(/connect/fr) > Blogs (/connect/fr/blogs) > Security Response (/connect/fr/symantec-blogs/symantec-security-response)

Security Response

(https://twitter.com/threatintel) (http://www.symantec.com/connect/fr/item-feeds/blog/2261/feed/all/en/all)

+5
5 Votes

Symantec Official Blog

Spam offering fake Visa benefits, rewards leads to TeslaCrypt ransomware

Spam campaign baits users with Visa Total Rewards emails containing malware that leads to Trojan.Cryptolocker.N infections.

Par: **Joji Hamada (/connect/fr/user/joji-hamada)** EMPLOYÉ SYMANTEC

Créé 01 Mars 2016

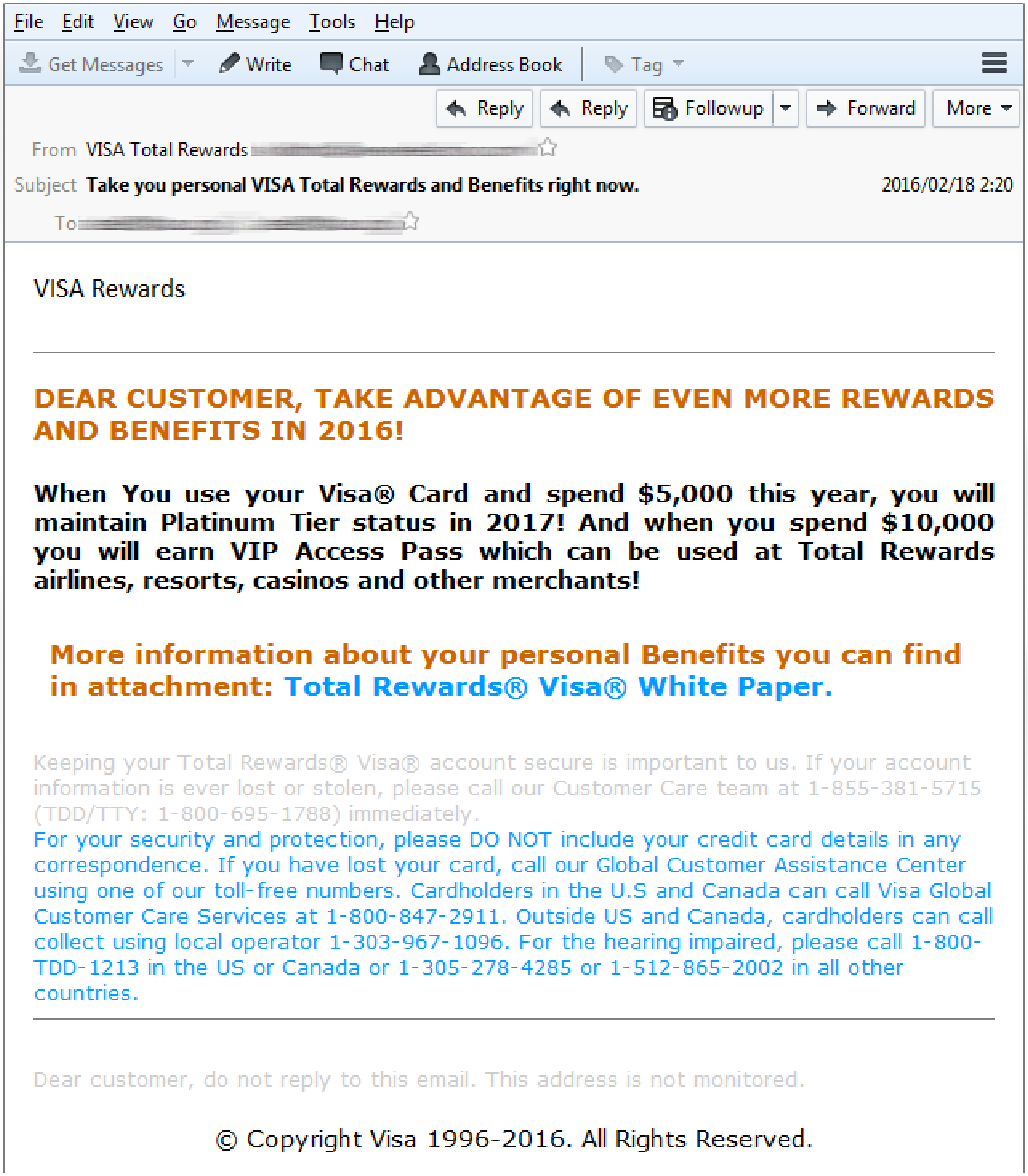
0

Partage

Spam related to credit cards is a typical scam observed on a daily basis. Some attempt to fool recipients into giving up their personal information along with their credit card numbers in the form of phishing attacks, while others attempt to lure victims into various online scams.

On the other hand, credit card-related spam campaigns involving malware are not as commonly seen. Symantec Security Response has, however, recently observed a spam campaign offering fake Visa rewards and benefits as bait to deliver ransomware to recipients’ computers.

The email in this particular campaign purports to come from Visa Total Rewards and provides details about the benefits of using Visa credit cards. Attached to the email is an archive file which poses as a whitepaper containing more information about the supposed rewards and benefits offered by the program. If the recipient opens the attachment, they will see only an obfuscated JavaScript file (detected as JS.Downloader (https://www.symantec.com/security_response/writeup.jsp?docid=2003-102718-1528-99)).



From VISA Total Rewards [redacted]

Subject **Take you personal VISA Total Rewards and Benefits right now.** 2016/02/18 2:20

To [redacted]

VISA Rewards

DEAR CUSTOMER, TAKE ADVANTAGE OF EVEN MORE REWARDS AND BENEFITS IN 2016!

When You use your Visa® Card and spend $5,000 this year, you will maintain Platinum Tier status in 2017! And when you spend $10,000 you will earn VIP Access Pass which can be used at Total Rewards airlines, resorts, casinos and other merchants!

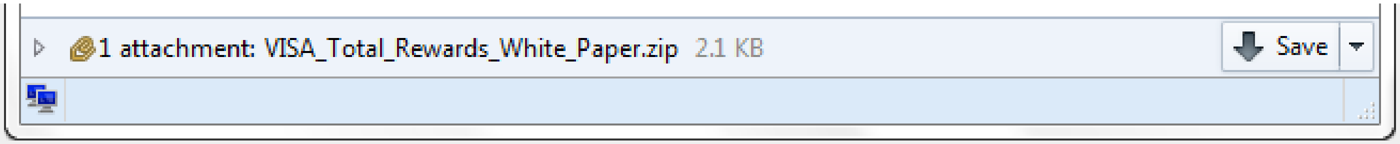
More information about your personal Benefits you can find in attachment: Total Rewards® Visa® White Paper.

Keeping your Total Rewards® Visa® account secure is important to us. If your account information is ever lost or stolen, please call our Customer Care team at 1-855-381-5715 (TDD/TTY: 1-800-695-1788) immediately.

For your security and protection, please DO NOT include your credit card details in any correspondence. If you have lost your card, call our Global Customer Assistance Center using one of our toll-free numbers. Cardholders in the U.S and Canada can call Visa Global Customer Care Services at 1-800-847-2911. Outside US and Canada, cardholders can call collect using local operator 1-303-967-1096. For the hearing impaired, please call 1-800-TDD-1213 in the US or Canada or 1-305-278-4285 or 1-512-865-2002 in all other countries.

Dear customer, do not reply to this email. This address is not monitored.

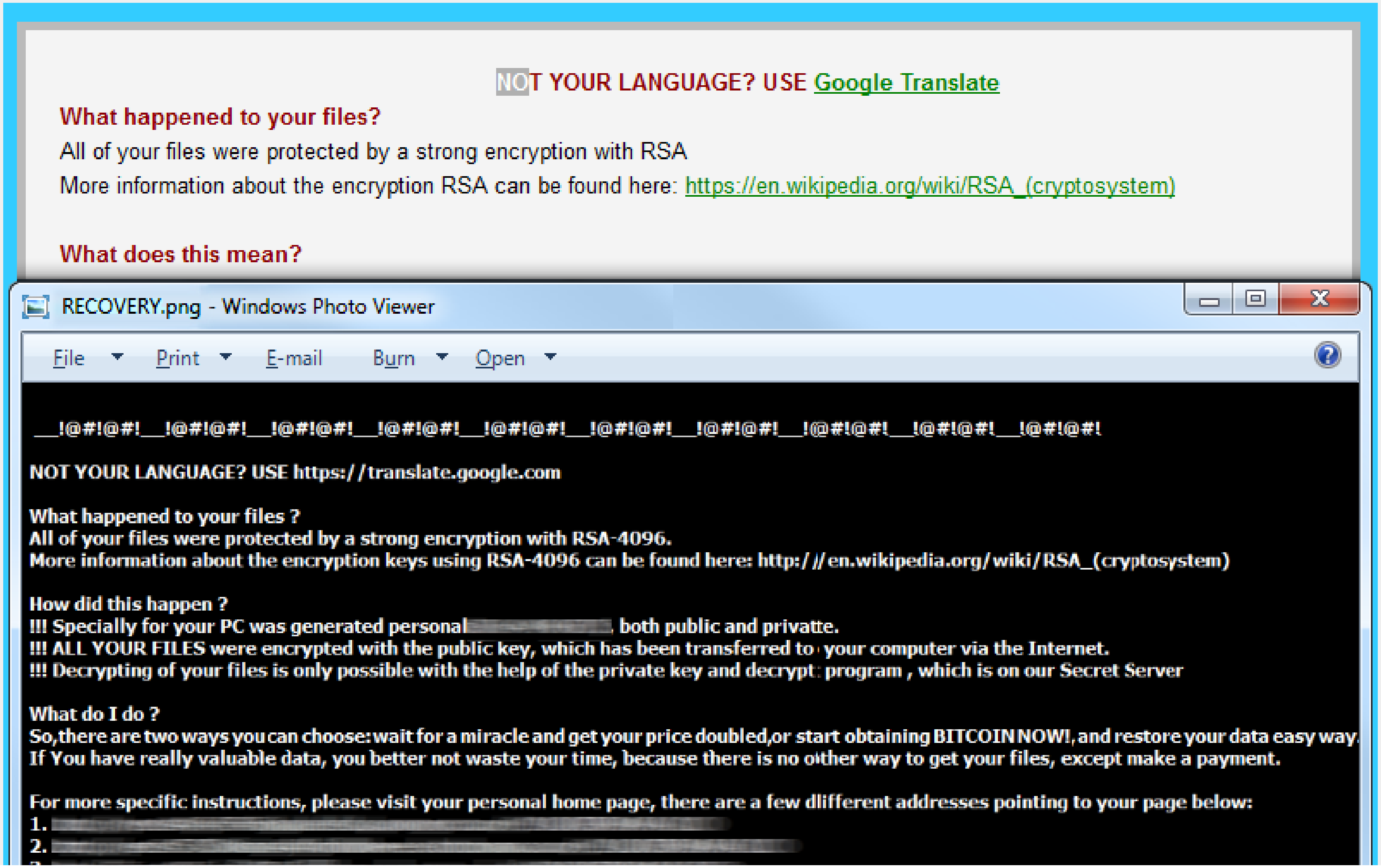
© Copyright Visa 1996-2016. All Rights Reserved.



1 attachment: VISA_Total_Rewards_White_Paper.zip 2.1 KB

Figure 1. Malicious spam contains a fake whitepaper—an archive file containing JS.Downloader

If the recipient is fooled into opening the JavaScript file, the script downloads a variant of the TeslaCrypt ransomware (detected as Trojan.Cryptolocker.N (http://www.symantec.com/security_response/writeup.jsp?docid=2015-030201-5710-99)) from the specified URL and runs it. A few minutes later, a message is displayed stating that all of the user's files have been encrypted and payment in Bitcoin is required to decrypt the files.



NOT YOUR LANGUAGE? USE Google Translate

What happened to your files?

All of your files were protected by a strong encryption with RSA

More information about the encryption RSA can be found here: https://en.wikipedia.org/wiki/RSA_(cryptosystem)

What does this mean?

__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!__!@#!@#!

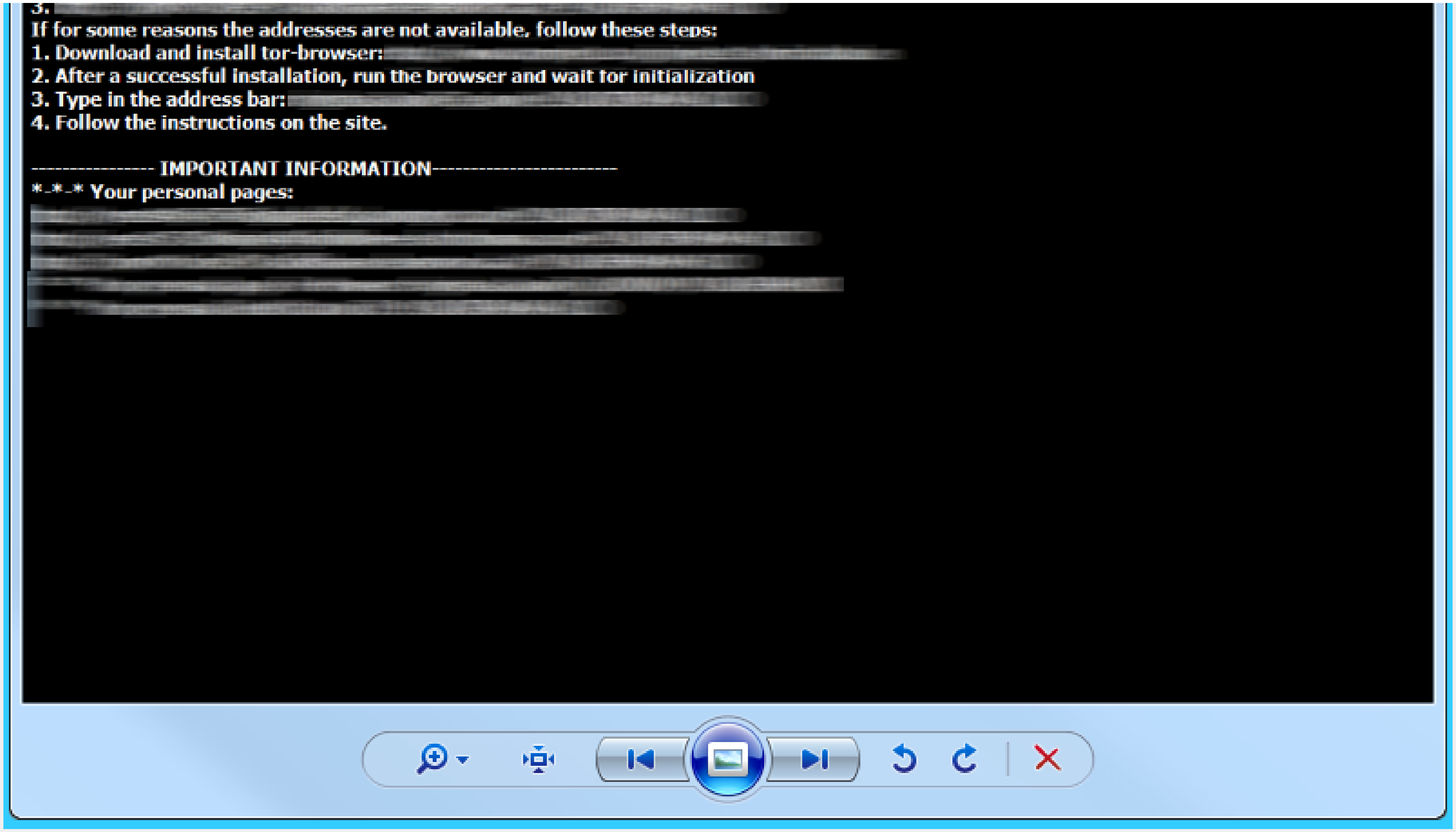
NOT YOUR LANGUAGE? USE https://translate.google.com

What happened to your files ?
All of your files were protected by a strong encryption with RSA-4096.
More information about the encryption keys using RSA-4096 can be found here: http://en.wikipedia.org/wiki/RSA_(cryptosystem)

How did this happen ?
!!! Specially for your PC was generated personal [redacted] both public and privatte.
!!! ALL YOUR FILES were encrypted with the public key, which has been transferred to your computer via the Internet.
!!! Decrypting of your files is only possible with the help of the private key and decrypt program , which is on our Secret Server

What do I do ?
So,there are two ways you can choose: wait for a miracle and get your price doubled,or start obtaining BITCOIN NOW!, and restore your data easy way.
If You have really valuable data, you better not waste your time, because there is no other way to get your files, except make a payment.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:
1. [redacted]
2. [redacted]

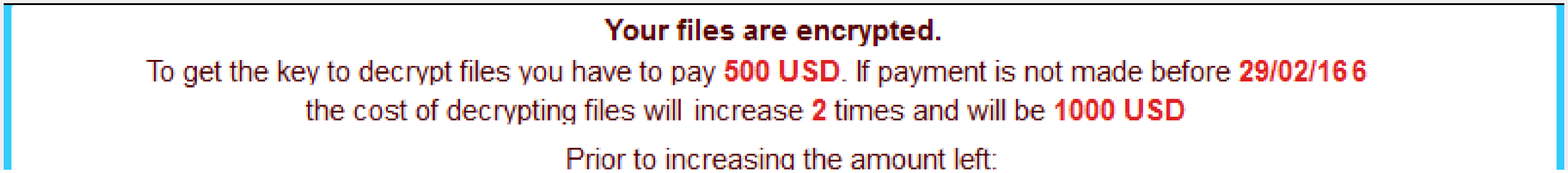


```
3. [redacted]
If for some reasons the addresses are not available, follow these steps:
1. Download and install tor-browser: [redacted]
2. After a successful installation, run the browser and wait for initialization
3. Type in the address bar: [redacted]
4. Follow the instructions on the site.

---------------- IMPORTANT INFORMATION------------------------
*-*-* Your personal pages:
[redacted]
```

Figure 2. JS.Downloader downloads TeslaCrypt ransomware, which informs victims their files have been encrypted

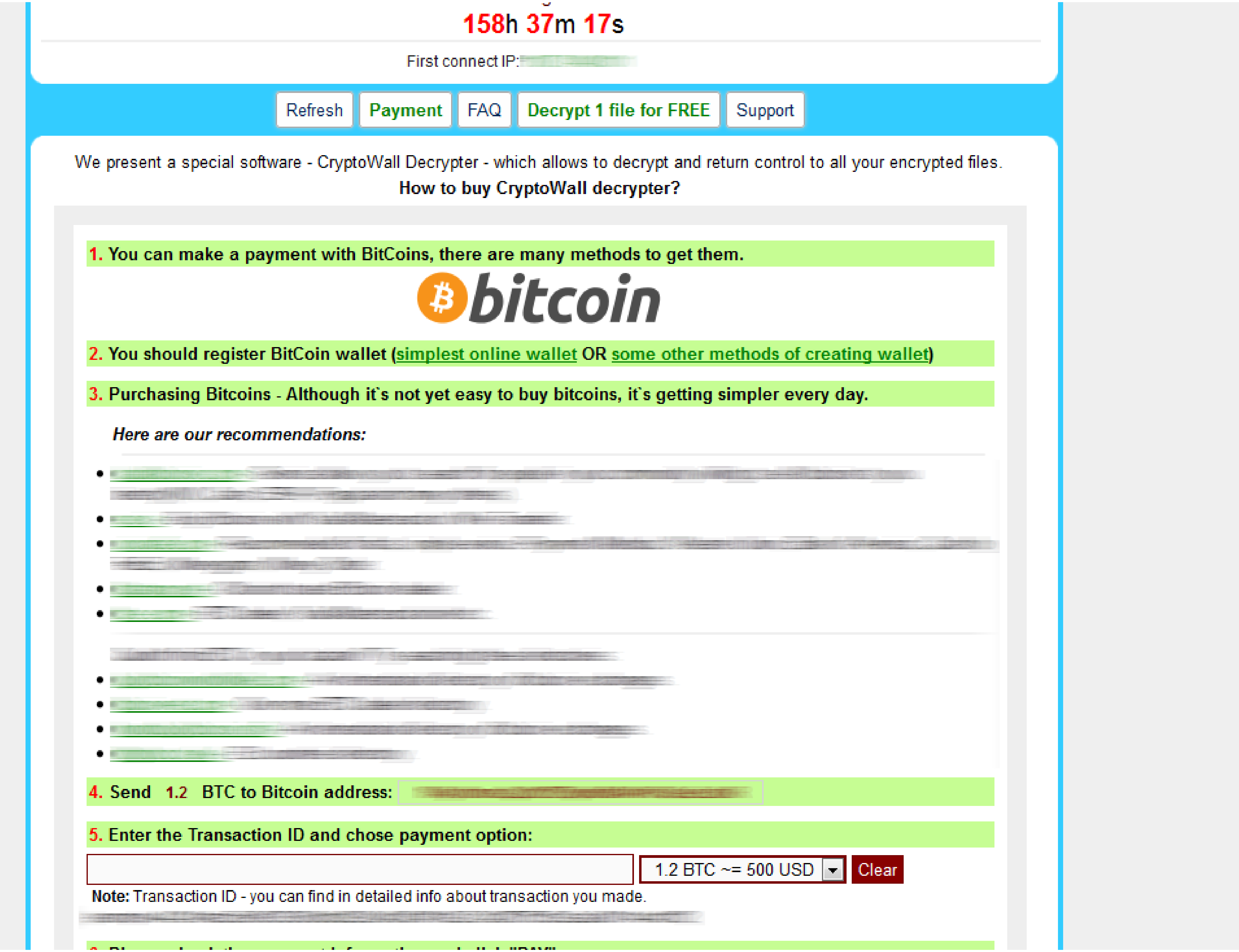
The ransomware provides more information to victims on a personalized home page and demands a payment of US$500 (or 1.2 bitcoins) within 160 hours of infection in order to unlock the encrypted files. If the transaction is not made within the specified time frame, the price doubles to $1,000. This page provides a contact form that offers assistance in case of payment issues or any other problems the victims may run into. There is also an opportunity to decrypt a single file for no fee to prove that the files can be properly decrypted.



Your files are encrypted.

To get the key to decrypt files you have to pay **500 USD**. If payment is not made before **29/02/166**
the cost of decrypting files will increase **2** times and will be **1000 USD**

Prior to increasing the amount left:



158h 37m 17s

First connect IP: [redacted]

We present a special software - CryptoWall Decrypter - which allows to decrypt and return control to all your encrypted files.

How to buy CryptoWall decrypter?

1. You can make a payment with BitCoins, there are many methods to get them.

bitcoin

2. You should register BitCoin wallet (simplest online wallet OR some other methods of creating wallet)

3. Purchasing Bitcoins - Although it`s not yet easy to buy bitcoins, it`s getting simpler every day.

Here are our recommendations:

[redacted]

4. Send 1.2 BTC to Bitcoin address: [redacted]

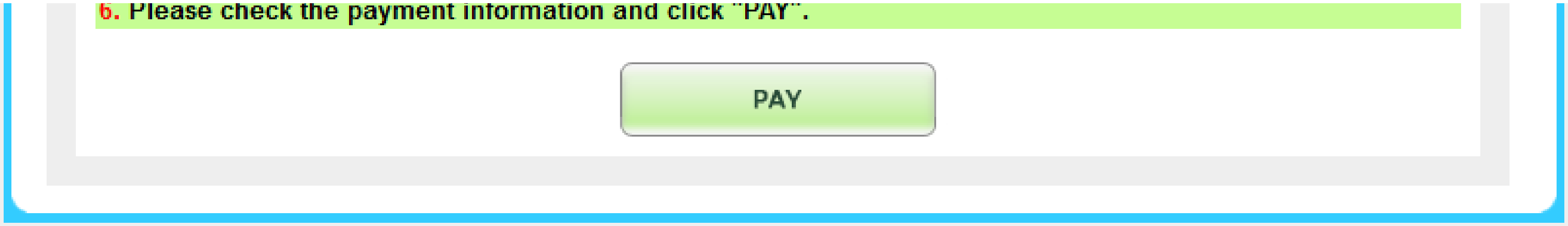
5. Enter the Transaction ID and chose payment option:

1.2 BTC ~= 500 USD

Note: Transaction ID - you can find in detailed info about transaction you made.

[redacted]

6. Please check the payment information and click "PAY".



6. Please check the payment information and click "PAY".

Figure 3. Victims are given 160 hours to pay US$500 (1.2 BTC) to have their files decrypted, after which the demand doubles

The vast majority of the spam is being distributed to English-speaking countries, with the UK (40 percent) and the US (36 percent) being the most targeted. Other regions around the globe are affected as well, as seen in Figure 4.

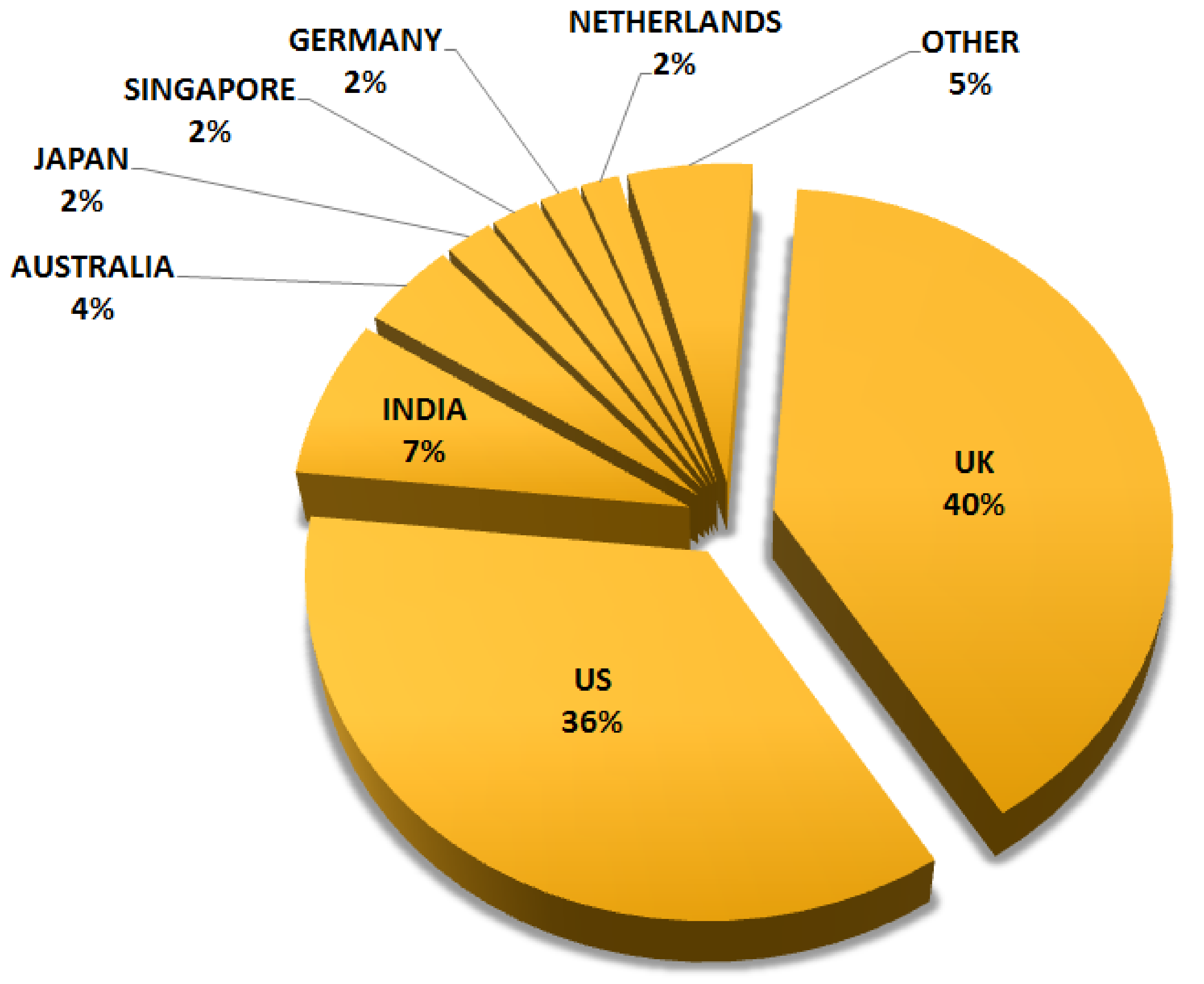


Figure 4. Majority of the spam is being distributed to the UK and the US

The spam campaign began as early as February 17 and is still ongoing. Although Symantec telemetry indicates the peak of the campaign may have already passed (see Figure 5), it would not be surprising if the campaign starts picking up again since the attackers behind TeslaCrypt are known to be very active. We may also come across spam runs using similar baits, so users need to be wary when receiving these types of messages in their mailboxes. Users must be especially vigilant if the email has an attachment with a JavaScript file inside, which is highly unusual.

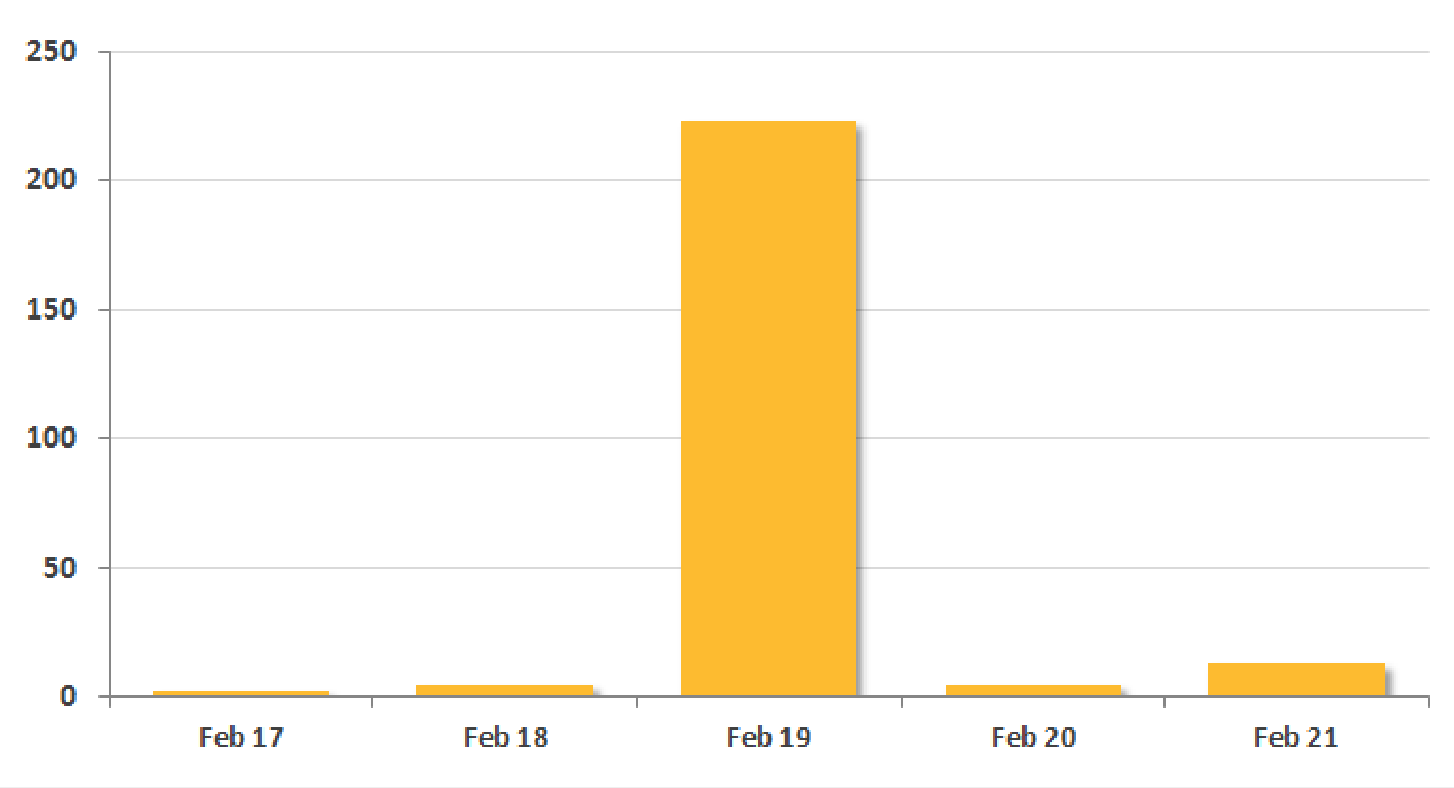


Figure 5. Traffic observed on Symantec Email Security.cloud

Protection

A full protection stack helps to defend against these attacks, including Symantec Email Security.cloud (http://www.symantec.com/page.jsp?id=email-security-cloud) which can block email-borne threats, Symantec Web Security.cloud (https://www.symantec.com/products/threat-protection/web-security-cloud) blocking web-based threats, and Symantec Endpoint Security (https://www.symantec.com/products/threat-protection/endpoint-family/endpoint-protection).

Symantec and Norton products protect against the threats involved in this campaign with the following detections:

Antivirus

- JS.Downloader (https://www.symantec.com/security_response/writeup.jsp?docid=2003-102718-1528-99)
- Trojan.Cryptolocker.N (http://www.symantec.com/security_response/writeup.jsp?docid=2015-030201-5710-99)

Tips on protecting yourself from ransomware

- Regularly back up any files stored on your computer. If your computer does become infected with ransomware, your files can be restored once the malware has been removed.
- Always keep your security software up to date to protect yourself against any new variants of malware.
- Keep your operating system and other software updated. Software updates will frequently include patches for newly discovered security vulnerabilities that could be exploited by attackers.
- Delete any suspicious-looking emails you receive, especially if they contain links or attachments.

Further information

You can read more about the topic of ransomware in our paper that offers a comprehensive review of the state of ransomware: The evolution of ransomware (http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf)

Etiquettes: Security (/connect/fr/communities/security), Security Response (/connect/fr/named-blogs/symantec-security-response), Email Security.cloud (/connect/fr/products/email-securitycloud), Endpoint Protection (AntiVirus) (/connect/fr/products/endpoint-protection-antivirus), Messaging Gateway (/connect/fr/products/messaging-gateway), Web Security.cloud (/connect/fr/products/web-securitycloud), javascript (/connect/fr/blog-tags/javascript), JS.Downloader (/connect/fr/taxonomy/term/97011), Ransomware (/connect/fr/blog-tags/ransomware), Spam (/connect/fr/blog-tags/spam), TeslaCrypt (/connect/fr/taxonomy/term/97001), Trojan.Cryptolocker (/connect/fr/blog-tags/trojancryptolocker), UK (/connect/fr/blog-tags/uk), USA (/connect/fr/blog-tags/usa), Visa (/connect/fr/blog-tags/visa), Visa Total Rewards (/connect/fr/blog-tags/visa-total-rewards)

Abonnements (0)

(/connect/fr/user/joji-hamada)

Joji Hamada (/connect/fr/user/joji-hamada)

View Profile (/connect/fr/user/joji-hamada)

Login (https://www-secure.symantec.com/connect/user/login?destination=node%2F3573191) or Register (https://www-secure.symantec.com/connect/user/register?destination=node%2F3573191) to post comments.

About Your Community

know
Please take a minute to complete our Security Response survey. Click here.

(https://www.surveymonkey.com/r/G7KVZWQ)