病毒威脅報告

2014 上半年(中文版)

SWITCH ON FREEDOM

芬安全 F-Secure

www.f-secure.com

目 錄

2014上半年威脅報告一覽表 ...

事件回顧

Page 6

一月

二月

- iOS 發布更新修復主要 SSL 的漏洞
- 主動攻擊利用新的 IE 零時差漏洞

三月

四月

- 使用Coremax進行瀏覽器綁架
- Windows XP 官方終止支援

五月

- 警察勒索軟體跨平台至 Android 系統

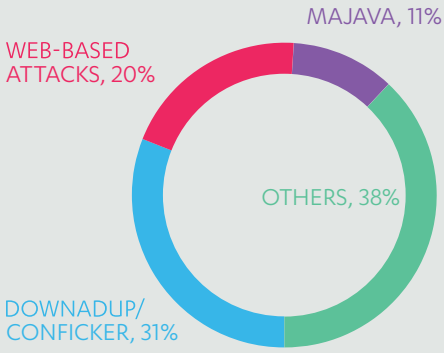
六月

- FBI 追捕 Gameover Zeus 病毒的發布者
- 'Oleg Pliss' 在莫斯科被拘捕

個人電腦中的惡意軟體 前十大的感染源

Page 9, 11

Windows 是現有的惡意軟體家族進行威脅的主要環境，其中一些已經存在多年，尤其是在未進行漏洞更新的電腦上繼續存在。



前十大感染源

DOWNADUP (aka CONFICKER)
這個有六年之久的蠕蟲病毒利用Windows系統中MS08-067的漏洞。經由可移動的媒體和網路共享散佈在網際網路上。

WEB-BASED ATTACKS
惡意軟體、技術或漏洞的一個整合系統，通常會將網頁重新導向到惡意網站，讓該系統可以進行更多的攻擊。

MAJAVA
針對JAVA開發平台的漏洞攻擊的整合系統，一旦攻擊成功，就能讓攻擊者進而控制整個系統。

以及...

SALITY | RAMNIT | AUTORUN | WORMLINK | BROWSER EXPLOIT | EXPIRO | ZEROACCESS

行動裝置 惡意軟體

Page 12

Android系統仍然是行動裝置中，大多數的威脅軟體最喜歡的攻擊目標，然而針對iOS的威脅不是沒有，只是數量很少。

ANDROID + iOS

294 個 新家族 or 變種

1 個新家族

SSLCREDTHIEF
簽署程式庫檔案被監聽並從SSL的連線資訊中竊取Apple的帳號和密碼。

大出擊 ANDROID 家族

SMSSEND
惡意軟體的大家族，會發送高額的SMS簡訊。

FAKEINST
會安裝其他app，且發送高額的SMS簡訊。

EROPL
從裝置上悄悄地收集資料並傳送到遠端伺服器。

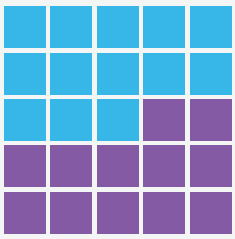
MAC 惡意軟體

Page 14

雖然 Windows 環境的威脅還是以老舊的與現在還存在的惡意軟體為主時， MAC 環境看來會是新的嘗試，不再有以往不受侵擾的光景。惡意軟體的技術能力與散佈方式在這段期間來看，也越來越複雜了。

25 個 新的變種

發現於 2014年 一月至六月之間



13 新的變種 屬於 **5** 新的家族

MASK
"The Mask"一種網路間諜行動，針對政府機關和能源企業。

CLIENTSNOW
被用來針對西藏和維吾爾族的攻擊。

LAOSHU
遠端存取的木馬程式，透過偽造的快遞郵件通知而進行散佈。

COINTHIEF
一種木馬間諜軟件主要在竊取加密貨幣。偽裝成 OS X 應用程式的破解版，但後來改為直接散佈有木馬病毒的加密貨幣應用程式。

COINSTEALER
比特幣偷竊者是利用應用程式的漏洞來存取 Mt.Gox 的交易資訊。

$ $ $ 要求高額的贖金

ANDROID

KOLER: 第一個勒索軟體
以警察為主題的手機擴充套件Reveton勒索軟體，聲稱對裝置上的文件進行了加密直到支付贖金，但實際上只禁用了返回的按鈕。

ANDROID

SLOCKER: 第一個TOR加密的勒索軟體
設備上圖片、文件和影片都會被加密；禁用返回按鈕來干擾用戶的操作。通訊方式是經由Tor網路或SMS簡訊聯繫控制伺服器。

iOS

Oleg Pliss 攻擊澳洲
今年五月，據報導指出'Oleg Pliss'鎖定在澳洲一個用戶門號的帳號，使用尋找我的iphone的功能並要求贖金。蘋果否認在在iCloud服務上有這個漏洞的推測。

前言

米戈・希伯能
by
Mikko Hypponen
首席研究長
F-Secure 病毒威脅實驗室

我記得我們建立的第一個網站，那是在1994年距離現在已有20年之久，當時的網站很陽春而且只有網站數量極少數，所以不難去預測未來網站是會逐漸增加。果然，這20年來網站數量已經有相當規模的發展，更重要的是，現在無時無刻都會有人在線上。要是在以前，你會發現只有怪咖和書呆子會在線上，而現在則是大家都隨時都在使用網路。

在1994年時，我們就在猜測是什麼會帶動網路的成長，網路的發展必須有線上內容，例如新聞或娛樂，當新聞和娛樂轉移到網路上時，總是需要有人來付費，但如何讓用戶支付收看線上內容？我們並不知道，也許報紙類開始收取每年的網路訂閱費，就像紙本的模式，又或許網路可以利用一些線上支付系統的形式，例如：用戶透過瀏覽器做小額支付的方法就可以存取內容，這樣的付費方式，換句話說，就是利用付費來閱讀今天的呆伯特連載漫畫。

“長期而言，我們這些用戶是非常有價值的，因為擁有用戶的使用習慣及行為模式等資訊”

正如所知，這樣的小額支付系統從來沒有發生過，即使在20年前就已經知道這樣的方式，反而另一種線上支付以完全不同的方式出現 - **廣告**。也許是在1995年或1996年，我記得在一個網站上看到第一個橫幅廣告，我對這家公司在別人的網站上付錢做廣告，展示他們產品的想法嗤之以鼻，但我不應該譏笑他們，因為現在這樣的做法幾乎在網路上造成一股風潮，就像Google和Facebook公司有效地運用廣告分析引擎締造了可觀的利潤。

Google是個利用分析使用者習慣獲利的好例子，Google所提供的服務，例如搜索、YouTube、地圖和Gmail，這些都是免費的。你使用它們是不需要付任何費用，但這些服務成本是相當昂貴的，光是電費帳單，一年就超過1億美元，你可能會認為運行這些服務的成本非常高卻不收取費用，鐵定會虧損，但事實不然，2013年Google的收入是600億，利潤就有120億，所以，保守估計若Google有十億用戶，則代表每個用戶在去年都為Google創造出12美元的利潤，但不需要用戶支付任何費用。

坦白地說，我會很高興每年支付12美元給Google使用他們的服務而沒有被追蹤或分析，我更願意每年支付100美元！但他們不會給我這樣的選擇，因為以長遠性來看，我們這些用戶是非常有價值的，因為可運用用戶的使用習慣及行為模式等資訊。

當然，Google是一個企業。他們並沒有違法對我們進行分析—我們是自願將資訊提供給他們，Google的服務的確是很棒，但我希望在未來，這樣的事情能有其他的方式來處理，我們可以有一個簡單的小額付費系統來規範使用的內容與服務。現在，隨著加密貨幣的崛起，這最後可能會成為事實。

值得注意

遊戲結束？
GAME OVER?

尚・沙利文
by
Sean Sullivan
資訊安全顧問
F-Secure 病毒威脅實驗室

GameOver ZeuS (GOZ) 殭屍網路病毒被多國執法機構[1]分頭進行非常成功地將它掃除，可是後續呢？殭屍網路病毒雖被阻斷，但沒有完全被瓦解，因為創造它的人並沒有被捕仍然在逃，而且正繼續開發新的殭屍網路病毒。

為什麼要瓦解GOZ?

CryptoLocker [2]，一個透過GOZ進行植入的強大木馬勒索軟體，這就是為什麼要針對殭屍網路病毒進行撤除的一大原因，CryptoLocker擁有能夠完整地將受害者硬碟上的所有文件、資料檔案進行加密的能力，除了支付贖金取得解密金鑰沒有其他解決方式，因此要停止CryptoLockr的運作，唯一辦法就是預防，因為CryptoLocker是透過GOZ散佈，所以GOZ就成為被掃除的對象。

逐步擴大

就因為CryptoLocker它的破壞力是這麼強大而且如此危險，所以這才是我們要掃蕩GOZ這樣的僵屍網的主要原因

"試著問問自己！如果CryptoLocker是如此成功，為什麼Slavik(GOZ主嫌在網路上的暱稱)不在殭屍網路上部署勒索軟體？"

答案很明顯：因為那樣的話他就不能擁有可被操縱的殭屍網路，因為在同一時間為數200萬的殭屍程序將無法同時執行CryptoLocker的植入程式且不破壞到GOZ的基礎架構。

若是這些基礎架構被撤除的話會損失什麼?又是什麼因素影響著GOZ的未來版本?除了讓這些沒在時限內與C&C伺服器溝通的殭屍網啟動一個自毀的指令(如植入加密炸彈)，告訴你它不會造成任何影響的。

進化

電腦惡意程式的沿革是進化的因素之一，而進化就是驅策捕食者與被捕食者間的動態。當每次獵物被發現後，新的逃避偵測的防守戰術又會繼續的出現。若是下一個防守戰術轉變成更激烈有害時，接下來將會發生什麼事呢？

病毒獵人應該要有所警惕！

> **"若是下一個防守戰術轉變成更激烈有害時，接下來將會發生什麼事呢？"**

來源

1. United States Department of Justice; *U.S. Leads Multi-National Action Against "Gameover Zeus" Botnet and "Cryptolocker" Ransomware, Charges Botnet Administrator*; 2 Jun 2014; http://www.justice.gov/opa/pr/2014/June/14-crm-584.html
2. F-Secure; *Trojan:W32/Cryptolocker;* http://www.f-secure.com/v-descs/trojan_w32_cryptolocker.shtml

2014上半年 事件回顧

數位自由

GCHQ 暗中監視 Yahoo 視頻聊天
二月
截取全球逾180萬個隨機用戶以及儲存影像

土耳其阻擋Twitter 以及Youtube
三月
土耳其政府斷絕其人民使用社交媒體工具

泰國暫時封鎖 Facebook
五月
IT部門聲稱他們收到了軍政府的禁令，但軍方斥責的表示那是「系統故障」

據報導美國國安局監聽巴哈馬群島的所有通話紀錄
五月
據說這樣的監聽是為了用來監控國際毒品販運者和特殊利益的不法份子

攻擊事件

雅虎郵件帳密遭受駭客攻擊與竊取
一月
攻擊者利用第三方偷來的用戶電子郵件帳戶的憑證竊取這些被鎖定用戶的密碼

駭客攻擊家用無線網路/辦公室路由器
三月
安全研究人員的報告中發現超過30萬的設備DNS被駭客修改過

比特幣銀行 Flexcoin 被搶
三月
攻擊者利用程式碼漏洞偷走896比特金幣(約為:60萬美金)

Windigo 攻擊感染 Linux 伺服器
三月
研究人員報告超過兩萬五千多台伺服器發送垃圾郵件，並且將使用者重新導向釣魚網站

安全性

依外國情報監視法要求科技龍頭提供資料數據
二月
美國官方對Google, Facebook等科技龍頭提出要求

TrustyCon 會議的抗議
二月
抗議RSA提供後門給美國國家安全局的抵制者拒絕出席RAS所舉辦的年會活動

Windows XP 正式終止提供更新服務(EOL)
四月
微軟已停止對XP的更新服務，建議用戶立即升級作業系統

eBay 被攻擊後強制更改密碼
五月
eBay用戶的資料被駭客獲取後，該公司聲明中宣布所有eBay用戶皆已被告知立即更改密碼以保障資料安全

執法事件

Spyeye 惡意軟體作者在美國認罪
一月
俄羅斯國家的開發商散佈針對無線電及銀行系統的詐騙惡意軟體

兩個盜版集團成員承認在Android上執行侵權
三月
美國第一起被定罪，散播假冒行動裝置應用程式

美國指責9個 Zeus 惡意軟體
四月
Zeus 惡意軟體被指控在美國感染成數千家企業

澳洲逮捕2個"匿名"的駭客
五月
法新社指責嫌犯篡改政府網站以及DoS攻擊

GAMEOVER ZEUS 殭屍網路病毒

三月：開始竊取比特幣錢包以及他們的加密密碼

三月：植入釣魚網站仿冒為一個求職網站讓求職者瀏覽

惡意軟體

新的改善勒索軟體計畫
一月
安全研究人員發現新的PowerLocker DIY套件

GameOver Zeus 開始竊取比特幣
一月
惡意軟體竊取比特幣錢包以及他們的加密密碼

TheMoon 蠕蟲在路由器上傳播
二月
Linksys路由器因韌體的漏洞被感染，並進行散播蠕蟲副本

瀏覽器挾持者 Coremax
四月
瀏覽器擴充遭廣告挾持且將用戶重新導向到來路不明的網站

漏洞

iOS 發表更新，以解決 SSL 的重大漏洞
二月
此漏洞可能允許駭客截取用戶之間的訊息

使用主動式攻擊新的IE零時差漏洞
二月
CVE-2014-1776漏洞在IE 瀏覽器10版以及9版上允許安裝惡意軟體

Flash Player 遭遇 driveby 的零時差攻擊
二月
利用Adobe公司的緊急修補漏洞程序，以無提示的方式安裝惡意軟體

全球零時差攻擊使用針對性的攻擊
三月
利用RTF格式的文件漏洞執行遠端程式碼

發生在2014年上半年事件回顧列出有趣的數位安全進展。
在事件回顧項目分別報告各入口網站的技術，安全研究刊物，法務部網站，
各大報紙以及芬安全部落格，來源清單在第15頁。

數位自由

由美國製造的路由器被植入後門
五月
美國國安局獲報成功攔截這些即將被外銷出口卻內含隱私監聽的問題路由器

由於 ISIS 的威脅，伊拉克阻擋社交媒體
六月
針對"干擾叛亂份子的通信"

泰國軍方為了壓制批評聲浪而控制線上活動
六月
超過一百個網站遭封鎖連線，並且禁止關鍵媒體報導此事

在土耳其的 Youtube, Twitter 已恢復存取
六月
Youtube 解鎖，Twitter 上個月已解除禁令

攻擊事件

Heartbleed 被利用連結駭客的 VPN
四月
紐約時報報導攻擊者使用漏洞進入特定公司的網路

AU-CERT 報導網路攻擊持續上升
五月
報告中提到 56% 企業的調查報告受到網路攻擊

TrueCrypt 加密工具被提出是有害不安全的
五月
TrueCrypt驅動器加密工具已在2014年5月WindowsXP退役時廢除使用，因為它可能包含某些安全性問題

香港爆發大規模 DDoS 攻擊
六月
300Gbps+流量攻擊民間全民投票系統

安全性

微軟推出 MyBulletins 簡化更新流程
五月
MyBulletins提供一個簡易的個性化列表列出重要的微軟安全公告事項

Google 首次亮相 '被遺忘的權利'的格式
五月
歐盟要求歐盟法庭判決歐搜尋引擎需移除'不相關'連結

Google 應用程式新增加密功能
五月
End-to-end提供給企業用戶電子郵件加密

Reset the Net 運動推廣
六月
聯盟組織發起了Reset the Net運動，鼓勵網民和企業針對不當的監控行為採取使用隱私保護工具措施。

執法事件

美國起訴 5 個中國駭客間諜罪
五月
司法部門指控中國人民解放軍成員駭入美國企業長達8年

近100個創作Blackshades木馬的駭客被捕
五月
在美國，歐盟以及其他國家散佈販售用來窺視用戶的木馬的駭客被捕

'Oleg Pliss' 駭客在莫斯科被補
六月
俄國內務部指出在奧茲逮捕2名利用iOS勒索攻擊的駭客

FBI 破獲 Gameover Zeus 的主嫌
六月
主嫌為俄羅斯人被控串謀，非法入侵他人電腦、電信欺詐、銀行欺詐和洗錢與其他涉嫌

GAMEOVER ZEUS 殭屍網路病毒

六月：美國聯邦調查局與合作夥伴推出"運行 Tovar "移除，呼籲使用者掃描他們的電腦

六月：FBI 提供了清除工具請使用者在 2 週內將個人電腦端清除病毒；但是殭屍網路病毒仍在漫延

惡意軟體

報導指出 Play 商店中的防毒軟體是場騙局
四月
移除無功能性的應用程式，並退還使用者購買費用

警察勒索軟體已跨平台至 Android 裝置
五月
Koler 惡意軟體試圖鎖定受影響的裝置以及顯示贖金要求

Windows 8 上的 BlackEnergy rootkit
六月
芬安全將新樣本傳送至 VirusTotal 服務上

Havex 獵取 ICS/SCADA 系統
六月
惡意軟體用於工業控制系統並使用針對性的攻擊檢測

漏洞

Heartbleed 漏洞成為全球性的新聞
四月
數百萬的網站、手機受到 OpenSSL 所影響

Java SE 更新修復 37 個重要性的問題
四月
修補程序解決了多個問題，其中包含4個為'重要性'

發布非週期性更新程式包含 Windows XP
五月
微軟以例外方式處理已停止服務的作業系統，XP 獲得 IE8 的零時差修補程序

科技龍頭資助重要的項目
五月 Core Infrastructure 核心基礎架構計畫資助 OpenSSL , OpenSSH ...等。

2014 上半年 威脅狀況概述

整體趨勢

在2014年上半年桌上型以及行動裝置系統上，勒索軟體是最值得注意且有持續增長的趨勢。雖然 **Zeus** 殭屍網路[1]已於六月被發現並移除，中斷了 **Cryptolocker** 威脅的蔓延（至少一段時間）；整體而言，觀察這半年的威脅發現，勒索軟體還是在不斷發展，就像 **Cryptolocker** 更新他們散佈方式、加密方式和付款方式，規避執法單位的查緝工作。

當 **Koler**[2]病毒威脅首次在 Android 系統裝置上被發現，已證實勒索從PC端跨足到行動裝置，儘管這惡意程式具有威脅但其實際上並沒有對行動裝置內的檔案進行加密，但不久後發現的 **Slocker** 則是會對檔案進行加密[3]。一如往常，這兩個 Android 的勒索程式偽裝為合法的應用程式誘騙用戶安裝。

同時，勒索活動在 iOS 設備上採用了不同的花招。在 iOS 7 的介紹中，啟用鎖定功能是能夠使用Apple的帳號與密碼進行遠端鎖定特定 iOS 裝置，但這個功能遭到駭客惡意使用，駭客假借可獲得“免費”的內容，誘騙蘋果用戶登入Apple帳密，一旦用戶登入後即授權使用憑證，犯罪份子便可以更改密碼，透過尋找我的iphone功能鎖定裝置，藉此要求贖金，iOS平台上的勒索案例：**‘Oleg Pliss’**，發生在五月，受影響的用戶多位於澳大利亞，事件發生後有兩個人為此在莫斯科被逮捕[4]。

根據相關報導，安全研究人員的報告[5]中指出地下論壇正在進行討論開發 DIY 勒索套件。雖然這些都是未驗證的傳言，但事實上大部分的惡意軟體已經轉變為被程式化的開發工具了，也就是“一鍵製造”的程式，所以未來**勒索軟體的開發套件**釋出似乎也是合理的未來推測了

這些進展與對政府機構與企業發動針對性攻擊並收集資料的報告不謀而合，其中最受注目的案件包括 Nokia 勒索事件[6]。被這些攻擊程序擊中的案例已層出不窮，對於家庭、企業以及政府的用戶，只能持續強調數據安全的重要性。

同時，**Windows XP** 終於在2014年4月8日(停止服務)宣布退役(儘管如此，卻在停止服務後不久，額外提供修補程序)。儘管有鼓勵用戶升級到 Windows 8（確實，任何作業系統對此都是大力支持的），世界各地仍然有10%~30%的電腦用戶繼續使用現在已不在提供任何修補程序的系統[7]，這些族群就會受到攻擊者的青睞。雖然一些用戶(特別是政府與企業用戶)延長了 XP 的支援，但對於大多數用戶來說，從現在起，安全性將會變成“自助式服務”。

2014年上半年報導指出，各國政府機關的線上審查或資料處理工作，有可疑的監控行為。主要的高科技公司都作出了各種努力，以提高其產品的安全性，並向他們的政府機關施壓，要求增加透明度。相關細節請參閱我們2014年上半年事件回顧。

電腦惡意軟體

正如我們在2014年上半年統計前十大檢測數最普遍的威脅，與我們去年下半年用戶回報系統偵測的惡意軟體威脅大致相同，只是排名順序有所變動。在這半年期間 **Downadup**（俗稱Conficker）回報最多的威脅，特別是在中東，南美和亞洲。這隻已6歲大的蠕蟲病毒持續在世界各地不斷成長，由於Windows XP已停止更新服務，這些問題也不太可能改善。

除了Downadup，歐洲以及北美這半年最明顯的仍然是**Majava**和**網頁式攻擊**。而檔案感染者的**Sality**與**Ramnit**家族的威脅也已存在多年，除了北美與歐洲地區，它還繼續在各地製造麻煩。

惡意軟體家族 **Wormlink, BrowserExploit** 與**Expiro**是前10名的新成員。而有趣的是，相關的具體檢測在今年上半年有明顯的變化，已知漏洞(如:CVE-2013-2471)已經不在我們的前十大檢測名單內。

十大病毒威脅排行榜

%

31 DOWNADUP / CONFICKER

蠕蟲

利用Windows的MS08 - 067漏洞在網路上進行散佈(也透過可卸載的裝置和網路磁碟機)，該蠕蟲已經感染了全球200多個國家中的數百萬台電腦。經過了六年，在沒有修補漏洞的電腦上Downadup仍在運行。在上半年，它仍活躍於**巴西**、**阿拉伯聯合大公國**、**意大利**，以及**馬來西亞**還有這一年的**法國**。

20 WEB-BASED ATTACKS

重新導向

惡意軟體組織利用漏洞或技術將網路瀏覽器重新導向至惡意網站，讓瀏覽器或系統因此遭受更多的攻擊。從2013年年底的報告來看，未來應該是**法國**、**美國**和**瑞典**會有較多的檢測數量，但今年**馬來西亞**的檢測數量最多並超越了這三個國家。

11 MAJAVA

漏洞攻擊

一個針對Java開發平台的漏洞的攻擊。攻擊成功後，攻擊者就可獲得整個系統的控制權。報告中最常出現的是**美國**、**法國**和**英國**的用戶。

10 SALITY

病毒

一個非常大的病毒家族，感染執行檔並使用入口點遮蔽來隱藏他們的存在。其變種病毒還可以對電腦進行結束程序、竊取資料等行為。首次出現在2010年，Sality系列的病毒在**馬來西亞**，**巴西**，**土耳其**和**印度**最為活躍。

9 RAMNIT

病毒

感染的EXE，DLL和HTML文件，也可以植入一個會嘗試從遠端伺服器下載更多惡意軟體的檔案。

首例發現在2011年，Ramnit集中在亞洲地區，特別是**馬來西亞**、**印度**、**越南**和**印尼**。

7 AUTORUN

蠕蟲

多數是經由被感染的卸除裝置和硬碟來進行散佈。這個家族的變種包含了有害的負載程序，例如資料竊取程式。在AUTORUN的檢測報告中最常見的有**法國**、**馬來西亞**、**印度**、**波蘭**和**土耳其**。

4 WORMLINK

漏洞

檢測到惡意的捷徑圖示，以利用Windows的安全性漏洞CVE-2010-2568來取得系統的所有控制權。在這份威脅報告中顯示主要是來自**馬來西亞**、**土耳其**、**越南**和**印度**。

3 BROWSEREXPLOIT

漏洞

檢測到正在使用的瀏覽器程序遭植入並運行一個潛在的有害程序。這類的檢測報告大多來自於**美國**、**芬蘭**、**法國**和**英國**。

3 EXPIRO

病毒

感染可執行檔，並使用一個鍵盤記錄器的套件竊取信用卡的資訊。最常見的在**意大利**、**芬蘭**、**美國**、**法國**和**德國**。

2 ZEROACCESS

殭屍網路

這個殭屍網路的餘孽，繼續在**法國**、**美國**、**英國**、**瑞典**和**芬蘭**等地製造麻煩。

Mac 的惡意軟體

2014年開始首2個月就發現了20種獨特的新變體，儘管後來速度有減緩，但在上半年結束時，仍發現了25種新的Mac病毒。在這些獨特的新變體種中，有13個變體分別屬於五個新家族，**Mask**和**Clientsnow**均屬於針對性攻擊。剩下的三個新家族:**Coinstealer**,**Cointhief**和**LaoShu**則會影響一般Mac用戶。關於新型的Mac病毒在第14頁有更多詳細的介紹。

行動裝置

2014年第一季看到了許多著名的手機惡意軟體(在我們的2014年第一季行動威脅報告有更詳細敘述)。在2014年第二季，大多數的威脅在我們的Android手機安全軟體的用戶均持續回報至我們的針對Android平台設置的監測系統。木馬病毒仍是手機惡意軟體的主要類型，高度依賴簡單的社交工程來取得該設備與資料的存取權。

威脅報告中最常見的是SMSSend，FakeInst和Eropl三個家族。在這期間還意外地看到了兩個簡訊蠕蟲病毒，且還在現有的Android設備中流竄。Android相關惡意軟體的詳細介紹在第12頁。

iOS 的惡意軟體

在iOS平台上的實際惡意應用程序是寥寥可數，但它們確實存在。不同於Android的，惡意軟體在iOS上迄今只能有效地對抗越獄的裝置，安全研究人員對各種駭客裝備(而這些通常是利用在平台上未公開的漏洞來進行工作)製作的越獄工具是感興趣的。今年六月，適用於iOS7.1.1的**Pangu**工具意外被釋出，有些指控說它使用偷來的利用工具，以及擔憂這個工具會與應用程式商店中盜版的"shady"一併被安裝。在後續的更新中這兩個問題都已解決[8]。

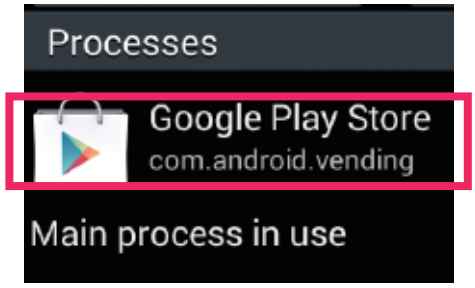
在上半年前期，reddit的用戶反映有可疑的程式庫檔案，隨後命名為**Unflod Baby Panda**。當越獄的iOS設備安裝了，惡意軟體監聽SSL連線的資訊傳送並竊取Apple的帳號與密碼[9]。更多iOS惡意軟體的詳細介紹在第14頁。

Constants

儘管各種創新和發展，我們看到過去的這個季度，許多行動裝置的相關研究結果，我們證明了在2013年H2威脅報告中的預測是正確的。當我們又看了看app store的安全性在2014年上半年（比較我們在app store獲得的樣本總數的數量），我們看到從我們記錄上次報告的結果沒有顯著變化。儘管四個新的惡意應用程序被發現，上半年並在Google的Play商店增溫，考慮應用程序廣大的市場，手機病毒的發病率較低（目前為止），且都有能迅速採取補救措施的團隊做處理，目前Play商店仍算是最安全的手機應用程式市場。

當中也有無顯著變化是惡意Android應用程序的包裝名稱，其中大多數都是假冒的，但用合法名稱（例如，com.software.app）讓使用者下載，或者直接使用無意義的名稱（如，fkjsgmjl.ceinnykas）。當中以Fakeinst病毒家族尤為普遍。

同時檢查軟體名字依然標準的安全防備措施為針對桌上型的威脅，同樣的方式卻很難用於Android，因為內容名稱的顯示幾乎不會顯示給使用者，而可見設備上僅用於正在運行的進程的設置下>應用程式>運行>進程功能表。這是不太可能很快就改善的，在下載時保持警惕仍然是現在最有效的讓使用者能預防並避免木馬的方式。



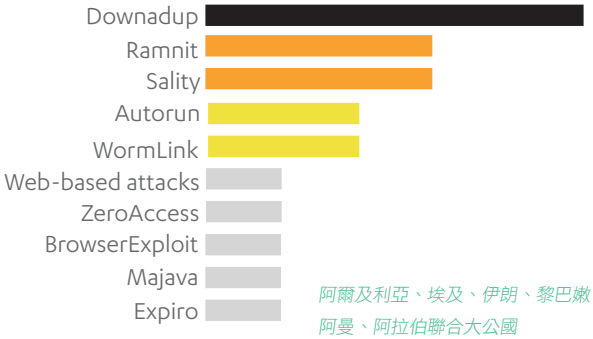
來源

1. Federal Bureau of Investigations; *GameOver Zeus Botnet Disrupted*; 2 Jun 2014; http://www.fbi.gov/news/stories/2014/june/gameover-zeus-botnet-disrupted/gameover-zeus-botnet-disrupted
2. F-Secure Weblog; *"Police Ransomware" Expands To Android Ecosystem*; 16 Jun 2014; http://www.f-secure.com/weblog/archives/00002704.html
3. F-Secure Weblog; *SLocker Android Ransomware Communicates Via Tor And SMS*; 16 Jun 2014; http://www.f-secure.com/weblog/archives/00002716.html
4. Info Security; *'Oleg Pliss' Apple Hackers Could Be Behind Bars*; 10 Jun 2014; http://www.infosecurity-magazine.com/news/oleg-pliss-apple-hackers-could-be/

十大病毒威脅排行榜 依地區統計
每1000名用戶

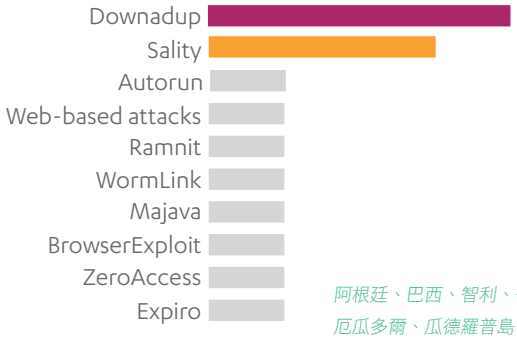
高於500 /每1 000個 | 介於250 - 500 /每 1 000個 | 介於100 - 250 /每1 000個 | 介於50 - 100 /每1 000個 | 介於0-50 /每1 000個

中東



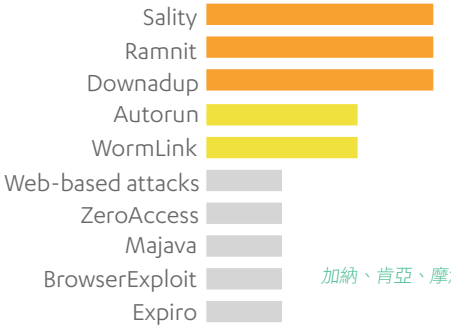
阿爾及利亞、埃及、伊朗、黎巴嫩、阿曼、阿拉伯聯合大公國

南美



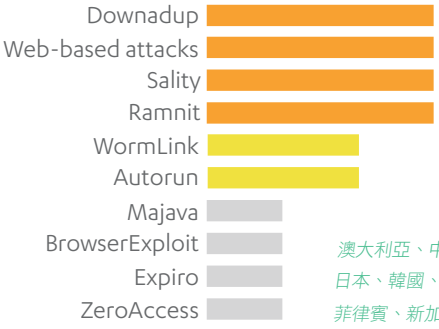
阿根廷、巴西、智利、哥倫比亞、哥斯達黎加、厄瓜多爾、瓜德羅普島

非洲



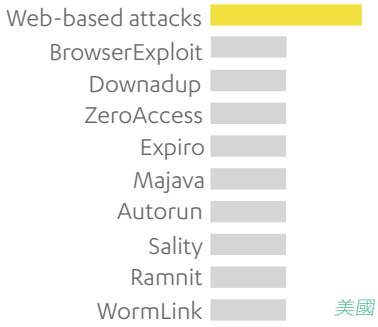
加納、肯亞、摩洛哥、南非、突尼斯

亞洲



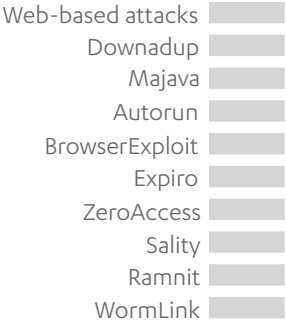
澳大利亞、中國、香港、印度、印尼、日本、韓國、馬來西亞、紐西蘭、巴基斯坦、菲律賓、新加坡、臺灣、泰國、土耳其、越南

北美



美國、加拿大、墨西哥

歐洲



奧蘭群島、奧地利、比利時、保加利亞、波士尼亞與赫塞哥維納、克羅地亞、 捷克、丹麥、愛沙尼亞、 芬蘭、法國、德國、希臘、匈牙利、愛爾蘭、意大利、拉脫維亞、立陶宛、盧森堡、荷蘭、挪威、 波蘭、葡萄牙、羅馬尼亞、俄羅斯、塞爾維亞、斯洛伐克、斯洛文尼亞、西班牙、瑞典、瑞士、烏克蘭、英國

備註：其他國家由於缺少有效的數據而排除

5. Arstechnica; Dan Goodin; *Researchers warn of new, meaner ransomware with unbreakable crypto*; 7 Jan 2014; http://arstechnica.com/security/2014/01/researchers-warn-of-new-meaner-ransomware-with-unbreakable-crypto/
6. BBC; *Nokia 'paid blackmail hackers millions'*; 18 Jun 2014; http://www.bbc.com/news/technology-27909096
7. Tech Republic; Tony Bradley; *Windows XP use declining, but millions still willingly at risk*; 16 Apr 2014; http://www.techrepublic.com/article/windows-xp-use-declining-but-millions-still-willingly-at-risk/
8. International Business Times; *Pangu 1.1.0 Apple iOS 7.1.1 Jailbreak Update Adds Mac OS X Support And Removes 25PP Option*; 30 Jun 2014; http://www.ibtimes.com/pangu-110-apple-ios-711-jailbreak-update-adds-mac-os-x-support-removes-25pp-option-1615366
9. SektionEins; *iOS Malware Campaign "Unflod Baby Panda"*; 18 Apr 2014; https://sektioneins.de/en/blog/14-04-18-iOS-malware-campaign-unflod-baby-panda.html

2014 第二季 行動裝置的惡意軟體

新發現 病毒家族或變種

294 Android

1 iPhone

Trojan:iPhoneOS/SSLCredThief
簽署程式庫檔案被監聽並從SSL的連線資訊中竊取Apple的帳號和密碼

前三名 ANDROID 家族

Trojan:Android/SMSSend
惡意軟體的大家族，會發送高額的SMS簡訊

Trojan:Android/FakeInst
會安裝其他app，且發送高額SMS簡訊

Trojan:Android/Eropl
從裝置上悄悄地收集資料並傳送到遠端伺服器

% 各國排名

- 23 英國
- 11 法國
- 9 阿拉伯
- 8 印度
- 8 德國
- 8 西班牙
- 5 芬蘭
- 3 馬來西亞
- 3 巴西
- 2 荷蘭
- 21 其他國家

$$ 索取贖金

第一個勒索軟體(應該是)

Trojan:Android/Koler是以警察為主題的手機擴充套件Reveton勒索軟體。五月首次報導，當使用者瀏覽惡意網站，會被提示下載一個應用程序，聲稱是用於色情視頻播放的應用程式，一旦安裝後，應用程式立即將使用者的國際移動用戶身份碼(IMEI)號碼上傳至遠端伺服器，並開啟瀏覽器顯示一個假的通知，告知違反安全政策， 雖然聲稱對裝置上的檔案進行加密，除非支付贖金否則無法解密，但實際上只禁用了返回的按鈕。

第一個 TOR 加密的勒索軟體

不同於Koler，Trojan:Android/Slocker惡意軟體確實會將設備上的圖片、文件和影片加密。與Koler一樣的是，它還會禁用返回按鈕和干擾用戶操作。Slocker的變種更可以經由Tor網路或SMS訊息與控制伺服器聯繫。

Oleg Pliss 攻擊澳洲

'Oleg Pliss' 在今年五月鎖定在澳洲一個用戶門號的帳號，使用尋找我的iphone的功能並要求贖金。蘋果否認在在iCloud服務上有這個漏洞的推測。(也有報導指出受駭者是遭到釣魚網站詐騙Apple ID)。有兩個人六月時在莫斯科被收押，並傳出俄羅斯與此攻擊事件有關。

來源

1. Malware don't need Coffee; Kafeine; *Police Locker land on Android Devices*; 4 May 2014; http://malware.dontneedcoffee.com/2014/05/police-locker-available-for-your.html
2. McAfee Blog; Christiaan Beek; *iDroid Bot for Sale Taps Into Mobile Wallet*; 10 Apr 2014; https://blogs.mcafee.com/mcafee-labs/idroid-bot-for-sale-taps-into-mobile-wallets
3. Apple Insider; *Hackers use 'Find My iPhone' to lockout, ransom Mac and iOS device owners in Australia*; 26 May 2014; http://appleinsider.com/articles/14/05/27/hackers-break-into-lock-macs-and-ios-devices-for-ransom-in-australia
4. GData Security Blog; *Android smartphone shipped with spyware*; 16 Jun 2014; https://blog.gdatasoftware.com/blog/article/android-smartphone-shipped-with-spyware.html
5. Palo Alto Networks Research Center; Claud Xiao, Zhi Xu; *Cardbuyer: New Smart Android Trojan Defeats Multi-factor Verification and Steals Prepaid Game Cards*; 24 Apr 2014; http://researchcenter.paloaltonetworks.com/2014/04/cardbuyer-new-smart-android-trojan/
6. SektionEins; *iOS Malware Campaign "Unflod Baby Panda"*; 18 Apr 2014; https://sektioneins.de/en/blog/14-04-18-iOS-malware-campaign-unflod-baby-panda.html

新聞

附加間諜軟體
一家資安公司的報告發現一支由工廠直接出廠的智慧型手機中發現間諜軟體(Trojan:Android/SmsSend.AC)，載入於設備的韌體中，該間諜軟體可以取得完全控制權限並存取手機上的資料。

預付卡竊取
木馬：Android / Cardbuyer 據報導能竊取各種用於網路遊戲或支付平台的驗證程序，並攔截簡訊以及用戶的帳戶並偷偷的購買預付卡。

iDroidBot 發售
今年四月，俄羅斯地下論壇張貼了一則廣告發售 iDroidBot ，針對 iOS 以及Android系統設備，並且能夠儲存竊取的信用卡詳細資料和 QIWI 錢包的信用，以及其他動作。

竊取 Apple 帳密
Reddit 書籤網站使用者回報一個可疑的物件，一旦安裝該物件將被偷取正在執行的程序，並監聽竊取傳出 SSL 連接 Apple ID 與密碼的詳細資訊。該惡意軟體隨後被命名為Unflod Baby Panda。

Worm: Android/ Samsapo. A

Это твои фото?
俄語：這是你的照片?

簡訊提示下載連結安裝該應用程式要註冊你的手機至 premiumrate 服務，竊取資料，自己發送到所有電話簿聯絡人等等。

"Dear [NAME], Look the Self-time, http://goo.gl/******

簡訊提式下載 "SelfTimer" 應用程式，並發送一則簡訊給20個聯絡人，並要求用戶下載一個附加的檔案。

Worm: Android/ Selfmite

Google Play 商店

Virus Shield
今年四月，在安卓警務網站爆發消息關於 Google Play 商店排名第一的的付費應用程式（超過 1 萬個下載和 4.7 星級），這個防毒軟體其實不過是個騙局。Google 立即將應用程式下架，並提供已購買者退款，包含商店信用卡的用戶。

★★★★ 美金3.99

BankMirage
一個針對以色列米茲拉銀行惡意複製的合法應用程式，該應用程式竊取用戶的帳號及登錄表單。研究人員推測，它的目是為了往後的攻擊去收集資料，因為該應用程式沒有收集密碼。一家資安公司報告該惡意軟體在 Google Play 商店幾天內便被刪除。

免費

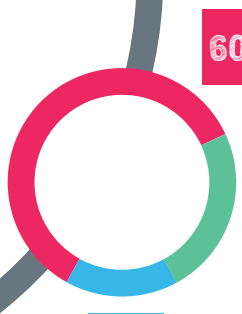
Songs & Prized
在第三方應用程式商店發現兩個 cryptocurrency 採礦應用程式。在設備充電時默默的進行數位貨幣採礦，並防止它進入休眠模式。Google Play 商店發現後立即刪除這兩個應用程式。

免費

7. WeliveSecurity; Robert Lipovsky; *Android malware worm catches unwary users*; 30 Apr 2014; http://www.welivesecurity.com/2014/04/30/android-sms-malware-catches-unwary-users/
8. Naked Security; Paul Ducklin; *Anatomy of an Android SMS virus - watch out for text messages, even from your friends!*; 29 Jun 2014; http://nakedsecurity.sophos.com/2014/06/29/anatomy-of-an-android-sms-virus-watch-out-for-text-messages-even-from-your-friends/
9. Android Police; Michael Crider; The #1 New Paid App In The Play Store Costs $4, Has Over 10,000 Downloads, A 4.7-Star Rating... And It's A Total Scam [Updated]; 10 Apr 2014; http://www.androidpolice.com/2014/04/06/the-1-new-paid-app-in-the-play-store-costs-4-has-over-10000-downloads-a-4-7-star-rating-and-its-a-total-scam/
10. Lookout Blog; Meghan Kelly; *Cloned banking app stealing usernames sneaks into Google Play*; 24 Jun 2014; https://blog.lookout.com/blog/2014/06/24/bankmirage/
11. ZDNet; Liam Tung; *Google yanks two battery-sucking Bitcoin mining Android apps from Play store*; 28 Mar 2014; http://www.zdnet.com/google-yanks-two-battery-sucking-bitcoin-mining-android-apps-from-play-store-7000027828/

2014 上半年 MAC 惡意軟體

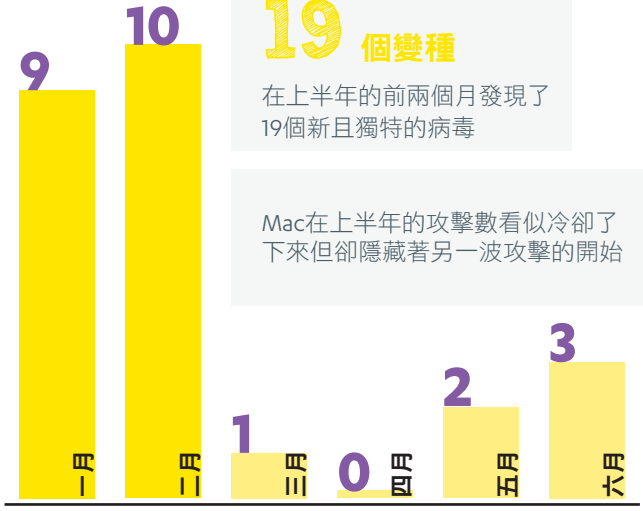
25
新變種
期間分別發現Mac的惡意軟體總數
2014 年 1 月至 6 月



60% **Backdoor**（後門）

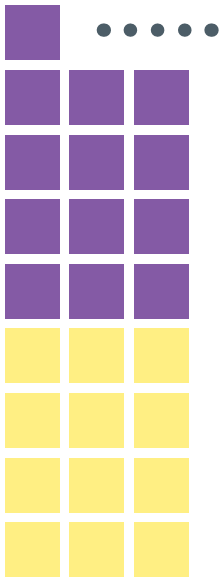
24% **Trojan**（木馬）

16% **Others**（其他）



19 個變種
在上半年的前兩個月發現了19個新且獨特的病毒

Mac在上半年的攻擊數看似冷卻了下來但卻隱藏著另一波攻擊的開始



13 (25個變種之中) **個變種**

屬於

5個新的家族

2個使用在目標式攻擊

CoinThief

3個定期影響Mac用戶

MASK

Mask家族是屬於高度專業化網路間諜所操作，它的目標是政府機關與能源公司

CLIENTSNOW

Clientsnow家族具有連結至間諜網路。這是許多攻擊MAC的惡意軟體家族之一，主要針對藏族和維吾爾族

COINTHIEF

CoinThief 家族是一個木馬間諜程序用於竊取cryptocurrencies。自2013年第二季，它已經成功透過BitTorrent散佈，冒充熱門的OSX應用程式破解版。但在2014年初，它改變了策略，開始透過網路論壇如Github和流行的下載論壇如 *downloads.com.* 來傳播木馬病毒cryptocurrency。

在戰術上證明這種變化是有效的，因為該cryptocurrency應用程式[1]已經被許多下載，而大多數的人他們都不希望在合法的下載網站發現木馬病毒應用程式。這導致許多用戶數量被影響，並且最終該家族被發現[2]。

LAOSHU

LaoShu(在中文翻譯為老鼠或小白鼠)家族是一個遠端存取木馬程序，經由偽裝的郵件進行散播

COINSTEALER

Coinstealer家族是一個比特幣的偷竊者，冒充比特幣交易平台Mt. Gox後台應用程式使訪問者[3]洩漏資訊。駭客是透過入侵Reddit書籤網站的個人帳戶以及其部落格。Mt. Gox的執行長[4]在關閉其比特幣交易平台後不提供任何的解釋[5]。它似乎並企圖利用該平台的漏洞，而當時Mt.Gox的客戶急著了解更多細節。

***註:** 圖中所示的數字是檢測到的獨特變種數量。這意味著重新打包安裝的惡意軟體不被計算多次而被算做一次。

資料來源

1. Twitter; Broderick Aquilino; 12 February 2014; https://twitter.com/BrodAquilino/status/433529401699864576
2. Threatpost; Michael Mimoso; *Mac Trojan Steals Bitcoin Wallet Credentials*; 10 February 2014; http://threatpost.com/mac-trojan-steals-bitcoin-wallet-credentials/104152
3. Wikipedia; *Front and back office application*; 24 March 2014; http://en.wikipedia.org/wiki/Front_and_back_office_application
4. Forbes; Andy Greenberg; *Hackers Hit Mt. Gox Exchange's CEO, Claim To Publish Evidence Of Fraud*; 9 March 2014; http://www.forbes.com/sites/andygreenberg/2014/03/09/hackers-hit-mt-gox-exchanges-ceo-claim-to-publish-evidence-of-fraud/
5. Forbes; Andy Greenberg; *Bitcoin's Price Plummets As Mt. Gox Goes Dark, With Massive Hack Rumored*; 25 February 2014; http://www.forbes.com/sites/andygreenberg/2014/02/25/bitcoins-price-plummets-as-mt-gox-goes-dark-with-massive-hack-rumored/

資料來源

2014上半年行事曆

數位自由

1. The Guardian; Spencer Ackerman, James Ball; *Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ*; 28 Feb 2014; http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo
2. Arstechnica; Sean Gallagher; *Turkey now trying to block YouTube as social media crackdown continues*; 28 Mar 2014; http://arstechnica.com/tech-policy/2014/03/turkey-now-trying-to-block-youtube-as-social-media-crackdown-continues/
3. Reuters; *Thai ministry sparks alarm with brief block of Facebook*; 28 May 2014; http://in.reuters.com/article/2014/05/28/thailand-politics-facebook-idINKBN0E80U520140528
4. Arstechnica; Sean Gallagher; *NSA loves The Bahamas so much it records all its cellphone calls*; 21 May 2014; http://arstechnica.com/tech-policy/2014/05/nsa-loves-the-bahamas-so-much-it-records-all-its-cellphone-calls/
5. Guardian; Glenn Greenwald; *How the NSA tampers with US-made internet routers*; 12 May 2014; http://www.theguardian.com/books/2014/may/12/glenn-greenwald-nsa-tampers-us-internet-routers-snowden
6. BBC; Joe Miller; *Iraq blocks Facebook and Twitter in bid to restrict Isis*; 16 Jun 2014; http://www.bbc.com/news/technology-27869112
7. CNET; Micheal Tan; *After Thailand's coup, a stifling of online dissent (Q&A)*; 12 Jun 2014; http://www.cnet.com/news/behind-thailands-high-tech-coup-stifling-online-dissent-q-a/
8. BBC; *YouTube access restored in Turkey*; 4 Jun 2014; http://www.bbc.com/news/technology-27691892

攻擊事件

9. Forbes; James Lyne; *Yahoo Hacked And How To Protect Your Passwords*; 31 Jan 2014; http://www.forbes.com/sites/jameslyne/2014/01/31/yahoo-hacked-and-how-to-protect-your-passwords/
10. Arstechnica; Dan Goodin; *Hackers hijack 300,000-plus wireless routers, make malicious changes*; 4 Mar 2014; http://arstechnica.com/security/2014/03/hackers-hijack-300000-plus-wireless-routers-make-malicious-changes/
11. Reuters; *Bitcoin bank Flexcoin shuts down after theft*; 4 Mar 2014; http://www.reuters.com/article/2014/03/04/us-bitcoin-flexcoin-idUSBREA2329B20140304
12. TechRadar; Stu Robarts; *Windigo malware attack infects 25,000 servers*; 19 Mar 2014; http://www.techradar.com/news/computing/windigo-malware-attack-infects-25-000-servers-1235128
13. NYTimes; Nicole Perlroth; Heartbleed exploited to hack VPN device; 18 Apr 2014; http://bits.blogs.nytimes.com/2014/04/18/heartbleed-internet-security-flaw-used-in-attack/?_php=true&_type=blogs&_r=0
14. The Australian; Cyber attacks on the rise; 29 May 2014; http://www.theaustralian.com.au/news/latest-news/cyber-attacks-on-the-rise/story-fn3dxiwe-1226936311311?nk=9a4d4fc48406e6e6a41b8e14de5fa4d6
15. KrebsonSecurity; Brian Krebs; *True Goodbye: 'Using TrueCrypt Is Not Secure'*; 29 May 2014; http://krebsonsecurity.com/2014/05/true-goodbye-using-truecrypt-is-not-secure/
16. The Register; Darren Pauli; *Massive DDoS attack hits Hong Kong*; 23 Jun 2014; http://www.theregister.co.uk/2014/06/23/most_sophisticated_ddos_strikes_hk_democracy_poll/

安全性

17. F-Secure Weblog; Sean Sullivan; *FISA Transparency*; 4 Feb 2014; http://www.f-secure.com/weblog/archives/00002666.html
18. F-Secure Weblog; Sean Sullivan; *TrustyCon Video*; 28 Feb 2014; http://www.f-secure.com/weblog/archives/00002679.html
19. ZDNet; Larry Seltzer; *Windows XP dies at 12 1/2 after long illness*; 8 Apr 2014; http://www.zdnet.com/windows-xp-dies-at-12-12-after-long-illness-7000028134/
20. BBC; Leo Kelion; *eBay makes users change their passwords after hack*; 21 May 2014; http://www.bbc.com/news/technology-27503290
21. PCWorld; Mark Hachman; *Microsoft simplifies security updates with MyBulletins*; 28 May 2014; http://www.pcworld.com/article/2207346/microsoft-simplifies-security-updates-with-mybulletins.html
22. PC Mag; Stephanie Mlot; *Google launches 'right to be forgotten' form*; 30 May 2014; http://www.pcmag.com/article2/0,2817,2458736,00.asp
23. Forbes; Ben Kepes; *No More Scroogled, No More NSA, Google Apps Gets Encryption*; 21 May 2014; http://www.forbes.com/sites/benkepes/2014/05/21/no-more-scroogled-no-more-nsa-google-apps-gets-encryption/
24. The Guardian; Dominic Rushe; *Edward Snowden calls for greater online privacy in Reset the Net campaign*; 5 Jun 2014; http://www.theguardian.com/world/2014/jun/05/edward-snowden-privacy-reset-the-net

執法事件

25. United States Department of Justice; *Cyber Criminal Pleads Guilty to Developing and Distributing Notorious Spyeye Malware*; 28 Jan 2014; http://www.justice.gov/opa/pr/2014/January/14-crm-091.html
26. United States Department of Justice; *Leader and Co-Conspirator of Android Mobile Device App Piracy Group Plead Guilty*; 24 Mar 2014; http://www.justice.gov/opa/pr/2014/March/14-crm-303.html
27. United States Department of Justice; *Nine Charged in Conspiracy to Steal Millions of Dollars Using "Zeus" Malware*; 11 Apr 2014; http://www.justice.gov/opa/pr/2014/April/14-crm-375.html
28. The Register; Simon Sharwood; *'Anons' cuffed by Australian Federal Police*; 22 May 2014; http://www.theregister.co.uk/2014/05/22/anons_cuffed_by_australian_federal_police/
29. The Register; Iain Thomson; *US authorities name five Chinese military hackers wanted for espionage*; 19 May 2014; http://www.theregister.co.uk/2014/05/19/us_authorities_name_five_chinese_military_hackers_wanted_for_espionage/
30. SC Magazine UK; Doug Drinkwater; *100 hackers arrested over Blackshades Trojan*; 19 May 2014; http://www.scmagazineuk.com/100-hackers-arrested-over-blackshades-trojan/article/347488/
31. Info Security; *'Oleg Pliss' Apple Hackers Could Be Behind Bars*; 10 Jun 2014; http://www.infosecurity-magazine.com/news/oleg-pliss-apple-hackers-could-be/
32. United States Department of Justice; *U.S. Leads Multi-National Action Against "Gameover Zeus" Botnet and "Cryptolocker" Ransomware, Charges Botnet Administrator*; 2 Jun 2014; http://www.justice.gov/opa/pr/2014/June/14-crm-584.html

惡意程式

33. Malware Must Die; *Threat Intelligence - New Locker: Prison Locker (aka: Power Locker ..or whatever those bad actor call it)*; 3 Jan 2014; http://blog.malwaremustdie.org/2014/01/threat-intelligence-new-locker-prison.html
34. F-Secure Weblog; Sean Sullivan; *Gameover ZeuS Jumps on the Bitcoin Bandwagon*; 14 Mar 2014; http://www.f-secure.com/weblog/archives/00002685.html
35. InfoSec Handlers Diary Blog; Johannes Ullrich; *Linksys Worm "TheMoon" Summary: What we know so far*; 13 Feb 2014; https://isc.sans.edu/diary/Linksys+Worm+%22TheMoon%22+Summary%3A+What+we+know+so+far/17633
36. F-Secure Weblog; *Coremex Innovates Search Engine Hijacking*; 1 Apr 2014; http://www.f-secure.com/weblog/archives/00002689.html
37. Android Police; Michael Crider; *The #1 New Paid App In The Play Store Costs $4, Has Over 10,000 Downloads, A 4.7-Star Rating... And It's A Total Scam [Updated]*; 10 Apr 2014; http://www.androidpolice.com/2014/04/06/the-1-new-paid-app-in-the-play-store-costs-4-has-over-10000-downloads-a-4-7-star-rating-and-its-a-total-scam/
38. F-Secure Weblog; *"Police Ransomware" Expands To Android Ecosystem*; 15 May 2014; http://www.f-secure.com/weblog/archives/00002704.html
39. F-Secure Weblog; Broderick Aquilino; *BlackEnergy Rootkit, Sort Of*; 13 Jun 2014; http://www.f-secure.com/weblog/archives/00002715.html
40. F-Secure Weblog; Daavid Hentunen; *Havex hunts ICS/SCADA systems*; 23 jun 2014; http://www.f-secure.com/weblog/archives/00002718.html

漏洞事件

41. ZDNet; Violet Blue; *Major Apple security flaw: Patch issued, users open to MITM attacks*; 22 Feb 2014; http://www.zdnet.com/major-apple-security-flaw-patch-issued-users-open-to-mitm-attacks-7000026624/
42. KrebsonSecurity; Brian Krebs; *Microsoft Warns of Attacks on IE Zero-Day*; 27 Apr 2014; http://krebsonsecurity.com/2014/04/microsoft-warns-of-attacks-on-ie-zero-day/
43. PCWorld; Ian Paul; *Adobe releases emergency Flash patch for Windows and OS X systems*; 8 Feb 2014; http://www.pcworld.com/article/2027624/adobe-releases-emergency-patch-for-windows-and-os-x-systems.html
44. Arstechnica; Dan Goodin; Zero-day vulnerability in Microsoft Word under active attack; 25 Mar 2014; http://arstechnica.com/security/2014/03/zero-day-vulnerability-in-microsoft-word-under-active-attack/
45. CNet; Richard Nieva; *Heartbleed bug: What you need to know (FAQ)*; 11 Apr 2014; http://www.cnet.com/news/heartbleed-bug-what-you-need-to-know-faq/
46. KrebsonSecurity; Brian Krebs; *Critical Java Update Plugs 37 Security Holes*; 16 Apr 2014; http://krebsonsecurity.com/2014/04/critical-java-update-plugs-37-security-holes/
47. Bit-tech; Gareth Halfacree; *Windows XP gets first post-EOL security patch*; 2 May 2014; http://www.bit-tech.net/news/bits/2014/05/02/winxp-eol-patch/1
48. SCMagazine; Marcos Colon; *Tech giants to fund vital projects*; 29 May 2014; http://www.scmagazine.com/core-infrastructure-initiative-to-fund-openssl-audit/article/349068/