

Forum: [Hack Forums](#)

Thread: [RAT Deployment](#)

Percyville - November 8, 2018, 1:40 pm

So over the past year or so, I have been playing around with RAT's

I have used nanocore, Orcus (Never been Crypted;for the record;due to respect for Armada), Revenge RAT, Netwire, NjRat, Babylon RAT, Metasploit, Agent Tesla (I know isn't a RAT), 888 RAT tool and a few others.

Through trial and error I have been able to learn a lot about these tools.

I have played around with crypters too, I have used Flow Crypter, 888Tools Crypter, Sheild Crypter, The Old Phantom Crypter, TomC's Crypter and a few others.

I can now create client files to an extent UD,

That's great and all, but I am now having deployment issues.

I can easy create an exploit to say use CVE 2018-0802, 2017-0199, HTA (VBS and JS) macro etc, However, the issues lie in the deployment still.

As a red team tester fairly new to the field, as we are doing a white box test I know our target Company is using Sophos web filter.

Due to this when I am running my exploits, the URL needed to download the exe / mp3 etc depending on what format I upload seems to be blocked.

Overall, this is causing my exploits to be not downloaded and run on the machine.

I need somewhere to upload my exploits, that will be guaranteed to deliver.

When making the exploits, I rename the file types to mp3, jpg, ect and upon deployment the file gets renamed to exe.

I have used mixtape.moe, worked (then removed) doko.moe worked (then removed) coka.la (Removed instantly upon uploading) rgho.st (Webfiltered)

All of these worked in testing apart from the ones specified, however after consulting the admin of the company, he gave me a tip after explaining to him my issue, he checked the filters and didn't want to whitelist the URL's as obviously this would give us an unbiased result for our tests.

Has anybody any experience in this field?

In need of some help as I'm hitting a road block here.

CyberStrike - November 8, 2018, 5:28 pm

So pretty much you are using 3rd party sites and they are removing your payloads. These sites are rather well known when it comes to malware. Get your own hosting, very simple solution.

Percyville - November 9, 2018, 2:27 am

Logical, Fair enough. :)

Thanks Silent Watch

Rit4lin - November 9, 2018, 4:36 am

Thanks helped a lot

Regards Rit4lin

Ren And Stimpy - November 9, 2018, 9:03 am

Purchase your own host/vps and host your files

05317832892 - November 10, 2018, 3:40 am

Try using something like mega.nz or google drive.

Percyville - November 10, 2018, 4:56 am

Mega.nz and googledrive are ok, however, when Im putting a URL into my exploits, it needs to be the direct link, as opposed to a site the creates a one time download link after clicking the "download here button"

I will be setting up a VPS today so this should resolve the issue hopefully :)

brainfix - November 10, 2018, 7:00 am

I recommended GoogleDrive, it can easily bypass Chrome security. However you can generate direct GoogleDrive URL here:

<https://www.wonderplugin.com/online-tools/google-drive-direct-link-generator/> Enjoy

Percyville - November 10, 2018, 7:49 am

@brainfix, Thats Brilliant!

I genuinly thought they were one time click links.

Emans8412 - November 11, 2018, 12:21 pm

Learnt one or two things from this post

Percyville - November 15, 2018, 12:30 pm

haha you and me both,

With Google drive, after upoading any payloads, it may prompt saying this exe file could be malicious,

I would advise getting the link after the continue this :)