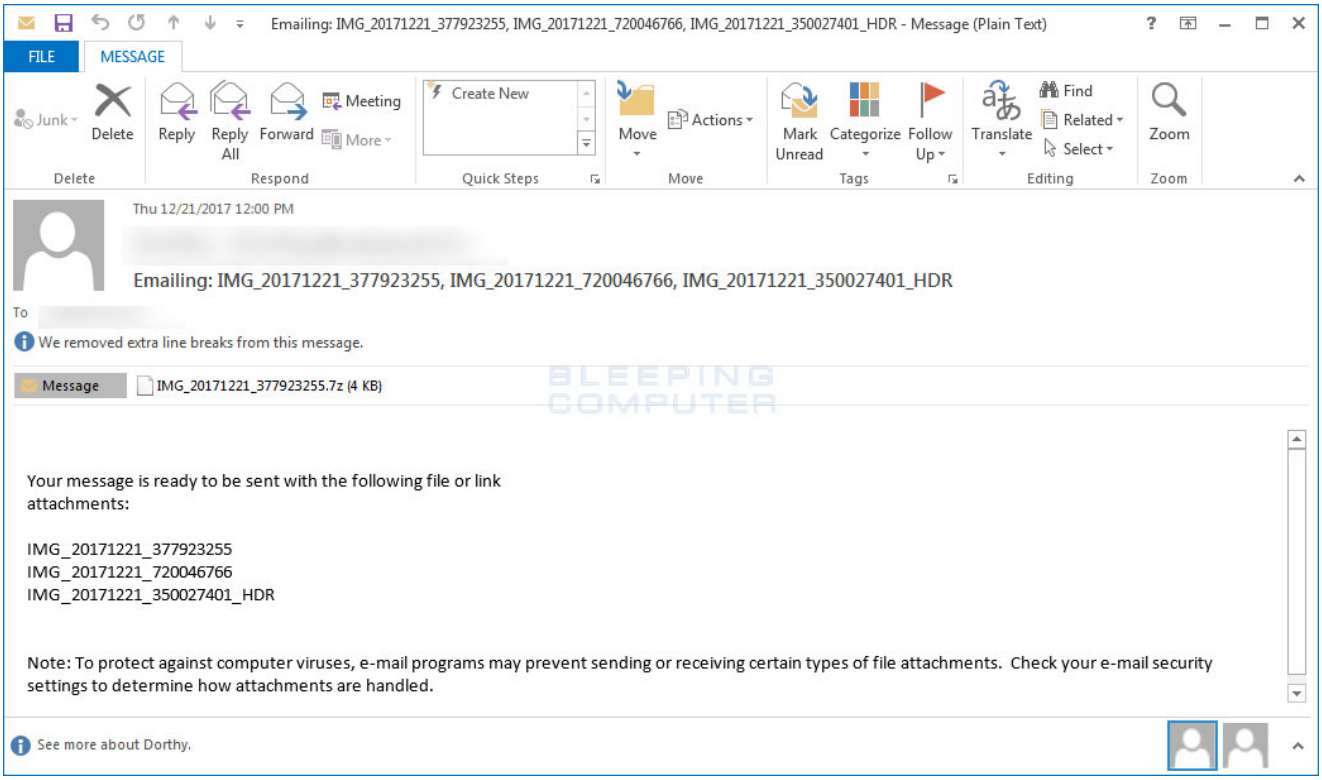
New .DOC GlobeImposter Ransomware Variant Malspam Campaign Underway

bleepingcomputer.com/news/security/new-doc-globeimposter-ransomware-variant-malspam-campaign-underway

By
Lawrence Abrams

- December 22, 2017
- 03:21 PM
- 2

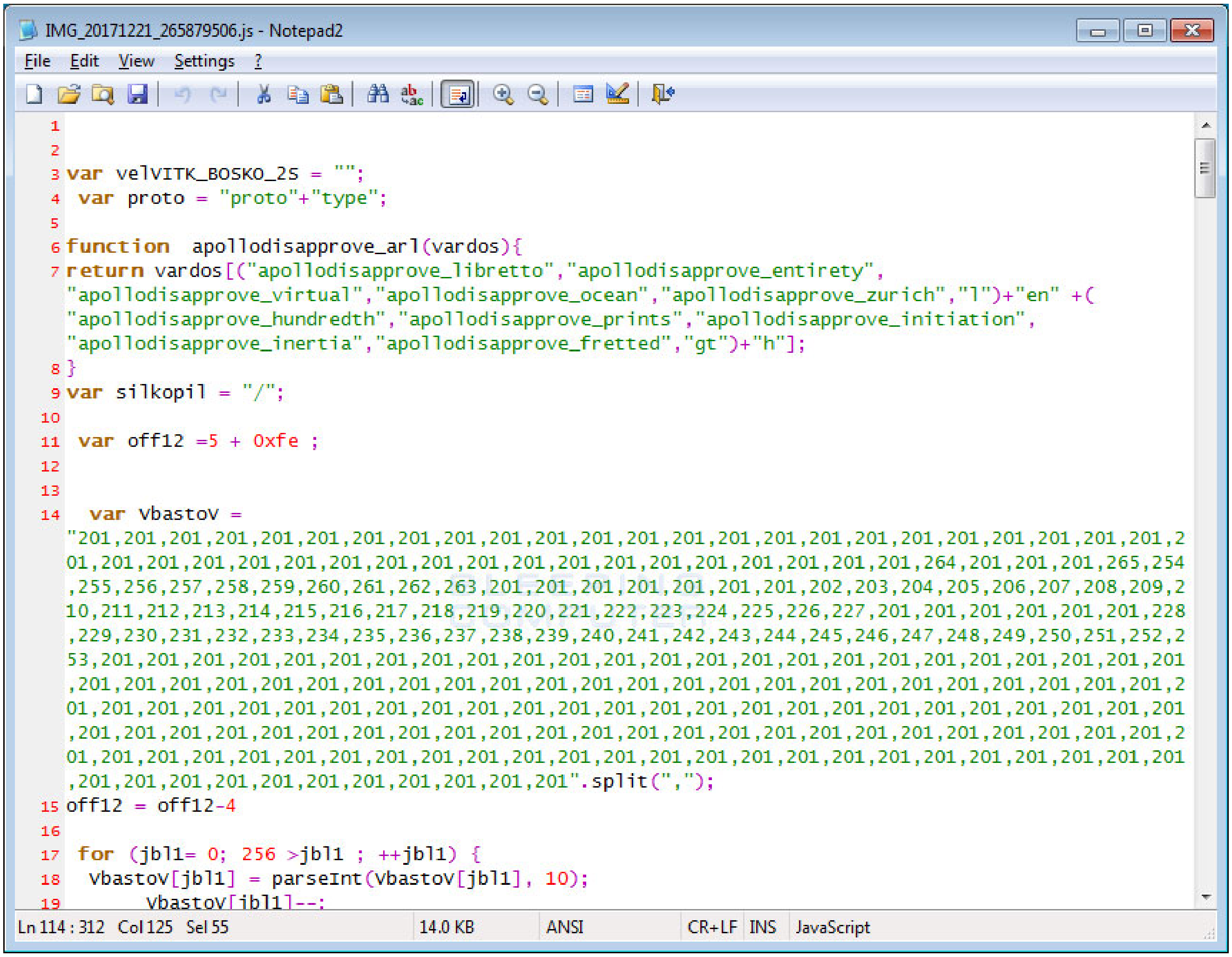
A new malspam campaign is underway that is distributing a GlobeImposter variant that appends the ..doc extension to encrypted files. This malspam is pretending to photos being sent to the recipient and will have a subject line that starts in a similar way to "Emailing: IMG_20171221_".



GlobeImposter MalSpam

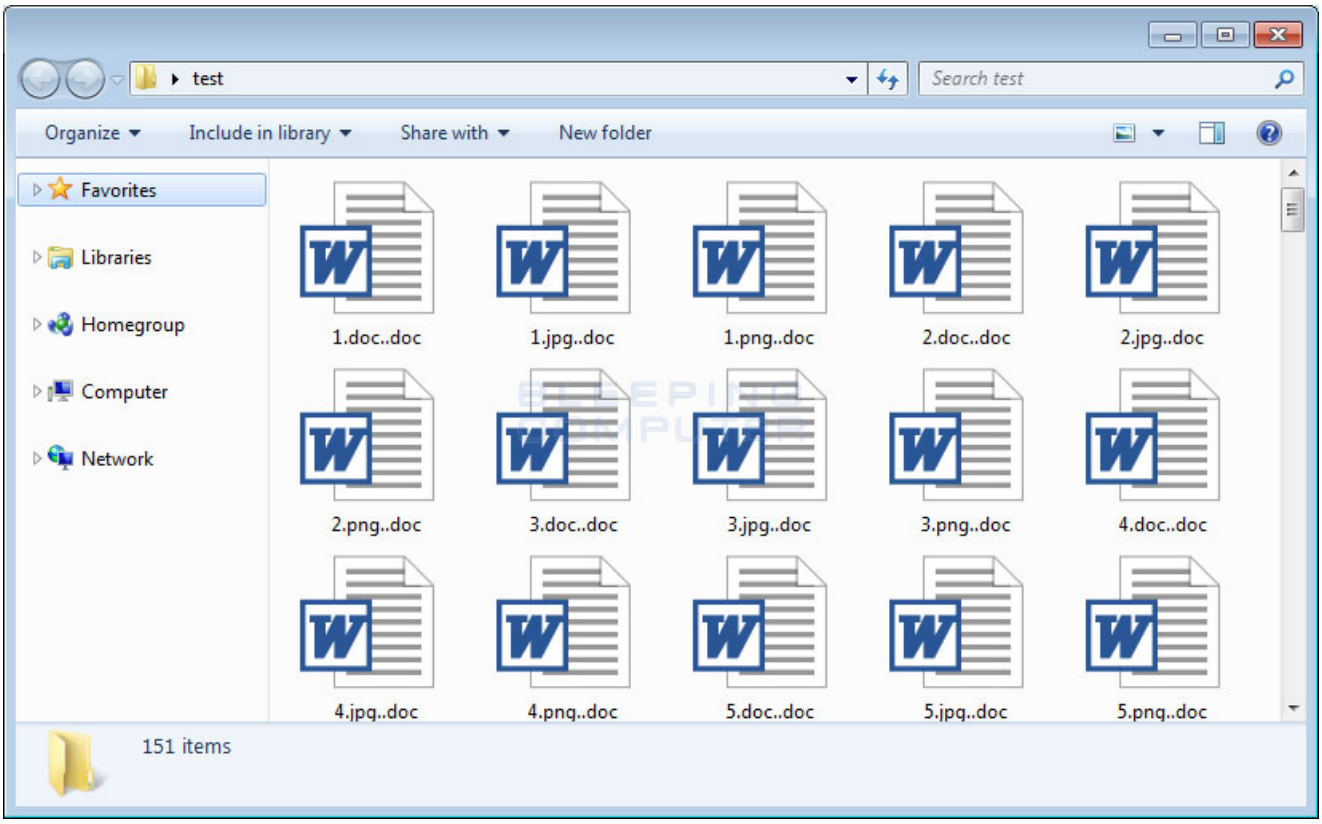
These malspam emails contain7zip (.7z) archive attachments that are named after a camera photo's filename such as IMG_[date]_[number]. These 7z files contain a obfuscated .js file that when double-clicked on will cause the GlobeImposter ransomware to be downloaded from a remote site and executed.

An example of this JS installer can be seen below.



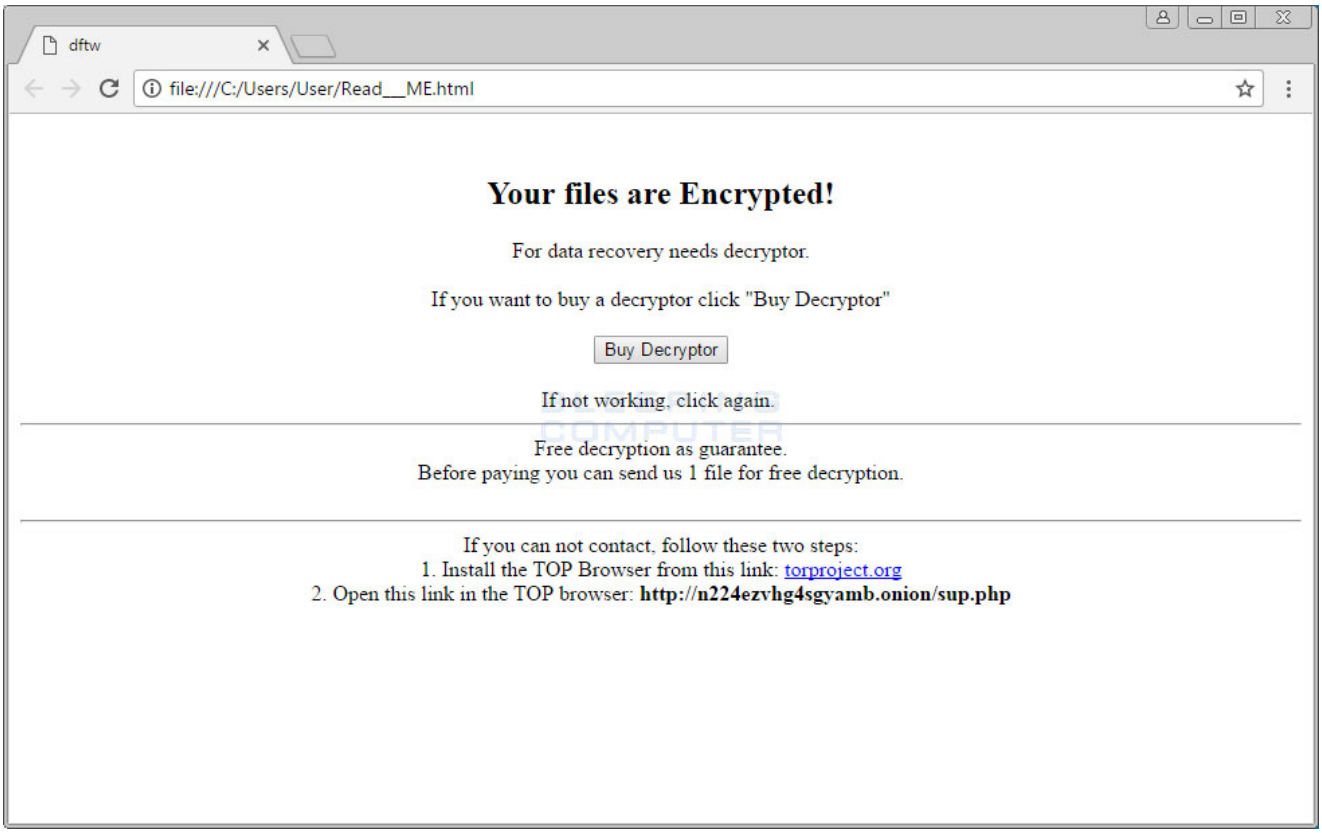
Obfuscated JS Installer

After the executable is downloaded, it will be executed and the GlobeImposter ransomware will begin to encrypt the computer. When encrypting files on the computer it will append the ..**doc** extension to encrypted file's name. For example, a file called **1.doc** would be renamed to **1.doc..doc**.



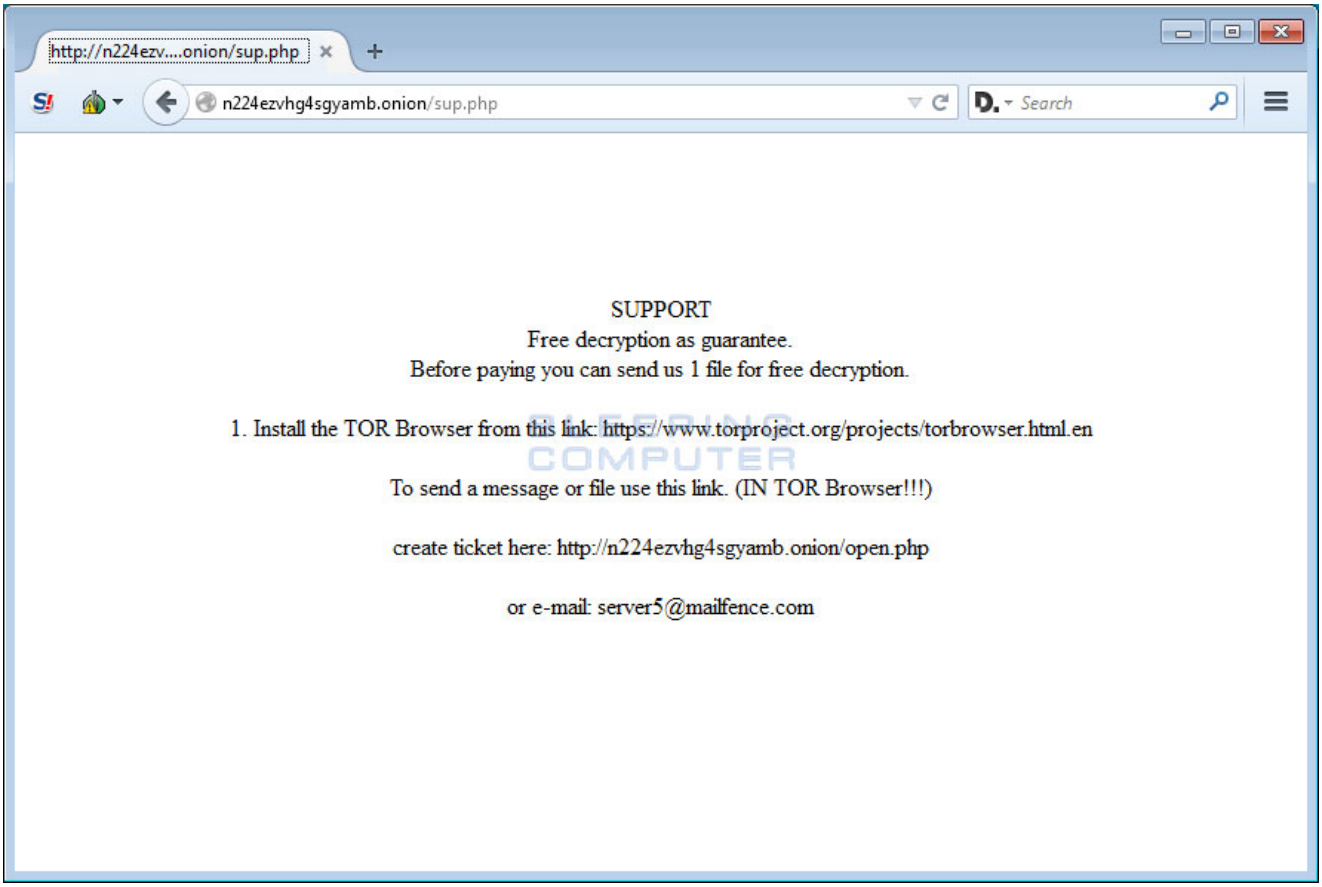
Encrypted Folder

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



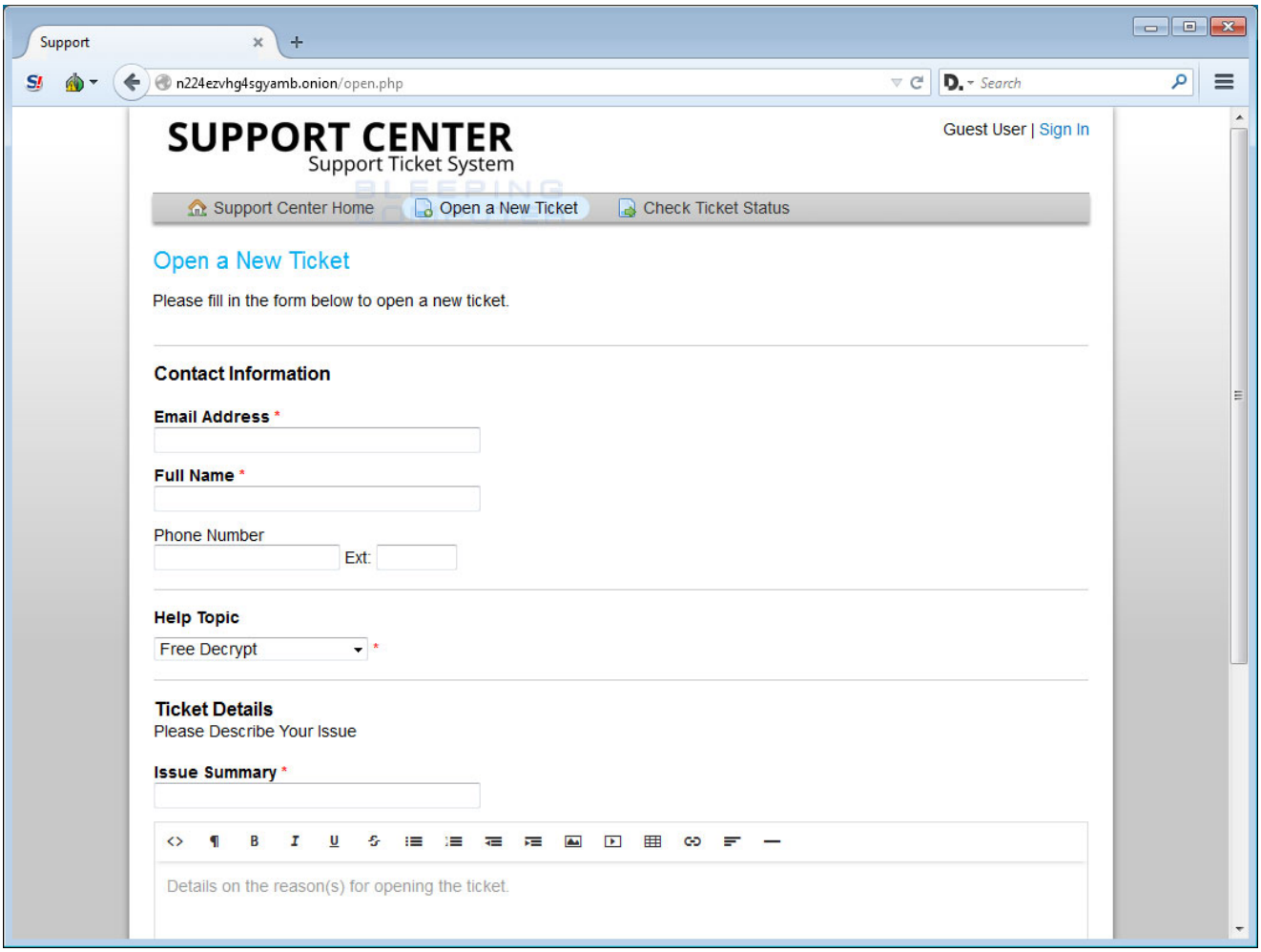
Ransom Note

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.

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

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
2. Open this link in the TOP browser: http://n224ezvhg4sgyamb.onion/sup.php
```

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.