New Nuclear BTCWare Ransomware Released (Updated)

By Lawrence Abrams

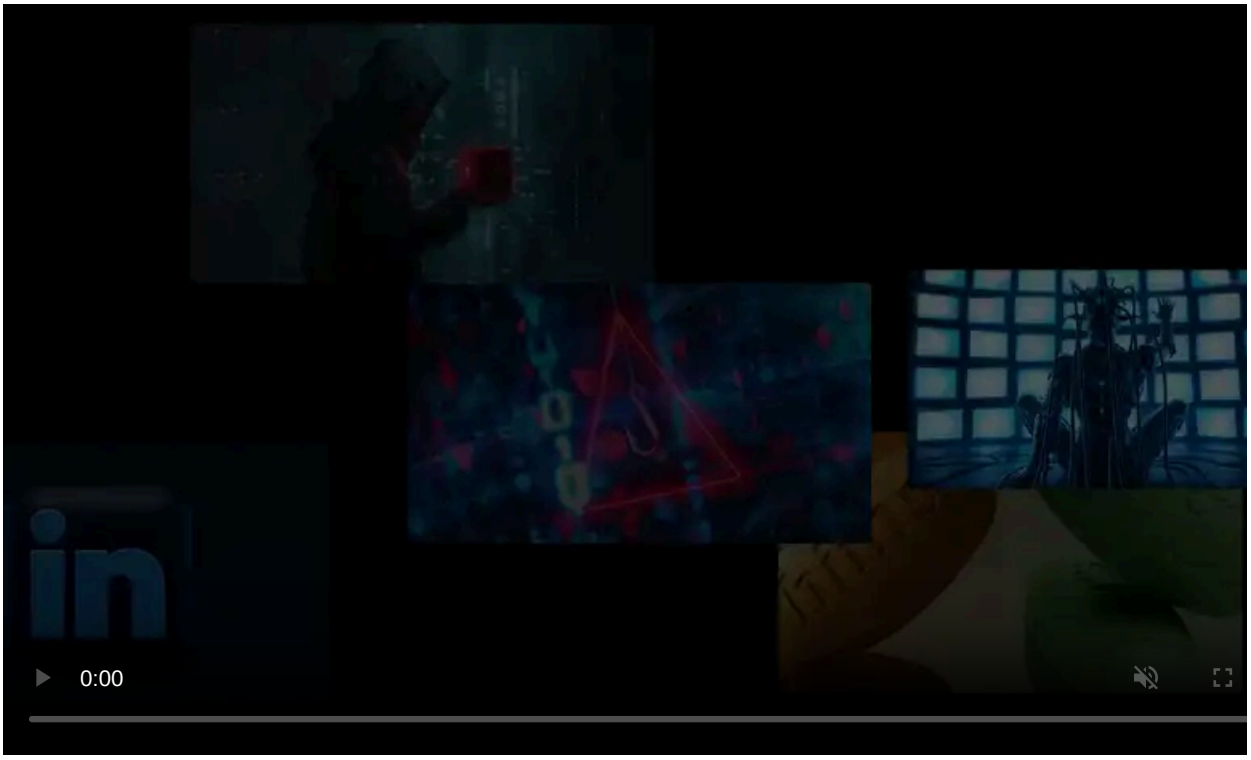
Published: 2017-08-28 · Archived: 2026-04-05 17:18:07 UTC

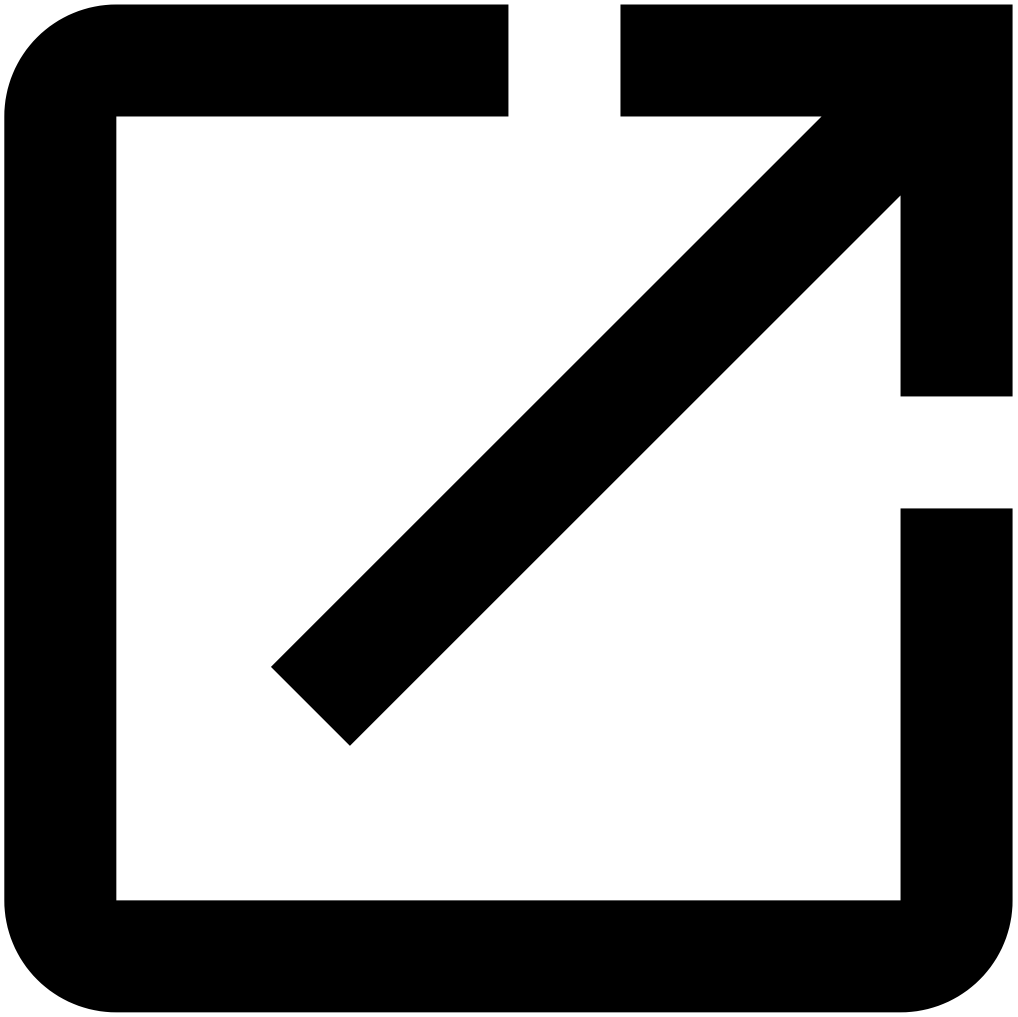
A new variant of the BTCWare ransomware was discovered by ID-Ransomware's Michael Gillespie that appends the **.[affiliate_email].nuclear** extension to encrypted files. The BTCWare family of ransomware is distributed by the developers hacking into remote computers with weak passwords using Remote Desktop 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.


0:00



Visit Advertiser websiteGO TO PAGE

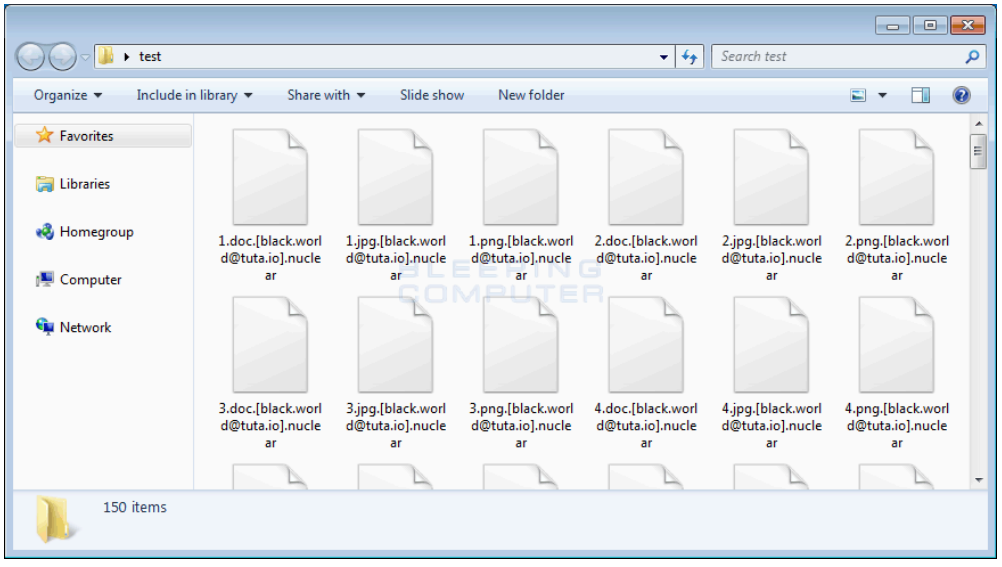
What's New in the Nuclear Ransomware BTCWare Variant

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.

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.



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+gNgaegG9PwsUXsxaqOLBg1zBxUxPcsJvUcQ/SKYWNsA49SIa
-----END PUBLIC KEY-----
```

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

IOCs

File Hashes:

```
SHA256: d5397a05b745f64ab16ff921fb4571e9072b54437080bc9630047465e6b06a41
```

Filenames associated with the Nuclear Ransomware Variant:

```
Help.hta
```

Nuclear BTCWare Ransomware Ransom Note Text:

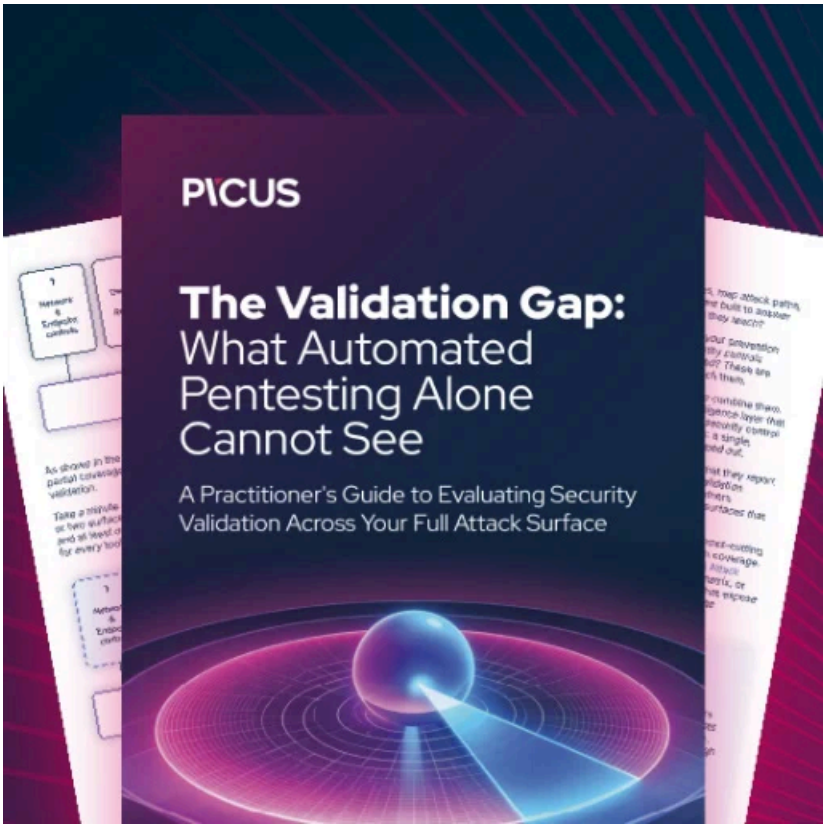
```
 All your files have been encrypted!
All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-
You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you
Free decryption as guarantee
Before paying you can send us up to 3 files for free decryption. The total size of files must be less than 1Mb (non archiv
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
```

Emails Associated with the Nuclear Ransomware:

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

Bundled Public RSA-1024 Keys:

```
 -----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDMwl0XpgillW5xCvuTbug+U+bVtZTaS0SRM+gNgaegG9PwsUXsxaqOLBg1zBxUxPcsJvUcQ/SKYWNsA49SIa
-----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-nuclear-btcware-ransomware-released-updated/