Threats & Research

Analysis of LockerGoga Ransomware

Share

Noora Hyvärinen
27.03.19 4 min. read

Tags: Boost Cryptopp LockerGoga Malware Ransomware Windows

We recently observed a new ransomware variant (which our products detect as **Trojan.TR/LockerGoga.qnfzd**) circulating in the wild. In this post, we'll provide some technical details of the new variant's functionalities, as well as some Indicators of Compromise (IOCs).

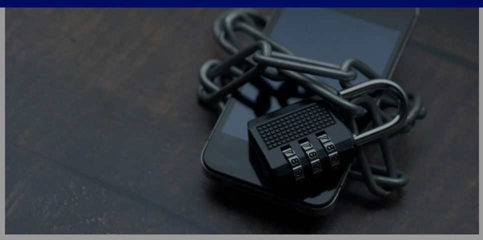
Overview

Compared to other ransomware variants that use Window's CRT library functions, this new variant relies heavily on the less commonly used Boost library. For example, instead CRT's rename function, it uses boost::filesystem::rename. The change makes technical analysis more difficult for researchers, as it makes function identification harder.

The functionalities for file enumeration and file encryption are split into different processes. File path sharing happens using the Boost.Interprocess library, which makes it harder to analyze the processes separately.

Highlighted article

THREATS & RESEARCH



Is iPhone's Stolen Device Protection Enough to be a Gamechanger? We Tested It.

Ash Shatrieh
18.03.24 6 min. read

first_create_process_api_monitor

The main functionality is inside the "master" process, it enumerates files on the infected system and executes child processes to encrypt files.

If we provide additional argument "-l", the process will create "*C:\\.log.txt*" file and write file paths and error messages.

To parse command line arguments, the sample uses *Boost.Program_options library (ref. screenshot below)*

master_process

Before starting the encryption phase, the "master" process enumerates sessions and logs off from all but the current process's session.

The process uses ProcessIdToSessionId function to get a session associated with the current process.

enum_sessions_second

second_changes_admin_passwords

The "master" process creates a "shared memory" using the Boost.Interprocess library and executes child processes (in the same executable) with the argument "-i SM-tgytutrc -s", where "-i " specifies a shared section name and "-s" stands for "slave".

According to Wikipedia: "*shared memory is memory that may be simultaneously accessed by multiple programs with an intent to provide communication among them or avoid redundant copies*"

On the screenshot, we see that, after changing passwords, it uses *Boost library* to initialize *shared memory* and execute child processes ("slave" processes):

change_admi_pswds_create_subProc

File paths are encoded with Base64:

Child processes decode the data from the shared memory.
The data on the *shared memory* has the following structure: The first "DWORD" represents the file index, while the second one represents the size of the "base64" encoded data:

After decoding a file path, a child process generates a key/IV pair using the Crypto++ library.

"*OS_RNG*" function uses CryptoGenRandom function from Windows, another function is from *Crypto++* library to generate a random numbers:

algorithm. It also appends the generated key/IV pair in an encrypted form to the end of the file. The key/IV pair is encrypted with the public key, which is embedded in the executable:

After it encrypts a file, a child process overwrites the first byte of the encoded data in shared memory with a "0" byte.

Network changes

Next, it deletes the executable via ".bat" file which contains commands to delete the executable and the bat file itself.

At the end it logs off the current process's session:

Conclusion

Overall, the latest variant of the **LockerGoga** ransomware is not complex or complicated. Because it uses the Boost library and Crypto++ instead of the more common CRT library functions however, it does make it a bit more troublesome for a threat researcher to analyze the sample.

Categories
Threats & Research

Tags
Boost Cryptopp LockerGoga Malware Ransomware Windows

Related posts

THREATS & RESEARCH
Stolen Device Protection Enough to be a Gamechanger? We Tested It.
Read article
Ash Shatrieh
18.03.24 6 min. read

THREATS & RESEARCH
disguised as wedding invitation sent to senior citizens
Read article
Amit Tambe
13.03.24 7 min. read

THREATS & RESEARCH

THREATS & RESEARCH