EINPRESSWIRE

PrivateLoader: Analyzing the Encryption and Decryption from ANY.RUN

DUBAI, UAE, April 28, 2023 /EINPresswire.com/ -- ANY.RUN, a cybersecurity company developing an interactive sandbox analytical platform for malware researchers, presents the Analyzing the Encryption and Decryption of PrivateLoader.

Here are some highlights from the inner workings of PrivateLoader:

What is PrivateLoader

PrivateLoader is a malicious loader family, written in C++ and first discovered in early 2021. It is known for distributing a wide range of malware, from simple information stealers to complex rootkits and spyware, utilizing payloads.

- The code itself involves the decryption of loaded libraries.
- At present, there are two versions of PrivateLoader available: one protected by VMProtect, and a regular version.
- Every day, between 2 and 4 samples of this malware are uploaded.

Static Analysis of the Source File

Analyzing the discovered strings allows us to identify several interesting elements:

- A user-agent, which is likely used to masquerade as a legitimate browser application
- URL addresses for determining the current IP and geolocation

PrivateLoader dynamic analysis with ANY.RUN

We analyzed the sample in ANY.RUN interactive malware sandbox.

Analyzing the process tree leads to the following conclusions:
1. The main PrivateLoader process creates a child process named “FhuC750omh76YtB1xgR7diEy.exe”, whose executable file is located in the user’s “Pictures” directory (T1564 – Hide Artifacts).
2. The created child process is added to the startup using Task Scheduler (T1053.005 – Scheduled Task/Job: Scheduled Task).

Technical Analysis of PrivateLoader

For the technical analysis, the following tasks were set:
1. Locate the C2 server within the code
2. Identify the encryption algorithms for the C2 server and, if possible, for strings as well.
3. Automate the decryption of the C2 server and strings

Example of automating C2 server decryption of PrivateLoader

To automate the extraction of data and configuration, we can use the Triton framework. It will emulate code blocks that contain all the necessary encrypted information.

Therefore, by emulating all the code blocks that contain encrypted data, we can obtain a set of strings with the necessary information, including the C2 server.

Extracting the PrivateLoader configuration

The decrypted data includes C2 addresses and strings. The strings contain information such as: used libraries and their functions, registry keys, paths to crypto wallets and browsers, etc.

PrivateLoader's main feature is the XOR of all strings it interacts with (C2, URLs, DLLs). Also, some samples are protected by VMprotect, which makes the code a bit more complex due to the use of many functions.

At ANY.RUN we understand the importance of cybersecurity in today's digital landscape. Our team of experts is dedicated to providing cutting-edge cybersecurity solutions to help organizations stay protected against evolving threats.

Read our article to see how ANY.RUN successfully analyzed PrivateLoader.

Vlada Belousova
ANYRUN FZCO
2027889264
email us here

Visit us on social media:
Twitter
YouTube