MS-ISAC®
Multi-State Information
Sharing & Analysis Center®

Security Primer
March 2019 – SP2019-0611

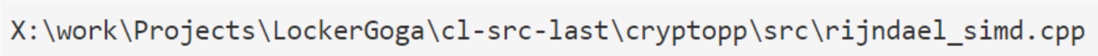
LockerGoga

Please Note: The information in this security primer is current as of March 28, 2019.

Overview

LockerGoga is a ransomware recently making headlines due to its disruptive effects on industrial and manufacturing firms' networks. Its recent victims include the Norwegian aluminum manufacturer Norsk Hydro, French engineering consulting firm Altran, and U.S. chemical companies Hexion and MPM Holdings (Momentive). The ransomware does not target or infect ICS systems, but its debilitating effects on the business and production networks tied to these industrial systems results in costly production down time. In the Norsk Hydro case, this involved temporarily moving to manual production. LockerGoga reportedly targets other sectors, although a disproportionate amount of victims reside in the industrial/manufacturing sector.

MalwareHunterTeam named the malware LockerGoga after discovering the name in a file path used for compiling source code into an executable. It also uses a .locked file extension for encrypted files.



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

At this time, the initial intrusion vector is unknown. The ransomware's code is digitally signed using valid certificates which could let it evade security tools and get on systems. The certificates used in known attacks were revoked. The CTAs reportedly use Metasploit and Cobalt Strike to move laterally across a network. They also reportedly use the Mimikatz tool to pull passwords out of memory to compromise other accounts, including those with higher privileges. It is believed that they then use admin level credentials to target an organization's Active Directory for widespread ransomware deployment. LockerGoga reportedly does not have any self-propagation mechanisms, meaning that the malware itself cannot spread across the network and needs to be manually deployed. However, Palo Alto Networks Unit 42 reports they observed "LockerGoga moving around a network via the server message block (SMB) protocol, which indicates the actors simply manually copy files from computer to computer."

The malware is dropped in the %TEMP% folder with random number extensions, such as the following:

- %TEMP%\svc{random}.{randomnumber}.exe
- executed as %TEMP%\svc{random}.{random number}.exe -{random} -{random} {random}
- Example: %TEMP%\tgytutrc{4 Random Numbers}.exe

After execution, the malware moves itself to the directory %TEMP% in order to cover the malicious activity. LockerGoga then attempts to clear the Windows event logs, creates the ransom note, and begins the encryption process.

Security researches discovered a few LockerGoga idiosyncrasies affecting the ransomware's execution and the ability for victims to access the ransom note.

Cybersecurity vendor Alert Logic reports that there is currently a flaw in some LockerGoga variants where the ransomware will not encrypt anything if it comes across a .lnk file. LNK is a file extension for a Microsoft Windows shortcut file to point to an executable file. Since this discovery is public knowledge, it is highly likely that the malware authors are aware and will resolve the issue in future variants.

Cisco's Talos group observed that some LockerGoga variants forcibly log victims off their devices. They are then unable to log back onto the device, which also means they may not see the ransom note. Furthermore, in some cases the network interface on each system was disabled and the local user account passwords were changed. This can cause confusion on the victim's end as to their issue's root cause. If this is an intentional feature, then it is possible that the CTAs have both financial and destructive motivations.

Additionally, LockerGoga reportedly does not use a command-and control (C2) infrastructure for communication nor to generate encryption keys. This is a novel feature and the purpose might be to evade security tools that look for malicious C2 traffic.

The CTA's ransom note readme file does not list an extortion amount and only provides email addresses, which can be contacted to negotiate a ransom amount. LockerGoga ransom note samples are available in the IOCs section.

RECOMMENDATIONS

The most important proactive step an organization can take for ransomware is the ability to recover from their backups. Use a backup system that allows multiple iterations of the backups to be saved and stored offline, in case the backups include encrypted or infected files. Routinely test backups for data integrity and to ensure you can recover from them.

Please visit the MS-ISAC Ransomware Security Primer for more information on ransomware, including further recommendations.

LockerGoga IOCs

Hash

SHA-256 Talos
https://blog.talosintelligence.com/2019/03/lockergoga.html

- c97d9bbc80b573bdeeda3812f4d00e5183493dd0d5805e2508728f65977dda15
- 88d149f3e47dc337695d76da52b25660e3a454768af0d7e59c913995af496a0f
- eda26a1cd80aac1c42cdbba9af813d9c4bc81f6052080bc33435d1e076e75aa0
- ba15c27f26265f4b063b65654e9d7c248d0d651919fafb68cb4765d1e057f93f
- 7bcd69b3085126f7e97406889f78ab74e87230c11812b79406d723a80c08dd26
- C3d334cb7f6007c9ebee1a68c4f3f72eac9b3c102461d39f2a0a4b32a053843a

SHA-1 Trend Micro
https://www.trendmicro.com/vinfo/hk-en/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware

- 37cdd1e3225f8da596dc13779e902d8d13637360
- b5fd5c913de8cbb8565d3c7c67c0fbaa4090122b

MD5
Palo Alto Networks Unit 42 - https://unit42.paloaltonetworks.com/

- 06e3924a863f12f57e903ae565052271740c4096bd4b47c38a9604951383bcd1
- 276104ba67006897630a7bdaa22343944983d9397a538504935f2ec7ac10b534
- 14e8a8095426245633cd6c3440afc5b29d0c8cd4acefd10e16f82eb3295077ca
- 050b4028b76cd907aabce3d07ebd9f38e56c48c991378d1c65442f9f5628aa9e
- f474a8c0f66dee3d504fff1e49342ee70dd6f402c3fa0687b15ea9d0dd15613a
- ffab69deafa647e2b54d8daf8c740b559a7982c3c7c1506ac6efc8de30c37fd5
- 31fdce53ee34dbc8e7a9f57b30a0fbb416ab1b3e0c145edd28b65bd6794047c1
- ae7e9839b7fb750128147a9227d3733dde2faacd13c478e8f4d8d6c6c2fc1a55
- 47f5a231f7cd0e36508ca6ff8c21c08a7248f0f2bd79c1e772b73443597b09b4
- 1f9b5fa30fd8835815270f7951f6246985293329317 25c1e17c41fd3dd040afe
- c1670e190409619b5a541706976e5a649bef75c75b4b82caf00e9d85afc91881
- 7852b47e7a9e3f792755395584c64dd81b68ab3cbcdf82f60e50dc5fa7385125
- e00a36f4295bb3ba17d36d75ee27f7d2c20646b6e0352e6d765b7ac738ebe5ee
- 9128e1c56463b3ce7d4578ef14ccdfdba15ccc2d73545cb541ea3e80344b173c
- 79c11575f0495a3daaf93392bc8134c652360c5561e6f32d002209bc41471a07
- 32d959169ab8ad7e9d4bd046cdb585036c71380d9c45e7bb9513935cd1e225b5
- 6d8f1a20dc0b67eb1c3393c6c7fc859f99a12abbca9c45dcbc0efd4dc712fb7c
- a845c34b0f675827444d6c502c0c461ed4445a00d83b31d5769646b88d7bbedf

Email Addresses

Palo Alto Networks Unit 42 - https://unit42.paloaltonetworks.com/

- QicifomuEjijika@o2[.]pl
- MayarChenot@protonmail[.]com
- CottleAkela@protonmail[.]com
- QyavauZehyco1994@o2[.]pl

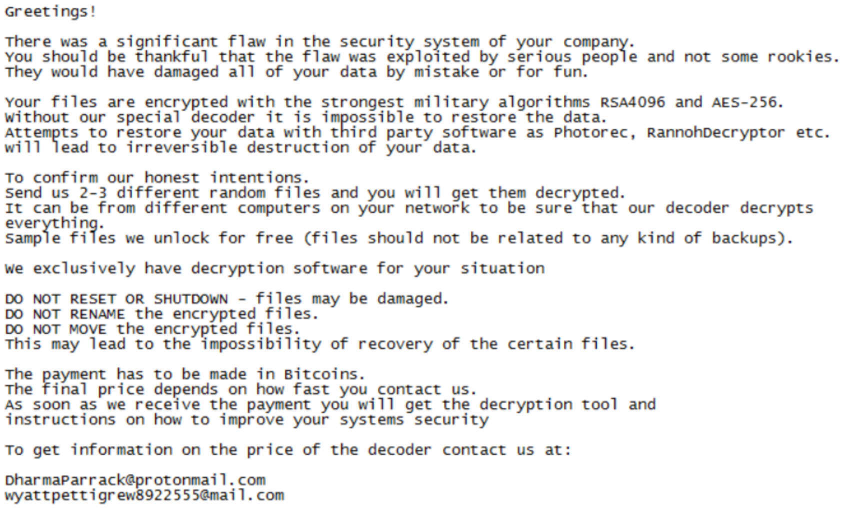
MalwareHunterTeam

- DharmaParrack@protonmail[.]com
- wyattpettigrew8922555@mail[.]com

Talos

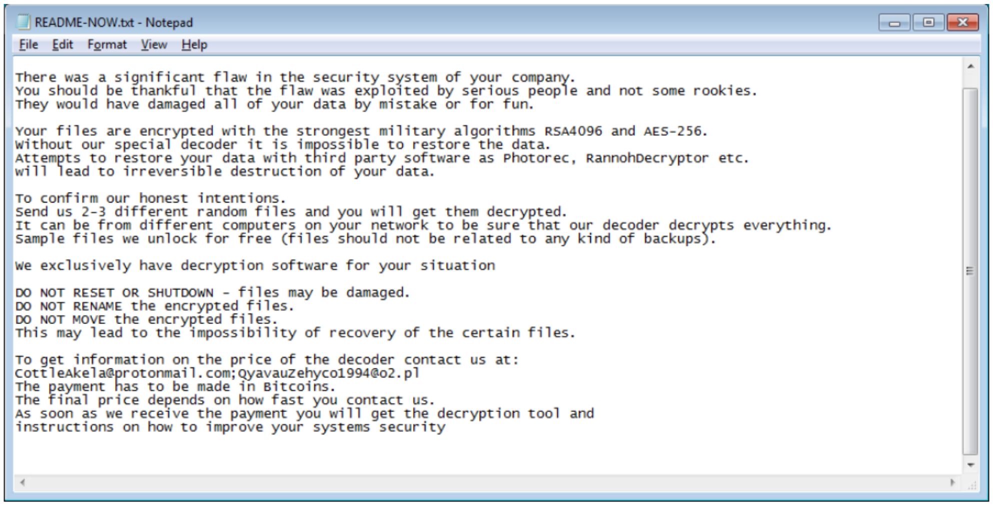
- AbbsChevis@protonmail[.]com
- IjuqodiSunovib98@02[.]pl
- SayanWalsworth96@protonmail[.]com
- SuzuMcpherson@protonmail[.]com
- AsuxidOruraep1999@o2[.]pl
- RezawyreEdipi1998@o2[.]pl

Ransom Note



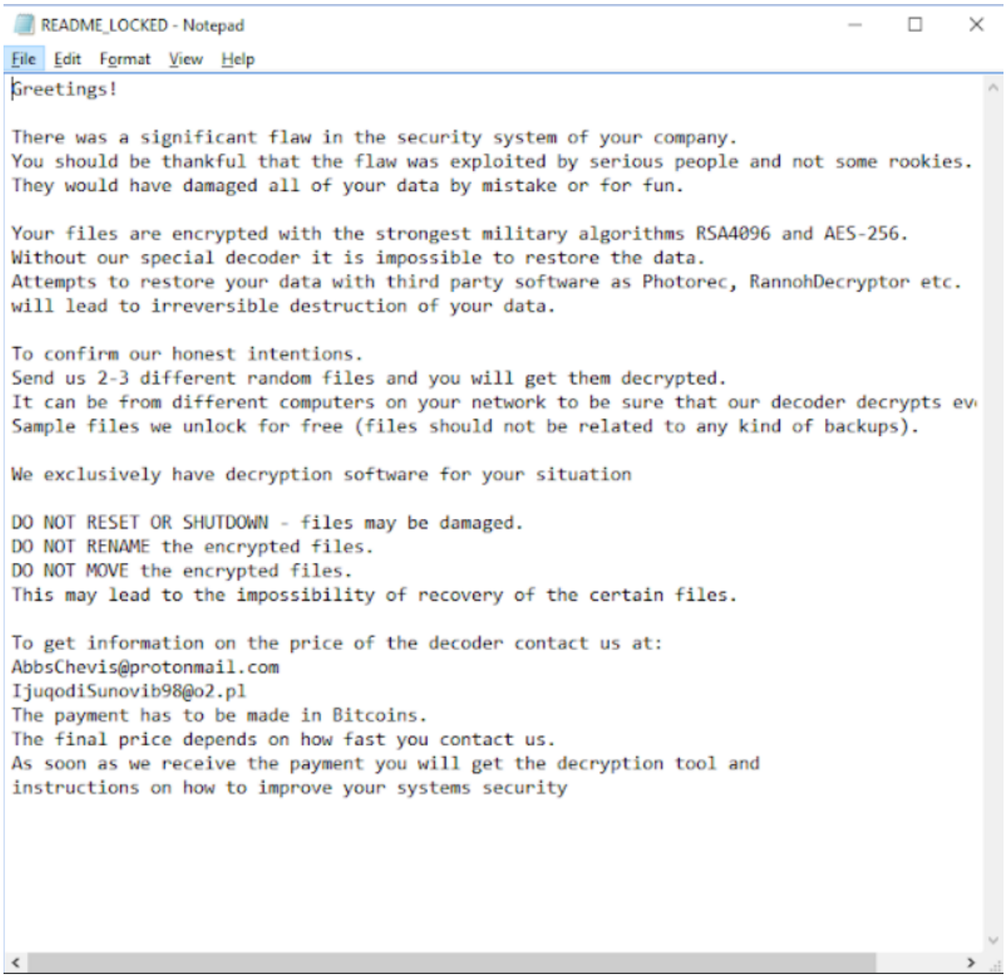
```
Greetings!

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.

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

To get information on the price of the decoder contact us at:

DharmaParrack@protonmail.com
wyattpettigrew8922555@mail.com
```

Source: MalwareHunterTeam (https://twitter.com/malwrhunterteam)



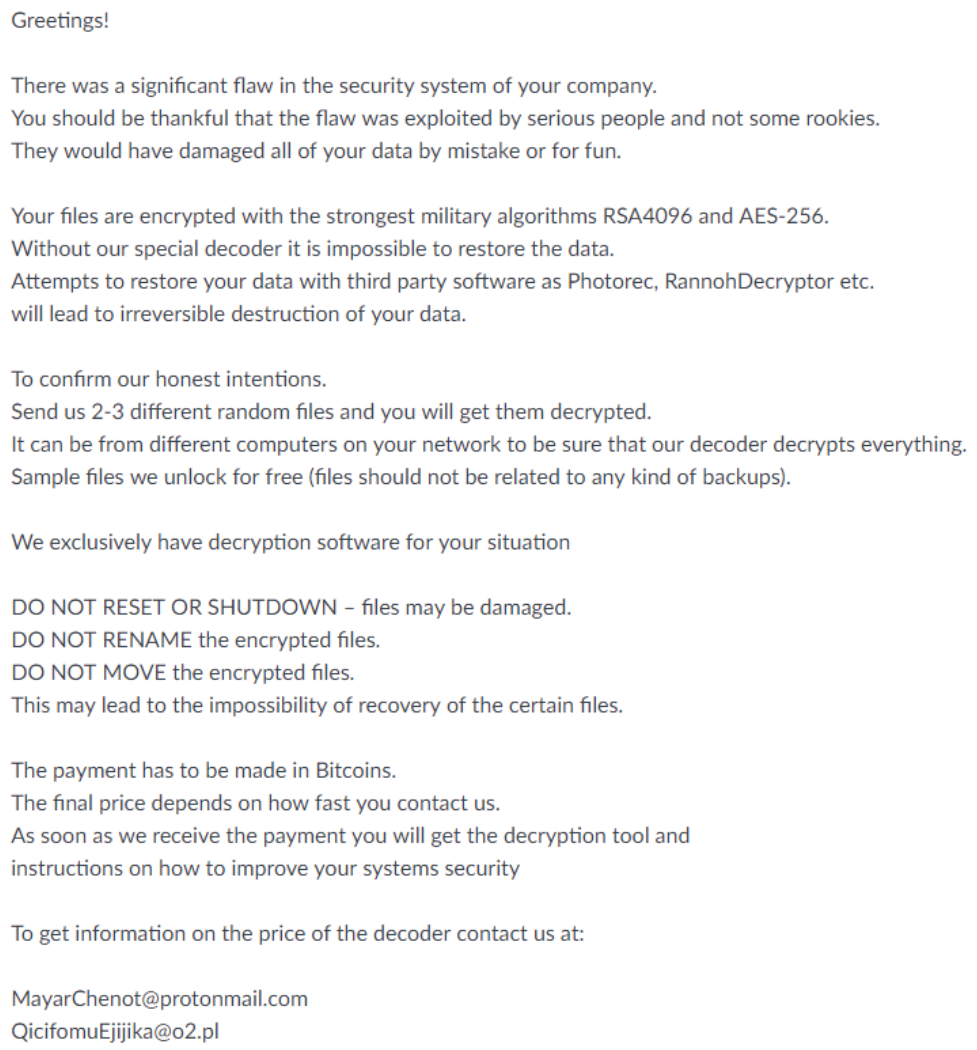
```
There was a significant flaw in the security system of your company.
You should be thankful that the flaw was exploited by serious people and not some rookies.
They would have damaged all of your data by mistake or for fun.

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
```

Source: Bleeping Computer (https://www.bleepingcomputer.com/news/security/new-lockergoga-ransomware-allegedly-used-in-altran-attack/)



```
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 ev
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:
AbbsChevis@protonmail.com
IjuqodiSunovib98@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
```

Source: Talos (https://blog.talosintelligence.com/2019/03/lockergoga.html)



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.

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

To get information on the price of the decoder contact us at:

MayarChenot@protonmail.com
QicifomuEjijika@o2.pl

Source: Palo Alto Networks Unit 42 (https://unit42.paloaltonetworks.com/born-this-way-origins-of-lockergoga/)

Encrypts
(Trend Micro)
.doc, .dot, .docx, .docb, .dotx, .wkb, .xlm, .xml, .xls, .xlsx, .xlt, .xltx, .xlsb, .xlw, .ppt, .pps, .pot, .ppsx, .pptx, .posx, .potx, .sldx, .pdf, .db, .sql, .cs, .ts, .js, .py

Extension
.locked

Encryption Algorithm
Crypto++ (Trend Micro)
RSA-OAEP MGF1 (Palo Alto Networks Unit 42)

The *MS-ISAC* is the focal point for cyber threat prevention, protection, response, and recovery for the nation’s state, local, tribal, and territorial (SLTT) governments. More information about this topic, as well as 24x7 cybersecurity assistance is available at 866-787-4722, *SOC@cisecurity.org*. The MS-ISAC is interested in your comments - an anonymous feedback *survey* is available.