New Azer CryptoMix Ransomware Variant Released

bleepingcomputer.com/news/security/new-azer-cryptomix-ransomware-variant-released/

Lawrence Abrams

By
Lawrence Abrams

- July 5, 2017
- 05:15 PM
- 0

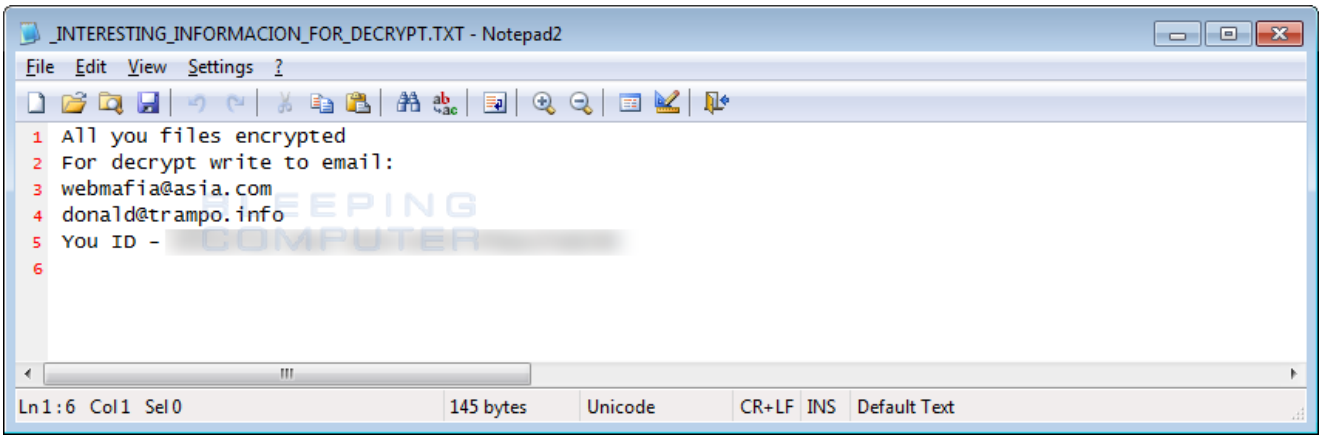
Today has been busy with ransomware and we have some some good news coming later today. For this story, though, we are going to take a look at the Azer variant of the Cryptomix ransomware. This version of Cryptomix was discovered today by security researcher MalwareHunterTeam right as a decryptor for the previous version, Mole02, was released.

While this ransomware encrypts files in a similar manner to all others in this family, I did notice some changes in this version that will be outlined below.

As we are always looking for weaknesses, if you are a victim of this variant and decide to pay the ransom, please send us the decryptor so we can take a look at it. You can also discuss or receive support for Cryptomix ransomware infections in our dedicated Cryptomix Help & Support Topic.

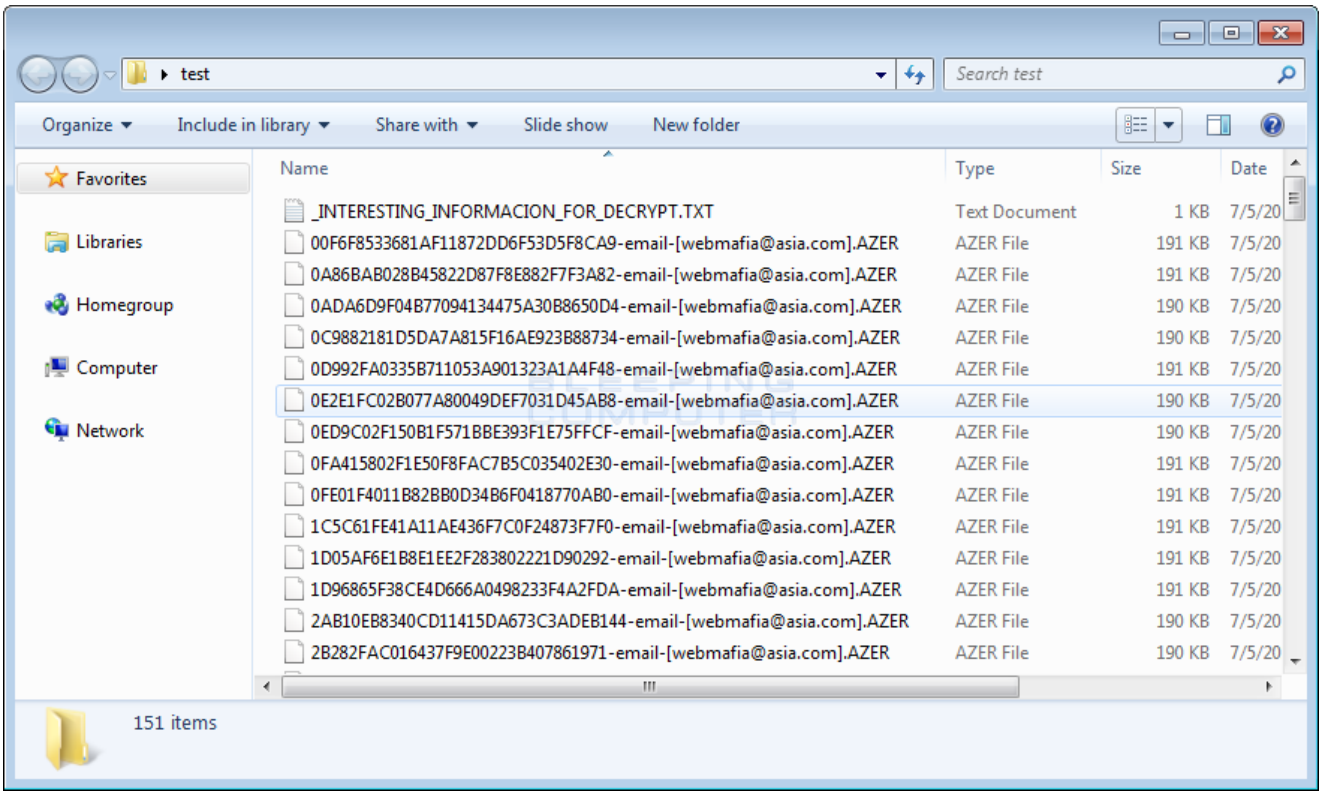
Changes in the Azer Cryptomix Ransomware Variant

While overall the encryption methods stay the same in this variant, there have been some differences. First and foremost, we have a new ransom note with a file name of **_INTERESTING_INFORMACION_FOR_DECRYPT.TXT**. This ransom note contains instructions to contact either **webmafia@asia.com** or **donald@trampo.info** for payment information.



Azer Ransom Note

The next noticeable change is the extension appended to encrypted files. With this version, when a file is encrypted by the ransomware, it will modify the filename and then append the string **-email-[email_address].AZER** to the encrypted file. For example, an test file encrypted by this variant has an encrypted file name of 32A1CD301F2322B032AA8C8625EC0768-email-[webmafia@asia.com].AZER.



Folder of Encrypted Azer Files

Last, but not least, this version performs no network communication and is completely offline. It also embeds ten different RSA-1024 public encryption keys, which are listed below. One of these keys will be selected to encrypt the AES key used to encrypt a victim's files. This is quite different compared to the Mole02 variant, which only included one public RSA-1024 key.

As this is just a cursory analysis of this new variant, if anything else is discovered, we will be sure to update this article.

Related Articles:

Dish Network confirms ransomware attack behind multi-day outage

New MortalKombat ransomware decryptor recovers your files for free

New 'MortalKombat' ransomware targets systems in the U.S.

U.S. Marshals Service investigating ransomware attack, data theft

New Exfiltrator-22 post-exploitation kit linked to LockBit ransomware

IOCs

File Hashes:

```
SHA256: 6f5f3bd509c22f0aec4a55fd4d08b7527be4708145b760bc3bd955c6e7538064
```

Filenames associated with the Azer Cryptomix Variant:

```
_INTERESTING_INFORMACION_FOR_DECRYPT.TXT
%AppData%\[random].exe
```

Azer Ransom Note Text:

```
All you files encrypted
For decrypt write to email:
webmafia@asia.com
donald@trampo.info
You ID - XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX
```

Emails Associated with the Azer Ransomware:

```
webmafia@asia.com
donald@trampo.info
```

Bundled Public RSA-1024 Keys:

```
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCTp02+iahQUVQQSGTYcAgUdyn8
R6D3+q/M1GwA4c6ePwXlsEJC8UC4hDE4otjs4Vae0MauQrvkYo2rnilCpiqsv0Oo
OjDgOHhHI1vUILpWjAVRu61DORWqdvQEH3x9GfGRIulKwhVdzll5sGS9pyGWAAGq
XvJ8T/ods5V+M3nFvQIDAQAB
-----END PUBLIC KEY-----

-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC2Zs4/PG+bhEhduEnmB/zS4Ps7
bD0EDn6q2tgpIwu7WF4NhDwnCQYeX9uweOs+x3pPKIHgZj7KtyOdwjJEMYt4yago
kMnp24CM413CbGz28tsSLifJpcDq7NdFlItv1foqE3EhxK4RnnsKRnlNnZOmJobj
BXWAK7kI6PMjAsycjQIDAQAB
-----END PUBLIC KEY-----

-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDdcVWIUztGfqsyayX8MJ+MilwA
OCMmaedwUkhcrOaZbEr/kjFAS/51dhxfUmoO2M6N51D1+Tlx1hFP0Bbea41ory14
/jXmBP/ARTPejT9wmAcdFSYL5RKqn21imymnSfllV7lLSS7fwzIhUibz/c13pk1w
UFQpsQKlAmge6nPWMQIDAQAB
-----END PUBLIC KEY-----

-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCoXHPF5pGepB37MwkGshTi4N+q
KaRbRAk6b6tDUxHK8AWyNDJTFKLygvaNTxjAcpY467SDTXQq6EyvaCh2juaSzCLH
qxcwIVRMH4mtBI8RKx5bycWssbuZD6XwQpcS7WABqE8+BuYDmALgeh1W0UVBQge5
Alv8dKw5oY2B84RApQIDAQAB
-----END PUBLIC KEY-----

-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCfshy8WocDLQBfn36LclXu7obD
X5hCJFAKntVU3Siyy6XKnumyu/qsiwekxG0QkDrEuWZWGk+/w5qVf+bw1wXbKnBr
h2FiYqtXgN8pX7h6vDhYNWd80RKg0fxA7sRYoB7HCtel99BCcGOKvWbsr9hcFq3j
EPtf81OdtqlTI6x6uwIDAQAB
-----END PUBLIC KEY-----

-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC3ncKb3ppnuXs7NtizXtdHcKcj
sfSIhS3E23j5Z4pxYfj3c3ipP8/gxu93/9b6qSQnQ87NRACf8NBbpr1XYR1kGkNK
cRk+u1QsKsVyYP8QoMtnCPbxaIAxZ9qc2o8eFPt44IbOFNo4TS682ZnrgvCIl/D+
taf9I8jbrBTSbfxQ3wIDAQAB
-----END PUBLIC KEY-----

-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCNdG6Kp5B6EHKVsENf2QudkLfe
TMzETNDGBk5cvGpj3On70vZGODVj/WfRe2iHyVE0ykT/iXXtb/C5gw3FePCSGVja
5S3qH9xh6Ncw5sFrsdgBbm7qPYSbRmux2VTjHlLE44ckkTTCSiTUL3KX/08cU04V
hb/JtNwKF5bg3ycuhQIDAQAB
-----END PUBLIC KEY-----

-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCqqapIMkQJgyt8mfVLZRPIEU20
V8c3+JbWNCdtDrIucv5nsKxJ/hCCDCau8gVjNN5jWtLltoQ0NvwR94HZaUkXAjGq
```

```
Iy+vvpc66SBLin8pJ/DzLtA3ouQBrYU2/9C75DrKGuCedEoAzoFkCjz/AokqjTkz
xSIkf+5//Rpoj22lHwIDAQAB
-----END PUBLIC KEY-----

-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCHZ0EKaGTzyOxqaX2ePqAs46RU
HhLRsApVWfO0z3BADXv4cv2iGjSXRZE1g7dU/KNEVZrjuBRaHksWpXKIwI6v7vSJ
ZcxsaNRZNS+RTwJbu5VNc5uHBc5YPa7sdqocVrt3b6eXXPbn5gZcQY3L18TTd+S3
DljCC6h8BC80BJI6OQIDAQAB
-----END PUBLIC KEY-----

-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCkrR8CoTgor4sIybnVarCSWzMN
RIoH51qIgCWDx49UQYXXqCn7I4T2XL7iOD5Fb/LO8LLS/BC7xNETIBGwUsOLMUXq
0LT3wlASZX4l491JPAAzlGfspmWqOnxwFZh4e2kqbix9uTGRw7oC0v7n6pACJSLW
ybODvrXAfJlITYUYIQIDAQAB
-----END PUBLIC KEY-----
```

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.