

Forum:[Hack Forums](#)

Thread: [My password were changed after downloading a RAT](#)

Badplum - December 8, 2014, 12:36 pm

Okay it was stupid of me I know. I downloaded a RAT by accident and I did a system restore. I though I was safe only to notice that my MC passwords were changed (I have 2 accounts) and I'm worried he will get my steam next. I dont even feel safe on the web right now until its removed. Ill have a link of were I downloaded it. Anyone know how to uninstall it? Im very nervous and fairly scared...

(removed)

Aura - December 8, 2014, 12:44 pm

Remove the download link if its infected. PM me it directly and I'll take a look to gather more information

-Hyperion - December 8, 2014, 6:20 pm

and you need to run a scan right away then change your passwords please follow these basic removal instructions <https://hackforums.net/showthread.php?tid=4558828> then post the logs. We can go more in depth after

Aura - December 8, 2014, 6:23 pm

(Dec 8, 2014 07:20 PM)-Hyperion Wrote: [\[CITE\]](#) and you need to run a scan right away then change your passwords please follow these basic removal instructions <https://hackforums.net/showthread.php?tid=4558828> then post the logs. We can go more in depth after

I got information about the file, its a DarkComet stub with a miner in it. Want screenshots and shit?

-Hyperion - December 8, 2014, 6:25 pm

(Dec 8, 2014 07:23 PM)Aur? Wrote: [\[CITE\]](#) I got information about the file, its a DarkComet stub with a miner in it. Want screenshots and shit?

if it was something good I might... hell even cryptolocker mundane now. Why don't you try running it on the new site I found and see what it finds as a test?

Aura - December 8, 2014, 6:27 pm

(Dec 8, 2014 07:25 PM)-Hyperion Wrote: [\[CITE\]](#) if it was something good I might... hell even cryptolocker mundane now. Why don't you try running it on the new site I found and see what it finds as a test?

Which new website? I'm not aware of any new website? And its a basic stub too. Killing the processes actually kills it and if you disable it in msconfig and delete the stubs, it doesn't comeback. Top tier skiddy material.

-Hyperion - December 8, 2014, 6:31 pm

<https://www.hybrid-analysis.com/> this one see what report it drops

Aura - December 8, 2014, 6:35 pm

(Dec 8, 2014 07:31 PM)-Hyperion Wrote: [\[CITE\]](#) <https://www.hybrid-analysis.com/> this one see what report it drops

Oh alright, let me boot up a VM.

Meanwhile:

<https://i.imgur.com/MgOH2NH.png>

<https://i.imgur.com/U0EiFnO.png>

<https://www.virustotal.com/en/file/a3cd7db1bd6e0eca2e735b073c1016df77a99e155ca3ef518e57a76e88c4e402/analysis/>

Badplum - December 8, 2014, 6:49 pm

Wait so it was only Dark comet? Nothings in my ms config that's suspicious I checked after running a scan and system restoring. If its not in the start up do you think im safe now? I changed my passwords but he got 1 of my mine craft accounts :(

"Whole Computer Scan"

"High severity";"6";"6";"0"

"Medium severity";"32";"32";"0"

"Scanned folders:";"Scan Whole Computer"

"Started:";"12/8/2014, 5:20:46 PM"

"Finished:";"12/8/2014, 6:48:45 PM"

"Scanned items:";"266848"

"Launched by:";"Badplum25"

"Name";"Description";"Status";"Status";"Priority"

"C:\Users\Badplum25\Desktop\Random RATS\Terraria.exe.exe";"Trojan horse
Downloader.Generic13.AWJB";"Secured";"Healed";"High"

"C:\Windows\system32\drivers\aswSnx.sys";"Inline hook win32k.sys W32pArgumentTable+0xBDC0
-> aswSnx.sys +0x2D9BC";"Secured";"Healed";"Medium"

"C:\Windows\system32\drivers\aswSnx.sys";"Inline hook win32k.sys
XLATEOBJ_cGetPalette+0x15CA4 -> aswSnx.sys +0x2F5C8";"Secured";"Healed";"Medium"

"C:\Windows\system32\drivers\aswSnx.sys";"Inline hook win32k.sys
XLATEOBJ_cGetPalette+0xF90 -> aswSnx.sys +0x2F614";"Secured";"Healed";"Medium"

"C:\Windows\system32\drivers\aswSnx.sys";"Inline hook win32k.sys W32pArgumentTable+0x8630
-> aswSnx.sys +0x2D6B0";"Secured";"Healed";"Medium"

"C:\Users\Badplum25\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\SIIT6E3K\BiTool[1].dll";"Adware Generic5.AOJI";"Secured";"Healed";"Medium"

"c:\Program Files (x86)\Spyrix Free Keylogger\spkl.exe (3048)";"Trojan horse
PSW.Generic12.ATPL";"Secured";"Healed";"High"

"C:\Windows\system32\drivers\aswSnx.sys";"Inline hook win32k.sys
W32pArgumentTable+0x12F34 -> aswSnx.sys +0x2E2F4";"Secured";"Healed";"Medium"

"C:\Windows\system32\drivers\aswSnx.sys";"Inline hook win32k.sys W32pArgumentTable+0xE368
-> aswSnx.sys +0x2E40C";"Secured";"Healed";"Medium"

"C:\Windows\system32\drivers\aswSnx.sys";"Inline hook win32k.sys
XLATEOBJ_cGetPalette+0x6440 -> aswSnx.sys +0x2FB28";"Secured";"Healed";"Medium"

"C:\Windows\system32\drivers\aswSnx.sys";"Inline hook win32k.sys W32pArgumentTable+0xB8A0
-> aswSnx.sys +0x2E190";"Secured";"Healed";"Medium"

"C:\Windows\system32\drivers\aswSnx.sys";"Inline hook win32k.sys EngFntCacheLookUp+0x8F20
-> aswSnx.sys +0x2F38C";"Secured";"Healed";"Medium"

"C:\Windows\system32\drivers\aswSnx.sys";"Inline hook win32k.sys
W32pArgumentTable+0x148E8 -> aswSnx.sys +0x2DBE0";"Secured";"Healed";"Medium"

"C:\Windows\system32\drivers\aswSnx.sys";"Inline hook win32k.sys W32pArgumentTable+0x6400
-> aswSnx.sys +0x2D760";"Secured";"Healed";"Medium"

"C:\Windows\system32\drivers\aswSnx.sys";"Inline hook win32k.sys W32pArgumentTable+0xBF2C
-> aswSnx.sys +0x2D938";"Secured";"Healed";"Medium"

"C:\Windows\system32\drivers\aswSnx.sys";"Inline hook win32k.sys EngPaint+0x914 ->
aswSnx.sys +0x2FE90";"Secured";"Healed";"Medium"

"C:\Users\Badplum25\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\R5WNQS50\setup[1].exe";"Found
 MalSign.Generic.2E0";"Secured";"Healed";"Medium"
 "C:\Windows\system32\drivers\aswSnx.sys";"Inline hook win32k.sys W32pArgumentTable+0x5AF8
 -> aswSnx.sys +0x2E438";"Secured";"Healed";"Medium"
 "C:\Windows\system32\drivers\aswSnx.sys";"Inline hook win32k.sys EngSetPointerTag+0x130 ->
 aswSnx.sys +0x30190";"Secured";"Healed";"Medium"
 "C:\Users\Badplum25\Desktop\Darkcomet\DarkComet.exe";"Trojan horse
 Downloader.Generic13.AWJB.dropper";"Secured";"Healed";"High"
 "C:\Windows\system32\drivers\aswSnx.sys";"Inline hook win32k.sys W32pArgumentTable+0x25DC
 -> aswSnx.sys +0x2DDF0";"Secured";"Healed";"Medium"
 "C:\Windows\system32\drivers\aswSnx.sys";"Inline hook win32k.sys W32pArgumentTable+0x81EC
 -> aswSnx.sys +0x2DB00";"Secured";"Healed";"Medium"
 "C:\Windows\system32\drivers\aswSnx.sys";"Inline hook win32k.sys
 STROBJ_fxBreakExtra+0x1E00 -> aswSnx.sys +0x3000C";"Secured";"Healed";"Medium"
 "C:\Windows\system32\drivers\aswSnx.sys";"Inline hook win32k.sys
 EngRestoreFloatingPointState+0x3EF8 -> aswSnx.sys +0x2D570";"Secured";"Healed";"Medium"
 "C:\Windows\system32\drivers\aswSnx.sys";"Inline hook win32k.sys W32pArgumentTable+0xE1EC
 -> aswSnx.sys +0x2E568";"Secured";"Healed";"Medium"
 "C:\Windows\system32\drivers\aswSnx.sys";"Inline hook win32k.sys
 EngRestoreFloatingPointState+0x1150 -> aswSnx.sys +0x2F568";"Secured";"Healed";"Medium"
 "C:\Windows\system32\drivers\aswSnx.sys";"Inline hook win32k.sys W32pArgumentTable+0x5788
 -> aswSnx.sys +0x2DCC0";"Secured";"Healed";"Medium"
 "C:\Windows\system32\drivers\aswSnx.sys";"Inline hook win32k.sys W32pArgumentTable+0x46C4
 -> aswSnx.sys +0x2D180";"Secured";"Healed";"Medium"
 "C:\Windows\system32\drivers\aswSnx.sys";"Inline hook win32k.sys
 W32pArgumentTable+0x7CCC -> aswSnx.sys +0x2E594";"Secured";"Healed";"Medium"
 "C:\Windows\system32\drivers\aswSnx.sys";"Inline hook win32k.sys
 EngFntCacheLookUp+0x1240C -> aswSnx.sys +0x2D390";"Secured";"Healed";"Medium"
 "C:\Users\Badplum25\Desktop\Darkcomet\Celesty Binder\Celesty.exe";"Trojan horse
 Generic23.AVVP.dropper";"Secured";"Healed";"High"
 "C:\Windows\system32\drivers\aswSnx.sys";"Inline hook win32k.sys W32pArgumentTable+0x6B5C
 -> aswSnx.sys +0x2E3E0";"Secured";"Healed";"Medium"
 "C:\Windows\system32\drivers\aswSnx.sys";"Inline hook win32k.sys W32pArgumentTable+0x9188
 -> aswSnx.sys +0x2E6BC";"Secured";"Healed";"Medium"
 "C:\Windows\system32\drivers\aswSnx.sys";"Inline hook win32k.sys EngBitBlt+0x606C ->
 aswSnx.sys +0x2E174";"Secured";"Healed";"Medium"
 "C:\Users\Badplum25\Desktop\Batch files\Skype.exe";"Found
 Win32/DH{ATZCKQ}";"Secured";"Healed";"High"
 "C:\Windows\system32\drivers\aswSnx.sys";"Inline hook win32k.sys W32pArgumentTable+0x2670
 -> aswSnx.sys +0x2DF04";"Secured";"Healed";"Medium"
 "C:\Games\Watch Dogs\bin\Watch_Dogs.exe";"Virus found
 Win32/Blacked";"Secured";"Healed";"High"
 "C:\Windows\system32\drivers\aswSnx.sys";"Inline hook win32k.sys EngCopyBits+0x16D8 ->
 aswSnx.sys +0x2F500";"Secured";"Healed";"Medium"

Heres my log

Aura - December 8, 2014, 6:50 pm

(Dec 8, 2014 07:49 PM)Badplum Wrote: [CITE](#) Wait so it was only Dark comet? Nothings in my ms config that's suspicious I checked after running a scan and system restoring. If its not in the start up do you think im safe now? I changed my passwords but he got 1 of my mine craft accounts :(I'm running the stub again in my VM to see if it have the same behavior. But the VirusTotal (and my

analysis) confirm that it's indeed a skiddy DarkComet RAT stub with a CPUMiner feature.
Well, that's some detailed analysis indeed, the scan time is just extremely long:

<https://www.hybrid-analysis.com/sample/a3cd7db1bd6e0eca2e735b073c1016df77a99e155ca3ef518e57a76e88c4e402/>

-Hyperion - December 8, 2014, 7:11 pm

did you follow all the directions OP? if so then change your passwords

Aura - December 8, 2014, 8:28 pm

(Dec 8, 2014 08:11 PM)-Hyperion Wrote: [\[CITE\]](#) did you follow all the directions OP? if so then change your passwords

Along with that, if possible, enable 2FA (Two-Factor Authentication) on every accounts you can to drastically increase the security of these accounts.

AcidBurnTrump - December 8, 2014, 8:55 pm

whats the link where you download the rat i would like to have it

add on skype AcidBurnTrump

Aura - December 8, 2014, 8:56 pm

(Dec 8, 2014 09:55 PM)AcidBurnTrump Wrote: [\[CITE\]](#) whats the link where you download the rat i would like to have it

add on skype AcidBurnTrump

I have it, why would you like to have it?

Accelerator. - December 8, 2014, 9:22 pm

Try Darkcomet Remover?

Wasn't it made by the same guy who made Darkcomet?

Aura - December 9, 2014, 4:52 am

(Dec 8, 2014 10:22 PM)Ken Kaneki. Wrote: [\[CITE\]](#) Try Darkcomet Remover?

Wasn't it made by the same guy who made Darkcomet?

No it wasn't plus this tool is completely useless. You should never use these small removal utilities nor rely on them.

Badplum - December 9, 2014, 5:07 am

Yes I did everything in the OP -Hyperion

Aura - December 9, 2014, 5:59 am

(Dec 9, 2014 06:07 AM)Badplum Wrote: [\[CITE\]](#) Yes I did everything in the OP -Hyperion

Is it possible to post all the logs that you got from running these scans, like asked in the tutorial?

Badplum - December 9, 2014, 12:36 pm

I don't have them anymore, although, if the RAT is not in ms config then does that mean its gone?

Non of them found anything besides the malware-bytes and the AdwCleaner.

Aura - December 9, 2014, 1:25 pm

(Dec 9, 2014 01:36 PM)Badplum Wrote: [\[CITE\]](#) I don't have them anymore, although, if the RAT is not in ms config then does that mean its gone?

Non of them found anything besides the malware-bytes and the AdwCleaner.

The stub you sent me was showing in msconfig, so if it doesn't show up anymore, I'm tempted to say that it's gone, however I can't be 100% sure of it. Honestly, I think it's gone but without me checking it manually, I can't be 100% sure.

OH, and run [TFC](#). Because the executables (and shortcuts) were in the %temp% folder, they'll be deleted by it.

Badplum - December 10, 2014, 3:12 pm

kk Thanks for the help. I ran TFC. (removed 300 MB) I'm fairly sure that the RAT is gone sense nothing weird has been happening and I downloaded the RAT again (On my very old computer) with the AVG virus scan. AVG detected the RAT after I downloaded it again so It shouldn't be on my computer anymore. Again thank you and Hyperion A LOT! (I'm surprised I only lost one old unused 20 dollar minecraft account and not my \$300 worth of games spent on steam.) :)

Aura - December 10, 2014, 3:13 pm

(Dec 10, 2014 04:12 PM)Badplum Wrote: [\[CITE\]](#) kk Thanks for the help. I ran TFC. (removed 300 MB) I'm fairly sure that the RAT is gone sense nothing weird has been happening and I downloaded the RAT again (On my very old computer) with the AVG virus scan. AVG detected the RAT after I downloaded it again so It shouldn't be on my computer anymore. Again thank you and Hyperion A LOT! (I'm surprised I only lost one old unused 20 dollar minecraft account and not my \$300 worth of games spent on steam.) :)

All good, if I were you, I would swap AVG for Avira, way better free Antivirus but it's up to you. Glad that we could be of assistance.