LimeRAT Malware Analysis from ANY.RUN: Extracting the Config

DUBAI, UNITED ARAB EMIRATES, March 29, 2023 /EINPresswire.com/ -- ANY.RUN, a cybersecurity company developing an interactive sandbox analytical platform for malware researchers, presents the LimeRAT Malware Analysis. Here are some highlights from the hood of a modular RAT — LimeRAT:

What is LimeRat

LimeRAT is a Remote Access Trojan (RAT) that's been around for a few years now. It's a versatile piece of malware designed to give attackers control over an infected system. What makes LimeRAT particularly interesting is its ability to perform a wide range of malicious activities. Some of these include keylogging, stealing passwords, and capturing screenshots. Additionally, LimeRAT can execute arbitrary commands, drop other malware, download and upload files, and even use the infected machine for crypto-mining or DDoS attacks.

LimeRAT malware analysis

ANY.RUN opened a sample in Detect It Easy. Upon inspection, ANY.RUN observed that the code has been obfuscated (MITRE T1027) and unreadable: the names of classes, methods, and variables are made out of random glyphs. Since the sample is written in a .NET language, ANY.RUN opened it in DnSpy.

LimeRAT decryption algorithm

1. Instances of the RijndaelManaged and MD5CryptoServiceProvider classes are created. If

analysts search for the RijndaelManaged class on MSDN, they see that it is essentially an obsolete implementation of the AES encryption algorithm (MITRE T1027). The MD5CryptoServiceProvider class, as the name implies, is used to compute an MD5 hash.

2. An array of 32 bytes is created and initialized with zeros. This array will be used to store the AES key.

3. To generate the key, the MD5 hash of another string from the configuration class is first computed (in our case, the string is “20[.]199.13.167”).

4. Next, the first 15 bytes and then the first 16 bytes of the computed hash are copied to the previously created array. The last element of the array remains zero.

5. The generated key is set to the key property of the RijndaelManaged instance. The Mode property is set to CipherMode.ECB.

6. Finally, the original string is decoded using the Base64 algorithm and decrypted using the AES256-ECB algorithm.

ANY.RUN efficiently extracts configurations for malware like LimeRAT, ultimately saving security researchers precious time and resources.

Read our article to see how ANY.RUN successfully analyzed LimeRAT, uncovered its configuration and determined the decryption algorithm employed to decode the string containing the C2 address.

Galina Zueva
ANYRUN FZCO
email us here
Visit us on social media:
Twitter
LinkedIn
