

個案分析-

Quimonk 木馬攻擊事件

分析報告

TACERT

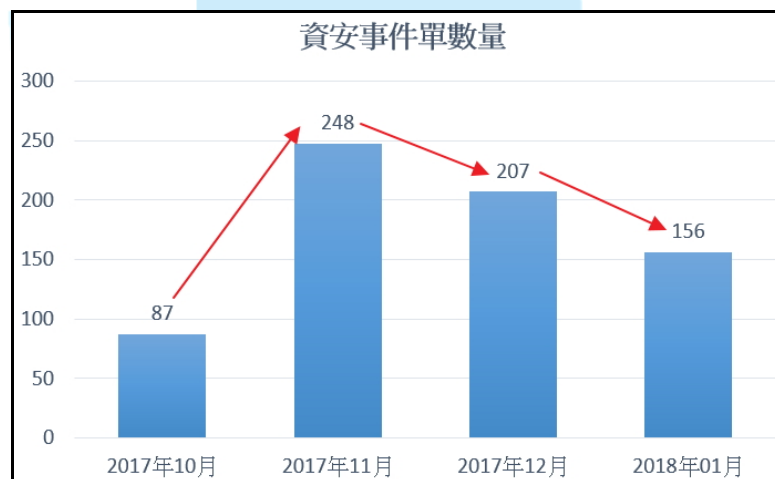
臺灣學術網路危機處理中心團隊(TACERT)製

107 年 2 月

1. 事件簡介

1. 在學術網路中有許多木馬攻擊事件，其中因 Quimonk 木馬程式(偵測規則 MALWARE-CNC Win.Trojan.Quimonk variant outbound connection detected)所觸發的資安事件在 2017 年 11 月至 12 月期間開單量遽增，而且連續兩個月位居 N-ASOC 偵測規則第一名。

事件單編號: AISAC-134			
原發布編號	SOC-INT-201801-134	原發布時間	2018-01-24
事件類型	殭屍電腦(Bot)	原發現時間	2018-01-24
事件主旨	教育部資安事件通告— 大學 [140.112.43.199] 主機進行惡意程式連線警訊通知 (MALWARE-CNC Win.Trojan.Quimonk variant outbound connection detected)		
事件描述	來源IP主機可能存在未修補之弱點遭駭客攻擊，感染惡意程式或遭植入木馬程式導致觸發此事件，將可能導致主機機敏資料外洩，或成為殭屍網路一員而對外發動攻擊。入侵偵測防禦系統偵測到來源IP (140.112.43.199)，包含疑似惡意程式連線行為特徵之封包，對目標IP (多個目標IP) 進行連線。此事件來源PORT (多個來源PORT)，目標PORT (多個目標PORT)。		
手法研判			
建議措施	請檢視來源IP該連線行為是否已得到合法授權。若來源IP該連線為異常行為，可先利用掃毒軟體進行全系統掃描，並利用ACL暫時阻擋該可疑IP。同時建議管理者進行以下檢查：a. 請查看來源IP有無異常動作(如：新增帳號、開啟不明Port、執行不明程式)。b. 確認防毒軟體的病毒碼已更新為最新版本，並進入系統安全模式下進行全系統掃描作業、系統是否已安裝相關修正檔，或關閉不使用的應用軟體與相關通訊埠。若來源IP為DNS server、NAT主機或IP分享器等設備IP時，表示有內部主機透過這些設備向外連線時而觸發偵測規則，則需先請設備管理者透過事件單所附之資訊(目的地IP、時間、來源port)，來協助查找內部觸發偵測規則之主機，再依前述建議處理措施進行作業。		



2. 從該類型資安事件的佐證資料得知，受害主機會以 80port 連線至下列三個中國 IP: 123.57.151.113、120.76.122.200、120.26.109.229 之其中之一或二個 IP。
3. 為了瞭解該類型資安事件的觸發原因與攻擊行為，本中心取得樣本後進行檢測。

II. 事件檢測

1. 首先，將樣本 sudajidnhf.exe 送至 Virustotal 網站檢測，發現其為惡意之比例有 53/66，而且多家防毒公司稱它為 QjMonkey、QIWMONK、Qjwmonkey 或 Downloader。

SHA256:	775c7bd9e820c4dfd0fabdfcade2de901414bd46d2691ea5020a818f6a42eb83
檔案名稱:	sudajidnhf.exe
偵測率:	53 / 66
分析日期:	2018-01-22 07:36:45 UTC (0 分鐘 前)

SentinelOne (Static ML)	static engine - malicious	20180115
Sophos AV	QjMonkey (PUA)	20180122
SUPERAntiSpyware	PUP.Bundler.Variant	20180122
Symantec	SMG.Heur.C	20180122
Tencent	Win32.Adware.Download.Ugiz	20180122
TrendMicro	PUA_QIWMONK	20180122
TrendMicro-HouseCall	PUA_QIWMONK	20180122
VBA32	Downloader.Agent	20180120
VIPRE	Trojan.Win32.GenericIBT	20180122
ViRobot	Adware.Qjwmonkey.826120.F	20180122
Webroot	W32.Adware.Qiwmonk	20180122
Yandex	PUA.Downloader!	20180112
Zillya	Adware.Qjwmonkey.Win32.248	20180119
ZoneAlarm by Check Point	not-a-virus:Downloader.Win32.Agent.hdxo	20180122

2. 在 Win 7 系統上執行程式 sudajidnhf.exe，會出現安裝 WinRAR 的安裝程式畫面，WinRAR 為一般電腦常用免費軟體，容易降低使用者戒心，而點選程式來進行安裝。

WinRAR
 软件大小: 2066KB
 人气指数: 23015
 软件语言: 简体中文
 软件评级: ★★★★★
 安全检测: 360杀毒通过
 QQ检测通过
 金山毒霸通过

快速安裝

热门推荐软件:
 爱奇艺
 精彩视频在线观看
 立即体验
 安全套装
 安全软件先睹为快
 立即体验
 360浏览器
 保护你上网安全
 立即体验
 速压
 极速压缩体验
 立即体验

软件简介:
 WinRAR 是一款功能强大的压缩包管理器，它是档案工具RAR 在 Windows 环境下的图形界面。WinRAR 可以让你很轻易地，将压缩后的文件放在支持ZIP和RAR的格式。而在压缩时可以根据压缩等级的不同，而可以

3. 執行完後出現下載成功訊息，同時桌面上出現名稱為 wrar550scp 的應用程式檔，可見此 sudajidnhf.exe 主要功能為下載程式。



4. 點選視窗上「打開文件」選項，出現 WinRAR 程式安裝畫面，點選「安裝」則開始安裝該程式。



5. 在安裝 WinRAR 同時檢視主機對外連線狀態，發現除了 WinRAR 程式本身有對外連線外，另外有產生許多不明程式的執行檔進行對外連線，因為在背景偷偷執行程式，一般使用者無法發現此狀況。

2018/1/22	下午 03:08:42	Added	WinRAR.exe	TCP	192.168.195.144:49227	119.145.148.32:80
2018/1/22	下午 03:08:42	Added	WinRAR.exe	TCP	192.168.195.144:49228	119.146.74.49:80
2018/1/22	下午 03:08:42	Added	WinRAR.exe	TCP	192.168.195.144:49229	119.146.74.49:80
2018/1/22	下午 03:08:42	Added	svchost.exe	UDP	0.0.0.0:54309	*:*
2018/1/22	下午 03:08:42	Added	WinRAR.exe	UDP	127.0.0.1:56635	*:*
2018/1/22	下午 03:08:44	Added	WinRAR.exe	TCP	192.168.195.144:49230	203.74.117.22:443
2018/1/22	下午 03:08:44	Added	WinRAR.exe	TCP	192.168.195.144:49231	203.74.117.22:443
2018/1/22	下午 03:08:44	Added	WinRAR.exe	TCP	192.168.195.144:49232	23.59.139.27:80
2018/1/22	下午 03:08:44	Added	WinRAR.exe	TCP	192.168.195.144:49233	23.59.139.27:80
2018/1/22	下午 03:08:44	Added	WinRAR.exe	TCP	192.168.195.144:49234	23.59.139.27:80
2018/1/22	下午 03:08:44	Added	WinRAR.exe	TCP	192.168.195.144:49235	23.59.139.27:80
2018/1/22	下午 03:08:44	Added	WinRAR.exe	TCP	192.168.195.144:49236	103.235.46.191:80
2018/1/22	下午 03:08:44	Added	WinRAR.exe	TCP	192.168.195.144:49237	119.145.148.32:80


2018/1/22	下午 03:12:39	Added	sudajidnhf.exe.exe	TCP	192.168.195.144:49465	123.57.151.113:80
2018/1/22	下午 03:12:39	Added	zny.znywbkb039.exe	TCP	192.168.195.144:49466	106.75.24.100:80
2018/1/22	下午 03:12:39	Added	Unknown	TCP	192.168.195.144:49467	223.26.106.39:443
2018/1/22	下午 03:12:39	Added	svchost.exe	TCP	192.168.195.144:64473	192.168.195.2:53
2018/1/22	下午 03:12:39	Added	IQIYI\setup_baizhu@kb001.exe	TCP	192.168.195.144:64474	211.151.142.113:80
2018/1/22	下午 03:12:42	Added	Unknown	TCP	192.168.195.144:49466	106.75.24.100:80
2018/1/22	下午 03:12:42	Added	Inst13__3112087__3f7372633d6c6d266c733d6e31343463316364383939_68616f2e3336302e636e_0c70.exe	TCP	192.168.195.144:64476	223.26.76.129:443
2018/1/22	下午 03:12:42	Added	Unknown	TCP	192.168.195.144:64476	223.26.76.129:443
2018/1/22	下午 03:12:46	Added	KuaiZip_Setup_1970971572_liutc3_001.exe	TCP	192.168.195.144:64477	110.53.246.34:80
2018/1/22	下午 03:12:48	Added	Unknown	TCP	192.168.195.144:64477	110.53.246.34:80
2018/1/22	下午 03:12:48	Added	Unknown	TCP	192.168.195.144:64478	61.221.181.46:80
2018/1/22	下午 03:12:48	Added	SCWBWizard.exe	TCP	192.168.195.144:64479	106.75.11.174:80
2018/1/22	下午 03:12:50	Added	svchost.exe	UDP	0.0.0.0:60282	*:*
2018/1/22	下午 03:12:52	Added	SCWBMutual.exe	TCP	192.168.195.144:64480	106.75.78.250:80
2018/1/22	下午 03:12:52	Added	SCWBManager.exe	TCP	192.168.195.144:64481	61.221.181.46:80
2018/1/22	下午 03:12:54	Added	svchost.exe	UDP	0.0.0.0:52655	*:*
2018/1/22	下午 03:12:56	Added	KuaiZip_Setup_1970971572_liutc3_001.exe	TCP	192.168.195.144:64482	106.75.95.184:80
2018/1/22	下午 03:12:58	Added	Unknown	TCP	192.168.195.144:64482	106.75.95.184:80
2018/1/22	下午 03:12:58	Added	svchost.exe	UDP	0.0.0.0:53868	*:*

6. 在安裝過程中，我們發現受測主機會連到兩個中國 IP:123.57.151.113 與 120.76.122.200，而這兩個 IP 與該類型資安事件的佐證資料目的 IP 相同。

2018/1/22 下午 03:12:39 Added sudajidnhf.exe.exe TCP 192.168.195.144:49465 123.57.151.113:80

2018/1/22 下午 02:58:15 Added sudajidnhf.exe.exe TCP 192.168.195.144:49196 120.76.122.200:80


將兩個中國 IP 送至 Virustotal 檢測，發現這兩個 IP 對應到網址 <http://api.baizhu.cc>，該網址被 Virustotal 檢測為惡意的比例為 3/66。



123.57.151.113 IP 位址資訊

Geolocation: Country CN, Autonomous System 45096 (Alibaba (Beijing) Technology Co., Ltd.)

Passive DNS replication: 2017-11-20 xn--kbr267d.net, 2017-11-19 xn--kbr267d.com, 2017-09-26 api.baizhu.cc, 2016-08-29 funho.net.cn



120.76.122.200 IP 位址資訊

Geolocation: Country CN

Passive DNS replication: 2016-04-09 api.baizhu.cc

Latest detected URLs: 2/65 2017-04-20 05:46:45 http://api.baizhu.cc/, 2/64 2017-04-19 23:00:35 http://api.baizhu.cc/api/open, 2/64 2017-04-06 21:47:45 http://api.baizhu.cc/api/getdown, 1/64 2017-03-28 12:35:04 http://api.baizhu.cc/api/getlist



URL: <http://api.baizhu.cc/>

偵測率: 3 / 66

分析日期: 2018-01-09 09:55:43 UTC (2週前)

分析: 其他資訊 評論 0 投票

網址掃描器	結果
CyRadar	Malicious site
Forcepoint ThreatSeeker	Malicious site
Fortinet	Malware site

7. 檢視封包內容，發現受測主機連線至 IP:123.57.151.113:80(對應主機:api.baizhu.cc)並上傳資訊「&appid=1&sid=360&ver=2」到/api/getdown 資料夾，而主機回傳軟體下載路徑資訊給受測主機。

```
RSA Security Analytics Reconstruction for session ID: 127 ( Source 192.168.195.148 : 49230, Target 123.57.151.113 : 80 )
Time 1/22/2018 15:54:59 to 1/22/2018 15:55:00 Packet Size 35,570 bytes Payload Size 33,128 bytes
Protocol: 3048/6:80 - Flags: Keep-Assembled-AppMeta-NetworkMeta - Packet Count: 42

REQUEST
POST /api/getdown HTTP/1.1
Host: api.baizhu.cc
Content-Length: 22
Connection:close
Accept-Language: zh-cn
Cache-Control:no-cache
Content-Type:application/x-www-form-urlencoded

&appid=1&sid=360&ver=2

RESPONSE
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 22 Jan 2018 07:55:00 GMT
Content-Type: text/html;Charset=utf-8;Charset=UTF-8
Connection: close
Vary: Accept-Encoding

{"close":false,"loading":false,"XLDOWN":20000000,"charset":"utf-8","xlurl":"http://cdn.baizhu.cc/exel/ThunderSpeed1.0.35.366.exe","smallrange":0,"ip":"140.144.44","color":0,"logo":"http://cdn.baizhu.cc/logo.zip","mainres":"","mainres2":"http://cdn.baizhu.cc/mainres/mainres180111.zip","tempdir":"gzss","setres":"http://cdn.baizhu.cc/skin/skintest0912_lao.zip","exthistory":{"mime":"","name":"qyhelper.dll","url":"http://cdn.baizhu.cc/dll/qyhelper.dll","param":"bd_8501","type":2},"favo":[],"favo1":[{"sort":1,"name":"\u7f51\u5740\u5927\u5168","url":"http://daohang.scj.016272.com/","logo":"http://daohang.scj.016272.com/favicon.ico","mime":"1,3,4,5,8,9,10,11,13","list":[{"id":1,"proc":""}, {"id":3,"proc":""}, {"id":4,"proc":""}, {"id":5,"proc":""}, {"id":8,"proc":""}, {"id":9,"proc":""}, {"id":10,"proc":""}, {"id":11,"proc":""}, {"id":13,"proc":""}], {"sort":2,"name":"\u767e\u5ea6","url":"http://baidu.scj.xrcch.com/","logo":"http://bd.scj.
```

8. 檢視封包內容，發現受測主機連線至 IP:120.76.122.200:80(對應主機:api.baizhu.cc)並上傳資訊「&type=7&appid=1&sid=360&ver=2&tg1=1&tg2=1&tg3=1&tg4=1&tg5=1&tg6=1」到/api/open 資料夾。

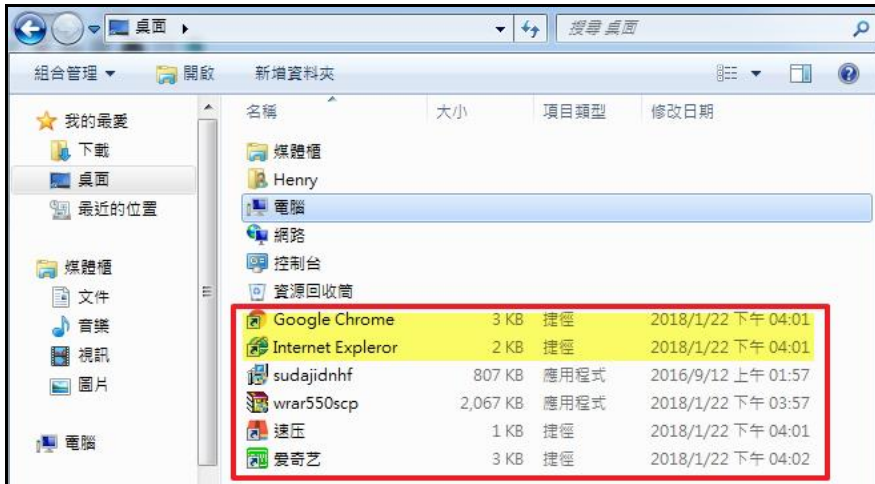
```
RSA Security Analytics Reconstruction for session ID: 41 ( Source 192.168.195.148 : 49488, Target 120.76.122.200 : 80 )
Time 1/22/2018 16:01:19 to 1/22/2018 16:01:20 Packet Size 952 bytes Payload Size 418 bytes
Protocol: 3048/6:80 - Flags: Keep-Assembled-AppMeta-NetworkMeta - Packet Count: 0

REQUEST
POST /api/open HTTP/1.1
Host: api.baizhu.cc
Content-Length: 65
Connection:close
Accept-Language: zh-cn
Cache-Control:no-cache
Content-Type:application/x-www-form-urlencoded

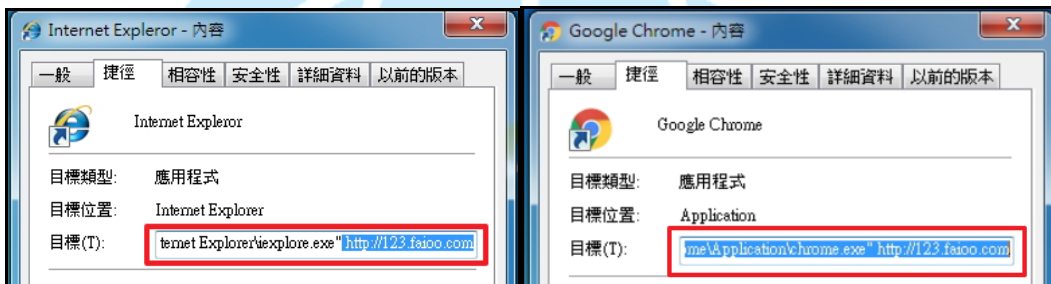
&type=7&appid=1&sid=360&ver=2&tg1=1&tg2=1&tg3=1&tg4=1&tg5=1&tg6=1

RESPONSE
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 22 Jan 2018 08:01:20 GMT
Content-Type: text/html;Charset=utf-8;Charset=UTF-8
Connection: close
Vary: Accept-Encoding
```

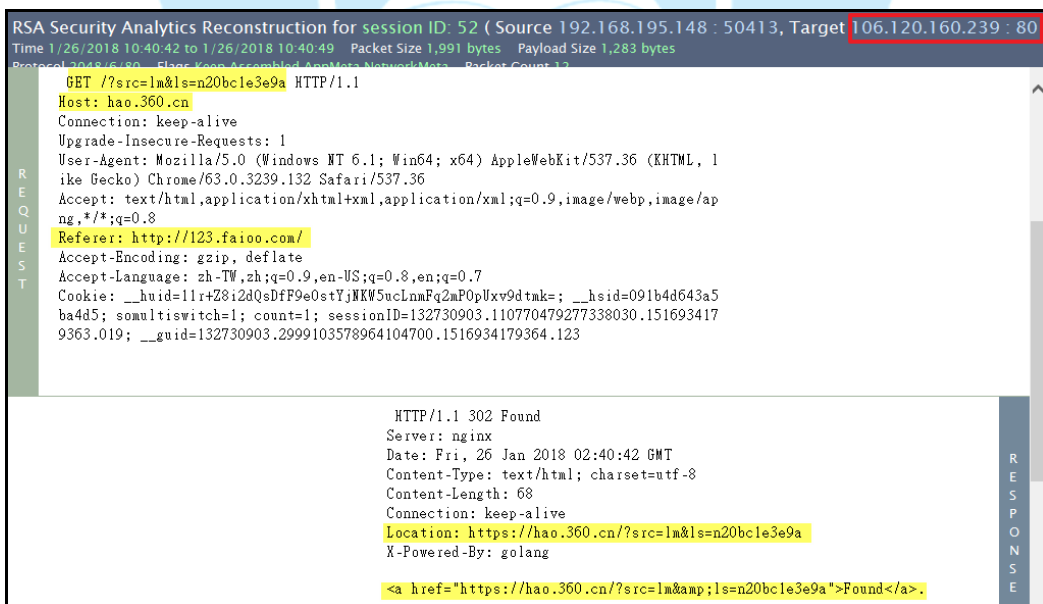
9. 在 WinRAR 安裝完成後，桌面出現我們未授權安裝的程式捷徑，如速壓與愛奇藝的捷徑，也發現 Internet Explorer 之內容被修改過。



10. 檢視桌面瀏覽器 Internet Explorer 與 Google Chrome 的內容，發現被植入開啟瀏覽器後連到 <http://123.faioo.com> 的語法。



(1) 當開啟瀏覽器時一開始會連線至 <http://123.faioo.com>，之後會轉址到中國 360 導航的網站 (<https://hao.360.cn/?src=lm&ls=n20bc1e3e9a>)。



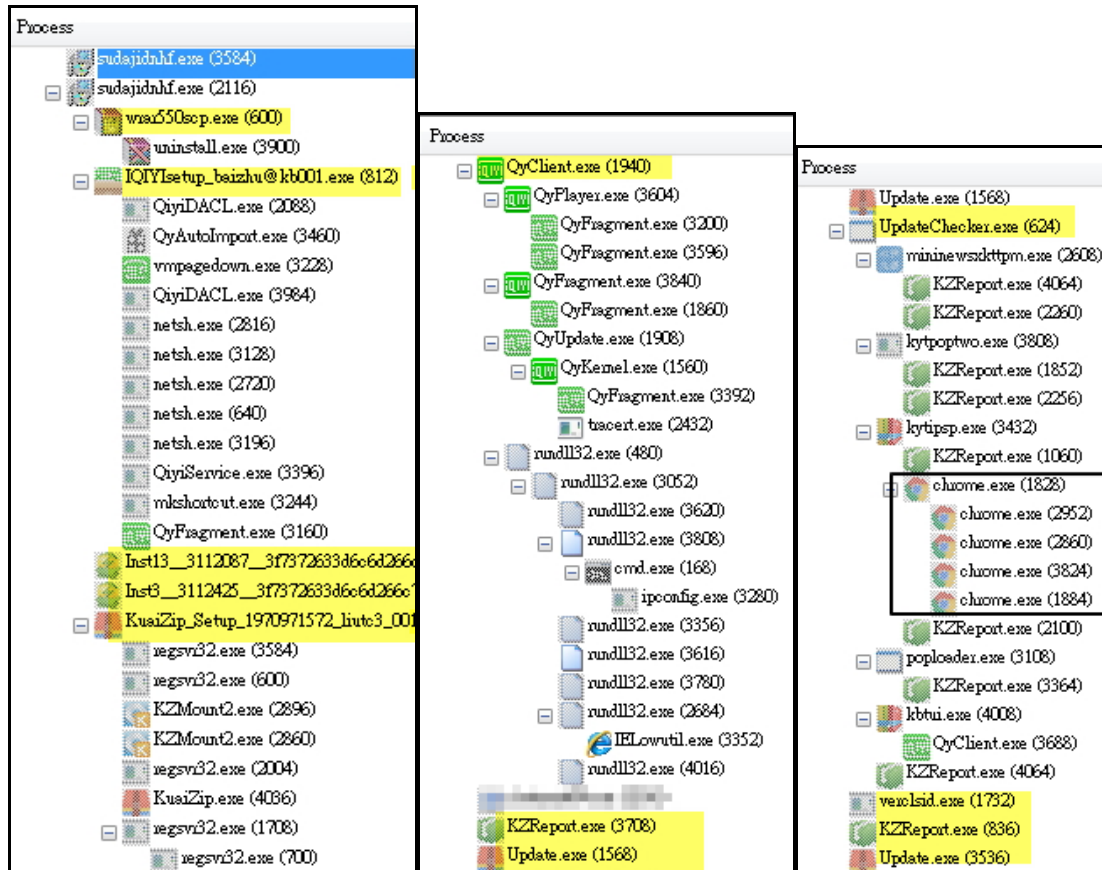


(2)將此兩個網址送至 virustotal 檢測，發現其惡意比例為 0/67。



11. 檢視背景程式運作情形，發現在執行 sudajidnhf.exe 後，除安裝 WinRAR 外，該程式陸續下載安裝與執行一些程式(如下列所示)，可見此程式 sudajidnhf.exe 為一個軟體下載器。

- (1) 愛奇藝安裝程式 IAIYIsetup_baizhu@kb001.exe
- (2) Inst13__3112087__3f7372633d6c6d266c733d6e31343463316364383939__68616f2e3336302e636e__0c70.exe
- (3) 速壓安裝包 KuaiZip_Setup_1970971572_liutc3_001.exe
- (4) 愛奇藝客戶端 QyClient.exe
- (5) KZreport.exe
- (6) 檢查更新程式 Update.exe 與快壓檢查更新 UpdateChecker.exe



12. 檢視背景程式執行狀況時，發現在執行 updatechecker.exe 時，會去更動 Chrome.exe 內容，開啟首頁時會連到大陸掏寶網站。

kytipsp.exe (3432)	小貼士	
KZReport.exe (1060)	KZReport	Kuazip Compression softw...
chrome.exe (1828)	Google Chrome	Google Inc.
chrome.exe (2952)	Google Chrome	Google Inc.
chrome.exe (2860)	Google Chrome	Google Inc.
chrome.exe (3824)	Google Chrome	Google Inc.
chrome.exe (1884)	Google Chrome	Google Inc.
KZReport.exe (2100)	KZReport	Kuazip Compression softw...

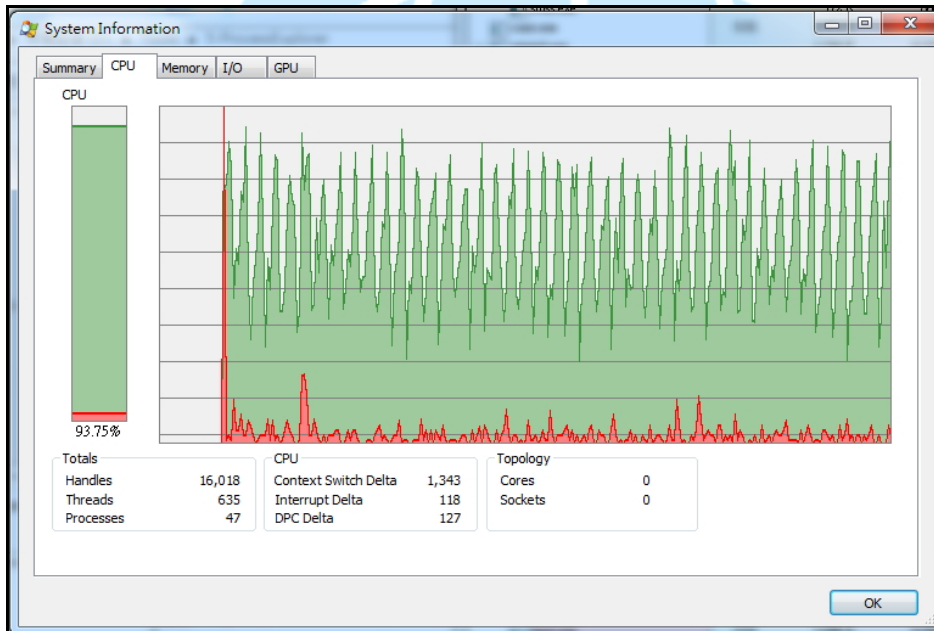
Description:	Google Chrome
Company:	Google Inc.
Path:	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
Command:	"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -- "https://s.click.taobao.com/pA0lkJw"

13. 用 AutoRun 工具檢視系統開機情形，發現有兩個程式 HCDNClient 與 QyClient 會在系統開機時自動執行，可見 sudajidnhf.exe 除了下載軟體安裝外，也會更改系統開機的設定。

Autoun Entry	Description	Publisher	Image Path	Timestamp
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2018/1/22 下午 04:02
<input checked="" type="checkbox"/> HCDNClient	IQIYI Video Helper	IQIYI.COM	c:\program files (x86)\iqiyi video\style\6.2.57.5300\qykemel.exe	2017/12/4 下午 06:10
<input checked="" type="checkbox"/> QyClient	爱奇艺视频客户端	爱奇艺	c:\program files (x86)\iqiyi video\style\6.2.57.5300\qyclient.exe	2017/12/7 下午 06:36

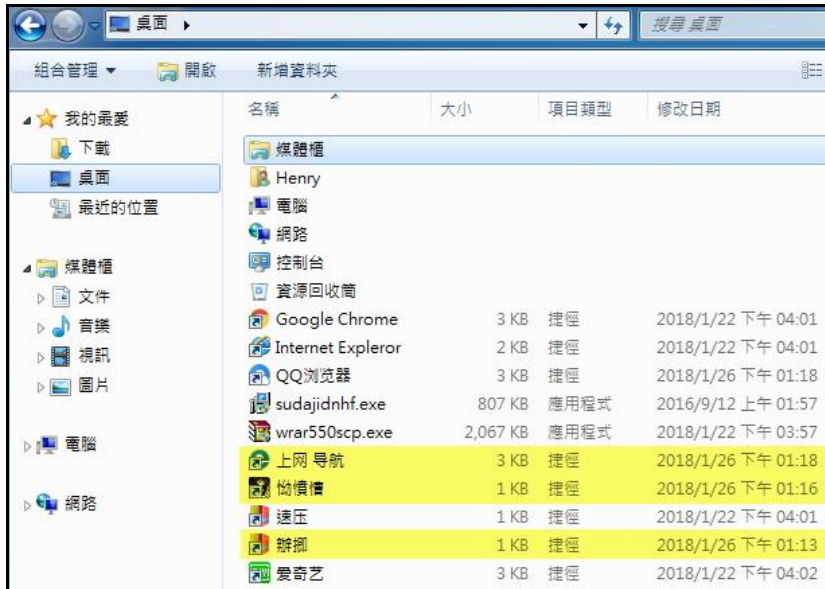
14. 當迷你新聞的程式在執行時，發現 CPU 使用率將近 100%，而且程式迷你新聞與小貼士的執行檔送至 Virustotal 檢測發現其惡意比例分別為 24/66 與 21/68，可見 sudajidnhf.exe 所下載安裝的軟體有惡意程式存在。

QyClient.exe (3024)	爱奇艺视频客户端	C:\Program Files (x86)\IQIYI Video\LS\style\6.2.57.5300\QyClient.exe	爱奇艺
QyPlayer.exe (2676)	爱奇艺视频播放器组件	C:\Program Files (x86)\IQIYI Video\LS\style\6.2.57.5300\QyPlayer.exe	爱奇艺
QyFragment.exe (836)	爱奇艺视频辅助程序	C:\Program Files (x86)\IQIYI Video\LS\style\6.2.57.5300\QyFragment.exe	爱奇艺
QyKernel.exe (1872)	IQIYI Video Helper	C:\Program Files (x86)\IQIYI Video\LS\style\6.2.57.5300\QyKernel.exe	IQIYI.COM
rundll32.exe (628)	Windows 主機處理程序 (Rundll32)	C:\Windows\SysWOW64\rundll32.exe	Microsoft Corporation
mininewsdkttam.exe (1436)	迷你新聞	C:\Users\Henry\AppData\Roaming\Kuaizip\mininewsdkttam.exe	
kytipsa.exe (3708)	小貼士	C:\Users\Henry\AppData\Roaming\Kuaizip\kytipsa.exe	



mininewsdkttam.exe	58.97	161,864 K	169,476 K	1436 迷你新聞	24/66
kytipsa.exe	< 0.01	4,164 K	9,548 K	3708 小貼士	21/68

15. 在 WinRAR 安裝完成後，發現該受測主機會在每隔一段時間後，不經使用者允許，自行連線並下載安裝一些程式。



III. 網路架構圖



1. 駭客將偽裝成WinRAR安裝程式的Quimonk木馬程式上傳至軟體下載網站或透過社交工程方式散播。
2. 受害者透過 APT 社交工程或軟體網站下載 WinRAR 安裝程式。
3. 受害者執行 WinRAR 安裝程式來安裝 WinRAR 軟體。
4. 受害主機對外連線 api.baizhu.cc 取得其他軟體下載安裝資訊。
5. WinRAR 程式安裝時自動安裝未經受害者授權安裝的惡意軟體於受害主機內。

IV. 建議與總結

1. 本個案類型資安事件之惡意程式會以下載器的形式，自行下載、安裝含有惡意軟體的程式，並且更改系統開機與現有瀏覽器首頁的設定，也會不定時執行更新與安裝新的軟體。
2. 本個案所安裝的軟體除了WinRAR外，還有愛奇藝的客戶端軟體包與一些小軟體，而有些軟體會讓CPU資源衝到100%。
3. 經本中心檢測發現，若受害者透過使用防毒軟體掃描、惡意軟體清除程式掃毒或將被安裝的軟體移除的方式來解決此問題，並無法將問題完全解決，因為無法完全地將被修改或安裝的多個程式還原或移除。因此，建議受害者將受害主機的資料備份後，重新安裝系統，這樣才能完全將該惡意程式所安裝或更動的軟體完全移除。