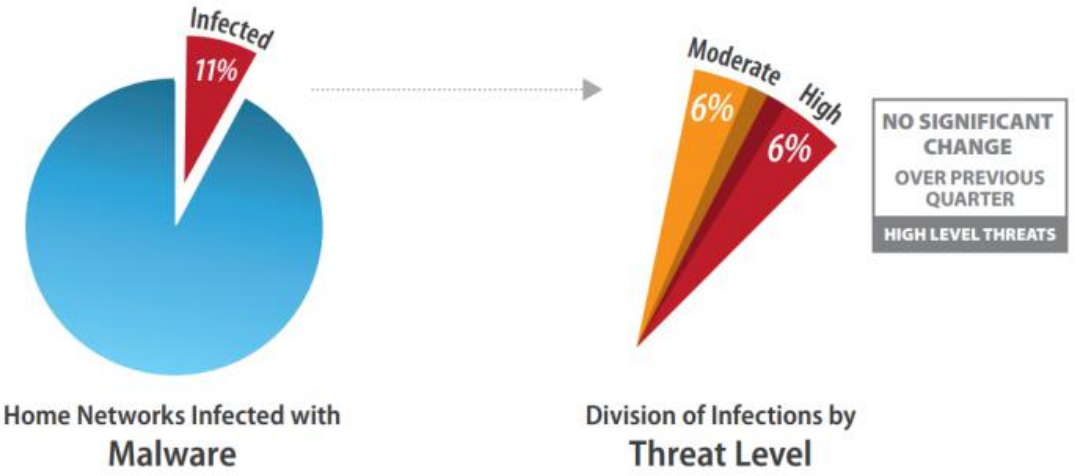
惡意程式發展趨勢
Android 安全威脅大幅成長

資料來源：Malware Wold; InSecure Magazine #37

翻譯整理：叡揚資訊 資訊安全事業處

行動網路中毒增加 67%

Kindsight 最新發佈關於家庭網路和行動網路安全報告指出，家庭網路感染惡意程式略為下降，但行動網路感染卻大幅上升。報告重點包含：



- 2012 年第四季家庭網路中毒率由 13%下降至 11%，其中 6%屬高威脅性的殭屍程式、Rootkits、金融木馬(banking Trojans)等。
- ZeroAccess 殭屍網路仍是最常見的威脅，有 0.8%寬頻網路用戶中毒。
- 0.5%的行動網路裝置存在高威脅惡意程式，相較於前一季的 0.3%中毒率，增加了 67%。
- Android 惡意程式樣本數相較於前一季，大幅增加 5.5 倍。

此份報告也首次列出年度數據：

- 2012 年北美地區 13%家庭網路被植入惡意程式，7%的寬頻用戶，被植入高威脅惡意程式。
- 2012 年前五大高威脅惡意程式，殭屍網路佔了四名，包括 ZeroAccess, TDSS, Alureon, Flashback。

惡意程式用釣魚手法繞過銀行安檢

銀行木馬採取瀏覽器中間人 (Man-in-the-Browser)攻擊手法，過去已有成功案例，像是讓用戶填寫看似為合法網站的假表單，或是綁架驗證過的議程(Session)，取得用戶的帳戶轉帳權限，用背景轉帳，將錢轉給歹徒設立的收款帳戶。

GSS Galaxy Software Services 叡揚資訊
台北總公司：10461 台北市中山區德惠街 9 號 5 樓 TEL：(02)2586-7890 FAX：(02)2586-8787
高雄辦公室：80453 高雄市明華路 317 號 6 樓 TEL：(07)586-6195
海外據點：上海、北京 營業範圍：兩岸三地及日本 www.gss.com.tw

不過金融機構也已開始反制，監控瀏覽器與應用系統之間的議程(Session)，類似 Tinba, Tilon, Shylock 這類採用 Man-in-the-Browser 手法的惡意行為，已經可以偵測與防禦；所以惡意程式作者必須採用新手法來躲避監控。

最近 Trusteer 公司發現改寫過的 Tinba 與 Tilon 惡意程式，試圖用釣魚和阻擋用戶進入銀行真正頁面的手法，來發動攻擊。

“Trusteer 技術長 Amit Klein 指出：當受害者想登入網路銀行，惡意程式會偽冒網銀登入頁面，等待受害者輸入認證資訊到這個偽冒頁面後，惡意程式會輸出錯誤訊息，告知受害人目前網銀服務中斷，但同時惡意程式已經取得受害人認證資訊，於是歹徒可以用另一台電腦登入受害者帳戶，進行冒領等詐騙交易。”

“即使銀行採取一次性密碼、憑證卡片等雙因認證(Two-factor authentication)機制，惡意程式也能透過偽冒網頁取得這些資訊。加上惡意程式阻擋用戶進入真正的網路銀行網頁，所以銀行端後台安全系統完全無法查覺任何這類惡意程式的異常活動或是詐騙行為。”

所幸目前這種改版的惡意程式詐騙活動不多；然而銀行必須能夠同時防禦綁架對話(session hijacking)和偷取憑證(credential’ s theft)兩種攻擊手法，才不致於讓網銀客戶身處險境。

能躲避偵查的惡意程式

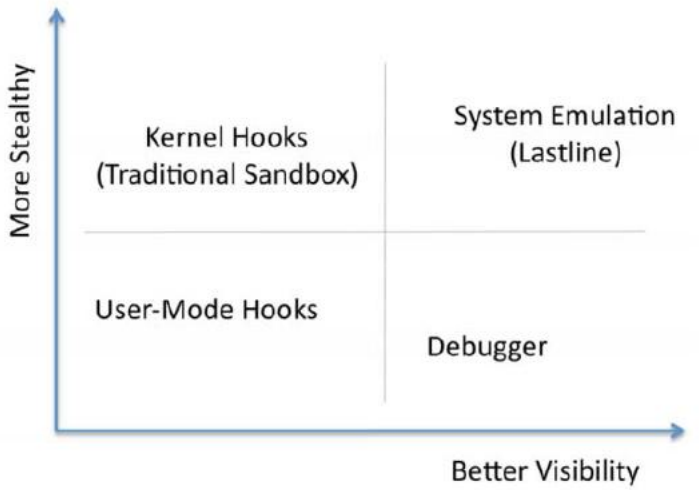


Figure 1: Visibility versus stealth for different malware analysis approaches

Lastline 公司最近的研究報告說明了惡意程式作者如何利用一般砂箱偵測技術的限制，有效發動特定目標攻擊和零時差攻擊；以及採用延遲發動程式(stalling codes)技術，將是惡意程式躲避偵查的主要發展方向之一。

此份報告指出兩種惡意程式作者採用的躲避手法：環境檢查(environmental checks)與延遲發動程式。惡意程式透過檢查運行環境來決定後續行動的手法已很常見，而延遲發動程式則是散播惡意程式的最新手法；它會刻意延遲惡意程式碼在砂箱內的執行，並且用看似合法的執行碼來魚目混珠，讓砂箱誤判，等到砂箱檢查結束(time-out)，這個會躲避偵查的惡意程式才會開始肆無忌憚地發動攻擊。報告指出這種延遲發動程式特別棘手，因為就算已知其手法，傳統的砂箱偵查仍然無法應付。

GSS 叡揚資訊 Galaxy Software Services
台北總公司：10461 台北市中山區德惠街 9 號 5 樓 TEL：(02)2586-7890 FAX：(02)2586-8787
高雄辦公室：80453 高雄市明華路 317 號 6 樓 TEL：(07)586-6195
海外據點：上海、北京 營業範圍：兩岸三地及日本 www.gss.com.tw

老牌惡意程式對歐洲政府的間諜活動

Kaspersky 實驗室最近分析一系列採用全新，高度客製化，而且超迷你的後門型惡意程式 MiniDuke，利用 Adobe Reader 安全漏洞(CVE-2013-0640)，對政府部門(大多數在歐洲)發動攻擊的資安事件後，發表了一份新的研究報告。

Kaspersky 實驗室創辦人兼執行長 Eugene Kaspersky 指出，" MiniDuke 是用組合語言編寫，高度客製化的後門程式，而且它只有 20KB 大小。"

"結合一群老牌資深惡意程式作者，運用已知安全漏洞和社交工程手法，來攻破重要目標，特別可怕！ "

MiniDuke 仍然十分活躍，最近一次攻擊，在 2013/2/20。為達目的，攻擊者使用極為有效的社交工程手法：送出帶有惡意程式的 PDF 文件給受害者。這類 PDF 文件都與 Adobe Reader 9, 10, 11 版的安全漏洞有關，惡意攻擊者利用這些漏洞來避開砂箱檢查。

惡意程式侵入作業系統後，會將僅有 20KB 的下載程式植入受害者磁碟。每一個下載程式都是獨一無二，包含用組合語言寫成的後門程式，在系統開機時會被載入執行，並且用一組公式，算出受害系統特徵值，再用這個特徵值來加密後續通訊。

這個惡意程式可以躲過某些採取固定模式(hardcoded)分析的系統偵查 (如 VMware)，當它發現偵查工具的痕跡，會立即停止活動，避免因為進行其他作業而把尚未曝光的內容和功能解密。這說明惡意程式作者已經熟知防毒專家和資安專家分析與標示惡意程式的方法。

一旦受害目標符合預設條件，惡意程式會在受害者不知情的狀況下，用預設帳號進入 Twitter，並且找到特定的推文(tweets)。這些預設帳號是 MiniDuke Command & Control (C2)後台操縱者事先建立的，而這些特定的推文則註記了一堆加密網址(URL)，讓後門程式使用。

這些網址讓後門程式得以進入 C2，取得後續攻擊指令，並且可以透過 GIF 形式加密傳送更多的後門程式碼，到受害者端。

分析結果更顯示，MiniDuke 使用動態備援系統來躲避偵查。如果 Twitter 暫停或是帳號停用，後門程式也可以用 Google 搜尋來發現下一個 C2 的加密字串。

這個機動模式讓 C2 後台操縱者可以經常改變後門程式取得後續攻擊指令或是下載更多惡意程式碼的方法。

隨後 Bitdefender 研究人員發現某一版的 MiniDuke 已經運作至少 21 個月，最近 Kaspersky 實驗室的專家更找出兩項 MiniDuke 過去未被發現，以 Web 為本的入侵機制。

西班牙警方破獲勒索軟體犯罪集團並逮捕 11 人

西班牙警方與歐洲刑警組織的歐洲網路犯罪中心密切合作，破獲最大也最複雜，專門散佈勒索軟體（ransomware，或稱警察木馬），然後假冒警方對受害者進行勒索的網路犯罪組織(Reveton)。估計此一犯罪集團影響全球數以萬計的電腦，每年獲利超過百萬歐元。

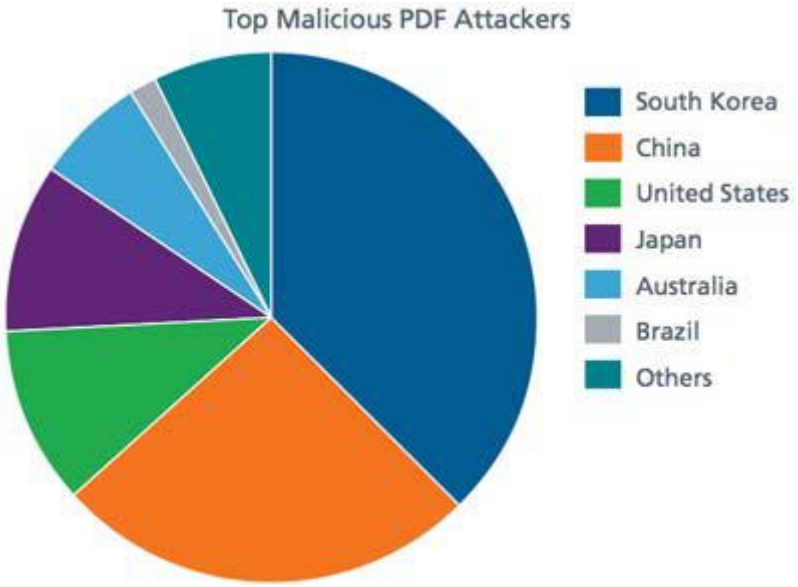
代號 Operation Ransom 的行動逮捕 11 名罪犯，搜索馬拉加省六個地點，沒收犯罪用資訊設備。調查人員還找

GSS 叡揚資訊 Galaxy Software Services
台北總公司：10461 台北市中山區德惠街 9 號 5 樓 TEL：(02)2586-7890 FAX：(02)2586-8787
高雄辦公室：80453 高雄市明華路 317 號 6 樓 TEL：(07)586-6195
海外據點：上海、北京 營業範圍：兩岸三地及日本 www.gss.com.tw

到用來提領被害者電子支付(UKash、Paysafecard、MoneyPak)款項的信用卡，以及大約 200 張在逮捕前已領出 26,000 歐元現金的信用卡。

這個犯罪集團的金融組織專門進行洗錢，而且是洗不法所得的電子錢幣。他們雙管齊下，同時用專門洗錢的虛擬系統與其他一般系統(像是各種線上遊戲入口網站、電子支付閘門和虛擬錢幣等)來洗錢。並且盜用信用卡，在西班牙境內使用 ATM 來提領贖金。最後再透過匯兌和客服中心的每日國際匯款，確認贓款轉到目的地：俄羅斯。

惡意網址取代殭屍網路成為主流



McAfee 實驗室發現，原本鎖定金融服務業的精密攻擊，也開始攻擊其他重要經濟產業，並發展一套新手法和新技術，來躲避產業標準安全措施(industrial-standard security measure)。

McAfee 實驗室資深副總裁 Vincent Weafer 指出： “我們發現攻擊目標轉向許多領域，包含工廠、企業、政府機關，以及串連這些機構的基礎設施(infrastructure)。 "

2012 年第四季，McAfee 實驗室列出下列趨勢：

- 網路罪犯明瞭用戶身份憑證是在多數電腦上都存在的高價值智慧資產之一 (專門竊取用戶密碼的木馬大增)。
- 受殭屍網路操控的系統數量有下降趨勢，部分原因是因為司法機關破獲或關閉殭屍網路。
- 作業系統底層中毒比例增加 - 主啟動磁區(MBR)類型的惡意程式比例，上升至前所未見的 27%。
- 惡意程式使用簽章躲避系統安全檢查 - 2012 年第四季帶有電子簽章的惡意程式樣本倍增。
- 行動網路惡意程式持續增加與演進 - 網路罪犯目前重心放在攻擊 Android 平台，單單在 2012 年第四季，Android 平台的惡意程式樣本大增 85%。

GSS 叡揚資訊 Galaxy Software Services
台北總公司：10461 台北市中山區德惠街 9 號 5 樓 TEL：(02)2586-7890 FAX：(02)2586-8787
高雄辦公室：80453 高雄市明華路 317 號 6 樓 TEL：(07)586-6195
海外據點：上海、北京 營業範圍：兩岸三地及日本 www.gss.com.tw