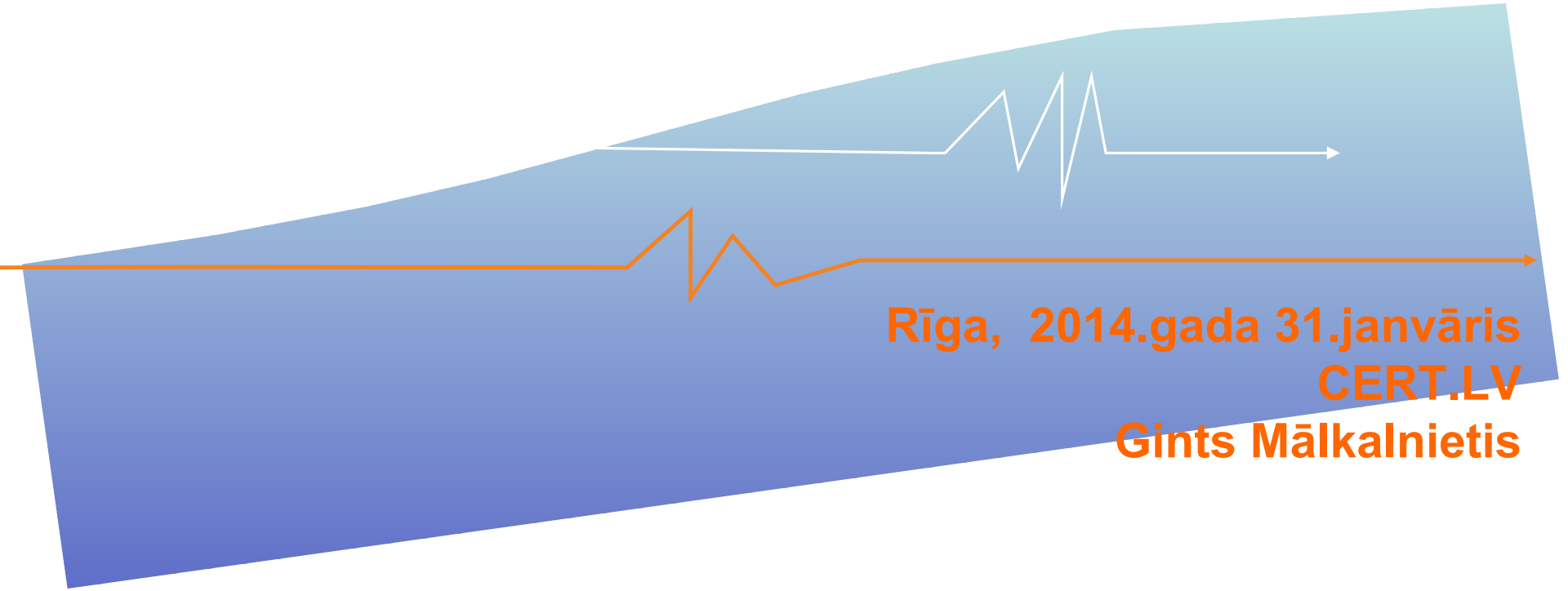
Mobilo ierīču un tīklu drošība



Rīga, 2014.gada 31.janvāris

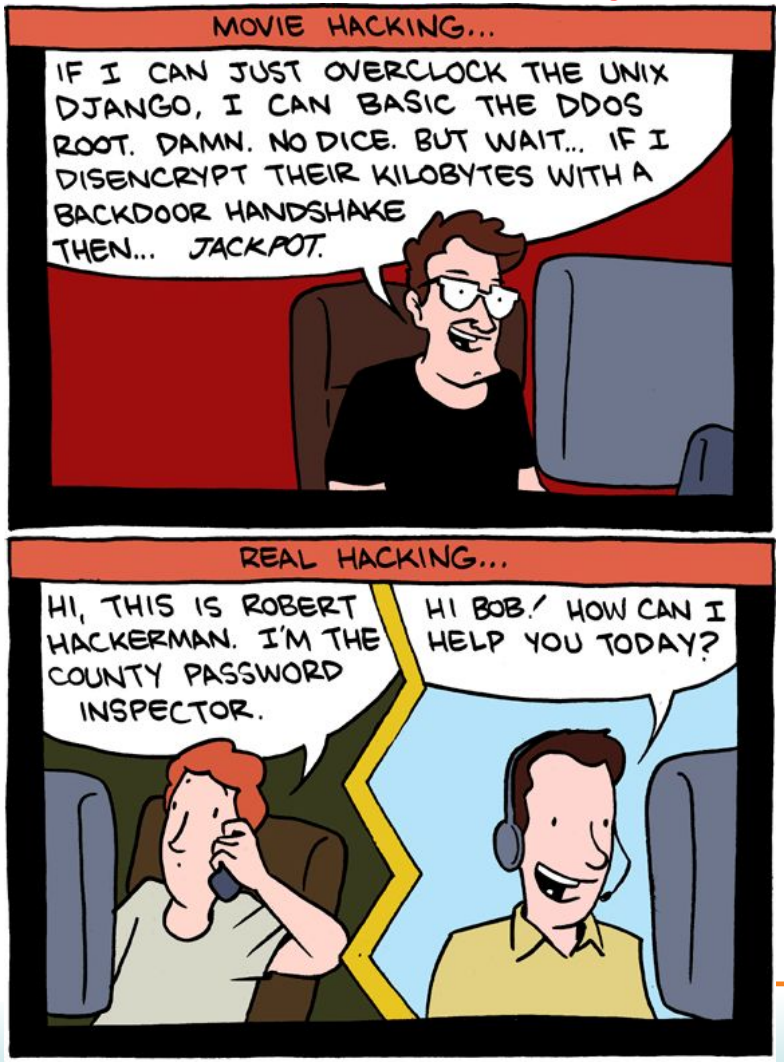
CERT.LV
Gints Mālkalnietis

Saturs

- Ievads
- Riski mūsdienu tehnoloģijās
- Ko īstenībā dara mobilās aplikācijas
- Tīkla segmentu nodalīšana
- “Drošas” datorvides izveide
- Kā atrast vainīgo

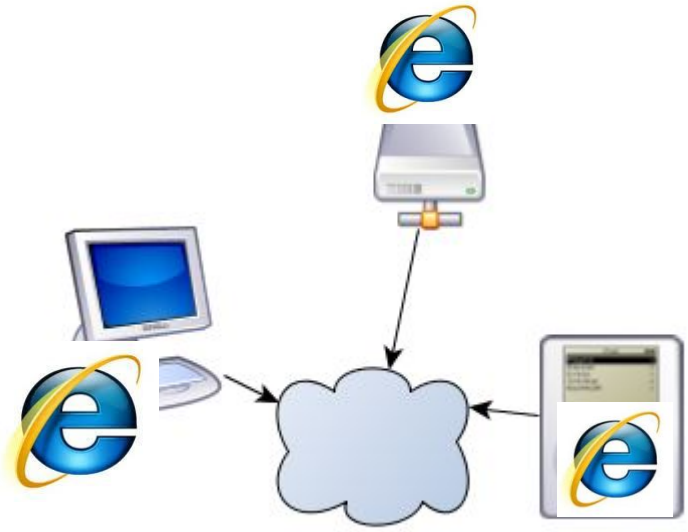
Riski mūsdienu tehnoloģijās

- Neviens drošības tehniskais risinājums nav 100% drošs!



Interneta pārlūks = dators (OS + app.)

- Interneta pārlūks = pilnvērtīgs dators
- Veiksmīgs uzbrukums pārlūkam – pilnīga kontrole pār lietotāja datiem
- Dažādas ierīces – viena ievainojamība



Jebkura iekārta = serveris

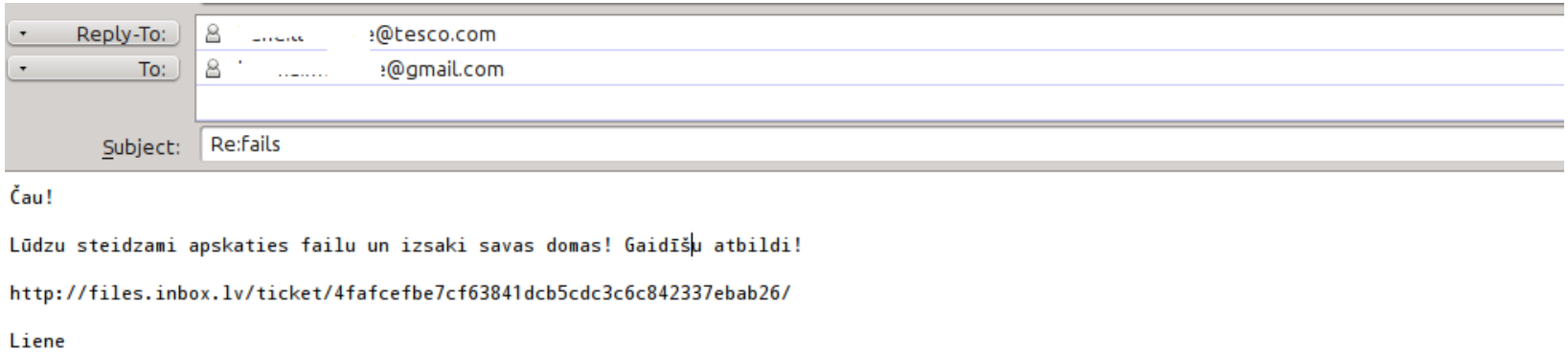
- Veiktspēja >kā 5 gadus vecam serverim
- Vienmēr – pievienots internetam
- Parasti – ar novecojušām, nelabotām programmām
- Dažreiz – ar pārāk lielām lietotāja pilnvarām veikt tajā izmaiņas

Uzbrucēju mērķauditorija

1. Sociālo tīklu lietotāji
   - %{HTTP_REFERER} ^(tweet|twit|linkedin|instagram|facebook\.|myspace\.|bebo\.)
   - %{HTTP_REFERER} ^(hi5\.|blogspot\.|friendfeed\.|friendster\.|google\.)
1. Apmeklētāji no dažādiem meklēšanas rīkiem
   - %{HTTP_REFERER} ^(yahoo\.|bing\.|msn\.|ask\.|excite\.|altavista\.|netscape\.)
   - %{HTTP_REFERER} ^(aol\.|hotbot\.|goto\.|infoseek\.|mamma\.|alltheweb\.)
   - %{HTTP_REFERER} ^(lycos\.|metacrawler\.|mail\.|dogpile\?)



Uzbrukuma mērķis – cilvēks!



- Saistošs teksts, lai mudinātu atvērt failu

Čau!
Lūdzu steidzami apskaties failu un izsaki savas domas! Gaidīšu atbildi!

- Vēstule atsūtīta no zināmas personas
- Fails izvietots Latvijas vietnē

http://files.inbox.lv/ticket/4fafcefbe7cf63841dcb5cdc3c6c842337ebab26/

virustotal

SHA256: 20904cf65177c788a9f5f09233d6abb1033ebf10765823e9126a58ccc9cfc8f6

File name: rc_atskaite_371.exe

Detection ratio: 0 / 48

Analysis date: 2013-10-03 07:39:42 UTC (0 minūšu ago)

More details

Analysis | File detail | Additional information | Comments | Votes

Antivirus	Result	Update
Agnitum		20131002
AhnLab-V3		20131002
AntiVir		20131002
Antiy-AVL		20131003
Avast		20131003
AVG		20131002
Baidu-International		20131002
BitDefender		20131003
Bkav		20131002
ByteHero		20130928
CAT-QuickHeal		20131003
ClamAV		20131003
Commtouch		20131003
Comodo		20131003
DrWeb		20131003
Emsisoft		20131003
ESET-NOD32		20131002
F-Prot		20131003
F-Secure		20131003
Fortinet		20131003

CERT.LV

- Reāla datorvīrusa izplatīšanas kampaņa
- Jauna vīrusa versija – ik pa 12 stundām
- Profesionāli kaitīgā koda veidotāji izmanto automatizētus rīkus sava koda slēpšanai

virustotal

SHA256: 20904cf65177c788a9f5f09233d6abb1033ebf10765823e9126a58ccc9cfc8f6

File name: rc_atskaite_371.exe

Detection ratio: 12 / 47

Analysis date: 2013-11-04 07:36:01 UTC (0 minūšu ago)

More details

Analysis | File detail | Additional information | Comments | Votes

Antivirus	Result	Update
Agnitum	✓	20131103
AhnLab-V3	Trojan/Win32.Zbot	20131104
AntiVir	✓	20131104
Antiy-AVL	✓	20131101
Avast	Win32:Malware-gen	20131104
AVG	✓	20131103
Baidu-International	✓	20131103
BitDefender	✓	20131104
Bkav	✓	20131102
ByteHero	✓	20131028
CAT-QuickHeal	✓	20131103
ClamAV	✓	20131104
Commtouch	✓	20131104
Comodo	UnclassifiedMalware	20131104
DrWeb	✓	20131104
Emsisoft	✓	20131104
ESET-NOD32	a variant of Win32/Injector.ANTK	20131103
F-Prot	✓	20131104
F-Secure	✓	20131104
Fortinet	✓	20131104

- Atkārtota analīze mēnesi vēlāk – detektē tikai 12 no 47 AV!
- Citas šīs kampaņas vīrusa versijas ķer vairāki AV
- Datorvīruss nodarbojas ar vairāku Latvijas banku tiešsaites piekļuves paroļu zādzību
- Kopē arī citas datorā ievadītās paroles

Atbalsts un aizsardzība:

Atlikušais laiks: 47:52:08

paysafecard

IP: [redacted]

Valsts: **LV Latvia**
Rajons: **Riga**
Pilsēta: **Riga**
ISP: **SIA Lattelecom**
OperētājSistēma: **Windows XP (32-bit)**
Lietotāja Vārds: **Ginc**

UZMANĪBU! Jūsu dators ir bloķēts zemāk norādīto drošības apsvērumu dēļ.

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").

Latvijas Republikas Krimināllikuma 215. pants paredz brīvības atņemšanu uz laiku no 5 līdz 8 gadiem un/vai soda naudu līdz LVL 100.000 latu apmērā.

PIN Kods | Summa

50

1 2 3 4 5 6 7 8 9 0

Apmaksāt PaySafeCard

Kur es varu saņemt naudas sertifikātu PaySafeCard?

Pārskats par tirgotājiem: Latvijā PaySafeCard tu vari iegādāties visos **Plus Punkts** veikalos un **Narvesen** un **Qiwi** mašīna. Tu vari iegādāties PaySafeCard daudzos lielveikalos, pirmās nepieciešamības preču veikalos, degvielas uzpildes stacijās un kioskos (**R-Kiosk**).

R kiosk

copyright alliance

vp.gov.lv.id146025375-5118247904.n2195.com/?flow_id=3289&569750=39670/case_id=94281

VALSTS POLICIJA

Jūsu informācija ir šifrēta. Nemēģiniet atbloķēt jūsu datoru.

Uzmanību!

Jūs pārkapāt citu personu autortiesības vai saistītas tiesības (videomateriāli, mūzika, programmatūra) un nelegāli izmantojat aizsargātus materiālus, pārkapājot 1. panta, 8. daļas, 8. noteikumu, zināmu arī, kā Latvijas republikas krimināllikums.
1. panta, 8. daļas, 8. noteikums paredz sodu no diviem līdz pieciem simtiem minimālu algu apmērā, vai brīvības atņemšanu no diviem līdz astoņiem gadiem.
Jūs esat skatījis/jusi vai izplatījis/jusi aizliegtus pornogrāfiskus materiālus (pornogrāfija ar bērniem vai citi materiāli tika atrasti jūsu datorā). Jūs pārkapāt Latvijas krimināllikuma 202. Pantu, kas paredz brīvības atņemšanu no četriem līdz divpadsmit gadiem.
Nelegāla piekļuve datiem tika iniciēta no jūsu datora bez jūsu zināšanas, kas varētu but datora piesārņojuma dēļ ar vīrusiem, toties jūs pārkapāt likumu par nolaidīgu datora izmantošanu. Latvijas krimināllikuma 210. Pants paredz sodu līdz 100,000 Eur un brīvības atņemšanu no četriem līdz deviņiem gadiem. Ievērojot krimināllikuma grozījumus (ja pārkāpums tika konstatēts pirmo reizi), jūs netiksiet sodīts, ja samaksāsiet sodu.
Lai atbloķētu jūsu datoru un izvairīties no legālam sekām, jums ir obligāti jāsamaksā atbrīvošanas maksa 100 Eur apmērā caur PAYSAFECARD (jums ir jāiegādājas PAYSAFECARD, jāpapildina konts par 100 Eur un jāievadā kods). Jūs varat nopirkt kodu jebkura veikalā vai DUS. PAYSAFECARD ir pieejama visos nacionālajos veikalos.

Kā es varu samaksāt sodu un atbloķēt savu datoru?
1. Atrādiet PAYSAFECARD tirgošanas vietu jums blakus:

QIWI · plus punkts svarīgi sīkumi · R kiosk · NARVESEN

2. Saņemiet PAYSAFECARD ar priekšapmaksas opciju un papildiniet balansu par 100 Eur skaidrā naudā pie kases.
3. Ievadiet jusu PAYSAFECARD kodu un nospiediet submit un "Atbloķējiet jūsu datoru tagad"

Jūsu IP adrese: [redacted]
Atrašanas vieta: Riga, Riga, Latvia

paysafecard pay cash. pay safe — Drošas transakcijas forma

Ievadiet PAYSAFECARD kodu

Lūdzu ievadiet PAYSAFECARD kodu izmantojot PIN tastatūru apakšā

1	2	3	4	5	6	7	8	9	0	Izdzēst

Atbloķējiet jūsu datoru tagad!

Uzmanību: Soda naudai jābūt samaksātai **12.** stundu laikā. Pēc 12. stundām nebūs iespējas samaksāt sodu.
Visi jūsu dati tiks aizturēti un pret jums tiks uzsākts kriminālprocess, ja sods nebūs samaksāts.

Vērtības jūsu datorā

1. Nauda bankas kontā
2. Kredītkaršu dati
3. Gmail konts – tajā ir ne tikai e-pasts
4. Twitter, Facebook, Hotmail konts
5. Tiešsaistes spēļu konti un virtuālie spēļu rīki
6. Pases dati – var tikt izmantoti viltotas pases izgatavošanā!
7. Privātas fotogrāfijas šantāžai
8. Datora resursi – webcoin mining, paroļu uzlaušana, DDOS, mēstuļu izsūtīšana

Datu “mākonis” – neglābj no vecām kļūdām!

• 2009 – Vairāk kā 300 dokumentu par TWITTER biznesa plāniem tika nozagti no Google Apps. Iemesls – vāja parole.
• 2010 – Izveidota programma WiFi paroļu uzlaušanai, izmantojot Amazon E2 Cloud
• 2011 – Amazon E2 Cloud tiek izmantot uzbrukumā Sony PSN
• 2011 – Dropbox kļūdas pēc uz vairākām stundām atslēdz autentifikācijas pārbaudi. Iespējams lejuplādēt jebkuru failu.

Ko īstenībā dara mobilās aplikācijas?

- Vienādas funkcionalitātes aplikācijas pieprasa dažādas pieejas tiesības
- Lietotājam ir vajadzīga vēlamā funkcionalitāte, nevis desmitiem papildiespēju!
- Mobilās ierīces lietotājs NEREDZ un NESAPROT kādus datus pārsūta ierīce!
- Jaunas aplikāciju versijas, pieprasa papildus tiesības!

Ko īstenībā dara mobilās aplikācijas?

- Vienādas funkcionalitātes aplikācijas pieprasa dažādas pieejas tiesības

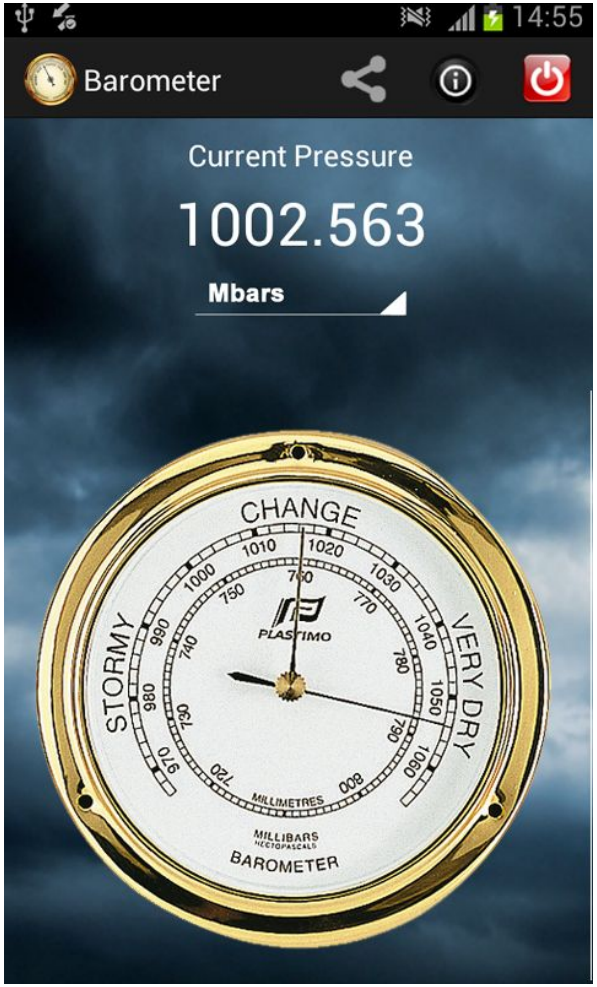
Šī lietotne var piekļūt šādām atļaujām:

- Jūsu atrašanās vieta
precīza atrašanās vieta (izmantojot GPS un tīklu)
aptuvena atrašanās vieta (izmantojot tīklu)
- Tīkla sakari
skatīt tīkla savienojumus
pilnīga piekļuve tīklam
- Atmiņa
pārveidot vai dzēst USB atmiņas saturu
- Sistēmas rīki
pārbaudīt piekļuvi aizsargātai krātuvei
- Jūsu lietojumprogrammu informācija
palaist startējot

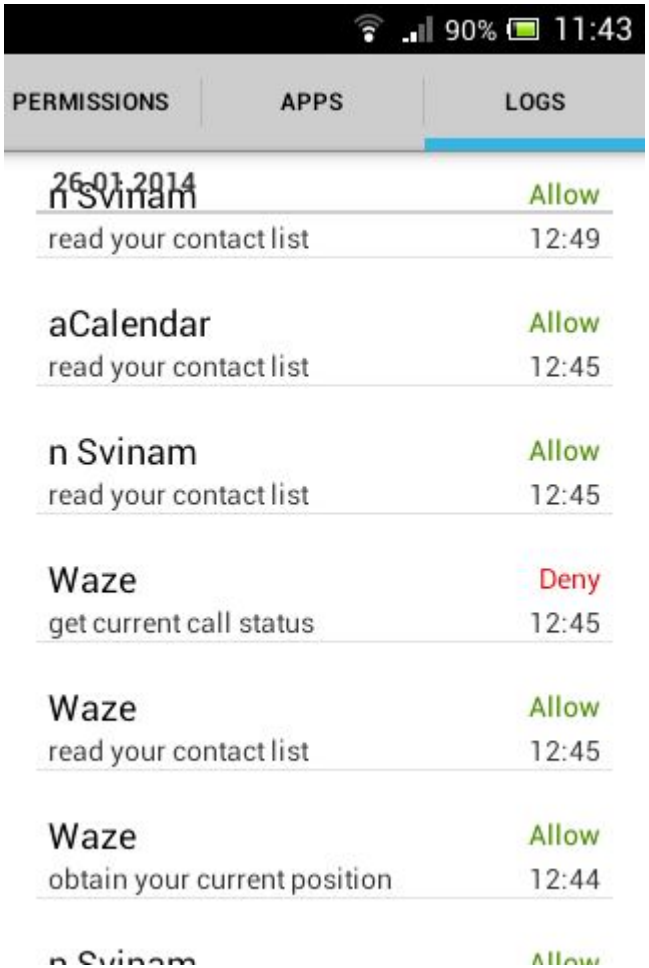
Šī lietotne var piekļūt šādām atļaujām:

- Tīkla sakari
pilnīga piekļuve tīklam
skatīt tīkla savienojumus

Ko īstenībā dara mobilās aplikācijas?



Ko īstenībā dara mobilās aplikācijas?



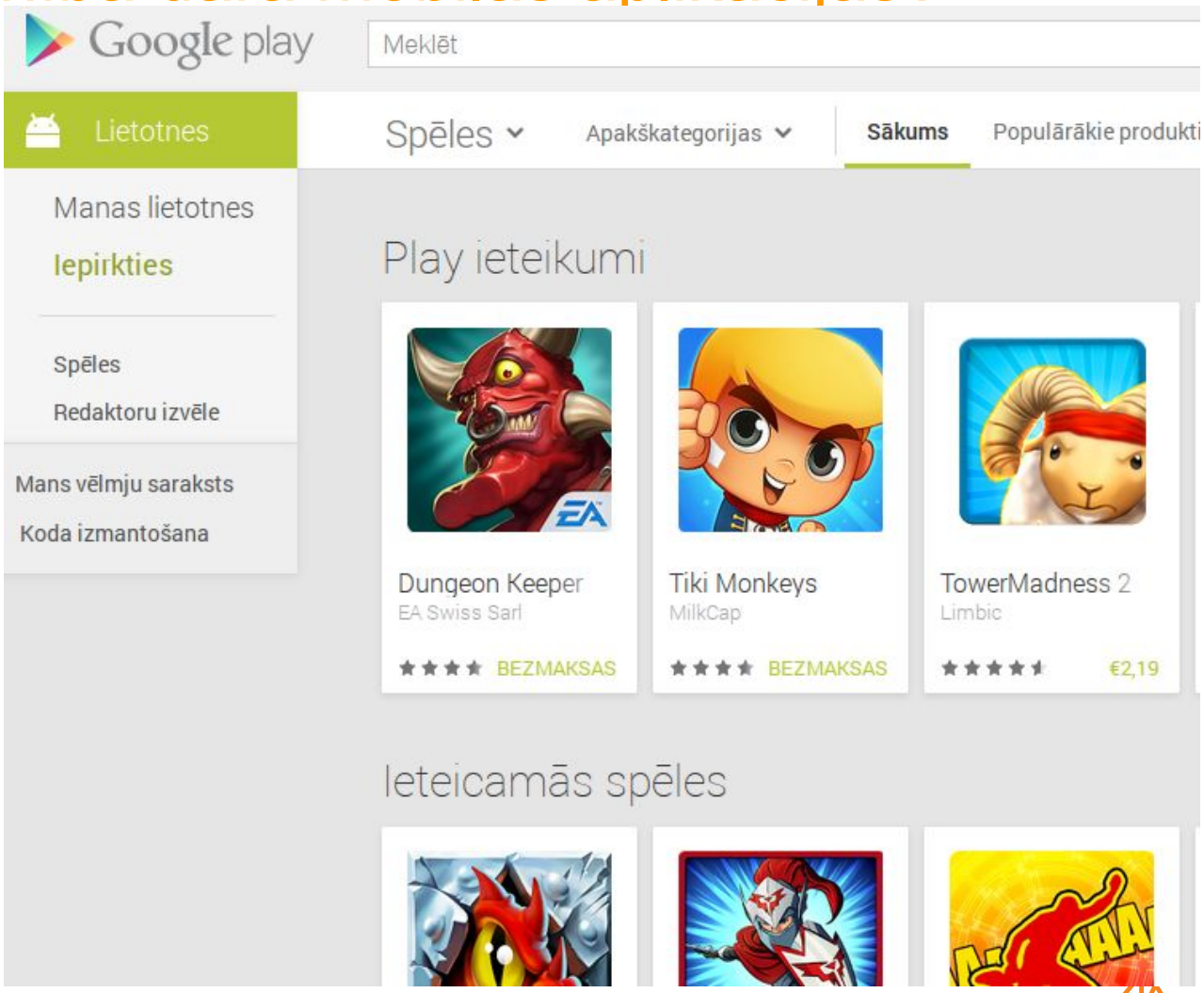
Ko īstenībā dara mobilās aplikācijas?

• Mobilās ierīces lietotājs NEREDZ un NESAPROT kādus datus pārsūta ierīce!

Šī lietotne var piekļūt šādām atļaujām:
• Tīkla sakari
pilnīga piekļuve tīklam
skatīt tīkla savienojumus
skatīt Wi-Fi savienojumus
• Tālruņa zvani
lasīt tālruņa statusu un identitāti
• Atmiņa
pārveidot vai dzēst USB atmiņas saturu
• Jūsu lietojumprogrammu informācija
izgūt izmantotās lietotnes
• Sistēmas rīki
pārbaudīt piekļuvi aizsargātai krātuvei

Šī lietotne var piekļūt šādām atļaujām:
• Tīkla sakari
saņemt datus no interneta
pilnīga piekļuve tīklam
skatīt tīkla savienojumus
skatīt Wi-Fi savienojumus
▪ Tālruņa zvani
lasīt tālruņa statusu un identitāti
• Atmiņa
pārveidot vai dzēst USB atmiņas saturu
• Jūsu konti
atrast kontus ierīcē
• Sistēmas rīki
pārveidot sistēmas iestatījumus
pārbaudīt piekļuvi aizsargātai krātuvei
• Ietekmē akumulatora darbību
novērst ierīces pāriešanu miega režīmā

Ko īstenībā dara mobilās aplikācijas?



Tīkla segmentu nodalīšana = drošāka datu pārraide

- Atdaliet publiskos tīklus no darba vides!
  - Dažādi pieslēgumi internetam
  - Fiziski nodalītas vides – WiFi+vadu tīkli
  - Dažādi WiFi SSID
  - Dažādi maršrutētāji
  - Dažādi VLAN vienā maršrutētājā

- WiFi un vadu tīkli vienā maršrutētājā, standarta konfigurācijā, ir apvienoti vienotā datu pārraides tīklā
  - VLAN darbojas arī WiFi tīklā, bet nav apvienojams ar VLAN citā interfeisā
- Iespējas veidot un nodalīt VLAN segmentus ir jāparedz izvēloties maršrutētāja modeli
- Labāk darbojas viena, jaudīga iekārta, nevis piecas mazas!

Tīkla segmentu nodalīšana = drošāka datu pārraide

- Atdaliet publiskos tīklus no darba vides!
  - Dažādi pieslēgumi internetam
  - Fiziski nodalītas vides – WiFi+vadu tīkli
  - Dažādi WiFi SSID
  - Dažādi maršrutētāji
  - Dažādi VLAN vienā maršrutētājā

- WiFi un vadu tīkli vienā maršrutētājā, standarta konfigurācijā, ir apvienoti vienotā datu pārraides tīklā
  - VLAN darbojas arī WiFi tīklā, bet nav apvienojams ar VLAN citā interfeisā
- Iespējas veidot un nodalīt VLAN segmentus ir jāparedz izvēloties maršrutētāja modeli
- Labāk darbojas viena, jaudīga iekārta, nevis piecas mazas!

Tīkla segmentu nodalīšana = drošāka datu pārraide

- Populārākās maršrutētāju OS, kas atbalsta vairāku SSID WiFi tīklu veidošanu
  - **DD-WRT** =bezmaksas, iespējas atkarīgas no konkrētā maršrutētāja, ierobežots iekārtu atbalsts
  - **RouterOS** (MicroTik) = maksas, iegādājama kopā ar iekārtu
  - **CISCO** = maksas, iegādājama kopā ar iekārtu

“Drošas” datorvides izveide

- Nepietiek ar aizsardzību pret **ārējiem** uzbrukumiem!
- **Viena** inficēta iekārta tīklā, var tikt izmantota uzbrukumam citām
- Lietotāja tiesības uz datora: **mazāk = drošāk!**
    - SRP+AppLocker = iespējams atslēgt “svešu” datorprogrammu izpildi
    - “Kiosk režīms” – ierobežots funkciju un palaižamo programmu klāsts
- Pārlūkprogrammu papildinājumi:
    - NoScript = atspējo JavaSript interneta vietnēs
    - AdBlock = novāc uzmācīgās reklāmas
    - Vēlams atinstalēt AdobeAcrobat, AdobeFlash un Oracle Java
- Datoru “klonēšana” – iespēja ātri atjaunot darbaspējas, bez garām instalācijām
- Virtualizācija – piekļuve dažādām OS, bez papildus instalācijas
    - Ātri atjaunojama konfigurācija
    - Daudz “datoru” uz viena servera

Dažas noderīgas adreses

Failu antivīrusu pārbaude- http://www.virustotal.com/
Pārlūkprogrammas drošības pārbaude - https://browsercheck.qualys.com/
Kaspersku Virus Removal- http://devbuilds.kaspersky-labs.com/devbuilds/AVPTool/
Bitdefender Rescue CD- http://kb.bitdefender.com/site/article/650/

Paldies par uzmanību!!!

Gints Mālkalnietis
E-pasts: gints.malkalnietis@cert.lv
Tīmekļa vietne: http://www.cert.lv
Portāla Esi drošs tīmekļa vietne: http://www.esidross.lv
CERT.LV Twitter vietne: http://twitter.com/certlv