New Azer CryptoMix Ransomware Variant Released

By Lawrence Abrams

Published: 2017-07-05 · Archived: 2026-04-06 00:09:25 UTC

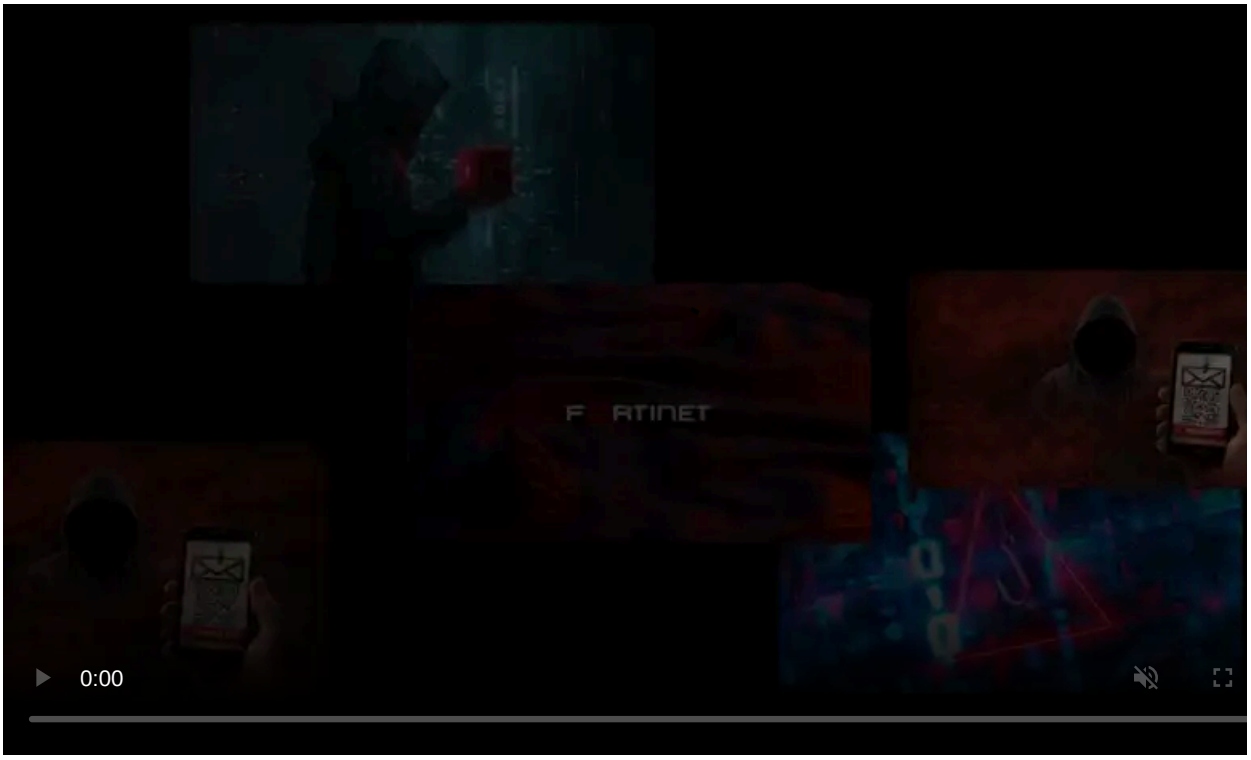
Today has been busy with ransomware and we have some some good news coming later today. For this story, though, we are going to take a look at the Azer variant of the Cryptomix ransomware. This version of Cryptomix was discovered today by security researcher MalwareHunterTeam right as a decryptor for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

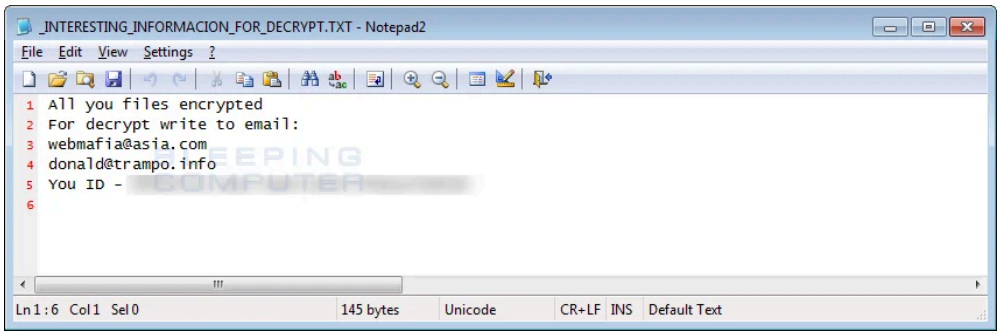
While this ransomware encrypts files in a similar manner to all others in this family, I did notice some changes in this version that will be outlined below.

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

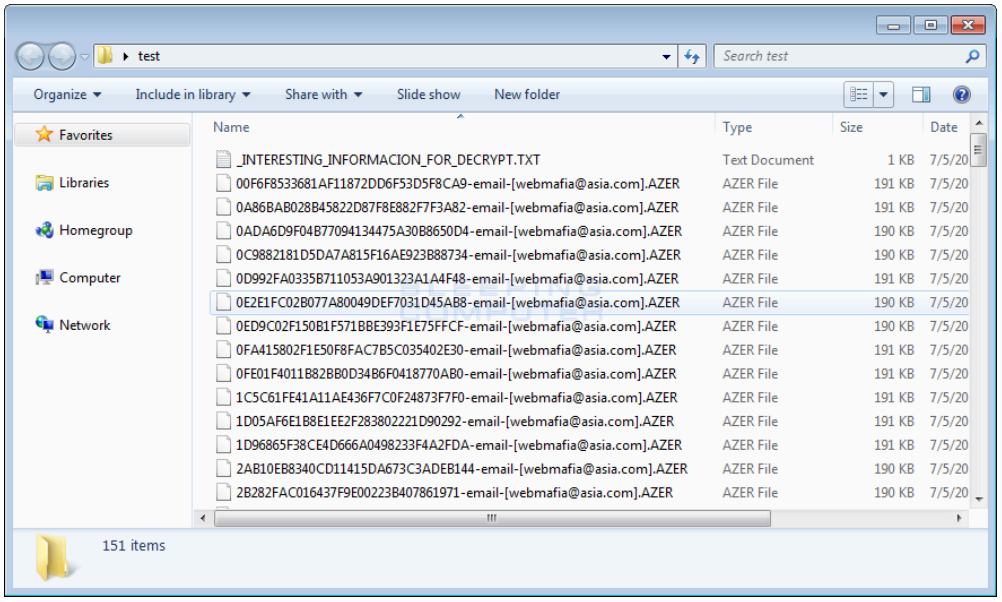
While overall the encryption methods stay the same in this variant, there have been some differences. First and foremost, we have a new ransom note with a file name of **_INTERESTING_INFORMACION_FOR_DECRYPT.TXT**. This ransom note contains instructions to contact either **webmafia@asia.com** or **donald@trampo.info**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


F RTINET
0:00



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.

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
```

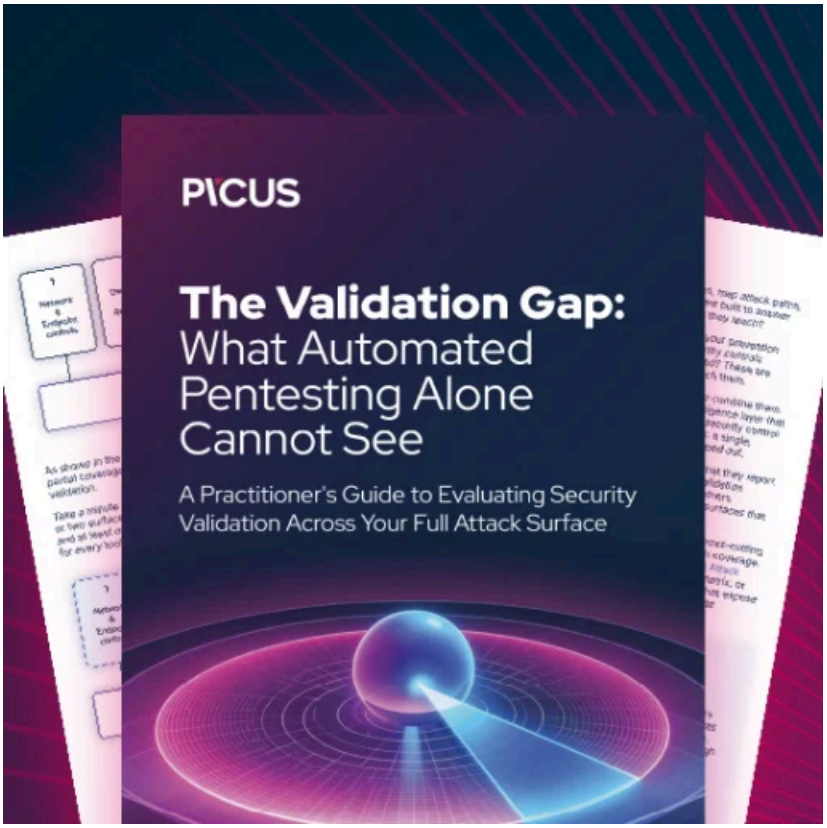
Emails Associated with the Azer Ransomware:

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

Bundled Public RSA-1024 Keys:

```
 -----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCTp02+iahQUVQQSGTYcAgUdyn8 R6D3+q/M1GwA4c6ePwXlsEJC8UC4hDE4otjs4Vae0MauQrvkYo2rnilCp
-----END PUBLIC KEY-----

-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC2Zs4/PG+bhEhduEnmB/zS4Ps7 bD0EDn6q2tgpIwu7WF4NhDwnCQYeX9uweOs+x3pPKIHgZj7KtyOdwjJEM
-----END PUBLIC KEY-----

-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDdcVWIUztGfqsyayX8MJ+MilwA OCMmaedwUkhcrOaZbEr/kjFAS/51dhxfUmoO2M6N51D1+Tlx1hFP0Bbea
-----END PUBLIC KEY-----

-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCoXHPF5pGepB37MwkGshTi4N+q KaRbRAk6b6tDUxHK8AWyNDJTFKLygvaNTxjAcpY467SDTXQq6EyvaCh2j
-----END PUBLIC KEY-----

-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCfshy8WocDLQBfn36LclXu7obD X5hCJFAKntVU3Siyy6XKnumyu/qsiwekxG0QkDrEuWZWGk+/w5qVf+bw7
-----END PUBLIC KEY-----

-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC3ncKb3ppnuXs7NtizXtdHcKcj sfSIhS3E23j5Z4pxYfj3c3ipP8/gxu93/9b6qSQnQ87NRACf8NBbpr1XV
-----END PUBLIC KEY-----

-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCNdG6Kp5B6EHKVsENf2QudkLfe TMzETNDGBk5cvGpj3On70vZGODVj/WfRe2iHyVE0ykT/iXXtb/C5gw3Fe
-----END PUBLIC KEY-----

-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCqqapIMkQJgyt8mfVLZRPIEU20 V8c3+JbWNCdtDrIucv5nsKxJ/hCCDCau8gVjNN5jWtLltoQ0NvwR94HZa
-----END PUBLIC KEY-----

-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCHZ0EKaGTzyOxqaX2ePqAs46RU HhLRsApVWfO0z3BADXv4cv2iGjSXRZE1g7dU/KNEVZrjuBRaHksWpXKIv
-----END PUBLIC KEY-----

-----BEGIN PUBLIC KEY-----
```

```
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCkrR8CoTgor4sIybnVarCSWzMN RIoH51qIgCWDx49UQYXXqCn7I4T2XL7iOD5Fb/LO8LLS/BC7xNETIBGwL
-----END PUBLIC KEY-----
```



[Automated Pentesting Covers Only 1 of 6 Surfaces.]

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/new-azer-cryptomix-ransomware-variant-released/