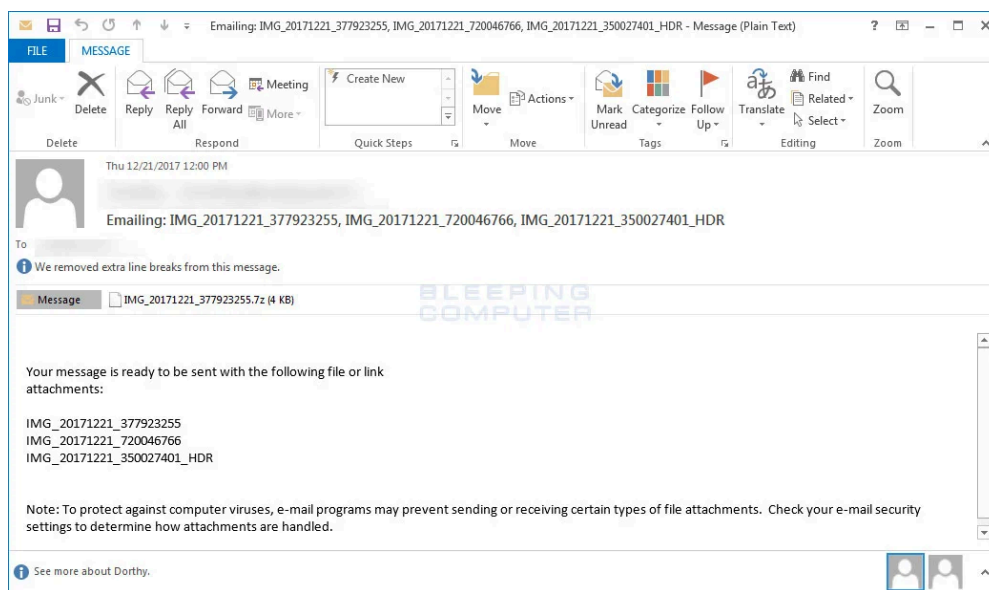


## New .DOC GlobeImposter Ransomware Variant Malspam Campaign Underway

By Lawrence Abrams

Published: 2017-12-22 · Archived: 2026-04-05 16:14:34 UTC

A new malspam campaign is underway that is distributing a GlobeImposter variant that appends the ..doc extension to encrypted files. This malspam is pretending to photos being sent to the recipient and will have a subject line that starts in a similar way to "Emailing: IMG\_20171221\_".

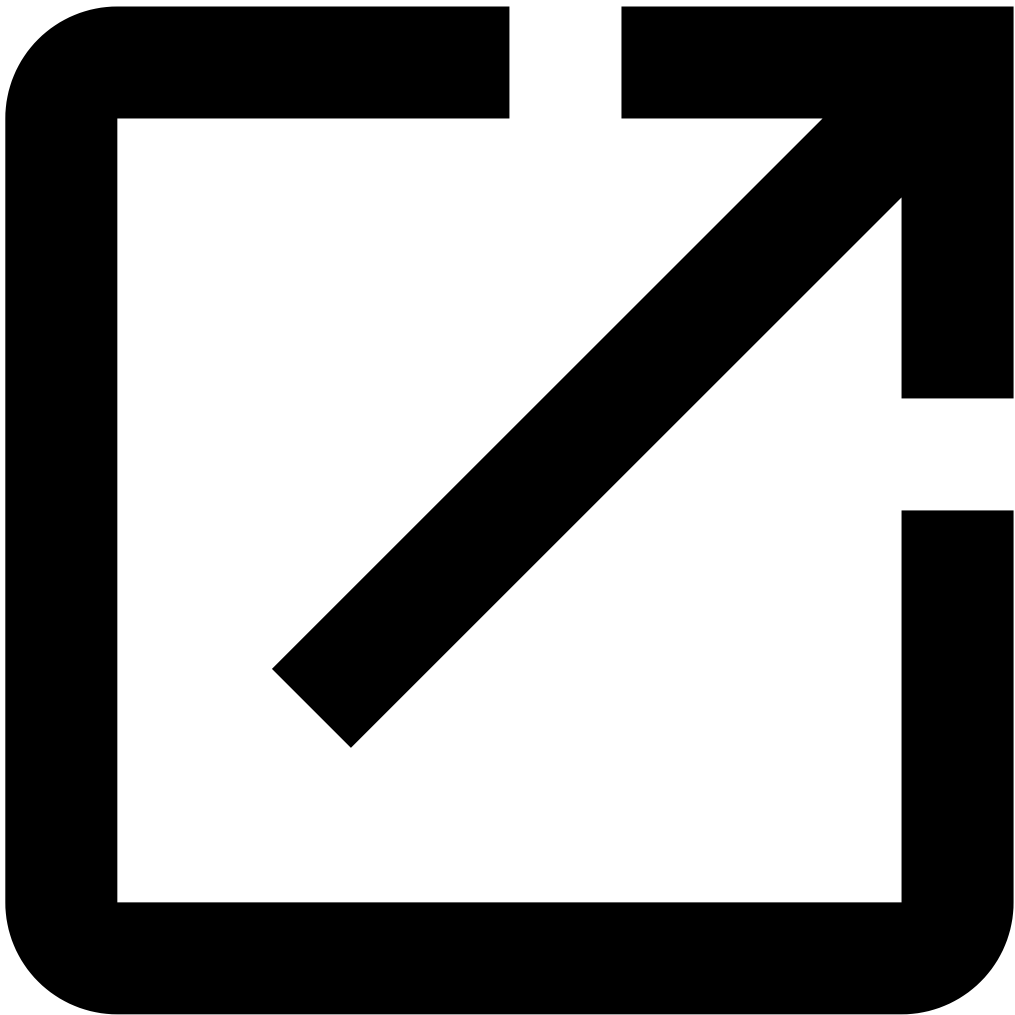
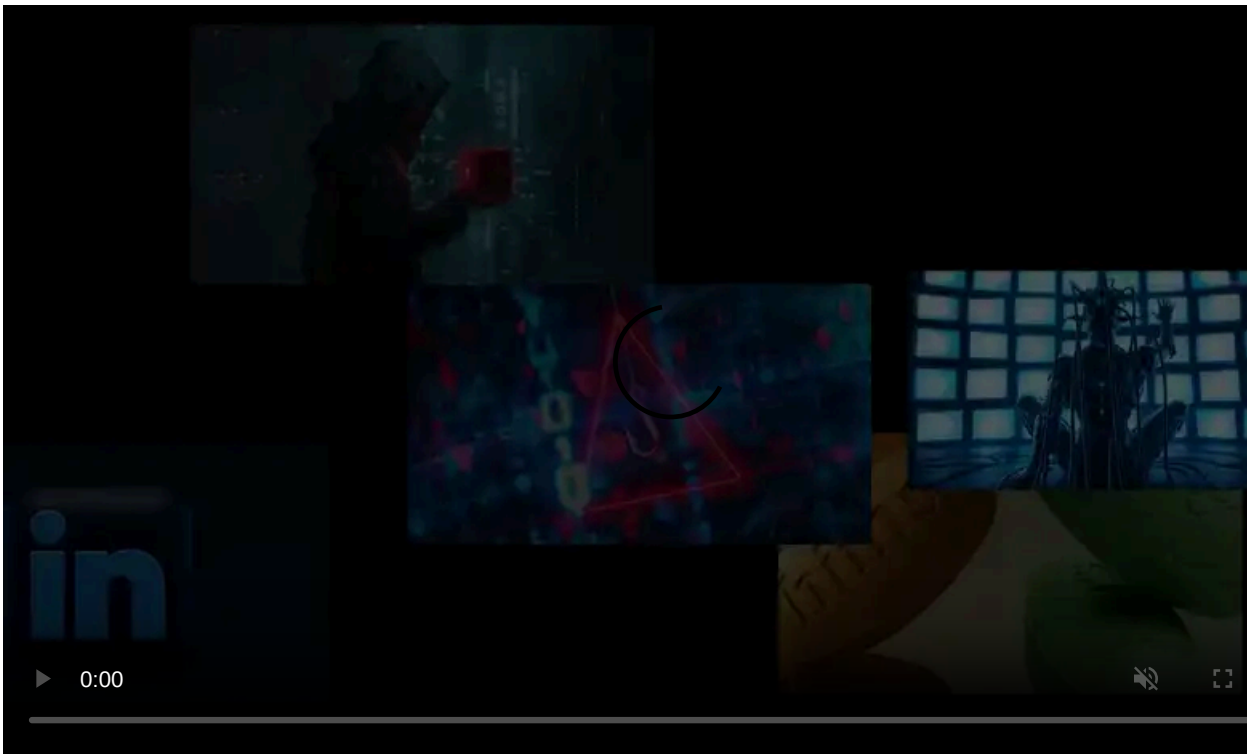


### GlobeImposter Malspam

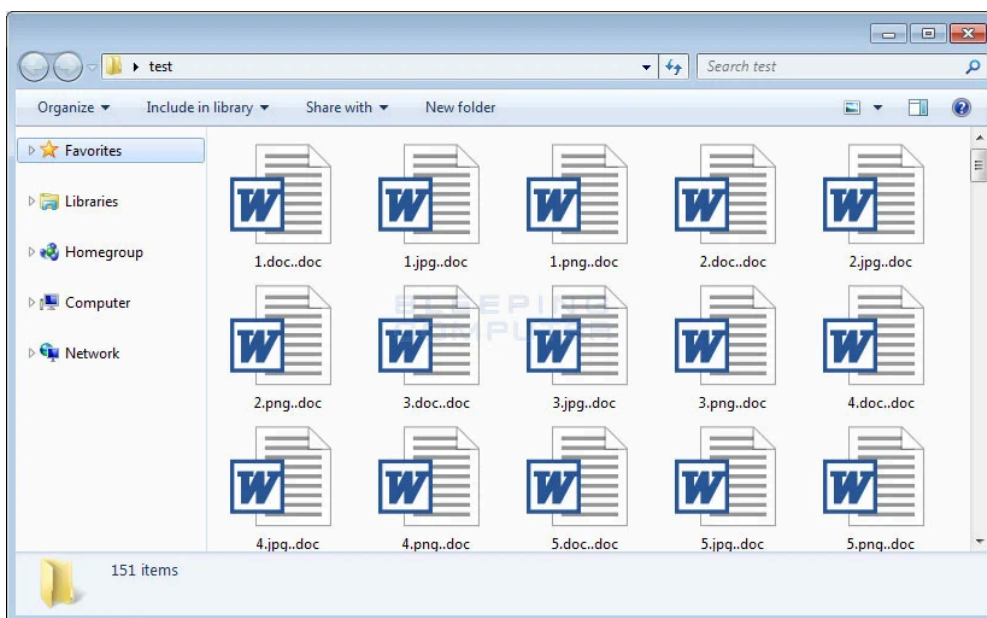
These malspam emails contain 7zip (.7z) archive attachments that are named after a camera photo's filename such as IMG\_[date]\_[number]. These 7z files contain an obfuscated .js file that when double-clicked on will cause the GlobeImposter ransomware to be downloaded from a remote site and executed.

An example of this JS installer can be seen below.



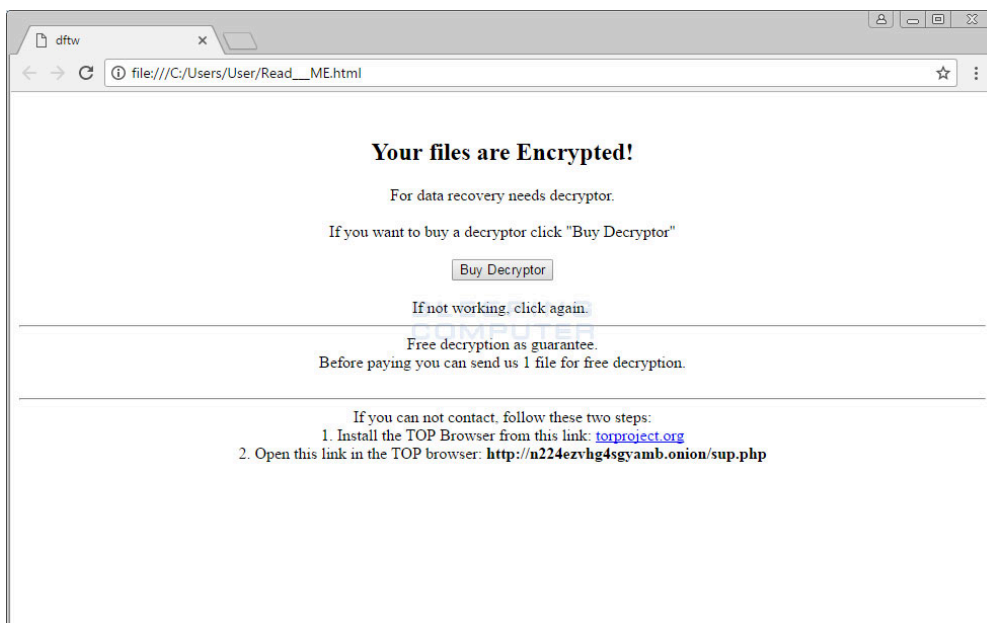


Visit Advertiser website [GO TO PAGE](#)



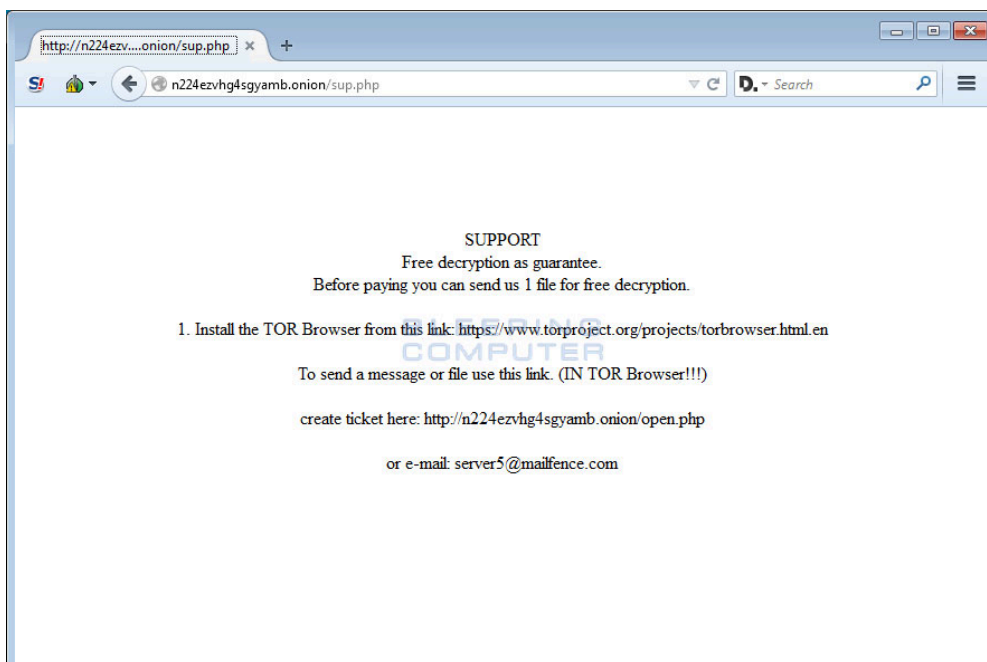
### Encrypted Folder

When GlobeImposter encrypts files it will also create a ransom note named **Read\_\_ME.html** in each folder a file is encrypted.



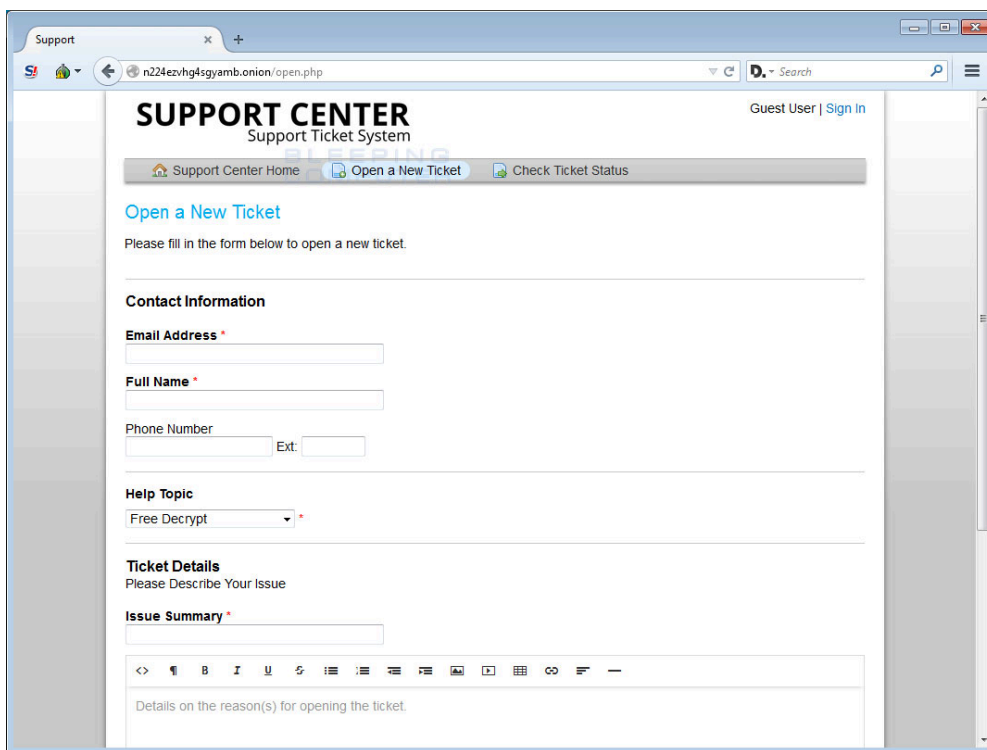
### Ransom Note

This ransom note contains instructions to use Tor to go to the <http://n224ezvhg4sgyamb.onion/sup.php> onion site. This site then tells you to contact them to receive payment instructions and to decrypt one file for free. It also lists the email server5@mailfence.com as a way to contact them.



### Tor Payment Site

It also contains a link to a support site where you can send them a message.



### Tor Support Site

Unfortunately, at this time there is no way to decrypt GlobeImposter files for free. For support or help with this ransomware infection, you can ask in our dedicated [GlobeImposter Ransomware Support](#) topic.

## How to protect yourself from the GlobeImposter Ransomware

In order to protect yourself from the GlobeImposter Ransomware you should use standard security practices. This includes using 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 incorporates behavioral detections to combat ransomware and not just signature detections or heuristics. For example, [Emsisoft Anti-Malware](#) and [Malwarebytes Anti-Malware](#) both contain behavioral detection that can prevent many, if not most, ransomware infections from encrypting a computer.

Last, but not least, make sure you practice the following 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.
- Enable the [showing of file extensions](#).
- If an attachment ends with .js, .vbs, .exe, .scr, or .bat, do not open them for any reason.
- 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 that uses behavioral detections or white list technology. White listing can be a pain to train, but if your willing to stock with it, could have the biggest payoffs.
- Use hard passwords and never reuse the same password at multiple sites.

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

A big thanks to [Eric Taylor](#) of IT-Simplified for pointing out the malspam campaign.

## IOCs

### Doc GlobeImposter Variant Hashes:

```
SHA256: 15e8c986c4602c61a474b51d250e03d5bb178eabc8c5a82a242c1a0fa2227704
```

### Doc GlobeImposter Variant Associated Files:

```
Read__ME.html
```

### Doc GlobeImposter Variant Network Connections:

```
http://n224ezvhg4sgyamb.onion/sup.php
```

### Doc GlobeImposter Variant Email addresses:

```
server5@mailfence.com
```

### Doc GlobeImposter Variant Ransom Note:

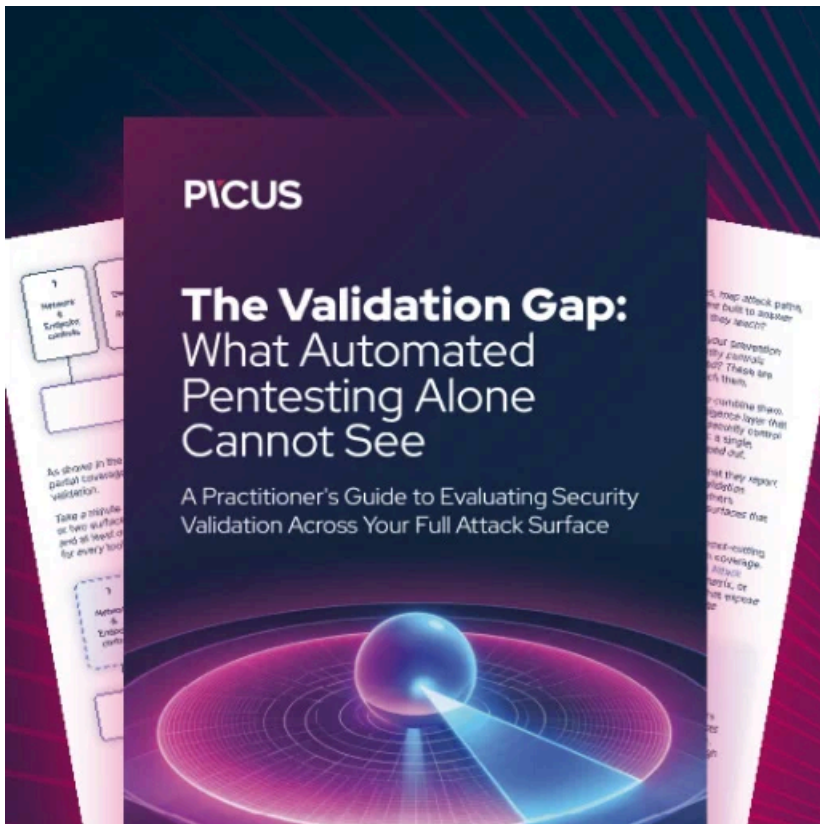
```
Your files are Encrypted!  
  
For data recovery needs decryptor.  
  
If you want to buy a decryptor click "Buy Decryptor"  
  
Buy Decryptor  
  
If not working, click again.
```

Free decryption as guarantee.

Before paying you can send us 1 file for free decryption.

If you can not contact, follow these two steps:

1. Install the TOP Browser from this link: [torproject.org](http://torproject.org)
2. Open this link in the TOP browser: <http://n224ezvhg4sgyamb.onion/sup.php>



### [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-doc-globeimposter-ransomware-variant-malspam-campaign-underway/>