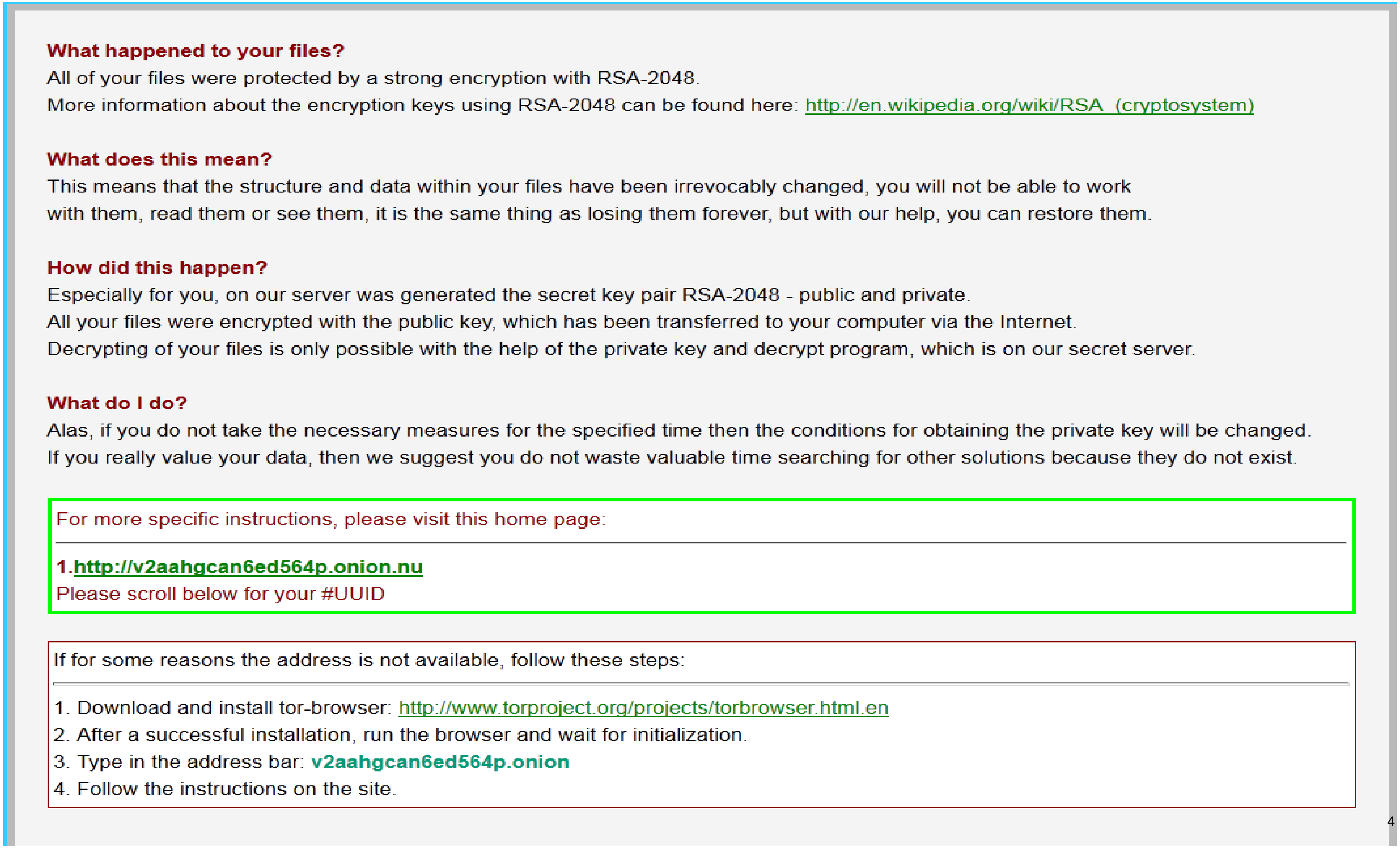
Network Security

Ransomware Experience

- Investigated 9 ransomware incidents, 100s of Trojan, phishing, etc. cases
- In 8 ransomware cases I was able to pinpoint when and where the ransomware was executed
- In 1 case I advised client to pay ransom
- In all other cases, I was able to restore very recent data from backups

Ransomware experience

- Most significant case:
    - Client executed ransomware (a fake resume in an email) at 8:19 am on a Monday morning
    - It began encrypting all documents, images and spreadsheets, making them unusable
    - It completed encrypting the contents of 33,889 folders 16 hours later
    - No one recognized this had happened until 8 am the next day
    - Due to backups completing on Friday, I advised to pay $500 ransom
    - After finding enough bitcoin funding sites to convert $500 to bitcoin, I paid the ransom at 3 pm that same day
    - Received decrypt instructions 15 hours later and began decrypting



What happened to your files?

All of your files were protected by a strong encryption with RSA-2048.
More information about the encryption keys using 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 value your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.

For more specific instructions, please visit this home page:

1.http://v2aahgcan6ed564p.onion.nu
Please scroll below for your #UUID

If for some reasons the address is 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 address bar: **v2aahgcan6ed564p.onion**
4. Follow the instructions on the site.

How to reduce exposure to ransomware

- Backups, Backups, Backups. Check your backups daily/weekly!
- User awareness training. Users are the first line of defense and your weakest link. Use simulated phishing tests to give users valid examples. (knowbe4.com)
- Use email spam/content filtering
- Use a smart content filtering firewall
- Use a DNS filtering service (opendns.org)
- Implement automated security update/patch distribution & management

How to reduce exposure to ransomware

- Implement advanced security measures to lower your risk
  - Remove all users from domain administrator groups
  - Remove all users from local administrator groups
  - Disable unneeded services on all workstations and servers
  - Implement applocker/software restriction policies
  - Use respected Antivirus and set to maximum security
  - Be aware of CEO fraud and how it can be used to steal from your organization

  - Remove all listings of church email addresses from the web
  - Limit social media connections to work (I know it’s tough, but I have a story…)

Network Security

- Questions?