New Nuclear BTCWare Ransomware Released (Updated)

bleepingcomputer.com/news/security/new-nuclear-btcware-ransomware-released-updated

By
Lawrence Abrams

- August 28, 2017
- 04:01 PM
- 17

A new variant of the BTCWare ransomware was discovered by ID-Ransomware's Michael Gillespie that appends the **.[affiliate_email].nuclear** extension to encrypted files. The BTCWare family of ransomware is distributed by the developers hacking into remote computers with weak passwords using Remote Desktop services. Once they are able to gain access to a computer, they will install the ransomware and encrypt the victim's files.

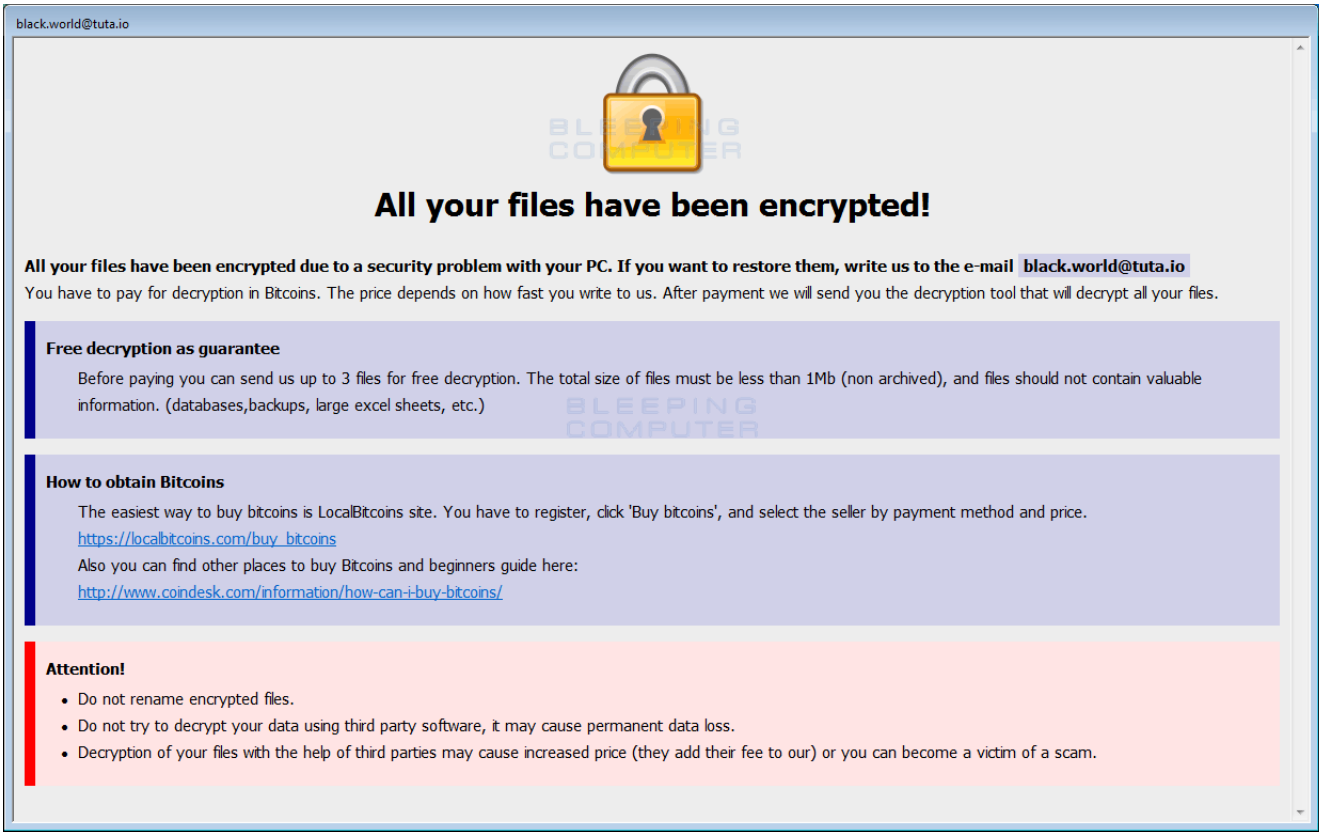
Unfortunately, at this time there is no way to decrypt files encrypted by the Nuclear BTCware Ransomware variant for free. If you wish to discuss this ransomware or receive any support, you can use our dedicated Btcware Ransomware Support Topic. In the past, the developers have released the decryption keys for variants that were no longer in distribution. It appears they decided to no longer offer this to their victims. We hope they change their mind.

Update 8/30/17:

Michael Gillespie discovered that the developers of this variant messed up on the encryption of files greater than 10MB in file size and will not be able to decrypt them. It was also discovered that this same behavior was seen with other files of random sizes. Therefore, it is advised that you do not pay the ransom as there is a good chance many of your files not be able to be decrypted.

What's New in the Nuclear Ransomware BTCWare 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 **HELP.hta**. This ransom note contains instructions to contact **black.world@tuta.io** for payment information as shown below.



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 black.world@tuta.io
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 3 files for free decryption. The total size of files must be less than 1Mb (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/

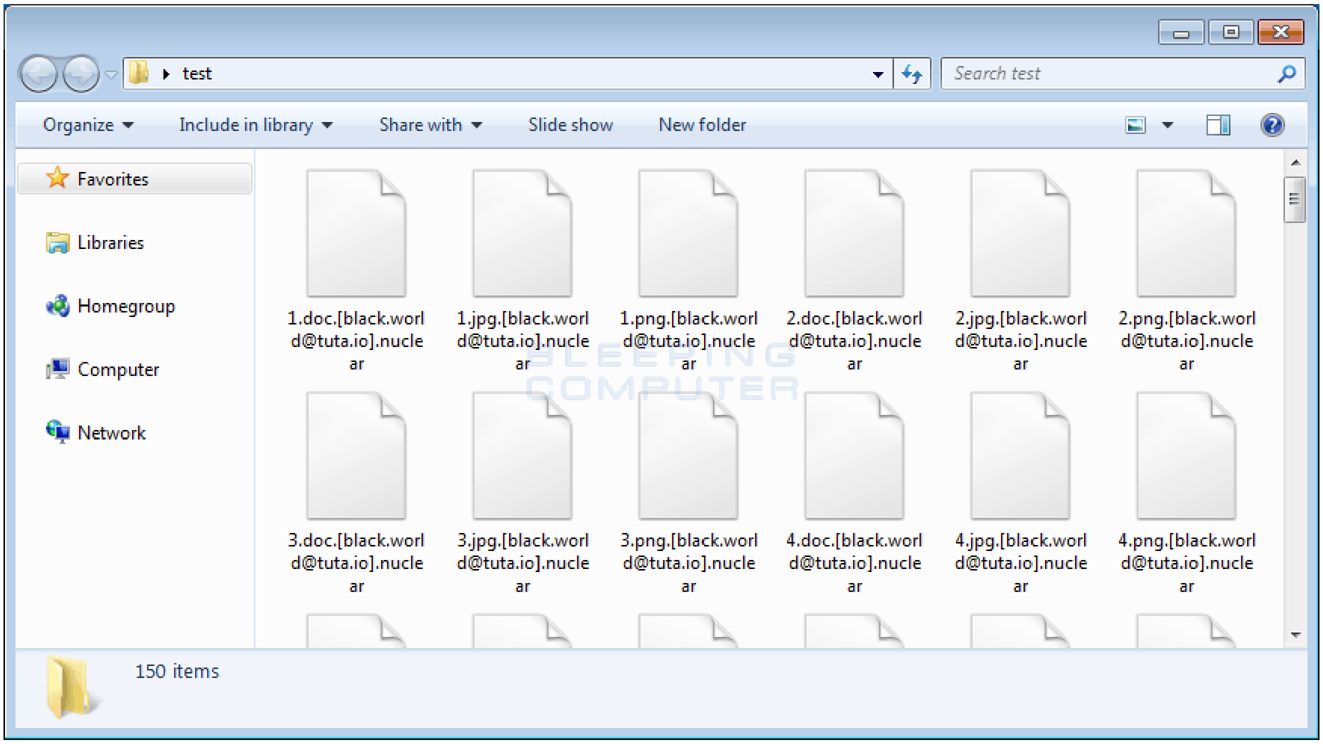
Attention!

- 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.

Nuclear Ransomware (BTCWare) 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 **.[affiliate_email].nuclear** extension to encrypted file's name. For example, the current version will encrypt a file called **test.jpg** and rename it to **test.jpg.[black.world@tuta.io].nuclear**.

You can see an example of an encrypted folder below.



1.doc.[blackworld@tuta.io].nuclear
1.jpg.[blackworld@tuta.io].nuclear
1.png.[blackworld@tuta.io].nuclear
2.doc.[blackworld@tuta.io].nuclear
2.jpg.[blackworld@tuta.io].nuclear
2.png.[blackworld@tuta.io].nuclear
3.doc.[blackworld@tuta.io].nuclear
3.jpg.[blackworld@tuta.io].nuclear
3.png.[blackworld@tuta.io].nuclear
4.doc.[blackworld@tuta.io].nuclear
4.jpg.[blackworld@tuta.io].nuclear
4.png.[blackworld@tuta.io].nuclear

Folder of Encrypted nuclear Files

This variant also uses a different public RSA encryption key that is used to encrypt the victim's AES encryption key. This public encryption key is:

```
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDMwl0XpgillW5xCvuTbug+U+bVtZTaS0SRM+gNgaegG9PwsL

-----END PUBLIC KEY-----
```

If any new information or methods to decrypt the files becomes available, we will be sure to update this article.

Related Articles:

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

SpiceJet airline passengers stranded after 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

IOCs

File Hashes:

```
SHA256: d5397a05b745f64ab16ff921fb4571e9072b54437080bc9630047465e6b06a41
```

Filenames associated with the Nuclear Ransomware Variant:

```
Help.hta
```

Nuclear BTCWare Ransomware Ransom Note Text:

```
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 black.world@tuta.io
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 3 files for free decryption. The total size of
files must be less than 1Mb (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.
```

Emails Associated with the Nuclear Ransomware:

```
black.world@tuta.io
```

Bundled Public RSA-1024 Keys:

```
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDMwl0XpgillW5xCvuTbug+U+bVtZTaS0SRM+gNgaegG9PwsL

-----END PUBLIC KEY-----
```

- BTCWare
- Nuclear
- 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

- jmuniz - 4 years ago

  I got hit with Nuclear this week and after negotiating a price from $2000 to $500, the decryptor did not do all files, specially SQL Server files. It rendered my server useless. I look forward to your findings on this particular ransomeware.

-

  mastergka - 4 years ago

  Any Chance of Uploading the Decrypter for Testing?

-

  jarred1990 - 4 years ago

  I do not know about you, but I came across the same virus just the mail averia@tuta.io so the guys rebuilt everything without problems.

-

  TechInAFlash - 4 years ago

  I paid for the decrypter as well. It did not decrypt everything. It didn't even touch my external hard drive despite saying all drives had been decrypted.

  Here is the copy of the file provided for decrypting..

  https://www.dropbox.com/s/cvi2turvrywwdz8/btcw.zip?dl=0

  If anyone can find a way to force it to decrypt specific files, it does show the private key as well.

-

  Demonslay335 - 4 years ago

  You can use my BTCWareDecrypter with the key they gave you, it lets you specify a directory.

-

  dottormarc - 4 years ago

  Probably we found a way to recover files with extension [decr@cock.li].nuclear but we need additional files to do our tests.
  If anyone has the same problem could send some files to nuclear_decr@dottormarc.it?

-

  mastergka - 4 years ago

  Hi, our files are encrypt with the extension [kod.zapuska@tuta.io].nuclear . if you want to test i can send you some files.

  The File from TechInAFlash (ThX you) doesn't work for us.
  I have recovery the Payload.exe. if anybody need it for research i can upload this.

-

  Demonslay335 - 4 years ago

  As a note, this message was made with a false assumption about the malware's behaviour. I've confirmed there is no way to decrypt for a certain email variant or.anything like that.

-

  miba - 4 years ago

  Hello, here is link to my files. One file is original .pst Outlook file and the second one is encrypted with .nuclear, but content must be the same. Please test and compare this files if you find the key.
  https://www.dropbox.com/s/oto5448sczcflk1/Reansomware_decrypt.7z?dl=0

-

  mgiammarco - 4 years ago

  Hello,
  a customer of mine got it too. It is the goldwave@india.com variant. What can I do? Can I provide some file? Are there any news?

-

  ebernal - 4 years ago

  Hola,
  he sido victima de este ransomware. Alguien sabe de algún descecriptador o alguna solución para recuperar los archivos?.

-

  ebernal - 4 years ago

  Hello,
  I have been a victim of this ransomware. Does anyone know of some descecriptador or some solution to recover the archives ?.

-

  Demonslay335 - 4 years ago

  You may PM me your ransom note and an encrypted file, and I'll see if I am able to help.

-

  ebernal - 4 years ago

  Hello!! in the link below load two files one is the original and the other is encrypted by the virus. The note of rescue nope I have it only because its files have been encrypted and that contact to the mail helperss@protonmail.com. The id is in the name of the encrypted file

  https://drive.google.com/file/d/1XCnXMmrsH5wZlZQMaRXwA7D_Y8YuieWb/view?usp=sharing

-

  Demonslay335 - 4 years ago

  Your files were encrypted by CrySiS/Dharma, which is not decryptable without paying the criminals.

-
  ebernal - 4 years ago

  So, to date, there is no software to decrypt the files?

-

  Demonslay335 - 4 years ago

  Not without paying the criminals as I just said. And do not expose RDP to the internet, put it behind VPN.

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: