



香港保安觀察報告

**2014** 年第二季度

# 前言

---

## 認知保安狀況 提高網絡安全

現今，有很多「隱形」電腦，在使用者還不知道的情況下，被攻擊者入侵及控制。在這些電腦上的數據可能每天都被盜取及暴露，並用於不同種類的犯罪活動上。

香港保安觀察報告旨在提高公眾對香港被入侵電腦狀況的「能見度」，以便他們可以做得更好資訊保安的決策。

報告提供在香港被發現曾經遭受或參與各類型網絡攻擊活動的電腦的數據，包括網頁塗改，釣魚網站，惡意程式寄存，殭屍網絡控制中心(C&C)或殭屍電腦等。香港的電腦的定義，是處於香港網絡內，或其主機名稱的頂級域名是「.hk」或「.香港」的電腦。

## 善用全球資訊的力量

本報告是 HKCERT 和全球各地的資訊保安研究人員協作的成果。很多資訊保安研究人員具有能力去偵測針對他們或其客戶的攻擊，有些會把錄得的攻擊來源的可疑 IP 地址或惡意活動網絡連結的數據提供給其他資訊保安機構，目的是改善互聯網的整體安全。他們有良好的實務守則，在分享數據之前刪除個人身份的數據。

HKCERT 建立 Information Feed Analysis System (IFAS) 系統，收集和匯聚這些寶貴的數據，對有關香港的資料進行分析。數據的來源 (附錄 1) 非常分散及可靠，可以持平地反映香港的資訊保安情況。

我們會移除來自多個數據來源的重複報告，並以下面的統計指標來確保統計數據的質量：

網絡攻擊類型	統計指標
網頁塗改、釣魚網站、惡意程式寄存	在本報告所述期間，錄得有關的唯一網址的數量
殭屍網絡控制中心 (C&C)	在本報告所述期間，錄得有關的唯一 IP 地址的數量
殭屍電腦	在本報告所述期間，錄得各個殭屍網絡在季度內的同日唯一 IP 地址數量的最高值的總和。

## 更好的資訊，更好的服務

我們將來會加入更多的有價值的數據來源和進行更深入的分析，持續改善這報告。我們亦會探討如何利用這些數據改進我們的服務。請以電郵 ([hkcert@hkcert.org](mailto:hkcert@hkcert.org)) 給我們你的反饋意見。

### 報告的局限

本報告的數據有不同的來源，他們採用不同的收集方法、收集週期、表達方式和有各自的局限，因此數據宜作參考之用，不宜用於直接比較或視為反映現實的全貌。

### 免責聲明

本中心可隨時更新或修正報告，恕不另行通知。對於本報告內容及數據中出現的任何錯誤、偏頗、疏漏或延誤，或據此而採取之任何行動，本中心概不負上任何責任。對於因使用本報告內容及數據而產生的任何特殊的、附帶或相應的損失，本中心概不負上任何責任。

### 授權條款

本報告是採用創用 CC 姓名標示 4.0 國際 授權條款。任何人只要表明來源始於 HKCERT，均可以合法共享本報告的內容，制作衍生的內容，作任何用途。

<http://creativecommons.org/licenses/by/4.0/>



# 目錄

---

報告概要.....	4
詳細數據.....	10
1.    網頁塗改.....	10
1.1    數據統計.....	10
2.    釣魚網站.....	12
2.1    數據統計.....	12
3.    惡意程式寄存.....	14
3.1    數據統計.....	14
4.    殭屍網絡.....	16
4.1    殭屍網絡控制中心(C&C).....	16
4.2    殭屍電腦.....	17
附錄.....	19
附錄 1 –資料來源.....	19
附錄 2 –地理位置識別方法.....	19
附錄 3 –主要殭屍網絡.....	20

# 報告概要

本報告是 2014 年第二季季度報告。

有關香港的唯一的網絡攻擊數據共有 16,589 個。數據經 IFAS<sup>1</sup>系統由 19 個來源<sup>2</sup>收集。它們並不是來自 HKCERT 所收到的事故報告。

## 安全事故趨勢

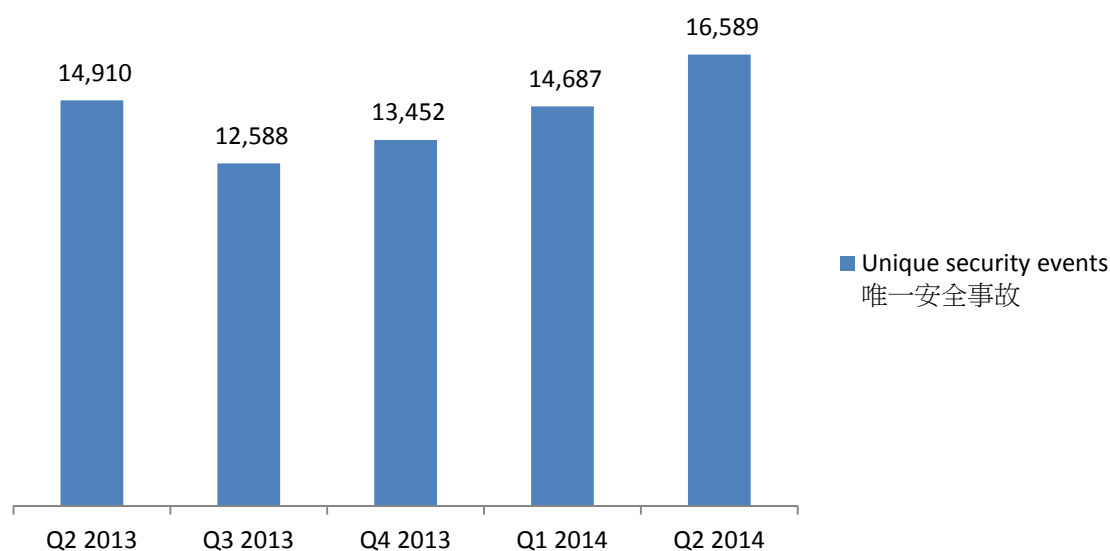


圖 1-安全事件趨勢<sup>3</sup>

本季度安全事件的總數比上季有所增加，持續了由 2013 年第三季開始的升勢。

<sup>1</sup> IFAS - Information Feed Analysis System(IFAS) 是 HKCERT 建立的系統，用作收集有關香港的環球保安資訊來源中有關香港的保安數據作分析之用

<sup>2</sup> 參照附錄 1 -資料來源

<sup>3</sup> 數字曾被調整以排除未被確定的網頁塗改事件

## 與伺服器有關的安全事件

與伺服器有關的安全事件有：惡意程式寄存、釣魚網站和網頁塗改。以下為其趨勢和分佈：

### 與伺服器有關的安全事件的趨勢和分佈

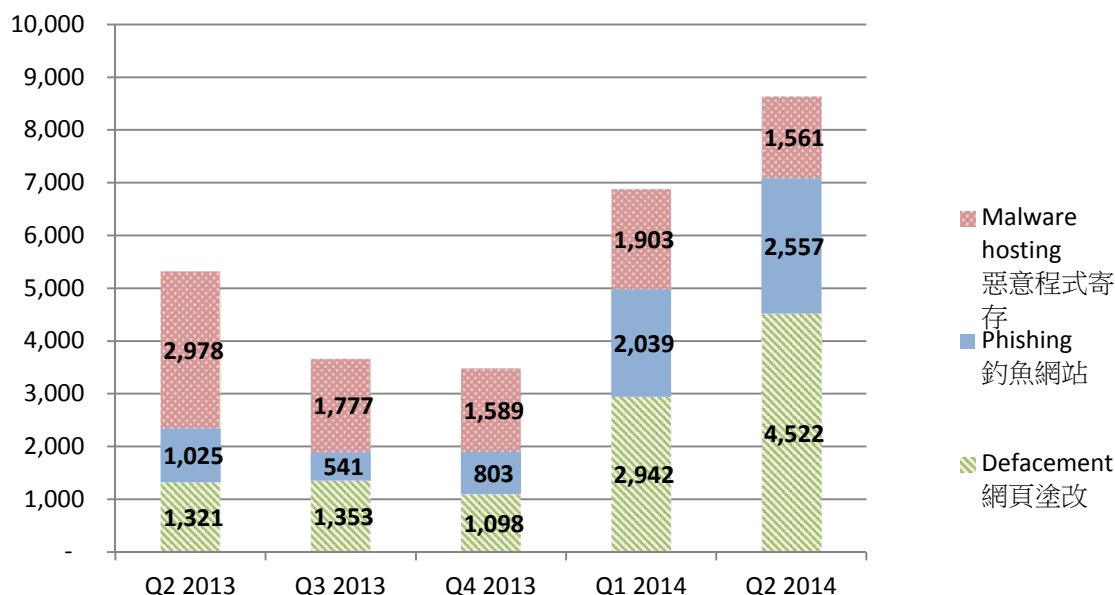


圖 2 -與伺服器有關的安全事件的趨勢和分佈<sup>4</sup>

有關伺服器的安全事件的數量在 2014 年第二季中度增加。

惡意程式寄存的數量在本季度下降了 18%，網頁塗改攻擊和釣魚網站攻擊的數量則分別上升了 54%和 25%。

本季的報告新增了網頁塗改、釣魚網站和惡意程式寄存安全事件唯一網址/IP 比的報告。與伺服器有關的安全事件數量以唯一網址來計算，這種計算方法並不能反映被入侵伺服器的數字，因為一台伺服器可以提供數以百計，甚至千計的唯一網址。例如在本季，其中一宗大型網頁塗改事件，其中一個 IP 地址便提供了 635 個唯一網址。新增的唯一網址/IP 比可以反映大型網頁塗改事件的數量，唯一網址/IP 比越高代表越多大型網頁塗改事件。

從 Zone-H 的數據 (圖 3)顯示，本季大約三分一的網頁塗改事件是被透過已知漏洞攻擊。這些漏洞可以透過安裝安全更新來移除。系統和應用程式管理員應在安全漏洞被利用前安裝最新的安全更新。

<sup>4</sup> 數字曾被調整以排除未被確定的網頁塗改事件

除此之外，有百分之十一的事件是透過社交工程<sup>5</sup>被攻擊。社交工程是透過欺詐誘使他人提供機密信息或做出某些行為。要避免跌入網絡罪犯的陷阱，網絡使用者必需提高信息安全意識。伺服器管理員，網站擁有者及其他相關人仕應該接受足夠的信息安全訓練。處理敏感資料或關鍵業務的伺服器應部署更多保護措施，例如職責分離，以減低個別員工造成的影響。

### 網頁塗改事件 - 主要攻擊向量

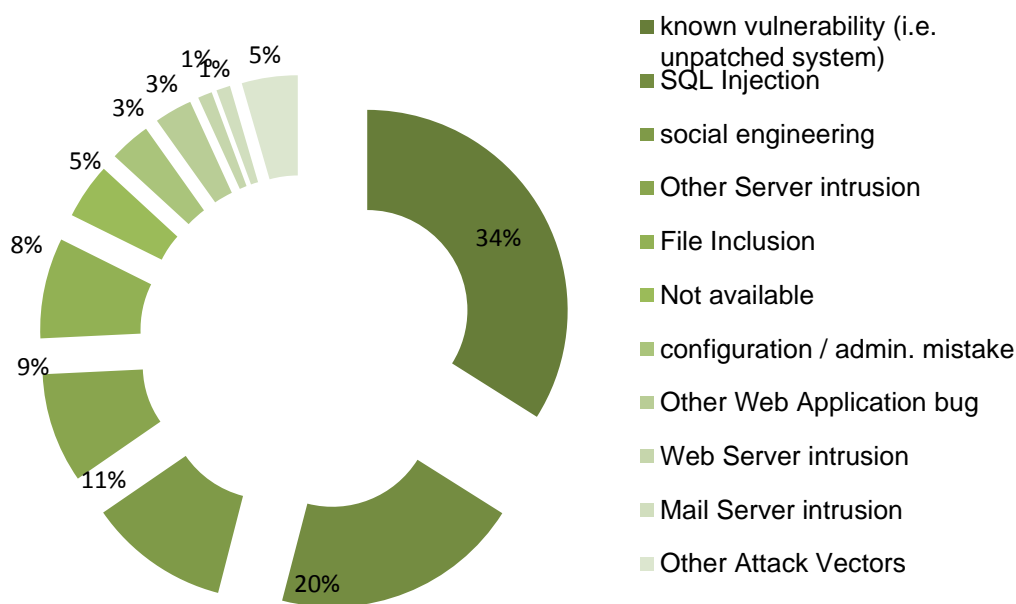



圖 3 - 主要攻擊向量



**HKCERT 促請系統和應用程式管理員保護好伺服器**

- 為伺服器安裝最新修補程式及更新，以避免已知漏洞被利用
- 更新網站應用程式和插件至最新版本
- 按照最佳實務守則來管理使用者帳戶和密碼
- 必須核實客戶在網上應用程式的輸入，及系統的輸出
- 在管理控制界面使用強認證，例如：雙重認證
- 獲取信息安全知識以防止社交工程

<sup>5</sup> <http://zh.wikipedia.org/wiki/%E7%A4%BE%E4%BC%9A%E5%B7%A5%E7%A8%8B%E5%AD%A6>

## 殭屍網絡相關的安全事件

殭屍網絡相關的安全事件可以分為兩類：

殭屍網絡控制中心(C&C) 安全事件 — 涉及少數擁有較強能力的電腦，向殭屍電腦發送指令。受影響的主要是伺服器。

殭屍電腦安全事件 — 涉及到大量的電腦，它們接收來自殭屍網絡控制中心(C&C) 的指令。受影響的主要是家用電腦。

### 殭屍網絡控制中心安全事件

以下將是殭屍網絡控制中心(C&C)安全事件的趨勢:

## 殭屍網絡控制中心(C&C)安全事件趨勢

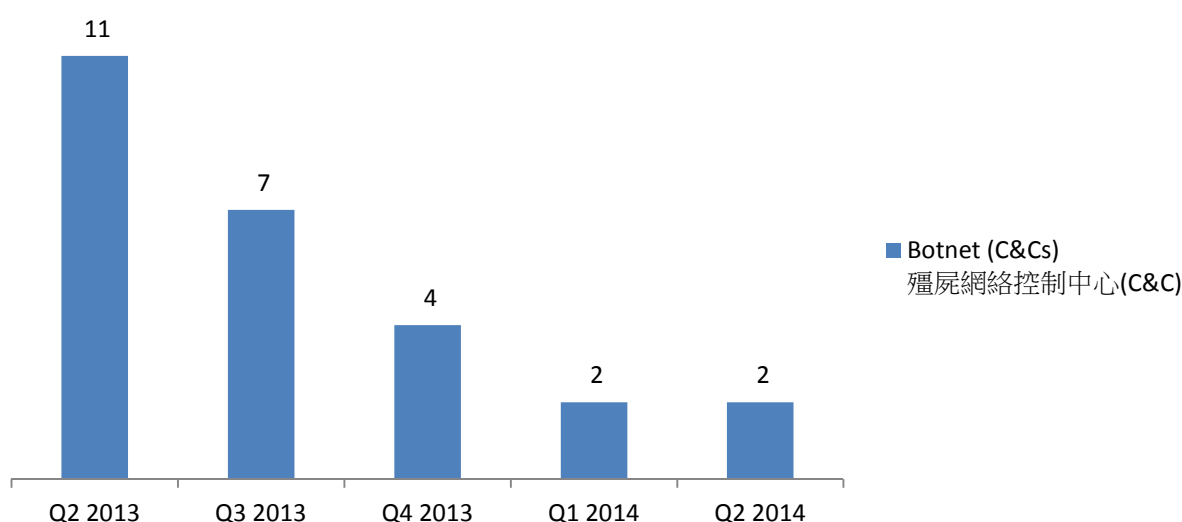


圖 4 –殭屍網絡控制中心(C&C)安全事件的趨勢

殭屍網絡控制中心的數字連續四個季度都有減少。

本季有 2 個殭屍網絡控制中心的報告。其中一個被確定為 Zeus 的殭屍網絡控制中心，另外一個是 IRC 殭屍網絡控制中心。

### 殭屍電腦安全事件

以下為殭屍電腦安全事件的趨勢:



## 殭屍網絡(殭屍電腦)安全事件趨勢

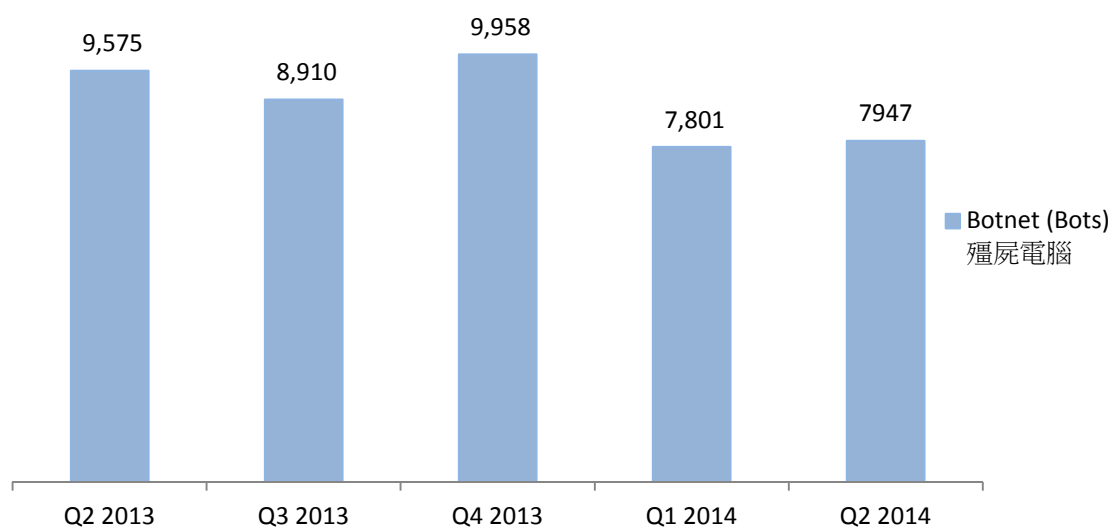


圖 5 -殭屍電腦安全事件的趨勢<sup>6</sup>

殭屍電腦安全事件在本季度有所減少。

在 2014 年第二季，香港的殭屍電腦感染的數字上升了 2%。十大殭屍網絡當中，七個的感染數目都出現下跌或保持平穩。

本季 Conficker 仍然是本港最大的殭屍網絡，一個研究<sup>7</sup>指出 Conficker 的感染數字持續高企是由於有一定數量的公司仍使用受 Conficker 威脅的 Windows XP。這反映香港網絡內 Windows XP 的數字仍然高企。

十大殭屍網絡當中，Zeus 的感染數字錄得最高增長 – 增加了 58%或 927 宗事件。Zeus 感染數字的增長是由於一個取締行動，令很多受害電腦的 IP 地址被發現。本年六月，美國執法者與其他國家的執法者及一些網絡安全公司採取了一個名為“Operation Tovar”的聯合行動。行動截取了殭屍電腦與犯罪份子伺服器之間的通訊，並把通訊重新導向到美國政府控制的 sinkhole<sup>8</sup>。聯邦調查局辨認受害電腦的 IP 地址後，把相關信息提供給世界各地的電腦保安事故協調中心，其中包括本中心 HKCERT。本中心已與有關機構合作處理受感染電腦。<sup>9</sup>

<sup>6</sup> 由於 Zeus 殭屍網絡的數字有更新，2013 年第四季度殭屍網絡(殭屍電腦)安全事件的數字有所調整

<sup>7</sup> <http://blog.trendmicro.com/trendlabs-security-intelligence/downad-tops-malware-spam-source-in-q2-2014/>

<sup>8</sup> <http://www.fbi.gov/news/stories/2014/june/gameover-zeus-botnet-disrupted>

<sup>9</sup> [https://www.hkcert.org/my\\_url/blog/14061302](https://www.hkcert.org/my_url/blog/14061302)

四月下旬，IFAS 首次錄得 Palevo 殭屍網絡的事件。該殭屍網絡迅速擴張，到五月已成為本港第四大的殭屍網絡，並持續至六月。Palevo 是一種透過即時通訊，點對點網絡及外置硬碟傳播的蠕蟲。它會在受害電腦開啟後門並竊取受害人的敏感資料。要防止 Palevo 繼續擴張，遇到可疑的連結及文件時不應打開。



HKCERT 促請使用者保護好電腦，免淪為殭屍網絡的一部分。

- 安裝最新修補程式及更新
- 安裝及使用有效的保安防護工具，並定期掃描
- 設定強密碼以防止密碼容易被破解
- 不要使用盜版的 Windows 系統，多媒體檔案及軟件
- 不要使用沒有安全更新的 Windows 系統及軟件

自 2013 年 6 月，本中心一直有跟進接收到的保安事件，並主動接觸本地互聯網供應商以清除殭屍網絡。現在殭屍網絡的清除行動仍在進行中，針對的是幾個主要的殭屍網絡家族，包括 Pushdo, Citadel, ZeroAccess 及 GameOverZeus。

本中心促請市民大眾參與殭屍網絡清除行動，確保自己的電腦沒有被惡意程式感染及控制。

為己為人，請保持網絡世界潔淨。



使用者可 HKCERT 提供的指引，偵測及清理殭屍網絡。

- 殭屍網絡偵測及清理指引  
<https://www.hkcert.org/botnet>

# 詳細數據

## 1. 網頁塗改

### 1.1 數據統計

#### 網頁塗改安全事件趨勢

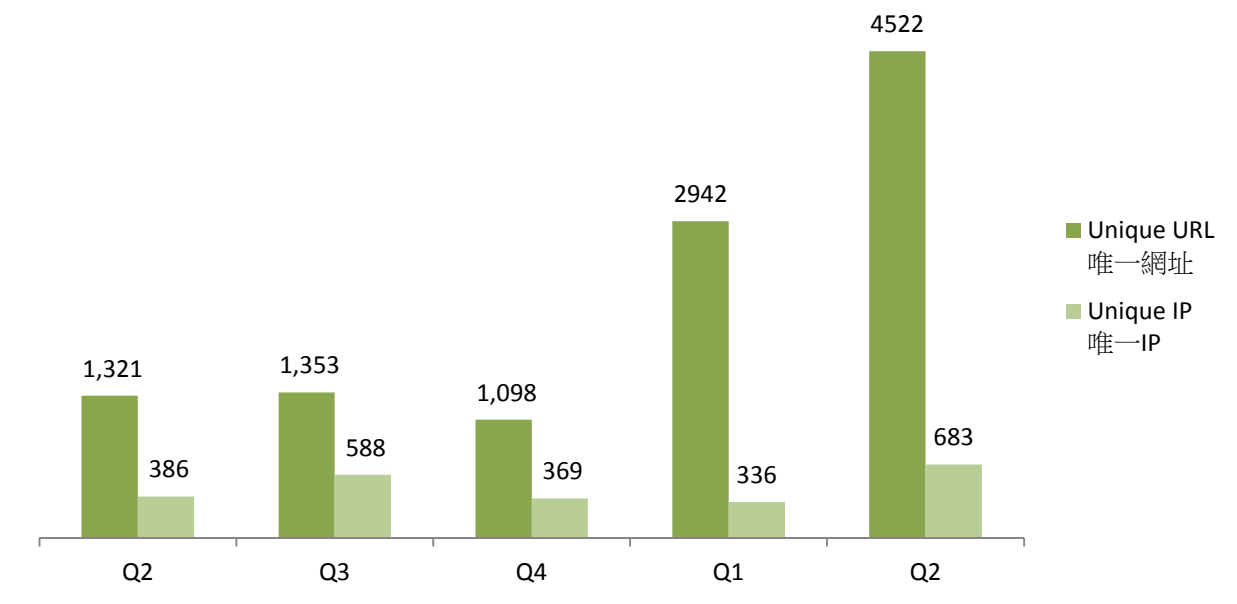


圖 6 – 網頁塗改安全事件趨勢<sup>10</sup>



#### 什麼是網頁塗改?

- 網頁塗改是在未經授權下，使用黑客攻擊方法去更改合法網站的內容。

#### 有什麼潛在影響?

- 網站內容的完整性被破壞
- 不能存取網站原來的內容
- 合法網站的擁有者的聲譽或受損害
- 伺服器上存儲處理的其他資訊亦有可能被黑客入侵，用作其他攻擊

<sup>10</sup>數字曾被調整以排除未被確定的網頁塗改事件

## 網頁塗改安全事件唯一網址/IP比

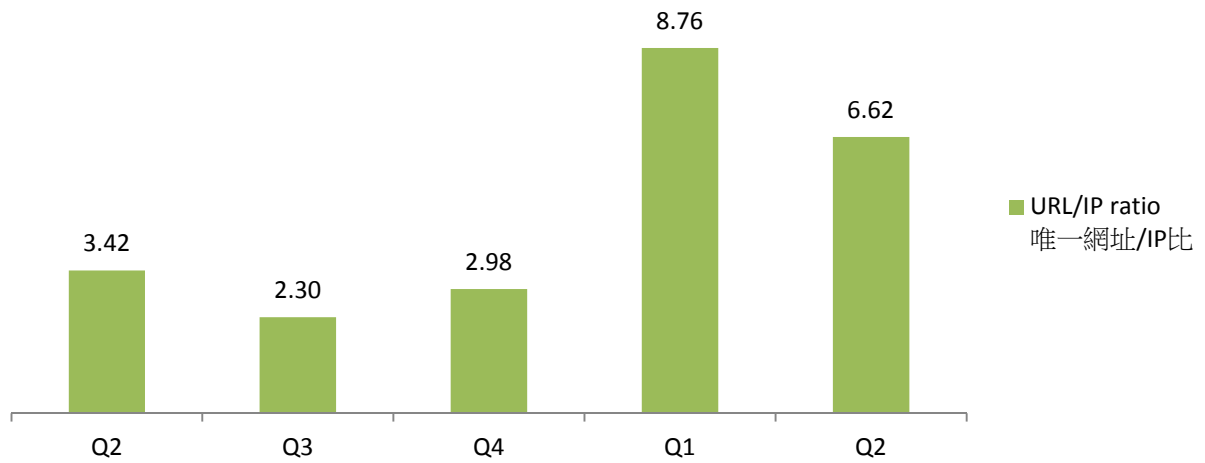


圖 7 - 網頁塗改安全事件唯一網址/IP 比



### 甚麼是唯一網址/IP 比？

- 它是以唯一網址計算的安全事件數量除以以 IP 地址計算的安全事件數量

### 這個比例能顯示甚麼？

- 以唯一網址計算的安全事件數量並不能反映被入侵伺服器的數量，因為一台伺服器可能提期很多唯一網址
- 以 IP 地址計算的安全事件數量能更能關聯被入侵伺服器的數量
- 這個比例越高，代表越多大型入侵事件

資料來源:

- Zone-H

## 2. 釣魚網站

### 2.1 數據統計

#### 釣魚網站安全事件趨勢

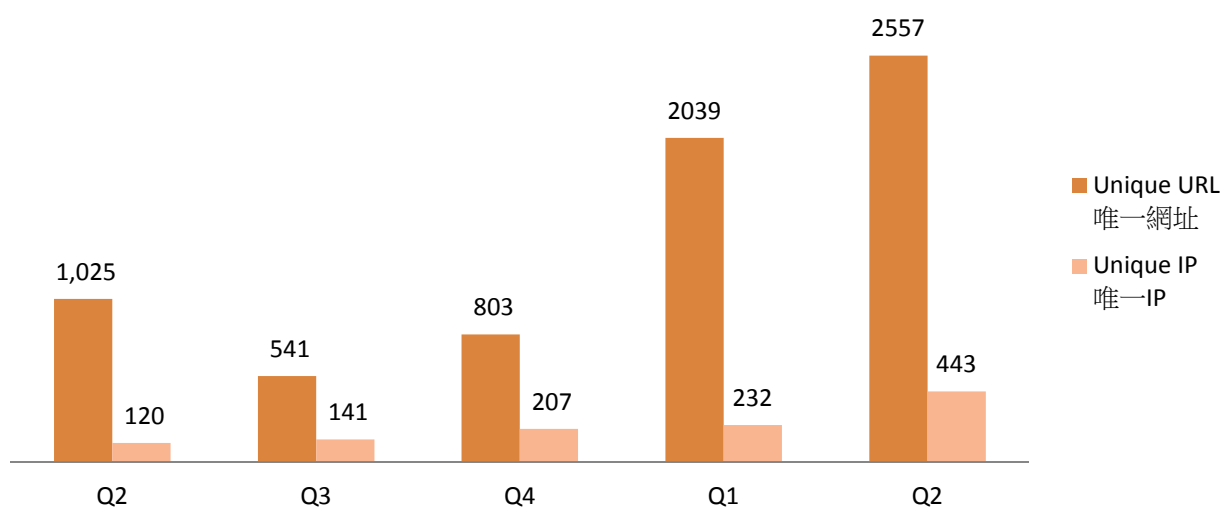


圖 8 - 釣魚網站安全事件趨勢



#### 什麼是釣魚網站?

- 釣魚網站是冒充一個合法網站，以達到詐騙的目的。

#### 有什麼潛在影響?

- 訪客的個人資料可能被盜取，導致金錢上的損失。
- 不能存取網站原來的內容
- 合法網站的擁有者的聲譽或受損害
- 伺服器可能被黑客進一步入侵，用作其他攻擊。

## 釣魚網站安全事件唯一網址/IP比

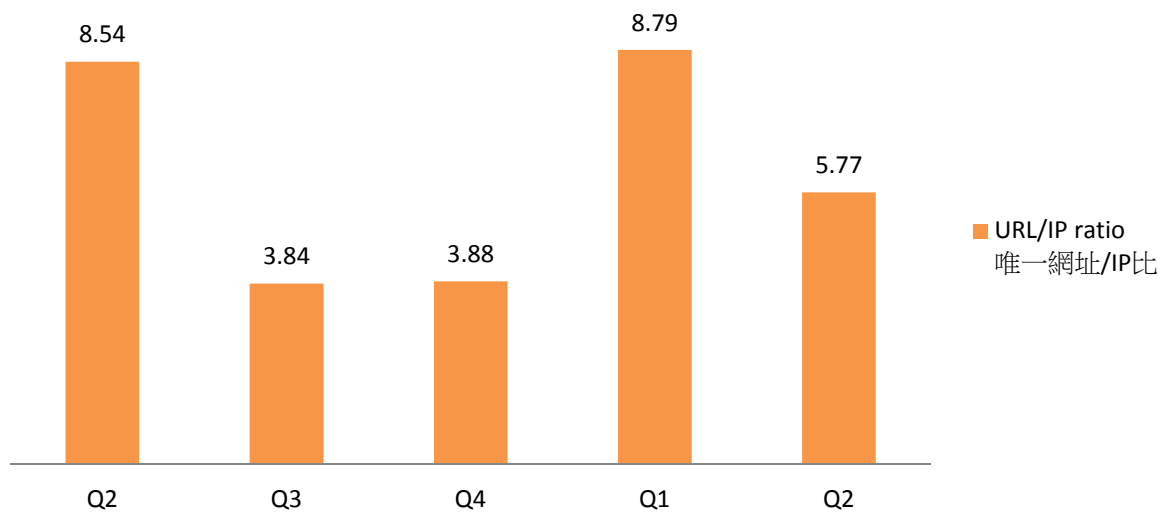


圖 9 - 釣魚網站安全事件唯一網址/IP 比



### 甚麼是唯一網址/IP 比？

- 它是以唯一網址計算的安全事件數量除以以 IP 地址計算的安全事件數量

### 這個比例能顯示甚麼？

- 以唯一網址計算的安全事件數量並不能反映被入侵伺服器的數量，因為一台伺服器可能提期很多唯一網址
- 以 IP 地址計算的安全事件數量能更能關聯被入侵伺服器的數量
- 這個比例越高，代表越多大型入侵事件

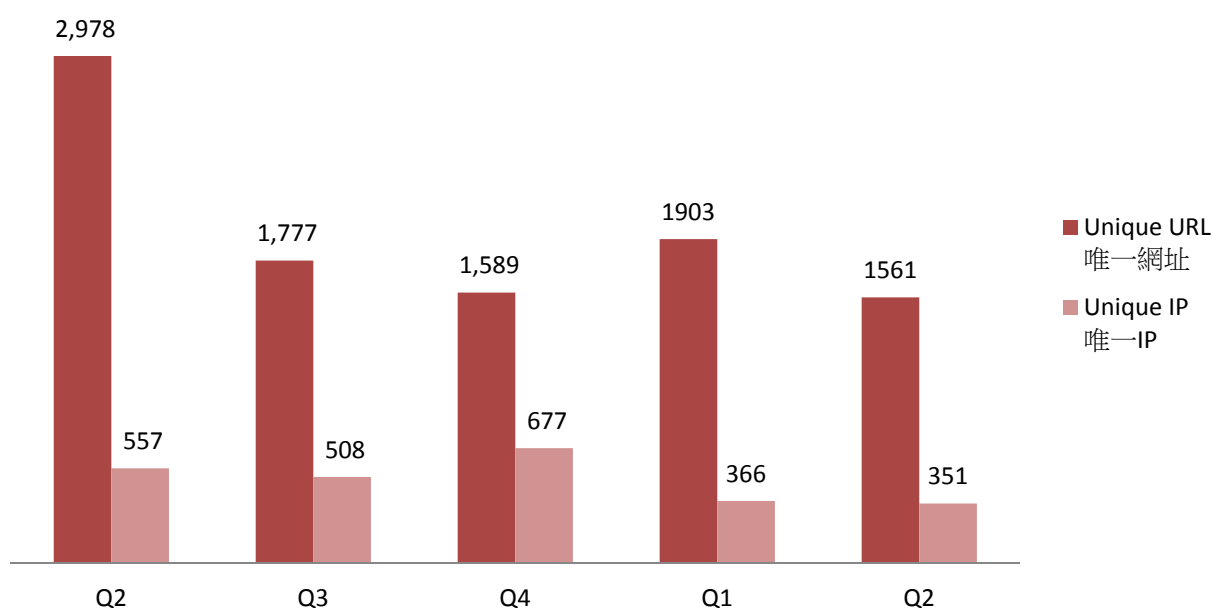
### 資料來源:

- ArborNetwork – Atlas SRF
- CleanMX – phishing
- Millersmiles
- Phishtank

### 3. 惡意程式寄存

#### 3.1 數據統計

#### 惡意程式寄存安全事件趨勢



2 圖 10 – 惡意程式寄存安全事件趨勢



#### 什麼是惡意程式寄存？

- 惡意程式寄存是透過網站散播惡意程式

#### 有什麼潛在影響？

- 訪客可能下載及安裝惡意程式，或執行網頁的惡意程式碼，導致被入侵。
- 不能存取網站原來的內容
- 網站的擁有者的聲譽或受損害
- 伺服器可能被黑客進一步入侵，用作其他攻擊。

## 惡意程式寄存安全事件唯一網址/IP比

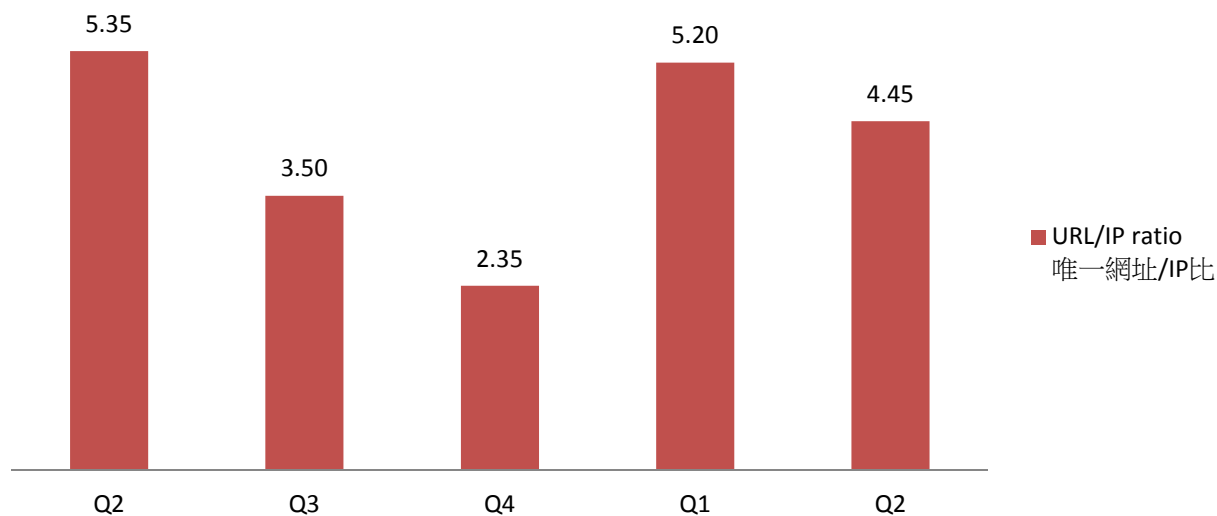


圖 11 – 惡意程式寄存安全事件唯一網址/IP 比



### 甚麼是唯一網址/IP 比？

- 它是以唯一網址計算的安全事件數量除以以 IP 地址計算的安全事件數量

### 這個比例能顯示甚麼？

- 以唯一網址計算的安全事件數量並不能反映被入侵伺服器的數量，因為一台伺服器可能提期很多唯一網址
- 以 IP 地址計算的安全事件數量能更能關聯被入侵伺服器的數量
- 這個比例越高，代表越多大型入侵事件

### 資料來源:

- Abuse.ch: Zeus Tracker – Binary URL
- Abuse.ch: SpyEye Tracker – Binary URL
- CleanMX – Malware
- Malc0de
- MalwareDomainList
- Sacour.cn



## 4. 殭屍網絡

### 4.1 殭屍網絡控制中心(C&C)

#### 殭屍網絡控制中心安全事件的趨勢和分佈

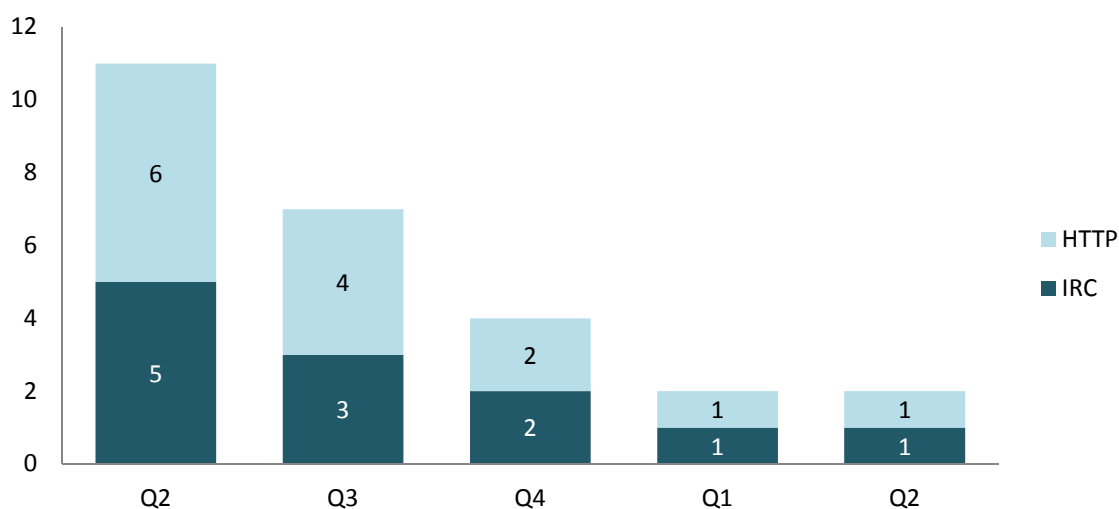


圖 12 – 殭屍網絡(控制中心)安全事件的趨勢和分佈



#### 什麼是殭屍網絡控制中心？

- 殭屍網絡控制中心是網絡罪犯用來控制殭屍電腦的伺服器，通過發送命令來遙控殭屍電腦執行惡意活動，例如竊取個人信息財務信息和分散式阻斷服務攻擊。

#### 有什麼潛在影響？

- 當很多殭屍電腦連接時，伺服器可能嚴重負荷。
- 伺服器可能收集到大量由殭屍電腦盜取的個人或財務數據。

資料來源：

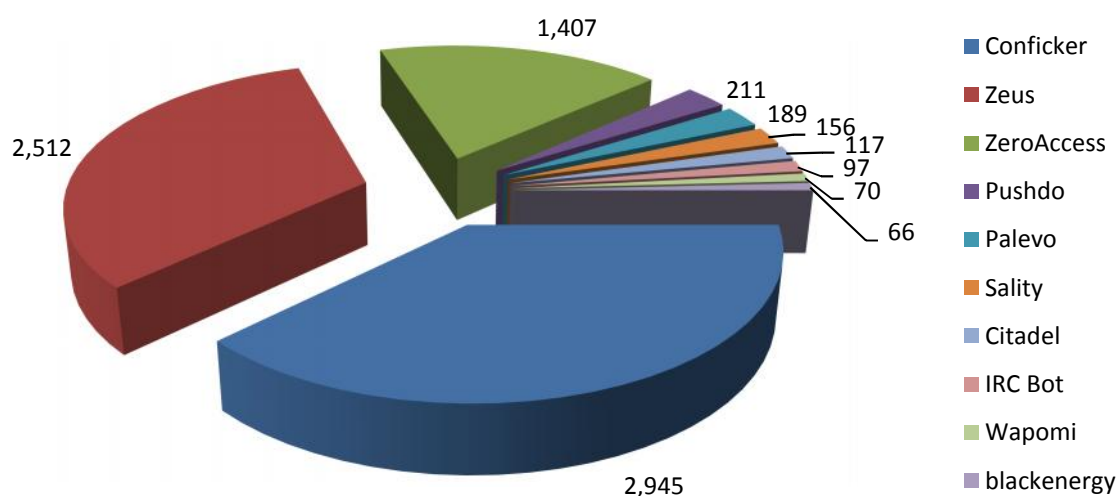
- Zeus Tracker
- SpyEye Tracker
- Palevo Tracker
- Shadowserver – C&Cs

## 4.2 殭屍電腦

### 4.2.1 香港網絡內的主要殭屍網絡<sup>11</sup>

殭屍網絡的規模是計算在報告時間內，每天嘗試連接到殭屍網絡的唯一 IP 地址的總數的最大值。換句話說，因為不是所有殭屍電腦都一定在同一天開機，殭屍網絡的真實規模應該比所見的數字更大。

香港網絡內的主要殭屍網絡



排名	↑↓	殭屍網絡名稱	唯一 IP 地址 (本季每天內最高數字)	變化
1	-	Conficker	2,945	1%
2	↑	Zeus	2,512	58%
3	↓	ZeroAccess	1,407	-26%
4	-	Pushdo	211	-69%
5	NEW	Palevo	189	NA
6	-	Sality	156	15%
7	↓	Citadel	117	-30%
8	↓	IRC Bot	97	-11%
9	↑	Wapomi	70	30%
10	↓	blackenergy	66	-6%

圖 13 – 香港網絡內的主要殭屍網絡的殭屍電腦數量

<sup>11</sup>主要殭屍網絡指殭屍網絡在報告時間內，透過資訊來源有可觀及持續穩定的數據。

## Trend of Top 5 Botnet Families in Hong Kong Network

### 五大主要殭屍網絡趨勢

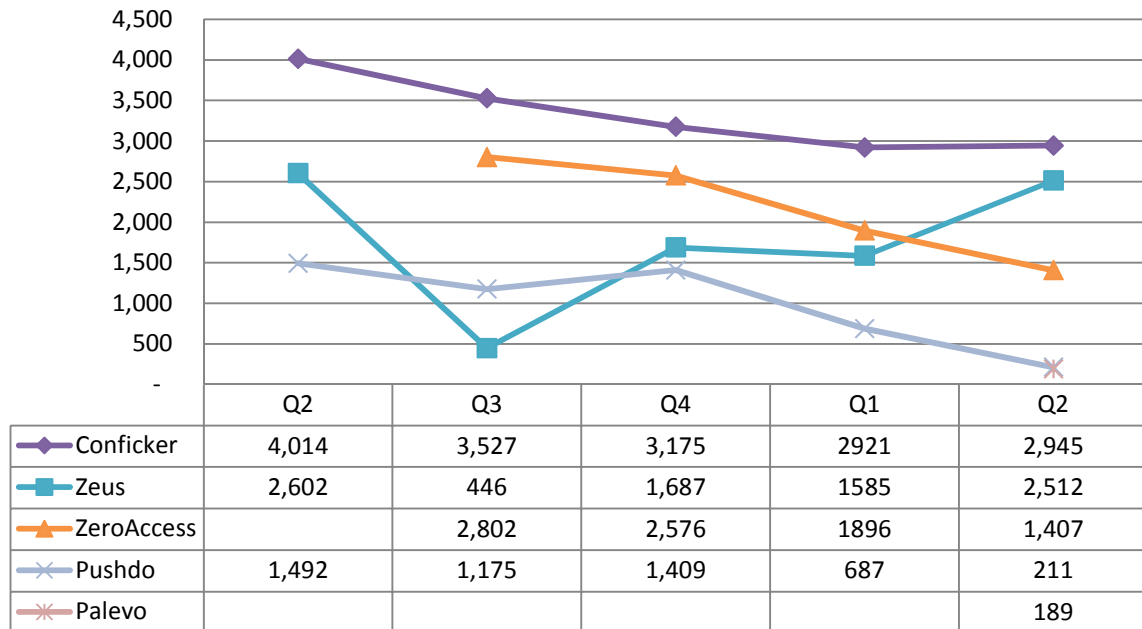


圖 14 –五大主要殭屍網絡趨勢

\*注意: 有關 ZeroAccess 的感染數據自 2013 年第三季才穩定, 因此未能與 2013 年第二季作直接比較。



#### 什麼是殭屍網絡?

- 殭屍網絡由一群殭屍電腦組成。殭屍電腦，大多數是一般的電腦，由於被惡意程式感染而成為殭屍電腦。當被感染後，惡意程式會用盡方法隱藏，並隱身連接到命令與控制服務器，得到黑客的指令，並進行攻擊。

#### 有什麼潛在影響？

- 伺服器資源被佔用，並使用於犯罪活動上。
- 盜取個人資料被及導致金錢上損失。
- 黑客的指令可能導致其他惡意活動，例如：散播惡意程式和進行分散式阻斷服務攻擊(DDoS)

資料來源:

- ArborNetwork – Atlas SRF – conficker
- ShadowServer – botnet\_drone
- ShadowServer – sinkhole\_http\_drone
- ShadowServer – Microsoft\_sinkhole

# 附錄

## 附錄 1 – 資料來源

以下是資料的來源:

網絡攻擊類別	資料來源	首次使用日期
網頁塗改	Zone -H	2013-04
釣魚網站	A rborNetwork: A tlas SRF-Phishing	2013-04
釣魚網站	C leanM X - Phishing	2013-04
釣魚網站	M illersm iles	2013-04
釣魚網站	Phish tank	2013-04
惡意程式寄存	A buse.ch: Zeus Tracker - B inary URL	2013-04
惡意程式寄存	A buse.ch: SpyEye Tracker - B inary URL	2013-04
惡意程式寄存	C leanM X - M alware	2013-04
惡意程式寄存	M alc0de	2013-04
惡意程式寄存	M alwareDom ainL ist	2013-04
惡意程式寄存	Sacour.cn	2013-04
殭屍網絡控制中心(C&C)	A buse.ch: Zeus Tracker - C&C s	2013-04
殭屍網絡控制中心(C&C)	A buse.ch: SpyEye Tracker - C&C s	2013-04
殭屍網絡控制中心(C&C)	A buse.ch: Palevo Tracker - C&C s	2013-04
殭屍網絡控制中心(C&C)	Shadow server-C&C s	2013-09
殭屍電腦	A rborNetwork: A tlas SRF - C onficker	2013-08
殭屍電腦	Shadow server- botnet_ drone	2013-08
殭屍電腦	Shadow server- sinkhole_ http_ drone	2013-08
殭屍電腦	Shadow server - m icrosoft_ sinkhole	2013-08

## 附錄 2 – 地理位置識別方法

我們採用以下方法去識別方網絡的地理位置是否香港。

方法名稱	最近更新日期
M axm ind	2013-10-29

### 附錄 3 – 主要殭屍網絡

主要殭屍網絡	別名	性質	感染方法	攻擊影響
BankPatch	<ul style="list-style-type: none"> <li>• MultiBanker</li> <li>• Patcher</li> <li>• BankPatcher</li> </ul>	針對網上銀行的木馬程式	<ul style="list-style-type: none"> <li>• 透過成人網站</li> <li>• 有問題的多媒體編解碼器</li> <li>• 垃圾電郵</li> <li>• 即時通訊系統</li> </ul>	<ul style="list-style-type: none"> <li>• 監視特定的銀行網站並竊取用戶密碼、信用卡資料及其他敏感財務數據</li> </ul>
BlackEnergy	無	DDoS 木馬程式	<ul style="list-style-type: none"> <li>• 以 rootkit 技術保持隱藏</li> <li>• 使用流程注入技術</li> <li>• 擁有強的加密技術和模塊化的架構</li> </ul>	<ul style="list-style-type: none"> <li>• 發動分散式阻斷服務攻擊(DDoS)</li> </ul>
Citadel	無	針對網上銀行的木馬程式	<ul style="list-style-type: none"> <li>• 逃避及停止安全檢測工具</li> </ul>	<ul style="list-style-type: none"> <li>• 竊取銀行登入認證資料及敏感資料</li> <li>• 按鍵記錄</li> <li>• 截圖擷取</li> <li>• 視訊擷取</li> <li>• 瀏覽器中間人攻擊</li> <li>• 勒索軟件</li> </ul>
Conficker	<ul style="list-style-type: none"> <li>• Dow nadup</li> <li>• Kido</li> </ul>	蠕蟲	<ul style="list-style-type: none"> <li>• 動態網域產生演算法(DGA)能力</li> <li>• 通過 P2P 網絡進行通訊</li> <li>• 停止安全檢測工具</li> </ul>	<ul style="list-style-type: none"> <li>• 利用 Window 伺服器服務漏洞(MS08-067)</li> <li>• 暴力破解管理員密碼，在網絡上傳播</li> <li>• 利用 Window 自動運行(auto-run)，透過外置磁碟機傳播</li> </ul>
Glupteba	Nil	木馬程式	<ul style="list-style-type: none"> <li>• 利用「路過式下載」(drive-by-download)感染系統</li> </ul>	<ul style="list-style-type: none"> <li>• 推送內容關聯廣告</li> <li>• 點擊劫持</li> </ul>
IRC Botnet	無	木馬程式	<ul style="list-style-type: none"> <li>• 通過 IRC 網絡進行通訊</li> </ul>	<ul style="list-style-type: none"> <li>• 後門程式，允許未經授權的存取</li> <li>• 發動分散式阻斷服務攻擊(DDoS)</li> <li>• 發送垃圾郵件</li> </ul>

Palevo	<ul style="list-style-type: none"> <li>• Rim ecud</li> <li>• Butterfly bot</li> <li>• Pilleuz</li> <li>• M ariposa</li> <li>• V aklik</li> </ul>	蠕蟲	<ul style="list-style-type: none"> <li>• 即時通訊系統, 點對點網絡及外置磁碟機</li> </ul>	<ul style="list-style-type: none"> <li>• 後門程式, 允許未經授權的存取</li> <li>• 竊取登入認證資料及敏感資料</li> <li>• 利用洗黑錢手法直接用銀行竊取金錢</li> </ul>
Pushdo	<ul style="list-style-type: none"> <li>• Cutw ail</li> <li>• Pandex</li> </ul>	下載器	<ul style="list-style-type: none"> <li>• 隱藏惡意網絡流量</li> <li>• 動態網域產生演算法 (DGA) 能力</li> <li>• 利用「路過式下載」(drive-by-down load)感染系統</li> <li>• 利用瀏覽器和插件漏洞</li> </ul>	<ul style="list-style-type: none"> <li>• 下載其他針對網上銀行的惡意程式(例如: Zeus 和 Spyeeye)</li> <li>• 發動分散式阻斷服務攻擊(DDoS)</li> <li>• 發送垃圾郵件</li> </ul>
Sality	無	木馬程式	<ul style="list-style-type: none"> <li>• 以 rookit 技術保持隱藏</li> <li>• 通過 P2P 網絡進行通訊</li> <li>• 透過外置磁碟機或共享傳播</li> <li>• 停止安全檢測工具</li> <li>• 使用多態性和遮蔽切入點 (Entry Point Obscuring) 技術來感染檔案</li> </ul>	<ul style="list-style-type: none"> <li>• 發送垃圾郵件</li> <li>• 通信代理</li> <li>• 竊取敏感資料</li> <li>• 感染網絡伺服器 and /或發佈計算任務來達到處理密集型任務目的 (例如: 破解密碼)</li> <li>• 下載其他惡意程式</li> </ul>
Slenfbot	無	蠕蟲	<ul style="list-style-type: none"> <li>• 透過外置磁碟機或共享傳播</li> </ul>	<ul style="list-style-type: none"> <li>• 後門程式, 允許未經授權的存取</li> <li>• 其他針對網上銀行的惡意程式</li> <li>• 發動分散式阻斷服務攻擊(DDoS)</li> <li>• 發送垃圾郵件</li> </ul>
Torpig	<ul style="list-style-type: none"> <li>• Sinow al</li> <li>• Anserin</li> </ul>	木馬程式	<ul style="list-style-type: none"> <li>• 以 rookit 技術保持隱藏 (M ebroot rookit)</li> <li>• 動態網域產生演算法 (DGA) 能力</li> <li>• 利用「路過式下載」(drive-by-down load)感染系統</li> </ul>	<ul style="list-style-type: none"> <li>• 竊取敏感資料</li> <li>• 瀏覽器中間人攻擊</li> </ul>

W apom i	N il	蠕蟲	<ul style="list-style-type: none"> <li>● 透過外置磁碟機或共享傳播</li> <li>● 感染可執行文件</li> </ul>	<ul style="list-style-type: none"> <li>● 後門程式，允許未經授權的存取</li> <li>● 下載其他惡意程式</li> <li>● 改動重要文件，導致系統不穩定</li> <li>● 收集電腦活動數據，竊取個人資料，並令降低電腦效能</li> </ul>
ZeroA ccess	<ul style="list-style-type: none"> <li>● m ax++</li> <li>● S irefef</li> </ul>	木馬程式	<ul style="list-style-type: none"> <li>● 以 rookit 技術保持隱藏</li> <li>● 通過 P2P 網絡進行通訊</li> <li>● 利用「路過式下載」(drive-by-dow n load)感染系統</li> <li>● 偽裝成有效檔案(例如：多媒體檔案，keygen)</li> </ul>	<ul style="list-style-type: none"> <li>● 下載其他惡意程式</li> <li>● 採礦比特幣和欺詐點擊</li> </ul>
Zeus	● G am eover	針對網上銀行的木馬程式	<ul style="list-style-type: none"> <li>● 隱身技術</li> <li>● 利用「路過式下載」(drive-by-dow n load)感染系統</li> <li>● 通過 P2P 網絡進行通訊</li> </ul>	<ul style="list-style-type: none"> <li>● 竊取銀行登入認證資料及敏感資料</li> <li>● 瀏覽器中間人攻擊</li> <li>● 按鍵記錄</li> <li>● 下載其他惡意程式(例如：Cryptolocker)</li> <li>● 發動分散式阻斷服務攻擊(DDoS)</li> </ul>