lastline

April 2019

THREAT ALERT

Threat Alert

# LockerGoga: When Ransomware Strikes Back

Ransomware attacks have made the headlines multiple times in the course of recent years. LockerGoga is yet another example. The malware disrupted the operation of a number of organizations (some researchers speculate dozens) in the industrial and manufacturing sectors. While initially lacking in sophistication, later versions can cause extensive damage.

This blog post introduces LockerGoga, details its main features, and presents a timeline of the attacks made public so far. It also points out the major changes observed between versions. We conclude with a recap of all available information.

## The Attacks

While the initial infection vector is still unknown, it is believed that the attackers may have used a variety of techniques to get a foothold in target organizations' networks, including phishing emails and exploiting vulnerabilities. LockerGoga does not self-propagate by infecting other hosts on the target network. Having said that, fellow researchers that linked LockerGoga to FIN6 threat group (known for point-of-sale attacks aimed at stealing financial information), have reason to believe that the propagation took place by means of batch scripts using the SMB protocol and 'psexec' to copy and execute the payload.

LockerGoga was first discovered in January of this year after it was allegedly used in an attack against Altran Technologies, a French engineering consultancy. On January 29th the company published a statement claiming that they suffered an attack on the 24th and, as a consequence, they had to shut down their systems to protect their clients' data. On January 25th two samples were uploaded on VirusTotal (VT), from Romania and The Netherlands, indicating that the attack took place 4 days before the company published any statements.

A second attack took place on March 12th when, according to a post on BleepingComputer, two U.S. companies had been hit by the ransomware. Hexion and Momentive, controlled by the same investment fund, published a near-identical statement saying that the attack primarily affected corporate functions. Samples were uploaded to VirusTotal from several locations around the globe with only a few matching the physical locations of the two companies' offices. All uploaded samples included a number of new features, validating LockerGoga as a fairly active actor in the threat landscape.

The latest attack took place on March 19th against the global aluminum producer Norsk Hydro. It started around midnight, local time, and escalated throughout the night. The company disclosed the attack the very same day and announced that they switched to manual operations. Multiple samples linked to the Norsk Hydro attack were made available. Confirming the trend, these new samples have been found to implement yet another batch of new features. While the first samples featured a sometimes sloppy implementation, it is now clear how the threat is becoming more and more sophisticated.

## LockerGoga

The sample (`73171ffa6dfee5f9264e3d20a1b6926ec1b60897`) used in the attack against Altran Technologies became available on VirusTotal on January 24th. This version encrypts most of the files stored on the infected systems. As soon as the payload executes, a new process is started (the process uses a name similar to Microsoft system services, “svch0st.<random-number>.exe”) to query all files on the system and subsequently spawn a new process to encrypt each file separately, making it ultimately very slow (this was the sloppy aspect noted by many researchers).

The files that are targeted for encryption are DOT, WBK, DOCX, DOTX, DOCB, XLM, XLSX, XLTX, XLSB, XLW, PPT, POT, PPS, PPTX, POTX, PPSX, SLDX, and PDF files. Encryption is performed as follows:

1. Each file is passed as a parameter
2. A “.locked” extension is appended to its filename
3. The file is mapped in memory and encrypted
4. It gets unmapped and synchronized with the file on the disk
5. The process terminates

Ultimately LockerGoga places on the desktop a ransom note that demands the user inquire about the price of the decryption tool. The victim can contact the attackers using the email addresses that are included at the end of the ransom note.

A quite interesting aspect of LockerGoga is that it initially came digitally signed by a UK company named “MIKL LIMITED”. The underlying reason is easy to guess: any digitally signed software is often able to bypass standard security solution just because of the signature itself. This also explains why VT coverage was, at first, quite sub-optimal: many researchers kept “discovering” new LockerGoga samples with zero detections on VT during the weeks following the first attack.

The malware was immediately termed LockerGoga because of a debug path name that could be found within the binary of one of its variants: X:\work\Projects\LockerGoga\. As we will detail in the next section, further iterations of the malware (specifically the one used to attack Altran) seem to forego this specific string in the binary.

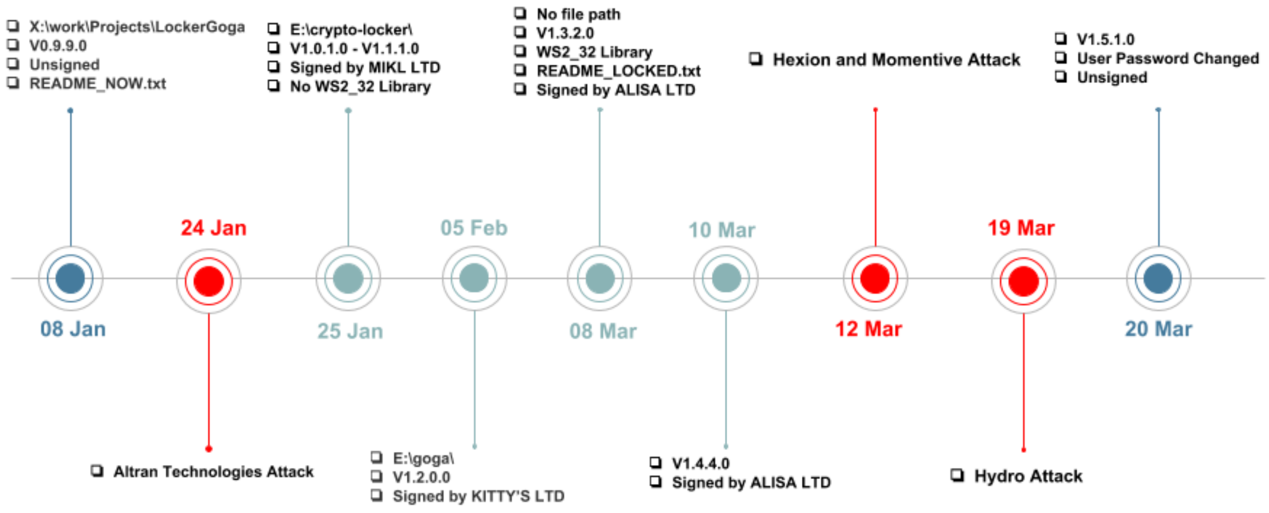


Figure 1: Evolution of LockerGoga in 2019.

## Evolution

LockerGoga has been evolving since its first appearance. In this section, we present all major changes, and detail what version has been used in which attack. Figure 1 shows a timeline connecting all these events to the attacks.

Note that we extracted the version numbers from the PE header; while metadata cannot be normally considered as a trusted source, we found no reason to believe they have been tampered or forged by the attacker for deception purposes. We now summarize the main feature introduced by each version.

**Version 0.9.9.0**: This is an early version of the sample used to attack Altran. While it is not clear when (and if) this specific version had been used in the wild, VirusTotal recorded these samples as submitted from The Netherlands. It leaks its name in a string embedded in the binary (X:\work\Projects\LockerGoga\); unlike later versions, it is not signed and maybe for this reason ultimately less successful.

**Version 1.0.1.0, 1.0.2.0, and v1.1.0.0**: These are the versions used in the attack against Altran's systems. The debug path included in the binary references an entirely new directory: "E:\crypto-locker". There seems no real reason for this change besides suggesting some sort of link between LockerGoga and other disruptive ransomware families. These new samples became available on VT at different dates, both before and after the attack. The malware is signed with a certificate issued to "MIKL LIMITED".

**Version 1.2.0.0**: In early February two new samples were uploaded, this time from Spain and Germany. The executables were identified as LockerGoga but signed with a new certificate issued to "KITTY's LTD" (Comodo still being the certification authority). The binaries include yet a new path, "E:\goga", suggesting that the developers settled on the name of the malware as they removed all references to "Locker" or "CryptoLocker." This version did not introduce any new features.

**Version 1.3.2.0**: Within one month of v1.2.0.0 a new version appeared in the wild signed by yet another entity, "ALISA LTD." While there is no pathname inside the binary, the executable is for some reason linked against a new library, WS2_32.dll. This library is responsible for sockets creation when establishing a new network connection. It's too early to say whether this implies that the authors have been experimenting with self-propagation mechanisms. Another difference introduced by this version is a new name for the file containing the ransom note: README_LOCKED.txt. All these modifications make this version the most significant update so far.

**Version 1.4.4.0**: Two more variants were made available on VT less than 5 days later. The ransom note features the same filename, there is no new path hard-coded in the binary, and it is still signed by "ALISA LTD." The samples were uploaded on March 12th and 19th respectively and have been deemed responsible for the attacks against US and Norwegian companies.

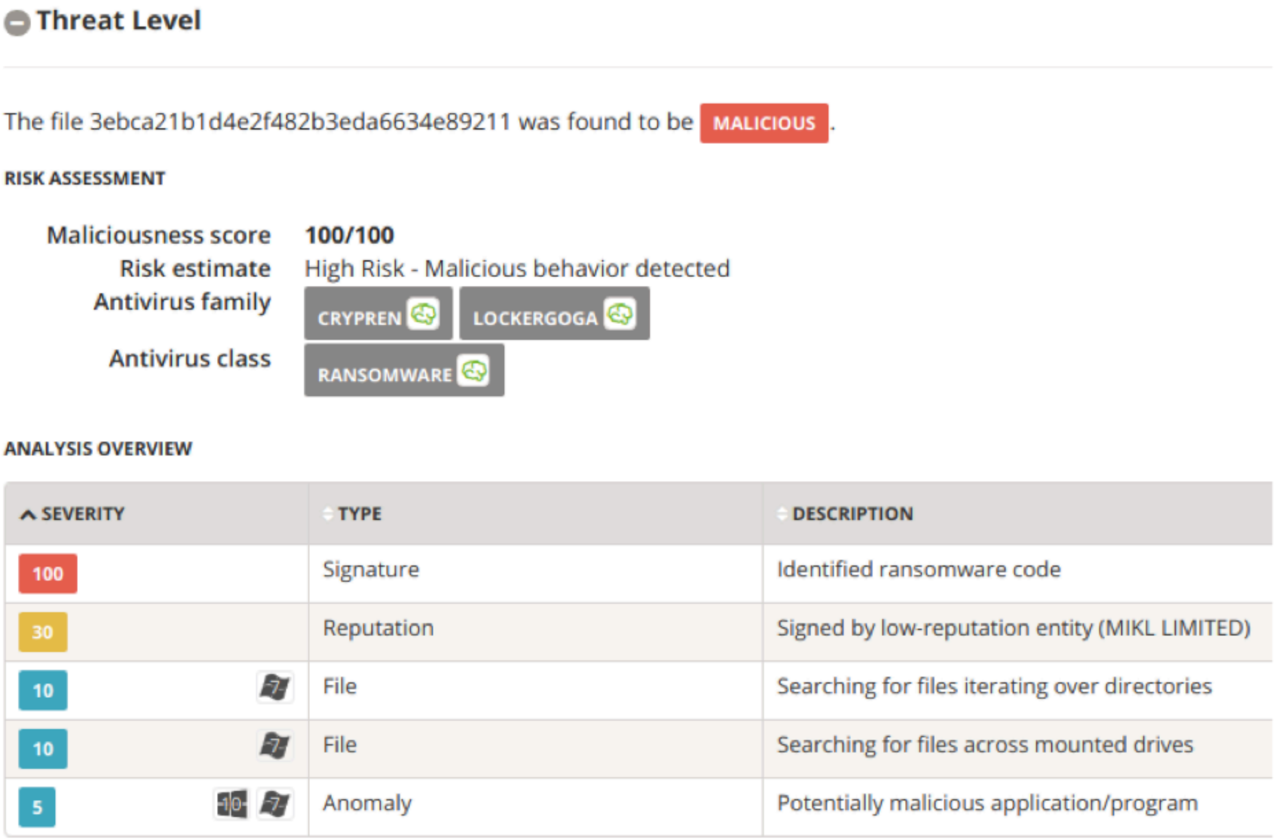
**Version 1.5.1.0**: The latest version of LockerGoga sample was uploaded just a few days after the previous one. It is not signed, but it is still linked against the WS2_32 library. In an expected turn of events, this version behaves more like a wiper than ransomware: it now forces a logout and changes all user passwords to "HuHuHUHoHo283283@dJD". The consequence is that the victim is not able to view the ransom note, basically making the ransomware not monetizable by the attacker. If this is intentional, it implies that the attacker is actually more interested in causing a denial of service.

## Conclusions

The creators of LockerGoga have been improving the capabilities of the malware by adding more and more features: linking against network libraries and changing the user password being the latest and greatest. All these additions indicate a level of sophistication that was not evident in the first version. While the network library might be an indication of some scheduled developments, changing the user passwords seem to suggest a more destructive aim. While there is no public information whether payments have been made and the victims managed to retrieve their files, this ransomware has already caused major disruptions and harm, leading to million-dollar losses.

All these new additions raise even more questions about the intentions of the threat actor. What are they trying to achieve? Are they merely motivated by disrupting operations? Has the motive always been financial profit?

Given the rapid evolution of this malware, signatures can hardly keep up. While signature-based detection provides good protection from known malware, behavioral detection techniques are required to deal with unknown threats. Our behavioral scanners (see Figure 2) identify all samples listed in this blog post as malicious, thus protecting our customers from known and unknown variants of LockerGoga. In the Appendix below we also provide a list of all indicators collected so far by our analysts. The e-mail addresses were extracted from the ransom notes.



Threat Level

The file 3ebca21b1d4e2f482b3eda6634e89211 was found to be MALICIOUS.

RISK ASSESSMENT

| | |
|---|---|
| Maliciousness score | **100/100** |
| Risk estimate | High Risk - Malicious behavior detected |
| Antivirus family | CRYPREN<br>LOCKERGOGA |
| Antivirus class | RANSOMWARE |

ANALYSIS OVERVIEW

| SEVERITY | TYPE | DESCRIPTION |
|---|---|---|
| 100 | Signature | Identified ransomware code |
| 30 | Reputation | Signed by low-reputation entity (MIKL LIMITED) |
| 10 | File | Searching for files iterating over directories |
| 10 | File | Searching for files across mounted drives |
| 5 | Anomaly | Potentially malicious application/program |

Figure 2: Result of Lastline dynamic analysis and extracted behaviors.

## Appendix

### Email Address

CottleAkela@protonmail[.]com
QyavauZehyco1994@o2[.]pl
AbbsChevis@protonmail[.]com
IjuqodiSunovib98@o2[.]pl
RomanchukEyla@protonmail[.]com
CouwetIzotofo@o2[.]pl
PhanthavongsaNeveyah@protonmail[.]com
AperywsQaroci@o2[.]pl
mayarchenot@protonmail[.]com
RezawyreEdipi1998@o2[.]pl
DharmaParrack@protonmail[.]com
wyattpettigrew8922555@mail[.]com
kv8f6fx@protonmail[.]com
SuzuMcpherson@protonmail[.]com
AsuxidOruraep1999@o2[.]pl
SayanWalsworth96@protonmail[.]com
QicifomuEjijika@o2[.]pl

### Hashes

d1c2dfedc602f5d5f2036b0ba5541cac8f8b4b95
31fbfe814628db3b459ddc87bf5ed538700db17a
61fdebb3c9dfa880b54e82579256acfcd4d6d406
3da0a217bbda09561780f52f163a6aafeb721d60
73171ffa6dfee5f9264e3d20a1b6926ec1b60897
f92339e73c7e901c0c852d8e65615cfb588a4ff6
37cdd1e3225f8da596dc13779e902d8d13637360
50f5a5ec13d21d4df119140547d63bc40f93b079
baa9f65be5177d1af5c5e8e822d756c799bb03ae
e00ec019409a078e9819e09d0f3915cb41fc131f
fcd241fdcd462199f2907ca34c73ce9c89b03e5f
7dea7ff735023418b902d093964028aefbc486a5
34fb03a35e723d27e99776ed3e81967229b3afe1
a25bc5442c86bdeb0dec6583f0e80e241745fb73
eb3eaaef52eafece1b91ced557e2071f1362f226
b2a701225c8c7f839be3c5009d52b4421063d93e
b5fd5c913de8cbb8565d3c7c67c0fbaa4090122b
442ed0cac2abe062d8e630f3ece803af687751db
8096fff66323cd753eab24d0c4f501220c0974b3
3b8e32af16e1c351c93b307893fcb3018cc6502a
fe2dcbf7da2910dbf29caa7d7166ab2ec36facfd
c46abb02c682683a4e92657a07da2bedc8d640ad
51f4c82afed2952349279fe573cabcdc0a7810f3
8574335dfdba758fa6e8a0405ad3cb5ddf544f4f
7cca904e7a581057bd3d21545a097b336fff3fc9
0ea96a4aef3e3297f593b6ab0a35316c6c532438
3d186c48300093fb6d4b48b9e430f86261705cc0
ba9c03f885bc79e08c39c030f86fc48566e302c0
498707d5f24e0b0561a40316d5d4b0c44d3f50fb
81733f0b7ac73e123369189b1324a4bbcfe2d62f
b36dba835e767510845eaa958c4b2844de4a2b39
baf0c9582ca9cc6c4f63dac7e535301e405e16a1
d61d4100d1dbafec2f7f774f210e0d2766e47101
55f3b39346b1c4782abbf4a4509b2df65e7f57b0
9006366f6da38ffbff3bd9b0fdc7516d1c412d98