

Forum:[Hack Forums](#)

Thread: [I accidentally infect myself with LuminosityLink + GhostCrypter](#)

Puffer Fish - April 17, 2016, 4:35 pm

Yes, hypothetically i accidentally opened my LuminosityLink stub crypted in GhostCrypter.

GhostCrypter Settings:

- Mutex
- Hidden on Startup
- Remove Assembly

LuminosityLink Settings:

- Process Persistence Only

I uninstalled myself in LL client but i still got this annoying random mutex/process. How do i remove this? (abvvxc2511266671sde.exe, bqauhhjsj2sa.exe) it's random. When it gets analyze by AVAST, it will be deleted and come back again with new random name.

_Valor - April 17, 2016, 5:56 pm

Hello, my name is _Valor and I'm going to try to help you the best that I can.

As you explained in your post, the executable is being detected by avast? That's a very good sign.

Now, to kill the processes that are produced, run a tool called rkill(Click [here](#) to download it). Rkill will kill all processes unknown to the system, and produce a log. I'd like you to:Run rkill

run a full scan with avast! Antivirus

Upload the rkill log to pastebin(make sure it's set to private/unlisted)

Send me the avast! log that was produced by the scan(you can just tell me what it detects)

Puffer Fish - April 17, 2016, 6:11 pm

(Apr 17, 2016 05:56 PM)_Valor Wrote: [\[CITE\]](#) Hello, my name is _Valor and I'm going to try to help you the best that I can.

As you explained in your post, the executable is being detected by avast? That's a very good sign.

Now, to kill the processes that are produced, run a tool called rkill(Click [here](#) to download it). Rkill will kill all processes unknown to the system, and produce a log. I'd like you to:Run rkill

run a full scan with avast! Antivirus

Upload the rkill log to pastebin(make sure it's set to private/unlisted)

Send me the avast! log that was produced by the scan(you can just tell me what it detects)

rkill logs: <http://pastebin.com/XUvqDEjx>

AVAST: (Avast can't detect it as i used crypter on my stub, thus my pc is clean)

ProtectNull™ - April 17, 2016, 6:22 pm

(Apr 17, 2016 06:11 PM)Norous Wrote: [\[CITE\]](#) rkill logs: <http://pastebin.com/XUvqDEjx>

AVAST: (Avast can't detect it as i used crypter on my stub, thus my pc is clean)

Download [Farbar Recovery Scan Tool](#) and save it to your Desktop.

Farbar Recovery Scanning Tool

Right click to run as administrator (XP users click run after receipt of Windows Security Warning - Open File). When the tool opens click Yes to disclaimer.

Press Scan button.

It will produce a log called FRST.txt in the same directory the tool is run from.

Please copy and paste the log back here

The first time the tool is run it generates another log (Addition.txt - also located in the same directory as FRST.exe/FRST64.exe). Please also paste that along with the FRST.txt into your reply.

Puffer Fish - April 17, 2016, 6:41 pm

(Apr 17, 2016 06:22 PM)ProtectNull™ Wrote: [\[CITE\]](#) Download [Farbar Recovery Scan Tool](#) and save it to your Desktop.

Farbar Recovery Scanning Tool

Right click to run as administrator (XP users click run after receipt of Windows Security Warning - Open File). When the tool opens click Yes to disclaimer.

Press Scan button.

It will produce a log called FRST.txt in the same directory the tool is run from.

Please copy and paste the log back here

The first time the tool is run it generates another log (Addition.txt - also located in the same directory as FRST.exe/FRST64.exe). Please also paste that along with the FRST.txt into your reply.

FRST: <http://pastebin.com/2hvDuvYs>

I disabled my AVAST because it's keep detecting the random weird .exe, It's annoying. I already deleted myself in LuminosityLink.

(Apr 17, 2016 06:41 PM)Norous Wrote: [\[CITE\]](#) FRST: <http://pastebin.com/2hvDuvYs>

I disabled my AVAST because it's keep detecting the random weird .exe, It's annoying. I already deleted myself in LuminosityLink.

Please open notepad and copy paste the contents in the codebox below. (Do not include "Code:" tags)

Code start

CloseProcesses:

HKU\S-1-5-21-563482115-3036595567-2997201845-1001\...\RunOnce: [Microsoft Corporation WddblKiPaDSUGKHd] => C:\Users\DEPP\AppData\Roaming\WddblKiPaDSUGKHd.exe [1595392 2016-04-18] ()

GroupPolicy: Restriction - Chrome <===== ATTENTION

GroupPolicyScripts: Restriction <===== ATTENTION

GroupPolicyScripts\User: Restriction <===== ATTENTION

CHR HKLM\SOFTWARE\Policies\Google: Restriction <===== ATTENTION

CHR HKU\S-1-5-21-563482115-3036595567-2997201845-1001\SOFTWARE\Policies\Google: Restriction <===== ATTENTION

Toolbar: HKU\S-1-5-21-563482115-3036595567-2997201845-1001 -> No Name - {2318C2B1-4965-11D4-9B18-009027A5CD4F} - No File

BHO: No Name -> {C35B7206-62EB-F808-5475-18A6FDE7DD94} -> No File

SearchScopes: HKLM -> DefaultScope {E9410C70-B6AE-41FF-AB71-32F4B279EA5F} URL = hxxp://searchinterneat-a.akamaihd.net/s?eq=U0EeE1xZE1oZB1ZEfQwKUV1JEAYTbQFdWV9cFQAbdRRaVfJDFFB1Q5dUF0QQw0WJh9aFQQTSEcFME0FCFwEURNNfX1REloeV1BROXhIEQ==&q={searchTerms}

SearchScopes: HKLM -> OldSearch URL = hxxps://www.google.com/search?trackid=sp-006&q={searchTerms}
SearchScopes: HKLM -> {6586d803-df30-46d3-a89a-4136c8571d45} URL = hxxp://www.palikan.com/results.php?f=4&a=bfp_coinisre_16_09&cd=2XzuyEtN2Y1L1Qzu0AtD0FtA0CtC0CyEtCtBtBtCtDzy0EyEtN0D0Tzu0StCyDtByEtN1L2XzutAtFtCzztFtCtFyDtN1L1Czu1ByEtN1L1G1B1V1N2Y1L1Qzu2StByD0A0CyC0DtAtBtGtBtDtA0BtG0B0Fzy0DtGtBtDzy0FtGtBtCzz0CtByE0DtDyD0B0CtC2QtN1M1F1B2Z1V1N2Y1L1Qzu2S0AzytDtByD0CtD0FtGtA0D0CzztGyEtAzytDtG0B yBtDyDtG0A0CyB0F0CyC0AyB0F0CtDyB2QtN0A0LzutB&cr=343473937&ir=&q={searchTerms}

SearchScopes: HKLM -> {E9410C70-B6AE-41FF-AB71-32F4B279EA5F} URL = hxxp://searchinterneat-a.akamaihd.net/s?eq=U0EeE1xZE1oZB1ZEfQwKUV1JEAYTbQFdWV9cFQAbdRRaVfJDFFB1Q5dUF0QQw0WJh9aFQQTSEcFME0FCFwEURNNfX1REloeV1BROXhIEQ==&q={searchTerms}

SearchScopes: HKU\S-1-5-21-563482115-3036595567-2997201845-1001 -> DefaultScope {E9410C70-B6AE-41FF-AB71-32F4B279EA5F} URL = hxxp://searchinterneat-a.akamaihd.net/s?eq=U0EeE1xZE1oZB1ZEfQwKUV1JEAYTbQFdWV9cFQAbdRRaVfJDFFB1Q5dUF0QQw0WJh9aFQQTSEcFME0FCFwEURNNfX1REloeV1BROXhIEQ==&q={searchTerms}

SearchScopes: HKU\S-1-5-21-563482115-3036595567-2997201845-1001 -> OldSearch URL = hxxps://www.google.com/search?trackid=sp-006&q={searchTerms}

SearchScopes: HKU\S-1-5-21-563482115-3036595567-2997201845-1001 -> {0ECD796-C2DC-4d79-A620-CCE0C0A66CC9} URL = hxxp://www.delta-search.com/?q={searchTerms}&affID=121631&babsrc=SP_ss&mnrId=D07C002522987BAD

SearchScopes: HKU\S-1-5-21-563482115-3036595567-2997201845-1001 -> {2802DE9B-C921-45D8-B15E-2F5CFEEB6301} URL = hxxps://ph.search.yahoo.com/search?fr=chr-greentree_ie&ei=utf-8&ilc=12&type=830633&p={searchTerms}

SearchScopes: HKU\S-1-5-21-563482115-3036595567-2997201845-1001 ->
{6586d803-df30-46d3-a89a-4136c8571d45} URL =
hxxp://www.palikan.com/results.php?f=4&a=bfp_coinisre_16_09&cd=2XzuyEtN2Y1L1Qzu0AtD0FtA
0CtC0CyEtCtBtBtCtDzy0EyEtN0D0Tzu0StCyDtByEtN1L2XzutAtFtCzztFtCtFyDtN1L1Czu1ByEtN1L
1G1B1V1N2Y1L1Qzu2StByD0A0CyC0DtAtBtGtBtDtA0BtG0B0Fzy0DtGtBtDzy0FtGtBtCzz0CtByE0
DtDyD0B0CtC2QtN1M1F1B2Z1V1N2Y1L1Qzu2S0AzytDtByD0CtD0FtGtA0D0CzztGyEtAzytDtG0B
yBtDyDtG0A0CyB0F0CyC0AyB0F0CtDyB2QtN0A0LzutB&cr=343473937&ir=&q={searchTerms}
SearchScopes: HKU\S-1-5-21-563482115-3036595567-2997201845-1001 ->
{883A7FD9-E6BB-481F-A75D-8ABA018A7BB5} URL =
hxxp://www.mysearchresults.com/search?c=2402&t=15&q={searchTerms}
SearchScopes: HKU\S-1-5-21-563482115-3036595567-2997201845-1001 ->
{E9410C70-B6AE-41FF-AB71-32F4B279EA5F} URL =
hxxp://searchinterneat-a.akamaihd.net/s?eq=U0EeE1xZE1oZB1ZEfQwKUV1JEAYTbQFdWV9cFQ
AbdRRaVfJDFFBtIQ5dUF0QQw0WJh9aFQQTSEcFME0FCFwEURNNfX1REloeV1BROXhIEQ==&
q={searchTerms}
BHO: No Name -> {0055C089-8582-441B-A0BF-17B458C2A3A8} -> No File
HKLM\Software\Microsoft\Internet Explorer\Main,Start Page =
hxxp://searchinterneat-a.akamaihd.net/h?eq=U0EeCFZVBB8SRggWcgIcWQhCERgbJQFeTA1EGQ
AOIgxawRQVQ1QUJQhcAftJFFMFik0FA1ADB0VXfVBdFEIXTwhnKUpbDk8UU0xiMEk=
HKLM\Software\Microsoft\Internet Explorer\Main,Search Page =
hxxps://www.google.com/search?trackid=sp-006&q={searchTerms}
HKLM\Software\Microsoft\Internet Explorer\Main,Default_Page_URL =
HKLM\Software\Microsoft\Internet Explorer\Main,Default_Search_URL =
HKU\S-1-5-21-563482115-3036595567-2997201845-1001\Software\Microsoft\Internet
Explorer\Main,Search Page = hxxps://www.google.com/search?trackid=sp-006&q={searchTerms}
FF Plugin: @microsoft.com/GENUINE -> disabled [No File]
FF user.js: detected! =>
C:\Users\DEPP\AppData\Roaming\Mozilla\Firefox\Profiles\9ee226kc.default\user.js [2016-01-10]
FF HKU\S-1-5-21-563482115-3036595567-2997201845-1001\...\Firefox\Extensions:
[mozilla_cc@internetdownloadmanager.com] - C:\Users\DEPP\AppData\Roaming\IDM\idmmzcc5
=> not found
FF HKU\S-1-5-21-563482115-3036595567-2997201845-1001\...\SeaMonkey\Extensions:
[mozilla_cc@internetdownloadmanager.com] - C:\Users\DEPP\AppData\Roaming\IDM\idmmzcc5
=> not found
C:\Users\DEPP\AppData\Roaming\WddblKiPaDSUGKHd.exe
C:\ProgramData\085d0e68c7b0c248384148018c7afe1bc9b2a42d
CustomCLSID:
HKU\S-1-5-21-563482115-3036595567-2997201845-1001_Classes\CLSID\{F5DF8D65-559D-4b75-
8562-5302BD2F5F20}\InprocServer32 ->
C:\Users\DEPP\AppData\Roaming\2XClient\TuxClientSystem.dll => No File
CustomCLSID:
HKU\S-1-5-21-563482115-3036595567-2997201845-1001_Classes\CLSID\{A2DF06F9-A21A-44A8
-8A99-8B9C84F29160}\localserver32 ->
C:\Users\DEPP\AppData\Local\Chromium\Application\46.0.2472.0\delegate_execute.exe (The
Chromium Authors) <==== ATTENTION
CustomCLSID:
HKU\S-1-5-21-563482115-3036595567-2997201845-1001_Classes\CLSID\{5E71E4F3-E8C7-4906-
9626-973E418762B6}\InprocServer32 ->
C:\Users\DEPP\AppData\Local\Facebook\Update\1.2.205.0\goopdate.dll (Facebook Inc.)
CustomCLSID:
HKU\S-1-5-21-563482115-3036595567-2997201845-1001_Classes\CLSID\{1FD1FE74-9E3C-4C1
C-AEEB-AAB592AD770F}\localserver32 ->
C:\Users\DEPP\AppData\Local\Facebook\Update\FacebookUpdate.exe (Facebook Inc.)

Task: {CE65177F-2C1E-418B-82A0-A70336985643} -
System32\Tasks\FacebookUpdateTaskUserS-1-5-21-563482115-3036595567-2997201845-1001C
ore => C:\Users\DEPP\AppData\Local\Facebook\Update\FacebookUpdate.exe [2014-04-30]
(Facebook Inc.)
Task:
C:\Windows\Tasks\FacebookUpdateTaskUserS-1-5-21-563482115-3036595567-2997201845-1001
Core.job => C:\Users\DEPP\AppData\Local\Facebook\Update\FacebookUpdate.exe
Task:
C:\Windows\Tasks\FacebookUpdateTaskUserS-1-5-21-563482115-3036595567-2997201845-1001
UA.job => C:\Users\DEPP\AppData\Local\Facebook\Update\FacebookUpdate.exe
FirewallRules: [TCP Query
User{E2F3C37A-3294-4204-8FFB-66B132298E2A}C:\users\depp\desktop\dark-comet
v5.3\dark-comet v5.3\darkcomet.exe] => (Allow) C:\users\depp\desktop\dark-comet v5.3\dark-comet
v5.3\darkcomet.exe
FirewallRules: [UDP Query
User{1E0487C9-09E5-457E-AC68-1E434AA5049C}C:\users\depp\desktop\dark-comet
v5.3\dark-comet v5.3\darkcomet.exe] => (Allow) C:\users\depp\desktop\dark-comet v5.3\dark-comet
v5.3\darkcomet.exe
FirewallRules: [{FA974AEF-3545-4308-8175-F64ACE4E507E}] => (Allow)
C:\Users\DEPP\AppData\Local\Facebook\Video\Skype\FacebookVideoCalling.exe
FirewallRules: [TCP Query
User{B46E5783-6207-4B14-BE71-D2C22E449D22}C:\users\depp\appdata\local\temp\7zo938a.tmp\l
isten.exe] => (Allow) C:\users\depp\appdata\local\temp\7zo938a.tmp\listen.exe
FirewallRules: [UDP Query
User{331CD783-A727-4B54-959F-E6380D79C2CC}C:\users\depp\appdata\local\temp\7zo938a.tmp
\listen.exe] => (Allow) C:\users\depp\appdata\local\temp\7zo938a.tmp\listen.exe
FirewallRules: [TCP Query
User{BD5A401C-81E9-4D99-9A01-F20C6D4ACF21}C:\users\depp\desktop\pack\luminosity.exe] =>
(Allow) C:\users\depp\desktop\pack\luminosity.exe
FirewallRules: [UDP Query
User{F1E0593D-3610-424A-BA99-B8A293A1E6A1}C:\users\depp\desktop\pack\luminosity.exe] =>
(Allow) C:\users\depp\desktop\pack\luminosity.exe
FirewallRules: [TCP Query
User{94876418-B8BC-406C-A1DE-5CF824906208}C:\users\depp\desktop\p\luminosity.exe] =>
(Allow) C:\users\depp\desktop\p\luminosity.exe
FirewallRules: [UDP Query
User{4274D4BC-BF87-4042-A15A-DD35A5FB9F73}C:\users\depp\desktop\p\luminosity.exe] =>
(Allow) C:\users\depp\desktop\p\luminosity.exe
FirewallRules: [{2F1D295E-630E-493A-A8E5-115E7D347806}] => (Allow) LPort=3547
EmptyTemp:
Hosts:

Click File, Save As and enter fixlist.txt as the file name.

NOTE. It's important that both files, FRST/FRST64 and fixlist.txt are in the same location or the fix will not work.

NOTICE: This script was written specifically for this user, for use on that particular machine. Running this on another machine may cause damage to your operating system

Run FRST/FRST64 and press the Fix button just once and wait.
If for some reason the tool needs a restart, please make sure you let the system restart normally.
After that let the tool complete its run.

When finished FRST will generate a log on the Desktop (Fixlog.txt). Please post it to your reply.

_Valor - April 17, 2016, 7:17 pm

Follow the instructions that ProtectNull™ provided you with.

Puffer Fish - April 17, 2016, 7:25 pm

(Apr 17, 2016 07:17 PM)_Valor Wrote: [\[CITE\]](#) Follow the instructions that ProtectNull™ provided you with.

Fixlogs

Here you go: <http://pastebin.com/LZvGX5Ji>

ProtectNull™ - April 17, 2016, 7:28 pm

(Apr 17, 2016 07:25 PM)Norous Wrote: [\[CITE\]](#) Fixlogs

Here you go: <http://pastebin.com/LZvGX5Ji>

Please do a FRST log again. ?

sugarboi007 - April 18, 2016, 6:33 am

is ghost crypter very good for luminosity link? i hav no victims wen i crypt and send with cyberseal

memesaregreat - April 18, 2016, 7:12 am

sugarboi wrong section.

Not sure if trolling

Puffer Fish - April 18, 2016, 7:33 am

(Apr 17, 2016 07:28 PM)ProtectNull™ Wrote: [\[CITE\]](#) Please do a FRST log again. ?

Indeed, its finally removed i used kapersky ,rkill and frst scanner, Thank you for spending your time for me to fix this issue, i appreciate it so much, +1 :)

ProtectNull™ - April 18, 2016, 2:10 pm

(Apr 18, 2016 07:33 AM)Norous Wrote: [\[CITE\]](#) Indeed, its finally removed i used kapersky ,rkill and frst scanner, Thank you for spending your time for me to fix this issue, i appreciate it so much, +1 :)

Not a problem.

Please close thread.

Nadisty - April 18, 2016, 2:12 pm

(Apr 18, 2016 07:12 AM)memesaregreat Wrote: [\[CITE\]](#) sugarboi wrong section.

Not sure if trolling

I can't stop laughing at that lmao