To see what other don't see ©
Contact :
Emmanuelle Werner - Opération Manager
e.werner@cyber-detect.com
+33 6 88 41 31 94

LockerGoga is smashed by GORILLE©

March, 22nd, 2019

Autor: Jean-Yves Marion
Co-Autor: Fabrice Sabatier

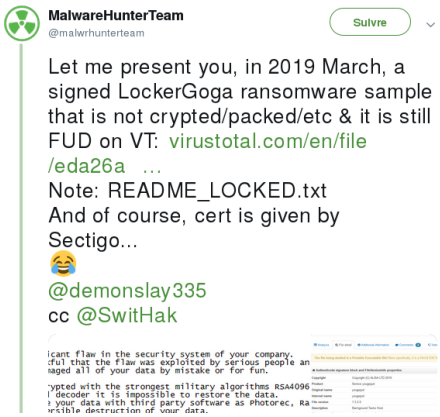
Today, we begin our blog. Our objective is to illustrate the uses of our software that we develop at CYBER-DETECT. Recent attacks of LockerGoga against Altran in France [1] and Norsk Hydro in Norway [2] illustrate the necessity to have advanced anti-malware defences. The attack in France happened in January and the one in Norway in March. Those attacks should have been stopped. That's why we begin by this post today. Indeed, the behaviour engine GORILLE designed by CYBER-DETECT allows to detect LockerGoga and its variants without signature.

In a nutshell, GORILLE identifies malicious threats embedded in Linux, MacOS and Windows binary files. For this, GORILLE knows a collection of malicious behaviours. Each binary file submitted to GORILLE is then scanned and as soon as a set of malicious inter-link behaviours is detected, GORILLE raises an alert. There is no magic behind, just several years of hard work at Loria's Computer Science Lab. But I guess we will come back in a future post on how GORILLE works and for the time being let's come back to LockerGoga.

Since GORILLE search process is based on a collection of malicious behaviours, the first question which comes in mind is whether or not GORILLE is able to detect LockerGoga. GORILLE knows about 100,000 malicious behaviours. And GORILLE identifies 55 malicious behaviours in the submitted sample of LockerGoga.

```
> GORILLE -d LockerGogaAltran.bin
info : Start processing files
DIST: "LockerGogaAltran.bin": 55 matching sites
54 from Hmir.tpz
```

The sample named *LockerGogaAltran.bin* [3] corresponds to the malware that attacks Altran in January 25th, 2019. On March 8th, 2019 that is two months later, MalwareHunter [4] discovered that a variant of LockerGoga, that we name here *no-detected_LockerGoga.bin*, was undetected by all anti-virus products in Virus Total [5].



Contact :
Emmanuelle Werner - Opération Manager
e.werner@cyber-detect.com
+33 6 88 41 31 94

As we see below, GORILLE detects 55 malicious behaviours in the yet undetected sample of LockerGoga, which are identical to the previous identified ones! The technological advance of GORILLE allows to stop variants of unknown threats.

```
> GORILLE -d LockerGoga/no-detected_LockerGoga.bin
info : Start processing files
DIST: "no-detected_LockerGoga.bin": 55 matching sites
54 from Hmir.tpz
```

Actually, we can play with GORILLE a little bit more. Indeed, GORILLE is able to learn the specific malicious functionalities of LockerGoga by itself.

```
> GORILLE -l LockerGoga.db LockerGogaAltran.bin
info : Start processing files
LEARN_OK: "LockerGogaAltran.bin", 24632 sites
info : Saving database
```

GORILLE finds 24632 sites in LockerGoga, which represent 24632 seen behaviours, not only bad ones. In fact, LockerGoga incorporates, as usual in any software, third party libraries coming from Microsoft and open source libraries. Collectively, third party libraries also denote behaviours. That said, we can compare all behaviours of LockerGogaAltran.bin, which were involved in Altran incident and the no-detected_LockerGoga.bin of MalwareHunter.

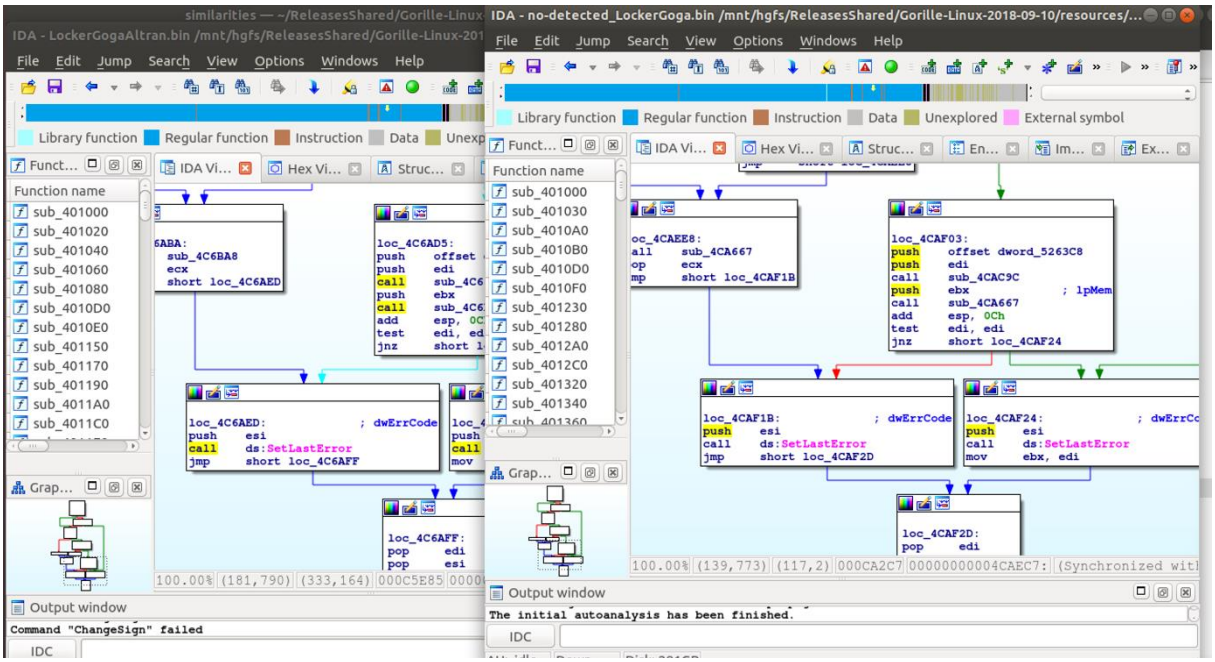
```
> GORILLE -d LockerGoga.db no-detected_LockerGoga.bin
info : Start processing files
DIST: "no-detected_LockerGoga.bin": 17951 matching sites
```

There are 17951 common behaviours, roughly the half, that are common between both samples. Then, using our tool binsim from the expert GORILLE suite, we can synchronize both codes, that is to find the correspondence between functions of LockerGogaAltran.bin and no-detected_LockerGoga.bin. Here is an excerpt of the output of binsim:

```
> binsim no-detected_LockerGoga.bin LockerGogaAltran.bin
match 4c6a9a  - 4caec8 score 273742
….
```

It indicates that the code of no-detected_LockerGoga.bin at address 0x4c6a9ah is very similar to the one at address 0x4caec8h. **And this is confirmed by IDA as it is shown in the Figure below:**

Contact :
Emmanuelle Werner - Opération Manager
e.werner@cyber-detect.com
+33 6 88 41 31 94



Similarly, GORILLE shows that the sample LockerGoga_Norsk-Hydro.exe involved in the attack of Norsk Hydro in March 2019 has again 50% of similar behaviours.

```
>GORILLE LockerGoga.db LockerGoga_Norsk-Hydro.exe
info : Start processing files
DIST: "LockerGoga_Norsk-Hydro.exe": 18021 matching sites
```

The conclusion is that GORILLE would have detected LockerGoga_Norsk-Hydro and stopped the attack, as well as it could have detected the Altran attack. When we know that the most severe attacks come from unknown threats or fresh repacked good-old malware, that are most of the time undetected, we need application that think out of the box and GORILLE is one of them!