

Forum:[Hack Forums](#)

Thread: [\[njRat\] \[ALERT\] I downloaded njRAT by the link on HF. HACKED. \[UPDATED info\]](#)

Dafuq - May 20, 2015, 3:08 am

As soon as I downloaded it, and ran it, i saw a error, had my AV disabled.

Within few mins my cursor started moving, and pages started refreshing. Definitely hacked. 100% sure!!

Would like to submit the file for testing in case somebody is interested.

I tried posting this on his Thread, but it wont let me post. Had to make a new thread!!

download link for both s/w i was using.

<http://ge.tt/6wLWnIG2>

Okay, so now i get a link via PM claiming this is the original njRAT -

<http://up.dev-point.com/downloadf-844b1a166eab1-rar.html>

check the md5, size and whatever u people want.

Dickleson - May 20, 2015, 3:10 am

You should 100% post in here [Malware, Rat, and Virus Removal](#)

Ask for a system check-up.

Koekert - May 20, 2015, 3:11 am

Couldn't it have been something you had recently downloaded before? Since Vuln's thread has 77 pages and I think you're the first to experience problems

Dafuq - May 20, 2015, 3:15 am

(May 20, 2015 03:11 AM)debeste95 Wrote: [\[CITE\]](#) Couldn't it have been something you had recently downloaded before? Since Vuln's thread has 77 pages and I think you're the first to experience problems

I just downloaded 2 things

1. VPN client

2. njRat

VPN client is obviously appearing to be clean, but I would get it checked as well, in case its the one.

but Somehow I'm unable to post on xVulnerables thread, thats why i find it fishy!!

(May 20, 2015 03:10 AM)Wallahi Wrote: [\[CITE\]](#) You should 100% post in here [Malware, Rat, and Virus Removal](#)

Ask for a system check-up.

Made a thread there, thank u!

Meow - May 20, 2015, 3:17 am

lol wtf

Dickleson - May 20, 2015, 3:19 am

(May 20, 2015 03:17 AM)Meow. Wrote: [\[CITE\]](#)

lol wtf

That's not indicating that it is dangerous to the downloader though.

That's simply because the file is a RAT. Even the UI and stuff gets classed as malware because of the coding behind it all.

Lovesosa - May 20, 2015, 3:19 am

(May 20, 2015 03:17 AM)Meow. Wrote: [\[CITE\]](#)

lol wtf

thats normal ofc the program is an rat, so it will be deected as an malware.

Meow - May 20, 2015, 3:20 am

(May 20, 2015 03:19 AM)Mitzz Wrote: [\[CITE\]](#) thats normal ofc the program is an rat, so it will be deected as an malware.

"I want to download malware" ??

Koekert - May 20, 2015, 3:21 am

(May 20, 2015 03:15 AM)Dafuq. Wrote: [\[CITE\]](#) I just downloaded 2 things

1. VPN client

2. njRat

VPN client is obviously appearing to be clean, but I would get it checked as well, in case its the one.

but Somehow I'm unable to post on xVulnerables thread, thats why i find it fishy!!

Made a thread there, thank u!You mean you can't post on your pc? Because your post did show up, which I guess you posted via your phone.

Lovesosa - May 20, 2015, 3:24 am

somebody test this shit with an vm , i dont have an vm otherwise i wud.

Dafuq - May 20, 2015, 3:27 am

(May 20, 2015 03:24 AM)Mitzz Wrote: [\[CITE\]](#) somebody test this shit with an vm , i dont have an vm otherwise i wud.

I would appreciate if someone can test it, coz then we will be sure.

gherardus - May 20, 2015, 3:28 am

if the file is crypted it could not work on a vm.

BahNahNah - May 20, 2015, 3:31 am

I ran it sandboxie and nothing abnormal.

There is a possibility that it wont execute the trojan (if it is infected) if it detects a vm/sandboxie.

Dafuq - May 20, 2015, 3:32 am

(May 20, 2015 03:31 AM)BahNahNah Wrote: [\[CITE\]](#) I ran it sandboxie and nothing abnormal.

There is a possibility that it wont execute the trojan (if it is infected) if it detects a vm/sandboxie.

I ran it on my System, coz xVulnerables was supposedly "HQ" and "Trusted"

I am indeed shocked.

BahNahNah - May 20, 2015, 3:34 am

(May 20, 2015 03:32 AM)Dafuq. Wrote: [\[CITE\]](#) I ran it on my System, coz xVulnerables was supposedly "HQ" and "Trusted"

I am indeed shocked.

Download autoruns and see if there is anything abnormal in your startup (check for things in Appdata/temp)

<https://technet.microsoft.com/en-us/sysinternals/bb963902.aspx>

Lovesosa - May 20, 2015, 3:35 am

well this doesnt say anything it just 1 report, we gotta wait for more reports to make sure is backdoored.

Dafuq - May 20, 2015, 3:36 am

(May 20, 2015 03:34 AM)BahNahNah Wrote: [\[CITE\]](#) Download autoruns and see if there is anything abnormal in your startup (check for things in Appdata/temp)

<https://technet.microsoft.com/en-us/sysinternals/bb963902.aspx>

i'm already proceeding as per MRT's instructions.

Wi??iam - May 20, 2015, 3:39 am

So xVulnerable waited years of hard work to helping people just so he could move your cursor and refresh your pages.

seems legit

Dafuq - May 20, 2015, 3:45 am

(May 20, 2015 03:39 AM)PwnyCode. Wrote: [\[CITE\]](#) So xVulnerable waited years of hard work to helping people just so he could move your cursor and refresh your pages.

seems legit

I am not here to pick a fight with You or xVulnerables or anybody else. I just posted whatever happened.

240sx - May 20, 2015, 3:47 am

You can just use <http://malwr.com> should work on there to test it.

Dafuq - May 20, 2015, 3:48 am

(May 20, 2015 03:47 AM)Badger Wrote: [\[CITE\]](#) You can just use <http://malwr.com> should work on there to test it.

What's this? I am supposed to upload the file here?

Meow - May 20, 2015, 3:50 am

(May 20, 2015 03:48 AM)Dafuq. Wrote: [\[CITE\]](#) What's this? I am supposed to upload the file here?

Yes you are fucking supposed to upload file there..

Do the captcha and click big SELECT FILE button.

It's is going to come out as malware probably because it's RAT so there is no point in even uploading it. ?

Wi??iam - May 20, 2015, 3:50 am

(May 20, 2015 03:45 AM)Dafuq. Wrote: [\[CITE\]](#) I am not here to pick a fight with You or xVulnerables or anybody else. I just posted whatever happened.

Yes, I know that but I'm just saying isn't it very unlikely that is was his program?

Maybe you were infected for a long time and he has just decided to mess with you now.

Dafuq - May 20, 2015, 3:55 am

(May 20, 2015 03:50 AM)PwnyCode. Wrote: [\[CITE\]](#) Yes, I know that but I'm just saying isn't it very unlikely that is was his program?

Maybe you were infected for a long time and he has just decided to mess with you now.

I recently installed a new OS on my Laptop. like 3 days back. Since then I have installed just two programs on my system. Firenet VPN and njRAT. Both Today.

As soon as I installed njRAT, my screen flickered a little, i thought its nothing.

Then I was busy with my phone, and i noticed my mouse moving and HF page refreshing. We all know, spreading with a RAT tool is way easier than spreading with a VPN client. coz VPN means business. I am still considering the possibility that the Client from VPN might be infected. But testing it, showed 0/34 on nodistribute.com

(May 20, 2015 03:50 AM)Meow. Wrote: [\[CITE\]](#) Yes you are fucking supposed to upload file there..

Do the captcha and click big SELECT FILE button.

It's is going to come out as malware probably because it's RAT so there is no point in even uploading it. ?

Yeah, it is a Malware, hence this is pointless.

Memzy135 - May 20, 2015, 3:59 am

(May 20, 2015 03:20 AM)Meow. Wrote: [\[CITE\]](#) "I want to download malware" ??

THATs there because the hosting service that he uploaded it too will take it down if he dont put that.....

send the same file that you have dafuq sned it to me !

Dafuq - May 20, 2015, 4:03 am

okay, sending you two files. one vpn the other rat.

Business - May 20, 2015, 4:05 am

1. If you post in the white hat section and ask for someone qualified, they will assist you.

2. Did your mouse really start moving? I highly doubt that if xVuln. decided to RAT people he would be that blatant.

Dafuq - May 20, 2015, 4:09 am

(May 20, 2015 04:05 AM)?usiness Wrote: [\[CITE\]](#) 1. If you post in the white hat section and ask for someone qualified, they will assist you.

2. Did your mouse really start moving? I highly doubt that if xVuln. decided to RAT people he would be that blatant.

1. I did post and I am currently following the steps.

2. yes the mouse was moving, my home page of HF was being refreshed, I was being shown that I am hacked.

Ainan007 - May 20, 2015, 6:07 am

Ask a MRT to analyze the download maybe they can find something?

Although, I downloaded njRAT from xVuln a month ago and nothing fishy came up when I downloaded it.

Now that I think about it...

That "I want to download malware" seems real fishy...

supreme00. - May 20, 2015, 6:10 am

wich one did you download 0.7 or 0.6 , i've been using 0.7 and it's clean

edit:

njrat is fine theres no backdoor

<https://malwr.com/analysis/MWViNTA5NmI2NTFiNDliMmJjZDRjZDA3ODIIOGI2ZmQ/>

Dafuq - May 20, 2015, 6:12 am

(May 20, 2015 06:07 AM)Ainan007 Wrote: [\[CITE\]](#) Ask a MRT to analyze the download maybe they can find something?

Although, I downloaded njRAT from xVuln a month ago and nothing fishy came up when I downloaded it.

Now that I think about it...

That "I want to download malware" seems real fishy...

Even I am having second thoughts, maybe its something else, but that was the latest program I downloaded and this happened, hence this alert. Dont mean to offend nobody for no reason. I posted this coz this is how things happened at my end.

HIGH PAID FELLA - May 20, 2015, 6:15 am

I already found my concussions, won't post it.

Just hinting you to the right direction: MD5 lookup

Dafuq - May 20, 2015, 6:16 am

(May 20, 2015 06:15 AM)Asterea Wrote: [\[CITE\]](#) I already found my concussions, won't post it.

Just hinting you to the right direction: MD5 lookup

PM me please? I would appreciate it!

(May 20, 2015 06:10 AM)supreme00. Wrote: [\[CITE\]](#) wich one did you download 0.7 or 0.6 , i've been using 0.7 and it's clean

edit:

njrat is fine theres no backdoo

<https://malwr.com/analysis/MWViNTA5NmI2NTFiNDliMmJjZDRjZDA3ODIIOGI2ZmQ/>

I used 0.7. i have no idea why this happened. ?

HIGH PAID FELLA - May 20, 2015, 6:18 am

ip-176-98-110-78.static.mo-nex.cz:49261

The network communication.

Looks like the network operator is using a VPN.

Spoiler ([Click to View](#)) TCP:Connects to 178.91.212.186.megaline.telecom.kz (178.91.212.186:55297)
TCP:Connects to x1-6-c0-3f-0e-de-b2-98.cpe.webspeed.dk (87.52.5.216:55760)
TCP:Connects to WIN-QTQ30GSEEHT (222.252.78.214:20550)
TCP:Connects to vpn.at.xsuset.net (91.235.168.198:53726)
TCP:Connects to subs13-223-255-229-78.three.co.id (223.255.229.78:41055)
TCP:Connects to ris91-h01-5-50-88-173.dsl.sta.abo.bbox.fr (5.50.88.173:49670)
TCP:Connects to rez-243-109.xgbe.cz (79.127.243.109:57299)
TCP:Connects to rev-212-98-133-151.terra.net.lb (212.98.133.151:7123)
TCP:Connects to ptr-90-159-235-192.is.net.tr (90.159.235.192:49244)
TCP:Connects to ptr.abcom.al (109.69.5.32:4287)
TCP:Connects to pppoe.178-67-93-38.avangarddsl.ru (178.67.93.38:58388)
TCP:Connects to ppp-58-11-120-74.revip2.asianet.co.th (58.11.120.74:51061)
TCP:Connects to ppp-5.137.45.16.nsk.rt.ru (5.137.45.16:49718)
TCP:Connects to ppp-151-167.terra.net.lb (212.98.151.167:26556)
TCP:Connects to ppp-124-122-235-117.revip2.asianet.co.th (124.122.235.117:49359)
TCP:Connects to p57B7A196.dip0.t-ipconnect.de (87.183.161.150:58415)

Dafuq - May 20, 2015, 6:21 am

(May 20, 2015 06:18 AM)Asterea Wrote: ([CITE](#)) ip-176-98-110-78.static.mo-nex.cz:49261

The network communication.

Looks like the network operator is using a VPN.

Spoiler ([Click to View](#)) TCP:Connects to 178.91.212.186.megaline.telecom.kz (178.91.212.186:55297)
TCP:Connects to x1-6-c0-3f-0e-de-b2-98.cpe.webspeed.dk (87.52.5.216:55760)
TCP:Connects to WIN-QTQ30GSEEHT (222.252.78.214:20550)
TCP:Connects to vpn.at.xsuset.net (91.235.168.198:53726)
TCP:Connects to subs13-223-255-229-78.three.co.id (223.255.229.78:41055)
TCP:Connects to ris91-h01-5-50-88-173.dsl.sta.abo.bbox.fr (5.50.88.173:49670)
TCP:Connects to rez-243-109.xgbe.cz (79.127.243.109:57299)
TCP:Connects to rev-212-98-133-151.terra.net.lb (212.98.133.151:7123)
TCP:Connects to ptr-90-159-235-192.is.net.tr (90.159.235.192:49244)
TCP:Connects to ptr.abcom.al (109.69.5.32:4287)
TCP:Connects to pppoe.178-67-93-38.avangarddsl.ru (178.67.93.38:58388)
TCP:Connects to ppp-58-11-120-74.revip2.asianet.co.th (58.11.120.74:51061)
TCP:Connects to ppp-5.137.45.16.nsk.rt.ru (5.137.45.16:49718)
TCP:Connects to ppp-151-167.terra.net.lb (212.98.151.167:26556)
TCP:Connects to ppp-124-122-235-117.revip2.asianet.co.th (124.122.235.117:49359)
TCP:Connects to p57B7A196.dip0.t-ipconnect.de (87.183.161.150:58415)
That implies it is backdoored?

HIGH PAID FELLA - May 20, 2015, 6:23 am

(May 20, 2015 06:21 AM)Dafuq. Wrote: [\[CITE\]](#) That implies it is backdoored?

I just did some lookup on the web, I don't have the required stuff to check it out for you (computer).

Dafuq - May 20, 2015, 6:24 am

(May 20, 2015 06:23 AM)Asterea Wrote: [\[CITE\]](#) I just did some lookup on the web, I don't have the required stuff to check it out for you (computer).

Can u check it later? If so, at least we will know the root of this problem.

HIGH PAID FELLA - May 20, 2015, 6:24 am

(May 20, 2015 06:24 AM)Dafuq. Wrote: [\[CITE\]](#) Can u check it later? If so, at least we will know the root of this problem.

You can use twitter to ask malware analysers.

Darkcometz - May 20, 2015, 6:36 am

I've been using njRAT for a long time and nothing happened to me..

HIGH PAID FELLA - May 20, 2015, 6:37 am

Upload the 'VPN' you downloaded to VirusTotal and post the link.

#Skyline - May 20, 2015, 6:37 am

I'd suggest sending this to staff also.

Because if it's true that it is backdoored, other HF users are downloading it.

lavic2001 - May 20, 2015, 6:40 am

He could edit and post clear version.

Dafuq - May 20, 2015, 6:43 am

Check these both if u ppl can.

<http://ge.tt/6wLWnIG2>

Dafuq - May 20, 2015, 6:52 am

(May 20, 2015 06:45 AM)Yani Wrote: [\[CITE\]](#) The link you included is an analysis that tells us that the executable has a backdoor.

It drops the payload to the appdata folder and adds itself to startup.

It even has a botkiller.

Exactly. nd yet he says its clean. :/

HIGH PAID FELLA - May 20, 2015, 6:54 am

(May 20, 2015 06:45 AM)Yani Wrote: [\[CITE\]](#) The link you included is an analysis that tells us that the executable has a backdoor.

It drops the payload to the appdata folder and adds itself to startup.

It even has a botkiller.

What did I say? :)

If I could I would of made a video and fuck the shit out of him :(

21st Century Schizoid Man - May 20, 2015, 6:54 am

Wait? ? my pc broke recently and on startup it would try to delete something and my MBAM got fucked up, my cursor moved by its self multiple times, and this was like a weak after i download njrat...

Dafuq - May 20, 2015, 6:55 am

(May 20, 2015 06:54 AM)?olf Wrote: [\[CITE\]](#) Wait? ? my pc broke recently and on startup it would try to delete something and my MBAM got fucked up, my cursor moved by its self multiple times, and this was like a week after i download njrat...

My malwarebytes got fucked too.. It doesnt update. Just shows your Malware Bytes is outdated.

21st Century Schizoid Man - May 20, 2015, 6:56 am

Imagine xVuln is a cop and fucks everyone LMAO

HIGH PAID FELLA - May 20, 2015, 6:56 am

(May 20, 2015 06:56 AM)?olf Wrote: [\[CITE\]](#) Imagine xVuln is a cop and fucks everyone LMAO
No, he's a 15 year old pathetic kid.

21st Century Schizoid Man - May 20, 2015, 6:57 am

(May 20, 2015 06:55 AM)Dafuq. Wrote: [\[CITE\]](#) My malwarebytes got fucked too.. It doesnt update. Just shows your Malware Bytes is outdated.

YEAH THATS WHAT HAPPEND, it just never updated and would keep prompting me to.

Ainan007 - May 20, 2015, 6:57 am

Ooooo shit is getting fishy ;-;

21st Century Schizoid Man - May 20, 2015, 6:58 am

yo lets fuck this guy up, he's ratting HF users and getting away with it, someone contact staff and do more reaserch

I have a spare hp laptop, going to search this thing through and get his ip/dns/ports and such

Dafuq - May 20, 2015, 7:00 am

(May 20, 2015 06:58 AM)?olf Wrote: [\[CITE\]](#) yo lets fuck this guy up, he's ratting HF users and getting away with it, someone contact staff and do more reaserch

I have a spare hp laptop, going to search this thing through and get his ip/dns/ports and such
I have no idea why a guy who has been an HQ member on HF for so long would suddenly risk everything to do something so stupid?

21st Century Schizoid Man - May 20, 2015, 7:01 am

(May 20, 2015 07:00 AM)Dafuq. Wrote: [\[CITE\]](#) I have no idea why a guy who has been an HQ member on HF for so long would suddenly risk everything to do something so stupid?

idk man, thats why i said a cop before, all i know is, 2 weeks i was bored download njrat to make a setup tutorial,mouse glitches the fuck out, clicking in background stuff deleted its self and my mbam would not work, and i believe my windows 32 fie got deleted ?

FreeAnneFrank - May 20, 2015, 7:02 am

(May 20, 2015 03:39 AM)PwnyCode. Wrote: [\[CITE\]](#) So xVulnerable waited years of hard work to helping people just so he could move your cursor and refresh your pages.
seems legit

This just made me laugh so hard nigga. Get that +1. Will register on vhf to buy you rep. Nigga i love you for this.

Darkcometz - May 20, 2015, 7:02 am

Time to use darkcomet again!111111 lolol

HIGH PAID FELLA - May 20, 2015, 7:03 am

(May 20, 2015 07:02 AM)1312 Wrote: [\[CITE\]](#) This just made me laugh so hard nigga. Get that +1. Will register on vhf to buy you rep. Nigga i love you for this. Paypal, Bitcoin, HackForums accounts, you can get a lot of money with them?

ninen2001 - May 20, 2015, 7:03 am

I don't think it's xVulnerables njRAT. It has alot of downloads and alot of posts and no issues. I also downloaded it and got no issues. And I think xVuln is pretty safe.

HIGH PAID FELLA - May 20, 2015, 7:03 am

(May 20, 2015 07:03 AM)ninen2001 Wrote: [\[CITE\]](#) I don't think it's xVulnerables njRAT. It has alot of downloads and alot of posts and no issues. I also downloaded it and got no issues. And I think xVuln is pretty safe.

You think. You think. Keep thinking, but you're infected idiot.

Scklyic - May 20, 2015, 7:04 am

So I was one to download and extract his njRAT v0.7, I never ran the .exe or anything. Should a deletion of that folder and a MalwareBytes scan clean things up?

21st Century Schizoid Man - May 20, 2015, 7:04 am

(May 20, 2015 07:03 AM)ninen2001 Wrote: [\[CITE\]](#) I don't think it's xVulnerables njRAT. It has alot of downloads and alot of posts and no issues. I also downloaded it and got no issues. And I think xVuln is pretty safe.

idk man, my pc almost had signs and hiccups that it was ratted, stuff got fucked and this was after i downloaded nj soooo... and someone found a backdoor in it in this thread ?

HIGH PAID FELLA - May 20, 2015, 7:04 am

(May 20, 2015 07:04 AM)Scklyic Wrote: [\[CITE\]](#) So I was one to download and extract his njRAT v0.7, I never ran the .exe or anything. Should a deletion of that folder and a MalwareBytes scan clean things up?

If you ran nothing it did not harm your system.

FreeAnneFrank - May 20, 2015, 7:05 am

(May 20, 2015 07:03 AM)Asterea Wrote: [\[CITE\]](#) Paypal, Bitcoin, HackForums accounts, you can get a lot of money with them?

Just Noticed vhf got sized.

But what do you mean by that?

ninen2001 - May 20, 2015, 7:06 am

Actually, I have noticed that my webcam lights randomly turns on sometimes. This did not happen before using njRAT. I have had no other issues other than that.

HIGH PAID FELLA - May 20, 2015, 7:06 am

(May 20, 2015 07:05 AM)1312 Wrote: [\[CITE\]](#) Just Noticed vhf got sized.

But what do you mean by that?

HF account, let's do an exchange, scam some people etc...

Paypal, lets send all the funds to buy stuff, send it, etc...

Bitcoin, lets steal all your bitcoins.

And much more.

Dafuq - May 20, 2015, 7:06 am

See, to be really brutally honest, I didnt know xVulnerable until today, I dont think we ever interacted in person, so I can neither Speak positively nor negatively about him as a person.

As far as my problem is concerned, I posted as it happened, as soon as it happened. Didnt exaggerate. Spoke the truth. I have posted the files as i got them. People can check things for themselves before taking sides here.

this is not a Fight between xVulnerable and me, or anybody and me, this is just an issue, which I faced and posted regarding it without delaying it.

21st Century Schizoid Man - May 20, 2015, 7:06 am

(May 20, 2015 07:05 AM)1312 Wrote: [\[CITE\]](#) Just Noticed vhf got sized.

But what do you mean by that?I belive he quoted the wrong person, someone said, "Why would such a HQ user do this?"

Dafuq - May 20, 2015, 7:07 am

(May 20, 2015 07:06 AM)ninen2001 Wrote: [\[CITE\]](#) Actually, I have noticed that my webcam lights randomly turns on sometimes. This did not happen before using njRAT. I have had no other issues other than that.

Now you are talking sense. Webcam light turning on means your webcam has AI and loves u, hence keeps checking on u? No right?

You are RATED!!

HIGH PAID FELLA - May 20, 2015, 7:07 am

(May 20, 2015 07:05 AM)Yani Wrote: [\[CITE\]](#) What I commented on the malwr link could also be because it's a RAT client.

I'll do some analysis later today myself and will post my findings.

A RAT client with very supicious network communication, installs itself on autorun, detected, etc.

FreeAnneFrank - May 20, 2015, 7:08 am

(May 20, 2015 07:06 AM)Asterea Wrote: [\[CITE\]](#) HF account, let's do an exchange, scam some people etc...

Paypal, lets send all the funds to buy stuff, send it, etc...

Bitcoin, lets steal all your bitcoins.

And much more.

niggu what the fuck r u talking about

21st Century Schizoid Man - May 20, 2015, 7:08 am

Yo this motherfucker, didn't he own Jspy at one point also?

HIGH PAID FELLA - May 20, 2015, 7:09 am

(May 20, 2015 07:08 AM)1312 Wrote: [\[CITE\]](#) niggu what the fuck r u talking about

You quoted, why would a 'trusted member' give out a backdoored software. Well, that's why...

ninen2001 - May 20, 2015, 7:09 am

(May 20, 2015 07:07 AM)Dafuq. Wrote: [\[CITE\]](#) Now you are talking sense. Webcam light turning on means your webcam has AI and loves u, hence keeps checking on u? No right?

You are RATED!!

Of course I am. Imma disconnect from internet and scan and check for startup keys/files.

Dafuq - May 20, 2015, 7:10 am

(May 20, 2015 07:09 AM)ninen2001 Wrote: [\[CITE\]](#) Of course I am. Imma disconnect from internet and scan and check for startup keys/files.

Better post a thread in MRT section asap. Before you get fucked royally!

21st Century Schizoid Man - May 20, 2015, 7:11 am

Did anyones Malware bytes get fucked after they download njrat?

Dafuq - May 20, 2015, 7:12 am

(May 20, 2015 07:11 AM)?olf Wrote: [\[CITE\]](#) Did anyones Malware bytes get fucked after they download njrat?

Mine did, wouldnt update, just keeps saying ur Software is outdated. Wont even scan!!

Darkcometz - May 20, 2015, 7:12 am

(May 20, 2015 07:11 AM)?olf Wrote: [\[CITE\]](#) Did anyones Malware bytes get fucked after they download njrat?

Nope, and I always check processes running + start up files. I see nothing.

ninen2001 - May 20, 2015, 7:13 am

(May 20, 2015 07:11 AM)?olf Wrote: [\[CITE\]](#) Did anyones Malware bytes get fucked after they download njrat?

No issues here. Only thing I ever noticed was random webcam lights going on. No stolen logins or anything.

HIGH PAID FELLA - May 20, 2015, 7:13 am

(May 20, 2015 07:12 AM)Dafuq. Wrote: [\[CITE\]](#) Mine did, wouldnt update, just keeps saying ur Software is outdated. Wont even scan!!

That's a feature, check your hosts file. It probably edited AMB.

Dafuq - May 20, 2015, 7:14 am

Check this out. This is a clear indication!!

HIGH PAID FELLA - May 20, 2015, 7:14 am

(May 20, 2015 07:12 AM)Darkcometz Wrote: [\[CITE\]](#) Nope, and I always check processes running + start up files. I see nothing.

It can be hidden... I'm trying to help but do your research first please before posting...

21st Century Schizoid Man - May 20, 2015, 7:14 am

(May 20, 2015 07:12 AM)Dafuq. Wrote: [\[CITE\]](#) Mine did, wouldnt update, just keeps saying ur Software is outdated. Wont even scan!!

same thing bro, wouldn't do anything

HIGH PAID FELLA - May 20, 2015, 7:15 am

(May 20, 2015 07:14 AM)Dafuq. Wrote: [\[CITE\]](#) Check this out. This is a clear indication!!

[img]http://prntscr.com/77crpg[/img]

Read my previous post please.

Wi??iam - May 20, 2015, 7:15 am

The moment when you refresh the page every second.

HIGH PAID FELLA - May 20, 2015, 7:16 am

(May 20, 2015 07:15 AM)PwnyCode. Wrote: [\[CITE\]](#) The moment when you refresh the page every second.

Yeah, same feeling. F5'ing to explain what's going on to this people...

21st Century Schizoid Man - May 20, 2015, 7:16 am

(May 20, 2015 07:15 AM)PwnyCode. Wrote: [\[CITE\]](#) The moment when you refresh the page every second.

Dude get the fuck out,this is a problem "Be a spoke in the wheel, not a naill in the tire"

Darkcometz - May 20, 2015, 7:17 am

(May 20, 2015 07:14 AM)Asterea Wrote: [\[CITE\]](#) It can be hidden... I'm trying to help but do your research first please before posting...

Nothing suspicious happens on my desktop, no webcam lights, nothing broke.

Maybe I downloaded an old link? since he updated the link when people said that the link broke..

Dafuq - May 20, 2015, 7:17 am

(May 20, 2015 07:15 AM)Asterea Wrote: [\[CITE\]](#) Read my previous post please.

I didnt really understand what u meant, bit more explanation would be helpful. :P

Wi??iam - May 20, 2015, 7:17 am

(May 20, 2015 07:16 AM)?olf Wrote: [\[CITE\]](#) Dude get the fuck out,this is a problem "Be a spoke in the wheel, not a naill in the tire"

Just trying to lighten the mood, sorry boss.

HIGH PAID FELLA - May 20, 2015, 7:18 am

(May 20, 2015 07:17 AM)Dafuq. Wrote: [\[CITE\]](#) I didnt really understand what u meant, bit more explanation would be helpful. :P

His malware has deleted malwarebytes from your hosts, that's the shit that makes it update when you click that button.

Dafuq - May 20, 2015, 7:18 am

TBH, this thread is moving a lot faster than expected. Hope we can get some Analysers in to analyse it without bias and post results.

HIGH PAID FELLA - May 20, 2015, 7:19 am

(May 20, 2015 07:17 AM)Darkcometz Wrote: [\[CITE\]](#) Nothing suspicious happens on my desktop, no webcam lights, nothing broke.

Maybe I downloaded an old link? since he updated the link when people said that the link broke..
It does not have to be supicious to have a malware...

Dafuq - May 20, 2015, 7:20 am

(May 20, 2015 07:18 AM)Asterea Wrote: [\[CITE\]](#) His malware has deleted malwarebytes from your hosts, that's the shit that makes it update when you click that button.

Okay, i uninstalled and re-installed it, now its working!

HIGH PAID FELLA - May 20, 2015, 7:21 am

(May 20, 2015 07:20 AM)Dafuq. Wrote: [\[CITE\]](#) Okay, i uninstalled and re-installed it, now its working!
Like I said, good luck removing.

21st Century Schizoid Man - May 20, 2015, 7:22 am

Im asking some questions to some people now in my newest thread, hope i get some answers out of this.

Tyler Durden. - May 20, 2015, 7:22 am

Why don't we get someone with decent knowledge in this area to research and analyze the file?

HIGH PAID FELLA - May 20, 2015, 7:23 am

(May 20, 2015 07:22 AM)Tyler Durden. Wrote: [\[CITE\]](#) Why don't we get someone with decent knowledge in this area to research and analyze the file?

I don't have a computer available or I would.

ninen2001 - May 20, 2015, 7:24 am

(May 20, 2015 07:22 AM)Tyler Durden. Wrote: [\[CITE\]](#) Why don't we get someone with decent knowledge in this area to research and analyze the file?

Definitely agree on this!

21st Century Schizoid Man - May 20, 2015, 7:25 am

same I'm on my macbook, because my pc lost its shit from no where ?

Dafuq - May 20, 2015, 7:25 am

I would like to see some malware analyzer from HF analyzing the files. It would help us clear the doubts and know for sure whats wrong!

21st Century Schizoid Man - May 20, 2015, 7:27 am

(May 20, 2015 07:25 AM)Dafuq. Wrote: [\[CITE\]](#) I would like to see some malware analyzer from HF analyzing the files. It would help us clear the doubts and know for sure whats wrong!

post it in the white hat section,you will get some answer, maybe we can get some to decompile it

Dafuq - May 20, 2015, 7:29 am

(May 20, 2015 07:27 AM)?olf Wrote: [\[CITE\]](#) post it in the white hat section,you will get some answer, maybe we can get some to decompile it

I have already posted my logs in MRT section. I am waiting for a response. Its taking longer than usual

(May 20, 2015 07:23 AM)Asterea Wrote: [\[CITE\]](#) I don't have a computer available or I would. Get a computer from a friend maybe, plz bbi! ?

yhi00 - May 20, 2015, 7:37 am

install a AV

& remove the rat & other malcious files

Dafuq - May 20, 2015, 7:39 am

(May 20, 2015 07:37 AM)yhi00 Wrote: [\[CITE\]](#) install a AV

& remove the rat & other malcious files

Thank you, your post is the most helpful out of all the posts till now. ???

smaxzax - May 20, 2015, 7:39 am

why dont you clear all you connections on shitty pc.. thne run it..
then do a netstat -an ?

Dafuq - May 20, 2015, 7:41 am

(May 20, 2015 07:39 AM)smaxzax Wrote: [\[CITE\]](#) why dont you clear all you connections on shitty pc.. thne run it..

then do a netstat -an ?

All that is done, I am currently following the procedure of MRT on HF. Hoping to get this resolved. Else I will just format my pc.

Lovesosa - May 20, 2015, 7:51 am

if heared more people get the problem a guy on skype told me thath hes webcam lights has been going on and off.

Mr. Money™ - May 20, 2015, 7:58 am

I download the rat to and everything on my pc is fine.

What you could do is run a botkill and see if the (If there is a backdoor) Get's removed. Another thing you could do is create a new account on your computer and run the file on that account to and see if anything strange happends if not then it might have been another file causing this!

SIM-2212192 - May 20, 2015, 7:59 am

o shit

If this is true, xvulnerable has a pretty bigass botnet, and you can only imagine how many bots he would have if he coded in some kind of bot-stealer.

I have it downloaded in a ratting VM, so I wouldn't really care as I don't have anything valuable there.

Dafuq - May 20, 2015, 8:03 am

(May 20, 2015 07:45 AM)Yani Wrote: [\[CITE\]](#) I'm sure some people are already analyzing it. I don't have a test machine currently (my laptop is broken) so I can't really do a full analysis. I checked it a little on my main machine and it doesn't look too fishy.

I'm unable to find anything regarding this connection.
I am not a Malware Analyzer, so cant really comment on this.

(May 20, 2015 07:51 AM)Mitzz Wrote: [\[CITE\]](#) if heared more people get the problem a guy on skype told me thath hes webcam lights has been going on and off.
I have heard the same from many now. Via this thread.

(May 20, 2015 07:58 AM)Reddington™ Wrote: [\[CITE\]](#) I download the rat to and everything on my pc is fine.

What you could do is run a botkill and see if the (If there is a backdoor) Get's removed. Another thing you could do is create a new account on your computer and run the file on that account to and see if anything strange happends if not then it might have been another file causing this!
I will try that soon. but it cant b any other file, Either this or a VPN. VPN is highly unlikely, but I have posted both the files to be analyzed by someone who can.

(May 20, 2015 07:59 AM)EmeraldRebel Wrote: [\[CITE\]](#) o shit
If this is true, xvulnerable has a pretty bigass botnet, and you can only imagine how many bots he would have if he coded in some kind of bot-stealer.

I have it downloaded in a ratting VM, so I wouldn't really care as I don't have anything valuable there.

I have no idea why this is happening. But since it has happened with many guys now, I would suggest to take precautions, a VM is totally fine though! unless he knows how to bypass VM!?

supreme00. - May 20, 2015, 8:22 am

(May 20, 2015 06:45 AM)Yani Wrote: [\[CITE\]](#) The link you included is an analysis that tells us that the executable has a backdoor.

It drops the payload to the appdata folder and adds itself to startup.

It even has a botkiller.

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

<https://i.imgur.com/8QPwcll.png>

edit:

just seen

C:\DOCUME~1\User\LOCALS~1\Temp\njRAT v0.7d.INI

C:/DOCUME~1

C:/DOCUME~1/User

C:/DOCUME~1/User/LOCALS~1

C:/DOCUME~1/User/LOCALS~1/Temp

C:\WINDOWS\assembly\pubpol1.dat

but i recently got my computer scanned by a whitehat helper and he said it's clean

also mbam is working fine , checked my startups and looks like theres nothing

Dafuq - May 20, 2015, 8:23 am

(May 20, 2015 08:22 AM)supreme00. Wrote: [\[CITE\]](#) <https://i.imgur.com/pdRcJWW.png>

<https://i.imgur.com/8QPwcll.png>

Which site is this now? lmk!

NullRootix - May 20, 2015, 8:25 am

(May 20, 2015 08:23 AM)Dafuq. Wrote: [\[CITE\]](#) Which site is this now? lmk!

<http://malwr.com> ?

Dafuq - May 20, 2015, 8:30 am

(May 20, 2015 08:22 AM)supreme00. Wrote: [\[CITE\]](#) <https://i.imgur.com/pdRcJWW.png>

<https://i.imgur.com/8QPwcll.png>

edit:

just seen

C:\DOCUME~1\User\LOCALS~1\Temp\njRAT v0.7d.INI

C:/DOCUME~1

C:/DOCUME~1/User

C:/DOCUME~1/User/LOCALS~1

C:/DOCUME~1/User/LOCALS~1/Temp

C:\WINDOWS\assembly\pubpol1.dat

but i recently got my computer scanned by a whitehat helper and he said it's clean

also mbam is working fine , checked my startups and looks like theres nothing

But u see that files are being dropped right?

supreme00. - May 20, 2015, 8:32 am

(May 20, 2015 08:30 AM)Dafuq. Wrote: [\[CITE\]](#) But u see that files are being dropped right?

they are .ini files and .dat i doubt it's a rat + no network activity check yourself

i had 1400\$ btcs in my wallet for months now nothing happened

ubbelol - May 20, 2015, 8:35 am

(May 20, 2015 08:30 AM)Dafuq. Wrote: [\[CITE\]](#) But u see that files are being dropped right?

Dropping an .INI file is hardly an indication of malicious activity... Why don't you all calm down for a second and at least wait for an official response from xVulnerable or whoever made the RAT before throwing accusations left and right? It may be that you had malware installed earlier and this shit starting to happen along with the njRat download is a mere coincidence.

If I get some time over I'll analyze the file to see if there's something fishy with it.

Dafuq - May 20, 2015, 8:37 am

(May 20, 2015 08:32 AM)supreme00. Wrote: [\[CITE\]](#) they are .ini files and .dat i doubt it's a rat + no network activity check yourself
i had 1400\$ btcs in my wallet for months now nothing happened
I seriously have no idea how these things work tbh. I wish I could analyze it myself. But I am totally dependent on third parties for it. and Many users are reporting it as malware now, not just me.

Many guys are saying they saw their webcam turn on/off after using njrat. Some are reporting problems with MBAM just like me.

supreme00. - May 20, 2015, 8:38 am

(May 20, 2015 08:37 AM)Dafuq. Wrote: [\[CITE\]](#) I seriously have no idea how these things work tbh. I wish I could analyze it myself. But I am totally dependent on third parties for it. and Many users are reporting it as malware now, not just me.

Many guys are saying they saw their webcam turn on/off after using njrat. Some are reporting problems with MBAM just like me.
you and them may have download a rat somewhere else my mbam is working fine and my webcam never opened
just gave a look at your posts and i see you have downloaded jwatch and amother thing

Dafuq - May 20, 2015, 8:38 am

(May 20, 2015 08:35 AM)ubbelol Wrote: [\[CITE\]](#) Dropping an .INI file is hardly an indication of malicious activity... Why don't you all calm down for a second and at least wait for an official response from xVulnerable or whoever made the RAT before throwing accusations left and right? It may be that you had malware installed earlier and this shit starting to happen along with the njRat download is a mere coincidence.

If I get some time over I'll analyze the file to see if there's something fishy with it.
I am totally calm bro, I am not fighting with anyone, this post is just to Alert the HF members for now, coz I and some others are facing this problem. Not to defame anyone, or pick a useless fight.

Wieno - May 20, 2015, 9:22 am

What if his site got hacked and somebody putted his backdoored njrat as download.

number7 - May 20, 2015, 9:23 am

you should always have a separate pc for ratting anyway a clean pc with no real info on it just for rating in my opinion
not like u need a super fast pc for rating most people have a old pc laying around that could be reformatted and set up just for this and only give it internet connection when needed :)

just my opinion

Dafuq - May 20, 2015, 9:24 am

(May 20, 2015 09:22 AM)Wieno Wrote: [\[CITE\]](#) What if his site got hacked and somebody putted his backdoored njrat as download.

I never said that xVulnerables is definitely the one responsible, i just stated the events. I dont know who did it and why. :)

(May 20, 2015 09:23 AM)dn5050 Wrote: [\[CITE\]](#) you should always have a separate pc for ratting

anyway a clean pc with no real info on it just for rating in my opinion
not like u need a super fast pc for rating most people have a old pc laying around that could be reformatted and set up just for this and only give it internet connection when needed :)

just my opinion

Totally correct. I will keep it in mind considering I have two laptops at my disposal.

Geo Trouvetou - May 20, 2015, 10:38 am

MD5 Checksum are same from the original link given by xVuln's post and one you sent.

- 473e1a7be89c3a727176d4f9f5a64b69

njRAT install itself at startup and drop configs and *.exe files in your Temp folder at start, while running it connects to the IP: ip-176-98-110-78.static.mo-nex.cz:49261(VPN)

Spoiler ([Click to View](#))

TCP:

Connects to 178.91.212.186.megaline.telecom.kz (178.91.212.186:55297)

TCP:

Connects to x1-6-c0-3f-0e-de-b2-98.cpe.webspeed.dk (87.52.5.216:55760)

TCP:

Connects to WIN-QTQ30GSEEHT (222.252.78.214:20550)

TCP:

Connects to vpn.at.xsusenet.com (91.235.168.198:53726)

TCP:

Connects to subs13-223-255-229-78.three.co.id (223.255.229.78:41055)

TCP:

Connects to ris91-h01-5-50-88-173.dsl.sta.abo.bbox.fr (5.50.88.173:49670)

TCP:

Connects to rez-243-109.xgbe.cz (79.127.243.109:57299)

TCP:

Connects to rev-212-98-133-151.terra.net.lb (212.98.133.151:7123)

TCP:

Connects to ptr-90-159-235-192.is.net.tr (90.159.235.192:49244)

TCP:

Connects to ptr.abcom.al (109.69.5.32:4287)

TCP:

Connects to pppoe.178-67-93-38.avangarddsl.ru (178.67.93.38:58388)

TCP:

Connects to ppp-58-11-120-74.revip2.asianet.co.th (58.11.120.74:51061)

TCP:

Connects to ppp-5.137.45.16.nsk.rt.ru (5.137.45.16:49718)

TCP:

Connects to ppp-151-167.terra.net.lb (212.98.151.167:26556)

TCP:

Connects to ppp-124-122-235-117.revip2.asianet.co.th (124.122.235.117:49359)

TCP:

Connects to p57B7A196.dip0.t-ipconnect.de (87.183.161.150:58415)

TCP:

Connects to net-31-132-210-207.king-online.ru (31.132.210.207:58038)

TCP:

Connects to nat-88-212-36-36.antik.sk (88.212.36.36:64023)

TCP:

Connects to nat06.jhcomp.cz (178.23.219.6:1934)

TCP:

Connects to ip-78-102-115-64.net.upcbroadband.cz (78.102.115.64:49433)

I found nothing more, hope than someone can make a reverse engineering and say to us if it's backdoor or not.

Dafuq - May 20, 2015, 10:42 am

(May 20, 2015 10:38 AM)Geo Trouvetou Wrote: [\[CITE\]](#) MD5 Checksum are same from the original link given by xVuln's post and one you sent.

- 473e1a7be89c3a727176d4f9f5a64b69

njRAT install itself at startup and drop configs and *.exe files in your Temp folder at start, while running it connects to the IP: ip-176-98-110-78.static.mo-nex.cz:49261(VPN)

Spoiler ([Click to View](#))

TCP:

Connects to 178.91.212.186.megaline.telecom.kz (178.91.212.186:55297)

TCP:

Connects to x1-6-c0-3f-0e-de-b2-98.cpe.webspeed.dk (87.52.5.216:55760)

TCP:

Connects to WIN-QTQ30GSEEHT (222.252.78.214:20550)

TCP:

Connects to vpn.at.xsusenet.com (91.235.168.198:53726)

TCP:

Connects to subs13-223-255-229-78.three.co.id (223.255.229.78:41055)

TCP:

Connects to ris91-h01-5-50-88-173.dsl.sta.abo.bbox.fr (5.50.88.173:49670)

TCP:

Connects to rez-243-109.xgbe.cz (79.127.243.109:57299)

TCP:

Connects to rev-212-98-133-151.terra.net.lb (212.98.133.151:7123)

TCP:

Connects to ptr-90-159-235-192.is.net.tr (90.159.235.192:49244)

TCP:

Connects to ptr.abcom.al (109.69.5.32:4287)

TCP:

Connects to pppoe.178-67-93-38.avangarddsl.ru (178.67.93.38:58388)

TCP:

Connects to ppp-58-11-120-74.revip2.asianet.co.th (58.11.120.74:51061)

TCP:

Connects to ppp-5.137.45.16.nsk.rt.ru (5.137.45.16:49718)

TCP:

Connects to ppp-151-167.terra.net.lb (212.98.151.167:26556)

TCP:

Connects to ppp-124-122-235-117.revip2.asianet.co.th (124.122.235.117:49359)

TCP:

Connects to p57B7A196.dip0.t-ipconnect.de (87.183.161.150:58415)

TCP:

Connects to net-31-132-210-207.king-online.ru (31.132.210.207:58038)

TCP:

Connects to nat-88-212-36-36.antik.sk (88.212.36.36:64023)

TCP:

Connects to nat06.jhcomp.cz (178.23.219.6:1934)

TCP:

Connects to ip-78-102-115-64.net.upcbroadband.cz (78.102.115.64:49433)

I found nothing more, hope than someone can make a reverse engineering and say to us if it's backdoor or not.

I am waiting for the same. A mentor asked me to take up with matter with omni, but I think that we should wait for xVulnerable. Lets c what he says.

mrfong - May 20, 2015, 10:42 am

Confirmed, this is infected, it fucked my whole system, my passwords got changed, everything i have started acting wierd, atleast i dont have a cam :D so there is no problems with that, i'm not sure if xvuln did it , but the link is backdoored atm.

Dafuq - May 20, 2015, 10:44 am

(May 20, 2015 10:42 AM)mrfong Wrote: [\[CITE\]](#) Confirmed, this is infected, it fucked my whole system, my passwords got changed, everything i have started acting wierd, atleast i dont have a cam :D so there is no problems with that, i'm not sure if xvuln did it , but the link is backdoored atm. I understand u and a few others are sharing the same problem as me. We can only wait to see what he has to say.

Geo Trouvetou - May 20, 2015, 10:48 am

Yep, but i do not think he will tell us yes or not it is infected, lol.

A lot of AV's say at result: MSIL/Bladabindi

So, when we go to the Microsoft website, they said:

- <http://www.microsoft.com/security/portal/threat/encyclopedia/Entry.aspx?Name=MSIL/Bladabindi>

Hoping that this matter be resolved quickly!

(May 20, 2015 10:45 AM)Joker™ Wrote: [\[CITE\]](#) Hey op you can compare md5 of mine and his njRat.

<https://hackforums.net/showthread.php?tid=4829453>

473E1A7BE89C3A727176D4F9F5A64B69

It's the same.

lavic2001 - May 20, 2015, 10:51 am

Im 100% sure he did this. Just take a look:

(This post was last modified: 03-22-2015 04:12 PM by xVulnerable.

The GRim - May 20, 2015, 10:53 am

Ah damn, I might have downloaded it lol.

Dafuq - May 20, 2015, 11:01 am

(May 20, 2015 10:53 AM)The GRim Wrote: [\[CITE\]](#) Ah damn, I might have downloaded it lol. I just hope someone can say for sure which one of the two files was backdoor-ed.

(May 20, 2015 10:51 AM)lavic2001 Wrote: [\[CITE\]](#) Im 100% sure he did this. Just take a look:

(This post was last modified: 03-22-2015 04:12 PM by xVulnerable.

i know abt the recent modification. Still, lets c..

mrfong - May 20, 2015, 11:03 am

Guys, i took 4 njrats from 4 diffrent places 2 from hf , 1 from dev point and 1 from ratting arab group, all of them are the same size and with the same md5 hash, it might be another file that is with njrat it self..

supreme00. - May 20, 2015, 11:05 am

<https://i.imgur.com/8pRVgeH.png>

2.exe = vuln's download of 2 months ago

njrat.exe = vuln's 6 months old download

joker = joker's download

all three files have the same md5 and from the malwr's scan i made looks like there is no rat binded to it

Cammy - May 20, 2015, 11:09 am

(May 20, 2015 11:05 AM)supreme00. Wrote: [\[CITE\]](#) <https://i.imgur.com/8pRVgeH.png>

2.exe = vuln's download of 2 months ago

njrat.exe = vuln's 6 months old download

joker = joker's download

all three files have the same md5 and from the malwr's scan i made looks like there is no rat binded to it

there is more than 1 file in the rar, could you check each and every one of them please? ty

Dafuq - May 20, 2015, 11:10 am

All the dlls with njRAT are detected as trojans. Was submitting my report to mrt when I noticed this.

mrfong - May 20, 2015, 11:11 am

(May 20, 2015 11:09 AM)Joker™ Wrote: [\[CITE\]](#) Maybe it's cuz of any other app you downloaded?

But the op stated that he got only the vpn and that rat.. so it's kinda of impossible, but how come it happend with many people and today?

Dafuq - May 20, 2015, 11:14 am

(May 20, 2015 11:11 AM)mrfong Wrote: [\[CITE\]](#) But the op stated that he got only the vpn and that rat.. so it's kinda of impossible, but how come it happend with many people and today?

The only reason I m waiting for it to be analysed is coz I did run another vpn on it with just a few mins in between. Otherwise I would have known for sure it was solely NjRAT. I would request u ppl to check the vpn as well for any malware.

Cammy - May 20, 2015, 11:16 am

ok so xvulns website currently redirects to <https://hostr.co/m8v3A4GzWerB> to download njrat

and the stats for this file are:

12 Dec 13 at 5:34 AM

1.2MB 83,717 downloads

Geo Trouvetou - May 20, 2015, 11:17 am

(May 20, 2015 11:09 AM)????2k??? Wrote: [\[CITE\]](#) there is more than 1 file in the rar, could you check each and every one of them please? ty

All have the same MD5 Checksum from the Joker's post and xVuln'post.

mrfong - May 20, 2015, 11:19 am

(May 20, 2015 11:14 AM)Dafuq. Wrote: [\[CITE\]](#) The only reason I m waiting for it to be analysed is coz I did run another vpn on it with just a few mins in between. Otherwise I would have known for sure it was solely NjRAT. I would request u ppl to check the vpn as well for any malware.Send me and i'll check them.

Dafuq - May 20, 2015, 11:20 am

(May 20, 2015 11:16 AM)???2k??? Wrote: [\[CITE\]](#) ok so xvulns website currently redirects to <https://hostr.co/m8v3A4GzWerB> to download njrat

and the stats for this file are:

12 Dec 13 at 5:34 AM

1.2MB 83,717 downloads

Yeah, I saw that too, before downloading. That's why I was even more shocked. :/

mrfong - May 20, 2015, 11:20 am

(May 20, 2015 11:16 AM)???2k??? Wrote: [\[CITE\]](#) ok so xvulns website currently redirects to <https://hostr.co/m8v3A4GzWerB> to download njrat

and the stats for this file are:

12 Dec 13 at 5:34 AM

1.2MB 83,717 downloadsYeah, It's not from his side then.. but oh well, it might be the original owner who did this, who knows.. or all of us are effected from other programs wich is almost impossible

Dafuq - May 20, 2015, 11:21 am

(May 20, 2015 11:19 AM)mrfong Wrote: [\[CITE\]](#) Send me and i'll check them.

I've posted the ge.tt link in the original post. Check the first page, frst post. And u can download from there.

supreme00. - May 20, 2015, 11:22 am

(May 20, 2015 11:09 AM)???2k??? Wrote: [\[CITE\]](#) there is more than 1 file in the rar, could you check each and every one of them please? ty<https://i.imgur.com/BDJTpAx.png>
joker's rar file is 1300kb and vuln's one is 1200kb

Dafuq - May 20, 2015, 11:22 am

(May 20, 2015 11:20 AM)mrfong Wrote: [\[CITE\]](#) Yeah, It's not from his side then.. but oh well, it might be the original owner who did this, who knows.. or all of us are effected from other programs wich is almost impossible

That's the thing. All having the same issue, downloading from the same source, what r the odds that such a thing happens because of something other than the major link we all know we have?

Will still wait and see. :)

Geo Trouvetou - May 20, 2015, 11:27 am

(May 20, 2015 11:22 AM)supreme00. Wrote: [\[CITE\]](#) <https://i.imgur.com/BDJTpAx.png>
joker's rar file is 1300kb and vuln's one is 1200kb

If you have already launch njRAT it's normal. He create somes files when you start it. (+you have a *.rar file in the xVuln'folder)

Retry your MD5 Checksum with a clean download of njRAT, MD5 Checksum are same.

Just wait for someone can can reverse engineering that soft and say us if it's backdoor or no.

Bitdefender - May 20, 2015, 11:42 am

F*ck... I downloaded NJRat a while ago. Time to get rid of that sh*t.

Holy crap. If it actually is infected, which I doubt though, that'd be gigantic... He would have infected so many users, so many logins he'd gather.

I never had any "special" movements or anything on my PC but I also downloaded it quite a while ago.

xVulnerable - May 20, 2015, 11:44 am

My links are not infected.....If you are infected it is probably because you already were. Do a system restore or format your PC if you're paranoid. You didn't show proof.

Meow - May 20, 2015, 11:45 am

(May 20, 2015 11:16 AM)???2k??? Wrote: [\[CITE\]](#) ok so xvulns website currently redirects to <https://hostr.co/m8v3A4GzWerB> to download njrat

and the stats for this file are:

12 Dec 13 at 5:34 AM

1.2MB 83,717 downloads

So there is possibility he was infecting users back in 2013/2014 ?

edit: well looks like file is clean.

Bitdefender - May 20, 2015, 11:45 am

(May 20, 2015 11:44 AM)xVulnerable Wrote: [\[CITE\]](#) You didn't show proof.

Why does this "sound" so strange to me?

mrfong - May 20, 2015, 11:46 am

(May 20, 2015 11:44 AM)xVulnerable Wrote: [\[CITE\]](#) My links are not infected.....If you are infected it is probably because you already were. Do a system restore or format your PC if you're paranoid. You didn't show proof.Yea, i'm sure you didn't do it, it might be something else

lol, i got a link from the original dev aswell and i compared to xvuln one , they're the same.. idk

Dafuq - May 20, 2015, 12:00 pm

(May 20, 2015 11:44 AM)xVulnerable Wrote: [\[CITE\]](#) My links are not infected.....If you are infected it is probably because you already were. Do a system restore or format your PC if you're paranoid. You didn't show proof.

I cant show proof, what kinda proof am I expected to show? Firstly, I am not Accusing u of ratting me, I am saying that I got a Virus through ur link, coz that was the most recent, and it happened like 5 mins after i ran njRat.

Secondly I have mentioned the other file I was using as well, so that people can check it as well, if that was the one responsible for such an incident. But as of now, nobody has said anything about the VPN software that i used.

@xVulnerable: This thread is not to defame u, or hurt ur sentiments, its here just to get an answer as to what happened and why. Dont take it personally!

Bitdefender - May 20, 2015, 12:03 pm

(May 20, 2015 12:00 PM)Dafuq. Wrote: [\[CITE\]](#) I cant show proof, what kinda proof am I expected to show? Firstly, I am not Accusing u of ratting me, I am saying that I got a Virus through ur link, coz

that was the most recent, and it happened like 5 mins after i ran njRat.

Secondly I have mentioned the other file I was using as well, so that people can check it as well, if that was the one responsible for such an incident. But as of now, nobody has said anything about the VPN software that i used.

@xVulnerable: This thread is not to defame u, or hurt ur sentiments, its here just to get an answer as to what happened and why. Dont take it personally!

He wants proof. If you ask me, that sounds kind of fucked up and there is something sketchy behind it I think...

Geo Trouvetou - May 20, 2015, 12:06 pm

Think is not good, wait for an analyse.

Business - May 20, 2015, 12:08 pm

Probably something else you ran. If you get proof, post it!

Dafuq - May 20, 2015, 12:12 pm

(May 20, 2015 12:08 PM)?usiness Wrote: [\[CITE\]](#) Probably something else you ran. If you get proof, post it!

What kinda proof are we talking about? Many users have posted some IP that this njRAT connects to as soon as it is installed. They have also posted stuff related to this RAT dropping files in APPdata. I am not a pro, I am just a guy, who wanted to see how njRAT worked. I have used DarkComet before, never faced such issues. And I dont blame people uselessly.

supreme00. - May 20, 2015, 12:13 pm

(May 20, 2015 12:12 PM)Dafuq. Wrote: [\[CITE\]](#) What kinda proof are we talking about? Many users have posted some IP that this njRAT connects to as soon as it is installed. They have also posted stuff related to this RAT dropping files in APPdata. I am not a pro, I am just a guy, who wanted to see how njRAT worked. I have used DarkComet before, never faced such issues. And I dont blame people uselessly.

they are probs lying there is no way njrat is backdoored it doesn't drop anything nor it connects to an ip

mrfong - May 20, 2015, 12:15 pm

that vpn is clean, now, if you only downloades these 2 , it might be the new windows you installed installs something else? i don't know alot about this, but njrat is infected, i tested 3 diffrent ones, and they drop some shit on temp now, it didnt happen with me before and i didn't renew my links, i installed this a month ago and today faced the issue , now about that guy who posted a vpn ip, can someone continue what he did it and get something else than a vpn ip?

Dafuq - May 20, 2015, 12:16 pm

This is the reply I am referring to.

(May 20, 2015 10:38 AM)Geo Trouvetou Wrote: [\[CITE\]](#) MD5 Checksum are same from the original link given by xVuln's post and one you sent.

- 473e1a7be89c3a727176d4f9f5a64b69

njRAT install itself at startup and drop configs and *.exe files in your Temp folder at start, while running it connects to the IP: ip-176-98-110-78.static.mo-nex.cz:49261(VPN)

Spoiler ([Click to View](#))

TCP:

Connects to 178.91.212.186.megaline.telecom.kz (178.91.212.186:55297)
TCP:
Connects to x1-6-c0-3f-0e-de-b2-98.cpe.webspeed.dk (87.52.5.216:55760)
TCP:
Connects to WIN-QTQ30GSEEHT (222.252.78.214:20550)
TCP:
Connects to vpn.at.xsusenet.com (91.235.168.198:53726)
TCP:
Connects to subs13-223-255-229-78.three.co.id (223.255.229.78:41055)
TCP:
Connects to ris91-h01-5-50-88-173.dsl.sta.abo.bbox.fr (5.50.88.173:49670)
TCP:
Connects to rez-243-109.xgbe.cz (79.127.243.109:57299)
TCP:
Connects to rev-212-98-133-151.terra.net.lb (212.98.133.151:7123)
TCP:
Connects to ptr-90-159-235-192.is.net.tr (90.159.235.192:49244)
TCP:
Connects to ptr.abcom.al (109.69.5.32:4287)
TCP:
Connects to pppoe.178-67-93-38.avangarddsl.ru (178.67.93.38:58388)
TCP:
Connects to ppp-58-11-120-74.revip2.asianet.co.th (58.11.120.74:51061)
TCP:
Connects to ppp-5.137.45.16.nsk.rt.ru (5.137.45.16:49718)
TCP:
Connects to ppp-151-167.terra.net.lb (212.98.151.167:26556)
TCP:
Connects to ppp-124-122-235-117.revip2.asianet.co.th (124.122.235.117:49359)
TCP:
Connects to p57B7A196.dip0.t-ipconnect.de (87.183.161.150:58415)
TCP:
Connects to net-31-132-210-207.king-online.ru (31.132.210.207:58038)
TCP:
Connects to nat-88-212-36-36.antik.sk (88.212.36.36:64023)
TCP:
Connects to nat06.jhcomp.cz (178.23.219.6:1934)
TCP:
Connects to ip-78-102-115-64.net.upcbroadband.cz (78.102.115.64:49433)

I found nothing more, hope than someone can make a reverse engineering and say to us if it's backdoor or not.

mrfong - May 20, 2015, 12:16 pm

(May 20, 2015 12:13 PM)supreme00. Wrote: [\[CITE\]](#) they are probs lying there is no way njrat is backdoored it doesn't drop anything nor it connects to an ip
They aren't, and i'm not lying too, my passwords were hacked today, and the only thing i opend was njrat, i analyazed it and it says it drops files and it runs on startup?

Dafuq - May 20, 2015, 12:19 pm

(May 20, 2015 12:15 PM)mrfong Wrote: [\[CITE\]](#) that vpn is clean, now, if you only downloades these 2 , it might be the new windows you installed installs something else? i don't know alot about this,

but njrat is infected, i tested 3 different ones, and they drop some shit on temp now, it didn't happen with me before and i didn't renew my links, i installed this a month ago and today faced the issue , now about that guy who posted a vpn ip, can someone continue what he did it and get something else than a vpn ip?

My OS is 100% original. I did not download a Pirated Version. Hence Backdoor or Virus in my OS by default is Impossible.

I didn't use anything else apart from these two programs that could compromise my Laptop's Security. The other Programs I installed include -

1. Chrome
2. Skype
3. McAfee
4. MBAM
5. Virtual Router [to create Hotspot from my laptop]

That's All.

mrfong - May 20, 2015, 12:21 pm

@op, i sent you a pm , check it out :P

Dafuq - May 20, 2015, 12:23 pm

(May 20, 2015 12:21 PM)mrfong Wrote: [\[CITE\]](#) @op, i sent you a pm , check it out :P Responded, the dlls belong to njRAT. You can test it urself.

mrfong - May 20, 2015, 12:24 pm

(May 20, 2015 12:23 PM)Dafuq. Wrote: [\[CITE\]](#) Responded, the dlls belong to njRAT. You can test it urself.Confirmed, checked them out.. all of them belong to njrat :(

Dafuq - May 20, 2015, 12:25 pm

(May 20, 2015 12:24 PM)mrfong Wrote: [\[CITE\]](#) Confirmed, checked them out.. all of them belong to njrat :(

And all of them detected as Trojan/Virus. Isn't it?

Just a noob question, is it normal for Plugins to be detected as Virus? All DLL files belonging to njRAT are detected as Malware and Trojan.

21st Century Schizoid Man - May 20, 2015, 12:31 pm

The only problem is that,if it is him, he probably updates his website often

mrfong - May 20, 2015, 12:32 pm

alright guys, i sent pm to njq8 (njrat original owner) i asked him about this so he can give me the original files so we can compare..

hold on a min, why the original rat rar file size is 1.17 MB ?

Dafuq - May 20, 2015, 12:41 pm

<http://up.dev-point.com/downloadf-844b1a166eab1-rar.html>

Here is supposedly the original RAT and it's .5mb less than the size of what we are getting here on HF!

He B TeMy - May 20, 2015, 12:44 pm

(May 20, 2015 12:41 PM)Dafuq. Wrote: [\[CITE\]](#)
<http://up.dev-point.com/downloadf-844b1a166eab1-rar.html>

Here is supposedly the original RAT and it's .5mb less than the size of what we are getting here on HF!

That's only the size of an average DC stub, yey !

Anyway, just shit-posting here, have nothing to do with this and will never use it.

xVulnerable - May 20, 2015, 12:45 pm

Please. <https://hackforums.net/showthread.php?tid=4829620>

mrfong - May 20, 2015, 12:45 pm

(May 20, 2015 12:44 PM)He B TeMy Wrote: [\[CITE\]](#) That's only the size of an average DC stub, yey !

Anyway, just shit-posting here, have nothing to do with this and will never use it.

lol, you're acctually right :p

Dafuq - May 20, 2015, 12:53 pm

(May 20, 2015 12:45 PM)mrfong Wrote: [\[CITE\]](#) lol, you're acctually right :p

I still didnt get any response for the extra "0.5mb" from anyone. ???

SIM-2285183 - May 20, 2015, 12:57 pm

There's no VPN in the .zip file I downloaded?

I only got the rat software, the .dlls, and that's it, as well as other bits to make the program run.

Dafuq - May 20, 2015, 12:58 pm

(May 20, 2015 12:57 PM)xSnipez Wrote: [\[CITE\]](#) There's no VPN in the .zip file I downloaded?

I only got the rat software, the .dlls, and that's it, as well as other bits to make the program run.

I never said there is a VPN in njRAT. It's a different software altogether. But users have tested it, and they say its totally clean. Whereas njRat's DLL's all come up as Trojan horse/Virus.

SIM-2285183 - May 20, 2015, 1:01 pm

They obviously will come up as a trojan/virus, as they're required for the program to run.

The program within itself it fine, my mouse hasn't move, and my camera hasn't been turned on, neither have any of my passwords been changed.

Dafuq - May 20, 2015, 1:05 pm

(May 20, 2015 01:01 PM)xSnipez Wrote: [\[CITE\]](#) They obviously will come up as a trojan/virus, as they're required for the program to run.

The program within itself it fine, my mouse hasn't move, and my camera hasn't been turned on, neither have any of my passwords been changed.

But mine did. It really did. I have no reason to Lie against xVulnerable. For all I know he might be the best guy around on HF. I am not Disputing that. I just posted whatever happened at my end after I downloaded njRAT.