

VÕRGUNDUSE JA INFOTURBE  
**SUMMIT 2016**

# SUMMIT 2016

**Toomas Bergmann**, IT turvajuht  
Siseministeeriumi infotehnoloogia- ja arenduskeskus

**Kaido Raiend**, infoturbejuht  
AS SEB Pank

**Anto Veldre**, kommunikatsiooniosakonna analüütik  
Riigi Infosüsteemide Amet



# VÕRGUNDUSE JA INFOTURBE SUMMIT 2016

**HOIATUS!**

**Lugupidanud klient!**  
Olete siin! Kuna statistiliste näitajate alusel on ilmnenud kõrgendatud risk, et Teie arvuti on nakatunud arvutivirusega.

Kui arvuti peitseb pahavara, võib see varastada Teie andmeid, saada välja päämmi või ummistada Teie internetühenduse. Samuti kujutavad arvutivirused nakatunud arvuti endast ohtu Elioni sidevõrgu ja Elioni teenuste toimimise turvalisusele. Projekti raames teab Elion koostööd Eesti infoturbe tsentriga tegeleva üksusega CERT Eesti (Computer Emergency Response Team).



Eesti eelistatuma internetipakkujana on Elioni eesmärgiks ennetada võimalikke turvatsidente ning vähendada klientide turvariske.

Käesolev Elioni teade on informeeriv ja selle eesmärk on juhida Teie lähelegaru turvaliselt olemasolu. Kui olete andnud kinnituse, et olete ohtudest teadlik, saate interneti kasutamist tavapäraselt viisi jätkata.

**Soovitame kasutada järgnevaid abinõusid:**

- 1. Kodus / kontorisisese WiFi võrgu olemasolu korral peame kontrollida, kas võrk on kinnine, kaitsitud paroolidega ning ei ole arvuti komandatele oopooltele. Kui võrk on avatud, soovitame see koheselt **paroolidega kaitsta**.
- 2. Kontrollige oma arvuti tasuta **Online Scammerit**, et tuvastada võimalikud viirused. (Online Scammer ei pruugi tuvastada kõiki Teie viirusi, seetõttu kasutage võimalusel ka sarnalaidaid programme).
- 3. Veenduge, et Teie arvutisse on paigaldatud viirusestõrje programid koos viimaste uuendustega.
- 4. Veenduge, et Teie arvuti operatsioonisüsteemile on paigaldatud **turvasuundused**.

Turvalist interneti kasutamist soovides,  
Elion



Olen ohtudest te  
**Jätkan**

© Elion 2010 | X-teenindus: 105 | Teenuste tugi: 600 9900 [tugi@elion.ee](mailto:tugi@elion.ee)  
| Aabivõrd teenindus: 1001 | Teenuste tugi: 600 9922 [abivord@elion.ee](mailto:abivord@elion.ee)



CryptoLocker

## Payment for private key



Private key will be destroyed on  
9/20/2013  
6:48 PM

Time left  
**71 : 57 : 22**

Choose a convenient payment method:  
Bitcoin (most cheap option)



Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without a financial institution.

You have to send below specified amount to Bitcoin address  
**1KP72fBmh3XBRfuJDMn53APaqM6iMRspCh** and specify the transaction ID. The transaction will be verified and confirmed.

[Home Page](#)  
[Getting started with Bitcoin](#)

Enter the transaction ID and press «Pay»:

<< Back PA

CryptoWall

Decrypt service

file:///C:/Users/user/Desktop/DECRYPT\_INSTRUCTION.HTML

### What happened to your files?

All of your files were protected by a strong encryption with RSA-2048 using CryptoWall. More information about the encryption keys using RSA-2048 can be found here: [http://en.wikipedia.org/wiki/RSA\\_\(cryptosystem\)](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 your personal home page, there are a few different addresses pointing to your page below:

1. <https://kpa17ycr7jxqk1p.torexplorer.com/4dQj>
2. <https://kpa17ycr7jxqk1p.tor2web.org/4dQj>
3. <https://kpa17ycr7jxqk1p.onion.to/4dQj>

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 address bar: [kpa17ycr7jxqk1p.onion.to/4dQj](https://kpa17ycr7jxqk1p.onion.to/4dQj)
4. Follow the instructions on the site.

### IMPORTANT INFORMATION:

Your Personal PAGE: <https://kpa17ycr7jxqk1p.torexplorer.com/4dQj>  
Your Personal PAGE(using TOR): [kpa17ycr7jxqk1p.onion.to/4dQj](https://kpa17ycr7jxqk1p.onion.to/4dQj)  
Your personal code (if you open the site (or TOR 's) directly): **4dQj**

**Botnet:**

\$60 päevas  
\$400 nädalas

**Kompromiteeritud masin:**

Cpanel: \$3-\$5  
RDP: \$10-\$25

Kehtiv krediitkaart kõigi andmetega - \$30

**Ransomware:**

\$1000 kuus

**Ründevara laenuvus:**

\$50 päevas  
\$400 nädalas  
\$600 kuus

**Netimakseteenuse konto:**

\$400-\$1000 saldoga: \$20-\$50  
\$1000-\$2500 saldoga: \$50-\$120  
\$2500-\$5000 saldoga: \$120-\$200  
\$5000-\$8000 saldoga: \$200-\$300

**„kuulikindel“ majutusteenus:**

100GB kettapinda, 2GB mälu - \$75 kuus



VÖRGUNDUSE JA INFOTURBE  
SUMMIT 2016



