TLP-WHITE - Free to share

last updated on 05-04-2019 23.30 CET by PO (Note: Added Fireeye report)

Note: If you have questions or additional public information to share, drop us a line at cert@abuse.io

Update:
	full report: https://www.fireeye.com/blog/threat-research/2019/04/pick-six-intercepting-a-fin6-intrusion.html

	TLDR;

	* FireEye has observed FIN6 conducting intrusions to deploy either Ryuk or LockerGoga ransomware
	* the initial phase of an intrusion using stolen credentials to an internet facing system and moving laterally using the Windows' Remote Desktop Protocol (RDP)
	* Using Cobalt Strike, Metasploit, and publicly available tools such as Adfind and 7-Zip to conduct internal reconnaissance, compress data, and aid their overall miss
	* Using powershell to execute encoded command(s) consisting of a byte array containing base64 encoded payload
	* Using paste site 'https://pastebin.com' to download and execute powershell commands
	* Creating (using Metasplot) a Windows Service named with a random 16-char string to execute encoded powershell commands.
	* Communicating with C2 servers using port 80 and 443
	* Utilized a named pipe impersonation technique included within the Metasploit framework that allows for SYSTEM-level privilege escalation.
	* Internal reconnaissance with a Windows batch file leveraging Adfind to query Active Directory, then 7-zip to compress the results for exfiltration
	 adfind.exe -f (objectcategory=person) > ad_users.txt
	 adfind.exe -f objectcategory=computer > ad_computers.txt
	 adfind.exe -f (objectcategory=organizationalUnit) > ad_ous.txt
	 adfind.exe -subnets -f (objectCategory=subnet) > ad_subnets.txt
	 adfind.exe -f "(objectcategory=group)" > ad_group.txt
	 adfind.exe -gcb -sc trustdmp > ad_trustdmp.txt
	 7.exe a -mx3 ad.7z ad_*
	* Configuring compromised internal servers als malware distribution servers and stage the LockerGoga ransomware, utilities and deployment scripts to automate the inst

	 - automated the deployment of kill.bat and the LockerGoga ransomware using batch script files. But also created a number of BAT files on the malware distribution se
	 - renamed the psexec service name to 'mstdc' in order to masquerade as the legitimate Windows executable 'msdtc.'
	 - running: start copy svchost.exe \\10.1.1.1\c$\windows\temp\start psexec.exe \\10.1.1.1 -u domain\domainadmin -p "password" -d -h -r mstdc -s -accepteula -nobanner

reported Hashes:
	c7a69dcfb6a3fe433a52a71d85a7e90df25b1db1bc843a541eb08ea2fd1052a4 (CONFIRMED, NOVERSION, UNSIGNED, RANSOMNOTE-MATCH)
	c3d334cb7f6007c9ebee1a68c4f3f72eac9b3c102461d39f2a0a4b32a053843a (CONFIRMED, NOVERSION, UNSIGNED, EMAIL-MATCH, RANSOMNOTE-MATCH)
	f3c58f6de17d2ef3e894c09bc68c0afcce23254916c182e44056db3cad710192 (CONFIRMED, NOVERSION, UNSIGNED, EMAIL-MATCH, RANSOMNOTE-MATCH)
	a84171501074bac584348f2942964c8550374c39247ec6af0f4a69756ea9fc7a (CONFIRMED, V0.9.9.0, UNSIGNED, NODETAILS)
	97a2ab7a94148d605f3c0a1146a70ba5c436a438b23298a1f02f71866f420c43 (CONFIRMED, V0.9.9.0, UNSIGNED, NODETAILS)
	5b0b972713cd8611b04e4673676cdff70345ac7301b2c23173cdfeaff564225c (CONFIRMED, V1.0.1.0, MIKL-SIGNATURE, EMAIL-MATCH, RANSOMNOTE-MATCH)
	8cfbd38855d2d6033847142fdfa74710b796daf465ab94216fbbbe85971aee29 (CONFIRMED, V1.0.2.0, MIKL-SIGNATURE, EMAIL-MATCH, RANSOMNOTE-MATCH)
	bef41d3c76aa98e774ca0185eb5d37da7bf128e3d855ebc699fed90f3988c7d3 (CONFIRMED, V1.1.0.0, MIKL-SIGNATURE, EMAIL-MATCH, RANSOMNOTE-MATCH)
	bdf36127817413f625d2625d3133760af724d6ad2410bea7297ddc116abc268f (CONFIRMED, V1.1.0.0, MIKL-SIGNATURE, EMAIL-MATCH, RANSOMNOTE-MATCH)
	14e8a8095426245633cd6c3440afc5b29d0c8cd4acefd10e16f82eb3295077ca (CONFIRMED, V1.1.1.0, MIKL-SIGNATURE, EMAIL-MATCH, RANSOMNOTE-MATCH)
	6e69548b1ae61d951452b65db15716a5ee2f9373be05011e897c61118c239a77 (CONFIRMED, V1.1.1.0, MIKL-SIGNATURE, EMAIL-MATCH, RANSOMNOTE-MATCH)
	7852b47e7a9e3f792755395584c64dd81b68ab3cbcdf82f60e50dc5fa7385125 (CONFIRMED, V1.2.0.0, KITTY-SIGNATURE, EMAIL-MATCH, RANSOMNOTE-MATCH)
	47f5a231f7cd0e36508ca6ff8c21c08a7248f0f2bd79c1e772b73443597b09b4 (CONFIRMED, V1.2.0.0, KITTY-SIGNATURE, EMAIL-MATCH, RANSOMNOTE-MATCH)
	eda26a1cd80aac1c42cdbba9af813d9c4bc81f6052080bc33435d1e076e75aa0 (CONFIRMED, V1.3.2.0, ALISA-SIGNATURE, EMAIL-MATCH, RANSOMNOTE-MATCH)
	ba15c27f26265f4b063b65654e9d7c248d0d651919fafb68cb4765d1e057f93f (CONFIRMED, V1.4.4.0, ALISA-SIGNATURE, EMAIL-MATCH, RANSOMNOTE-MATCH)
	7bcd69b3085126f7e97406889f78ab74e87230c11812b79406d723a80c08dd26 (CONFIRMED, V1.4.4.0, ALISA-SIGNATURE, EMAIL-MATCH, RANSOMNOTE-MATCH)
	c97d9bbc80b573bdeeda3812f4d00e5183493dd0d5805e2508728f65977dda15 (CONFIRMED, V1.5.1.0, ALISA-SIGNATURE, EMAIL-MATCH, RANSOMNOTE-MATCH)
	88d149f3e47dc337695d76da52b25660e3a454768af0d7e59c913995af496a0f (CONFIRMED, V1.5.1.0, ALISA-SIGNATURE, EMAIL-MATCH, RANSOMNOTE-MATCH)
	ec52b27743056ef6182bc58d639f477f9aab645722f8707300231fd13a4aa51f (CONFIRMED, V1.5.1.0, ALISA-SIGNATURE, EMAIL-MATCH, RANSOMNOTE-MATCH)

	2fe3c29913f66c255cb7aa5c34821ab182f889e7f96c25bad31267adc8a19e5b (CONFIRMED, V1.5.1.0, ALISA-SIGNATURE, SIGNATURE-MISMATCH, EMAIL-MATCH, RANSOMNOTE-MATCH)
		^^ Modified exe by submittor? c97d9bbc80b573bdeeda3812f4d00e5183493dd0d5805e2508728f65977dda15_new1.exe
	65d5dd067e5550867b532f4e52af47b320bd31bc906d7bf5db889d0ff3f73041 (CONFIRMED, V1.5.1.0, ALISA-SIGNATURE, SIGNATURE-MISMATCH, EMAIL-MATCH, RANSOMNOTE-MATCH)
		^^ Modified exe by submittor? c97d9bbc80b573bdeeda3812f4d00e5183493dd0d5805e2508728f65977dda15_new2.exe

	b686c88bce6629088ce1044b30ad1d5b978fd754601b8b463bc1f611b01d05d7 (Ransom note itself, no binary)
	39e298627215ed3bed76686f52eb741335195c2cd09b6918189 2b4fa9f53f514 (Ransom note itself, no binary)
	9128e1c56463b3ce7d4578ef14ccdfdba15ccc2d73545cb541ea3e80344b173c (Link based on Virustotal report, not confirmed)
	0e874661b6bc116f18230dd6b50f792a944f4ba8e3f58edf1f128517ce8d44ee (Link based on Virustotal report, not confirmed)
	7a059301a1c6198bb3a2cb2ae8cd358486f806ea1b202c4ca8613846a9c3cc64 (ZIP Containing c97d9bbc80b573bdeeda3812f4d00e5183493dd0d5805e2508728f65977dda15)

	The following hashes have been reporting by Palo Alta, but could not be confirmed yet:

	ae7e9839b7fb750128147a9227d3733dde2faacd13c478e8f4d8d6c6c2fc1a55
	f474a8c0f66dee3d504fff1e49342ee70dd6f402c3fa0687b15ea9d0dd15613a
	ffab69deafa647e2b54d8daf8c740b559a7982c3c7c1506ac6efc8de30c37fd5
	c1670e190409619b5a541706976e5a649bef75c75b4b82caf00e9d85afc91881
	31fdce53ee34dbc8e7a9f57b30a0fbb416ab1b3e0c145edd28b65bd6794047c1
	32d959169ab8ad7e9d4bd046cdb585036c71380d9c45e7bb9513935cd1e225b5
	e00a36f4295bb3ba17d36d75ee27f7d2c20646b6e0352e6d765b7ac738ebe5ee
	6d8f1a20dc0b67eb1c3393c6c7fc859f99a12abbca9c45dcbc0efd4dc712fb7c
	79c11575f0495a3daaf93392bc8134c652360c5561e6f32d002209bc41471a07
	050b4028b76cd907aabce3d07ebd9f38e56c48c991378d1c65442f9f5628aa9e
	1f9b5fa30fd8835815270f7951f624698529332931725c1e17c41fd3dd040afe
	276104ba67006897630a7bdaa22343944983d9397a538504935f2ec7ac10b534
	06e3924a863f12f57e903ae565052271740c4096bd4b47c38a9604951383bcd1
	a845c34b0f675827444d6c502c0c461ed4445a00d83b31d5769646b88d7bbedf

TLDR; Downloads:
	https://abuse.io/lockergoga/14e8a8095426245633cd6c3440afc5b29d0c8cd4acefd10e16f82eb3295077ca.zip
	https://abuse.io/lockergoga/8cfbd38855d2d6033847142fdfa74710b796daf465ab94216fbbbe85971aee29.zip
	https://abuse.io/lockergoga/47f5a231f7cd0e36508ca6ff8c21c08a7248f0f2bd79c1e772b73443597b09b4.zip
	https://abuse.io/lockergoga/bdf36127817413f625d2625d3133760af724d6ad2410bea7297ddc116abc268f.zip
	https://abuse.io/lockergoga/5b0b972713cd8611b04e4673676cdff70345ac7301b2c23173cdfeaff564225c.zip
	https://abuse.io/lockergoga/c7a69dcfb6a3fe433a52a71d85a7e90df25b1db1bc843a541eb08ea2fd1052a4.zip

https://abuse.io/lockergoga/6e69548b1ae61d951452b65db15716a5ee2f9373be05011e897c61118c239a77.zip
https://abuse.io/lockergoga/c97d9bbc80b573bdeeda3812f4d00e5183493dd0d5805e2508728f65977dda15.zip
https://abuse.io/lockergoga/7bcd69b3085126f7e97406889f78ab74e87230c11812b79406d723a80c08dd26.zip
https://abuse.io/lockergoga/eda26a1cd80aac1c42cdbba9af813d9c4bc81f6052080bc33435d1e076e75aa0.zip
https://abuse.io/lockergoga/5DA173EB1AC76340AC058E1FF4BF5E1B.crt
https://abuse.io/lockergoga/3d2580e89526f7852b570654efd9a8bf.crt
https://abuse.io/lockergoga/378d5543048e583a06a0819f25bd9e85.crt
https://abuse.io/lockergoga/pubkeys.txt
https://abuse.io/lockergoga/kill.bat.zip

linked public analysis:
https://www.vmray.com/analyses/ba15c27f2626/report/overview.html
https://www.joesandbox.com/analysis/115502/0/html
https://www.joesandbox.com/analysis/115449/0/html
https://www.joesandbox.com/analysis/117835/0/html
https://cuckoo.cert.ee/analysis/985741/behavior/
https://www.hybrid-analysis.com/sample/eda26a1cd80aac1c42cdbba9af813d9c4bc81f6052080bc33435d1e076e75aa0
https://www.hybrid-analysis.com/sample/ba15c27f26265f4b063b65654e9d7c248d0d651919fafb68cb4765d1e057f93f
https://www.hybrid-analysis.com/sample/7bcd69b3085126f7e97406889f78ab74e87230c11812b79406d723a80c08dd26
https://www.hybrid-analysis.com/sample/c97d9bbc80b573bdeeda3812f4d00e5183493dd0d5805e2508728f65977dda15
https://www.hybrid-analysis.com/sample/6e69548b1ae61d951452b65db15716a5ee2f9373be05011e897c61118c239a77
https://www.hybrid-analysis.com/sample/f3c58f6de17d2ef3e894c09bc68c0afcce23254916c182e44056db3cad710192
https://otx.alienvault.com/pulse/5c91064110773b02d94457fc?utm_medium=InProduct&utm_source=OTX&utm_content=Email&utm_campaign=new_pulse_from_subscribed

Possible mitigation (created and tested by AbuseIO):

(1) By blacklisting the code signing certificates:

Download each of the signing certificates and add them into the 'Untrusted Certificates' store. When starting the program
it will directly result in a file system error with code 65535 or that the administration has blocked this and stopping execution.
Even though the certificates seem to be revoked, only when 'blacklisting' will it actually have any effect. As its highly unlikely
that these certificates are used, they should be deployable on a large scale. Also with Active Directory its fairly easy to deploy.
Tested on Windows 7, if anyone deploy's this on other systems ... please share your results!

Example of mitigation tests:

test with sample 1 : https://app.any.run/tasks/5c563567-5d6e-43e0-a4e4-efb16e22d53f
test with sample 2 : https://app.any.run/tasks/81f27e59-2335-4e46-918d-1610de07dedf
test with sample 3 : https://app.any.run/tasks/8f419d29-0b8b-4b42-8e0a-a137fd38a254

You will need these 3 certicates, which you can download from AbuseIO or its origin:

CN=ALISA LTD:
Origin: https://www.hybrid-analysis.com/sample/eda26a1cd80aac1c42cdbba9af813d9c4bc81f6052080bc33435d1e076e75aa0?environmentId=100
direct download: https://abuse.io/lockergoga/5DA173EB1AC76340AC058E1FF4BF5E1B.crt

CN=MIKL LIMITED:
Origin: https://www.hybrid-analysis.com/sample/bdf36127817413f625d2625d3133760af724d6ad2410bea7297ddc116abc268f?environmentId=100
direct download: https://abuse.io/lockergoga/3d2580e89526f7852b570654efd9a8bf.crt

CN=KITTY'S LTD:
Origin: https://www.hybrid-analysis.com/sample/47f5a231f7cd0e36508ca6ff8c21c08a7248f0f2bd79c1e772b73443597b09b4?environmentId=100
direct download: https://abuse.io/lockergoga/378d5543048e583a06a0819f25bd9e85.crt

NOTE: You must add it to the UNTRUSTED CERTIFICATES folder.
NOTE: To download the files from the Hybrid Analysis website you will need to have a vetted account
NOTE: Always double check the certicate against the expected serial (listed below) for validation
WARNING: If you use the Origin's certificates as a source, please note they include the signing CA as well (Sectigo, Comodo and USERTrust RSA Code Signing CA's)
which for obvious reasons you DO NOT want to be added to your untrusted certificates. After importing the Binary certificate file(s) remove the CA's and only
leave the CN's listed on this page! To clarify: If you download the certificates from AbuseIO you will get the certificates with any CA's attached and are
directly usable for GPO usage.
Starting point for AD GPO deployment: https://docs.microsoft.com/nl-nl/windows-server/identity/ad-fs/deployment/distribute-certificates-to-client-computers-by-using-g

Yara rules:
https://otx.alienvault.com/indicator/yara/1f49429f805663702acf221177dd0e99f6ba3f46

Activation:
not fully known, however indications are that the attacker gained access in advance and moved up into the Active Directory until gained
a privileged account. Then the privileged account seems to be used to start powershell scripts and/or batch files on each system that stops several
services (see https://abuse.io/lockergoga/kill.bat for details) like antivirus and then starts this ransomware binary to encrypt the data.
In several cases arguments are passed onto the binary, such as -m $emailaddress, and this given e-mail address is then found in the ransom
note.

It has to be noted that the binaries are signed with valid code signing certificates (listed below).

It has been noticed that once the binary has been start it _first_ places the ransom note, and then starts many childs to
encrypt files.

LockerGoga variants are reported to change the password of all administrator accounts on the infected Windows workstation to "HuHuHUHoHo283283@dJD". This
includes the local admin account.

Static analysis also revealed that LockerGoga enumerates the infected systemâ€™s Wi-Fi and/or Ethernet network adapters. It will then attempt to disable them
through the CreateProcessWfunction 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.

There is a different usage of 'logoff' in the ransomware noticed. In the version most seen all users are logged off except the currently logged in user,
other version all users including the logged in user is logged off, another version did not logoff any user at all.

More interesting is the uses of the registry to keep status of its childs at the following location:
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\ under SessionXXXX (numeric only, e.g. 0000)
Passing subkeys like Sequence, SessionHash, RegFilesHash, RegFilesXXXX and Owner. However when trying to create this key manually
and set permissions to block any changes, no registry changes are done and the encryption just continues.

Interesting posts :

by @_qaz_qaz (confirmed by CW):

LockerGoga creates a new process from the current executable with the '-m' argument ('m' stands for 'master process'), the
sample uses Boost.Process library to manage processes. 'master process' creates shared memory and writes file paths in based64
encoded form.
For IPC the sample uses Boost.Interprocess library then creates child processes with following arguments: '-i SM-tgytutrc -s'
'-i' specifies mapped memory, '-s' stands for 'slave'. 'child process' decodes the file path from shared memory, generates
key/IV pair using RNG, encrypts the file using AES/Rijndael, encrypts key/pair with the public key and appends encrypted key/iv
to the encrypted file. The sample uses CryptoPP library for encryption, Boost:Filesystem library to query and manipulate paths,
files, and directories. If you execute the sample with '-l' argument, it will create a log file at C:\.log.txt

Forcepoint:

Encrypted files contain a hardcoded marker in the format GOGAxxxx, where XXXX is a number valid linked to the version number. This
version is also linked onto the binary, for example version 1.5.1.0 uses marker GOGA1510.

Encryption and possible decription:
NioGuard has written an analysis of the Ransomware and explains the encryption used, the hardcoded public keys and the footer encryption part.
All the hardcoded public keys have been extracted and placed in https://abuse.io/lockergoga/pubkeys.txt as a reference.

During the initialization phase, the worker instantiates an RSAFunction object and loads the hardcoded public key (Modulus and Public exponent)
in the PEM format. The cryptolocker uses RSA-1024 with the 'MGF1(SHA-1)' mask generation function for the OAEP padding scheme to encrypt 40
bytes buffer that contain first 4 zero bytes, 16-byte file IV, 16-byte file key, and the terminating 4-byte string "goga". Once encrypted, the
footer is stored to the end of the encrypted file.

It is possible to decrypt an encrypted file if a memory dump has been taken when the worker was encrypting the file. The file path and corresponding
AES key and IV can be found in the memory dump by searching the version string e.g. 'GOGA1320' and 'goga' string identifiers. To decrypt an encrypted
file for which you have located the key and IV in the memory dump you must delete the 48-byte footer from the encrypted file and then decrypt it with
any cryptographic tool, for example:

```
openssl aes-128-ctr -d -in $filename.locked -K $key -iv $iv -out $filename
```

Full read at : https://www.nioguard.com/2019/03/analysis-of-lockergoga-ransomware.html

Other IoC's:

Talos has also observed versions of the LockerGoga ransomware that attempt to clear the Windows Event Logs using the following command syntax:
"C:\Windows\System32\wevtutil.exe" cl Microsoft-Windows-WMI-Activity/Trace
---

Commands used:

taskhost.exe	(note: the ransomware copies this original Windows file to its own working dir e.g. c:\windows\temp\)
kill.bat	https://abuse.io/lockergoga/kill.bat
x??.bat	
powershell	
psexec.exe	(start psexec.exe \\123.123.123.123 -u domain\user -p "pass" -d -h -r mstdc -s accepteula -nobanner c:\windows\temp\xax.bat) (note: the ransomware copies this original Windows file to its own working dir e.g. c:\windows\temp\)
wmic.exe	(start wmic /node:"123.123.123.123" /user:"domain\user" /password:"pass" process call create "cmd /c c:\windows\temp\kill.bat")
cmd.exe	
move.com	
logoff.exe	(is called, but in some versions tests it did not actually logoff the user and the process hangs)
net.exe	
conhost.exe	

+ spawns multiple copies of itself util CPU has reached an average of more then 90%, minimal seen 12

Certificates used:

Subject CN=ALISA LTD, O=ALISA LTD, STREET=71-75 Shelton Street Covent Garden, L=LONDON, S=LONDON, PostalCode=WC2H 9JQ, C=GB
issuer CN=Sectigo RSA Code Signing CA, O=Sectigo Limited, L=Salford, S=Greater Manchester, C=GB
Serial: 5DA173EB1AC76340AC058E1FF4BF5E1B (compromised certificate)
issued: 2/21/2019 4:00:00 PM

Subject CN=MIKL LIMITED, O=MIKL LIMITED, STREET=16 Australia Road Chickerell, L=WEYMOUTH, ST=WEYMOUTH, OID.2.5.4.17=DT3 4DD, C=GB
issuer CN=COMODO RSA Code Signing CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB
Serial: 3d2580e89526f7852b570654efd9a8bf (compromised certificate, currently revoked)
issued: 06/25/2018 02:00:00

Subject CN=KITTY'S LTD, O=KITTY'S LTD, STREET=Kemp House 160 City Road, L=LONDON, ST=LONDON, OID.2.5.4.17=EC1V 2NX, C=GB
issuer CN=Sectigo RSA Code Signing CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB
Serial: 378d5543048e583a06a0819f25bd9e85
issued: 02/01/2019 01:00:00

IP addresses used:
103.73.65.116
176.126.85.207
185.202.174.31
185.202.174.41
185.202.174.44
185.202.174.80
185.202.174.84

185.202.174.91
185.222.211.98
185.238.0.217
185.70.105.158
185.70.105.43
185.70.184.134
185.70.184.250
185.70.187.21
185.70.187.22
185.70.187.23
185.70.187.38
185.70.187.46
185.70.187.51
185.70.187.53
185.70.187.56
185.70.187.65
185.70.187.77
185.70.187.79
185.70.187.86
185.70.187.88
185.70.187.92
31.192.108.122
31.192.108.123
31.207.44.118
31.207.44.186
31.207.44.77
31.207.44.80
31.207.44.83
31.207.44.84
31.207.45.251
31.207.45.45
31.220.45.151
46.166.173.109
5.39.219.159
5.39.219.168
5.39.219.172
5.39.219.183
5.39.219.184
5.39.219.185
5.39.219.187
5.39.219.188
62.210.136.65
89.105.194.236
93.115.26.171

URL's used:
hxxps://176.126.85[.]207:443/7sJh
hxxps://176.126.85[.]207/ca
hxxps://176.126.85[.]207:443/ilX9zObq6LleAF8BBdsdHwRjapd8_1Tl4Y-9Rc6hMbPXHPgVTWTtb0xfb7BpIyC1Lia31F5gCN_btvkad7aR2JF5ySRLZmTtY
hxxps://pastebin[.]com/raw/0v6RiYEY
hxxps://pastebin[.]com/raw/YAm4QnE7
hxxps://pastebin[.]com/raw/p5U9siCD
hxxps://pastebin[.]com/raw/BKVLHWa0
hxxps://pastebin[.]com/raw/HPpvY00Q
hxxps://pastebin[.]com/raw/L4LQQfXE
hxxps://pastebin[.]com/raw/YAm4QnE7
hxxps://pastebin[.]com/raw/p5U9siCD
hxxps://pastebin[.]com/raw/tDAbbY52
hxxps://pastebin[.]com/raw/u9yYjTr7
hxxps://pastebin[.]com/raw/wrehJuGp
hxxps://pastebin[.]com/raw/tDAbbY52
hxxps://pastebin[.]com/raw/wrehJuGp
hxxps://pastebin[.]com/raw/Bber9jae
hxxps://pastebin[.]com/raw/7Qmz6q5v
hxxps://pastebin[.]com/raw/wdcq0Tda
hxxps://pastebin[.]com/raw/9ditgTZh
hxxps://pastebin[.]com/Mzd1HFrN

Dropped note:
README-NOW.txt (in %Desktop% or c:\users\public\Desktop)
README_LOCKED.txt (in %Desktop% or c:\users\public\Desktop)

Encrypted extensions:
.locked

E-mail addresses used:
AbbsChevis@protonmail.com
AperywsQaroci@o2.pl
AsuxidOruraep1999@o2.pl
CottleAkela@protonmail.com
CouwetIzotofo@o2.pl
DharmaParrack@protonmail.com
DutyuEnugev89@o2.pl
IjuqodiSunovib98@o2.pl
MayarChenot@protonmail.com
PhanthavongsaNeveyah@protonmail.com
QicifomuEjijika@o2.pl
QyavauZehyco1994@o2.pl
RezawyreEdipi1998@o2.pl

RomanchukEyla@protonmail.com
SayanWalsworth96@protonmail.com
SchreiberEleonora@protonmail.com
SuzuMcpherson@protonmail.com
wyattpettigrew8922555@mail.com

Encryption algorithm
RSA4096
AES-256

Publicly known targets
French engineering consultancy Altran Technologies
https://www.bleepingcomputer.com/news/security/new-lockergoga-ransomware-allegedly-used-in-altran-attack/
https://ml.globenewswire.com/Resource/Download/0663f8d4-0acf-4463-b0fd-bb05042d1373
Norsk Hydro ASA
webcast 1 (19-3-2019) http://webtv.hegnar.no/presentation.php?webcastId=97819442
webcast 2 (20-3-2019 14.00) http://webtv.hegnar.no/presentation.php?webcastId=97841296
U.K.'s Police Federation
https://techcrunch.com/2019/03/21/police-federation-ransomware/
Hexion and Momentive
https://motherboard.vice.com/en_us/article/8xyj7g/ransomware-forces-two-chemical-companies-to-order-hundreds-of-new-computers
https://www.businesswire.com/news/home/20190322005490/en/Hexion-Addresses-Network-Security-Incident
(and four more instances are known privately)

Interesting references (which are included on this page):
https://unit42.paloaltonetworks.com/born-this-way-origins-of-lockergoga/
https://kc.mcafee.com/resources/sites/MCAFEE/content/live/CORP_KNOWLEDGEBASE/91000/KB91373/en_US/McAfee Labs Threat Advisory - LockerGoga.pdf
https://www.nioguard.com/2019/03/analysis-of-lockergoga-ransomware.html
https://www.forcepoint.com/blog/security-labs/lockergoga-ransomware-how-it-works
https://kwttoday.com/what-you-need-to-know-about-the-lockergoga-ransomware/
https://www.carbonblack.com/2019/03/22/tau-threat-intelligence-notification-lockergoga-ransomware/
https://blog.talosintelligence.com/2019/03/lockergoga.html
https://doublepulsar.com/how-lockergoga-took-down-hydro-ransomware-used-in-targeted-attacks-aimed-at-big-business-c666551f5880