Threats & Research

Analysis of LockerGoga Ransomware

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

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.

File encryption

If we execute the sample without any arguments, it moves the executable to the %TEMP% directory with hard coded name “tgytutrc{number}.exe” and executes it with the “-m” argument (where “m” stands for “master process”):

As we can see on the screenshot, the main executable uses functions from Boost library to copy and execute the sample.

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

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.

This is a list of active sessions on a test machine since session “1” is the session of the process, it logs off only from session “0”:

After that, the “master” process changes the password for all administrator accounts to “**HuHuHUHoHo283283@dJD**“.

I’ve created a standard user, but it only changes the password for administrator accounts:

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):

Next, the "master" process enumerates files and writes their paths (encoded with Base64) in the shared memory.

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:

Before the encryption, a "slave" process renames a file using *Boost::Filesystem::rename* function:

Next, the child process encrypts the file's content using the Rijndael 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

After the encryption phase, the "master" process enumerates all network interfaces and disables them.

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.

Indicators of compromise (IOCs)

SHA256:

- C97d9bbc80b573bdeeda3812f4d00e5183493dd0d5805e2508728f65977dda15

Hard coded mutexes:

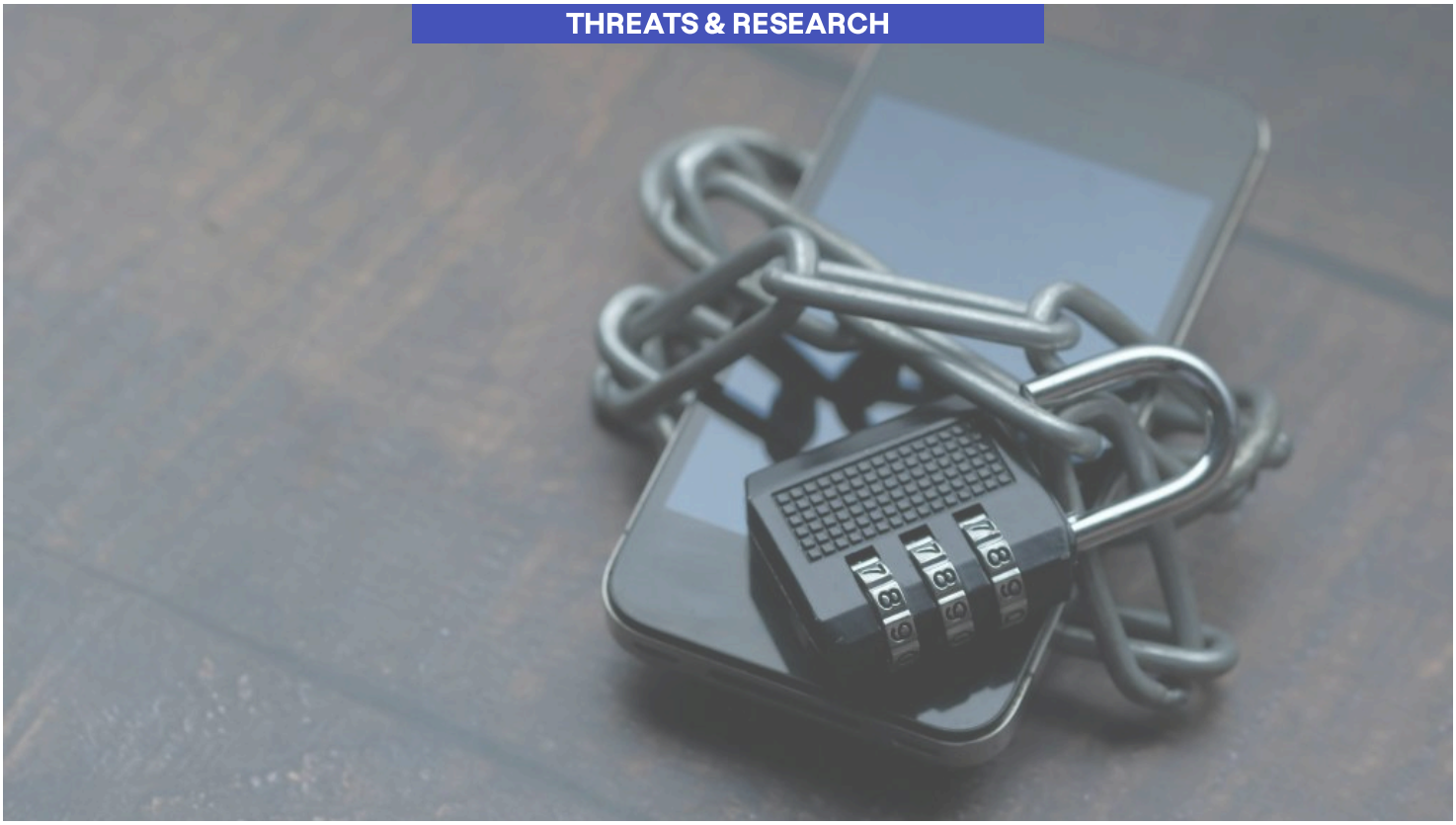
- MX-tgytutrc

Directory with malicious executables:

- %APPDATA%\Local\Temp\tgytutrc8.exe

Noora Hyvärinen
27.03.19 4 min. read

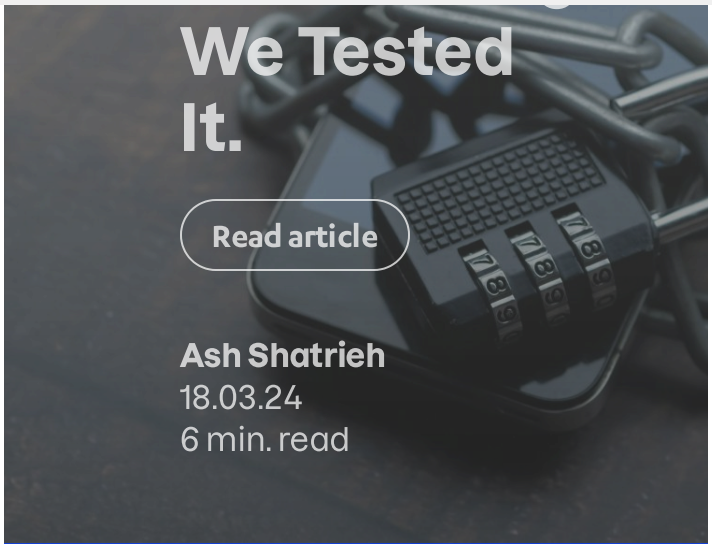
Highlighted article

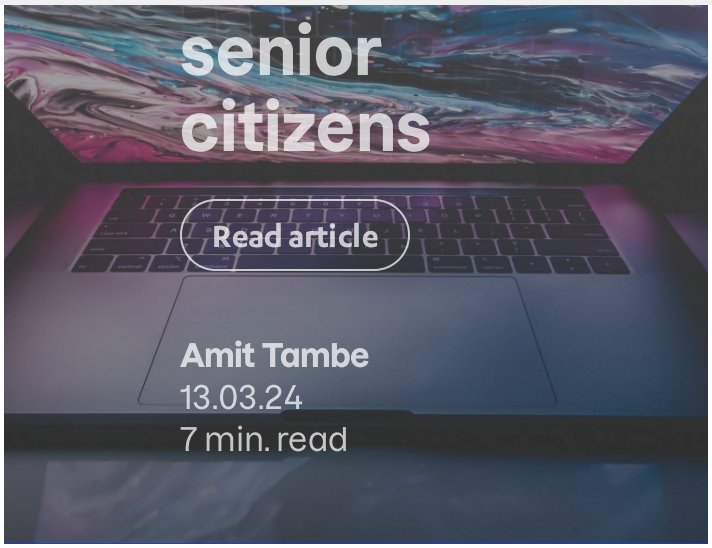


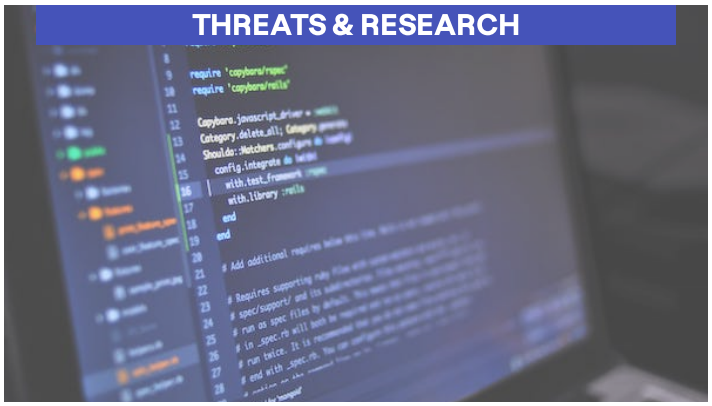
Is iPhone's Stolen Device Protection Enough to be a Gamechanger? We Tested It.

Ash Shatrieh
18.03.24 6 min. read

Related posts







Scams galore! Don't update later, update now!

Amit Tambe
20.02.24 3 min. read

Back to front page

Privacy Policy

Terms of Service

Follow us

Facebook
Instagram
Twitter
Youtube