INTEZER

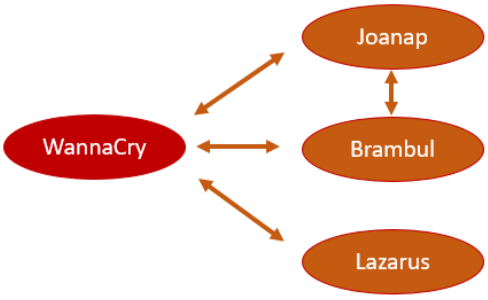
WannaCry Ransomware: Potential Link to North Korea

Overview

On Friday, 12 May 2017, a large cyber-attack using WannaCry ransomware was launched, infecting more than 230,000 computers in 150 countries, demanding ransom payments in the cryptocurrency bitcoin in 28 languages. WannaCry used the leaked EternalBlue exploit from the NSA, in order to spread itself throughout Windows networks.

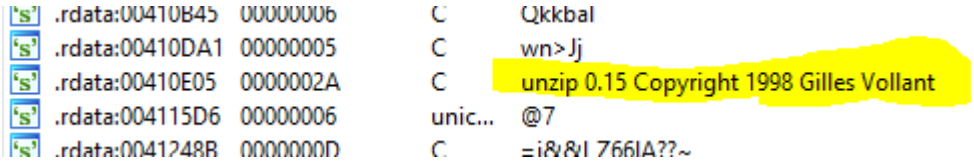
Potential Link to North Korea

Using Intezer's Code Intelligence™ technology, we were able to find strong links to other malware families, believed to be developed by North Korean hackers, or known to be used in attacks against South Korean organizations. In this document, we will share some of the details that led us to connect this large-scale ransomware attack to these malware families.

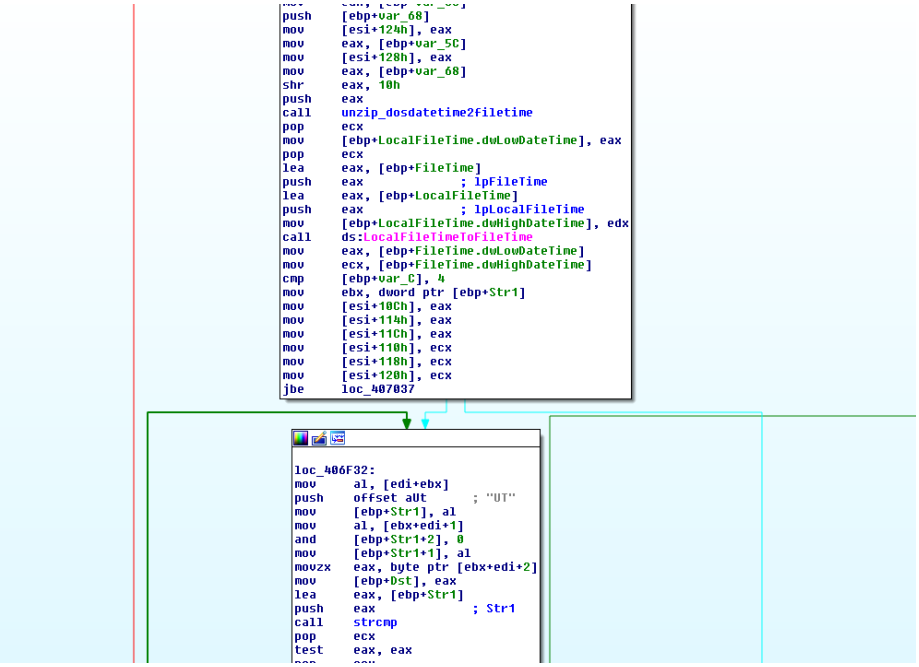


Unique Unzip Library

By extracting thousands of code-pieces ("genes") from WannaCry samples and identifying them in our Global Genome Database, which contains billions of code pieces of both malware and legitimate applications, we have found several pieces of code from a rare version of a known library. The original, more common library is "unzip 0.15 Copyright 1998 Gilles Vollant", as we can see in WannaCry's strings:



But this was actually a modified version of this popular library. The modified version of the library was seen only rarely – mostly in malicious programs. Here is the unique code ("gene") of this library version:

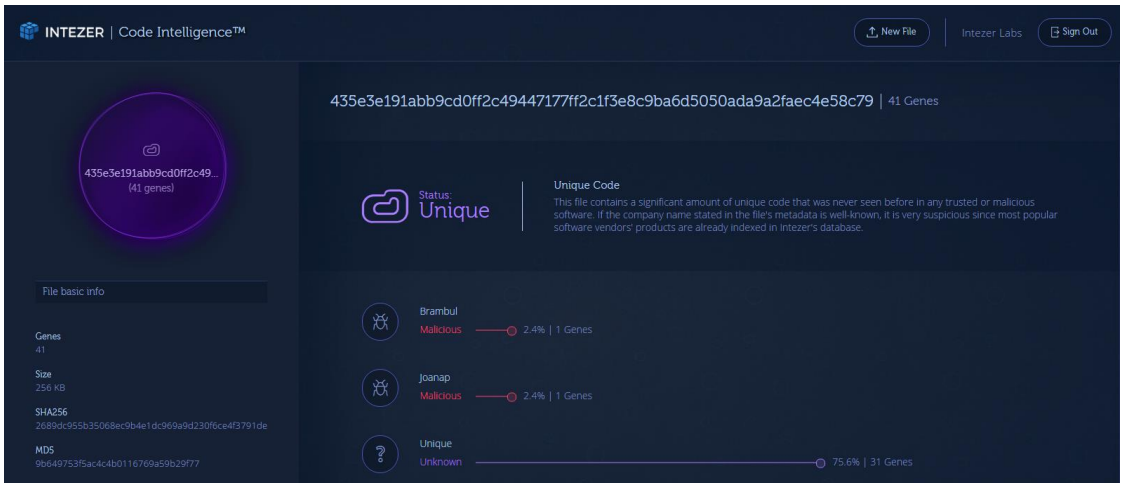


Code Intelligence™ technology was able to identify this piece of code as extremely unique and mostly seen in malware (e.g. Explosive Malware). Searching for clues, we have conducted a hunt in VirusTotal to find files using the same piece of code.

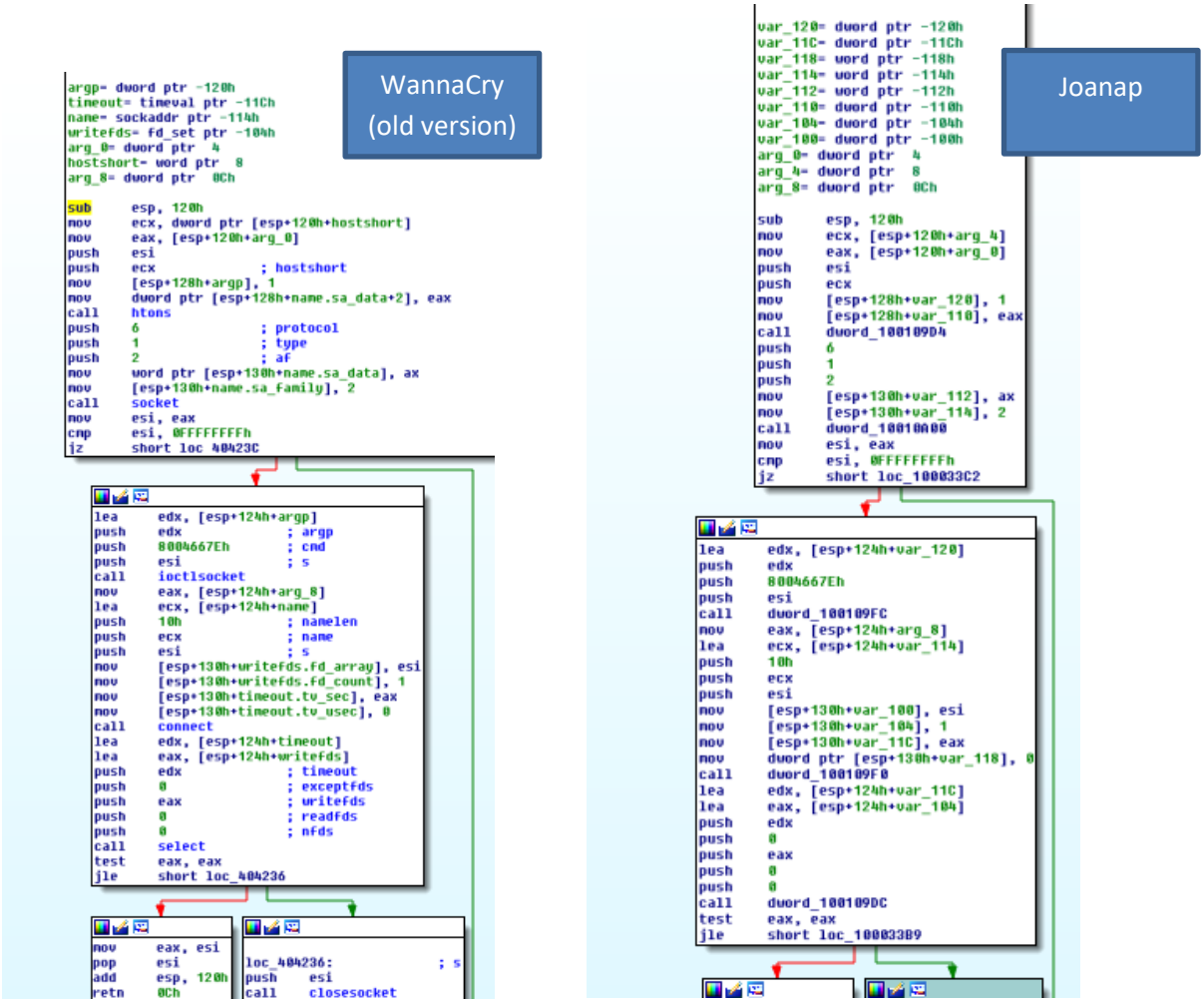
The search resulted in finding a relatively small set of files, many of them were versions of the WannaCry malware. Some of the WannaCry old versions, as of today (May-16, 2017), **are not detected by any Anti Virus (0 / 60 detections)**. These versions are most likely to be modules dumped from memory in a Dionaea (https://github.com/rep/dionaea) honeypot server, due to the special submission paths in VirusTotal, such as:
"/var/dionaea/binaries/smb-gse1z2_a.tmp"

The oldest sample uploaded by the honeypot was:
435e3e191abb9cd0ff2c49447177ff2c1f3e8c9ba6d5050ada9a2faec4e58c79 (SHA256)

We believe this is an older version of WannaCry due to its similar use of the rare library, the usage of TOR as C&C, and it's SMB Worm capability. A quick analysis using Code Intelligence gives the following results:



It is clear to see that this early version of WannaCry, first seen in 4/27/2017 17:06, shares code with Joanap and Brambul malware families, **which are known to attack South Korean organizations**. For example, this is a code piece found similar to Joanap in this sample:

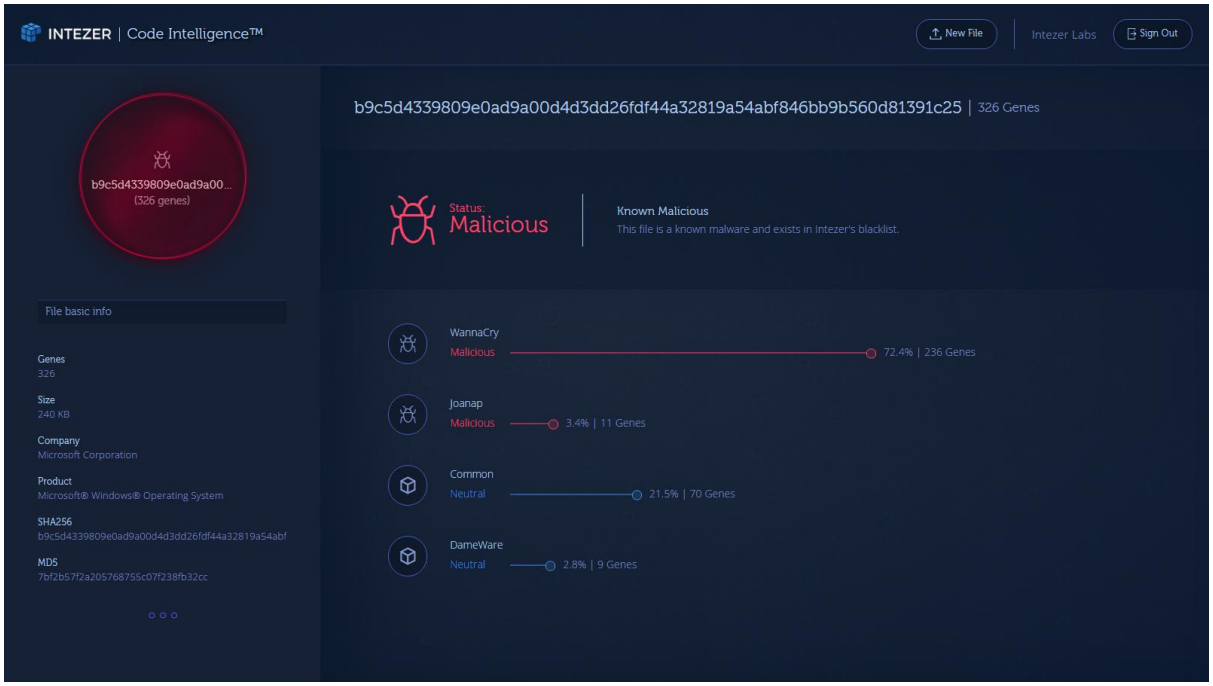


In addition, it seems that this sample contains an SMB brute-force capability and hardcoded password strings, which is very similar to the behavior of Brambul worm, as described in Symantec's blog (https://www.symantec.com/connect/blogs/duuzer-back-door-trojan-targets-south-korea-take-over-computers):

.data:00416653	00000007	C	master
.data:0041665B	00000007	C	dragon
.data:00416663	00000009	C	1qaz2wsx
.data:0041666F	00000007	C	111111
.data:00416677	00000007	C	abc123
.data:0041667F	0000000B	C	1234567890
.data:0041668B	00000008	C	welkome
.data:00416693	00000008	C	welcome
.data:0041669B	00000009	C	baseball
.data:004166A7	00000008	C	1234567
.data:004166AF	00000005	C	1234
.data:004166B7	00000009	C	football
.data:004166C3	0000000A	C	123456789
.data:004166CF	00000006	C	12345
.data:004166D7	00000007	C	qwerty
.data:004166DF	00000009	C	12345678
.data:004166EB	00000009	C	password

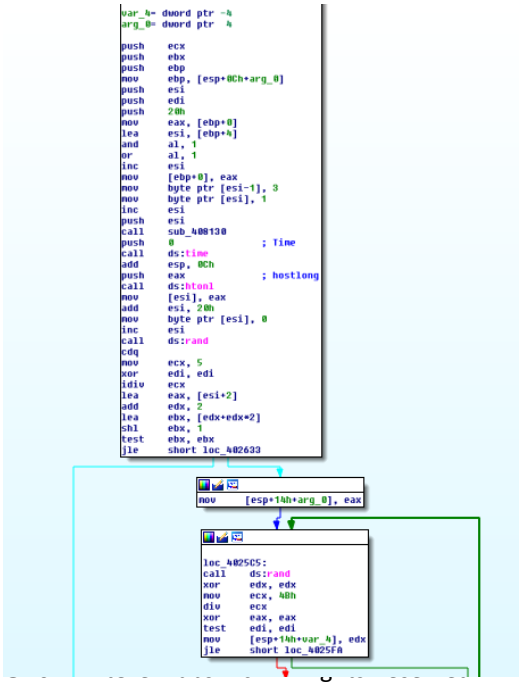
Clear Code Connections to Lazarus and Joanap

Intezer's Code Intelligence™ technology immediately found connections between the Joanap malware and recent WannaCry samples, as shown in the report below:



Moreover, Intezer's Code Intelligence™ technology immediately found connection between the Lazarus group, a hacking group associated with North Korea, and previous versions of WannaCry. These versions of WannaCry were found by our search for the unique library described in the previous section.

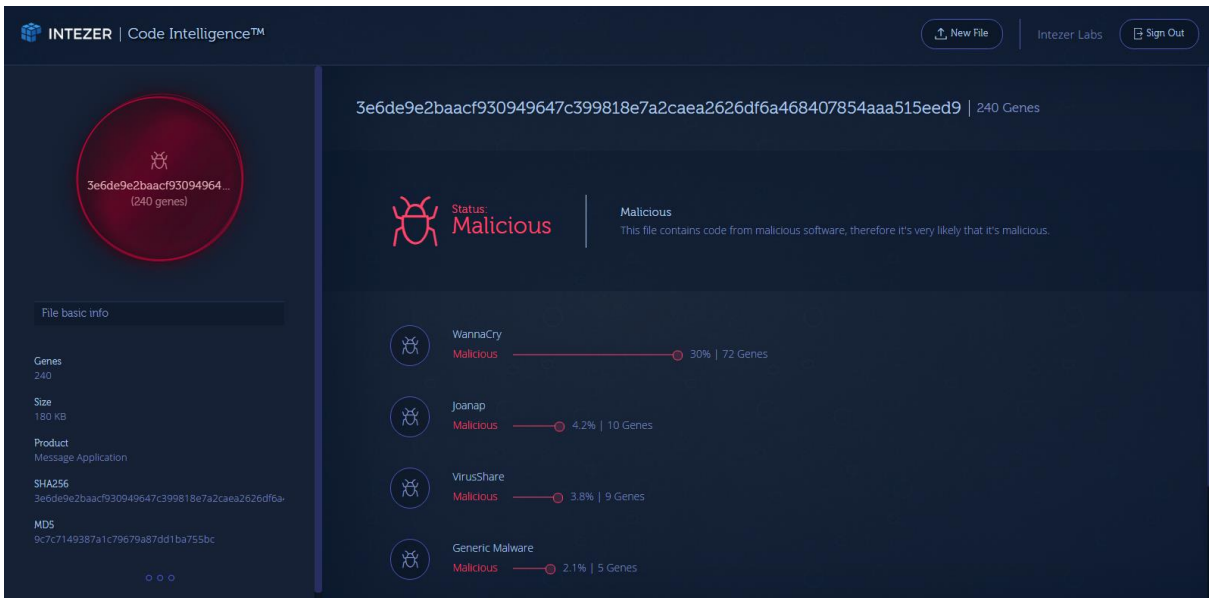
This is a piece of code from the WannaCry previous version, which according to our Global Genome Database, was seen before **only in the Lazarus group malware.** This specific code comparison analysis was already published by Neel Mehta.



Neel Mehta
@neelmehta
Following

9c7c7149387a1c79679a87dd1ba755bc @ 0x402560, 0x40F598
ac21c8ad899727137c4b94458d7aa8d8 @ 0x10004ba0, 0x10012AA4
#WannaCryptAttribution

The exact same sample had even stronger connections to the Joanap family, with 10 genes appearing in 5 different functions:



Summary

Intezer has seen clear code connections between previously unrelated malware families: WannaCry, Lazarus, Joanap and Brambul. This evidence strongly suggests that these hacking tools were written or modified by the same author. In numerous publications, some of the families are already attributed to North Korean hackers, thus it is highly probable that WannaCry ransomware was written or used by North Korean cyber attackers.

About Intezer

Intezer provides disruptive cyber security solutions based on its novel technology, Code Intelligence™. Code Intelligence™ is like “DNA Mapping” for software, able to identify the nature and origins of any unknown file or binary code. Intezer Labs Inc. was founded in 2015 by a unique team of cyber security professionals, including the founder and former CEO of CyberArk, and the former head of the Israeli Military CERT.

Code Intelligence™ Cloud Service

Intezer’s Code Intelligence™ Cloud Service is an online service for rapid File Investigation and Malware analysis that provides a fast, in-depth understanding of any file by mapping its code DNA. Providing a simple interface and API, it functions as a plug-and-play solution for any process within your organization’s incident response plans or daily cyber security monitoring.

This product is extremely effective in reducing false positives, accelerating incident response, and to deal with sophisticated attacks including Fileless malware or any other type of memory samples.
CONTACT US FOR AN INVITE CODE: contact@intezer.com

By detecting code reuse from both legit and malicious software, Code Intelligence™ provides a full understanding of the DNA of any unknown suspect, effectively transforming files and threats into an open book – as if an experienced Reverse Engineer has analyzed the whole assembly code.

Code Intelligence™ dissects any given file or binary into thousands of small fragments, and then compares them to a huge database to check in which software or malware these fragments were seen before, providing a full DNA mapping of the file.