New AgeLocker Ransomware uses Googler's utility to encrypt files

bleepingcomputer.com/news/security/new-agelocker-ransomware-uses-googlers-utility-to-encrypt-files/

Lawrence Abrams

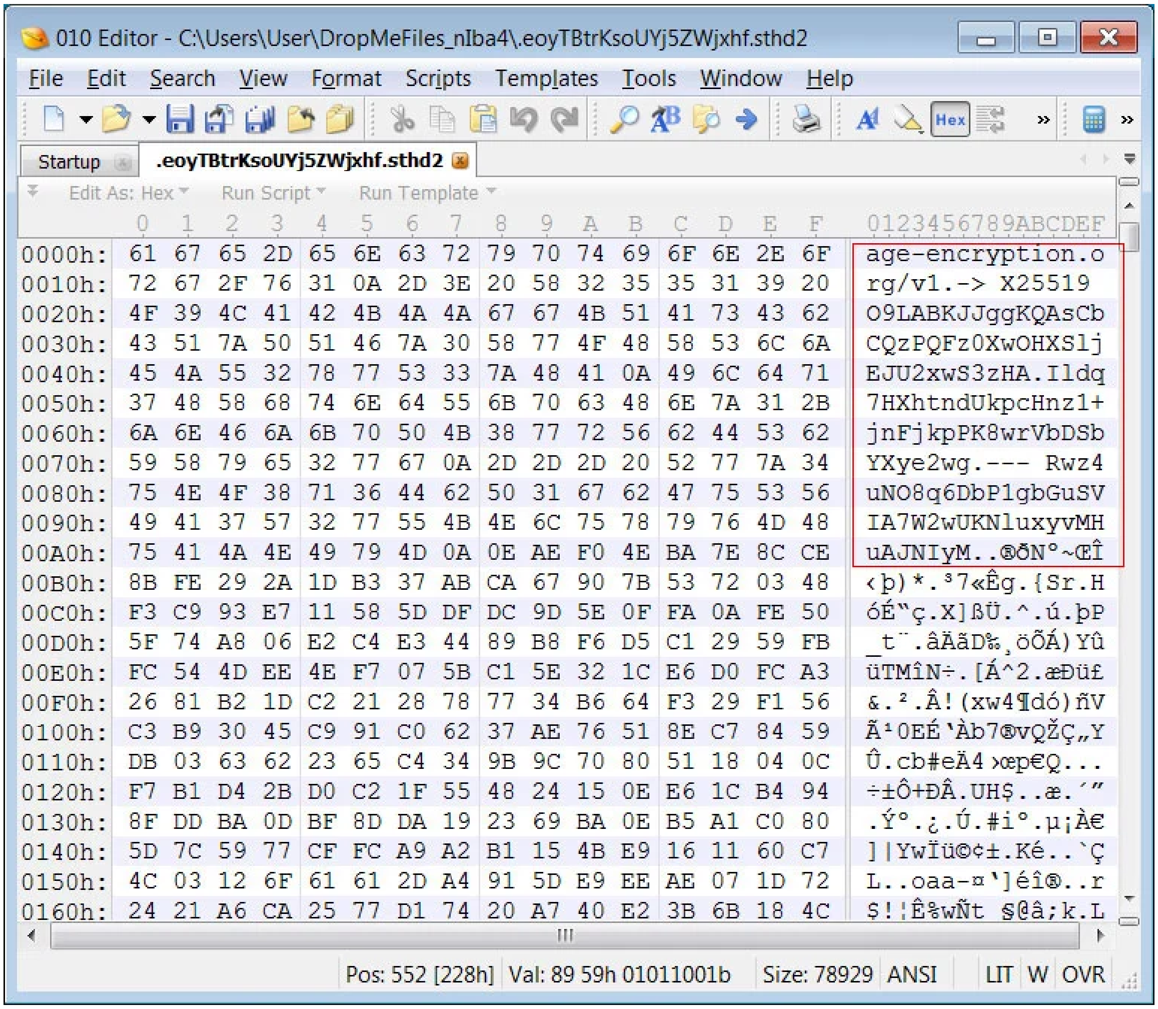
By
Lawrence Abrams

- July 13, 2020
- 09:57 PM
- 1

A new and targeted ransomware named AgeLocker utilizes the 'Age' encryption tool created by a Google employee to encrypt victim's files.

Yesterday, a consultant created a topic in the BleepingComputer forums about a new ransomware used in an attack against their client.

After examining the encrypted files, it was discovered that a text header was added to each file that starts with the URL 'age-encryption.org,' as shown below.


010 Editor - C:\Users\User\DropMeFiles_nIba4\.eoyTBtrKsoUYj5ZWjxhf.sthd2
File
Edit
Search
View
Format
Scripts
Templates
Tools
Window
Help
Hex
Startup
.eoyTBtrKsoUYj5ZWjxhf.sthd2
Edit As: Hex
Run Script
Run Template

```
         0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000h: 61 67 65 2D 65 6E 63 72 79 70 74 69 6F 6E 2E 6F  age-encryption.o
0010h: 72 67 2F 76 31 0A 2D 3E 20 58 32 35 35 31 39 20  rg/v1.-> X25519 
0020h: 4F 39 4C 41 42 4B 4A 4A 67 67 4B 51 41 73 43 62  O9LABKJJggKQAsCb
0030h: 43 51 7A 50 51 46 7A 30 58 77 4F 48 58 53 6C 6A  CQzPQFz0XwOHXSlj
0040h: 45 4A 55 32 78 77 53 33 7A 48 41 0A 49 6C 64 71  EJU2xwS3zHA.Ildq
0050h: 37 48 58 68 74 6E 64 55 6B 70 63 48 6E 7A 31 2B  7HXhtndUkpcHnz1+
0060h: 6A 6E 46 6A 6B 70 50 4B 38 77 72 56 62 44 53 62  jnFjkpPK8wrVbDSb
0070h: 59 58 79 65 32 77 67 0A 2D 2D 2D 20 52 77 7A 34  YXye2wg.--- Rwz4
0080h: 75 4E 4F 38 71 36 44 62 50 31 67 62 47 75 53 56  uNO8q6DbP1gbGuSV
0090h: 49 41 37 57 32 77 55 4B 4E 6C 75 78 79 76 4D 48  IA7W2wUKNluxyvMH
00A0h: 75 41 4A 4E 49 79 4D 0A 0E AE F0 4E BA 7E 8C CE  uAJNIyM..®ðN°~ŒÎ
00B0h: 8B FE 29 2A 1D B3 37 AB CA 67 90 7B 53 72 03 48  ‹þ)*.³7«Êg.{Sr.H
00C0h: F3 C9 93 E7 11 58 5D DF DC 9D 5E 0F FA 0A FE 50  óÉ“ç.X]ßÜ.^.ú.þP
00D0h: 5F 74 A8 06 E2 C4 E3 44 89 B8 F6 D5 C1 29 59 FB  _t¨.âÄãD‰¸öÕÁ)Yû
00E0h: FC 54 4D EE 4E F7 07 5B C1 5E 32 1C E6 D0 FC A3  üTMîN÷.[Á^2.æÐü£
00F0h: 26 81 B2 1D C2 21 28 78 77 34 B6 64 F3 29 F1 56  &.².Â!(xw4¶dó)ñV
0100h: C3 B9 30 45 C9 91 C0 62 37 AE 76 51 8E C7 84 59  Ã¹0EÉ‘Àb7®vQŽÇ„Y
0110h: DB 03 63 62 23 65 C4 34 9B 9C 70 80 51 18 04 0C  Û.cb#eÄ4›œp€Q...
0120h: F7 B1 D4 2B D0 C2 1F 55 48 24 15 0E E6 1C B4 94  ÷±Ô+ÐÂ.UH$..æ.´”
0130h: 8F DD BA 0D BF 8D DA 19 23 69 BA 0E B5 A1 C0 80  .Ý°.¿.Ú.#i°.µ¡À€
0140h: 5D 7C 59 77 CF FC A9 A2 B1 15 4B E9 16 11 60 C7  ]|YwÏü©¢±.Ké..`Ç
0150h: 4C 03 12 6F 61 61 2D A4 91 5D E9 EE AE 07 1D 72  L..oaa-¤‘]éî®..r
0160h: 24 21 A6 CA 25 77 D1 74 20 A7 40 E2 3B 6B 18 4C  $!¦Ê%wÑt §@â;k.L

Pos: 552 [228h]  Val: 89 59h 01011001b  Size: 78929  ANSI  LIT  W  OVR
```

AgeLocker encrypted file

An example of the text header appended to an encrypted file is below:

```
age-encryption.org/v1
-> X25519 O9LABKJJggKQAsCbCQzPQFz0XwOHXSljEJU2xwS3zHA
Ildq7HXhtndUkpcHnz1+jnFjkpPK8wrVbDSbYXye2wg
--- Rwz4uNO8q6DbP1gbGuSVIA7W2wUKNluxyvMHuAJNIyM
```

The URL age-encryption.org brings you to a GitHub repository for an encryption utility called 'Age' created by Filippo Valsorda, cryptographer, and Go security lead at Google.

According to the Age manual, the utility was designed as a replacement for GPG to encrypt "files, backups, and streams."

"This is a design for a simple file encryption CLI tool, Go library, and format.
It’s meant to replace the use of gpg for encrypting files, backups, streams, etc.
It’s called “age”, which might be an acronym for Actually Good Encryption, and it’s pronounced like the Japanese 上げ (with a hard g)."

Instead of creating a ransomware that utilizes commonly used encryption algorithms such as AES+RSA, the threat actors behind AgeLocker appear to be using the Age command line tool to encrypt a victim's files.

Ransomware decryption expert, Michael Gillespie, told BleepingComputer that Age uses the X25519 (an ECDH curve), ChaChar20-Poly1305, and HMAC-SHA256 algorithms, which makes it a very secure method to encrypt a file.

BleepingComputer has reached out to Valsorda to see if he had any advice that can be offered to victims but has not heard back.

AgeLocker ransom note sent via email

It is not known how the threat actors are gaining access to victim's computers, but once they gain access to the system, they utilize the Age encryption tool to encrypt the victim's files.

While encrypting data, a custom extension created with the victim's initials will be appended to each encrypted filename.

In a first for ransomware infections, instead of creating ransom notes on the encrypted system, the attackers emailed the ransom demand to the victim.

After the company's devices were encrypted in the reported attack, they received an email with a subject line of "[company name] security audit."

This ransom note listed the devices encrypted by the ransomware and instructions on how to get payment information.

```
Hello XXX and XXX,

Unfortunately a malware has infected your network and a millions of files has been
encrypted using a hybrid encryption scheme.
File names encrypted too.

Encrypted hosts are:

Storage:
1. XXX
2. XXX
3. XXX
4. XXX
5. XXX
Mac + external drives
1. XXX?
2. XXX?
3. XXX
4. XXX
5. XXX
6. XXX

You have to pay for decryption in Bitcoins.
The price depends on how fast you write us.
After payment we will send you the tool(for mac and linux) that will decrypt all
your files.

Free decryption as guarantee

Before paying you can send us up to 5 files for free decryption.
The total size of files must be less than 4Mb (non archived), and files should not
contain valuable information. (databases, backups, large excel sheets, etc.), file
name shouldn't be changed.

How to obtain Bitcoins

The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click
'Buy bitcoins', and select the seller by payment method and price.
https://localbitcoins.com/buy_bitcoins

Also you can find other places to buy Bitcoins and beginners guide here:
http://www.coindesk.com/information/how-can-i-buy-bitcoins/

Attention!
Do not rename encrypted files.
Do not try to decrypt your data using third party software, it may cause permanent
data loss.

Note: we can answer up to 6-9 hours, because of another timezone."
```

According to the victim, the threat actors are asking for 7 bitcoins, or approximately $64,500, to decrypt the files.

Unfortunately, it does not appear possible to recover files encrypted by Age for free at this time.

Related Articles:

Ransom payment is roughly 15% of the total cost of ransomware attacks

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Google shut down caching servers at two Russian ISPs

Industrial Spy data extortion market gets into the ransomware game

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

- AgeLocker
- Google
- Ransom
- Ransomware

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.

- Previous Article
- Next Article

Comments

Andre_M - 1 year ago

Has somebody paid a ransomware and got their data back?

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: