

Forum:[Hack Forums](#)

Thread: [How scambaiters load the RAT on victims PC without him doing anything](#)

MR. Belfort - May 4, 2024, 5:40 am

I'm watching Scambait videos on YouTube of YouTubers that are managed to hack scammers PC via RAT.

The YouTuber manage to convince the scammer to connect to his PC via Anydesk, and than they open the file transfer and managed to install/load the RAT directly on the scammers PC unknowingly without him have to open the rat file.

How does the scam baiter is doing it?

Burger - May 4, 2024, 5:43 am

The methods your referring to were happening before Any Desk became a bit more secure. Also if your speaking of the guy with Blue hair then you must know that they work directly with Any Desk and have external resources that are being utilized. This is possible to do but with good experience and social engineering and many tries!

MR. Belfort - May 4, 2024, 6:21 am

There are small youtubers scam-baiters which won't have the help on ANydesk

whitepearl - May 4, 2024, 7:09 am

I've seen one spoof malware as important documents (passwords.csv, bitcoin.txt...). Although this requires the scammer to transfer the malware to his own machine.

Absence - May 4, 2024, 7:15 am

So typically they are doing this highly assisted through social engineering. Part of this feat is that the scam artist they are baiting is under the assumption they are dealing with an elderly person who is not good with technology, so when they receive files from this person, they aren't expecting them to be infected with any type of malware. They believe they are scamming 70 year old person who can barely type or can't tell the difference between chase.com and command prompt.

However they do this, can be different ways, but it involves getting them to open a file of some sort.

DramaKing - May 4, 2024, 10:46 am

(May 4, 2024 07:09 AM)whitepearl Wrote: [\[CITE\]](#) I've seen one spoof malware as important documents (passwords.csv, bitcoin.txt...).

Although this requires the scammer to transfer the malware to his own machine.

Macros are disabled in Excel; text editors can't run code.

(May 4, 2024 05:40 AM)MR. Belfort Wrote: [\[CITE\]](#) I'm watching Scambait videos on YouTube of YouTubers that are managed to hack scammers PC via RAT.

The YouTuber manage to convince the scammer to connect to his PC via Anydesk, and than they open the file transfer and managed to install/load the RAT directly on the scammers PC unknowingly without him have to open the rat file.

How does the scam baiter is doing it?

I was going to say that Anydesk (later versions at least) require accepting prompts before the user on the remote-controlled PC can upload or download files. And no way no how will Anydesk execute other programs. TeamViewer can execute scripts (with permission of the other user), but I have seen nothing like that in Anydesk.

MR. Belfort - May 5, 2024, 3:43 am

Non gave the right answer. Check YT scam baits. These guys have a trick

Absence - May 5, 2024, 3:53 am

(May 5, 2024 03:43 AM)MR. Belfort Wrote: [\[CITE\]](#) Non gave the right answer. Check YT scam baits. These guys have a trick

Yes, typically it involves them remote connecting to a honey pot, but anydesk has file transfer capabilities.

There is also another method probably at play in some of the videos, where they compromise one scammer and use it to infect others in the network. A lot of the scammers are not deploying cutting edge security, and when compromised, they have a plethora of information. Regardless, this comes down to person, there is no 0day vulnerabilities only known to scammers, it is more than likely some sort of social engineering.

The trick is to make them believe you are able to be fooled by them. Check the tricks that they use on youtube videos. They aren't anything complicated, on either side.

Amanillah - June 16, 2024, 8:18 am

(May 5, 2024 03:43 AM)MR. Belfort Wrote: [\[CITE\]](#) Non gave the right answer. Check YT scam baits. These guys have a trick
you are a good man

Ivanov_1 - August 23, 2024, 9:12 am

I have heard that scambaiter at some point uses a reverse shell, and after that he manages to interact with the scammers system. Of course pure speculations, i never seen proof of that.

James Clown - August 24, 2024, 1:28 am

(May 4, 2024 05:40 AM)MR. Belfort Wrote: [\[CITE\]](#) I'm watching Scambait videos on YouTube of YouTubers that are managed to hack scammers PC via RAT.

The YouTuber manage to convince the scammer to connect to his PC via Anydesk, and than they open the file transfer and managed to install/load the RAT directly on the scammers PC unknowingly without him have to open the rat file.

How does the scam baiter is doing it?

Not all scambaiters are legit. I know at least one who is faking the whole operation, for the likes.

Byte Wizard - August 25, 2024, 7:37 am

(May 4, 2024 05:40 AM)MR. Belfort Wrote: [\[CITE\]](#) I'm watching Scambait videos on YouTube of YouTubers that are managed to hack scammers PC via RAT.

The YouTuber manage to convince the scammer to connect to his PC via Anydesk, and than they open the file transfer and managed to install/load the RAT directly on the scammers PC unknowingly without him have to open the rat file.

How does the scam baiter is doing it?

You are all wrong and all correct

In a lot of cases its as simple as having malware on their VM desktop like Banking.txt.scr etc and the scammers sometimes steal this "valuable" file and open it
I saw one as simple as "sexy-nudes.png.exe" that had the admin/uac shield logo on it and asked for admin perms and multiple scammers still ran it

Another method is to get the scammer to give you their connection code instead and then pretend youre struggling to figure out how to give control over to them while you drop and run a payload

However there are in fact methods to interfere with the softwares communication and flip it
Will not disclose how it works or which software are vulnerable to it
It should still be possible in modern versions but the PoC's I was shown were all for older versions

Scammers are not intelligent people and likewise scambaiters rarely have to put in much effort at all
There are lots of problems in the scambaiting scene that the public is unaware of
I can personally confirm at least one of these youtubers is on HF and uses eWhoring to make money, took donations from viewers and bought luxury items for themself instead of paying anyone involved or buying tools that could help them etc

In fact most of the scambaiters you hear talking dont even do any of the work themselves
They are often just a face and voice

Jim Browning at least does work with authorities as best he can and does decent work
I cannot recommend getting into scambaiting it is quite futile and if you do anything more than talk to the scammer you are in fact breaking the law, hacking criminals is still hacking (very unlikely to be vanned for it of course but still needless risk)

Hreidmar - August 26, 2024, 2:13 pm

(Aug 25, 2024 07:37 AM)Byte Wizard Wrote: [\[CITE\]](#) Scammers are not intelligent people and likewise scambaiters rarely have to put in much effort at all

Exactly this! These scammers are being employed off of the street by these groups that not only they don't know much about computers themselves but I'm sure their employee doesn't make them do cybersecurity awareness training at work where they teach people how not to fall for basic social engineering tactics.

Then you also include poor IT infrastructure that is usually low quality and quite vulnerable.
So it's not that hard to make at least one of these guys fall for a trick then work from there by infecting their whole network.

It's funny though considering they are raking in millions each year yet they refuse to invest into better security themselves lol.