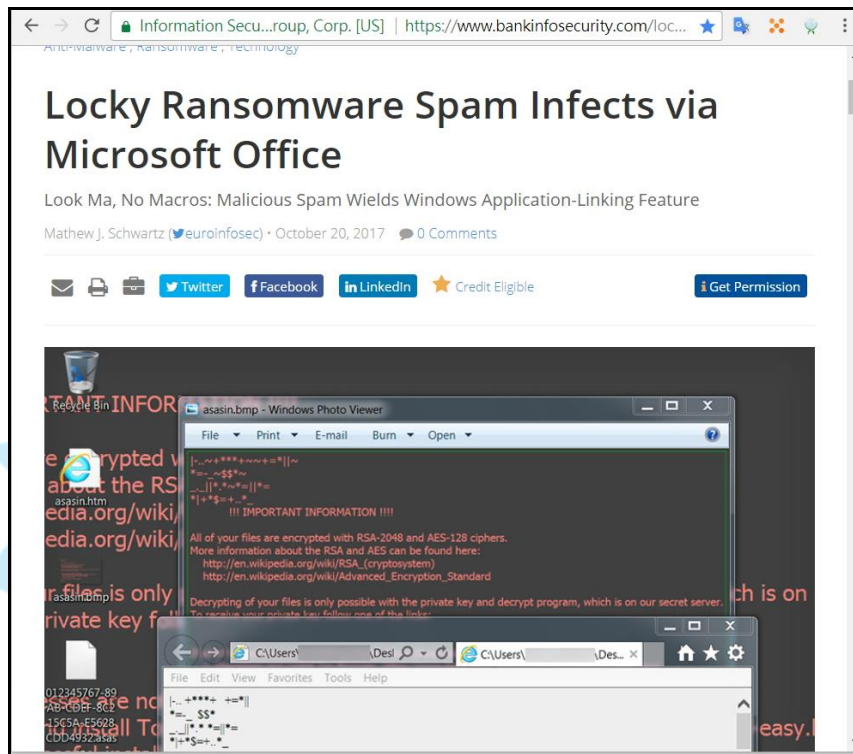


8. 建議使用者平時備份重要檔案，一旦感染惡意程式時，除使用防毒軟體掃毒外，對於無法被解密的檔案，可以先行備分，以等待未來新的解密程式產生時進行解密。

V. 相關報導

1. Locky Ransomware Spam Infects via Microsoft Office

<https://www.bankinfosecurity.com/locky-ransomware-spam-infects-via-microsoft-office-a-10392>



2. Locky Ransomware Attacks Exploit Microsoft DDE to Increase Effectiveness

<https://securityintelligence.com/news/locky-ransomware-attacks-exploit-microsoft-dde-to-increase-effectiveness/>



3. 空白 Word 暗藏木馬，俄國駭客組織用微軟 DDE 協定攻擊散佈惡意程式

<https://www.ithome.com.tw/news/118203>



The screenshot shows a web browser displaying a news article on the iThome website. The article title is "空白Word暗藏木馬，俄國駭客組織用微軟DDE協定攻擊散佈惡意程式". The text below the title states: "用戶如果在誘使下打開這份Word檔案會發現內文是空的。但檔案一經開啟，Office產品中的DDE功能即呼叫PowerShell執行指令，連上外部C&C伺服器，載入名為Seduploader的惡意程式". The article is attributed to "文/ 林妍濤 | 2017-11-13 發表".

4. Microsoft Disables DDE Feature in Word to Prevent Further Malware Attacks

<https://www.bleepingcomputer.com/news/microsoft/microsoft-disables-dde-feature-in-word-to-prevent-further-malware-attacks/>



The screenshot shows a web browser displaying a news article on the BleepingComputer website. The article title is "Microsoft Disables DDE Feature in Word to Prevent Further Malware Attacks". The article is attributed to "By Catalin Cimpanu" and dated "December 15, 2017". The article content is partially visible, showing the title and author information.