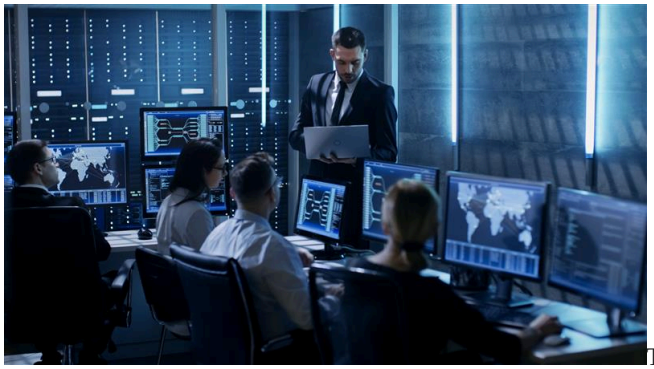
What You Need to Know About the LockerGoga Ransomware



The systems of Norwegian aluminum manufacturing company Norsk Hydro were reportedly struck last Tuesday, March 19, by LockerGoga ransomware. In a statement posted on their Facebook page, Norsk Hydro noted their “lack of ability to connect to the production systems causing production challenges and temporary stoppage at several plants.” The other plants, which had to be kept running, were forced to switchnews article to manual operations.

Trend Micro’s solutions, such as Trend Micro™ Securityproducts, Smart Protection Suites, and Worry-Free™ Business Security, actively detect and block LockerGoga. Trend Micro detects the ransomware and its variants as Ransom.Win32.LOCKERGOGA.THBOGAIopen on a new tab, Ransom.Win32.LOCKERGOGA.AAopen on a new tab, and Ransom.Win64.LOCKERGOGA.A. Our in-depth analysis of LockerGoga is still ongoing, and we will update this FAQ as we uncover more details on this threat.

Here’s what you need to know about the LockerGoga ransomware:

How does it arrive in the system?

Further research into LockerGoga revealed that the ransomware was dropped and executed by a renamed PsExec tool. It is the same system administration toolopen on a new tab abused by various ransomware such as SOREBRECTopen on a new tab and Bad Rabbitopen on a new tab. This could mean that the network was already compromised, and that the attackers conducted lateral movement. Since PsExec requires credentials to work, the attackers may have already obtained the credentials either through brute force, spearphishingopen on a new tab, or a previous malware infection or attack.

LockerGoga's destructive routines could also provide clues on how it is distributed. Since the ransomware neither gives the victims a chance to recover the files nor specifically asks for payment, LockerGoga's distribution was likely targeted and intended to disrupt operations.

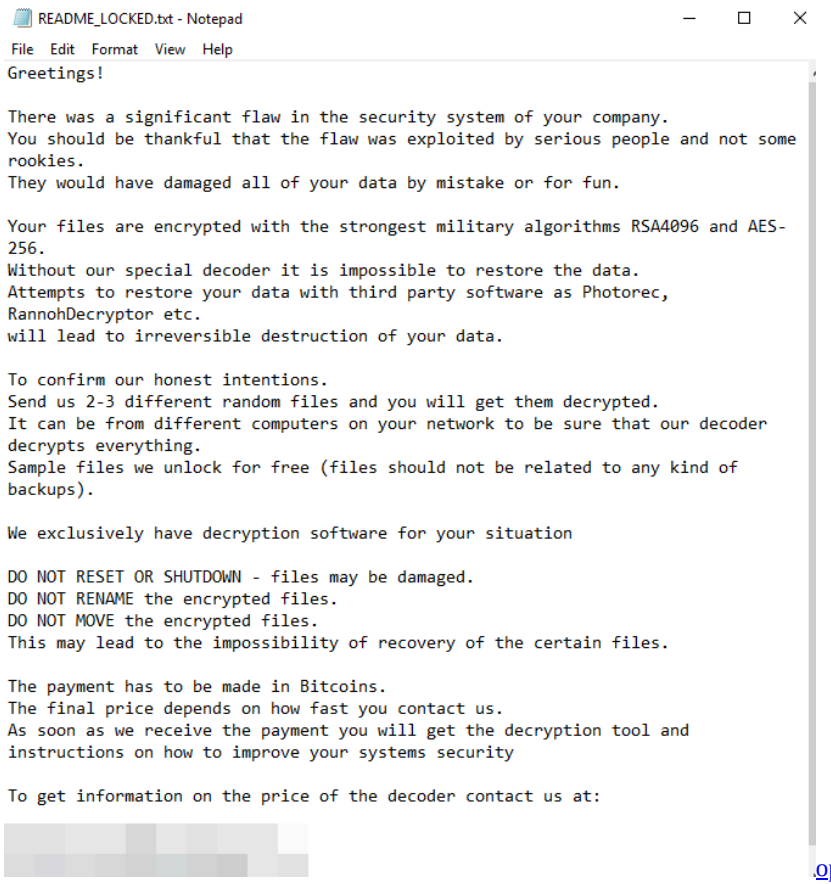
Is LockerGoga a new ransomware family?

LockerGoga first made the news in January this year after it was reportedlynews article used on an attack on Altran Technologies, an engineering consultancy company based in France. According to the company's press releasenews article, Altran Technologies shut down its IT networks and all applications to mitigate the threat. It also affected its operations in some countries in Europe.

What happens once LockerGoga infects a system?

Once installed, LockerGoga modifies the user accounts in the infected system by changing their passwords. It also tries to log off users logged in to the system. It would then relocate itself into a *temp* folder then rename itself using the command line (cmd). The command-line parameter used does not contain the file paths of the files targeted for encryption.

LockerGoga encrypts files stored on systems such as desktops, laptops, and servers. Each time LockerGoga encrypts a file, a registry key (*HKEY_CURRENT_USER\SOFTWARE\Microsoft\RestartManager\Session00{01-20}*) is modified. After the encryption process, LockerGoga leaves a ransom note in a text file (README_LOCKED.txt) in the desktop folder.



open on a new tab

Snapshot of LockerGoga's code showing the list of file extensions targeted for encryption

How does LockerGoga spread?

Initial analysis showed that LockerGoga, by itself, doesn't appear to have the capability to propagate like WannaCrynews-cybercrime-and-digital-threats or Petya/NotPetyanews- cybercrime-and-digital-threats.

Static analysis also revealed that LockerGoga enumerates the infected system's Wi-Fi and/or Ethernet network adapters. It will then attempt to disable them through the *CreateProcessW* function via command line (*netsh.exe interface set interface DISABLE*) to disconnect the system from any outside connection. LockerGoga runs this routine after its encryption process but before it logs out the current account. This is a notable behavior. Its file encryption routine could be considered less consequential since LockerGoga already locks the user out of the system by changing the accounts' passwords.

```
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_388B90("netsh.exe", 9);
```

[open on a new tab](#)

```
LOBYTE(v32) = 4;
CreateProcessRoutine_3B3CA0(&v25, &v13, "interface", "set", "interface", v3 + 40, "DISABLED", &v15, &unk_4730CA);
LOBYTE(v32) = 5;
if ( v13 && v13 != -1 )
```

[open on a new tab](#)

Snapshot of LockerGoga's code showing how LockerGoga disables the infected system's network adapter

How could LockerGoga evade traditional security solutions?

LockerGoga's code is digitally signed using various valid certificates — Alisa Ltd., Kitty's Ltd., and Mikl Limited. These certificates have since been revokednews article. Using a valid certificate could let the ransomware into the system. LockerGoga doesn't have network traffic, which can let it sidestep network-based defenses.

LockerGoga also has routines that can evade sandboxesnews article and virtual machines (VMs). The main process thread for some of LockerGoga's variants, for example, sleeps over 100 times before it executes. This is a technique used by various ransomware families and other threats, such as those used in targeted attacks. There are also some variants of LockerGoga that evade machine learning-based detection engines. We are still verifying these anti-sandbox and anti-machine learning capabilities in particular variants. This tactic isn't new: some Cerber ransomware variants, for instance, are known to have similar techniques.

What file types does LockerGoga encrypt?

LockerGoga's encryption process is instance-based, which is unusual compared to most ransomware families. This means that the ransomware spawns one process for each file that it encrypts. Some variants, however, encrypt more than one file per spawned process. LockerGoga encrypts documents and PDFs, spreadsheets and PowerPoint files, database files, and videos, as well as JavaScript and Python files. Here are some of the file extensions that LockerGoga targets to encrypt: *.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.*

Some of the variants of LockerGoga have certain parameters that include, but are not limited to: Encrypting a specific file, erasing a file, the email used in the ransom note, and even encryption of all file types.

In some of the samples we analyzed, LockerGoga prevents the victim from booting the infected system if it is restarted. LockerGoga's encryption process has little to no whitelist. This means that it will also encrypt Windows Boot Manager (BOOTMGR), which helps start the operating system. The image below shows the message displayed after an infected

system is restarted.

open on a new tab

The prompt displayed by an infected system after being restarted

Can systems and files encrypted by LockerGoga be decrypted?

At this time, there is no known way to unlock or decrypt systems and files encrypted by LockerGoga. It's worth noting that, compared to other ransomware families, some LockerGoga variants do not have a list of files to encrypt, and all of the variants that we have found do not allow an infected system to function well enough for the victim to pay the ransom or use a decryption tool.

Is LockerGoga a targeted attack?

There are no clear-cut indications that LockerGoga was used as part of an actual targeted attack, unlike the way attackers likely used Ryuk ransomwarenews- cybercrime-and-digital-threats. On the other hand, LockerGoga could be used and deployed to attack systems of certain targets, similar to the way HDDCryptor, Erebus Linux ransomware, and Crysis were used. LockerGoga, for instance, neither has network and command-and-control (C&C) activities nor relies on a C&C server to generate encryption keys, both of which are typical in cybercrime-driven ransomware attacks.

Does LockerGoga have any connection to the Ryuk ransomware?

While both ransomware families could be said to have been used against specific targets, LockerGoga doesn't appear to have direct links to the Ryuk ransomwarenews- cybercrime-and-digital-threats. For example, LockerGoga lacks certain routines that Ryuk has, such as network propagation and information theft. Here's a comparison between LockerGoga and Ryuk:

	Ryuk	**LockerGoga**
SHA-1	f047f4f4aa45c4ad3f158462178c0cfcc7373fe2	37cdd1e3225f8da596dc13779e902d8d13637360 b5fd5c913de8cbb8565d3c7c67c0fbaa4090122b
Platform	Windows NT	Windows NT
Compiler	Microsoft Visual C++	Microsoft Visual C++ (2015)
Ransom Note	RyukReadMe.txt	README-NOW.txt, README_LOCKED.txt (depends on variant)

Installation	Filename as is; executed from execution directory; injected in all running processes except *csrss.exe, explorer.exe, and lsaas.exe*	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	.ryk	.locked
Process Terminations	Stops AV-related processes or services, SQL-related applications, backup management software services, and Microsoft Office processes	
Startup Routine	*HKCU\Software\Microsoft\Windows\CurrentVersion\Run* and *svchos = {filepath as is \ filename as is}*	
Files Encrypted	Documents, images, spreadsheets, and PDFs except those in these folders: $Recycle.Bin, Windows, Mozilla, Chrome, AhnLab	Documents, spreadsheets, slideshows, media, and scripts among others, except in %Program Files%, %ProgramData%, %System Root%\Recycle Bin, and %System Root%\Boot
Notable Behavior	Deletes all Shadow Volume copies via *vssadmin.exe* and */all /Quiet*	Modifies passwords of all user accounts
Encryption Algorithm	RSA-4096 and AES-256 encryption algorithms	Crypto++
File Structure	Not Packed	Not Packed

How can users and businesses defend against LockerGoga?

Here are some of the best practicesnews- cybercrime-and-digital-threats against ransomware like LockerGoga:

- Regularly back up filesnews article.
- Keep systems and applications updated, or use virtual patchingnews article for legacy or unpatchable systems and software.
- Enforce the principle of least privilege: Secure system administrations toolsnews- cybercrime-and-digital-threats that attackers could abuse; implement network segmentationnews article and data categorizationnews article to minimize further exposure of mission-critical and sensitive data; disable third-party or outdated components that could be used as entry points.
- Secure email gatewaysnews- cybercrime-and-digital-threats to thwart threats via spam and avoid opening suspicious emails.
- Implement defense in depth: Additional layers of security like application controlproducts and behavior monitoringproducts helps thwart unwanted modifications to the system or execution of anomalous files.
- Foster a culture of security in the workplace.

Updated as of March 20, 2019, 8:20PM PDT to clarify the following details: how LockerGoga disables the infected system's network adapter; the use of RDP; deletion of backups; and file extensions targeted for encryption.

Updated as of March 28, 2019, 11:06PM PDT to add possible arrival methods and new updates on some other variants analyzed.

Updated as of April 11, 2019, 12:17AM PDT to clarify a subheading about LockerGoga being used as part of a targeted attack.

HIDE

Like it? Add this infographic to your site:

1. Click on the box below. 2. Press Ctrl+A to select all. 3. Press Ctrl+C to copy. 4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.
