Malware Analysis — njRAT

medium.com/@b.magnezi/malware-analysis-njrat-5633847bd6f1

0xMrMagnezi March 19, 2024

njRAT is a remote access Trojan (RAT) that allows attackers to gain unauthorized access to a victim's computer. It is capable of keylogging, taking screenshots, and controlling the victim's webcam and microphone. It can also download and execute additional malicious payloads.

0xMrMagnezi

--

Figure 1: Malware Bazaar Entry

After downloading and extracting the zip file, I used OLEtools because I knew I was going to deal with an Office file — specifically, a PowerPoint file.

Figure 2: shows the first analysis using oleid

After noticing the presence of Macros within the file, the tool olevba was used to gain more insight into what those Macros are.

Figure 3: Observing The Macros

It was observed that this macro contains a suspicious URL linking to Pastebin. It's also noteworthy that this macro is configured under the 'AutoOpen' feature, which automatically executes macros or actions when a presentation is opened.
It was decided to use curl to download the content from this URL and delve deeper into the analysis. This initial URL redirected to another URL, which contained another payload.

Figure 4: Downloading Stage 2 & 3

The output of stage 3 contained a simple VBS obfuscated code with recognizable words such as 'replace,' 'base64,' 'WScript,' and 'PowerShell,' as marked in Figure 5.

Figure 5: Obfuscated Stage 3 VBS code

Figure 6: After Deobfuscation of the variable

This variable contained a Base64-encoded string that needed to be decoded and reversed. I decided to use CyberChef, as shown in Figures 7 and 8.

Figure 7 & 8: Decoding from Base64 and extracting 2 URLs

Those two URLs contained two different obfuscated strings, as shown in Figure 9. The obfuscation appears to be related to the characters: '↓:↓↓'.

Figure 9: Obfuscated string

In the decoded output from CyberChef (Figure 8), the presence of the Replace function led me to believe that it was related to the next stage I extracted.

Figure 10: Showing the Replace Function

I decided to use this replacement technique to make sense of these long strings. My initial suspicion was that these two strings were intended to construct a new executable file.

Figure 11: Using CyberChef to decode on the First file

Figure 12: Using CyberChef to decode on the second file

My suspicion was correct; the first file is a DLL, and the second one is an executable, both written in .NET.

Figure 13: DiE on both files

This is the final stage of the malware, as it contains the actual malicious payload. Within the debugger, many functions related to a Keylogger and the transmission of information over a socket were observed.

Figure 14: Functions of the malware

We can also observe many of these functions, and more, using the tool PEstudio.

Figure 15: Using PEstudio on the executable

Figure 16: Using PEstudio on the DLL

At this point, I decided to run the malware to extract network-related IOCs.

Figure 17 & 18: Network Communication

IOCs:

- cefa4ebf82b3d077a68ce1933be3dc6e9cadce8bc27671a5fcd76ee2f4d04977.ppam — 6175e14e465756c626ccc0f398fcdcb0
- stage3.vbs — edf8f50f318c20bccb889743172d9fd2
- out1.dll — 4b7d118b20d8854372129f53365d529f
- out2.exe — d189af41737b287469ca5f5589dcbdf1
- hxxps://pt[.]textbin[.]net/download/itm1dkgz7c
- hxxps://paste[.]ee/d/ESa4q/0
- hxxps://pt[.]textbin[.]net/download/tmo7gc3cgs
- hxxps://pt[.]textbin[.]net/download/igvxdijw4q
- hxxps://paste[.]ee/d/jtSmT/0
- hxxps://paste[.]ee/d/ea2Mw/0
- hxxps://pt[.]textbin[.]net/download/insdj4bhn2

In conclusion, the analysis of njRAT revealed a sophisticated malware strain designed for remote access and data theft. Its initial infection vector through a malicious PowerPoint file underscores the need for caution with email attachments and files from unknown sources.

The malware's keylogger and socket communication capabilities indicate its potential for capturing sensitive information and enabling remote control of infected systems. Its use of obfuscation and encoding techniques highlights the complexity of modern malware.

This analysis underscores the ongoing threat of remote access Trojans and the importance of proactive security measures, including software updates, endpoint protection, and user education, to mitigate such risks.