New Arena Crysis Ransomware Variant Released

bleepingcomputer.com/news/security/new-arena-crysis-ransomware-variant-released

By
Lawrence Abrams

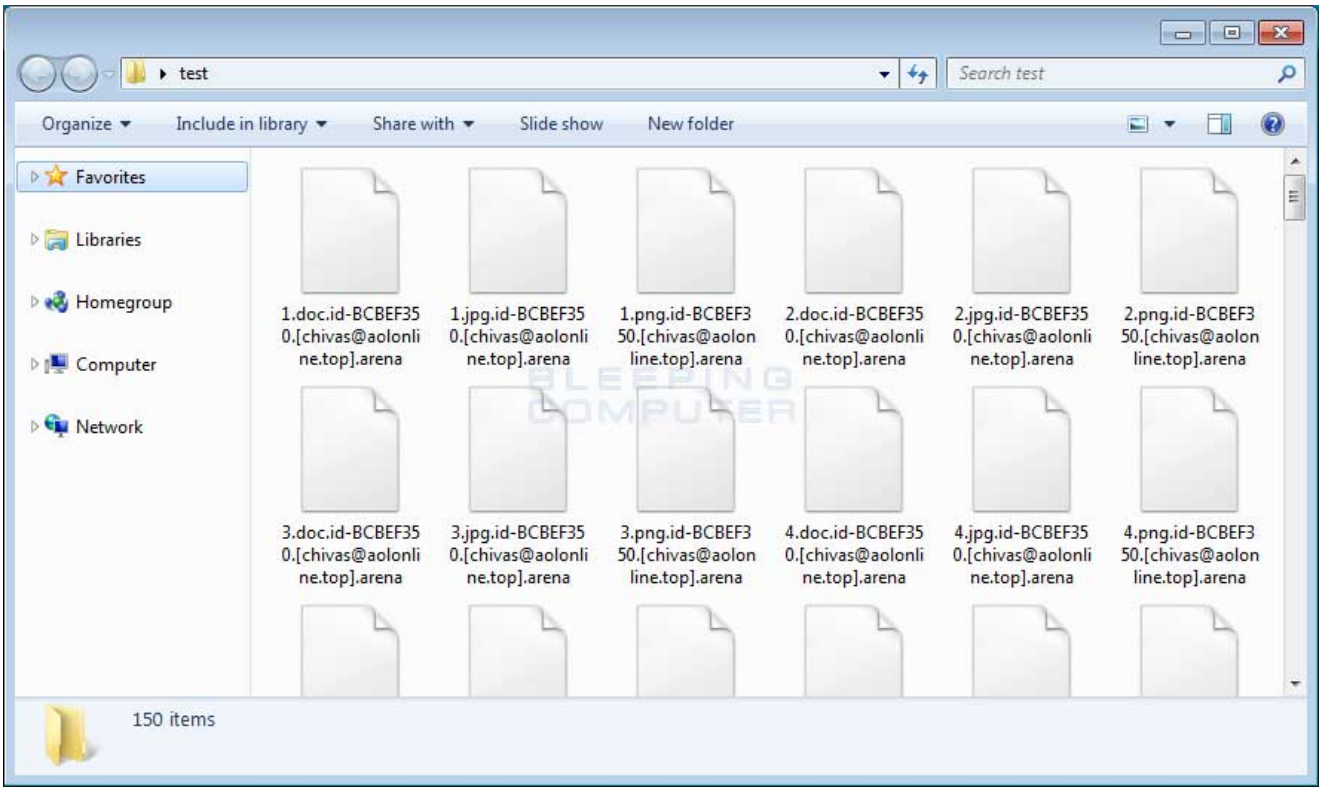
- August 25, 2017
- 03:12 PM
- 78

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.



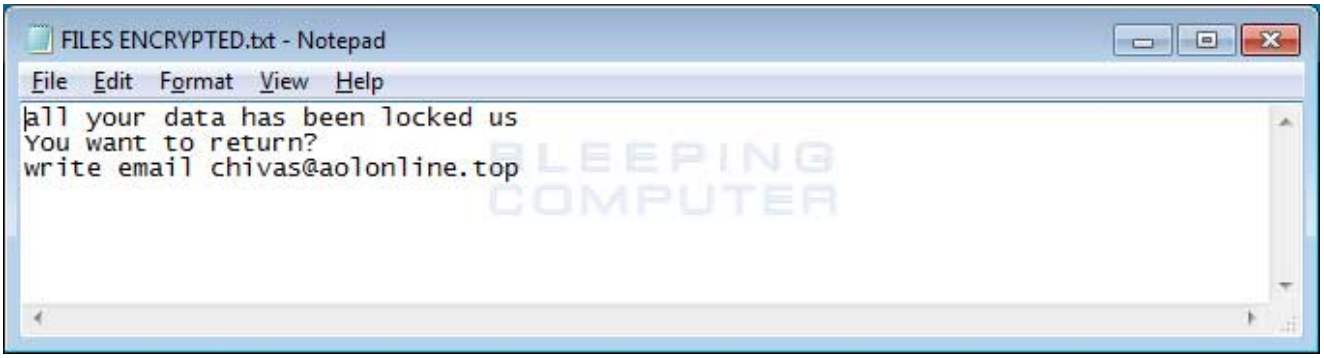
Files encrypted with the Crysis Arena Ransomware Variant

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.

Related Articles:

Indian airline SpiceJet's flights impacted by ransomware attack

US Senate: Govt’s ransomware fight hindered by limited reporting

New RansomHouse group sets up extortion market, adds first victims

Ransomware attack exposes data of 500,000 Chicago students

The Week in Ransomware - May 20th 2022 - Another one bites the dust

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-mail chivas@aolonline.top
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 the decryption tool 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 10Mb (non archived), and files should not contain valuable
information. (databases,backups, large excel sheets, etc.)
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.
Decryption of your files with the help of third parties may cause increased price
(they add their fee to our) or you can become a victim of a scam.
```

- Arena
- Crysis
- 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

- 

  joshbwood - 4 years ago

  I have a client that was infected by this variant. Is there anywhere to monitor for a decryption release?

- 

  Windblade89 - 4 years ago

  I am able to recover files but at this stage I can only recover MDF files.

- 

urosbe - 4 years ago

Do you maybe have any experiences with recovering Firebird 2.5 databases? Those databases are stores in single file with .FDB extension and they can be quite large (50MB-1GB).

- 

carrvirtual - 4 years ago

how did you recover mdf files?

- 

DoctorPartlow - 4 years ago

a client of mine got this, this morning. I have an exe file that was in c:\windows\temp if anyone can use it.

- 

  sumwand - 4 years ago

  my client infected by this ransomware variant.
  please let me know if there is a decryptor

  I already upload the encrypted sample file on id-ransomware.malwarehunterteam.com and www.nomoreransom.org.

  on virustotal.com detected as crysis.
  on id-ransomware detected as dharma (.cezar).

- 

  fahedenizi - 4 years ago

  me too

- 

  fahedenizi - 4 years ago

  Did anyone find a decrypter for this?

- 
  minhajbc - 4 years ago

  Our client infected by this ransom ware variant., please let me know if there is a decryption..

- 
  cyucuis - 4 years ago

  Has there been a decryption tool for this yet?

- 
  lolz84 - 4 years ago

  All my kids photos. gone. I'm almost suicidal.
  Please let me know if anyone finds a way to decrypt.

- 
  A_nester - 4 years ago

  My system infected .id-78C51056.[isera@cock.li].ARENA

- 

  Tommes123 - 4 years ago

  me too,
  *.id-606F5DBD.[help2017@cock.li].arena
  virusfile in registry: run=NZYN12_payload_2017-09-11_15-21.exe

- 

  Pre-ventas - 4 years ago

  id-785C34CF.[samurai@aolonline.top].arena

- 

  tom21186236001 - 4 years ago

  Hi. we paid the ransom for arena to samurai@aolonline.top and they then demanded more money and did not release the unlock key. happy to share my experience
  tom21186236001@gmail.com

- 

dottormarc - 4 years ago

Hi. Our customer paid the ransom for arena to brusli@aolonline.top and they then demanded more money too and did not release the unlock key.
Never pay them!

- 

tom21186236001 - 4 years ago

Does anybody still have the original virus? I have been speaking with some experts and they say If they get a copy they can maybe reverse engineer it?

- 

dragoss - 4 years ago

I sent you a private message with the arena virus i have. Let us know if you guys find some way to decrypt. Thanks

- 

tom21186236001 - 4 years ago

Thanks. Got it, I'll let everyone know when we have something working. meanwhile, if you or anyone else have a handful of small encrypted files you can send me for testing? there are a few keys in use so will be good to have a variety to test on.
thanks!

- 

lolz84 - 4 years ago

"Does anybody still have the original virus? I have been speaking with some experts and they say If they get a copy they can maybe reverse engineer it? "

Sent you a PM with a link to two files.

- 

fervillasenor92 - 4 years ago

thanks!

- 

msanchezwt - 4 years ago

I have more files

- 

fervillasenor92 - 4 years ago

I had exactly the same problem. Any suggestions?

- 

AriaDM - 4 years ago

How long has ransomware been a thing? Five years? Why are there people in these comments saying their clients have been infected? If you're an I.T. vendor, this is your job. It's your job to prevent this and to have backups.

DO YOUR JOBS.

- 

Gski - 4 years ago

I received the decryptor program which scanned my encrypted files and located 15 keys. This program then generated a file which was sent to the hacker. The hacker then sent me a key to paste into the same program and it restored all files which had his email address in the file name. along with the Hexidecimal code test.jpg.id-CC44FDAC. [email@Emailaddress].arena
I can upload the program and submitted and received keys if it helps someone. Still have a bunch of files with another email address in the name that were not decrypted. Hopefully someone can reverse engineer to help others.

- 

chaloupe - 4 years ago

I just had a call that a computer was infected in the last 24 hours with the arena extension. I'm in front of the computer and would love Gski if you could contact me with the upload program. Fingers crossed!!

- 

XeSSiV - 4 years ago

I just sent you a private message. If you could respond when you could that'd be great thank you!

- 

  stevo1985 - 4 years ago

  Hi, could i get a copy of the decryptor thanks

- 

  Tommes123 - 4 years ago

  Hello there, can you send me the files to try the "mission impossible"?
  I´m very interested in getting back my familyfotos and word-docs.
  Thank you !

- 

  Robert0101 - 4 years ago

  Gski, It would be a huge help to everyone if you could please update on your experience with the decryptor program. I would also like to get a copy of this decryptor and see if it will help with repairing the files I am in desperate need of repair.
  I think for sure there would be some reward money in it for you if you could supply more information and some of the major AntiVirus developers could produce a tool like the RakhniDecryptor. Please respond.

- 

andry79fi - 4 years ago

Hello
my server has been encrypted but was a Test Server.
On the server is still the ENCRYPTOR software!! Someone of you can "need" this to "TEST" and to generate a decryptor?

- 

kabelschoen - 4 years ago

Hello,
Got the virus too. Lost all my music and photo's on my NAS. Please help!!
Gski, can you please send me the decryptor program with keys? Hope it will work on my NAS.
Thanks, kind regards from Holland.

- 

felcoliveira - 4 years ago

Gski, an you please send me the decryptor program with keys too?

- 

  Stuart103 - 4 years ago

  Gski could you send me a copy or the decrypted and keys as well I Desperately need to get my files decrypted I have so many photos of my family some who are no longer with us.
  Would really appreciate any help to decrypt.....
  Thanks in advance fingers crossed.....

- 

  KostaF - 4 years ago

  Gski, i would greatly appreciate if you can send me decryptor with keys. Thank you sir

- 

  georgey78 - 4 years ago

  Gski can you pls send me a copy also, we have a huge situation here. Thanks

- 

Bill1006 - 4 years ago

Hay every one,
Let me start with this sucks I have my files on 3 different computers.....thought I was covered. All of the files now have this extension. Tension.mp3.id-F807A0A9.[min@zayka.pro].arena
Gski or any one else have a solution that would be great

- 

netmedia - 4 years ago

Is it posible to decrypt or not? Out customer have a big problem. All backup files are encrypt to.

- 

Gski - 4 years ago

I received this program from mailme@italymail.com

All my files were encrypted with either mailme@italymail.com or sconor3@aol.com in the file name descriptor

HELP_DECRYPT.PNG.id-CC44FDAC.[sconor3@aol.com].arena

This program & key only worked on the files with mailme@italymail.com in the file name:

Decryptor Program:

https://drive.google.com/open?id=0B_q_-yttmBtqelRhWk5FcG90MjQ

Encryption Key to insert after hitting Decrypt button:
Copy from this file and paste into program

https://drive.google.com/open?id=0B_q_-yttmBtqYnNsYll5SlV0UGc

Not sure it will work on anyone else's files unless you have mailme@italymail.com in the filename

Good luck

- 

netmedia - 4 years ago

Thanks, I'll try it out right away. however the e-mail address is different.
web-tables.xml.id-B8745C0A.[pepsicola@femconc.com].arena
(for example)

- 

Robert0101 - 4 years ago

Dear all,

If anyone has any more success with getting a decryption tool , or finds a solution to this terrible ransomware, it would help all here if they can share the experience.

Gski has done a great thing sharing his decryption tool from the hacker. I am working very hard on finding a solution for everyone too, plus I have some people working 20 hours per day on this.

1) Is this really a new variant of the CrySIS ransomware?
if so, then surely we should all be putting pressure on Kaspersky, Trend Micro and ESET to update their tools

https://www.nomoreransom.org/en/decryption-tools.html

I'm personally in direct communication with Kaspersky Virus Lab. I am persuading them to update the Rakhni Decryptor. I'm sure Gski's files are hugely helpful
https://noransom.kaspersky.com/

If there are any other received decryption tools , then please let me know in a private message asap.
Personally I am looking to recover design artwork files, but I'm sure for the greater good of all those who lost family photos etc, we will ALL appreciate a team effort to beat the hackers.

If I get any news from Kaspersky I will share on this post.

- 

FrJackHackett - 4 years ago

Any update? Appreciate the effort!

- 

KostaF - 4 years ago

Thank you GSKI,
I really appreciate you help.
I have tried your decryptor and keys. Unfortuanately they didnt work for me.

Robert0101 - thank you for helping.

- 

Matthew - 4 years ago

Hello ,
Same encryption over here , but different mailadress :
.[sm@uwmanage.com].arena
They decyphered a document for proof they got the key.
And they want 1 bitcoin for decryption tool.

- 

dkittitat - 4 years ago

Hi, I got my files encrypted too. I sent them an email and they asked how many infected computer, removable drive or NAS. The price for decryption tool is depending on infected computer. I answerd just 1 computer and they replied they wanted 1 bitcoin to decrypt my files.

- 

urosbe - 4 years ago

Same here. Our client's computer was encrypted with .id-BE00F590. [support@decrypt.ws].arena file extension due to open RDP port (non-default). Fortunatelly they have daily backup for most important data, but there are other files that I would like to recover. Data Recovery (Recuva was most efficient) did some small job, but not with large files. Price for decryption is 0.5 bitcoin if they pay within first 24 hours or 1 bitcoin after that. I have send them 3 sample files to decrypt but since then no answer so far. System is stable and running again, I have saved encrypted files for later and waiting for decrypting tool.
How long does it usually takes that encryption key is broken and is it possible that there won't be decryption tool at all for some randomware? I have read that some that it was not possible to break keys for some of them before attackers published their keys?

- 

MTguy - 4 years ago

Same here. Our company's computer was encrypted with .id C8621073. Does anyone get the encryption key? then i can restore the backup file.....

- 

cbrd07 - 4 years ago

Hello,
All of my files including the backup system i had just used was encrypted with id 04BCD9D4. I absolutely have to get these recovered. Please if anyone can help let me know.
Thanks

- 

help-decrypt - 4 years ago

Hello!
Someone who used the decryptor and got the key for decryption from intruders, please write to me private message.
There are a few questions...
Thanks!

- 

FrJackHackett - 4 years ago

Any update on a decryption key? Got hit on Friday after stupidly opening up RDP to a home media server (I know, I know :( ), several terabytes of media encrypted, which I can deal with, but some personal photos too. They're on a hard drive somewhere, but following a house move, so far unsuccessful in locating them!

- 

klyxmaster - 4 years ago

O man, I feel ya, I woke up and was already gonna reinstall winbloze, only becuase it was going slow lately (now I know why). But I also realized I forgot the shut down RDP. arg. and I have 200TB.I have most my critical files backed up, but still - this sux!

- 

Gski - 4 years ago

Do not pay a ransom to Sarah Conor at sconor3@aol.com. The hacker did provide evidence of the ability to decrypt 2 files, but when we paid in bitcoins for the decryptor program and key, the hacker stopped responding and did not provide either. Doesn't seem quite right, but there are hackers who are concerned about their reputations, this hacker obviously does not and will only take your money.

- 

Gski - 4 years ago

SCONOR3@aol.com - UPDATE

So my efforts with my 2nd decryptor program involving [sconor3@aol.com] continues. Four weeks after payment, I was contacted by sconor3@aol.com that there is a new person working there who can be trusted. They will send me the decryptor program and keys if I agree to write an endorsement here if successful. Their justification was the previous person was fired for being untrustworthy. I will let others know who follow me if I've had a successful transaction. Do not pay any bitcoins yet until I report back.

- 

Gski - 4 years ago

I have received a decryptor program from SCONOR3@aol.com as promised, scanned my files and the program generated a key file to return. I have sent the Key File to SCONOR3@aol.com and will report back if a SCONOR3@aol.com returns the decrypting key and all files are unlocked. Please be patient and do not pay your bitcoins until you hear back from me regarding success.

- 

Gski - 4 years ago

I am sorry to report that 15 hours after sending the program generated key I still have not received the unlock key. Waiting to see if the new management will keep their promises. Please do not send any bitcoins to SCONOR3@aol.com until you have confirmation from me that this person is trustworthy.

- 

Gski - 4 years ago

Sorry friends. I was under the impression that SCONOR3@aol.com was under a new person that could be trusted. It does not appear that you will have any success with SCONOR3@aol.com. Negotiations have not gone as planned and you should never pay this person.

- 

TheRonaldPerson - 4 years ago

I've seen a new version of this, with the extension [decrypt.guarantee@aol.com].block

The ransom note was identical otherwise, including the bad English.

We received decoded sample files as proof, so they do have the decryptor.

DO NOT PAY! We did, had no choice, but they DID NOT send the decryptor! They just kept demanding more money.

So, if this email address or file extension hits you, be warned, these guys DO NOT keep their word, even if you pay.

- 

help-decrypt - 4 years ago

Also:

Do not pay a ransom to "Can Help" with email restorefile@india.com !!!

They give a good discount - from 1 btc they lower the price 2-3 times, but the decryptor is not sent!
We have paid. As soon as we paid they stopped responding to emails. These hackers do not care about their reputation ...

But i would advise everyone not to pay ransom.

- 

help-decrypt - 4 years ago

So, my story with [restorefile@india.com] continues.
After almost two weeks after payment, extortionists contacted me and sent the decoder and keys! Their justification was - all my letters were in the spam.
I think it happened because I wrote on the web that they do not fulfill their obligations.
It worked with them - they even asked to edit the message.
Obviously [restorefile@india.com] take care of their reputation.

- 

klyxmaster - 4 years ago

Can you post or upload what you have to so others may benifit? My system has a differnt encryption, but It may work to unlock them - Much of my important stuff is on back up, but my academic stuff is encrypted.

- 

Robert0101 - 4 years ago

Update:

The Arena variant of this ransomware uses a "cryptographically secure algorithm". Kaspersky currently do not have a decryption tool, however imho I think they could and should update the RakhniDecryptor.

Kaspersky are calling "arena" a Crusis variant :
https://support.kaspersky.com/viruses/disinfection/10556#block1
Trojan-Ransom.Win32.Crusis:
.ID<...>.<mail>@<server>.<domain>.xtbl
.ID<...>.<mail>@<server>.<domain>.CrySiS
.id-<...>.<mail>@<server>.<domain>.xtbl
.id-<...>.<mail>@<server>.<domain>.wallet
.id-<...>.<mail>@<server>.<domain>.dhrama
.id-<...>.<mail>@<server>.<domain>.onion
.<mail>@<server>.<domain>.wallet
.<mail>@<server>.<domain>.dhrama
.<mail>@<server>.<domain>.onion

It all looks very familiar right?

I have given up on Kaspersky, I think it's possible they have much bigger fish to fry , especially in Russia with "Bad Rabbit" and other political issues.

I have had a long conversation with the hacker and its clear that they can only provide the decryption tool for the trojan virus they dropped with their email address in the file name.

E.g. support@decrypt.ws cannot decrypt the file locked by decrypt.guarantee@aol.com and vice versa.

Therefore the decryption tool that I might have received will not help anyone else , except a tiny possibility if you were infected by the same hacker as me. (same email address in the file name). But that would again be a chance in a million that the unlock keys actually worked on your cryptographic algorithm.

I know this is not the news we want to hear, but the only options you have now are:
1) Put all the file on a external disk and hold on for 6 months - 1 year to see if anyone updates the Crysis / Crusis / Dharma decryption tools.
Keep checking: https://www.nomoreransom.org/en/decryption-tools.html

2) Read post #1066 [CHAPTER 4]
https://www.bleepingcomputer.com/forums/t/632389/dharma-ransomware-filenameemailwalletceserarena-support-topic/page-72
Hope you get a result and only give money that you are prepared to lose.

3) Accept the loss and make sure have a better backup strategy because ransomware is going to increase as the price of bitcoin attracts more people.

- 
klyxmaster - 4 years ago

I will never pay - the key will surface. I am pretty patient. But that's not to say Im not steamed! I feel totally helpless, been on pc's since the early 80's, NEVER had this happen. And now that it does, it is a whooper!! I have stuff from the 90's I can no longer acess!!!

- 
deassuncao - 4 years ago

eu paguei 0,05 BTC e eles só me enviaram o decriptador...mas as chaves e o codigo nao me enviaram...Nao paguem nunca, sao inexcrupulosos

- F1L1O - 4 years ago

still no updates for the decryptor?

- 

caciavar - 4 years ago

I'm looking for a decryptor too. I was hit on Dec. 4th.

- 

Tommes123 - 4 years ago

At the moment it is not possible to decrypt.
Watch Kaspersky, Avast, Trendmicro and Eset.
The likelihood is greatest there.

- 

neco423 - 4 years ago

Any decryptor for new dhama variant? *.java ?

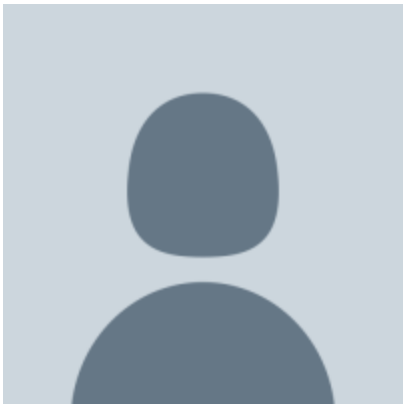
I have a lot of files encrypted :(

filename.id-406B4F5A.[black.mirror@qq.com].java

- 

Tommes123 - 4 years ago

https://security.stackexchange.com/questions/174961/dharma-ransomeware-files-decryption

- 

LuizConrado - 4 years ago

Hi, can anyone please let me know if this .java file has any decryption?
My computer where I had the pictures of my mom was infected.
I cannot lose these pictures. Please. I really need help.
(.id-08F95DA4.[dweezell@airmail.cc].java)
Thanks

- 

uroborosduo - 4 years ago

Dont pay they are scammers , they send you the first address and then they send you another address clayming its a new confirmed adress , you pay the first ramsom maybe you could even bargain the price but then they dont send you the keys claiming you paid to the wrong adress

- 

ahmerr3 - 4 years ago

hi. We have just been hit by the .arena ransomware, all of our important files have been encrypted. we are a small business and we do not have IT and did not keep a backup, which was agreed, very foolish of us. however we got a note as given above

"all you data has been locked us.
you want to return ?
email Macgregor@aolonline.top"

Please Please Please if anyone has a solution please help me!

- 

caciavar - 4 years ago

Has anyone ever used these guys? http://www.rm-ransomwarerecovery.com/
Are they reputable? Have you had any success recovering files encrypted with the .arena variant? They claim to be able to decrypt arena, but I'm skeptical...

- 

klyxmaster - 4 years ago

"Has anyone ever used these guys? http://www.rm-ransomwarerecovery.com/
Are they reputable? Have you had any success recovering files encrypted with the .arena variant? They claim to be able to decrypt arena, but I'm skeptical... "

I would be too, its not a secure site when dealing with these issues. Note the "http" vs "https". If it was something like an art site, or gaming site, no biggy, but we are talking about security issues, so either your promoting a suspicious site, or the site itself is subject.

- 

caciavar - 4 years ago

I can tell you that I'm definitely not promoting the site. A family member has been affected by this ransomware and i'm trying to look for solutions. I agree with your reasoning for why the site is suspicious.

- 

caciavar - 4 years ago

I can tell you that I'm definitely not promoting the site. A family member has been affected by this ransomware and i'm trying to look for solutions. I agree with your reasoning for why the site is suspicious.

- 

klyxmaster - 4 years ago

OK, lets use some common sense here:
INFECTION
Whether you like it or not, You, family member or employee made use of torrents, pirate sites or porn and any other suspect media to get what they wanted (and did not check it) Simple as that. Netflix, google, utility co. banks, phone co. etc.. major search engines etc.. are not gonna ransom your system.
With that said, these guys are bad guys (watch TV to better understand what a bad guy is). they have NO INTENTION OF HELPING YOU! They prey on the idiots that pay them. They don't care about those that are smart and know better. If you were smart you would have had a back up anyways of your "important" media (seriously, who doesn't back up their family pics, legal and business documents AND use that machine to surf the unprotected web). I had 16TB of data locked up. I just wiped all the drives and started from clean drives - why? I had all my good stuff backed up(stuff from 1992 yeowch!) - the rest of the stuff is replaceable over time.
So for those that feel the need to fork out money WASTEFULLY: PAY ME!! I need some work on my truck, and would like to start a down payment on a new houseand dump the condo scene (AND for those that have money to burn, pay me more - I would like to start a pc education biz for conducting internet safety and security LOL), . What do you get for paying me? same thing you get from these thieves: NOTHING. Just the peace of mind that it went to a good cause.

- 

caciavar - 4 years ago

I agree with you. More diligence needs to be taken with backing up sensitive data and revisiting backup strategies periodically.

One thing I should mention though is that the cause of this infection in most cases is not due to careless internet browsing, downloading torrents, porn or suspicious sites. This occurs when a hacker breaches port 3389 for remote desktop and logs into the target system to inflict the damage. The solution is better security practices such as hardening firewalls and using remote desktop over VPN.

In my case, port 3389 was forwarded to a desktop on my parent's network and the hacker exploited that security hole. It was my fault... I opened the back door to perform some VPN maintenance remotely, and forgot to close it when I was finished. I feel awful, but it's something I'll never do again.

- 

klyxmaster - 4 years ago

I retract the porn,torrent and other subjective media:

I "sorta agree", The only way for that port (or ANY port) to be exploited, is that it has to be forewarded - unless you are some super wanted politician, movie(**cough**)star or some other person of interest, and then you would be targeted. However, that does not seem to be the case here.

I run many game server, and host my own web server. Never really ran into any issue so to speak.

As you already admitted - you forwarded port 3389* - Many others I have dealt with, don't have a single port forwarded(or even know how to do it) outside some gaming ports for online gaming. But for the most part, those are pretty protected anyways. 9 already open and ripe for the picking? Random "port sniffing" might be the cause.

But I agree with you on the 3389, I forgot to turn mine off that night. I was hopping back and forth for some data, and just too lazy to shut it off. not too surprisingly, BAM! next morning system was running HORRIBLY slow. Takes awhile to lock up 16tb LOL. I was able to shut the system off before it killed my windows, but the damage was done. Restore took FOREVER!

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: