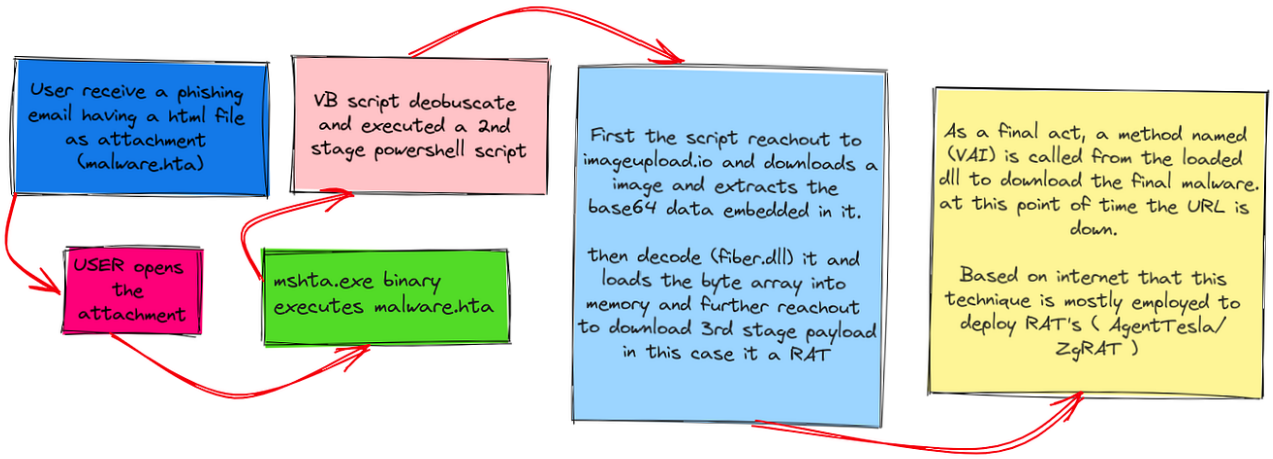
Unmasking NJRat: A Deep Dive into a Notorious Remote Access Trojan Part1

infosecwriteups.com/part1-static-code-analysis-of-the-rat-njrat-2f273408df43

JustAnother-Engineer November 21, 2023



NjRAT is a type of malware that allows a remote actor to gain control of an infected computer system. It is one of the most widely used types of malware on the Internet due to its easy accessibility, free tutorials available on clear web, and wide range of functionalities to evade detection tools.

the sample analyzed in this blog was first seen in the month of October of 2023. As of now the file is found to be malicious by multiple AV/EDR tools.

Virustotal result + PE headers of the file being analyzed.
By analyzing headers we see that this version of malware was compiled on Sep 2 2023. As its based on .Net we can statically reverse engineer and review the code of the binary/executable.

Initial review of string output of the binary we see few interesting stuff like a registry path , domain , few commands , executable names and network rules.

Floss output of the binary

Initialization :

The malware first create a registry key value pair “{di:!}” under current user and we see implement a mutual exclusion object to hinder concurrent infections on a single device.

Registry Key , Mutex initialization

Upon reviwing statically defined variables we see few interesting things as highlighted below , we see a port (18801) where connection is initiated , registry name (RG variable) , Registry path (sf variable) , VR version number , string in variable VN contains base64 encoded value of “HacKed”. The variable “Y” stores random character which is being used as separator while sending back the data to C&C server.

Interesting static variables
Reviewing the OK.RC function which was being passed to mutex which in turn calls a function OK.INS() which initialized persistence mechanisms.

Persistence Initialization function

Persistence :

Reviewing the INS function , first we see the malware trying to find the file “C:\\Windows\\Microsoft system.exe” and copy the malware to this path and deleting the current instance of the malware and starting the new process of malware as “Microsoft system.exe”.

Further we see exclusion being added via netsh for the traffic from this malware file. Then we see file being added to both current user and local machine registries. We also see the malware is being copied to startup folder with name “118f5683ac8ec11fa5ebd063bb65cc3b.exe” for persistence. Any app / exe placed inside startup folder would be launched upon booting the OS.

Registry and startup persistence
Further we see the malware killing a process “Exsample.exe” if its running. based on the research , it indicates that this file is a old version of same malware. We also see that the file copied to windir is being hidden.

Killing Exsample.exe and hiding the malware
further we see persistence via autorun , As highlighted below we see that the malware is again copied into ProgramFiles directory of each logical drives as “svchost.exe” and then creates a autorun.inf file to run them automatically. Further malware hides the created autorun file.

persistence via autorun

C&C communication

Connecting to the C&C server : reviewing the connect function we see that the malware is connecting the “0.tcp.eu.ngrck.io” host , on sucessful connection its sends below information.
- Environment variables
- machine name

- user name
- machine date
- Details OS information
- processor type
- camera status
- string “HacKed”

Connect function.
Further receiving the data from the threat actor , then that data is handled by creating a new thread.

Threat actor data handling.
There are multiple commands available in this RAT with in the OK.im however we will discuss only few in details which are interesting.

Below are the list of few capabilities observed in this RAT :

1. Can spawn new process.
2. Can modifies the startup page setting for Internet Explorer using the Registry to start a page/link upon opening. this can be used for Downloading other malwares , redirecting to phishing links , Exploit vulnerablities , installing other backdoors or to lauch a DDOS attacks.
3. Has capability to shutdown / restart / logoff the session
4. Can spawn custom error messages.
5. Can invoke the “speak” method on the speech synthesizer object to synthesize the specified text.
6. Uses Kernel32 Beep method to create beeps of specified frequency. further we see a command named “Piano” which leverage this function to create a music.
7. OpenCD / closeCD drive (this is the command which someone uses to troll their victims)
8. Disabling / enabling keyboard and mouse inputs.
9. Turning monitor on / off.
10. Taking over mouse control
11. Enabling / Disabling CMD.
12. Disabling/enabling built in registry tools, sytem restore functions and Task manager.
13. Taking over cursor.
14. Control music playing.

Few of the commands observed that attacker can use.
As this blog is already getting big we will discuss other functionalities, dynamic analysis and detection mechanisms for this malware strain in our next blog.

Thank you for your time!