

Bad Sites Botnets CTO Insights Exploits Internet of Everything Mac Malware Mobile Social Spam Targeted Attacks Vulnerabilities

blog.trendmicro.com Sites > TrendLabs Security Intelligence Blog > Malware > TorrentLocker Run Hits Italian Targets

Oct21 **TorrentLocker Run Hits Italian Targets**

7:44 pm (UTC-7) | by Joseph C Chen (Fraud Researcher)

[f Share](#) [f Recommend](#) 26 [t Tweet](#)

We recently observed a new ransomware variant, TorrentLocker, that was targeted at nearly 4,000 organizations and enterprises, many of which are located in Italy. TorrentLocker is similar to an earlier ransomware family ([CryptoLocker](#)), and also encrypts various files and forces users to pay a sum of money. TorrentLocker uses the TOR anonymity network to hide its network traffic, which may have been the origin of its name.

The said threat used spam email written in Italian with several templates as part of its social engineering tactics. Translated into English, these messages read:

1. Your question has been asked on the forum {day}/{month}/{year} {time}. Detailed answer refer to the following address: {malicious link}
2. He sent a bill that would have paid before {day}/{month}/{year}. Details found: {malicious link}
3. Your request has been initiated to revise the payment {malicious link}

**From:** Invoice  
**Date:** [REDACTED]  
**To:** [REDACTED]  
**Subject:** Ordine #791455726.

Ciao

E necessario pagare il debito dal

Informazioni dettagliate:

<http://nsindustrynetwork.ca/Versamento.zip>

Figure 1. Sample spam email

All the messages contain a link that points to .ZIP file. Decompressing the archive file yields a file disguise as .PDF document. PDF files are commonly passed around within organizations, and as such, employees who received this spammed message may be trick into thinking that it is legitimate.

Name


 Versamento.Pdf

Figure 2. Screenshot of the linked archive file

Some of the archive files have filenames such as *Versamento.zip*, *Transazione.zip*, *Compenso.zip*, or *Saldo.zip*. These file names translate to *payment*, *transaction*, *compensation*, and *balance*, respectively. However, instead of a PDF file, these files are actually a CryptoLocker variant detected by Trend Micro as **TROJ\_CRILOCK.YNG**.

Similar to other Cryptolocker variants, it encrypts a wide variety of file types including .DOTX, .DOCX, .DOC, .TXT, .PPT, .PPTX, and .XLSX, among others. All of these file types are associated with Microsoft Office products and are commonly used in enterprises in daily operations.



Search our blog:

## Shellshock



- » What Is Shellshock and How It Affects You
- » Malware Used to Exploit It
- » Attack Scenarios Using ShellShock
- » Real-World Attacks
- » Analysis of Shellshock Exploit C&Cs
- » Analysis of Active Shellshock Exploit Bot
- » More Shellshock Attack Attempts

## Targeted Attacks



- » Four Steps To An Effective Targeted Attack Response
- » Predator Pain and Limitless: Behind the Fraud
- » 2015 Predictions: The Invisible Becomes Visible

Bookmark the [Threat Intelligence Resources](#) site to stay updated on valuable information you can use in your APT defense strategy

## Popular Posts

- » A Killer Combo: Critical Vulnerability and 'Godmode' Exploitation on CVE-2014-6332
- » Root Cause Analysis of CVE-2014-1772 – An Internet Explorer Use After Free Vulnerability
- » November Patch Tuesday: Microsoft Rolls Out 14 Security Bulletins

## Recent Posts

- » Obfuscated Flash Files Make Their Mark in Exploit Kits

In order to receive the decryptor tool to supposedly retrieve crucial files of users, they need to pay the ransom in Bitcoins. One of the samples we found asked for a ransom of 1.375 BTC, which is worth around \$500, a type of digital currency.

## WARNING

### We have encrypted your files with CryptoLocker virus

Your important files (including those on the network disk(s), USB, etc): photos, videos, documents etc. were encrypted with CryptoLocker virus. The only way to get your files back is to buy our decryption software.

**Caution:** Removing of CryptoLocker will not restore access to your encrypted files. The only way to save your files is to buy a decryption software. Otherwise, your files will be lost.

[Click here to buy decryption software](#)

Our website should also be accessible from one of these links:

[http://](#)  
[http://](#)  
[http://](#)  
[http://](#)

#### Frequently Asked Questions

**[+] What happened to my files ?**  
Understanding the issue

**[+] How can I get my files back ?**  
The only way to restore your files

**[+] What should I do next ?**  
Buy decryption software

**[+] I can not access to your website, what should I do ?**  
Accessing website using mirrors

- » Hacking RFID Payment Cards Made Possible with Android App
- » The Other Side of Masque Attacks: Data Encryption Not Found in iOS Apps

#### Calendar

November 2014						
S	M	T	W	T	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						
« Oct						

#### About us



CryptoLocker decryption software
Buy Decryption Software
Decrypt Single File free
FAQ
Support

### Buy decryption software and get all your files back

Buy decryption software for 500 USD before **2014-10-22 5:44:46 PM**  
OR buy it later with the price of **1000 USD**  
Time left before price increase: **71 h. 3 m. 56 s.**

Current price: 1.375 BTC (around 500 USD)  
Paid until now: 0 BTC (around 0 USD)  
Remaining amount: 1.375 BTC (around 500 USD)

[BUY IT NOW ! 100% files back guaranteed](#)

#### Buy Decryption Software with bitcoin

- 1 **Register bitcoin wallet**  
You should register Bitcoin wallet, [see easy instructions](#) or [watch video](#) on YouTube
- 2 **Buy bitcoins**  
Please see recommended bitcoin sellers in your country  
[howtobuybitcoins.info](#) - List of places to buy bitcoins in your country.  
[localbitcoins.com](#) - Buy bitcoin. Fast, easy and safe. Near you.  
[www.happycoins.com](#) - European Bitcoin exchange with instant payment methods like Sofort, IDEAL, MisterCash.  
[dsagents.eu](#) - You can get your first Bitcoin with Sofort Überweisung, SEPA or Bank wire.  
[www.colnmana.com](#) - CoinMama allows you to buy Bitcoins with your credit card, Western Union, MoneyGram, Perfect Money and more!
- 3 **Send bitcoins for decryption software**  
Send 1.375 BTC (around 500 USD) to Bitcoin wallet address:  [Get QR code](#)
- 4 **Verify transaction & receive software**  
View detailed transaction info and write Transaction ID to the field below.  
Once bitcoin payment is made, transaction can be verified after 10-15 minutes.  
 [Where is Transaction ID?](#)

[Verify Transaction](#)

Payment status: Total 0 BTC was received.  
You need to pay more 1.375 BTC to receive decryption software.

Figures 3 and 4. Screenshots of ransomware (Click to enlarge)

Italian users are the most affected by this particular spam run, as just over half of all spam messages identified with this spam run were sent to users in Italy. A quarter came from Brazil, with other countries accounting for the remainder. At its peak, several thousand users were affected per day.

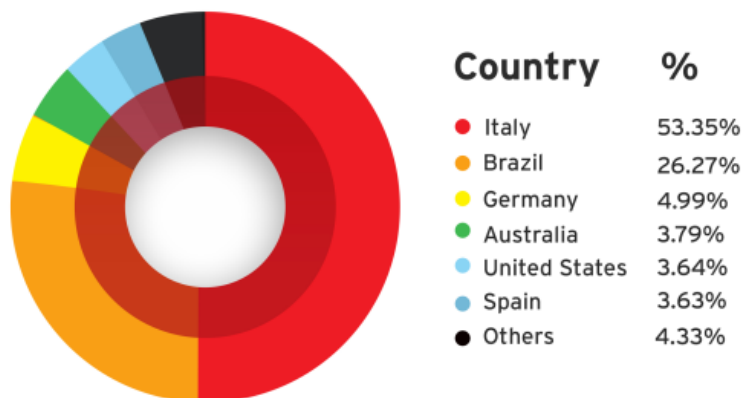


Figure 5. Distribution of TorrentLocker targets globally

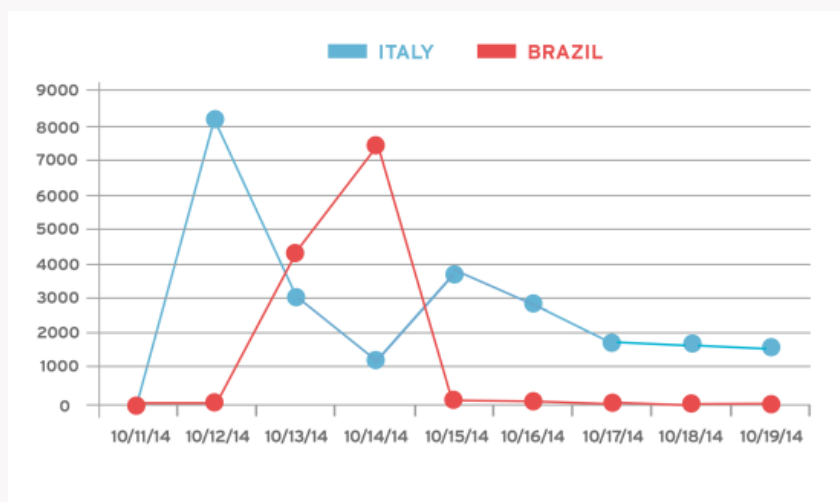


Figure 6. Number of affected targets per day

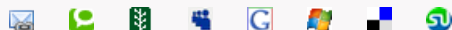
We protect our users against this threat by blocking the different facets of this threat. In addition to blocking the various spam messages, we also block the malicious URLs and detect the malicious files used in this attack.

The hashes of the file seen in this attack include:

- 050b21190591004cbee3a06019dcb34e766afe47
- 078838cb99e31913e661657241feeea9c20b965a
- 6b8ba758c4075e766d2cd928ffb92b2223c644d7
- 9a24a0c7079c569b5740152205f87ad2213a67ed
- c58fe7477c0a639e64bcf1a49df79dee58961a34
- de3c25f2b3577cc192cb33454616d22718d501dc

**Additional information provided by Grant Chen**

Share this article



Get the latest on malware protection from TrendLabs



This entry was posted on Tuesday, October 21st, 2014 at 7:44 pm and is filed under **Malware**, **Spam**. You can [leave a response](#), or [trackback](#) from your own site.











Disqus seems to be taking longer than usual. [Reload?](#)

[Microsoft Windows Hit By New Zero-Day Attack](#)

[Targeted Attacks: Stealing Information Through Google Drive](#)

#### Other Trend Micro blogs

-  [CTO Insights](#)
-  [CounterMeasures Blog](#)
-  [Cloud Security Blog](#)
-  [Consumerization Blog](#)
-  [Fearless Web](#)
-  [Internet Safety for Kids & Families](#)
-  [Simply Security News](#)
-  [Trend Micro Blog \[German\]](#)
-  [TrendLabs Security Blog \[Japan\]](#)
-  [Cloud Security APAC](#)



Do you have a product-related question? [Visit our eSupport website.](#)