

Operation GG (Good Game)



台灣最熱門網遊安裝檔 驚見APT後門

Kenny @ Chroot.org

大綱

- Introduction 玩家角度 (Kenny)
 - 如何發現 / 偵測?
 - Event TimeLine
- Operation Winnti (Kaspersky 報告) (GD)
- Operation Old Cooper 通報+追查(PK)
- Unplugging PlugX 清除 (Trend Micro)

I am just a Player.



Introduction



The screenshot shows the Garena website homepage. At the top is a navigation bar with the Garena logo (a red stylized 'G' with the tagline 'connecting the dots') and a menu with links for '平台' (Platform), '遊戲' (Games), '社群' (Community), '商城' (Store), and '服務' (Services). A '會員登入' (Member Login) button is on the right. Below the navigation bar is a large red banner with three cartoon characters. The first character holds a gift box, with the text '精品—最好玩的遊戲，才會進入 Garena 旗下！' (Premium—The most fun games will enter the Garena family!). The second character holds a heart, with the text '快樂—提供同理心、個人化服務，以及絕佳的遊戲體驗。' (Happy—Providing empathy, personalized service, and an exceptional gaming experience.). The third character holds a lightbulb, with the text '創意—In Garena's products, experience the surprise of carefully designed experiences!' (Creative—In Garena's products, experience the surprise of carefully designed experiences!). Below the banner is a '遊戲專區 | Game Zone' section. It features a grid of game icons: '英雄聯盟' (League of Legends), 'AVA', '流亡黯道' (Dota), 'Mstar', '全民踢足球' (All People Kick Soccer), '格鬥聯盟' (Fighting Alliance), and '都會特攻' (Metropolitan Assault). To the right of the grid is a large '英雄聯盟' (League of Legends) banner with the text '進入官網' (Enter Official Website) and a '15+' age rating. Below the banner is a description: '風靡全球 Dota 團隊新作品，超過 85 個原創角色，不斷線系統、防開圖機制，結合 RPG 遊戲元素。來點真正的遊戲吧！' (Global phenomenon Dota team's new work, over 85 original characters, continuous system, anti-map opening mechanism, combined with RPG game elements. Come play some real games!).

connecting the dots

平台 ▾ 遊戲 ▾ 社群 ▾ 商城 ▾ 服務 ▾ 會員登入

玩家滿意是我們回家唯一的路

精品—最好玩的遊戲，才會進入 Garena 旗下！

快樂—提供同理心、個人化服務，以及絕佳的遊戲體驗。

創意—In Garena's products, experience the surprise of carefully designed experiences!

遊戲專區 | Game Zone

英雄聯盟 AVA 流亡黯道 Mstar

全民踢足球 格鬥聯盟 都會特攻

英雄聯盟 LEAGUE-LEGENDS

進入官網 15+

風靡全球 Dota 團隊新作品，超過 85 個原創角色，不斷線系統、防開圖機制，結合 RPG 遊戲元素。來點真正的遊戲吧！

線上遊戲代理商，以串連世界玩家一同遊戲為主要事業。
在東南亞和台灣創造了最大的線上遊戲平台。

推薦遊戲



英雄連萌



AVA 戰地之王



流氓按到



Mstar



全民踢足球



格鬥聯盟



FIFA Online 3

英雄聯盟 LOL玩家數量全球最多！ 每百人中就有一人玩LOL

2014年10月29日 08:00

Riot(遊戲開發商) 公佈了《英雄聯盟》活躍玩家

全球每天活躍玩家數量約2700 萬。

而最多有750 萬玩家同時在同一時間進行遊戲。

而每月都會有6700 萬的玩家活躍在遊戲當中。

如何發現？

2014.12.26



好久沒玩LOL,
來虐菜(欺負新手)一下~

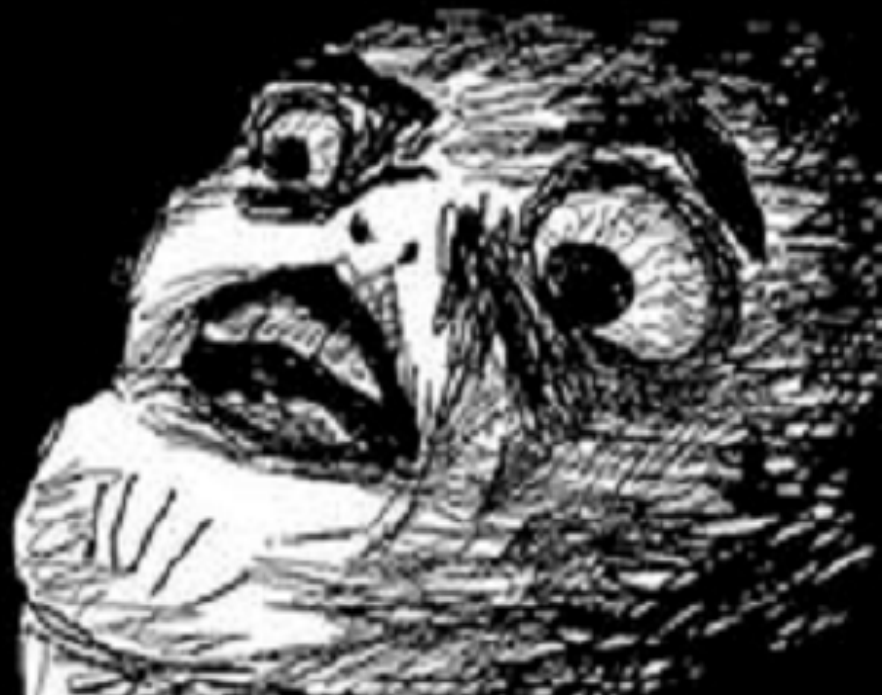
從『**官網**』下載了LOL主程式.....

開心地打開遊戲..



■ ■ ■ ■ ■ ■ ■ ■

有病毒!?

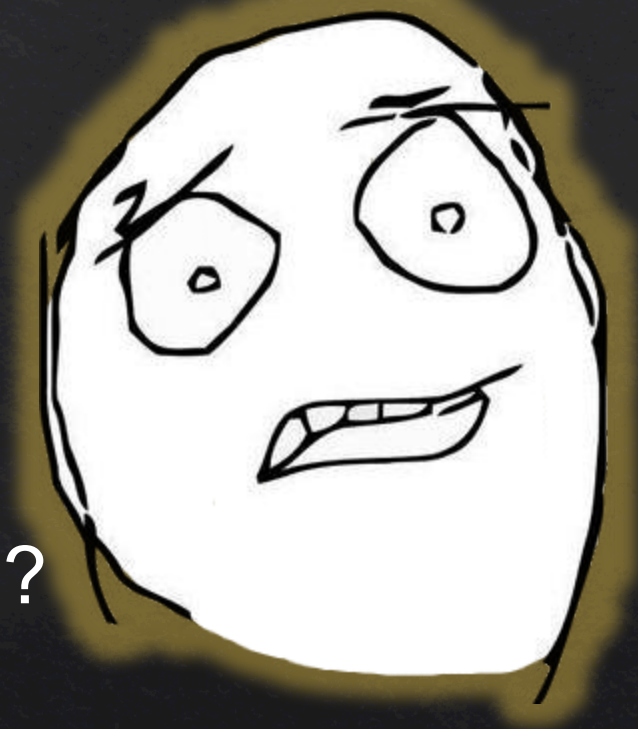


如果是一般玩家很可能.....



誰可以幫我處理？

我的謎片檔案安全嗎？

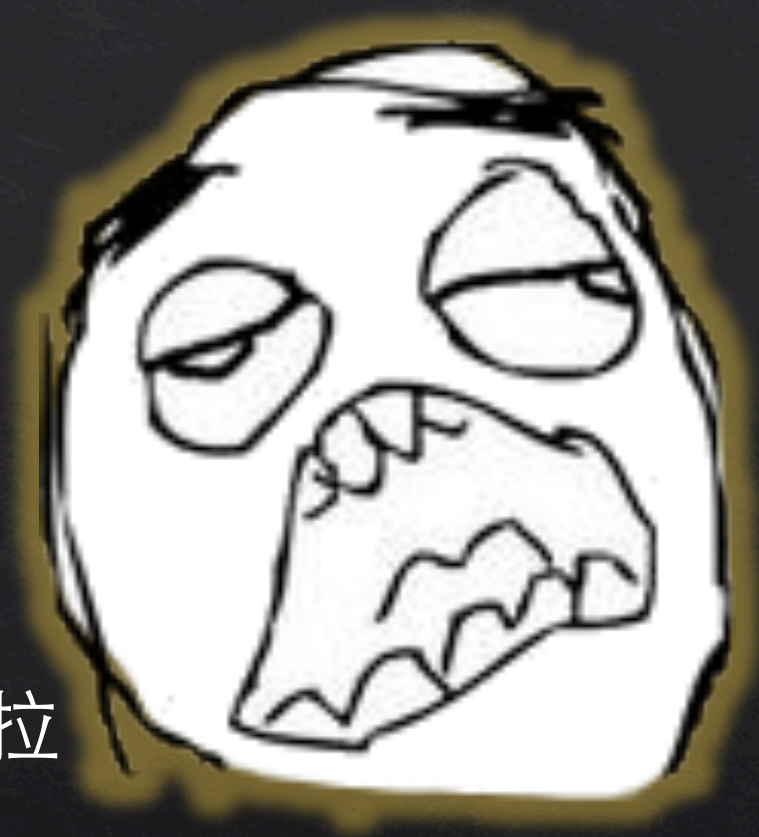


電腦會爆炸嗎？

驚慌失措類型

爛防毒拉

誤報拉



電腦關機
病毒就會餓死拉

有個性類型

第一時間我覺得...

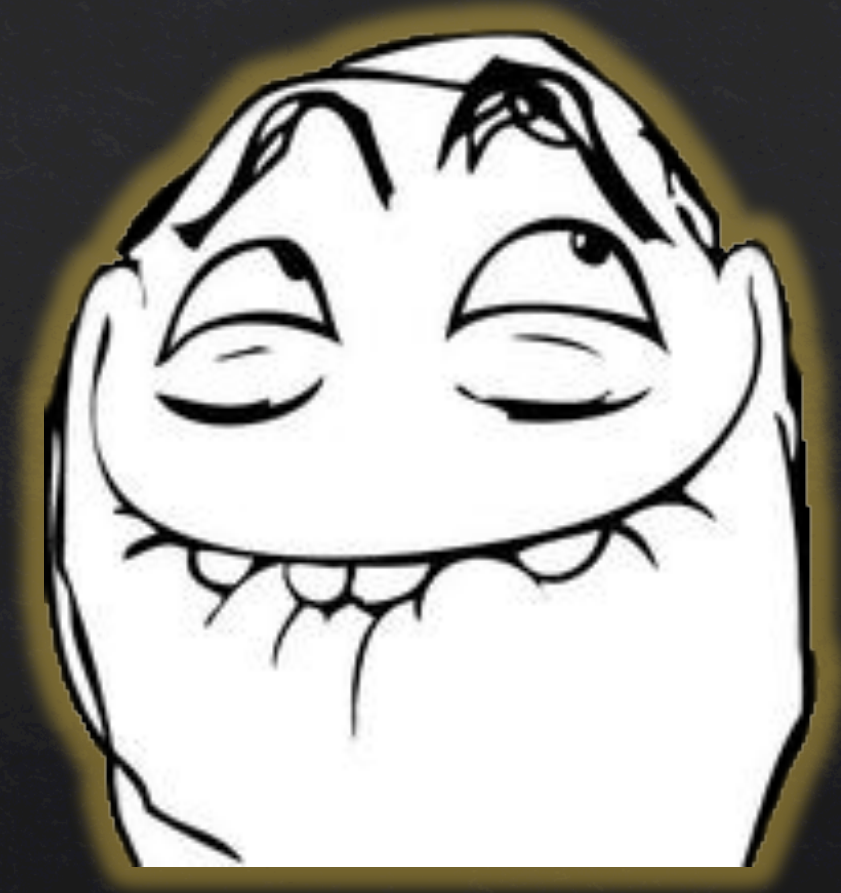
WTF !!

我只是想玩LOL

沒有要玩病毒阿....



但我剛好是略懂資安技能的玩家...



這下好玩了
研究一下病毒從哪來的呢？

最簡單的辨認方法



VirusTotal is a free service that **analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

 File

 URL

 Search

No file selected

Choose File

Maximum file size: 128MB

By clicking 'Scan it!', you consent to our [Terms of Service](#) and allow VirusTotal to share this file with the security community. See our [Privacy Policy](#) for details.

Scan it!

<https://www.virustotal.com/>

SHA256: 2b7e99541a29d17c541c31d9b24e4e888350b0a64c43bc87e6955e45cc507793

File name: LoLTWLauncher.exe

Detection ratio: 28 / 56

Analysis date: 2015-01-02 10:25:45 UTC (6 days, 4 hours ago)



Analysis

File detail

Relationships

Additional information

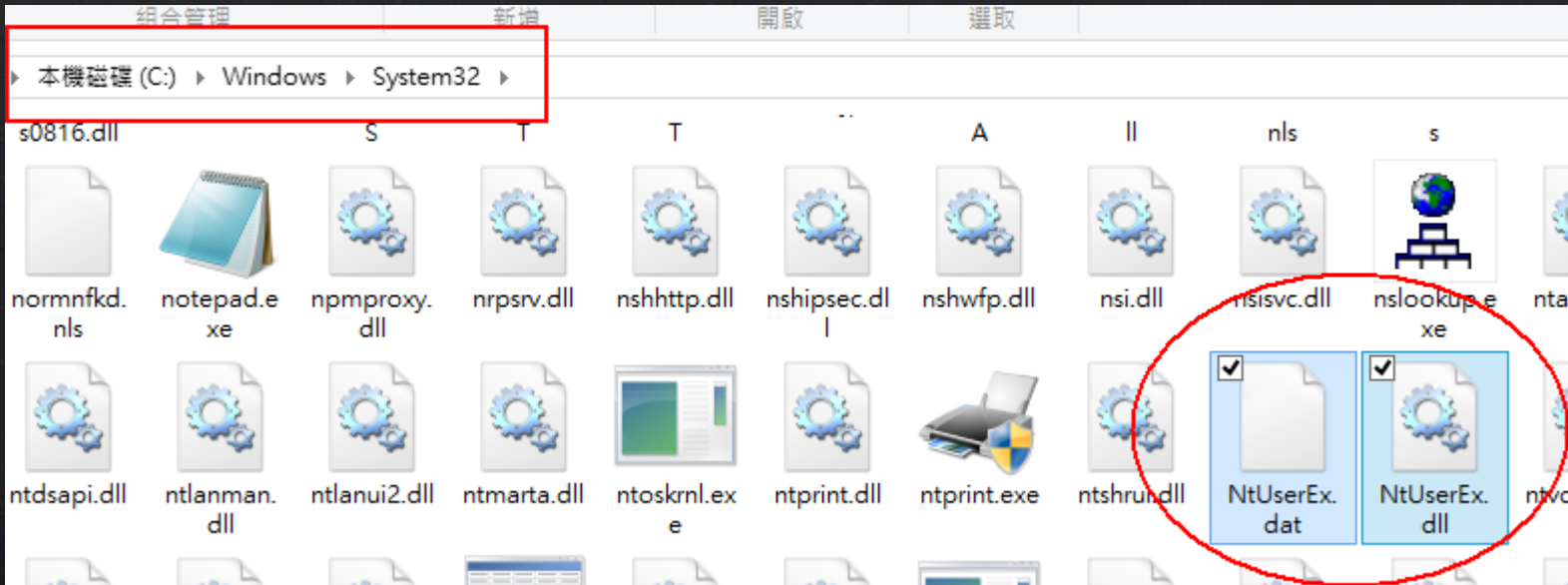
Comments 0

Votes

Behavioural information

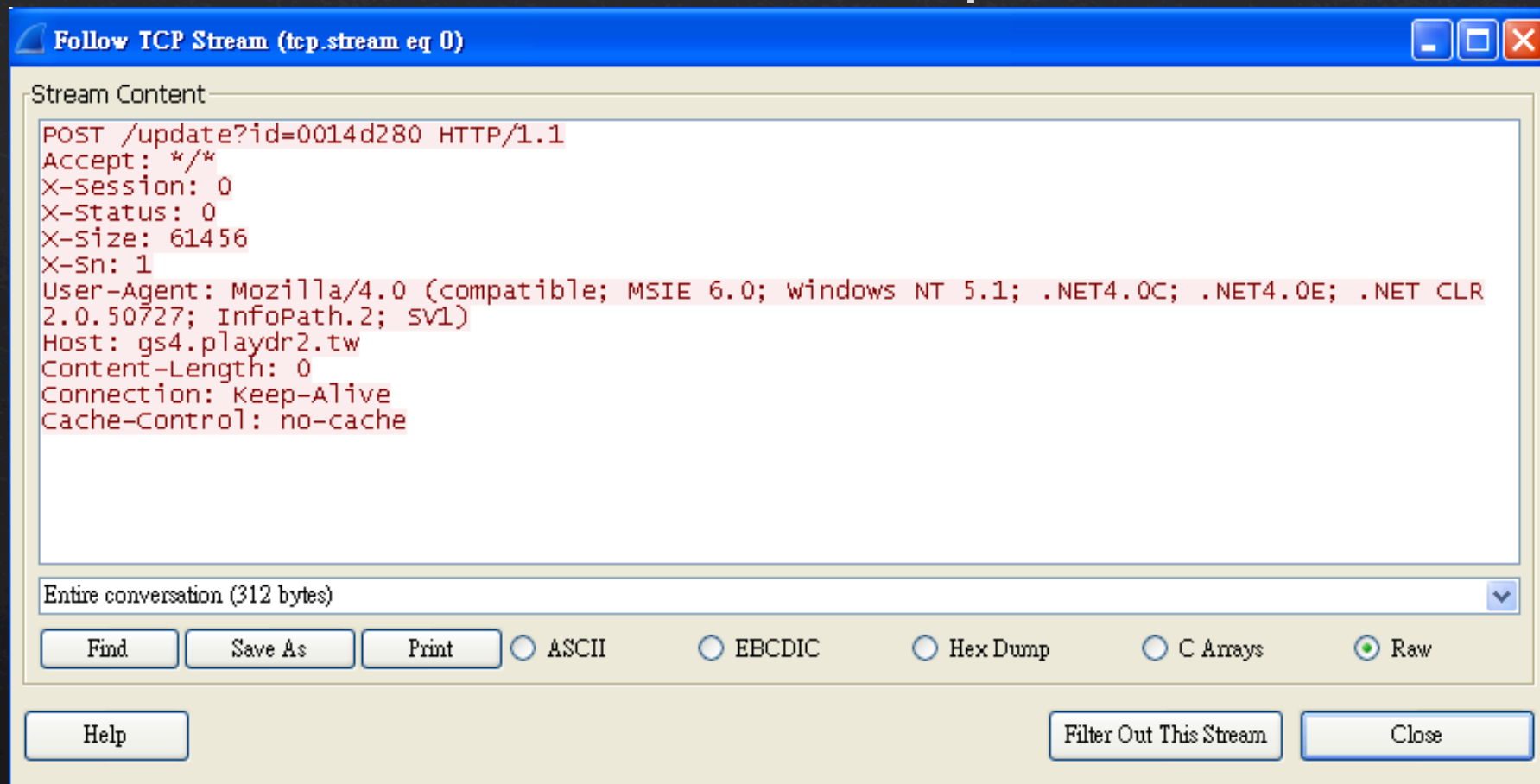
Antivirus	Result	Update
ALYac	Dropped:Trojan.Generic.12127006	20150102
AVG	SHeur4.CDWA	20150102
AVware	Trojan.Win32.Generic!BT	20150102
Ad-Aware	Dropped:Trojan.Generic.12127006	20150102
Agnitum	Trojan.Agent!VhR6TYjEdfg	20150101
BitDefender	Dropped:Trojan.Generic.12127006	20150102
Bkav	HW32.Packed.A869	20141230
Cyren	W32/Trojan.FZEK-3747	20150102
DrWeb	Trojan.DownLoader11.48120	20150102
Emsisoft	Dropped:Trojan.Generic.12127006 (B)	20150102

惡意後門存放位置



C:\windows\System32\NtUserEx.dll
C:\windows\System32\NtUserEx.dat

C&C Server位置



特徵：
update?id=00xxxxxx

Domain:
gs2.playdr2.tw
gs3.playdr2.tw
gs4.playdr2.tw

秉持著調查精神
決定更深入追查



取得遊戲管道

官網下載器



Cloud Server



Game



官網頁面



Game



調查結果

VulReport

關於網站

積分排名

漏洞列表

新聞列表

聯絡我們

通報漏洞

企業註冊

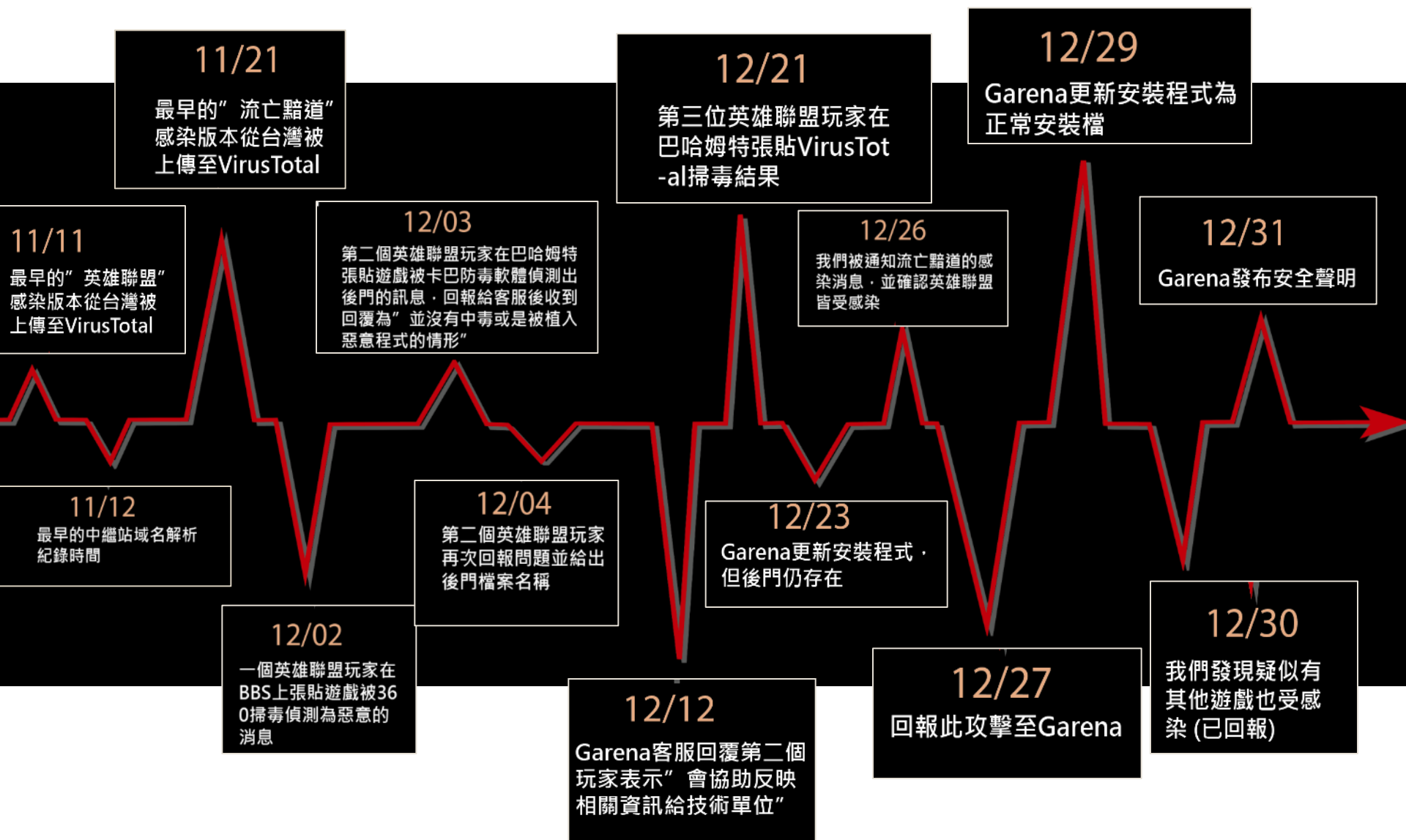
登入 / 註冊



Adobe Flash Player Heap Overflow

There is a heap overflow in Adobe Flash Player 14.0.0.125 on Windows 7 , which results in remote code execution.

<https://vulreport.net/>





11/11

最早的“英雄聯盟”
感染版本從台灣被
上傳至VirusTotal



11/11

最早的“英雄聯盟”
感染版本從台灣被
上傳至VirusTotal

11/12

最早的中繼站域名解析
紀錄時間

11/21

最早的“流亡黯道”
感染版本從台灣被
上傳至VirusTotal

11/11

最早的“英雄聯盟”
感染版本從台灣被
上傳至VirusTotal

11/12

最早的中繼站域名解析
紀錄時間

11/21

最早的“流亡黯道”
感染版本從台灣被
上傳至VirusTotal

11/11

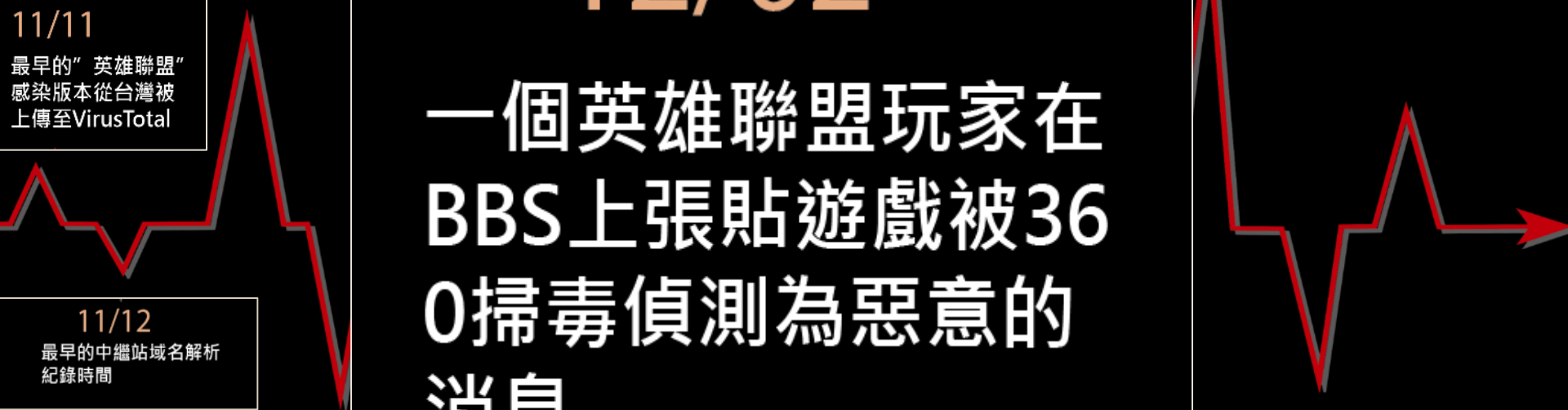
最早的“英雄聯盟”
感染版本從台灣被
上傳至VirusTotal

11/12

最早的中繼站域名解析
紀錄時間

12/02

一個英雄聯盟玩家在
BBS上張貼遊戲被36
0掃毒偵測為惡意的
消息



11/21

最早的“流亡黯道”
感染版本從台灣被
上傳至VirusTotal

12/21

第三位英雄聯盟玩家在
巴哈姆特張貼VirusTot

12/23

Garena更新安裝程式， 但後門仍存在

11/11

最早的“英雄聯盟”
感染版本從台灣被
上傳至VirusTotal

11/12

最早的中繼站域
紀錄時間

一個英雄聯盟玩家在
BBS上張貼遊戲被36
0掃毒偵測為惡意的
消息

12/12

Garena客服回覆第二個
玩家表示“會協助反映
相關資訊給技術單位”

11/21

最早的“流亡黯道”
感染版本從台灣被

12/21

第三位英雄聯盟玩家在

12/26

我們被通知流亡黯道的感
染消息，並確認英雄聯盟
皆受感染

11/11

最早的“英雄聯
感染版本從台灣
上傳至VirusTot

11/12

最早的中繼站
紀錄時間

BB5引擎和遊戲被360
掃毒偵測為惡意的
消息

12/12

Garena客服回覆第二個
玩家表示“會協助反映
相關資訊給技術單位”



11/21

最早的“流亡黯道”
感染版本從台灣被

12/21

第三位英雄聯盟玩家在
巴哈姆特張貼VirusTot

12/27

回報此攻擊至Garena

11/11

最早的“英雄聯
感染版本從台灣
上傳至VirusTot

11/12

最早的中繼站
紀錄時間

BBS上張貼遊戲被36
0掃毒偵測為惡意的
消息

12/12

Garena客服回覆第二個
玩家表示“會協助反映
相關資訊給技術單位”

11/21

最早的“流亡黯道”
感染版本從台灣被
上傳至VirusTotal

12/21

第三位英雄聯盟玩家在
巴哈姆特張貼VirusTot

11/11

最早的“英雄聯盟”
感染版本從台灣被
上傳至VirusTotal

12/29

Garena更新安裝程式為
正常安裝檔

11/12

最早的中繼站域名
紀錄時間

BBS上張貼遊戲被36
0掃毒偵測為惡意的
消息

12/12

Garena客服回覆第二個
玩家表示“會協助反映
相關資訊給技術單位”

12/27

回報此攻擊至Garena

11/21

最早的“流亡黯道”

12/21

第三位英雄聯盟玩家在

12/29

Garena更新安裝程式為
正常安裝檔

12/31

Garena發佈安全聲明

11/11

最早的“英雄
感染版本從台
上傳至VirusT

11/1

最早的中繼
紀錄時間

一個英雄聯盟玩家在
BBS上張貼遊戲被36
0掃毒偵測為惡意的
消息

12/12

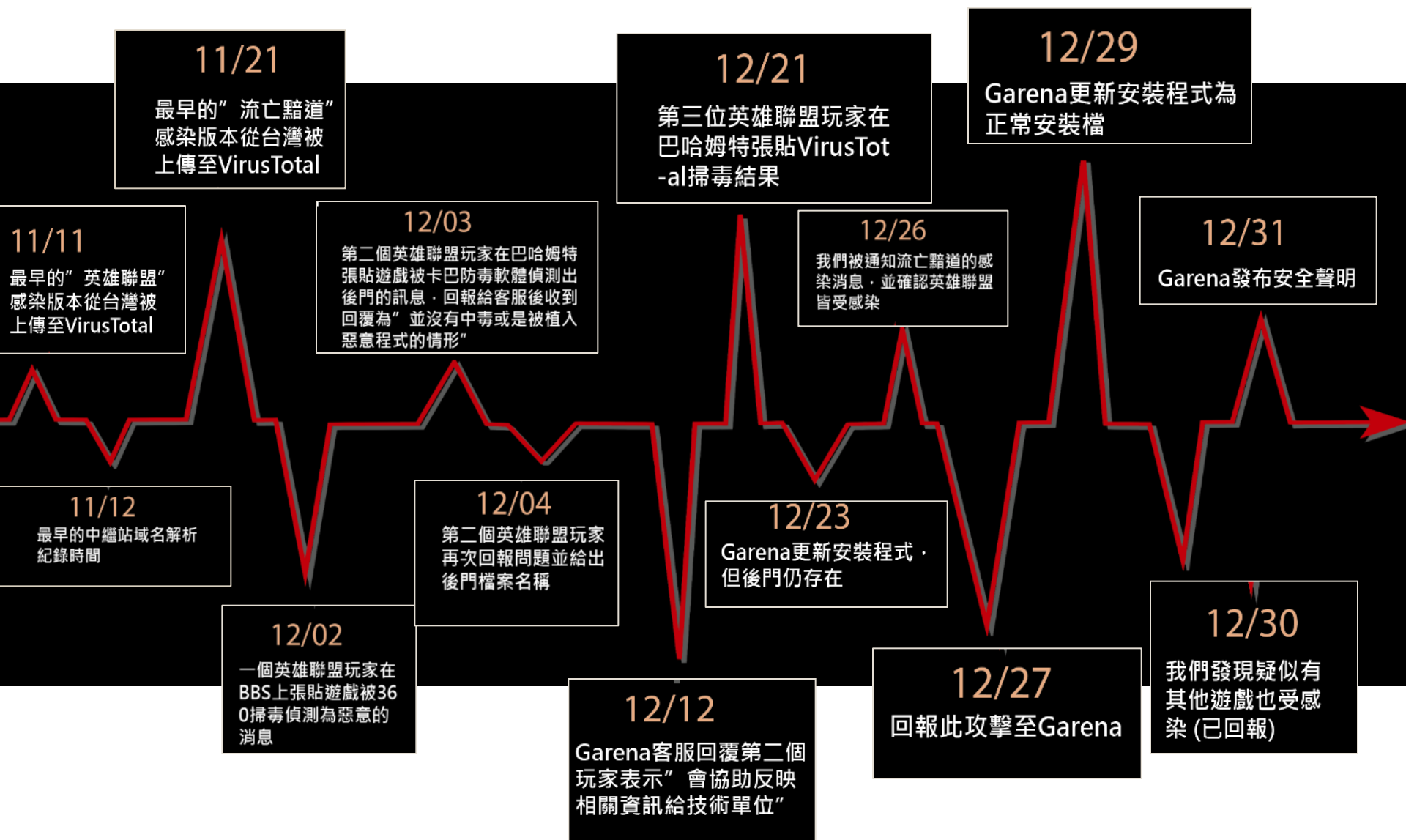
Garena客服回覆第二個
玩家表示“會協助反映
相關資訊給技術單位”

12/27

回報此攻擊至Garena

我們發現疑似有
其他遊戲也受感
染 (已回報)

30



事情有這麼單純嗎？



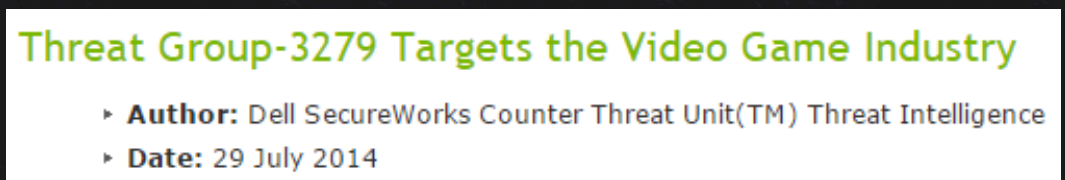
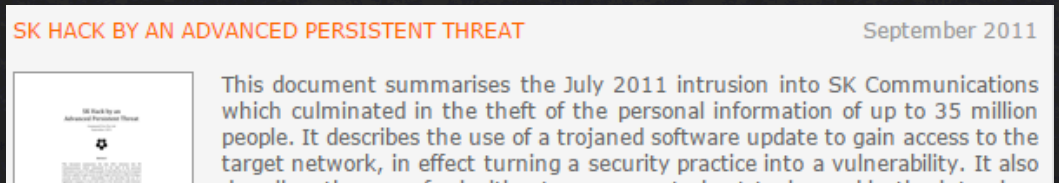
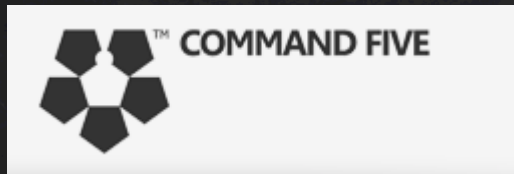
由這次的後門看出攻擊者可能有特殊身分
討論後有了更驚人的發現

惡意程式與中繼站關連

惡意程式：**PlugX** 木馬 (常見於網軍攻擊報告)

中繼站：**gs2.playdr2.tw** (出現在下列資安公司報告中)

卡巴斯基命名為 **Winnti Group**



卡巴斯基 Winnti Group 研究報告



“Winnti”

More than just a game

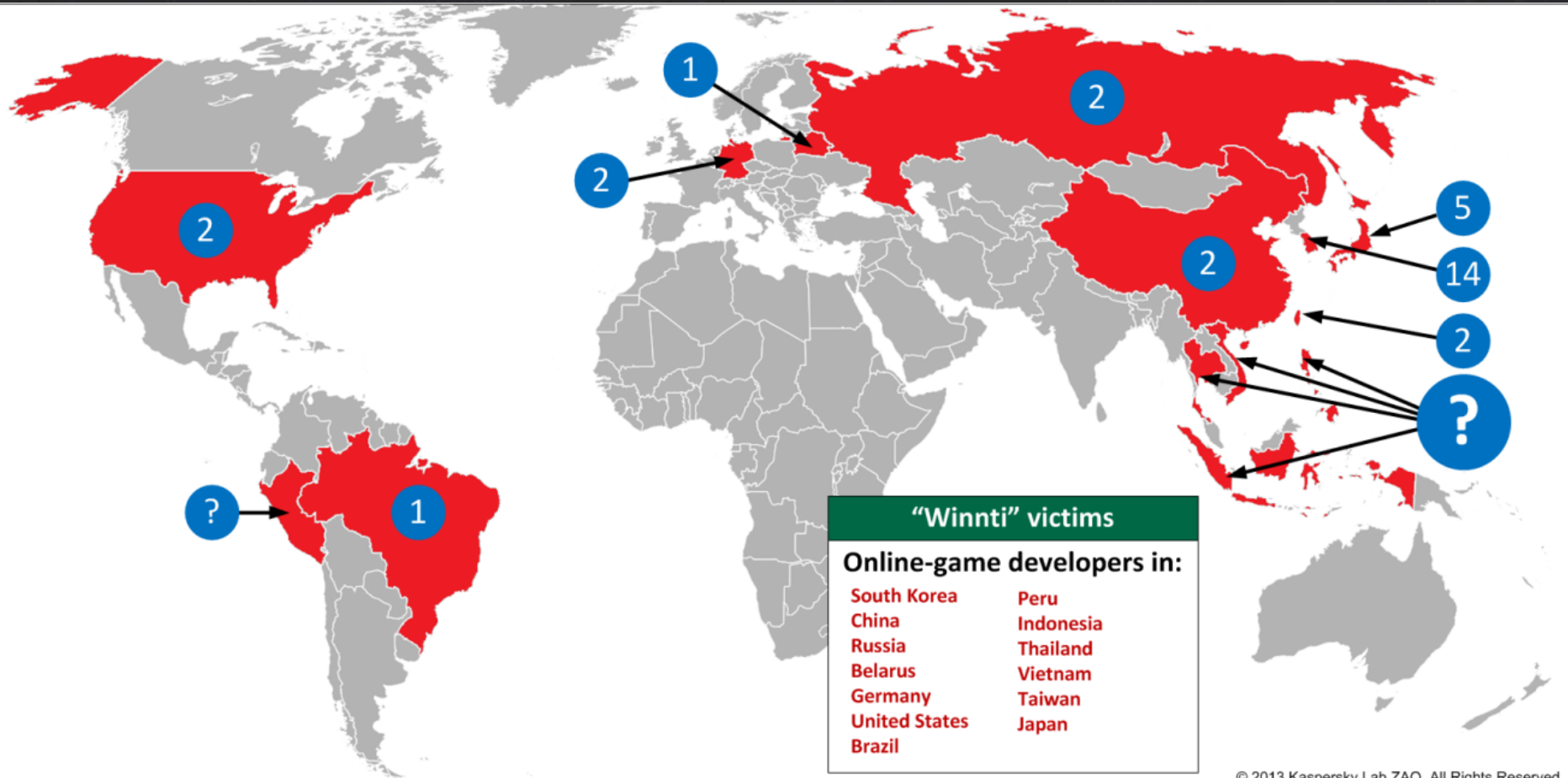
April 2013

Kaspersky Lab Global Research and Analysis Team

Winnti Group 攻擊許多遊戲公司



Winnti Group 受害公司遍及全球



Winnti Group 可能造成損害

- ◆ 偷取遊戲原始碼
- ◆ 偷取數位簽章(用來簽更多惡意程式)
- ◆ 偷取虛擬貨幣寶物
- ◆ 偷取遊戲玩家個資
- ◆ 遊戲更新程式網綁木馬(本事件新手法)

Reference

- ◇ <http://ragemaker.net/>
- ◇ <http://www.garena.tw/index/index.php>
- ◇ <http://www.ironforum.com.tw/newsdetail/1701/2>
- ◇ <http://travel.ettoday.net/article/418853.htm>
- ◇ <http://forum.gamer.com.tw/C.php?bsn=17532&snA=471877>

- ◇ <https://www.commandfive.com/research.html>
- ◇ <http://securelist.com/analysis/internal-threats-reports/37029/winnti-more-than-just-a-game/>
- ◇ <http://www.secureworks.com/cyber-threat-intelligence/threats/threat-group-3279-targets-the-video-game-industry/>