CERT.LV

Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija

IT drošības incidenti - aktualitātes un tendences

03.12.2015

Kārlis Podiņš, Varis Teivāns, CERT.LV

Tendences Latvijā

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Tendences

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- **Kibernoziedzība**
  - **Sarežģītāki**
  - **Labāk plānoti**
  - **Ar finanšu sektoru saistītie uzbrukumi**
- **Kiberspiegošana**
  - **Augsta sarežģītība**
  - **Mērķēti uzbrukumi valsts sektoram**
- **Saites starp noziedzību un spiegošanu**
- **Joprojām daudz incidentu, kuru iemesli ir nolaidība un paviršība**
  - **Neatjaunotas sistēmas**
- **Līdzīgi notikumi arī Igaunijā un Lietuvā**

Tendences

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- **Noziedzībā valda ekonomikas likumi**
- **Industrializācija = darba dalīšana**
- **Peļņas maksimizācija**
- **Jaunākās metodes vispirms pielieto:**
  - **1) Lielos&bagātos tirgos**
  - **2/3) Lielos tirgos**
  - **2/3) Bagātos tirgos**
  - **4) Latvijā**
- **Papildus faktors – dalība eirozonā**
  - **Vienota ātra maksājumu telpa**
- **Neplānoti apdraudējuma avoti – kampaņas, kas vērstas pret citiem tirgiem – g.k. Krievija**

«Policijas» vīruss

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

IP: [redacted]

Valsts: **Latvia**
Rajons: **--**
Pilsēta: **--**
Tava Atrašanās Vieta: **57,25**
OperētājSistēma:

UZMANĪBU!

Jūsu pārlūks ir bloķēts zemāk norādīto drošības apsvērumu dēļ. Visas šajā personālajā datorā veiktās darbības ir fiksētas. Visas jūsu datnes ir kodētas.

Jūs esat apsūdzēts par aizliegtu pornogrāfisku datu (bērnu pornogrāfija/ zoofilija/ izvarošana utt.) skatīšanos/uzglabāšanu un/vai izplatīšanu. Jūs esat pārkāpis Vispasaules deklarāciju par bērnu pornogrāfijas neizplatīšanu. Jūs esat apsūdzēts noziegumā, kas paredzēts Latvijas Republikas Krimināllikuma 161. pantā.

Latvijas Republikas Krimināllikuma 161. pants paredz brīvības atņemšanu uz laiku no **5** līdz **11** gadiem.

Tāpat jūs tiekat turēts aizdomās "par autortiesību un citu tiesību pārkāpumu" (pirātiskas mūzikas, video, programmatūras lejupielādēšanu un ar autortiesībām aizsargātu datu izmantošanu un/vai izplatīšanu. Tādējādi jūs tiekat turēts aizdomās par Latvijas Republikas Krimināllikuma 148. panta pārkāpšanu.

Latvijas Republikas Krimināllikuma 148. pants paredz brīvības atņemšanu uz laiku no **3** līdz **7** gadiem vai naudas sodu no **150** līdz **550** minimālo algu apmērā.

No jūsu datora ar nelikumīgas piekļuves starpniecību iegūta pieeja valsts nozīmes informācijai un publiskai pieejai slēgtiem datiem.

Iespējams, nesankcionēto piekļuvi jūs organizējāt pats ar savtīgu nolūku, vai tā tika organizēta, jums nezinot, bez jūsu piekrišanas, ja jūsu datora darbību ietekmē kaitīga programmatūra. Jūs tiekat turēts aizdomās - līdz brīdim, kad tiks izbeigta izmeklēšana - par Latvijas Republikas Krimināllikuma 215. panta pārkāpšanu ("Likums par nolaidīgu un nevērīgu apiešanos ar datoru un datoru palīglīdzekļu").

Atlikušais laiks: 47:59:58

paysafecard

PSC PIN Kods | Summa

Ierakstiet savu kodu | 100

1 2 3 4 5 6 7 8 9 0 ← skaidrs

Apmaksāt PaySafeCard

Kur es varu saņemt naudas sertifikātu PaySafeCard?

ATRODI TUVĀKĀS TIRDZNIECĪBAS VIETAS ŠEIT

Pārskats par tirgotājiem: Latvijā PaySafeCard tu vari iegādāties visos **Narvesen** veikalos un **Narvesen** un kioskos **R-Kiosk**.

NARVESEN

Izspiešana - šifrējošie datorvīrusi

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- **Iekārtas līmeņa DoS**
  - **Pretstatā tīkla DoS**
- **Mērķis:**
  - **Lietotāju datori**
  - **Serveri**
  - **Telefoni**

Pret lietotāju datoriem vērstās kampaņas

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- ***CTB-Locker* un *CryptoWall***
  - **Šifrē lietotāja dokumentus**
  - **Šifrē failus koplietošanas tīkla mapēs**
  - **Dzēš shadow files rezerves kopijas**
  - **Sazinās ar serveriem jau pēc dokumentu šifrēšanas**
  - **Saziņai izmanto TOR tīklu**
  - **Maksājumus pieņem Bitcoin**

CTB-Locker

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

CTB-Locker

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- **CTB-Locker**
  - **Upura saskarne latviešu valodā**
  - **Labi pārzina vietējos apstākļus**
    - **Latvijas failu apmaiņas servisi**
  - **Operatīvi maina e-pastu saturu**
  - **Kampaņas**
    - **12.2014. - inficēti banneri**
    - **Atkārtoti 01.2015., 02.2015., 11.2015. - inficēti epasta pielikumi**

CTB-Locker

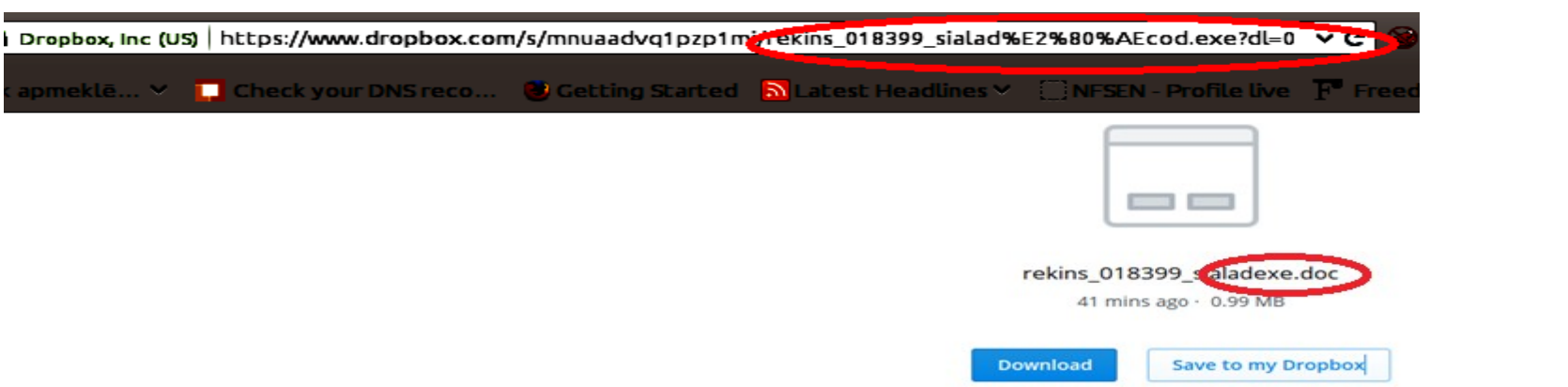
CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- **CTB-Locker mērķauditorija – augstas vērtības mērķi**
  - **Grāmatveži**
  - **Uzņēmumu vadītāji**
  - **Juristi**
  - **Lietvedes**
- **Koplietošanas tīkla mapes - viens inficēts dators var bojāt visus datus**
  - **Tiesības**
- **Grūti precīzi atklāt**
  - **t.sk. sensoru tīklā - dns+tor**
  - **Jāierobežo patvaļīgu datņu izpilde (SRP)**

CTB-Locker

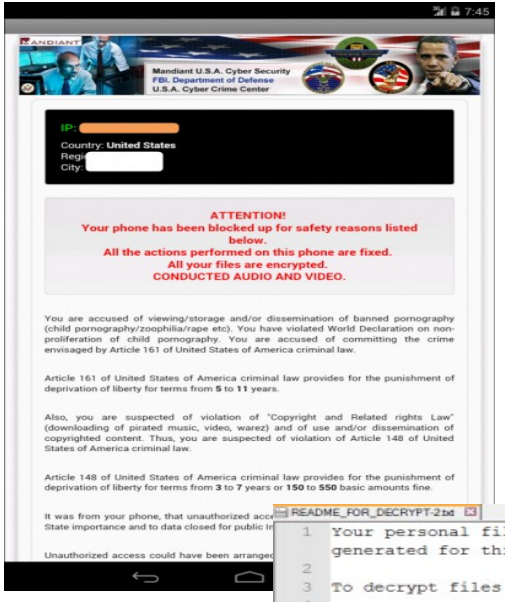
CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

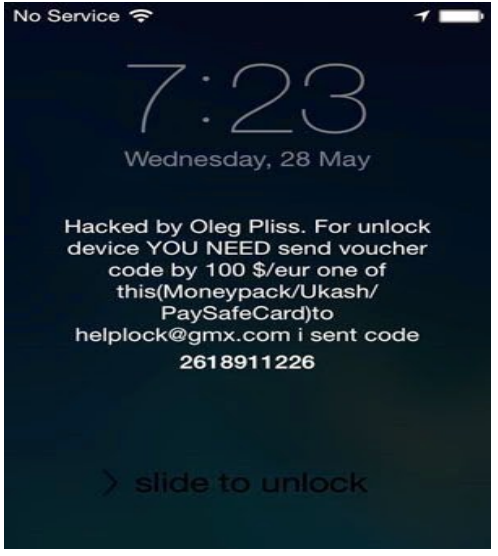
- **Izmanto UTF-8 kodēšanu lejupielādējamā faila tipa maskēšanai!**
  - **IOC: simboli U+202e, U+200f**



Citas platformas

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija



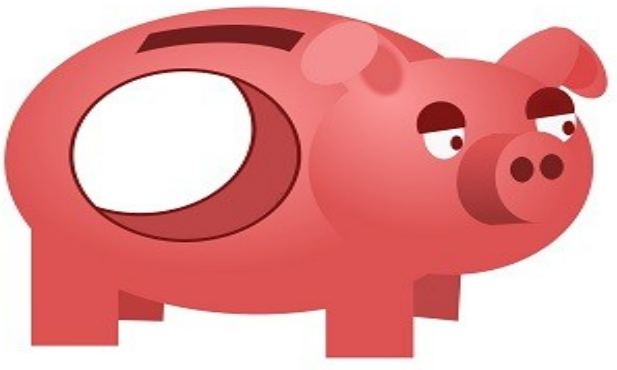


README_FOR_DECRYPT.txt

```
Your personal files are encrypted! Encryption was produced using a unique public key RSA-2048
generated for this computer.

To decrypt files you need to obtain the private key.

The single copy of the private key, which will allow to decrypt the files, located on a secret
server at the Internet. After that, nobody and never will be able to restore files...

To obtain the private key and php script for this computer, which will automatically decrypt
files, you need to pay 1 bitcoin(s) (~420 USD).
Without this key, you will never be able to get your original files back.



!!!!!!!!!!!!!!!!!!!!! PURSE FOR PAYMENT(ALSO AUTHORIZATION CODE):
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx !!!!!!!!!!!!!!!!!!!!!
WEBSITE: https://z54n57pg2el6uze2.onion.to

INSTRUCTION FOR DECRYPT:
```

Internetbanku datorvīrusi

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija



Internetbanku datorvīrusi - tendences

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- **Uzbrukuma vektori**
  - **Pikšķerēšana – samazinās**
  - **Ļaundabīga programmatūra - palielinās**
- **Interneta pārlūkā tiek izmainīts lapas saturs**
  - **Pārskaitījuma saturs**
  - **Maksājumu vēsture**
  - **Bilance**

Internetbanku datorvīrusi - kampaņa

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- **Zeus + Dyre**
  - **Pielāgotas versijas vairāku Latvijas internetbanku maksājumu pārtveršanai**
  - **Kampaņas 12.2014., 06.2015., 08.2015.**
  - **Izplata e-pasta pielikumos**

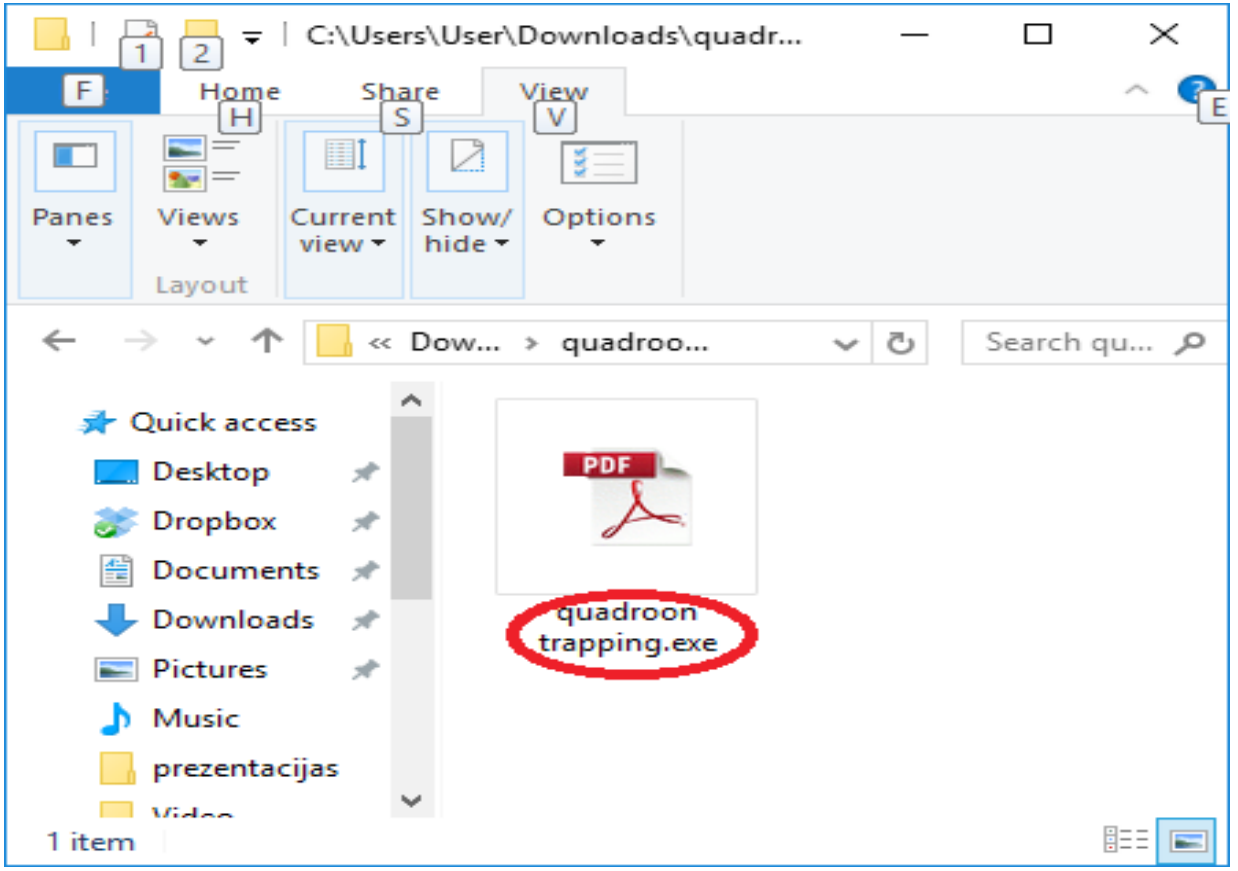
Internetbanku datorvīrusi

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- **Izplatīšana e-pastā**
  - **Vīrusa kopijas izsūta adrešu grāmatas kontaktiem**
    - **Izmanto uzticēšanos**
  - **Izpildāmais fails pielikumā:**
    - **Mazs**
    - **Slikti detektējams ar antivīrusu programmām**
    - **Filtrēt izpildāmos failus epasta pielikumos**
  - **Pielikumā esošais fails tiek attēlots ar PDF failam līdzīgu ikonu**

Internetbanku datorvīrusi

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija



Internetbanku datorvīrusi

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- **Kampaņu īpatnības**
  - **Precīzi mērķētas kampaņas**
    - **Specifiski uzņēmumi**
    - **Uz dažām e-pasta adresēm**
  - **Pārskaitītās summas tiek ātri pārvērstas skaidrā naudā**
  - **Inficētos datorus izmanto kā starpniekus citu kontu apzagšanā**

DDoS4BC

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- **Tīkla DoS**
- **DDoS for bitcoin un Armada izspiešanas uzbrukumi**
  - **5.2015. un 10.2015.**
  - **Vairākas Latvijas organizācijas (pamatā – bankas)**
  - **Izpirkuma maksa Bitcoin**
  - **Pieprasītās summas ir dažādas, sākot no 20BC**

DDoS4BC

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- **Latvijā līdz šim nav bijuši sekmīgi**
- **Demonstratīviem uzbrukumiem nesekoja nopietni DDoS gadījumi**
- **Izmakasas uzbrucējam**
  - **Botnetu īre liela apjoma DDoS ir dārga**

Pikšķerēšana

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- **Populārākie mērķi**
  - **Gmail**
  - **Paypal**
  - **Apple**
  - **Draugiem.lv**

iCloud.lv

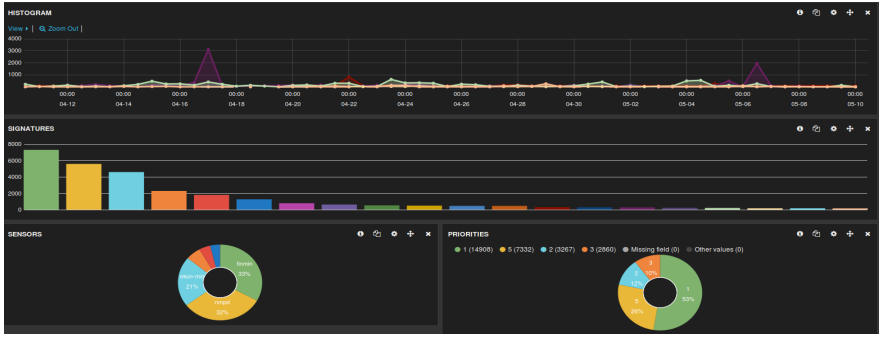
CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

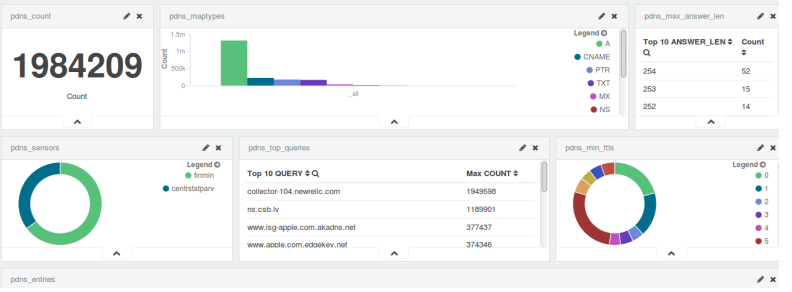
Sensoru tīkls Latvijā

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

zoomcharts

- **Tīkla IDS sensori**
  - **valsts un pašvaldību iestādēs**
- **Ieguvumi:**
  - **Apdraudējumu identificēšana**
  - **Apdraudējumu novēršana**
  - **Skaidrāka izpratne par situāciju .lv interneta telpā**

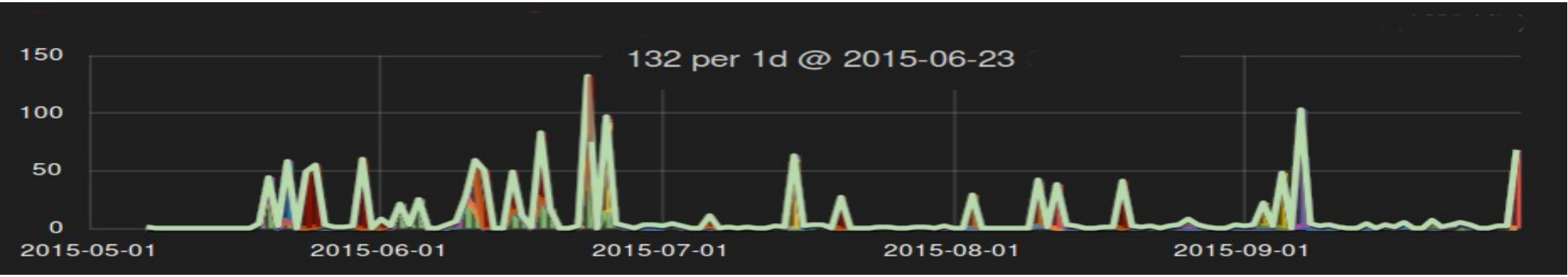




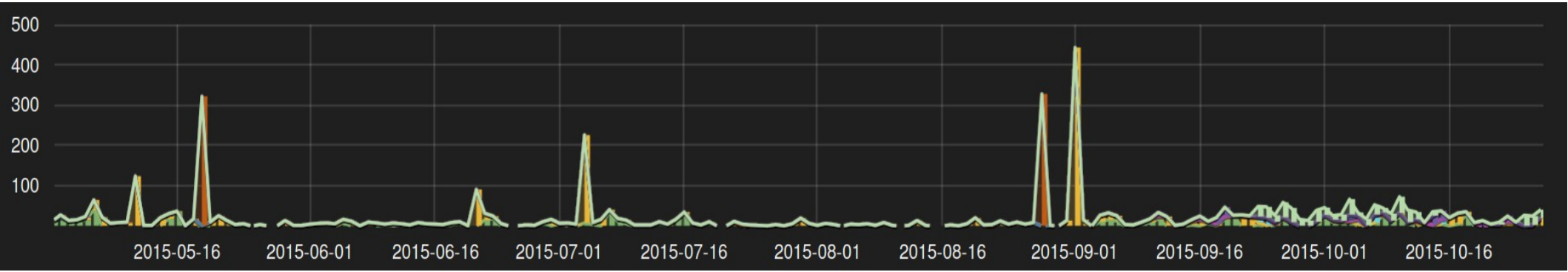
Sensoru tīkls - rezultāti

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- Uzbrukumi prezidentūras laikā



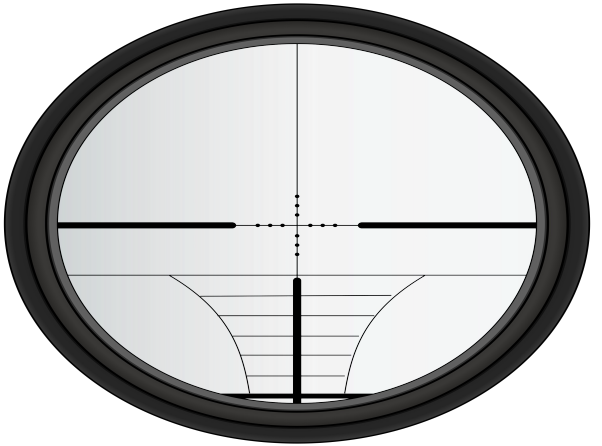
- Uzbrukumi valsts iestāžu mājas lapām



Mērķēti uzbrukumi

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- **Mērķērti uzbrukumi pret lielu LV uzņēmumu darbiniekiem**
  - **Ekonomiskā spiegošana?**
  - **Finanšu līdzekļu izkrāpšanas mēģinājumi?**
  - **Ļaundabīgā programmatūra pa pastu**



Kibernoziedzība – bez robežām

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- **Globālā noziedzība - .lv kā infrastruktūra uzbrukumos citām valstīm**
  - **Brazīlijas bankas**
  - **Paypal**
- **Lokālā noziedzība**
  - **cvvshop.lv**
  - **cvvshop1.lv**
  - **bigbase1.lv**

Incidenti ES prezidentūras kontekstā

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- **Tieslietu sektors: 25.01 – 30.01**

Incidenti ES prezidentūras kontekstā

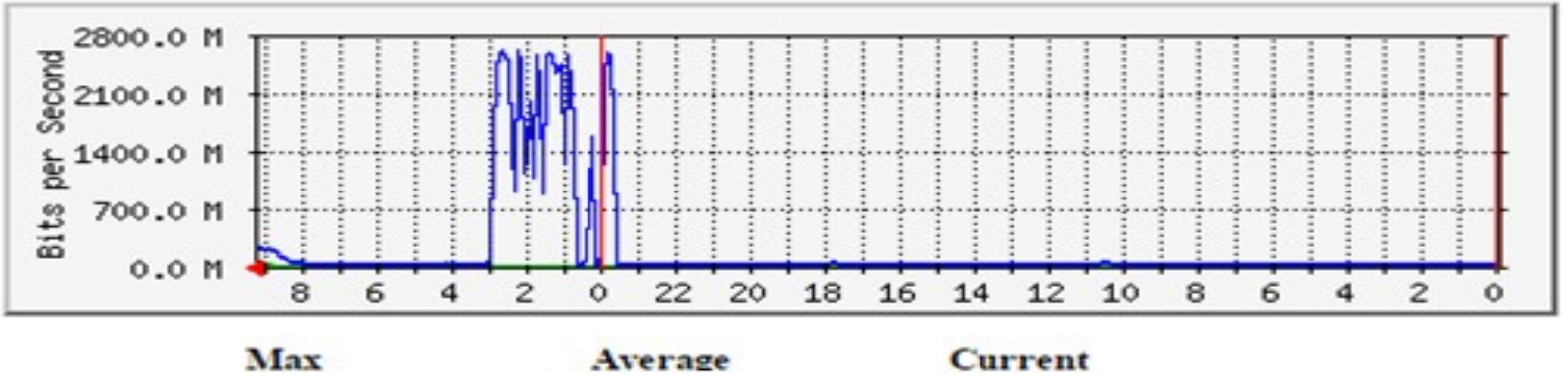
CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- **>3GBps = 4 milj. paketes sekundē**
    - **3 reizes pārsniegta iestādes tīkla tehniskā kapacitāte**
- **Ietekme**
    - **Būtiski apgrūtina tieslietu sektora darbu**
    - **Traucēta e-pastu aprite**
    - **Citi paklpojumi**
- **Tiek sasniegts arī apjoms, kas traucē IPS iekārtu darbību**
- **Naktī uz 28.01. visa TM/TNA datu plūsma tiek pārslēgta caur IPS aizsardzības risinājumu**
- **Šāda apjoma uzbrukumi TM pieredzēti pirmo reizi, taču tie nav vērtējami kā ārkārtīgi lieli**

Incidenti ES prezidentūras kontekstā

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- **Uzbrukuma avoti - slēpti**
    - **It kā globāls uzbrukums**
- **Ar tehniskiem līdzekļiem noskaidrots uzbrukuma patiesais avots**



Tendeces pasaulē

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Starptautiski incidenti

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- **Hacking Team**
  - **Uzlauzts kiberieroču ražotājs**
  - **Ievainojamas populārās platformas un produkti**
    - **IExplorer, Flash, Android**
  - **Stingras procedūras + rūpīga ievērošana**
- **Ashley madison**
  - **Vairākas pašnāvības**
  - **.mil adreses ~13 000**
  - **Čats ar robotiem**
  - **>2000 lv adreses**

Noziedzības evolūcija

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- **Ielaušanās ziņu aģentūrās**
    - **Piekļuve publicējamai (!) informācijai**

Page: 6 of 62 Automatic Zoom

SUMMARY

1. Defendants perpetrated an international fraudulent scheme by hacking the computer servers of at least two newswire services and stealing, through deception, confidential earnings information for numerous publicly-traded companies from press releases that had not yet been released to the public. Defendants then used that stolen material nonpublic information to trade securities and reap over $100 million in unlawful profits.

2. Over an approximately five-year period, defendants Ivan Turchynov and Oleksander Ieremenko—computer hackers residing in the Ukraine (the "hacker defendants")—

- **Piekļuve banku klientu datiem(100M+), mērķētas spam kampaņas + "pump and dump" manipulācijas vērtspapīru tirgū**
    - **>100M$ peļņa**

Nākotnes izaicinājumi

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Sliktais scenārijs

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Datorizētas sistēmas

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- **Iekārtas**

- **Biznesa procesi**

Iekārtas

- **Liels skaits**
- **24/7**
- **Lēns atjaunināšanas cikls**
- **LV Konstatēta masveida mājas maršrutētāju uzlaušana**
  - **Mainīta DNS konfigurācija**
  - **Iekārtu programmatūras atjaunināšana**
- **Noklusētā konfigurācija**

Populārākie uzbrukumu veidi

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- **Lietotāju kļūdas**
  - **Office dokumentu “macro” funkcionalitāte**
  - **Zip**
  - **Exe**
  - **Saites uz neleģitīmiem resursiem**
    - **Nespiest automātiski “yes”**
- **Lietotāju nolaidība**
  - **Neatjaunota programmatūra**
    - **Flash, pdf reader, java**

Profilakse

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- **Atjauninājumu nelietošana un novecojušas versijas = atvērtas durvis uzbrucējiem**
- **Serveriem un gala lietotājiem**
  - **Atjaunošana no rezerves kopijas → atkārtota ielaušanās**
  - **Windows XP = infekciju perēklis**
- **Atslēgt nevajadzīgu funkcionalitāti**
  - **Klienta pusē izpildāms kods**


Paldies!