Ransomware: Analysis of 2019 LockerGoga cyber-attack to Norsk Hydro multinational company and its countermeasures

Akramova Nargiza

Westminster International University in Tashkent
Teacher at Department of Technology, Education and Law
nargiza9772@gmail.com

ABSTRACT

Norsk Hydro, the world`s largest aluminum manufacturing giant has recently been a victim of severe ransomware attack, which forced the business to close its operations worldwide in 40 countries and switch to manual operations. This cyber-attack caused severe disruption to business by making its network unavailable to its legitimate users. This paper critically discuss the origin of the breach, attack severity, attack vector used and the ways to prevent and mitigate such type of attack in future. The current research paper was composed through studying the previous case studies and the lessons learned regarding the ransomware and propose secure controls to ensure security of sensitive and confidential information of Norsk Hydro company. This paper can be of a great significance to researchers throughout the globe that are focusing on cyber-threat and ransomware studies, in particular in the business domain.

Keywords: LockerGoga, Ransomware, cyber-attack, VM (Virtual Machine), WannaCry, Malware

I.Introduction

Norsk Hydro is a Norwegian aluminium and renewable energy company employing 35,000 people in 40 countries worldwide (Norsk Hydro ASA, 2019). In March of 2019, this giant company, headquartered in Norway (Oslo), was hit by a severe ransomware attack, which caused system irregularities i.e. Norsk Hydro suffered from production stoppages in Europe and the US (Fiveash, 2019). While combatting this lethal attack, company had to completely switch to manual operations and shut down the network throughout the offices. Fiveash (2019) argues that Norsk Hydro cyber-attack was done in chase of money, '*not war*'.

The Norsk Hydro company management advised their employees not to connect to the network and even not to log on their computers on Monday, 17 March, 2019. Later that week, it was evident that the attackers used LockerGoga ransomware for its mischief. LockerGoga is a type of ransomware that is capable of locking the computer files and demand a payment in return of decrypting them (Belton, 2019). In fact, researchers claim that LockerGoga, considered as a '*nasty*' and new breed of ransomware family, which has been increasingly targeting number of industrial firms of different sizes around the globe since the beginning of 2019 year (Greenberg, 2019). The same source states that Ransomware brings not just a mere damage, but also a '*crippling disruption*'. According to the Motherboard reports (Bicchierai, 2019), the same ransomware, LockerGoga, was able to infect two other American chemical companies in March, 2019 as well, blocking access to several IT systems and data related to their manufacturing operations.

Thus, the aim of this research paper is to critically analyse the Ransomware malware, in

particular LockerGoga ransomware, using the case of 2019 Norsk Hydro cyber-attack. Furthermore, the report will propose countermeasures that will help to prevent the cyber-threats similar to the case of Norsk Hydro ransomware and will also highlight attack vectors adopted by the Ransomware LockerGoga which made it successfully penetrate and disrupt the industrial operations. Section II and Section III are the main body of the document which will be devoted to critical evaluation of LockerGoga ransomware and vital countermeasures to mitigate any future risks respectively. Section IV concludes the research paper briefing the key findings established from this research.

II. Critical Analysis Of Lockergoga Ransomware And Its Performance

The main aim behind LockerGoga ransomware is 'to infect computers and ask for a ransom' (Adamov *et al*., 2019). In case of Norsk Hydro attack, the ransom notice was in a text file displayed on the staff laptop (see Appendix 1) and asked the users to transfer money in bitcoins in order to be able to log on their systems again. In fact, the recent victims of this threat show us that ransomware attacks prove to be costly and reputation crushing forms of attack (Donnell, 2019). Motherboard researchers studying LockerGoga ransomware argue that Lockergoga can be '…inefficient at collecting money, but it's apparently good enough to slow down multinational companies in both Europe and the United States'(Bicchierai, 2019) . To fully paralyze their victims LockerGoga attackers are targeting mostly multinational companies that manage their physical business activities with the help of computer automated processes.

Indeed, LockerGoga is different to the other known ransomware cyberattacks such as WannaCry and Petya, since the attackers are targeting the company networks and matching encryption according to their geographical regions. Based on the current research, although the attacker whereabouts of Norsk Hydro cyber-attack are still unknown, however the main motivation behind LockerGoga ransomware was gaining money (Belton, 20119)

a) Performance Evaluation of LockerGoga ransomware

The in depth-analysis of the Lockergoga attack was carried out by TrendMicro Security, Smart Protection Suites and Worry-Free Business Security researchers (Trend Micro, 2022). According to the research done by Trend Micro following the cyber-attack of Norsk Hydro on 19 March of 2019, it was clear that PsExec tool was used to drop and execute the ransomware. In fact, it is the same tool utilized for various popular ransomware including Sorebrect and Bad Rabbit. PSExec tool requires an attacker the credentials, so this leads to the idea that LockerGoga attackers could have gained the credentials previously through spear phishing.

Spear phishing is one of the phishing methods that target particular groups or individuals and use emails, social media or other ways in order to obtain personal information or sometimes lead to network compromise and data loss (Trend Micro, 2022). The attackers using spear phishing usually execute reconnaissance activities before starting the attacks. Trend Micro researchers report that 90% of all attacks launched in 2012 were using spear phishing attack, and this leads to the idea that in case of LockerGoga, spear phishing attack was launched to get the credentials before using PSExec Tool.

Further research on LockerGoga ransomware shows that the attack did not give the victims an opportunity to recover their files and ask for a particular amount of payment (see Appendix 1), the distribution of LockerGoga attack was targeted by the company competitors, and intended to disturb company operations.

As shown on Figure 1, there are three main steps in execution flow of LockerGoga ransomware, and it uses a 'master/slave module' to encrypt the victim`s files (Manuel and Salvio, 2019). The 'master' process is responsible for searching for files and writing their paths in the shared memory. While the 'slave' process gets the file path through shared memory and carries out the encryption.

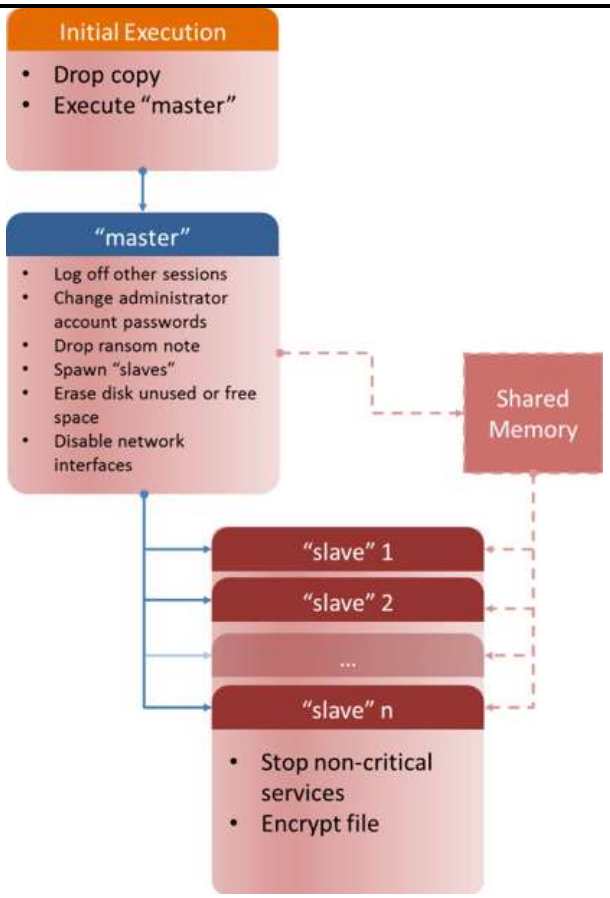


Figure 1: Execution flow of LockerGoga ransomware (Manuel and Salvio, 2019)

b) Technical Analysis of LockerGoga ransomware

Based on the research done by Trend Micro, Threat Intelligence Center and McAfee group, LockerGoga exhibits considerably unique technical behaviors that need to be studied (Appendix 3). The main differences between the LockerGoga and other ransomware types such as WannaCry and Ryuk are in the encryption and its ability of fast enumeration among the targeted system files (Lopez, 2019).

After being installed, LockerGoga changes the passwords and thus completely modifies the user accounts. In most cases with LockerGoga attack, the users were also logged off their systems.

Step 1: When first launched, LockerGoga`s first task is to move itself into 'UserTemp' directory using the following command line (Qihu 360 Software, 2022).

cmd.exe /c move /y tgtutrcXXXX.exe % TEMP %\tgytutrcYYYY.exe

Step 2: Then, using the command lines, the user accounts are also relocated in a temporary folder. The file paths aimed for encryption later cannot be seen in the command line parameter used by the attacker.

Step 3: In the next stage, LockerGoga ransomware encrypts all the files that are stored in users` servers and work computers. A registry key below is modified each time when LockerGoga is able to encrypt a file (Trend Micro, 2022).

HKEY_CURRENT_USER\SOFTWARE\Microsoft\ RestartManager\Session00{01-20}

LockerGoga encrypts the stored file with the help of CES mode AES algorithm (Figure 2). Its first 16 bytes are random numbers. This encryption method is referred as 'hybrid encryption' in some research papers, and allows assigning public and private keys for generated symmetric key in a random manner (Gupta and Sharma, 2012).

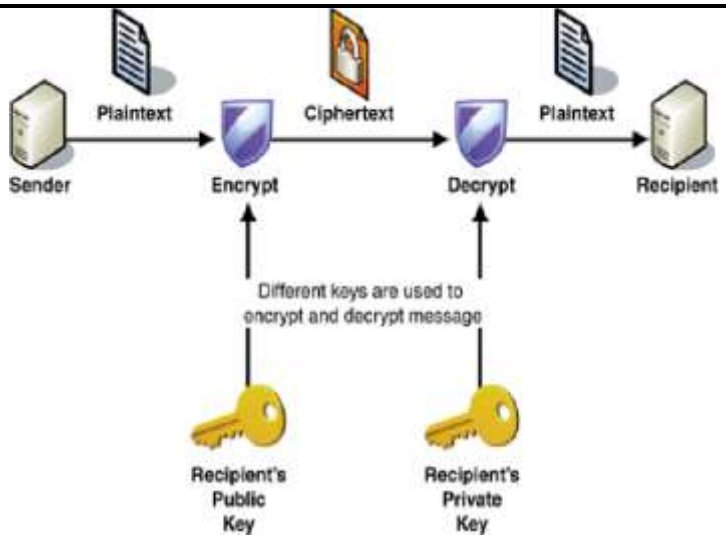


Figure 2: Hybrid encryption process, Taken from Gupta and Sharma (2012)

Step 4: In the final step, LockerGoga usually leaves a ransom note (README_LOCKED.txt) for the victims on their desktop. The snapshot 1 shows the list of file extensions marked for encryption.

```
aLnk            db '.lnk',0
                align 4
aDoc            db '.doc',0
                align 4
aDot            db '.dot',0
                align 4
aDocx           db '.docx',0
                align 4
aDocb           db '.docb',0
                align 4
aDotx           db '.dotx',0
                align 4
aDotb           db 'dotb',0
                align 4
aWkb            db '.wkb',0
                align 4
aXml            db '.xml',0
                align 4
aXls            db '.xls',0
                align 4
aXlsx           db '.xlsx',0
                align 4
aXlt            db '.xlt',0
                align 4
aXltx           db '.xltx',0
                align 4
aXlsb           db '.xlsb',0
                align 4
aXlw            db '.xlw',0
                align 4

aPpt            db '.ppt',0
                align 4
aPps            db '.pps',0
                align 4
aPot            db '.pot',0
                align 4
aPpsx           db '.ppsx',0
                align 4
aPptx           db '.pptx',0
                align 4
aPosx           db '.posx',0
                align 4
aPotx           db '.potx',0
                align 4
aSldx           db '.sldx',0
                align 4
aPdf            db '.pdf',0
                align 4
aDb             db '.db',0
aSql            db '.sql',0
                align 10h
aCs             db '.cs',0
aTs             db '.ts',0
aJs             db '.js',0
aPy             db '.py',0
```

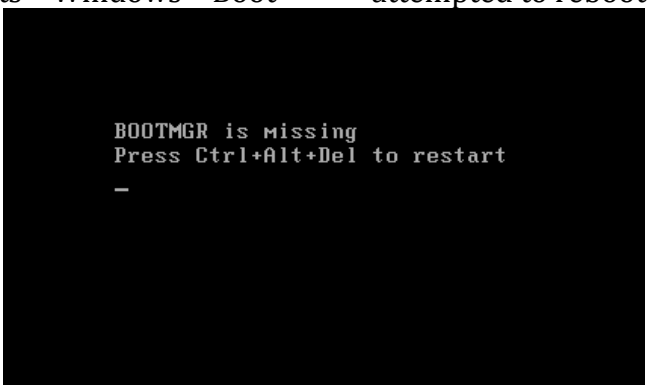
Snapshot 1: LockerGoga code that displays file extensions marked for encryption. Taken from Trend Micro (2019).

The static analysis carried out by 360 Threat Intelligence Center after Norsk Hydro attack reveals that LockerGoga spreads itself among the Wi-Fi of the infected system and network adapters. Then, a function (Snapshot 2) is run via the command line to disconnect the user from any outside connection.

```
v0 = GetAdaptersAddresses;
v1 = &AdapterAddresses;
SizePointer = 288;
v20 = &AdapterAddresses;
v2 = GetAdaptersAddresses(0, 0x1Cu, 0, &AdapterAddresses, &SizePointer);
if ( v2 == 111 )
{
  v1 = sub_430641(SizePointer);
  v20 = v1;
  if ( !v1 )
    return;
  if ( GetAdaptersAddresses(0, 0x1Cu, 0, v1, &SizePointer) )
    goto LABEL_36;
}
else if ( v2 )
{
  return;
}
v3 = v1;
if ( v1 )
{
  do
  {
    v15 = 0;
    if ( !sub_3F7269(&unk_49A40C, sub_3935B0, &unk_49A3A0) )
      sub_42F5C4(v3, v0);
    v16 = &unk_49A3A0;
    v23 = 0;
    v24 = 7;
    LOWORD(v22) = 0;
    v32 = 0;
    v29 = 0;
    v30 = 15;
    LOBYTE(lpMem) = 0;
    sub_388890("netsh.exe", 9);
```

Snapshot 2: LockerGoga code that displays how it disables the victim`s network adapter. Taken from Trend Micro (2019).

One of the success points of LockerGoga is that the ransomware prevents the victims from booting their systems after being infected even if it is restarted. This fact leads to another idea that LockerGoga encrypts Windows Boot manager(BOOTMGR) that is responsible for booting the operating system as well. The snapshot 3 displays the message that LockerGogare victims received when they attempted to reboot their infected systems.



Snapshot 3: The prompt that LockerGoga victims received while trying to restart the infected systems. Taken from Trend Micro (2022).

Unfortunately, the specialists were unable to decrypt the files encrypted by LockerGoga (Trend Micro, 2022), and this proves the fact that it is high time that companies should start strengthening their cyber-security to prevent LockerGoga ransomware.

III. Countermeasures To Lockergoga

The security analysis of LockerGoga ransomware in case of Norsk Hydro urges the researchers to figure out the necessary countermeasures to prevent this destructive virus. 360 Total Security suggests the company to *'update operating system security patches in time to prevent virus exploitation*', and scan computers on a regular basis (Qihu 360 Software, 2022). In this light, it is also necessary to keep the anti-virus software running well in the system.

Network Unlimited, Inc. (2022) has recently published an article releasing the countermeasures for most ransomware types including WannaCry, WannaCrypt and LockerGoga. One of the first preventative ways is not opening the email attachments that are not expected by users. As discussed above, in case of LockerGoga the attackers used spear phishing to put their LockerGoga virus on the

victims` computers (Norsk Hydro employees). Thus, there is usually high possibility of virus propagation once the users open the email attachments. Other countermeasures mentioned by research team are updating Microsoft Security Patch, and avoiding unlicensed or unknown software.

Beaumont and Pulsar (2019) urge all IT security teams in companies to block or flag the code that is signed with distrusted certificates as one necessary step to avoid LockerGoga or any similar ransomware types. It is also important to back up the files as often as possible, since the case of Norsk Hydro attack shows that the encrypted files by LockerGoga is never decrypted again.

Any password changes, specifically on servers should be detected and further analyzed by the local administrators, and in this light it is also helpful to detect the excessive usage of netsch.exe and lofoff.exe files on the system (Beaumont and Pulsar, 2019).

Center for Internet Security (2019) claims that companies should have an effective incident response plan which guides them the steps during major ransomware events. In case of Norsk Hydro ransomware attack, the recovery process was both slow and expensive. Duo Security (2022) states that the company spent approximately $ 40 million in a week after the attack, and still not all company operations are back to online regime.

Adamov *et al.* (2019) from Northumbria University analyzed the recommendations to protect vulnerable network and proposed the following basic steps as main countermeasures from ransomware:

- Backups: Storing most sensitive data in different devices
- Risk estimation: Conducting risk assessment in an organization
- Staff Trainings: Develop the staff knowledge on security measures
- Monitor the patch updates
- Monitor 'whitelisting' application: running only credited applications
- Incident Response Strategy: carefully planning, and exercising 'worst-case scenarios'.

The research article published on Computers & Electrical Engineering journal by Akbanov et al.(2019) gives a solution to ransomware mitigation by '*detecting suspicious activities through network traffic monitoring and blocking infected hosts by adding flow table entries into OpenFlow switches in real-time*'. These researchers used the case of WannaCry ransomware, happened on 9 February 2017, to come up with the mitigation solution. Accordingly, they built an experimental testbed consisting of six VMs. The researchers used Python-based plugins to monitor the network traffic, IP addresses and TCP ports. OpenvSwitch software, which supports, OpenFlow protocol was used to block a particular traffic flow when there is any kind of alert detected during checking process(Figure 3).

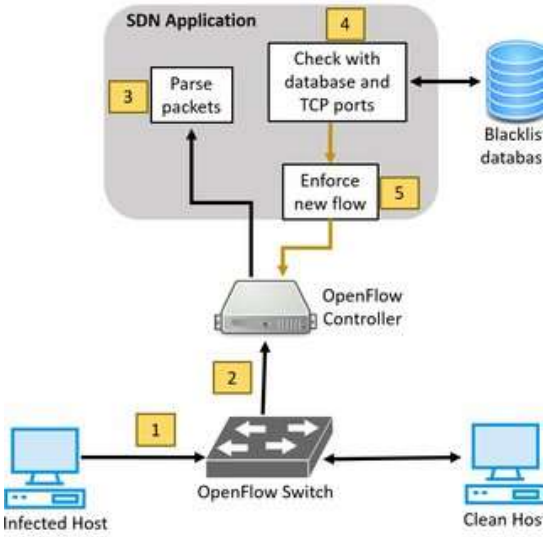


Figure 3: Ransomware detection and mitigation approach in case of WannaCry attack (Akbanov *et al.*,2019)

This feasible approach based on 'software-defined networking' is recommended to be implemented as a framework for LockerGoga detection and mitigation as well. As LockerGoga is a new family threat of ransomware and the researchers are still studying this sample, the approach brought by Akbanov et al. (2019) is believed to be the most appropriate framework for companies to implement in addition to other countermeasures stated above.

IV. Conclusion

After being attacked by LockerGoga ransomware, Norsk Hydro, Norwegian manufacturing giant, shut down several plants and also switched its plant operating model for a number of countries such as Norway, Qatar and Brazil to manual mode, which meant the employees had to spent at least 4 hours working on only one transaction (Bicchierai, cited in Qihu 360 Software, 2022). Following Norsk Hydro the same LockerGoga could infect American chemicals companies including Hexicon and Momentive, also blocking the computers and encrypting the server files. This paper was established to analyze LockerGoga ransomware and propose different methods to mitigate its risk. It is important to stress that LockerGoga is already on the top list of 10 biggest malware threats of 2019(Fuks, 2019), and it is preventable, but difficult to respond once being infected. Following Microsoft security practices, making online and offline data backups, avoiding suspicious attachments are discussed in this paper and believed to be most urgent countermeasures for LockerGoga ransomware. Furthermore, the paper has analyzed the particular framework helpful for alleviate the risk of ransomware threats such as WannaCry and believed to be an appropriate strategy for LockerGoga attack prevention. Yet, in addition to the discussed strategies, the role of security training and awareness from employees should not be overestimated. The simple security activities such as closing the browser when not using, encrypting sensitive information using appropriate tools and avoiding vulnerable operating systems such as Windows XP can prevent the danger of LockerGoga ransomware.

References

1. Adamo, A., Carlsson, A. and Surmacz, T. (2019). An analysis of LockerGoga Ransomware. IEEE Conference Paper. 10.1109.
2. Akbanov, M., Vassilakis, V. and Logothetis, M. (2019). Ransomware detection and mitigation using software-defined networking: The case of WannaCry. Computers & Electrical Engineering, 79(2019), pp.111-121.
3. Beaumont, K. (2019). How Lockergoga took down Hydro—ransomware used in targeted attacks aimed at big business [online] Available at:
4. https://doublepulsar.com/how-lockergoga-took- down-hydro-ransomware-used-in-targeted-attacks-aimed-at-big-business-c666551f5880 [Accessed 15 March. 2022].
5. Belton, J. (2019). Norsk Hydro hit by "severe" cyber attack [online]Available at:
6. https://www.itgovernance.eu/blog/en/norsk-hydro- hit-by-cyber-attack [Accessed 9 May. 2022].
7. Bichchierai, L. (2019). Ransomware Forces Two Chemical Companies to Order 'Hundreds of New Computers' [online] Available at: https://www.vice.com/en_us/article/8xyj7g/ransomw are-forces-two-chemical-companies-to-order-hundreds-of-new-computers [Accessed 12 May. 2022].
8. Center for Internet Security. (2019). Ransomware: Facts, Threats, and Countermeasures [online] Available at:
9. https://www.cisecurity.org/blog/ransomware-facts-threats-and-countermeasures/ [Accessed 16 May. 2022].
10. Fiveash, K. (2019). The Norsk Hydro cyber attack is about money, not war [online] Available at: https://www.wired.co.uk/article/norsk-hydro-cyber- attack [Accessed 8 May. 2022].
11. Fuks, L. (2019). 10 Ransomware Attacks You Should Know About in 2019 [online] Available at: https://www.allot.com/blog/10-ransomware-attacks- 2019/ [Accessed 18 May. 2022].
12. Gupta, Sh., Sharma, J.(2012). A hybrid encryption algorithm based on RSA and Diffie-Hellman. 2012 IEEE International

Conference on Computational Intelligence and Computing Research, pp.1-4.
13. Lopez, M. (2019). LockerGoga Ransomware Family Used in Targeted Attacks [online] Available at: https://securingtomorrow.mcafee.com/other- blogs/mcafee-labs/lockergoga-ransomware-family- used-in-targeted-attacks/ [Accessed 15 May. 2019].
14. Manual, J. and Salvio, J. (2019). LockerGoga: Ransomware Targeting Critical Infrastructure [online] Available at: https://www.fortinet.com/blog/threat-research/lockergoga-ransomeware-targeting-critical- infrastructure.html [Accessed 19 May. 2022].
15. Norsk Hydro ASA. (2019). About Hydro [online] Available at: https://www.hydro.com/en/about-hydro/ [Accessed 8 May. 2022].
16. O`Donnell, L. (2019). Norsk Hydro Calls Ransomware Attack 'Severe'[online] Available at: https://threatpost.com/norsk-hydro-calls-ransomware- attack-severe/142924/ [Accessed 8 May. 2021].
17. Qihu 360 Software Co. Limited. (2019). LockerGoga ransomware detailed analysis: targeted, efficient, destructive attacks [online] Available at: https://blog.360totalsecurity.com/en/lockergoga- ransomware-detailed-analysis-targeted-efficient- destructive-attacks/ [Accessed 15 May. 2021].
18. Rashid, F. (2019). Researchers Still Unraveling LockerGoga Ransomware [online] Available at: https://duo.com/decipher/researchers-still-unraveling- lockergoga-ransomware [Accessed 17 May. 2019].
19. Trend Micro. (2019). Spear phishing [online] Available at:
20. https://www.trendmicro.com/vinfo/us/security/definit ion/spear-phishing/ [Accessed 15 May. 2022].

APPENDICES

Appendix 1: A Ransom note received by LockerGoga victims in Norsk Hydro companies on 19 March, 2019. Adopted from Trend Micro (2019).


README_LOCKED.txt - Notepad

File Edit Format View Help

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).

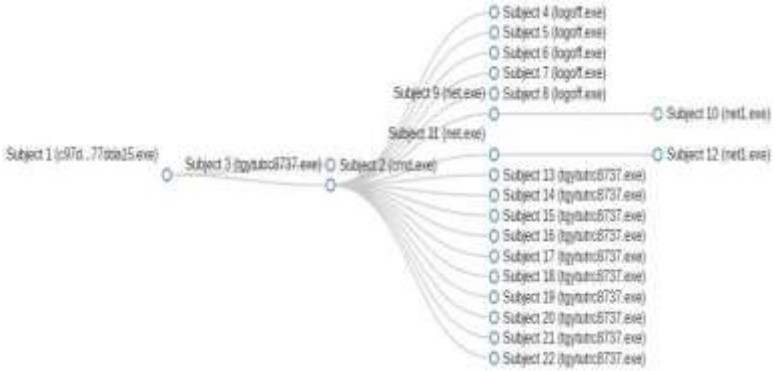
We exclusively have decryption software for your situation

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:

Appendix 2: Example of the process flow during execution of LockerGoga ransomware. Adopted from Qihu 360 Software (2022).



Appendix 3: Main features of LockerGoga ransomware. Adopted from Trend Micro (2019).

	LockerGoga
SHA-1	37cdd1e3225f8da596dc13779e902d8d13637360 b5fd5c913de8cbb8565d3c7c67c0fbaa4090122b
Platform	Windows NT
Compiler	Microsoft Visual C++ (2015)
Ransom Note	README-NOW.txt, README_LOCKED.txt (depends on variant)
Installation	Dropped as *%TEMP%\svc{random}.{random number}.exe*; executed as *%TEMP%\svc{random}.{random number}.exe -{random} -{random} {random}* *%TEMP%\tgytutrc{4 Random Numbers}.exe*
Extension appended to encrypted files	.locked
Process Terminations	
Startup Routine	
Files Encrypted	Documents, spreadsheets, slideshows, media, and scripts among others, except in %Program Files%, %ProgramData%, %System Root%\Recycle Bin, and %System Root%\Boot
Notable Behavior	Modifies passwords of all user accounts
Encryption Algorithm	Crypto++
File Structure	Not Packed