New LockerGoga Ransomware Allegedly Used in Altran Attack

bleepingcomputer.com/news/security/new-lockergoga-ransomware-allegedly-used-in-altran-attack/

Ionut Ilascu

By
Ionut Ilascu

- January 30, 2019
- 03:03 AM
- 2

Hackers have infected the systems of Altran Technologies with malware that spread through the company network, affecting operations in some European countries. To protect client data and their own assets, Altran decided to shut down its network and applications.

The attack occurred on January 24, but the French engineering consultancy released a public statement only yesterday and kept details to a bare minimum, saying that third-party technical experts and digital forensics specialists are on the case.

To protect our clients, employees and partners, we immediately shut down our IT network and all applications. The security of our clients and of data is and will always be our top priority. We have mobilized leading global third-party technical experts and forensics, and the investigation we have conducted with them has not identified any stolen data nor instances of a propagation of the incident to our clients

Altran allegedly hit with new LockerGoga ransomware

Altran made no reference to the type of malware affecting their network, but security researcher have been following the trail of public breadcrumbs found sufficient evidence to determine that it's a ransomware attack.

The first public mention of the cyberattack against Altran came in a tweet on January 25. A reply from computer security researcher V hinted that behind the incident is a malware sample uploaded to VirusTotal.

> (link: https://t.co/udeToPYHPo) https://t.co/17btK8Kc6g…
>
> — V (@vxsh4d0w) January 25, 2019

This sample has an initial detection rate of 26 engines out of 69, but the file was quickly picked up by other antivirus products on VirusTotal and now 43 of them recognize the malware. The sample was first uploaded to VirusTotal on January 24 from Romania and later that day it was added from the Netherlands.

If the file uploaded to Google's scanning service is same one that struck Altran's computers, then it is a ransomware called LockerGoga. This name of the threat comes from the path used for compiling the source code into an executable discovered by MalwareHunterTeam.

```
X:\work\Projects\LockerGoga\cl-src-last\cryptopp\src\rijndael_simd.cpp
```

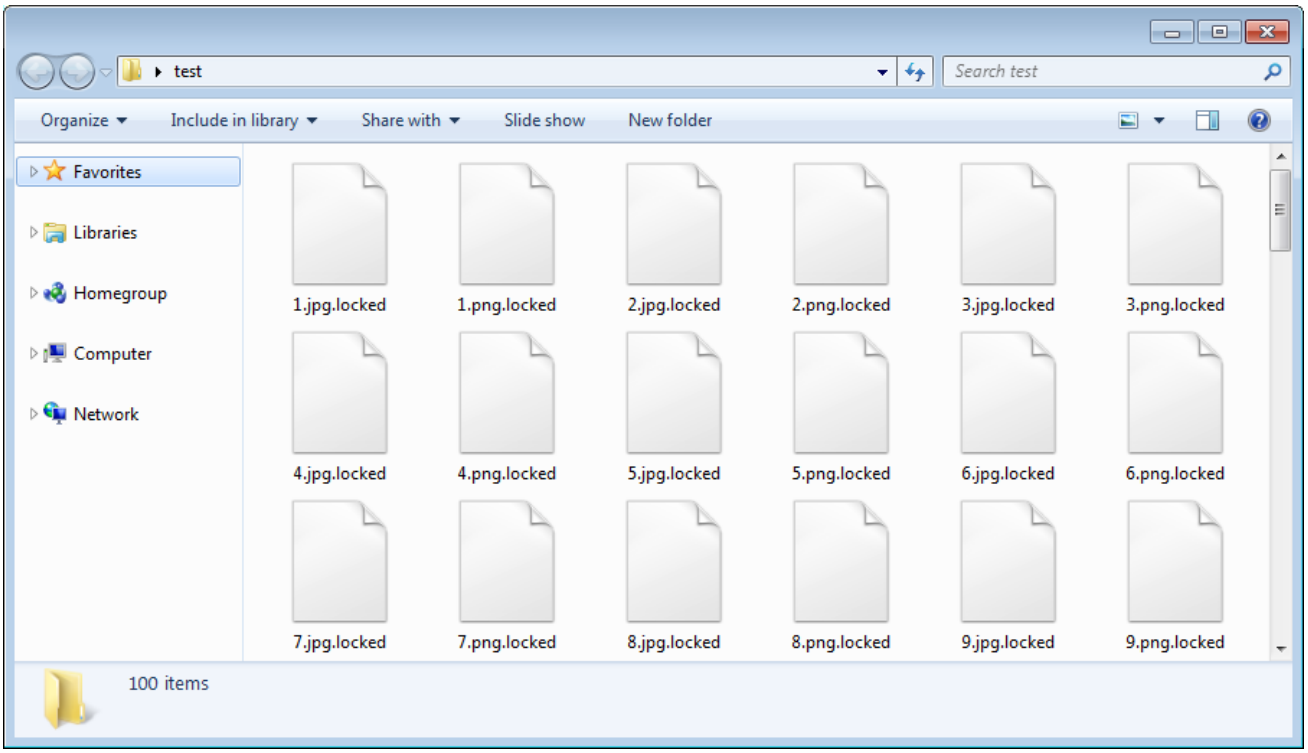
When BleepingComputer tested the ransomware, we found that it was very slow due to to how it spawned another process each time it encrypted a file. When discussing this with a security researcher named Valthek, we were told that the code was sloppy, slow, and made no effort to evade detection.

According to security research SwitHak, the ransomware will normally target DOC, DOT, WBK, DOCX, DOTX, DOCB, XLM, XLSX, XLTX, XLSB, XLW, PPT, POT, PPS, PPTX, POTX, PPSX, SLDX, and PDF files.

However, if launched with the '-w' command line argument, it will target all file types. Other switches supported are '-k' and '-m' for base 64 encoding and for providing the emails addresses to show in the ransom note.

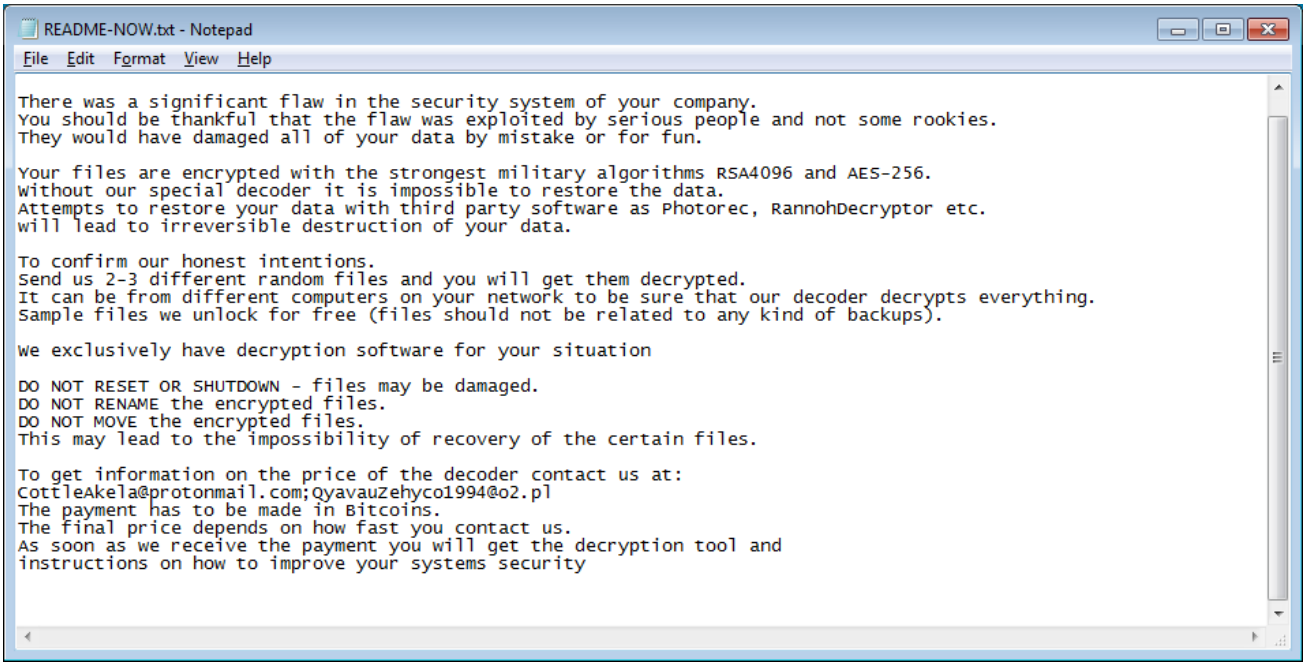
In BleepingComputer's test, the ransomware sample launched itself with the -w argument and also spawned a new process for each file it encrypted. This caused the encryption process to be very slow.

When encrypting files, the ransomware will append the **.locked** extension to the processed files. This means that a file named test.jpg would be encrypted and then renamed to test.jpg.locked as illustrated in the image below.



Furthermore, reports indicate that the sample may not wipe shadow volume copies, but we were not able to confirm that.

When done encrypting data on the computer, it will drop a ransom note named **README-NOW.txt** on the desktop, which includes instructions to contact the CottleAkela@protonmail.com or QyavauZehyco1994@o2.pl email addresses for payment instructions.



As you can see, the ransom note suggests that the malware operators target companies and offer to unlock a few files for free to prove that they have the decryption key.

LockerGoga's ransom note was also seen by security researcher MalwareHunterTeam in early January, although it included different ProtonMail and O2 addresses.

> We first seen this note (name and content), with different email addresses (but still one ProtonMail & one O2) on 6th evening. From then we seen victims from more than 5 countries. First victim/uploader was from Netherlands...
>
> — MalwareHunterTeam (@malwrhunterteam) January 26, 2019

According to SwitHak's attack scenario, the Romanian local team noticed the threat and checked it on VirusTotal. The network connection and network shares mounted on employee systems allowed LockerGoga to spread to offices in other countries, thus explaining the sample upload from the Netherlands.

> #Altran alleged attack timeline based on facts, hypothesis part based on our thoughts. pic.twitter.com/cxBrG8UY84
>
> — SwitHak (@SwitHak) January 26, 2019

Of course, this is all conjecture and there is no hard proof to indicate that this is what happened.

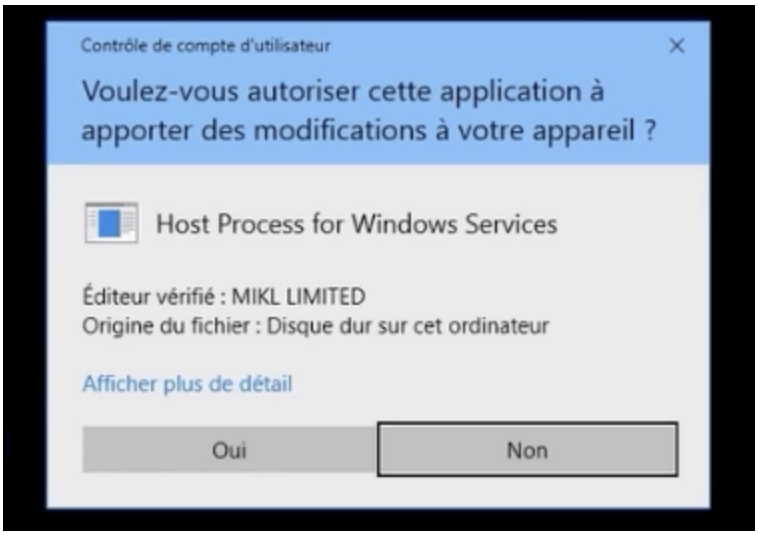
Another interesting bit of information is that the "Goga" in the ransomware's moniker is a Romanian family name. This info tidbit coupled with the location it was first uploaded from could make one wonder if the strain had its origin in Romania.

LockerGoga uses valid certificate

Analysis from Thomas Roccia, reverse engineer at McAfee, shows that the LockerGoga strain was signed with a valid certificate, which would increase the chances of its deployment on the victim hosts without raising suspicion in most cases.

```
[+] The file is signed, you may check the following certificate!
Version:                3
Serial Number:          2e:7c:87:cc:0e:93:4a:52:fe:94:fd:1c:b7:cd:34:af
Signature Algorithm:    SHA384_WITH_RSA_ENCRYPTION
Valid from:             2013-5-9 0:0:0
Valid to:               2028-5-8 23:59:59
Issuer:                 C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO RSA Certification Authority
Subject:                C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO RSA Code Signing CA
```

However, someone paying attention to the Windows alert asking for authorization of the certificate would notice that something is not right, because it is for a host process for Windows Services and the signature is from MIKL Limited.



The certificate, issued by Comodo Certificate Authority (acquired by Francisco Partners and known by its new brand name Sectigo) for code signing, has been revoked.

A cursory check reveals that MIKL Limited is an IT consultancy firm incorporated in the UK on December 17, 2014.

Known file samples for LockerGoga ransomware are 'worker' and 'worker32.' The malware launches a process with a name similar to what Microsoft uses for its Windows Services, such as 'svch0st' or 'svchub.'

For those looking to detect it this family of infections using Yara, security researcher V wrote the first rule that can help organizations protect their systems from getting hit by LockerGoga ransomware.

We were told at the time of writing, that the global information systems of Altran Technologies continue to be unavailable. BleepingComputer reached out to the Paris-based company to provide more information about the nature of the cyberattack that impacted its operations but has not heard back by publishing time.

Related Articles:

Austin Peay State University resumes after ransomware cyber attack

LockBit ransomware gang lurked in a U.S. gov network for months

BlackCat/ALPHV ransomware asks $5 million to unlock Austrian state

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Industrial Spy data extortion market gets into the ransomware game

IOCs

Hash:

```
73171ffa6dfee5f9264e3d20a1b6926ec1b60897
```

File names:

```
worker
worker32
bdf36127817413f625d2625d3133760af724d6ad2410bea7297ddc116abc268f_wQkb8SOVnc.bin
svch0st.5817.exe
svch0st.11077.exe
```

Associated email addresses:

```
CottleAkela@protonmail.com
QyavauZehyco1994@o2.pl
```

Ransom Note Text:

```
Greetings!

There was a significant flaw in the security system of your company.
You should be thankful that the flaw was exploited by serious people and not some
rookies.
They would have damaged all of your data by mistake or for fun.

Your files are encrypted with the strongest military algorithms RSA4096 and AES-256.
Without our special decoder it is impossible to restore the data.
Attempts to restore your data with third party software as Photorec, RannohDecryptor
etc.
will lead to irreversible destruction of your data.

To confirm our honest intentions.
Send us 2-3 different random files and you will get them decrypted.
It can be from different computers on your network to be sure that our decoder
decrypts everything.
Sample files we unlock for free (files should not be related to any kind of
backups).

We exclusively have decryption software for your situation

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME the encrypted files.
DO NOT MOVE the encrypted files.
This may lead to the impossibility of recovery of the certain files.

To get information on the price of the decoder contact us at:
CottleAkela@protonmail.com;QyavauZehyco1994@o2.pl
The payment has to be made in Bitcoins.
The final price depends on how fast you contact us.
As soon as we receive the payment you will get the decryption tool and
instructions on how to improve your systems security
```

- Altran
- Cyber Attack
- LockerGoga
- Ransomware

Ionut Ilascu

Ionut Ilascu is a technology writer with a focus on all things cybersecurity. The topics he writes about include malware, vulnerabilities, exploits and security defenses, as well as research and innovation in information security. His work has been published by Bitdefender, Netgear, The Security Ledger and Softpedia.

- Previous Article
- Next Article

Comments

- 

  Amigo-A - 3 years ago

  -
  -

  CottleAkela@protonmail.com and QyavauZehyco1994@o2.pl - in this variant
  AbbsChevis@protonmail.com and IjuqodiSunovib98@o2.pl - in another variant

- 

  Amigo-A - 2 years ago

  -
  -

  Description in the Digest "Crypto-Ransomware" about LockerGoga Ransomware:
  https://id-ransomware.blogspot.com/2019/01/lockergoga-worker32-ransomware.html

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: