

Forum:[Hack Forums](#)

Thread: [Has the ratting scene decreased?](#)

Archbe - March 3, 2023, 5:50 pm

Hey guys, for the last while I've been monitoring the remote administration tool's section. I know for a fact 8 years ago the scene was thriving.

Is my thought process right here?

Archbe - March 4, 2023, 6:29 am

(Mar 3, 2023 07:04 PM)Dyne Wrote: [\[CITE\]](#) The scene has shifted.

There are more simple tools to accomplish what, previously, people would use a Remote Administration Tool for.

Some only need credentials, so they opt for a specialized stealer.

Some need keystrokes, so they opt for a specialized keylogger.

Some need a reverse proxy, so they opt for socks servers.

Some need to mine, so they opt for mining / panel nets.

Some need financial information, so they opt for specialized hVNC and bankbots.

Some need red teaming penetration testing tools, so they opt for those.

Following a specialization greatly increases your chance for success. It lowers both heuristic detections(which maintaining the constant SSL/TLS connection, plugins, behaviors) and essentially bloatware of useless(to them) features. Serious threat actors are more focused on botnets and their client's/stub's longevity, and drop the specialized tools as they need it per individual circumstance. They don't often come to these forums and public messageboards looking for tutorials.

All of the above is why you typically only get newbies and uninformed people posting here now asking for "the best most advanced RAT".Well that made a lot of sense.

thigle - March 8, 2023, 4:15 am

so did the RAT scene died completely or is just in decline...? specificallay, is there anyything that allows to remotely access android phone with 0 to 1 click exploit cooked into interface for a nooblike me ? does the targeted phone need to be physically accessed ? if not, is some link necessary to be open by the user of the targeted phone or can be installed in stealth without him/her knowing ? sorry if these are very beginner's questions, but i am a beginner. thank you for any explanation

moom825 - March 8, 2023, 5:43 am

(Mar 8, 2023 05:15 AM)thigle Wrote: [\[CITE\]](#) so did the RAT scene died completely or is just in decline...? specificallay, is there anyything that allows to remotely access android phone with 0 to 1 click exploit cooked into interface for a nooblike me ? does the targeted phone need to be physically accessed ? if not, is some link necessary to be open by the user of the targeted phone or can be installed in stealth without him/her knowing ? sorry if these are very beginner's questions, but i am a beginner. thank you for any explanation

this thread is the wrong place to ask that. and a 0-1 click android exploit costs upwards to 2 million, and are generally not user friendly.

moom825 - March 8, 2023, 7:31 am

(Mar 8, 2023 08:26 AM)Dyne Wrote: [\[CITE\]](#) Hello,

Unfortunately you are incorrect.

There are many, many "one click" url droppers that are equivalent to java drive-bys that net around \$3-4k. These are rampant in SMS blasting campaigns.

There are 0 click/1 click exploits that exploit the MMS loading bay which security vendors are working hard at patching now

<https://thehackernews.com/2023/02/samsung-introduces-new-feature-to.html>

These range from 15 - 50k and often bundled with botnet loading panels and often subject to "refud Steganography" exploiting the vulnerable .heif, and .heic extensions as a spoofed downloader script.

There are 1 click exploits for the simple buffer queue data locator(audio/video codec) that again rely on spoofed extensions using `MimeTypeMap.getFileExtensionFromURL("")`

Android and mobile malware are fascinating, but greatly differ from Windows RATs/botnets. Often, people are under the assumption that they perform alike when in reality they have many mutually exclusive portions to their building block infrastructure.

I will say, however, that there are no exploits on either side of the fence that allow you to commit excessive financial fraud or take absolute control with a "Few clicks". Theory is often much different than reality.

oh, that is my mistake then, I expected it to be much more expensive then that. I guess I assumed the price of a windows 0 click would be similar to android, i suppose not. my mistake.

DI?E - March 9, 2023, 12:28 pm

(Mar 3, 2023 06:50 PM)Archbe Wrote: [\[CITE\]](#) Hey guys, for the last while I've been monitoring the remote administration tool's section.

I know for a fact 8 years ago the scene was thriving.

Is my thought process right here?

The rat scene here is dead. Has been for various years. All cut, copy and paste. Nothing new in the past few years. At least nothing of change that brings anything new to the table.

Midi-Chlorian - March 10, 2023, 9:22 am

Anti-virus engines are getting better at detecting malware which makes it harder for coders to keep their tools alive. It's a constant cat and mouse game and I feel it will swing in the other direction at some time.