TLP-WHITE - Free to share

last updated: 20-03-2019 14.45 CET

files:

- https://www.virustotal.com/#/file/ba15c27f26265f4b063b65654e9d7c248d0d651919fafb68cb4765d1e057f93f/detection
- https://www.virustotal.com/#/file/7bcd69b3085126f7e97406889f78ab74e87230c11812b79406d723a80c08dd26/detection
- https://www.virustotal.com/#/file/eda26a1cd80aac1c42cdbba9af813d9c4bc81f6052080bc33435d1e076e75aa0/detection
- https://www.virustotal.com/en/file/c97d9bbc80b573bdeeda3812f4d00e5183493dd0d5805e2508728f65977dda15/detection
- https://www.hybrid-analysis.com/sample/eda26a1cd80aac1c42cdbba9af813d9c4bc81f6052080bc33435d1e076e75aa0?environmentId=100

Hashes:

ba15c27f26265f4b063b65654e9d7c248d0d651919fafb68cb4765d1e057f93f
eda26a1cd80aac1c42cdbba9af813d9c4bc81f6052080bc33435d1e076e75aa0
7bcd69b3085126f7e97406889f78ab74e87230c11812b79406d723a80c08dd26
c97d9bbc80b573bdeeda3812f4d00e5183493dd0d5805e2508728f65977dda15
bdf36127817413f625d2625d3133760af724d6ad2410bea7297ddc116abc268f
5b0b972713cd8611b04e4673676cdff70345ac7301b2c23173cdfeaff564225c
6e69548b1ae61d951452b65db15716a5ee2f9373be05011e897c61118c239a77
0a960dd9c015545c2fe4d4f39bae6f9e7af1afb1933900f105c5ae9ec51a446d
88d149f3e47dc337695d76da52b25660e3a454768af0d7e59c913995af496a0f
8cfbd38855d2d6033847142fdfa74710b796daf465ab94216fbbbe85971aee29
97a2ab7a94148d605f3c0a1146a70ba5c436a438b23298a1f02f71866f420c43
a84171501074bac584348f2942964c8550374c39247ec6af0f4a69756ea9fc7a
bef41d3c76aa98e774ca0185eb5d37da7bf128e3d855ebc699fed90f3988c7d3
c3d334cb7f6007c9ebee1a68c4f3f72eac9b3c102461d39f2a0a4b32a053843a
c7a69dcfb6a3fe433a52a71d85a7e90df25b1db1bc843a541eb08ea2fd1052a4
f3c58f6de17d2ef3e894c09bc68c0afcce23254916c182e44056db3cad710192

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?environmentId=100
- https://otx.alienvault.com/pulse/5c91064110773b02d94457fc?utm_medium=InProduct&utm_source=OTX&utm_content=Email&utm_campaign=new_pulse_from_subscribed

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 a batch file that stops several services 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. Once the encryption has been started the user is logged out by running logoff.exe and the user cannot login anymore as the password is overwritten.

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

Commands used:

```
cmd.exe
move.com
logoff.exe
net.exe
conhost.exe
+ spawns multiple copies of itself, 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=GBCN=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:
None, yet.

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
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
(two more instances are known privately)