臺灣大學計資中心網路組
北區學術資訊安全維運中心

資訊安全分析報告

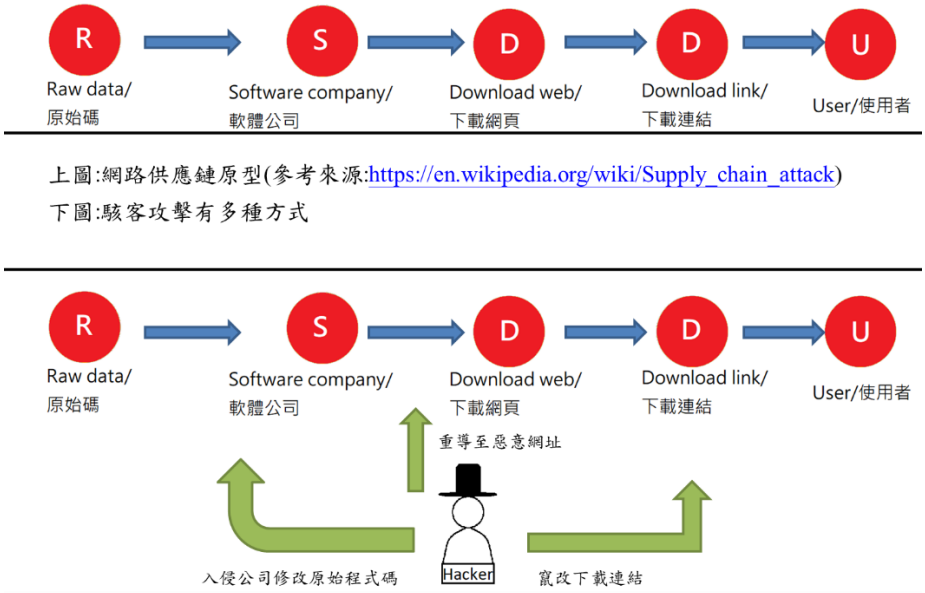
數位供應鏈的安全危機

臺灣大學計資中心網路組

北區學術資訊安全維運中心

一、 前言

今年九月中旬爆發的知名系統清理軟體 CCleaner 遭到後門程式入侵的攻擊事件 [1]，據統計全球約有兩百多萬用戶遭受到此典型的「數位供應鏈攻擊 (Digital Supply chain attack)」，此攻擊的最大特色是包覆在「合法授權」的保護傘之下，可以輕易繞過一些防毒軟體的檢測，讓使用者放下戒心安裝使用，造成大範圍的感染與擴散。



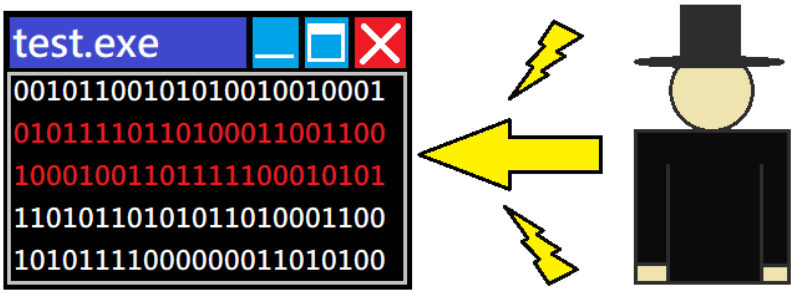
圖一. 數位供應鏈攻擊

「數位供應鏈攻擊」並非剛出現的新名詞，過去也曾發生過類似的資安事件，如著名的播放軟體 KMPlayer、知名瀏覽器 FireFox、公文系統 eClient 以及眾所周知的伊莉 (eyny) 論壇網站，皆遭受過「數位供應鏈攻擊」的威脅。隨著分析技術日異月新，「數位供應鏈攻擊」種類越來越多，惡意程式的功能也更加複雜，

以下將介紹過去的案例與相關資安議題，並分析此次 CCleaner 惡意程式的活動方式。

二、 數位供應鏈攻擊類型

1. 應用程式遭植入惡意程式碼



圖二. 駭客植入惡意程式

官方主機遭到駭客入侵後，將原始版本替換成修改後版本，造成的影響往往如同木馬程式一樣不容小覷，這裡舉出幾個案例。

近期所爆發的 CCleaner 事件便屬於其中之一。據 Cisco 旗下的 Talos 安全研究室指出，九月十三日便偵測到 32 位元版的 CCleaner 包含惡意程式碼 [2]。受到影響的版本是 32 位元的 CCleaner 5.33.6162 和 CCleaner Cloud 1.07.3191，該版本於今年八月中旬發布。據研究指出，疑似駭客入侵軟體開發部門，將惡意程式碼植入，導致本次資安事件。

學校及公務機關最切身相關的公文系統 (eClient)，也曾於 2013 年遭受到攻擊 [3]，駭客於公文系統用戶端軟體下載網站中，將原始安裝執行檔置換成包含惡意程式的版本，導致安裝此版本的使用者的主機自動連線至不明的中繼站傳送資料。據當時統計全台約有 7000 個政府機關受影響，逾六成電子公文有資料外

洩之風險。

第三個案例為 Xshell，官方在今年的八月七日公布受到影響版本 Xshell 5.0 Build 1322 (包含其餘四項產品)，駭客入侵開發人員的電腦，在 nssock2.dll 植入惡意程式碼 [4]，並回傳主機內部資訊給 C&C 伺服器。

另外，Firefox 與 KMPlayer，皆曾在 2013 年發生主機遭受駭客入侵，並置換成惡意程式版本。

以上案例皆因駭客將惡意程式植入官方的安裝或更新系統，讓不知情的用戶下載或更新而受害。因上述攻擊手法，技術層面較為複雜，須由網管層面相互配合，方能有效制止，我們將於本文結論提供建議與防護措施。

2. 惡意程式碼植入瀏覽器插件

除應用程式之外，瀏覽器的插件也經常成為惡意程式攻擊的目標。今年八月有資安專家公布 Google Chrome 瀏覽器插件被駭的清單 [5]，包含：Web Developer、Chrometana 1.1.3、Copyfish、Web Paint 1.2.1、Social Fixer 20.1.1、TouchVPN、BetternetVPN、Infinity New Tab 3.12.3。

瀏覽器插件被植入惡意程式，造成使用者暴露於資安威脅之中。Google 公司也意識到此問題之嚴重性，為了讓 Chrome 瀏覽器更加安全，他們提供「Software Removal Tool」給使用者掃描瀏覽器插件中的惡意軟體並將之清除 [6]。

3. 使用者不慎下載惡意程式

不少駭客利用使用者信任合法官網的習慣，在使用者不知情的狀態下點選下載惡意程式，導致裝置受到惡意程式感染，以下列舉三個案例。

第一個案例是今年四月下旬伊莉討論區首頁遭到駭客入侵置換，“提醒”瀏覽首頁的使用者更新 Flash Player 版本，要求使用者下載與安裝網站提供的更新

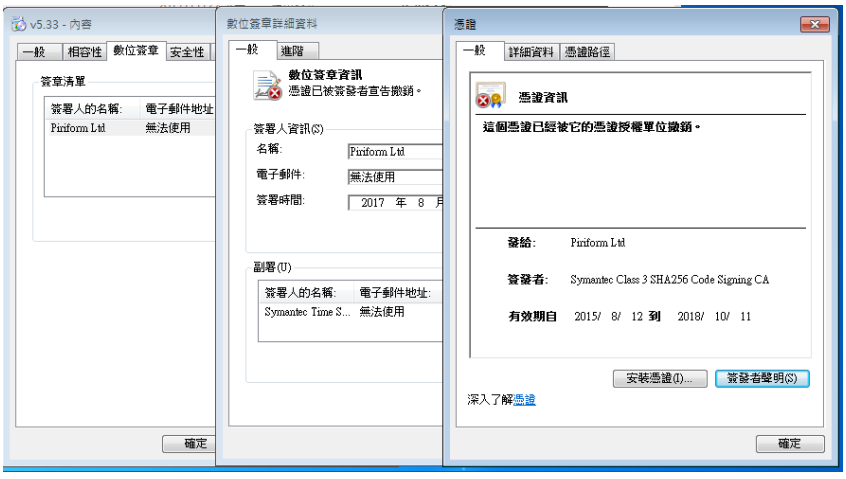
版本，當使用者安裝該 Flash Player 版本後立即執行勒索軟體 [7]。

第二個案例是去年年底發生的 ElTest 事件，駭客發送惡意電子郵件，當使用者點擊郵件中的連結被自動導向惡意網站時，出現「找不到字型」視窗，誘騙使用者更新並植入勒索軟體或是遠端存取被害者的主機 [8]。

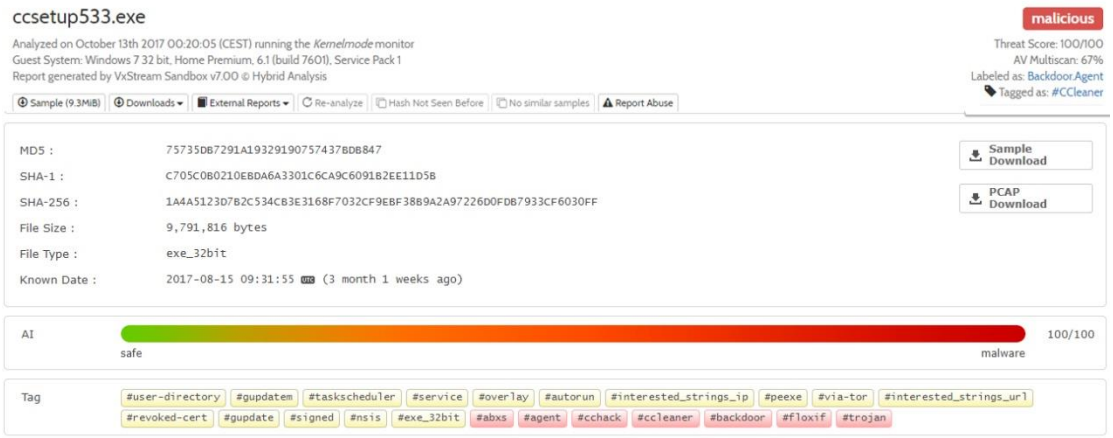
第三個案例是有關 Google Play 商店上數個 APP 被植入 ExpensiveWall 惡意程式。APP 開發人員使用遭駭客改寫過的 GTK 開發套件，惡意程式運作導致使用者的手機自動連線到 C&C 伺服器，擅自訂閱付費服務 [9]。

三、 CCleaner 遭植入後門程式分析

由 Piriform 所發行的 32 位元 CCleaner 5.33.6162 和 CCleaner Cloud 1.07.3191，因已被駭客從伺服器端入侵，即便是從官網中下載附有數位簽證的軟體也遭人竄改。如下圖所示，我們將具有數位簽證的 CCleaner 5.33.6162 透過惡意軟體分析網站掃描後，可發現存在多種資安漏洞。

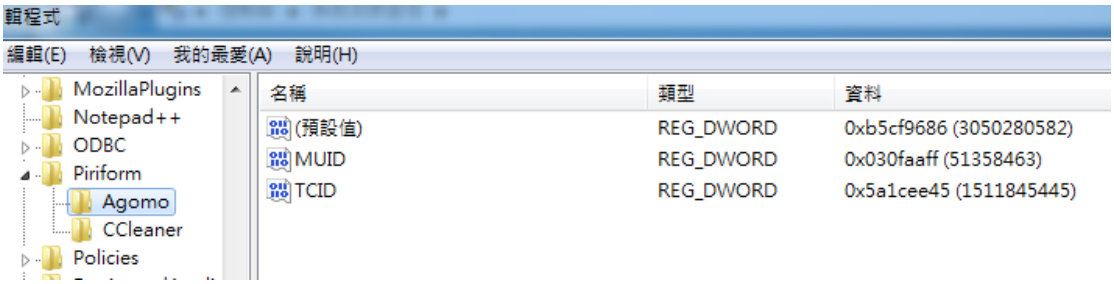


圖三. CCleaner 程式所附數位簽證



圖四.　CCleaner 5.33.6162 版本之資安漏洞 [10,11]

從被感染的 CCleaner 程式分析來看，程式在一開始安裝時便已被加入了木馬程式，並在機碼中新增 Agomo 的註冊值 [12]，儲存通訊加密金鑰 (MUID) 及通訊回報時間值 (TCID)，如圖五所示。



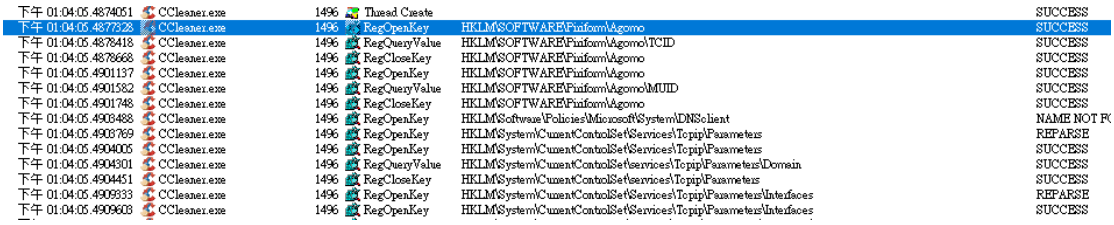
圖五.　CCleaner 新增非官方機碼

且惡意程式在 CCleaner 程式安裝之後，並不會立刻展開行動，反而刻意延遲 10 分鐘。透過封包分析，我們可以清楚的看到，CCleaner 5.33.6162 在安裝完畢後，便對 www.piriform.com 網域進行 DNS 查詢，為其第一次的網路行為，如下圖所示。

Time(Abs)	Source	Src port	Destination	Dest port	Protocol	info
2017-11-26 12:53:59.403…	192.168.111.129	58294	192.168.111.2	53	DNS	Standard query 0x64c9 A www.piriform.com
2017-11-26 12:53:59.421…	192.168.111.2	53	192.168.111.129	58294	DNS	Standard query response 0x64c9 A www.piriform.com CNAME f.global-s
2017-11-26 12:53:59.425…	192.168.111.129		151.101.0.64		ICMP	Echo (ping) request id=0x0001, seq=2/512, ttl=128 (reply in 77)
2017-11-26 12:53:59.495…	151.101.0.64		192.168.111.129		ICMP	Echo (ping) reply id=0x0001, seq=2/512, ttl=128 (request in 76)
2017-11-26 12:53:59.566…	192.168.111.129	52937	192.168.111.2	53	DNS	Standard query 0xe26b A service.piriform.com
2017-11-26 12:53:59.686…	192.168.111.2	53	192.168.111.129	52937	DNS	Standard query response 0xe26b A service.piriform.com CNAME f.glob
2017-11-26 12:53:59.687…	192.168.111.129	49165	151.101.0.64	80	TCP	49165 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1

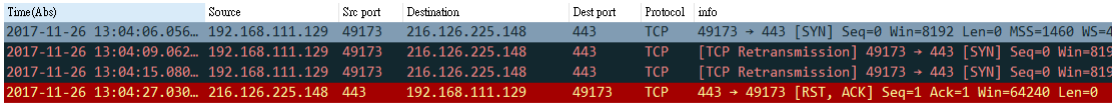
圖六.　程式安裝完後執行 DNS 查詢

惡意程式等過了十幾分鐘之後，才開始讀取 Agomo 機碼值並與 C&C 伺服器 (IP address: 216[.]126[.]225[.]148)連線，如圖七、圖八所示。



下午 01:04:05.4874051	CCleaner.exe	1496	Thread Create		SUCCESS
下午 01:04:05.4877328	CCleaner.exe	1496	RegOpenKey	HKLM\SOFTWARE\Funform\Agomo	SUCCESS
下午 01:04:05.4878418	CCleaner.exe	1496	RegQueryValue	HKLM\SOFTWARE\Funform\Agomo\TCID	SUCCESS
下午 01:04:05.4878668	CCleaner.exe	1496	RegCloseKey	HKLM\SOFTWARE\Funform\Agomo	SUCCESS
下午 01:04:05.4901137	CCleaner.exe	1496	RegOpenKey	HKLM\SOFTWARE\Funform\Agomo	SUCCESS
下午 01:04:05.4901582	CCleaner.exe	1496	RegQueryValue	HKLM\SOFTWARE\Funform\Agomo\MUID	SUCCESS
下午 01:04:05.4901748	CCleaner.exe	1496	RegCloseKey	HKLM\SOFTWARE\Funform\Agomo	SUCCESS
下午 01:04:05.4903488	CCleaner.exe	1496	RegOpenKey	HKLM\Software\Policies\Microsoft\System\DNSclient	NAME NOT FO
下午 01:04:05.4903769	CCleaner.exe	1496	RegOpenKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	REPARSE
下午 01:04:05.4904005	CCleaner.exe	1496	RegOpenKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	SUCCESS
下午 01:04:05.4904301	CCleaner.exe	1496	RegQueryValue	HKLM\System\CurrentControlSet\services\Tcpip\Parameters\Domain	SUCCESS
下午 01:04:05.4904451	CCleaner.exe	1496	RegCloseKey	HKLM\System\CurrentControlSet\services\Tcpip\Parameters	SUCCESS
下午 01:04:05.4909333	CCleaner.exe	1496	RegOpenKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces	REPARSE
下午 01:04:05.4909603	CCleaner.exe	1496	RegOpenKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces	SUCCESS

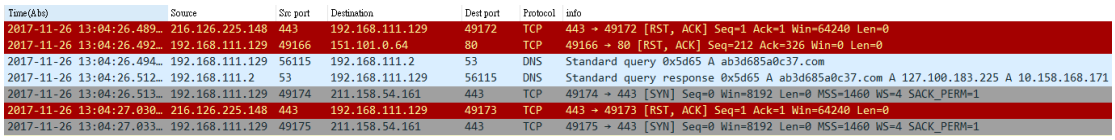
圖七.　讀取惡意程式機碼



Time(Abs)	Source	Src port	Destination	Dest port	Protocol	info
2017-11-26 13:04:06.056…	192.168.111.129	49173	216.126.225.148	443	TCP	49173 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4
2017-11-26 13:04:09.062…	192.168.111.129	49173	216.126.225.148	443	TCP	[TCP Retransmission] 49173 → 443 [SYN] Seq=0 Win=819
2017-11-26 13:04:15.080…	192.168.111.129	49173	216.126.225.148	443	TCP	[TCP Retransmission] 49173 → 443 [SYN] Seq=0 Win=819
2017-11-26 13:04:27.030…	216.126.225.148	443	192.168.111.129	49173	TCP	443 → 49173 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0

圖八.　連線 C&C 伺服器

如果上述 C&C 伺服器無回傳資料，惡意程式將透過亂數（月份）利用 DGA (Domain Generation Algorithm)產生一個網域名稱(Domain name)，進行 DNS 查詢如下圖所示。並且如 kill switch 的運作機制，如果 DNS 查詢有正常回應則停止活動。



Time(Abs)	Source	Src port	Destination	Dest port	Protocol	info
2017-11-26 13:04:26.489…	216.126.225.148	443	192.168.111.129	49172	TCP	443 → 49172 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
2017-11-26 13:04:26.492…	192.168.111.129	49166	151.101.0.64	80	TCP	49166 → 80 [RST, ACK] Seq=212 Ack=326 Win=0 Len=0
2017-11-26 13:04:26.494…	192.168.111.129	56115	192.168.111.2	53	DNS	Standard query 0x5d65 A ab3d685a0c37.com
2017-11-26 13:04:26.512…	192.168.111.2	53	192.168.111.129	56115	DNS	Standard query response 0x5d65 A ab3d685a0c37.com A 127.100.183.225 A 10.158.168.171
2017-11-26 13:04:26.513…	192.168.111.129	49174	211.158.54.161	443	TCP	49174 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
2017-11-26 13:04:27.030…	216.126.225.148	443	192.168.111.129	49173	TCP	443 → 49173 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
2017-11-26 13:04:27.033…	192.168.111.129	49175	211.158.54.161	443	TCP	49175 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1

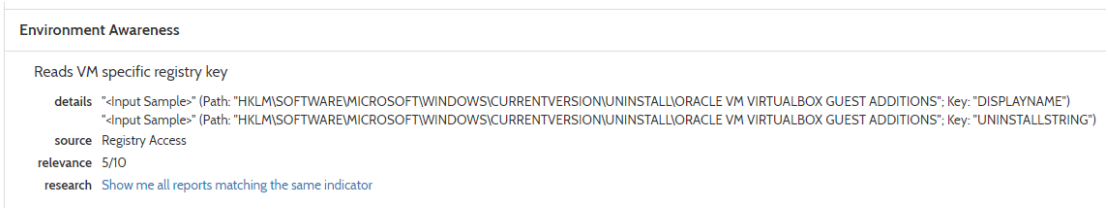
圖九.　進行特定網域名稱 DNS 查詢

若 DNS 查詢回應查無此網域時，程式才會繼續選擇第二個備援 C&C 伺服器 (216[.]126[.]225[.]163) 進行連線。

實驗過程中，因 C&C 伺服器已於事件發生過後停止服務，對程式的連線要求並不會回應，且 DGA 運算出的特定網域也都被註冊了，惡意程式透過 DGA 進行檢查偵測後停止活動。

經由上述過程，我們可以看出此惡意程式為了增加存活率及避免被沙箱分析，

在程式設計上刻意躲避檢查機制，從程式分析網站的報告中可看出，惡意程式加入了環境認知功能以確認是否處於 VM (虛擬機器)環境中，如圖十所示。



圖十.　惡意程式之環境偵測機制

四、 建議與防護策略

隨著網路攻擊越來越多樣化，單純只依靠使用者端的防禦已不符需求，多點聯防日趨重要，尤其公司、團體及政府單位等企業對於網路的依賴越來越重，如何讓資安管理者與使用者之間，面對資安問題能相互合作、各司其職，是相當重要的。

1. 使用者端

遨遊於網路花花世界容易讓人眼花撩亂，使用者需要時時提高警覺，如本文第三類數位供應鏈攻擊(使用者不慎下載惡意程式)，大多皆因使用者操作不慎而下載惡意程式，也是資安管理上最難防範的。因此，每年的資安宣導或資安課程都致力於宣導正確的電腦使用習慣，而良好的電腦使用習慣是需要時間培養的，如：不下載來源不明的軟體、不連線不受信任的網站、不點擊不明的廣告或連結、不在公共電腦上登入帳號密碼等等，希望使用者能時時刻刻銘記於心。

2. 資安管理者

現行的應用程式若遭植入惡意程式碼，因涉及較多技術層面，使用者可能無法及時發現，大部分只能被動地依賴資安產品的保護（阻止連線到惡意網址等等）

及資安管理人員的管制措施。

網路防毒公司「卡巴斯基」研究員於網路會議表示：「面對高難度威脅的防護策略應包含安全策略之建立、良好的教育訓練以及完善的系統管理」[13]。所以資安管理人員除注意軟體更新訊息、相關資安新聞、漏洞或攻擊發生時能立即進行系統更新與防護之外，對於應用程式管理也需要更嚴謹的規範及審核，必要時限制使用者瀏覽惡意網域，並對於特定的網址及通訊協定在防火牆上加以管控。在特徵掃描上，定期對於企業使用的軟體進行特徵碼掃描(如 MD5、SHA)，並於企業網路對外端點建置入侵偵測系統 (IPS)，對於企業進出的所有封包進行深入的檢查與過濾。

處於高科技的時代，面對多樣化的惡意程式攻擊，防禦措施已不局限於使用者一端，而是需要背後資安管理人員的全力支援，強化縱深防禦，方能有效降低惡意程式的威脅。

參考資料

1. iThome (2017-09-19)〈CCleaner 遭植入後門，雲端版及官網下載都中鏢〉。網址：https://www.ithome.com.tw/news/116900
2. TALOS (2017-09-18) 〈CCleanup: A Vast Number of Machines at Risk〉。網址：http://blog.talosintelligence.com/2017/09/avast-distributes-malware.html
3. iThome (2013-05-31)〈政府電子公文系統被駭，主管單位竟企圖遮掩〉。網址：https://www.ithome.com.tw/node/80703
4. iThome (2017-08-25)〈資安一周[0819-0825]：SSH 連線工具軟體 Xshell5 遭植入後門，暗中裝置資料〉。網址：https://www.ithome.com.tw/news/116477
5. BestVPN (2017-08-18)〈Eight Chrome Extensions Hacked – Including Two VPNs〉。網址：

https://www.bestvpn.com/privacy-news/chrome-extensions-vpn-hacked/

6. FreeGroup〈Google 推出惡意軟體移除工具 Software Removal Tool，修復 Chrome 瀏覽器綁架問題〉。2017-11-26 取自網址：https://free.com.tw/google-software-removal-tool/

7. Mobile01 (2017-05-04)〈恐怖綠色勒索病毒源自 eyny 伊莉論壇，八年多檔案全都無法開啟，但副檔名卻沒變〉。網址：https://www.mobile01.com/topicdetail.php?f=508&t=5139763

8. iThome (2017-09-05)〈Firefox 與 Chrome 跳出「找不到字型」視窗，小心是病毒作祟!〉。網址：https://www.ithome.com.tw/news/116656

9. ExpensiveWall (2017-09-14)〈A dangerous‘packed’malware on Google Play that will hit your wallet〉。網址：https://blog.checkpoint.com/2017/09/14/expensivewall-dangerous-packed-malware-google-play-will-hit-wallet/

10. Malwares.com (2017-08-15)〈CCleaner Installer 軟體分析〉。網址：https://www.malwares.com/report/file?hash=1A4A5123D7B2C534CB3E3168F7032CF9EBF38B9A2A97226D0FDB7933CF6030FF

11. Reverse.it (2017-10-13)〈ccsetup533.exe 軟體分析〉。網址：https://www.reverse.it/sample/1a4a5123d7b2c534cb3e3168f7032cf9ebf38b9a2a97226d0fdb7933cf6030ff?environmentId=100

12. Piriform Blog (2017-09-18)〈Security Notification for CCleaner v5.33.6162 and CCleaner Cloud v1.07.3191 for 32-bit Windows users〉。網址：https://www.piriform.com/news/blog/2017/9/18/security-notification-for-ccleaner-v5336162-and-ccleaner-cloud-v1073191-for-32-bit-windows-users

13. Wikipedia〈Supply chain attack〉。2017-11-22 取自網址：https://en.wikipedia.org/wiki/Supply_chain_attack