New Arena Crysis Ransomware Variant Released

By Lawrence Abrams

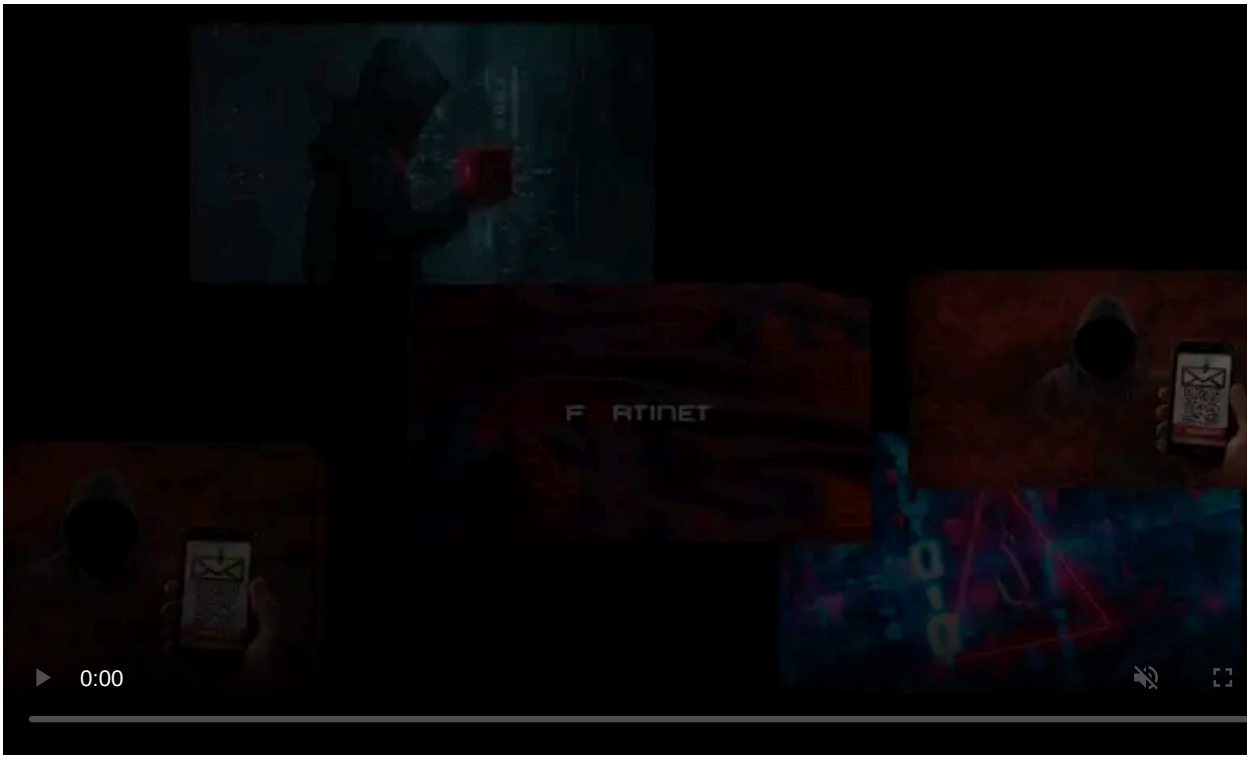
Published: 2017-08-25 · Archived: 2026-04-05 21:04:21 UTC

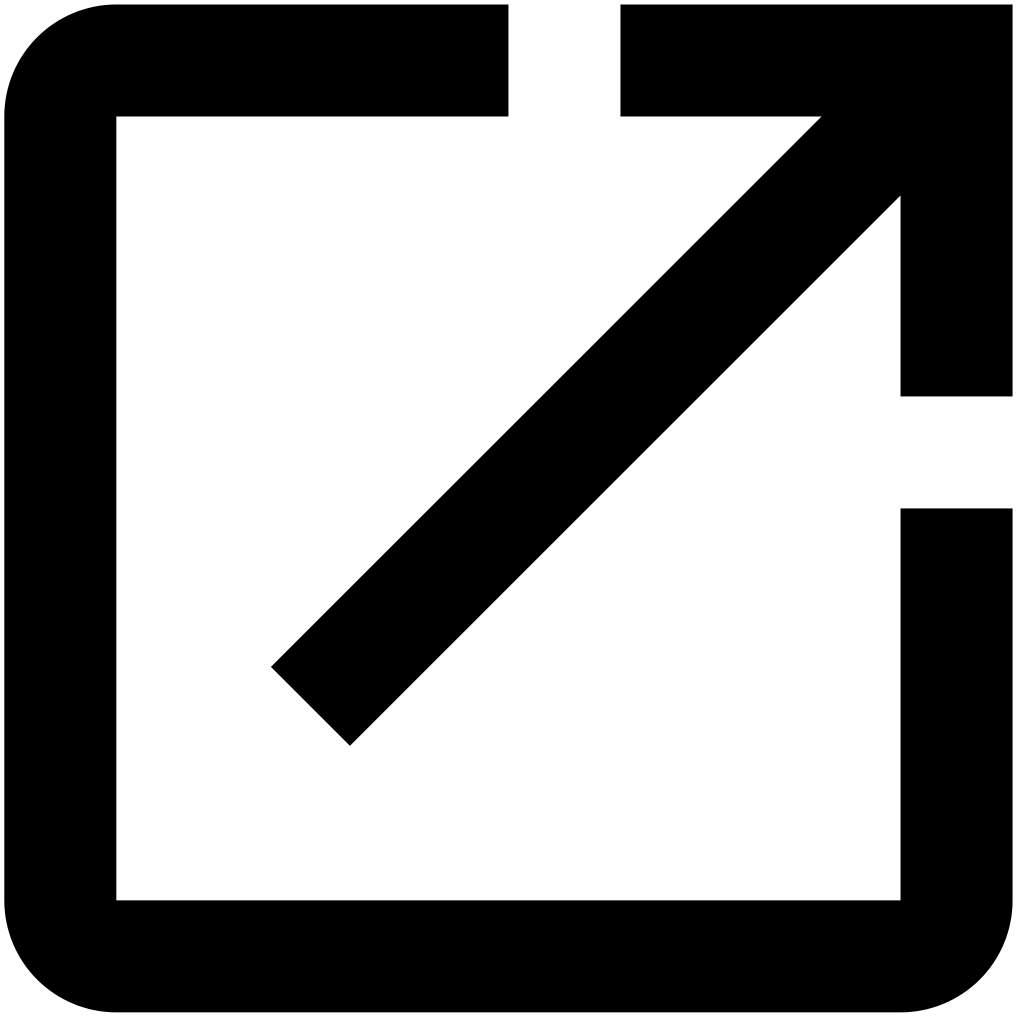
Yesterday, ID-Ransomware's Michael Gillespie discovered a new variant of the Crysis/Dharma ransomware that is appending the .arena extension to encrypted files. It is not known exactly how this variant is being distributed, but in the past Crysis was typically spread by hacking into Remote Desktop Services and manually installing the ransomware.

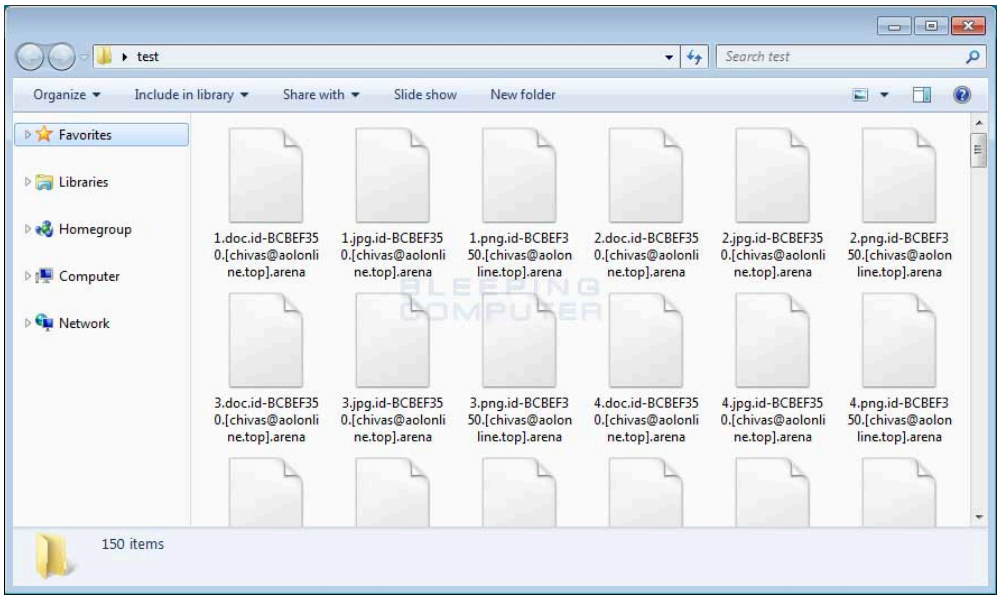
When this ransomware is installed, it will scan the computer for certain file types and encrypt them. When encrypting a file it will append an extension in the format of .id-[id].[email].arena. For example, a file called **test.jpg** would be encrypted and renamed to **test.jpg.id-BCBEF350.[chivas@aolonline.top].arena**.

It should be noted that this ransomware will encrypt mapped network drives and unmapped network shares. So it is important to make sure your network's shares are locked down so that only those who actually need access have permission.

You can see an example of an encrypted folder below.


F RTINET
0:00





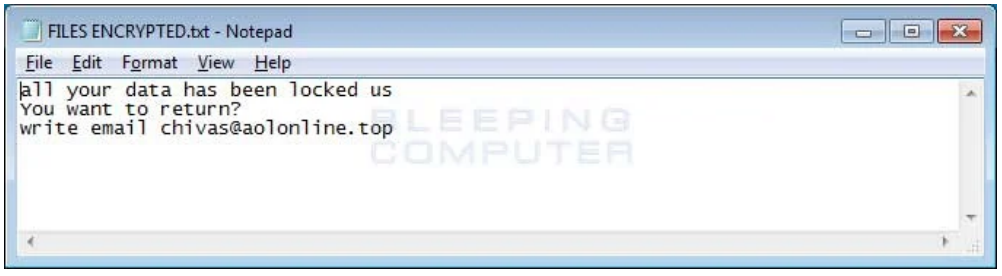
Files encrypted with the Crysis Arena Ransomware Variant

While encrypting a computer it will also remove all of the shadow volume copies so that you cannot use them to restore your files. It deletes them by running the **vssadmin delete shadows /all /quiet** command.

The Arena Crysis variant will also create two ransom notes. One is the **info.hta** file, which is launched by an autorun.

Crysis Arena Ransom Note

The other note is called **FILES ENCRYPTED.txt**.



FILES Encrypted Ransom Note

Both of these ransom notes contain instructions to contact **chivas@aolonline.top** in order to get payment instructions.

Finally, the ransomware will configure itself to automatically start when you login to Windows. This allows it to encrypt new files that are created since it was last executed.

It is not possible to decrypt the Crysis Arena Ransomware Variant

Unfortunately, at this time it is not possible to decrypt .arena files encrypted by the Crysis Ransomware for free.

The only way to recover encrypted files is via a backup, or if you are incredibly lucky, through Shadow Volume Copies. Though Crysis does attempt to remove Shadow Volume Copies, in rare cases ransomware infections fail to do so for whatever reason. Due to this, if you do not have a viable backup, I always suggest people try as a last resort to restore encrypted files from Shadow Volume Copies as well.

For those who wish to discuss the Crysis ransomware or need support, you can use our dedicated Crysis Ransomware Help & Support Topic.

How to protect yourself from the Crysis Ransomware

In order to protect yourself from Crysis, or from any ransomware, it is important that you use good computing habits and security software. First and foremost, you should always have a reliable and tested backup of your data that can be restored in the case of an emergency, such as a ransomware attack.

You should also have security software that contains behavioral detections such as Emsisoft Anti-Malware or Malwarebytes.

Last, but not least, make sure you practice the following good online security habits, which in many cases are the most important steps of all:

- Backup, Backup, Backup!
- Do not open attachments if you do not know who sent them.
- Do not open attachments until you confirm that the person actually sent you them,
- Scan attachments with tools like VirusTotal.
- Make sure all Windows updates are installed as soon as they come out! Also make sure you update all programs, especially Java, Flash, and Adobe Reader. Older programs contain security vulnerabilities that are commonly exploited by malware distributors. Therefore it is important to keep them updated.
- Make sure you use have some sort of security software installed.
- Use hard passwords and never reuse the same password at multiple sites.
- If you are using Remote Desktop Services, do not connect it directly to the Internet. Instead make it accessibly only via a VPN.

For a complete guide on ransomware protection, you visit our How to Protect and Harden a Computer against Ransomware article.

IOCs

Hash:

```
ARENA SHA256: a683494fc0d017fd3b4638f8b84caaaac145cc28bc211bd7361723368b4bb21e
```

Arena Crysis Ransomware FILES ENCRYPTED.TXT Ransom Note:

```
 all your data has been locked us
You want to return?
write email chivas@aolonline.top
```

Arena Crysis Ransomware INFO.hta Ransom Note:

```
All your files have been encrypted!
All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-
Write this ID in the title of your message [id]
In case of no answer in 24 hours write us to theese e-mails:chivas@aolonline.top
You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you
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 10Mb (non archi
How to obtain Bitcoins
The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller b
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.
Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can b
```

Source: https://www.bleepingcomputer.com/news/security/new-arena-crysis-ransomware-variant-released/