IT 威脅的演化： 2012 年第三季

出處：卡巴斯基研究室(SECURELIST)
原文網址：http://www.securelist.com/en/analysis/204792250/IT_Threat_Evolution_Q3_2012

內容

第三季的數據

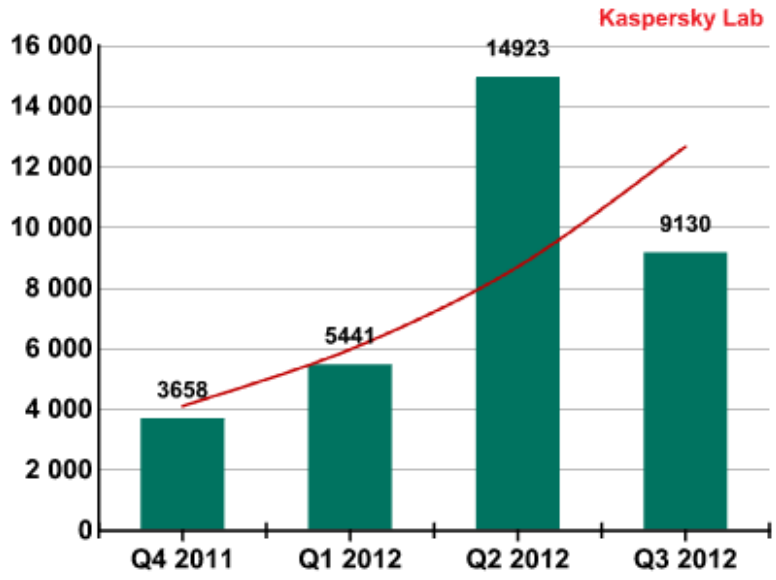
- 根據卡巴斯基研究室的資料，卡巴斯基的產品偵測並瓦解 1,347,231,728 起威脅事件在 2012 年第三季。
- 28%的手持裝置攻擊事件運行在 Android 系統 2.3.6 版本上，這個版本被發布於 2011 年九月。
- 第三季 56%被封鎖的漏洞是使用 Java 的弱點。
- 檢測到有 9190 萬的 URL 會提供惡意程式碼，比今年第二季增加 3%。

概述

手持裝置惡意軟體與作業系統

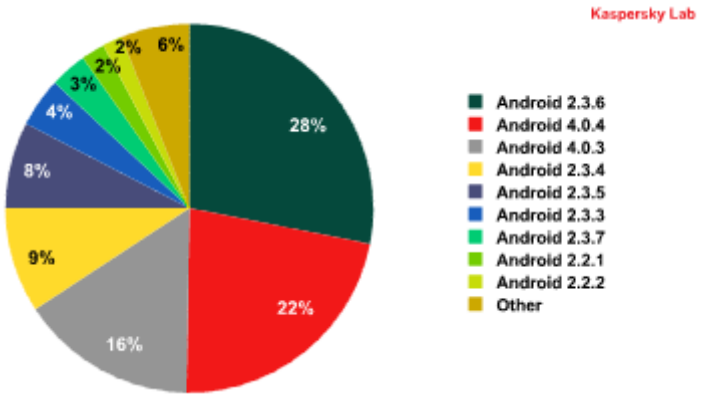
在 2012 年第三季期間，超過 9000 筆副檔名為.dex 的惡意檔案被加入我們的惡意軟體收集。跟上一季比起來減少大約 5000 筆，但是比 2012 年第一季增加了約 3500 筆。

這是因為在第二季時是採用啟發式的方式來進行惡意軟體的偵測與收集，而在第三季是採用標準的方式來進行的，並且我們使用一條線來表示我們從年初一開始所收集到的惡意軟體數量趨勢。



針對 Android 作業系統收集到的惡意軟體數量圖

令人驚訝的是 Android 版本成為網路攻擊最常見的目標。

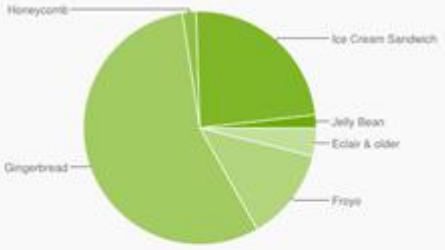


2012 年第三季所偵測到惡意軟體使用 Android 版本分佈圖

Android 2.3.6 的版本 “Gingerbread”，佔所有被封鎖的惡意軟體 28%，是最常被攻擊的版本。這個版本不是最新的，它被發布於 2011 年九月份。然而因為 Android 手持裝置於市場上的區隔，這個版本是最流行的版本之一。

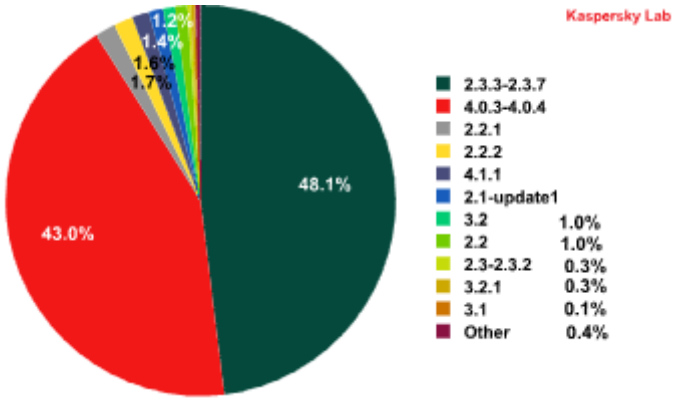
為了找出在手持裝置上 Android 系統版本的分佈與網路犯罪份子攻擊裝置上的系統分佈之間是否有相關，我們需要將我們的資料與 developer.android.com 這個官方的 Android 系統版本分佈圖做比較。以下是我們提供系統版本的百分比分佈圖於九月的最後兩周：

Version	Codename	API	Distribution
1.5	Cupcake	3	0.1%
1.6	Donut	4	0.4%
2.1	Eclair	7	3.4%
2.2	Froyo	8	12.9%
2.3 - 2.3.2	Gingerbread	9	0.3%
2.3.3 - 2.3.7		10	55.5%
3.1	Honeycomb	12	0.4%
3.2		13	1.5%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	23.7%
4.1	Jelly Bean	16	1.8%



Data collected during a 14-day period ending on October 1, 2012

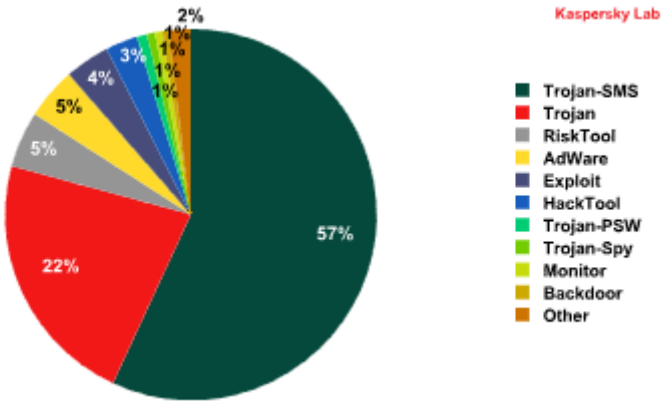
比較我們的資料於相同時期：



惡意軟體於 Android 系統上所偵測到的版本分佈圖，於九月的最後 14 天

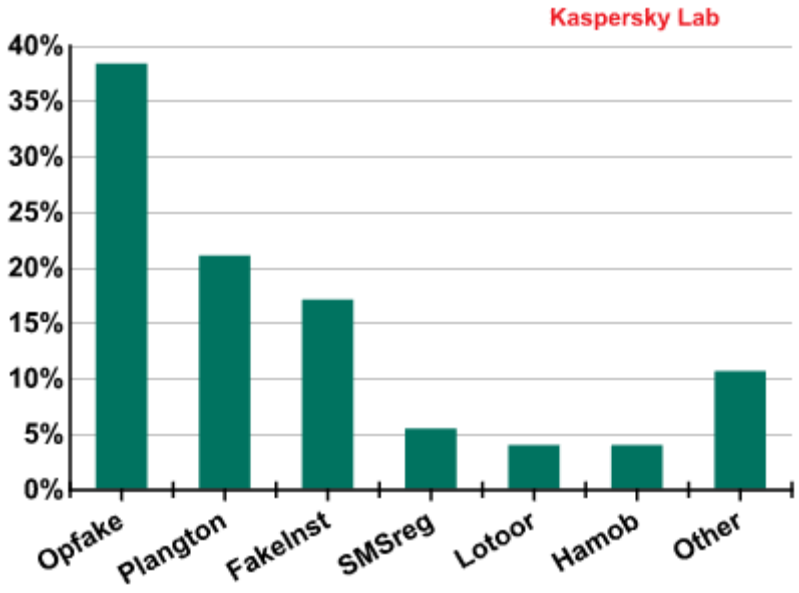
我們可以看到有些顯著地差異在兩張圖間：48%受感染的版本是使用 Gingerbread，佔所有手持裝置的 55%。43%受感染的版本是使用 Cream Sandwich，是目前最新的版本，佔所有手持裝置的 23.7%。

很明顯的，使用者會安裝最新版本的作業系統在他們的設備上是為了能更合適於線上使用。不幸的是，往往會導致使用者更有可能去拜訪有惡意內容的網站。以下我們使用卡巴斯基的統計資料來確定何種應用程序是最常被使用來攻擊使用者的設備。



惡意軟體攻擊 Android 作業系統所偵測到的行為分佈圖，於 2012 年第三季

所偵測到攻擊使用者智慧型手機的惡意軟體超過一半都是 SMS 木馬程式，這些惡意程式會藉由從受感染的手機寄送 SMS 訊息給高費率的號碼來竊取金錢。



被檢測的 Android 系統惡意軟體家族分佈圖

OpFake 家族已經成為最廣泛流行的手機惡意軟體家族。在這家族內的程式都會偽裝成 Opera Mini 這個應用程式。排名第三是 FakeInst，佔所有數量的 17%。這兩種類型的惡意軟體主要都透過網路犯罪份子所創建之應用程序商店來散佈。

排名第五的惡意程式是多功能化的木馬程式，被歸類於 Plangton 這個家族。在這個程式安裝於手機後，會開始收集手機上的資料，並寄送至命令伺服器和等候網路犯罪份子的命令。特別是這支惡意程式可以偷偷地更改書籤和首頁。

5%的是 not-a-virus:RiskTool.AndroidOS.SMSreg，會讓使用者去誤用昂貴的服務，這個家族的惡意程式主要鎖定美國、荷蘭、英國和馬來西亞的使用者。

4%的是 Exploit.AndroidOS.Lotoor 這個家族。為了獲得裝置的控制權，網路犯罪份子需要進行越獄，這隻惡意軟體會獲得使用者的權限，提供無限制的操作於系統上。

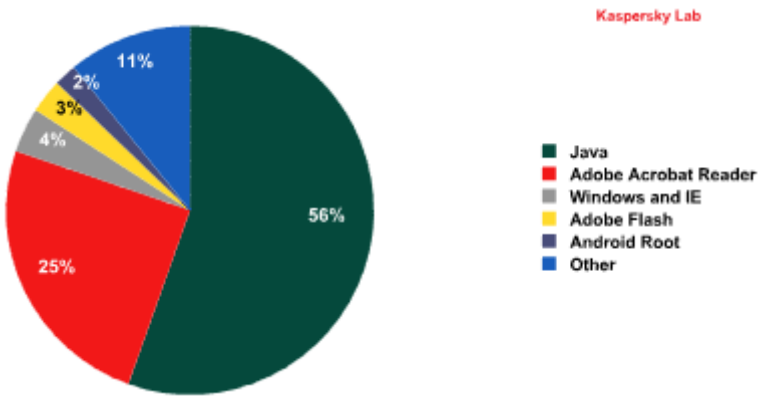
各種廣告程式被檢測為廣告軟體，也佔 4%在手機惡意軟體。其中最流行的屬於 Hamob 這個家族，他會在應用程式裡顯示廣告。

總結地說，網路犯罪份子在第三季最常見是針對 2.3.6 和 4.0.4 這兩種版本。攻擊者繞過安裝軟體來自於不受信任來源的限制，主要是利用良好的社交工程。在一般環境，使用多種方法從手機帳戶來竊取金錢的木馬程式是最普遍的，儘管它們已經逐漸被更先進的多功能木馬程式所取代。

漏洞攻擊(Exploit)：Java 漏洞的使用已經占所有攻擊的一半以上

網路攻擊主要透過各種漏洞攻擊來讓攻擊者可以下載惡意軟體到受害者的電腦，通常採取路過式下載的方式而不需要社交工程。漏洞攻擊成功的關鍵在於使用者機器上流行使用的應用程式所存在的漏洞。

這個圖顯示出何種應用程式的漏洞被鎖定利用在第三季。



應用程式漏洞被利用的比例，2012 年第三季

Java 漏洞在所有的攻擊中被拿來利用超過 50%。根據 Oracle，不同版本的虛擬機器安裝在電腦上的數量超過 11 億台。重要的是，軟體的更新是採用詢問需求而不是自動更新，這會增加漏洞的生存時間。Java 漏洞是可以輕易地使用在 Windows 版本，網路犯罪份子也會做額外的動作，如在 Flashfake 的案件中，跨版本的漏洞被創造出來。這也解釋了網路犯罪的特殊利益在 Java 的漏洞上，自然地，大部分都會檢測到各種的攻擊包。

在第三季中，網路犯罪份子所使用的數種漏洞被發現。CVE-2012-1723 被發現於 7 月，是利用一個在 HotSpot 組件上的錯誤，讓攻擊者可以執行這個模組，繞過 Java 虛擬機器的沙盒。CVE-2012-4681 發現於 8 月，這個漏洞一開始是被用來進行針對性攻擊，但是很快地被包含在流行的攻擊包裡面。

透過 Adobe Reader 進行攻擊排名第二。Adobe Reader 的漏洞普及率逐漸下降的原因是一個簡單的機制可以確保進行檢測，以及使用自動更新於最新版本。

針對在 Windows Help 以及支援中心，和各種版本的 IE 瀏覽器上的漏洞占 3%。特別是一個新的漏洞 CVE-2012-1876 被發現在 IE 版本 6~9。容易受攻擊的瀏覽器不能正確處理記憶體中的物件，它允許遠端攻擊者試圖訪問一個不存在的物件，從而導致緩衝區溢位。奇怪的是，這個漏洞有在 2012 年 3 月 CanSecWest 會議的 Pwn2Own 大賽上被使用過。

我們建議使用者應該更新那些熱門的程式，因為他們會釋放出更新檔來保護那些

漏洞攻擊，企業也應該要使用更新檔管理技術。

網絡間諜活動：Gauss、Madi 和其他惡意軟體

Q3 觀察到大量的間諜相關活動的事件。最重要的是 Madi、Gauss 和 Flame 惡意軟體，主要分佈在中東的活動。

一個進行滲透電腦系統的相關活動持續將近一年，目標使用者主要是在伊朗、以色列和阿富汗。我們與我們的合作夥伴，以色列一家名為 Seculert 的公司，聯合進行該惡意軟件的詳細研究。Madi 這個惡意程式是使用字串和識別字為基礎，這個惡意組件透過攻擊者使用簡單且常見的技術散佈，這表明受害者在網際網路的安全意識有很多地方需要改進。

這些攻擊會在 Delphi 的受害者電腦上安裝後門程式，這些惡意程式可能是由業餘的程式人員或是專業的開發者在短時間內所創造。該活動的目標在中東極為重要的基礎設施公司、政府機構、銀行和大學。這些被選擇的組織其通訊長時間一直被密切監視。

Gauss 惡意軟體在發現 Flame 惡意軟體的過程中被發現於一個由國際電訊聯盟（ITU）所發起的調查。從本質上講，Gauss 是一個民族國家所主持的“銀行”木馬程式，會偷竊受感染 Windows 機器上的各種資料，它所包含的惡意載體是加密的，其目的是不清楚的。Gauss 是基於 Flame 平台並且一些特徵是與 Flame 共有，像是會感染 USB 驅動程序的排程。

我們的專家也能從 Flame 的命令與控制(C&C)伺服器獲得新的資訊。卡巴斯基實驗室的專家進行一項研究，與我們的合作夥伴 - 賽門鐵克、ITU-IMPACT 和 CERT-Bund/BS - 使我們能夠做出一些重要的結論。首先， C&C 伺服器平台上的程式碼開發，早在 2006 年 12 月就開始。在原始碼中所留下的註解可知，該計畫至少有四個開發者，C&C 程式碼支援三種通訊協議。一個重要發現是，它進行請求處理的 4 個惡意程式，其程式名稱是由 SP、SPE、FL 和 IP 這四個作者為命名。

在這四個惡意程式中，只有兩個是當時所知道的：Flame 和 SPE (又名 miniFlame)。

根據研究所收集到的資料，我們可以說，網路間諜的事件在將來不久還會繼續。

統計

網路威脅

本節中的統計資料是來自於網絡的防毒解決方案，可以保護使用者盡快從被感染的網頁上傳惡意程式碼。感染來源可以找到於網頁中如允許使用者創建自己的內容（如論壇），即使是在合法的網頁已被駭客破壞。

檢測到的網路物件

在 2012 年第三季中，有 511,269,302 起攻擊事件被瓦解。這些事件來源都分佈於世界各地。在這些事件中，共有 165,732 件獨特修改過的惡意軟體和潛在的有害程序被檢測到。

前 20 件檢測到的惡意程序在網際網路上

Rank	Name*	% от всех атак**
1	% of all attacks**	90,70%
2	Trojan.Script.Generic	2,30%
3	Trojan.Script.Iframer	1,60%
4	Trojan-Downloader.SWF.Voleydaytor.h	0,40%
5	Trojan.Win32.Generic	0,40%
6	Exploit.Script.Blocker	0,30%
7	AdWare.Win32.IBryte.x	0,20%
8	Trojan-Downloader.JS.Iframe.cyq	0,20%
9	Exploit.Script.Generic	0,20%
10	Trojan-Downloader.JS.Agent.gsv	0,20%
11	Trojan-Downloader.JS.JScript.bp	0,20%
12	Hoax.HTML.FraudLoad.i	0,20%
13	Trojan-Downloader.Script.Generic	0,10%
14	Trojan.HTML.Redirector.am	0,10%
15	Trojan-Downloader.Win32.Generic	0,10%
16	Trojan-Downloader.JS.Iframe.czo	0,10%
17	AdWare.Win32.ScreenSaver.e	0,10%
18	Backdoor.MSIL.Agent.gtx	0,10%
19	Trojan.JS.Popupper.aw	0,10%
20	Exploit.Java.CVE-2012-4681.gen	0,10%

在本次排名中依然佔據第一名的是我們黑名單中的惡意 URL。他們觸發 90%的防毒警報，比前一季增加 5%。其中 4%的惡意 URL 被阻斷是因為即時的雲端運算更新，這些連結都是新的被遭到入侵的網站，或是新鮮的網路犯罪頁面。沒有安裝防毒軟體保護的使用者將面臨強迫下載攻擊當他們訪問這些頁面時。Trojan-Downloader.SWF.Voleydaytor.h 排名第三位，被檢測於各種成人內容的網站。雖然他自稱是影音播放程序的更新檔，實際上是提供各種惡意程式到使用者電腦上。

排在第七位是廣告程式 AdWare.Win32.IBryte.x，其傳播方式是當作一個流行免費軟體的下載器。一旦啟動，它會按使用者要求下載免費程式，同時安裝一個廣告軟體模組。它只是簡單的下載程式，需要從他們的官方網站刪除廣告軟體來節省麻煩。最近的一項研究表明，這種問題主要影響 IE 的使用者。

Hoax.HTML.FraudLoad.i（第 12 位）是有趣的。這種威脅主要影響的使用者是喜歡下載電影和軟體是免費的。從這個所檢測到的網頁，使用者聲稱可以下載內容，但首先需要發送一個已支付的訊息。使用者並沒有收到所需的文件，無論是 TXT 文件其中包含如何使用搜尋引擎的建議，或者是惡意程式。

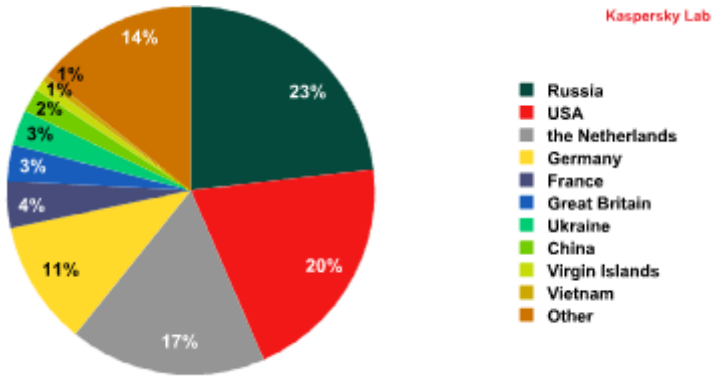
第 20 名是 Exploit.Java.CVE-2012-4681.gen，為 8 月下旬檢測到的一個漏洞攻擊，可以同時使用兩個 Java 漏洞。Java 的漏洞在網路犯罪份子是受歡迎的，因為設備安裝 Java 虛擬機器的數量在世界上超過 3 億台。

排名中的 12 個位置主要為惡意程式和提供木馬程序的組件結合使用攻擊受害者的電腦。

網路資源被惡意軟體感染的國家

這些圖案表示了含有惡意程式的網站其所在的實體位置，網頁攻擊的地理資源透過實際 IP 與域名的比較下被檢測出。

全球 10 個國家的網路資源用來傳播惡意軟體就佔總數的 86%。跟第二季比較，這個數字上升了 1%。



依國家所分網路資源帶有惡意程式的分佈圖，2012 年第三季

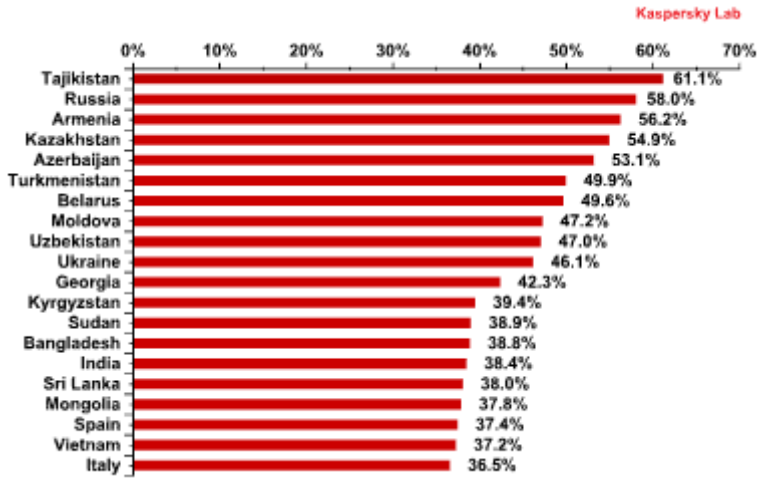
有一個新的指標性國家出現：俄羅斯已經超過美國。在過去的三個月中，惡意主機在俄羅斯的比例明顯增加(8.6%)，在同一時間點，美國的佔有率下降(-9.7%)，

可以反映出俄羅斯的崛起。荷蘭的惡意主機數量也有上升(5.8%)。60%的惡意主機就位於俄羅斯、美國和荷蘭三個國家。若執法機關和網路服務商不採取有效的行動，這種情形可能會維持數個月。

前 10 名的其他國家之間沒有顯著的變化，除了英國的佔有率下降 2.6%。

使用者透過網際網路受到感染最大風險的國家

針對特定的國家以評估使用者的感染風險，卡巴斯基實驗室計算網頁防毒檢測的頻率在不同的國家。



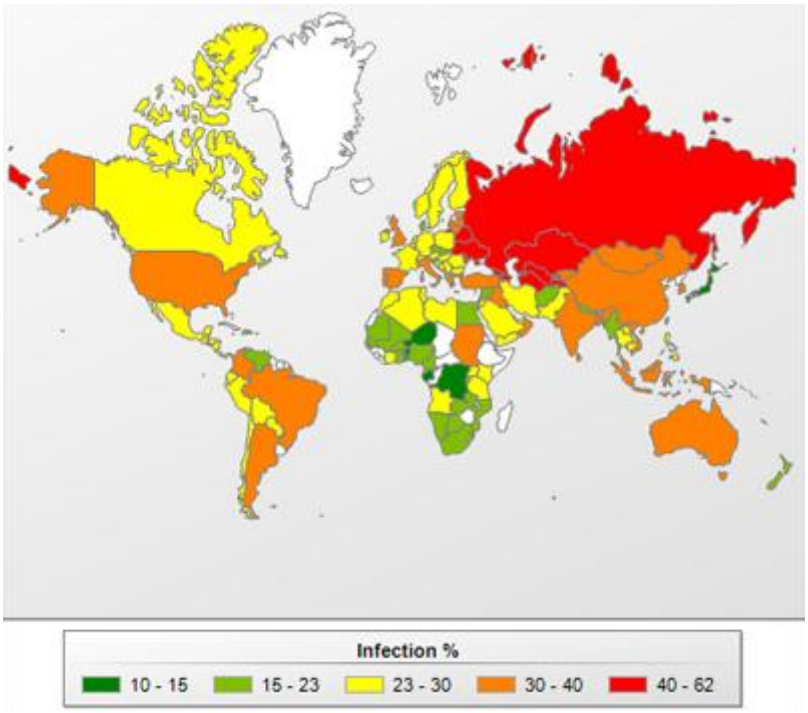
前 20 個國家受到網路感染的風險程度，2012 年第三季

在上一季中，排名前 20 位只包括前蘇聯、非洲和東南亞國家。這一次有兩個南歐國家出現名單上，即義大利(36.5%)和西班牙(37.4%)。

所有的國家可以分成四組

1. 最危險群的國家，其中超過60%的使用者至少一次在網路上遇到惡意軟體。第三季中，發現塔吉克(61.1%)在這個類別取代俄羅斯(58%)成為領導者。
2. 高危險群的國家，其中 41%至 60%的使用者在網路上至少有一次遇到惡意軟件。這組包括 TOP 20 內的 10 個國家，除了俄羅斯(58%)之外，該組包括哈薩克(54.9%)、白俄羅斯(49.6%)和烏克蘭(46.1%)。
3. 中度危險群(21-40%)，包括 99 個國家，有印度(38.4%)、西班牙(37.4%)、義大利(36.5%)、立陶宛(33.5%)、中國(33.4%)、土耳其(33.3%)、美國(32.4%)、巴西(32.9%)、英國(30.2%)、比利時(28.3%)和法國(28.2%)。
4. 低危險群包括 27 個國家，10.6%到 21%之間的使用者在網路上遇到惡意軟

件，最安全的是日本(13.6%)、丹麥(17.7%)、台灣(15.4%)、香港(19.3%)、盧森堡(19.7%)、斯洛伐克(20.7%)和新加坡(20.9%)。



受感染的風險程度於全世界，2012 年第三季

非洲國家是最安全的群組，但我們認為這些低風險的國家是因為其網際網路的使用率仍然落後所造成。

平均而言，在 2012 年第三季中，有 36.7%的卡巴斯基使用者的電腦被攻擊至少一次在網路上瀏覽。這樣的平均低於上一季 3%。

區域威脅

本節的報告包含一個統計分析是基於使用掃描器和掃描統計在不同磁碟上所獲得的資料。

在使用者的電腦上檢測到的惡意物件

在 2012 年第三季，卡巴斯基實驗室成功封鎖 882,545,490 筆嘗試感染本地端電腦的攻擊。

共有 328,804 筆獨特修改的惡意軟體和潛在有害程序被封鎖當它們常是想要啟動在使用者的電腦上。

前 20 名從使用者電腦檢測出的惡意物件

Rank	Name	%% of individual users*
1	Trojan.Win32.Generic	17,1%
2	DangerousObject.Multi.Generic	15,6%
3	Trojan.Win32.AutoRun.gen	14,5%
4	Trojan.Win32.Starter.yy	7,6%
5	Virus.Win32.Virut.ce	5,5%
6	Net-Worm.Win32.Kido.ih	4,8%
7	Virus.Win32.Sality.aa	3,9%
8	HiddenObject.Multi.Generic	3,9%
9	Virus.Win32.Generic	3,7%
10	Virus.Win32.Nimnul.a	3,2%
11	Trojan.WinLNK.Runner.bl	2,5%
12	Worm.Win32.AutoRun.hxw	1,8%
13	Virus.Win32.Sality.ag	1,5%
14	Trojan.Win32.Patched.dj	0,7%
15	Email-Worm.Win32.Runouce.b	0,5%
16	AdWare.Win32.BHO.awvu	0,4%
17	Trojan-Dropper.Script.Generic	0,4%
18	AdWare.Win32.GoonSearch.b	0,4%
19	Backdoor.Win64.Generic	0,3%
20	AdWare.Win32.RelevantKnowledge.a	0,3%

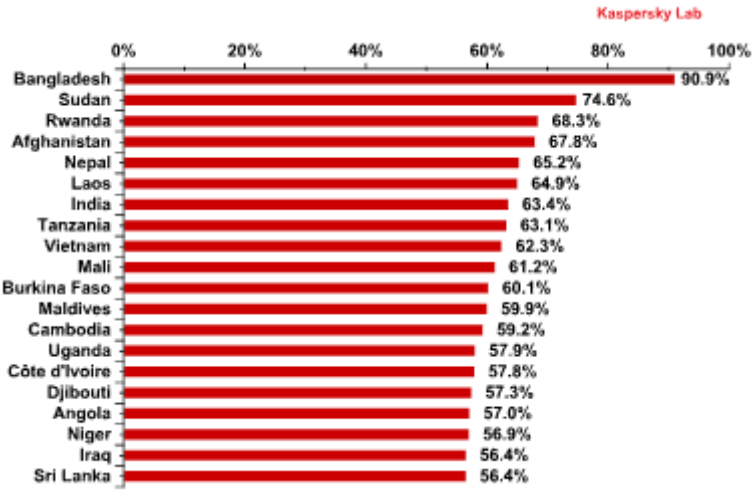
Trojan.Win32.Generic(17.1%)位於排名首位，這項判斷是由於啟發式的分析器會主動積極檢測各種惡意程式。

檢測到的惡意程式(DangerousObject.Multi.Generic，15.6%)由於有雲端計算技術的幫助下，也上移一個位置到第二名的位置。雲端技術在分析時，不採用簽名和啟發式的方法，而是立即能夠檢測到的惡意程式，但有關對象的資訊需要已經存在於雲端中。在本質上，這個惡意程式是最近所給出的判斷。

16 名、18 名和 20 名為廣告軟體程式。第三季偵測到的新種類，是惡意軟體家族 AdWare.Win32.RelevantKnowledge(0.3%)。屬於這個家族的程式整合到 Web 瀏覽器，並定期顯示一個使用者的查詢視窗。

使用者運行的國家最嚴重的局部感染的風險

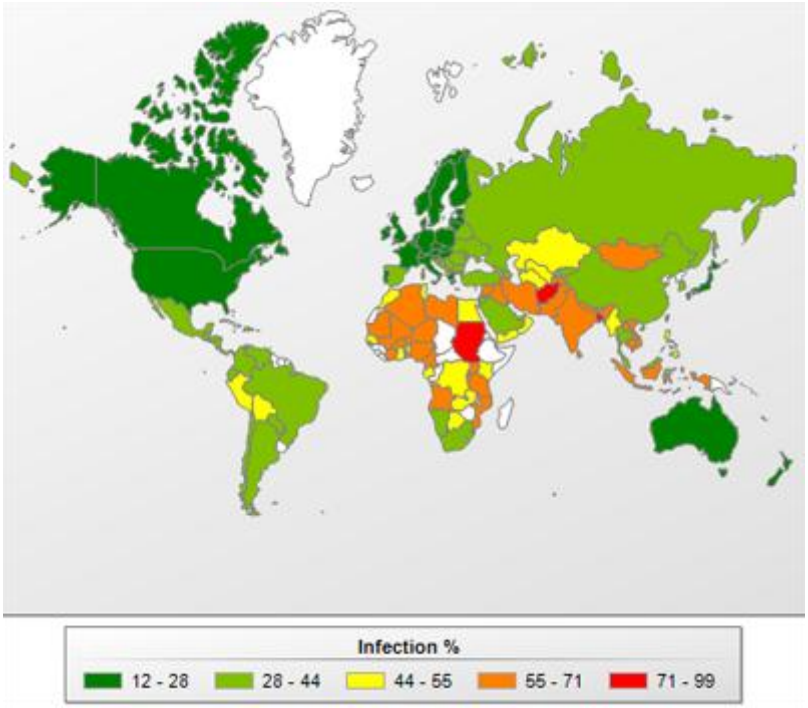
下圖顯示在不同國家電腦受感染的平均增長率，跟上一季比起來是減少 3.9%。



不同國家電腦受感染的程度，2012 年第三季

局部感染也可依感染程度分為不同的類別。

1. 最嚴重程度的局部感染(60%以上)：這群組現在擁有至少 9 個國家和包括 11 個亞洲國家(印度，越南，尼泊爾等)，中東國家(阿富汗)和非洲(蘇丹、馬利、坦尚尼亞等)。
2. 高程度的局部感染(41-60%)：39 個國家，包括印尼(53.5%)、埃及(46%)、泰國(42.3%)、中國(41.4%)和菲律賓(44.3%)。
3. 局部感染（21-40%）為中度程度的 56 個國家，包括土耳其、墨西哥、以色列、拉脫維亞、葡萄牙、義大利、俄羅斯和西班牙。
4. 局部感染為最低程度(21%)：包括 31 個國家，有美國、澳大利亞、加拿大、紐西蘭、波多黎各，19 個歐洲國家(包括挪威、愛沙尼亞和法國)和兩個亞洲國家日本和香港。



局部感染的危險程度於世界各地，2012 年第三季

使用者所面臨風險最低的局部感染前 10 個國家分別為：

Rank	Country	% of unique users
1	Denmark	10,5
2	Japan	10,6
3	Luxembourg	13,8
4	Switzerland	14,3
5	Sweden	14,7
6	Germany	15
7	Finland	15,1
8	Netherlands	15,1
9	Czech Republic	15,2
10	Ireland	15,5

愛爾蘭是新加入的成員於這個群組內。

漏洞

在 2012 年第 3 季，共 30,749,066 個有漏洞的程式和檔案被檢測出 - 平均每個受影響的電腦上有 8 個不同的漏洞。

下表中列出前 10 大的漏洞。

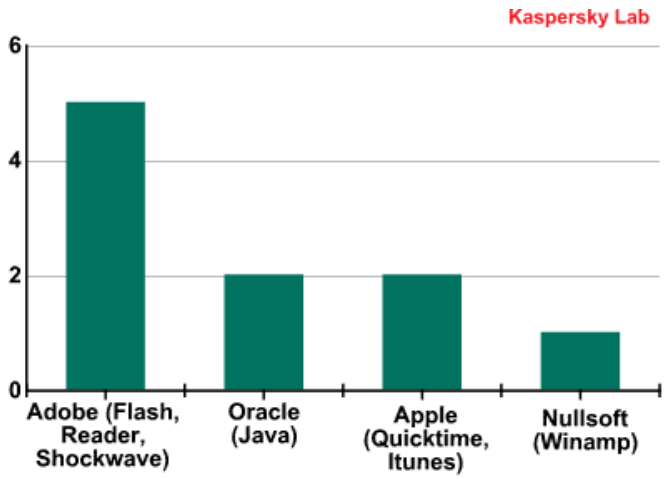
№	Secunia ID – Unique vulnerability number	Vulnerability name and link to description	What the vulnerability lets malicious users do	Percentage of users on whose computers the vulnerability was detected*	Date of latest change	Rating
1	SA 49472	Oracle Java Multiple Vulnerabilities	DoS-attack Gain access to a system and execute arbitrary code with local user privileges Cross-Site Scripting Gain access to sensitive data Manipulate data	35,00%	20.08.2012	Highly Critical
2	SA 50133	Oracle Java Three Vulnerabilities	Gain access to a system and execute arbitrary code with local user privileges	21,70%	31.08.2012	Extremely Critical
3	SA 50354	Adobe Flash Player Multiple Vulnerabilities	Gain access to a system and execute arbitrary code with local user privileges Gain access to sensitive data	19,00%	25.09.2012	Highly Critical
4	SA 49388	Adobe Flash Player Multiple Vulnerabilities	Gain access to a system and execute arbitrary code with local user privileges Bypass security systems	18,80%	18.06.2012	Highly Critical
5	SA 47133	Adobe Reader/Acrobat Multiple Vulnerabilities	Gain access to a system and execute arbitrary code with local user privileges	14,70%	11.01.2012	Extremely Critical

6	SA 47447	Apple QuickTime Multiple Vulnerabilities	Gain access to a system and execute arbitrary code with local user privileges	13,80%	23.08.2012	Highly Critical
7	SA 49489	Apple iTunes Multiple Vulnerabilities	Gain access to a system and execute arbitrary code with local user privileges	11,70%	10.07.2012	Highly Critical
8	SA 46624	Winamp AVI / IT File Processing Vulnerabilities	Gain access to a system and execute arbitrary code with local user privileges	10,90%	03.08.2012	Highly Critical
9	SA 50283	Adobe Shockwave Player Multiple Vulnerabilities	Gain access to a system and execute arbitrary code with local user privileges	10,80%	14.08.2012	Highly Critical
10	SA 41917	Adobe Flash Player Multiple Vulnerabilities	Gain access to a system and execute arbitrary code with local user privileges Bypass security systems Gain access to sensitive data	9,70%	09.11.2010	Extremely Critical

前兩名是 Oracle Java 上的漏洞，分別佔 35%和 21.7%。

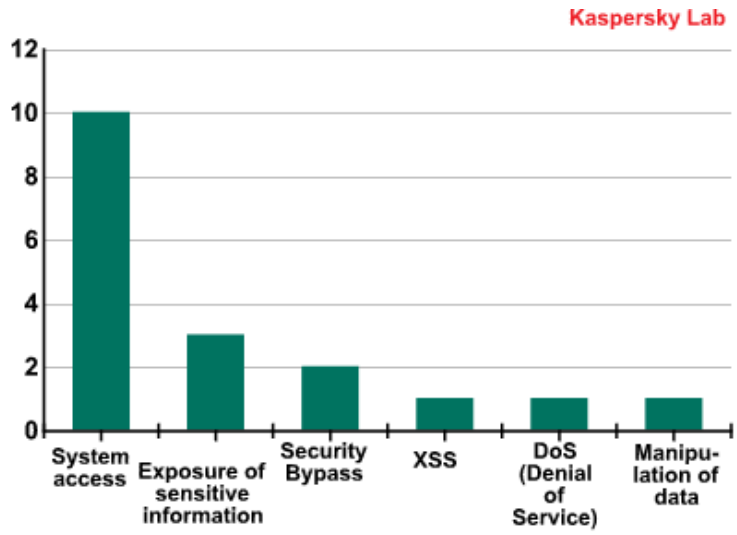
五種常見的漏洞影響 Adobe 產品：Flash 播放器、Shockwave 播放器和閱讀器，為一個流行的 PDF 文件閱讀器。

該排名還包括兩個蘋果程式 - QuickTime 播放器和 iTunes 以及流行的 Nullsoft 的 Winamp 媒體播放器。



前 10 個漏洞所擁有的產品供應商，2012 年第三季

排名前 10 的漏洞都有可能會危害電腦安全，因為它們都允許網路罪犯份子利用漏洞獲得完全系統控制權。在第二季，有三個漏洞使得攻擊者能進行訪問以獲取敏感資料。兩個 Flash Player 的漏洞允許網路犯罪份子繞過安全機制整合到應用程式。排名前 10 的漏洞也能使攻擊者操作資料和進行 DDoS 攻擊及 XSS 攻擊。



微軟的產品不再出現於前 10 名的產品漏洞中，這是因為自動更新的機制，現在已經得到很好的發展在最近版本的 Windows 作業系統。