SUMMIT 2016

VÕRGUNDUSE JA INFOTURBE
SUMMIT 2016

Toomas Bergmann, IT turvajuht
Siseministeeriumi infotehnoloogia- ja arenduskeskus

Kaido Raiend, infoturbejuht
AS SEB Pank

Anto Veldre, kommunikatsiooniosakonna analüütik
Riigi Infosüsteemide Amet

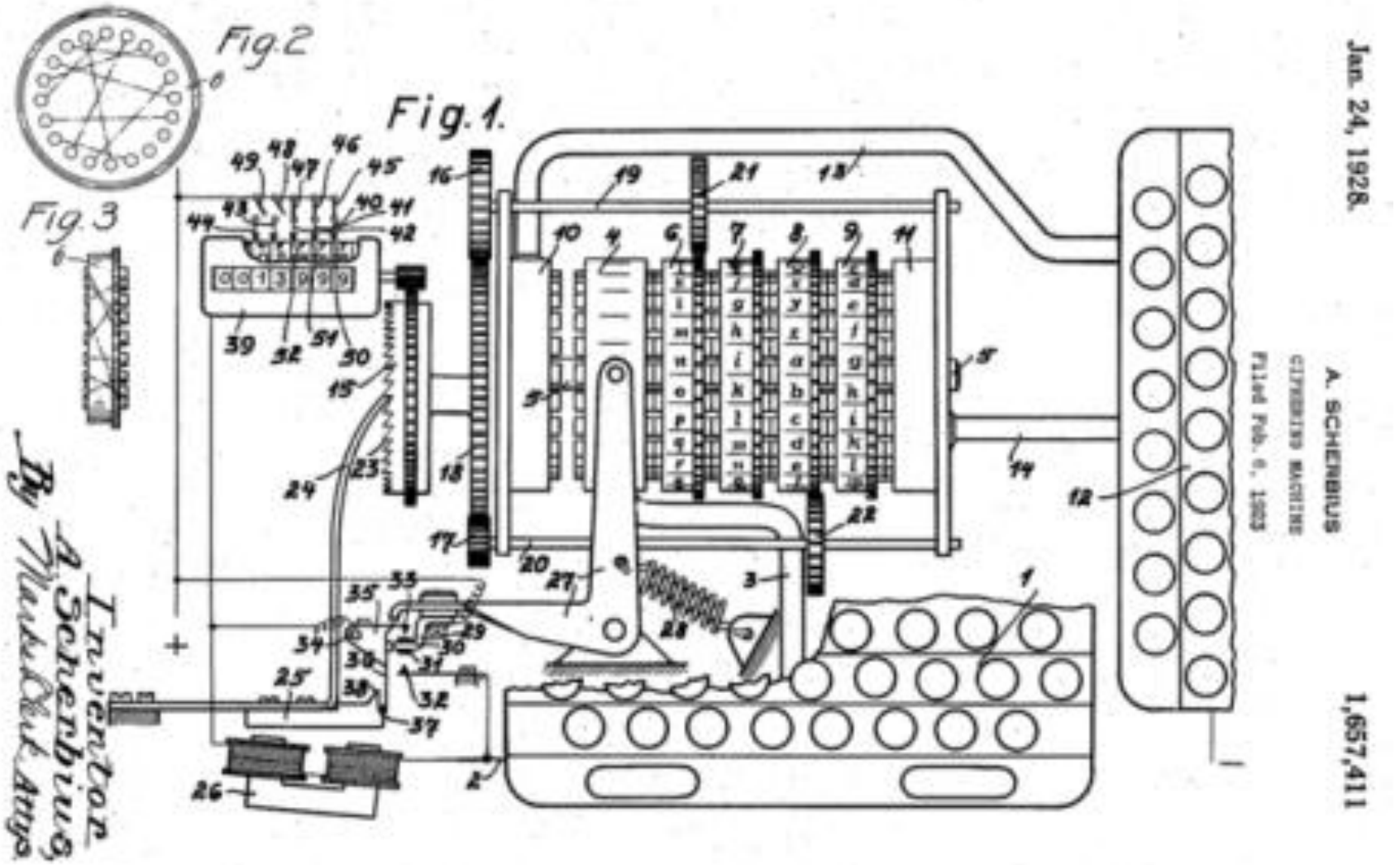
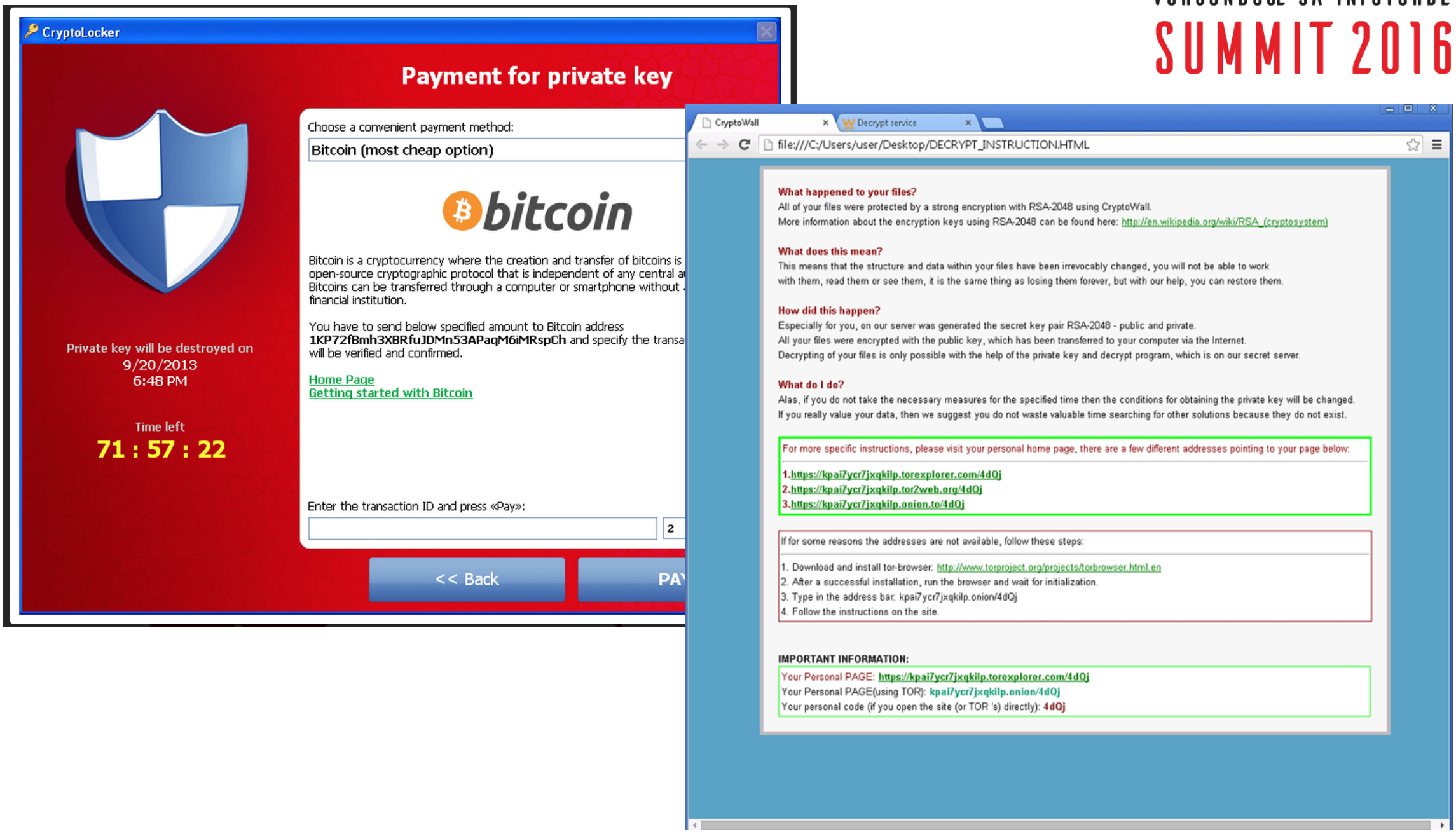


Fig. 2
Fig. 1.
Fig. 3
Jan. 24, 1928.
A. SCHERBIUS
1,657,411
Inventor
A. Scherbius
By Marks & Clerk Attys

VÕRGUNDUSE JA INFOTURBE

SUMMIT 2016


CryptoLocker
Payment for private key
Choose a convenient payment method:
Bitcoin (most cheap option)
bitcoin
Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is
open-source cryptographic protocol that is independent of any central a
Bitcoins can be transferred through a computer or smartphone without
financial institution.
You have to send below specified amount to Bitcoin address
1KP72fBmh3XBRfuJDMn53APaqM6iMRspCh and specify the transa
will be verified and confirmed.
Home Page
Getting started with Bitcoin
Private key will be destroyed on
9/20/2013
6:48 PM
Time left
71 : 57 : 22
Enter the transaction ID and press «Pay»:
2
<< 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)
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://kpai7ycr7jxqkilp.torexplorer.com/4dQj
2.https://kpai7ycr7jxqkilp.tor2web.org/4dQj
3.https://kpai7ycr7jxqkilp.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: kpai7ycr7jxqkilp.onion/4dQj
4. Follow the instructions on the site.
IMPORTANT INFORMATION:
Your Personal PAGE: https://kpai7ycr7jxqkilp.torexplorer.com/4dQj
Your Personal PAGE(using TOR): kpai7ycr7jxqkilp.onion/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

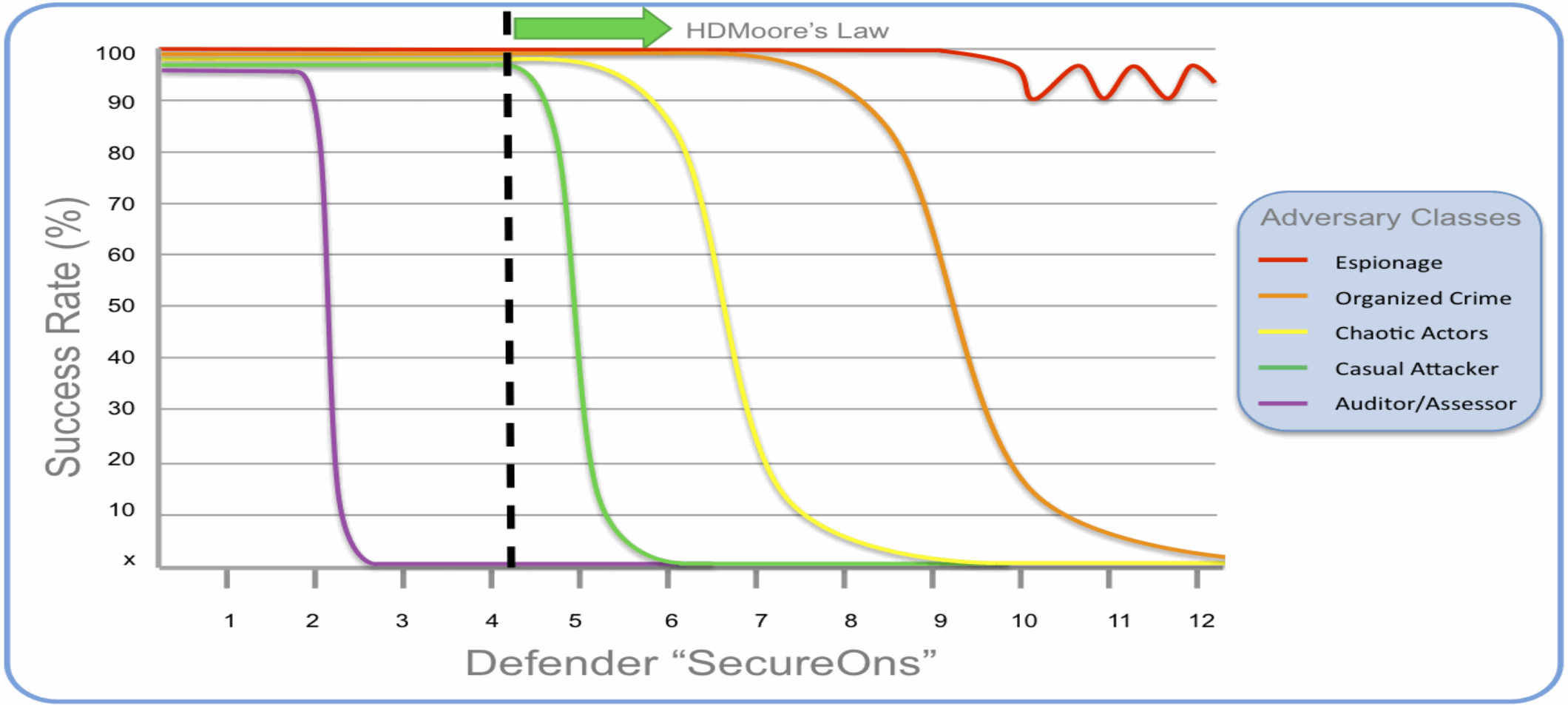
Ründevara laenutus:
$50 päevas
$400 nädalas
$600 kuus

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

VÕRGUNDUSE JA INFOTURBE

SUMMIT 2016


HDMoore's Law
Success Rate (%)
100
90
80
70
60
50
40
30
20
10
x
1
2
3
4
5
6
7
8
9
10
11
12
Defender "SecureOns"
Adversary Classes
Espionage
Organized Crime
Chaotic Actors
Casual Attacker
Auditor/Assessor