香港保安觀察報告

2019 第一季度

前言

認知保安狀況提高網絡安全

現今，有很多「隱形」系統（電腦及其他設備）在使用者不知情下被攻擊者入侵及控制。在這些系統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系統狀況的「能見度」，以便他們可以做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系統的數據，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。香港的系統的定義，是處於香港網絡內，或其主機名稱的頂級域名是「.hk」或「. 香港」的系統。

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：

Table 1: 網絡攻擊類型

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***）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

Contents

[1]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。

報告概要

本報告是 2019 第一季度報告。
在 2019 第一季度，有關香港的唯一的網絡攻擊數據共有 80,266 個。數據經 IFAS[2]系統由 13 個來源收集。它們並不是來自 HKCERT 所收到的事故報告。

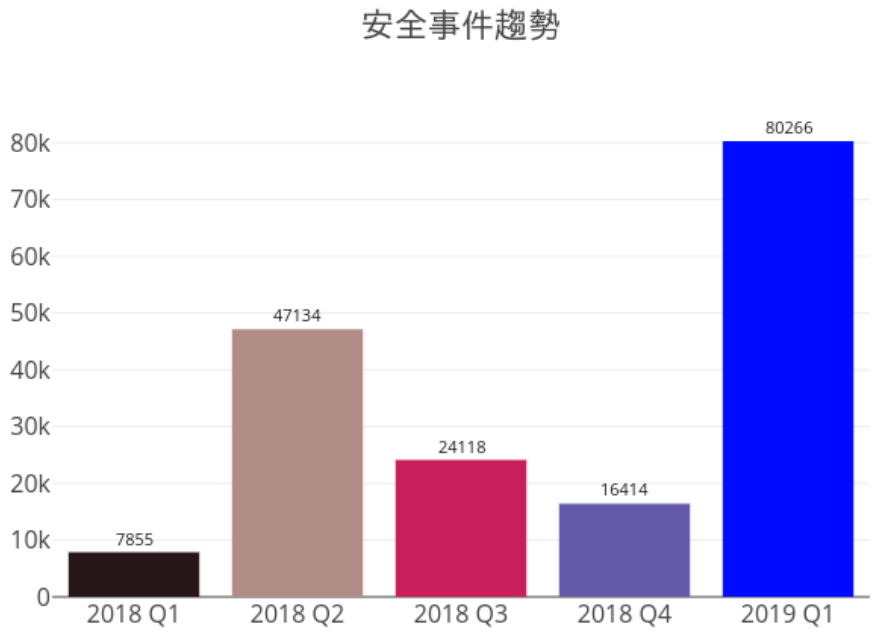

Figure 1: 安全事件趨勢

2019 年第一季度的安全事件總數比上一個季度躍升了 389% 或 63,852 宗。當網頁塗改和釣魚網站事件的數量呈下降趨勢，惡意程式寄存事件上比 2018 年第四季度大幅升近 8 倍，達到近年新高。(見 Figure 2)

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:

[2]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

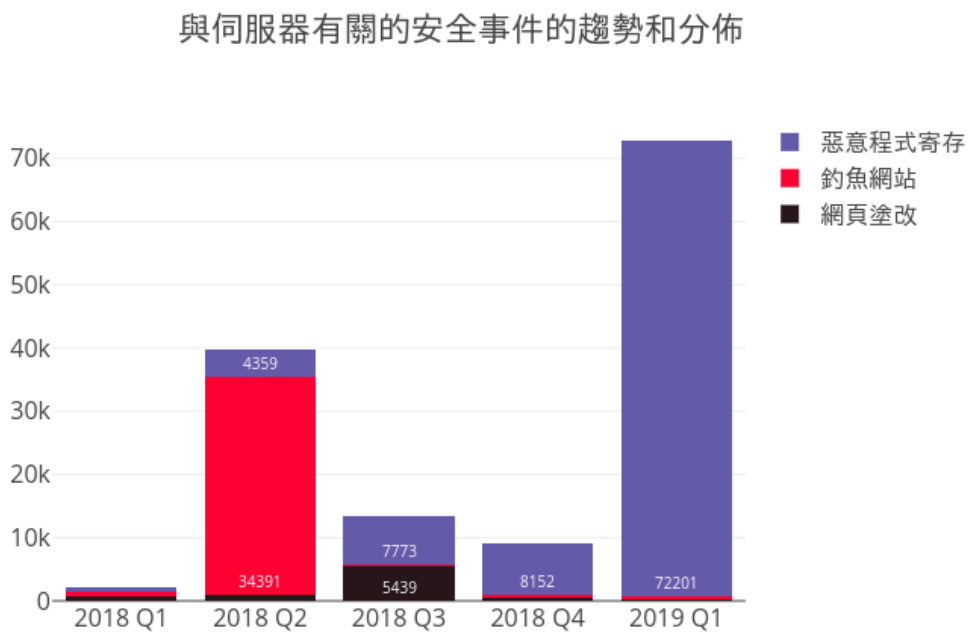

Figure 2: 與伺服器有關的安全事件的趨勢和分佈

事件類別	**2018 Q1**	**2018 Q2**	**2018 Q3**	**2018 Q4**	**2019 Q1**
網頁塗改	824	1,071	5,439	590	318
釣魚網站	634	34,391	319	365	289
惡意程式寄存	649	4,359	7,773	8,152	72,201

惡意程式寄存事件的數量從 2018 年第四季度的 8,152 宗大幅增加到 2019 年第一季度的 72,201 宗或增加了 786%。在這些事件中，每個事件都涉及一個唯一的惡意程式網址。儘管唯一網址/IP 比率從 53 倍減少逾半至 20 倍，前兩個 IP 43.240.13.41 和 45.124.72.40 分別佔 5,366 和 4,586 宗事件。與此同時，其唯一 IP 數量顯著地從 154 個攀升到 3,643 個。

根據日誌紀錄，間歇性的 Ramnit 網絡攻擊從 2019 年 3 月開始。於 2019 年 3 月 6 日，事件數量達到高峰的 11,464 宗。部分受感染的 IP (在同一 IP 位址區塊) 註冊大量類似的域名，可以看出這些 IP 在同一網路中受感染，並參與了大規模的事件。我們注意到另一個現象是有 138 個 IP 涉及超過 100 個唯一惡意程式網址，佔 53,801 宗或整體事件的 75%。由於 Ramnit 能於主機產生偽隨機連結，大量的惡意程式網址便生產了出來。儘管受感染的 IP 位址位於香港, 惡意程式寄存網站主要來自中國。其中一部分包含非法賭博內容。該攻擊活動並非主要針對香港。HKCERT 已通知受影響的人員進行清理其惡意程式寄存連結，並找出其伺服器是否出現安全漏洞。

另一方面，釣魚網站事件的數量從 2018 年第四季度的 365 宗輕微下降到 2019 年第一季度的 289 宗或下跌了 21%。在這些事件中，每個事件都涉及一個唯一的網絡釣魚網

址。其涉及的唯一 IP 數量亦降至 72 個。同時，網頁塗改事件數量亦逐漸下降到 318 宗，其唯一網址/IP 比率維持於 2。於 2019 第一季度，網絡釣魚及網頁塗改事件的數量均低於前幾個季度。

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

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:

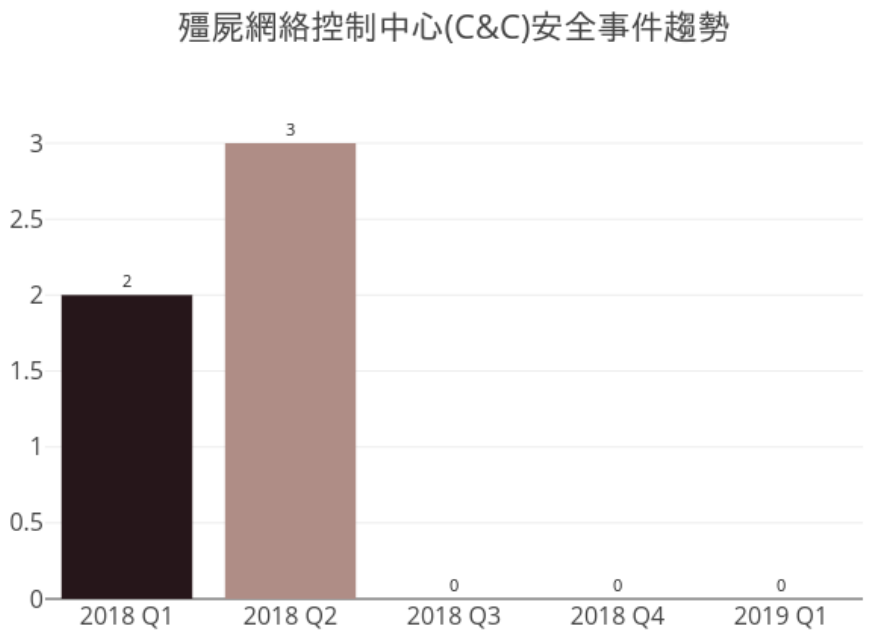

Figure 3: 殭屍網絡控制中心 (C&C) 安全事件的趨勢

在本季沒有收到殭屍網絡控制中心的事件報告。

殭屍電腦安全事件

以下為殭屍電腦安全事件的趨勢:

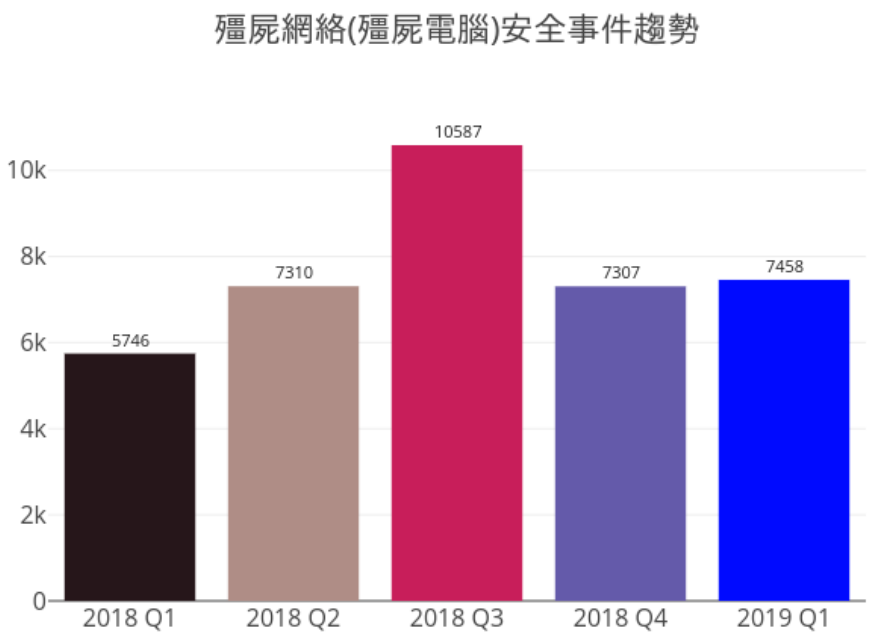

Figure 4: 殭屍電腦安全事件的趨勢

2019 年第一季度香港網絡上的殭屍網絡（殭屍電腦）宗數只輕微上升了 2%。五大殭屍網絡維持不變，Mirai 殭屍網絡仍是香港網絡上主要的殭屍網絡家族排名首位，佔 4,521 宗事件或總數的 61%。排名第二及第三的殭屍網絡家族分別為 WannaCry 及 Conficker，其唯一 IP 位址分別有 989 及 565 個。

與上個季度相比，Gamarue 的唯一 IP 位址從 1 個顯著增加至 112 個。Gamarue 有多種感染方法, 可以通過 USB、電子郵件、漏洞攻擊套件、軟件安裝等方式傳播。HKCERT 呼籲大眾提高安全意識, 以保護他們的伺服器和設備。

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 WannaCry, Avalanche, XCode Ghost, Pushdo, Citadel, Mumblehard, Ramnit, ZeroAccess 及 GameOver Zeus

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

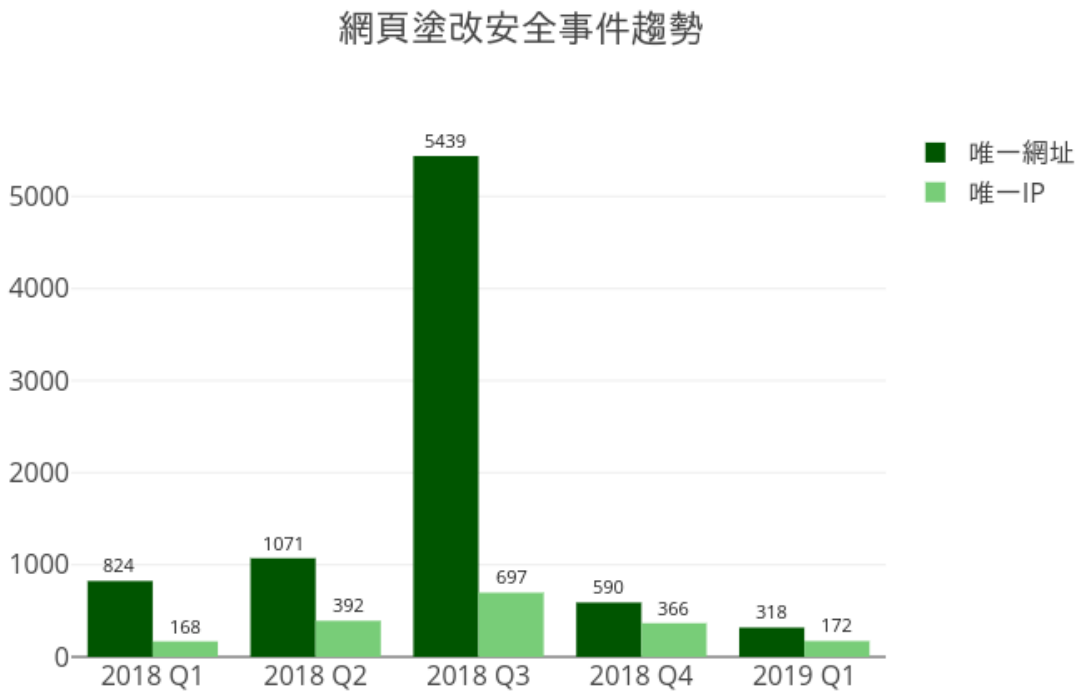

Figure 5: 網頁塗改安全事件趨勢

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

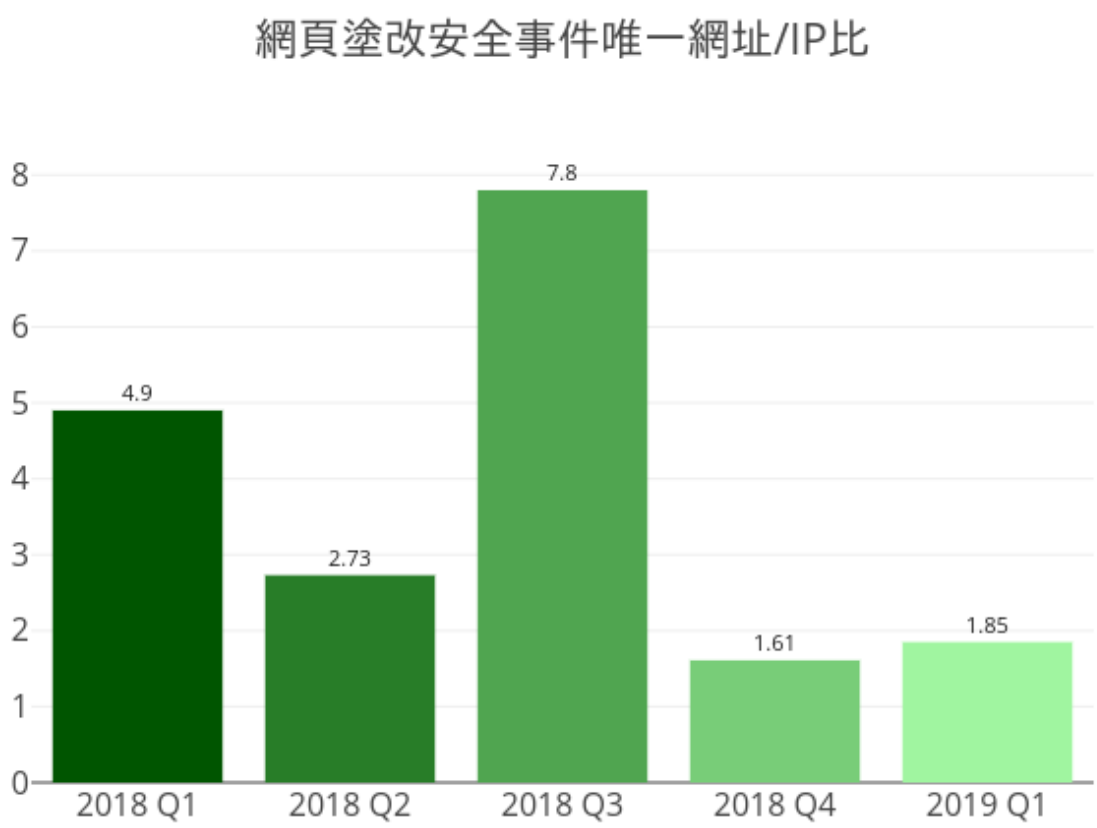

Figure 6: 網頁塗改全事件唯一網址/IP 比

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供很多唯一網址
- 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

Figure 7: 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。

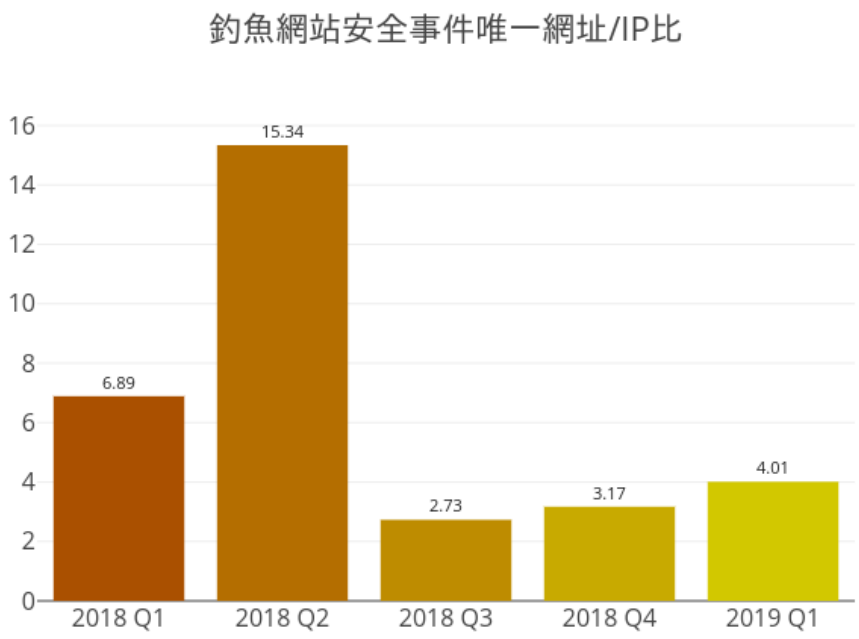

Figure 8: 釣魚網站安全事件唯一網址/IP 比

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供很多唯一網址
- 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：

- CleanMX - phishing
- Phishtank

3 惡意程式寄存

3.1 數據統計

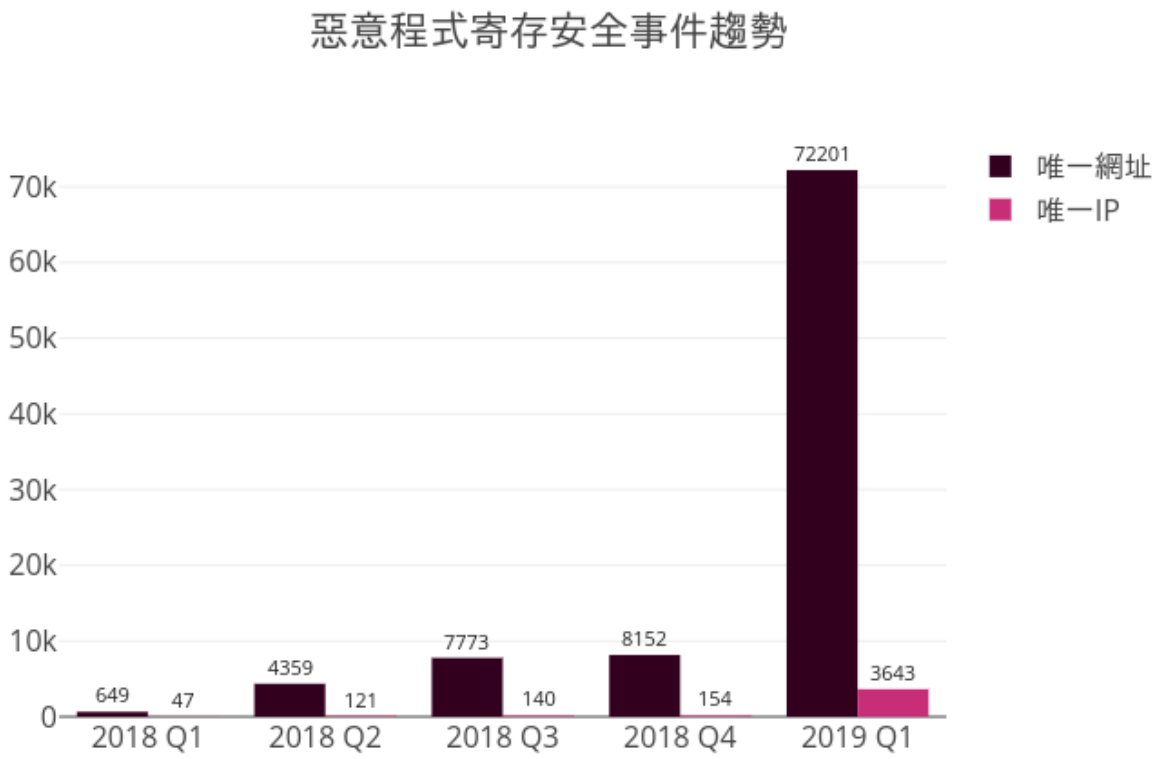

Figure 9: 惡意程式寄存安全事件趨勢

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。

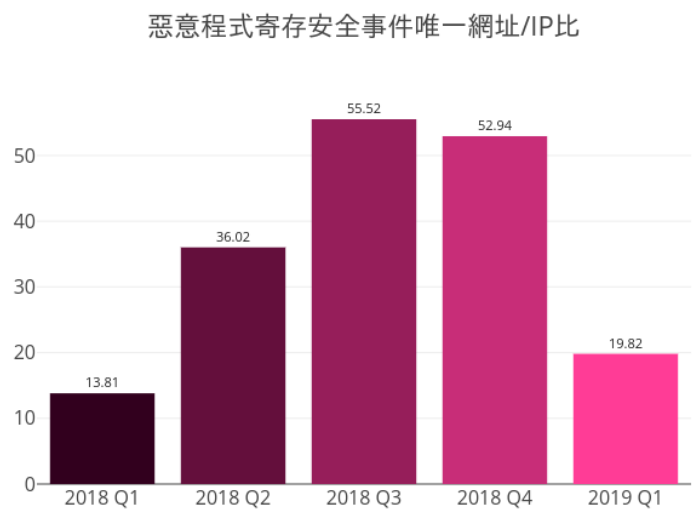

Figure 10: 惡意程式寄存安全事件唯一網址/IP 比

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供很多唯一網址
- 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
- CleanMX - Malware
- Malc0de
- MalwareDomainList

4 殭屍網絡

4.1 殭屍網絡控制中心 (C&C)

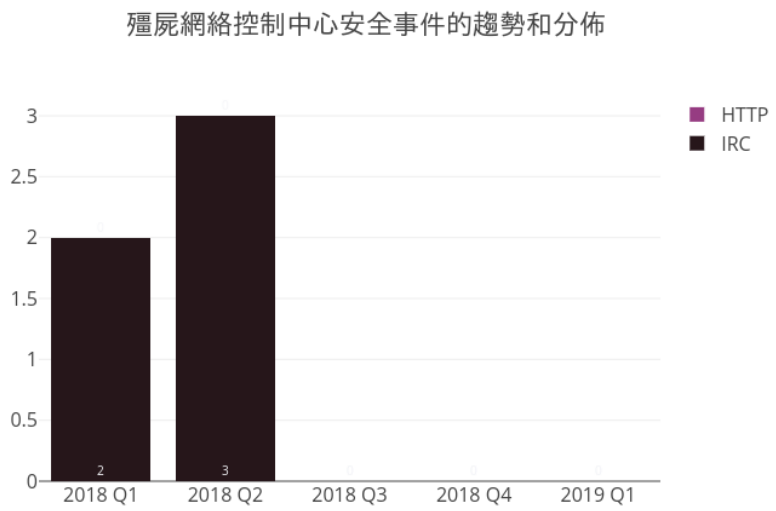

Figure 11: 殭屍網絡控制中心安全事件的趨勢和分佈

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
- 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[3]

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。

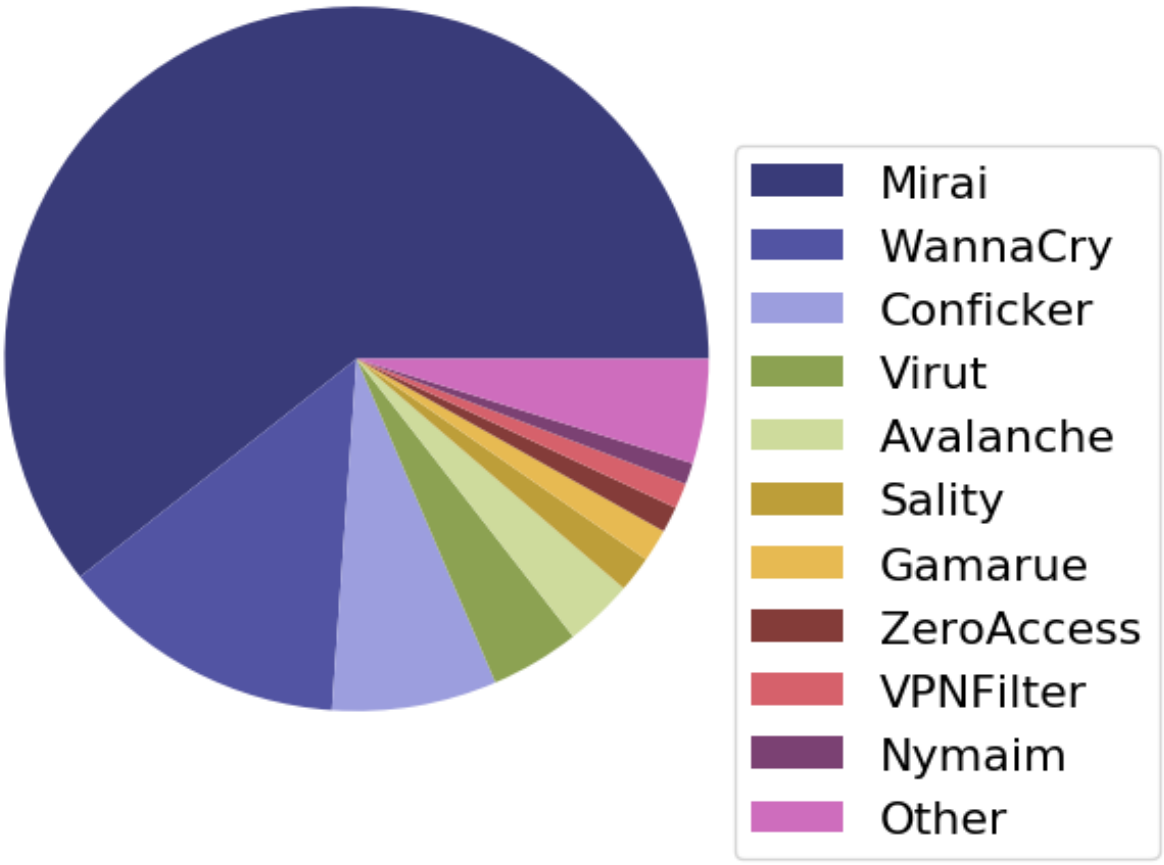

Figure 12: 香港網絡內的主要殭屍網絡

[3]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。

Table 2: 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	變化
1	→	Mirai	4521	9.7%
2	→	WannaCry	989	-18.1%
3	→	Conficker	565	-5.0%
4	→	Virut	305	9.7%
5	→	Avalanche	236	-2.1%
6	→	Sality	123	-16.9%
7	⇑	Gamarue	112	11100.0%
8	⇑	ZeroAccess	89	78.0%
9	⇓	VPNFilter	87	3.6%
10	⇓	Nymaim	73	15.9%

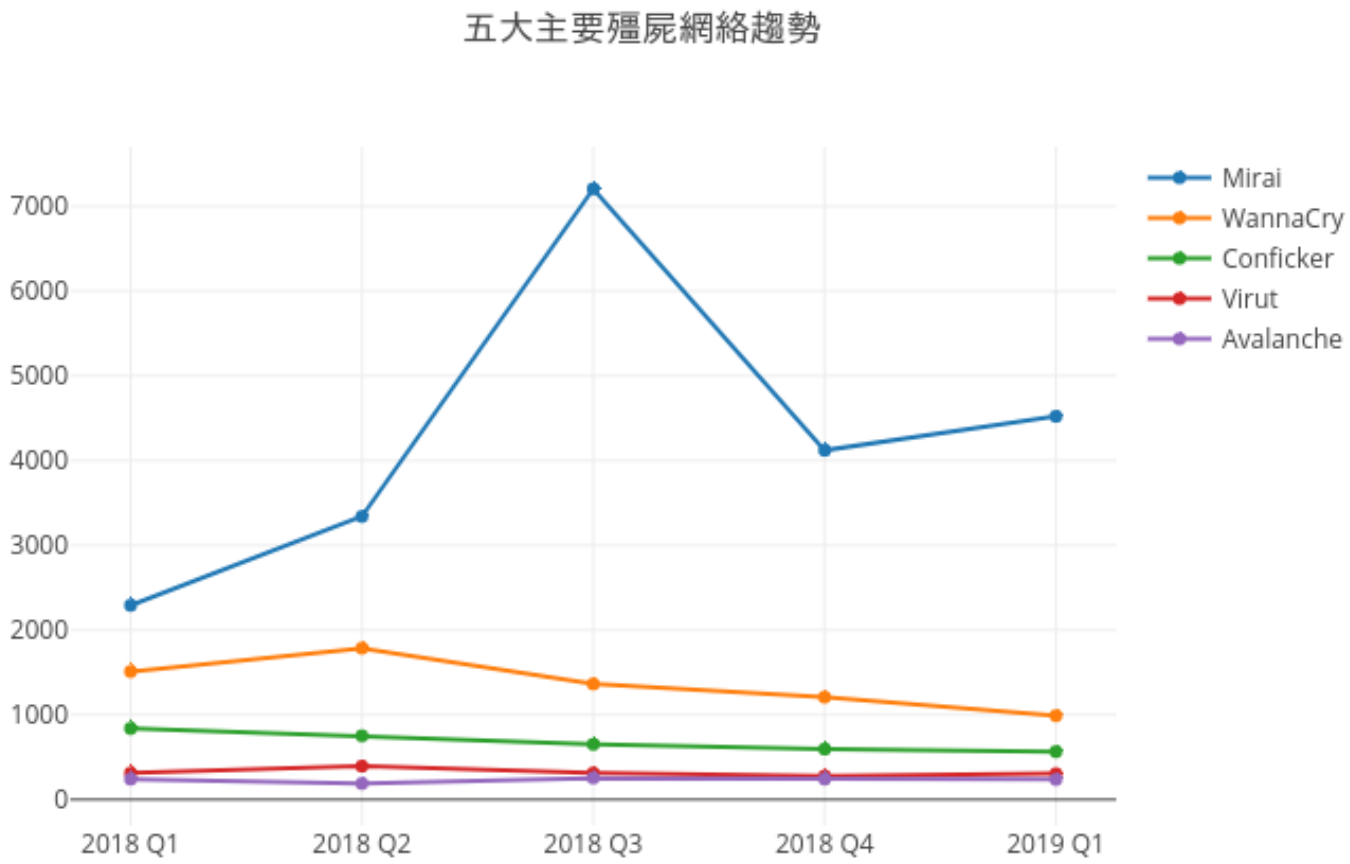

Figure 13: 五大主要殭屍網絡趨勢

Name	**2018 Q1**	**2018 Q2**	**2018 Q3**	**2018 Q4**	**2019 Q1**
Mirai	2,291	3,340	7,205	4,120	4,521
WannaCry	1,510	1,786	1,364	1,208	989
Conficker	838	752	651	595	565
Virut	311	394	313	278	305
Avalanche	241	189	254	241	236

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?C
- 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：

- ShadowServer - botnet_drone
- ShadowServer - sinkhole_http_drone
- Shadowserver - Microsoft_sinkhole

附錄

A 資料來源

以下是資料的來源:

以下是資料的來源:	資料來源	首次使用日期
網頁塗改	Zone - H	2013-04
網頁塗改	CleanMX - Phishing	2013-04
網頁塗改	Phishtank	2013-04
惡意程式寄存	Abuse.ch: Zeus Tracker - Binary URL	2013-04
惡意程式寄存	CleanMX - Malware	2013-04
惡意程式寄存	Malc0de	2013-04
惡意程式寄存	MalwareDomainList	2013-04
殭屍網絡控制中心 (C&Cs)	Abuse.ch: Zeus Tracker - C&Cs	2013-04
殭屍網絡控制中心 (C&Cs)	Abuse.ch: Palevo Tracker - C&Cs	2013-04
殭屍網絡控制中心 (C&Cs)	Shadowserver - C&Cs	2013-09
殭屍電腦	Shadowserver - botnet_drone	2013-08
殭屍電腦	Shadowserver - sinkhole_http_drone	2013-08
殭屍電腦	Shadowserver - microsoft_sinkhole	2013-08

B 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
Maxmind	2019-4-2

C 主要殭屍網絡

Table 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
Avalanche	無	網絡犯罪包辦服務	• 視乎惡意軟件	• 發送垃圾郵件 • 寄存釣魚網站 • 寄存惡意程式 • 竊取敏感資訊
Bamital	無	木馬程式	• 利用「路過式下載」(drive-by-download) • 透過 P2P 網絡	• 點擊詐騙 • 搜尋劫持
BankPatch	MultiBanker Patcher BankPatcher	針對網上銀行的木馬程式	• 透過成人網站 • 有問題的多媒體編解碼器 • 垃圾電郵 • 即時通訊系統	• 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
Bedep	無	木馬程式	• 透過漏洞攻擊包 • 惡意廣告	• 點擊詐騙 • 下載其他惡意軟件
BlackEnergy	無	DDoS 木馬程式	• 以 rootkit 技術保持隱藏 • 使用流程注入技術 • 擁有強的加密技術和模塊化的架構	• 發動分散式阻斷服務攻擊 (DDoS)
Citadel	無	針對網上銀行的木馬程式	• 逃避及停止安全檢測工具	• 竊取銀行登入認證資料及敏感資料 • 按鍵記錄 • 截圖擷取 • 視訊擷取 • 瀏覽器中間人攻擊 • 勒索軟件
Conficker	Downadup Kido	蠕蟲	• 動態網域產生演算法 (DGA) 能力 • 通過 P2P 網絡進行通訊 • 停止安全檢測運行工具	• 利用 Window 伺服器服務漏洞 MS08-067 • 暴力破解管理員密碼，在網絡上傳播 • 利用 Window 自動 (auto-run)，透過外置磁碟機傳播

Table 4: 主要殭屍網絡

主要殭屍網絡	別名	性質	感染方法	攻擊/影響
Corebot	無	針對網上銀行的木馬程式	• 透過下載器	• 竊取敏感資訊 • 安裝其他惡意程式 • 後門程式, 允許未經授權的存取
Dyre	無	針對網上銀行的木馬程式	• 透過垃圾電郵	• 誘騙受害人致電詐騙電話號碼以竊取銀行登入認證資料 • 發送垃圾電郵
Gamarue	Andromeda	下載器/蠕蟲	• 透過漏洞攻擊包 • 透過垃圾電郵 • 微軟 Word 巨集 • 透過外置磁碟機	• 竊取敏感資訊 • 允許未經授權的存取 • 安裝其他惡意程式
Ghost Push	無	手機惡意程式	• 透過安裝程式	• 獲取根權限 • 下載其他惡意程式
Glupteba	無	木馬程式	• 利用「路過式下載」(drive-by-download) 感染系統	• 推送內容關聯廣告 • 點擊劫持
IRC Botnet	無	木馬程式	• 通過 IRC 網絡進行通訊	• 後門程式，允許未經授權的存取 • 發動分散式阻斷服務攻擊 (DDoS) • 發送垃圾郵件
Mirai	無	蠕蟲	• 利用出廠密碼 telnet	• 發動分敗式阻斷服務攻擊 (DDoS)
Murofet	無	木馬程式	• 透過被感染的檔案 • 透過漏洞攻擊包	• 下載其他惡意軟件
Nivdort	無	木馬程式	• 透過垃圾電郵	• 竊取登入認證資料及敏感資料
Nymaim	無	木馬程式	• 透過垃圾電郵	• 鎖定受害系統 • 令受害人無法存取檔案 • 勒索贖金
Palevo	Rimecud Butterfly bot Pilleuz Mariposa Vaklik	蠕蟲	• 即時通訊系統, 點對點網絡及外置磁碟機	• 後門程式，允許未經授權的存取 • 竊取登入認證資料及敏感資料 • 利用洗黑錢手法直接用銀行竊取金錢

Table 5: 主要殭屍網絡

主要殭屍網絡	別名	性質	感染方法	攻擊/影響
Pushdo	Cutwail Pandex	下載器	• 隱藏惡意網絡流量 • 動態網域產生演算法 (DGA) 能力 • 利用「路過式下載」(drive-by-download) 感染系統 • 利用瀏覽器和插件漏洞	• 下載其他針對網上銀行的惡意程式 (例如: Zeus 和 Spyeye) • 發動分散式阻斷服務攻擊 (DDoS) • 發送垃圾郵件
Ramnit	無	蠕蟲	• 感染檔案 • 透過漏洞攻擊包 • 公開 FTP 伺服器	• 後門程式，允許未經授權的存取 • 竊取登入認證資料及敏感資料
Sality	無	木馬程式	• 以 rootkit 技術保持隱藏 • 通過 P2P 網絡進行通訊 • 透過外置磁碟機或共享傳播 • 停止安全檢測工具 • 使用多態性和遮蔽切入點（Entry Point Obscuring）技術來感染檔案	• 發送垃圾郵件 • 通信代理 • 竊取敏感資料 • 感染網絡伺服器和/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） • 下載其他惡意程式
Slenfbot	無	蠕蟲	• 透過外置磁碟機或共享傳播	• 後門程式，允許未經授權的存取 • 其他針對網上銀行的的惡意程式 • 發動分散式阻斷服務攻擊 (DDoS) • 發送垃圾郵件
Tinba	TinyBanker Zusy	針對網上銀行的木馬程式	• 透過漏洞攻擊包 • 透過垃圾電郵	• 竊取登入認證資料及敏感資料

Table 6: 主要殭屍網絡

主要殭屍網絡	別名	性質	感染方法	攻擊/影響
Torpig	Sinowal Anserin	木馬程式	• 以 rootkit 技術保持隱藏 (Mebroot rootkit) • 動態網域產生演算法 (DGA) 能力 利用「路過式下載」(drive-by-download) 感染系統	• 竊取敏感資料 • 瀏覽器中間人攻擊
Virut	無	木馬程式	• 透過外置磁碟機或共享傳播	• 發送垃圾郵件 • 發動分散式阻斷服務攻擊 (DDoS) • 詐騙 • 竊取資料
WannaCry	WannaCrypt	勒索軟件	• 於網絡中散播 • 利用 Windows SMB 漏洞	• 加密用戶數據 • 索取贖款 • 數據無法復原
Wapomi	無	蠕蟲	• 透過外置磁碟機或共享傳播 • 感染可執行檔案	• 後門程式，允許未經授權的存取 • 下載其他惡意程式 • 改動重要檔案，導致系統不穩定 • 收集電腦活動數據，竊取個人資料，並令降低電腦效能
ZeroAccess	max++ Sirefef	木馬程式	• 以 rootkit 技術保持隱藏 • 通過 P2P 網絡進行通訊 • 利用「路過式下載」(drive-by-download) 感染系統 • 偽裝成有效檔案 (例如: 多媒體檔案，keygen)	• 下載其他惡意程式 • 採礦比特幣和欺詐點擊
Zeus	Gameover	針對網上銀行的木馬程式	• 隱身技術 • 通過 P2P 網絡進行通訊 • 利用「路過式下載」(drive-by-download) 感染系統	• 竊取銀行登入認證資料及敏感資料 • 瀏覽器中間人攻擊 • 按鍵記錄 • 下載其他惡意程式 (例如:Cryptolocker) • 發動分散式阻斷服務攻擊 (DDoS)