



Datorvīrusu un uzbrukumu tendences Latvijā 2016

Gints Mākalnietis, CERT.LV

- **Aktīvs krāpniecības veids kopš 2015. gada beigām**
 - **Ievērojami zaudējumi : 10000-200000 EUR**
 - **Galvenie cietēji – preču eksportētāji un to ārzemju klienti**
 - **Izteikti daudz kokapstrādes uzņēmumu**
 - **Krāpšana netiek pamanīta vairākas dienas vai mēnešus**

- **Krāpšana notiek izmantojot e-pasta saziņu**
 - **Nepieciešama piekļuve kāda darījumu partnera e-pastam – parole iegūta ar pikšķerēšanu, datorvīrusu**
 - **Ilgstoši vēro saraksti, viltotos dokumentus iesūta pareizajā brīdī**
 - **Reģistrē upurim līdzīgus domēnus, veido weblapu kopijas**
 - **E-pastos lieto pārlicinošus tekstus, lai upuri mainītu maksājuma detaļas**

Viltoti rēķini

- **Darbības pamanot maksājumu:**
 - izveido viltus domēnu e-pastu saņemšanai, līdzīgu upura sadarbības partnera lietotajam
 - Norāda to e-pasta «REPLAY-TO» laukā
 - Turpmākā sarakste notiek tikai starp krāpnieku un upuri
 - Var izmantot līdzīgu shēmu lai sazinātos ar maksājuma saņēmēju, sūtītu tam viltotus maksājuma uzdevumus lai novilcinātu laiku

Viltoti rēķini



An attempt to deliver a parcel to you was not successful due to incomplete delivery address supplied.

We will attempt to deliver your parcel within 3 working days.

Parcel ID: 6270980360/GHB

[Please download your necessary AWB here...](#)

Please expect your package within 3 working days.

Enjoy!

- Customer Support

DHL.... We deliver the world!

Note: Please do not reply to this email as it has been sent from an address that does not accept incoming mails. Please follow the above link to complete your address.

Viltoti rēķini

File name: Parcel ID 6270980360GHB.exe_
Detection ratio: 23 / 56
Analysis date: 2016-11-24 13:17:01 UTC (2 nedēļas, 4 dienas ago)



Analysis

File detail

Additional information



Comments 0

Votes

Behavioural information

| Antivirus | Result | Update |
|-------------------------|--|----------|
| AVG | Luhe.Fiha.A | 20161124 |
| AVware | Trojan.Win32.Generic.pak/cobra | 20161124 |
| Avast | Win32:Evo-gen [Susp] | 20161124 |
| Avira (no cloud) | TR/Dropper.MSIL.kopuo | 20161124 |
| Baidu | Win32.Trojan.WisdomEyes.16070401.9500.9999 | 20161124 |
| CAT-QuickHeal | TrojanSpy.Agent | 20161124 |
| Comodo | TrojWare.MSIL.TrojanDropper.Injector.QFM | 20161124 |
| CrowdStrike Falcon (ML) | malicious_confidence_100% (D) | 20161024 |
| ESET-NOD32 | a variant of MSIL/Injector.QFM | 20161124 |
| Fortinet | MSIL/Injector.QFM!tr | 20161124 |
| GData | MSIL.Trojan.Injector.JF | 20161124 |

Viltoti rēķini

| | |
|---|---|
| imphash  | f34d5f2d4577ed6d9ceec516c1f5a744 |
| File size | 709.4 KB (726440 bytes) |
| File type | Win32 EXE |
| Magic literal | PE32 executable for MS Windows (GUI) Intel 80386 32-bit Mono/.Net assembly |
| TrID | Win32 Executable MS Visual C++ (generic) (41.0%) Win64 Executable (generic) (36.3%) Win32 Dynamic Link Library (generic) (8.6%) Win32 Executable (generic) (5.9%) Win16/32 Executable Delphi generic (2.7%) |
| Tags | peexe assembly overlay |
|  VirusTotal metadata | Vīruss upura datorā saņemts 10.09.2016! |
| <u>First submission</u> | 2016-11-24 13:17:01 UTC (2 nedēļas, 4 dienas ago) |
| Last submission | 2016-11-24 13:17:01 UTC (2 nedēļas, 4 dienas ago) |
| File names | Parcel ID 6270980360GHB.exe_ |

Viltoti rēķini

«I write to inform you that our Bankas - Swedbank, AB has been frozen this morning following the tax evasion allegation leveled against our company by our government. (find attached for detail)

For this reason, be advised not to remit the outstanding payment of 11108 EUR to the account until we furnish you with the account of our Parent company abroad for this payment.

Thanks for your understanding.»

Viltoti rēķini



Sąskaitos data/Issue date 2016-04-12

[REDACTED]
Pardavējas/Consignee
UAB [REDACTED]
Mācību iestāde: LT-93234, Klaipēda
Tel./faksas: +370 [REDACTED]
Im.kodas 1 [REDACTED]
PVM kodas LT4C [REDACTED]
Sąsk. nr. LT9373000: [REDACTED]
Bankas - Swedbank, AB
Banko kodas 73000
Paysera sąskaitos nr: EVP0 [REDACTED]
Bendrovė įregistruota juridinių asmenų registre
Valstybės įmonės Registrų centras, Klaipėdos
filialas registravimo Nr. 121534

UPDATED REMITTANCE INSTRUCTION

THE ACCOUNTANT,
SIA [REDACTED]
JMK [REDACTED]
PVM MOK.K.: LV4 [REDACTED]
REGISTRACIJOS ADRESAS:
[REDACTED] RIGA, LATVIJA

DEAR SIR/MADAM,

SUBSEQUENT TO THE RESOLUTION OF THE MANAGEMENT OF FIRST LOGISTICS UAB, BE INFORMED THAT THE UNDER LISTED ACCOUNT IS DESIGNATED FOR THE RECEIPT OF OUTSTANDING AND FUTURE PAYMENTS TO OUR COMPANY.

THIS DECISION IS BASED ON THE FACT THAT OUR REGULAR BANK ACCOUNT IS NOT ACTIVE TO RECEIVE PAYMENT DUE TO THE TAX EVASION ALLEGATION LEVELLED AGAINST OUR COMPANY BY OUR GOVERNMENT AS YOU WERE HIGHLIGHTED IN THE EARLIER TODAY.

OUR TEAM OF LAWYERS ARE WORKING ASSIDUOUSLY ON THE MATTER AND WE HAVE BEEN ASSURED THAT IT SHOULD BE RESOLVED NOT LATTER THAN END OF APRIL 2016. CONSEQUENTLY, OUR BOARD OF DIRECTORS HAS PASSED A RESOLUTION STATING THAT HENCEFORTH EVERY PENDING PAYMENT ARISING FROM WIRE TRANSFERS, LC AND CHEQUES SHOULD BE MADE THROUGH OUR PARENT COMPANY ACCOUNT IN UNITED KINGDOM AS STATED BELOW:

NATWEST BANK PLC
1-7 POWIS STREET
WOOLWICH.UK
SWIFT: NWBKGB2L
IBAN: GB32NWBK60242611327758
ACCOUNT NAME: LUBEGA JDK: [REDACTED]

THANKS FOR YOUR ANTICIPATED CO-OPERATION TO THIS OFFICIAL DIRECTIVE.

YOURS FAITHFULLY,

[REDACTED]
[REDACTED] AB
LT-93234 Klaipėda, Lithuania
Tel: +370 [REDACTED]
MŪSŲ TŪLUMS [REDACTED]

Viltoti rēķini

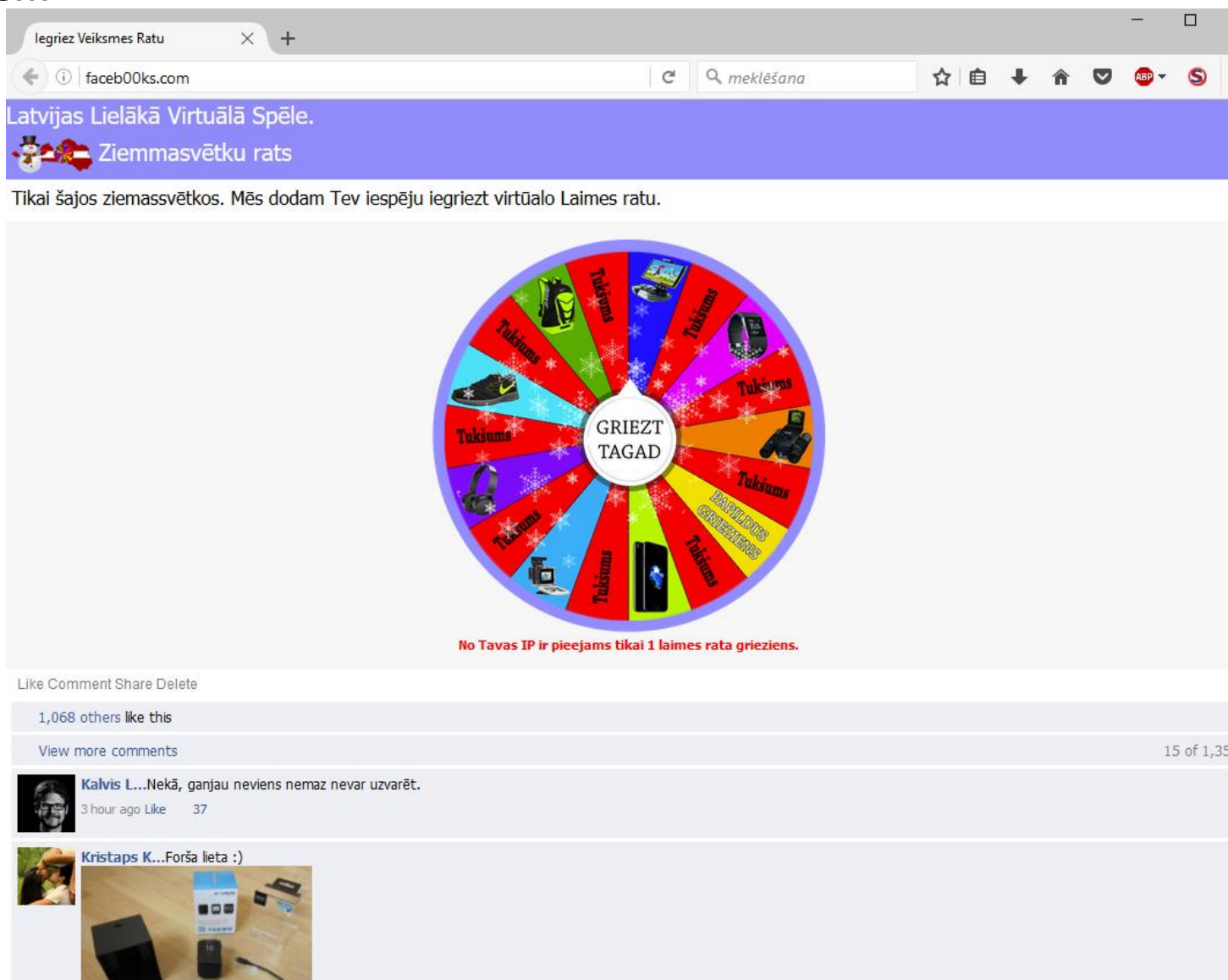
The screenshot shows a web browser window with the address bar containing '-sia.eu/Kontakts/'. The page features a logo with a tree and the letters 'SIA' on a green ribbon. Below the logo are three navigation buttons: 'Sākt', 'Produkcija', and 'Kontakts', with 'Kontakts' being the active one. The main content area has a teal background and is titled 'Kontakts'. It contains the following text:

Informācija par uzņēmumu
Reģistrācijas numurs 40003[redacted]
PVN LV40003315941
SEPA identifikators LV64ZZ40003[redacted]
Juridiskā adrese Kurzemes prospekts 3[redacted] Rīga, LV-1067
+371271[redacted]
kontakts@[redacted]-sia.eu

Below the text are three images: a variety of fresh fruits including watermelon, bananas, and apples; a display of fresh meat cuts; and several crates filled with fresh vegetables like tomatoes, onions, and carrots.

Viltus loterijas

- Lietotāji tiek pievilināti ar reklāmām, apmeklējot dažādas vietnes no mobilajiem telefoniem



legriez Veiksmes Ratu

faceb00ks.com

Latvijas Lielākā Virtuālā Spēle.

Ziemmasvētku rats

Tikai šajos ziemassvētkos. Mēs dodam Tev iespēju iegriezt virtuālo Laimes ratu.

GRIEZT TAGAD

No Tavas IP ir pieejams tikai 1 laimes rata grieziens.

Like Comment Share Delete

1,068 others like this

View more comments 15 of 1,356

Kalvis L...Nekā, ganjau neviens nemaz nevar uzvarēt.
3 hour ago Like 37

Kristaps K...Forša lieta :)

Viltus loterijas


```
713 <script type="text/javascript">
714   function spinnerAction() {
715     //alert("Welcome to Lucky Wheel!\n\nSpin the Wheel and you may win exclusive prizes!\n\nClick OK to Start the Game!")
716   }
717
718   function startSpin() {
719     var e = document.getElementById("spin"),
720         n = document.getElementById("win"),
721         t = document.getElementById("winP"),
722         o = document.getElementById("win2");
723     e.className = e.className + "spinAround", n.style.display = "none", t.style.display = "block", setTimeout(function() {
724       t.style.display = "none", o.style.display = "block"
725     }, 150), setTimeout(function() {
726       alert(" Apsveicam!\n\n Jūs uzgriezāt Papildus griezienu.\n\n Jums ir iespēja griez laimes ratu velreiz."), spin2enabled = !0
727     }, 6500)
728   }
729
730   function spin2() {
731     if (spin2enabled) {
732       var e = document.getElementById("spin"),
733           n = document.getElementById("win"),
734           t = document.getElementById("winP"),
735           o = document.getElementById("win2");
736       e.className = e.className + " spinAround2", n.style.display = "none", t.style.display = "block", setTimeout(function() {
737         t.style.display = "none", o.style.display = "block"
738       }, 150), setTimeout(function() {
739         var e = alert("Apsveicam!\n\n Jūs Uzgriezāt Apple iPhone 7 (Black, 32GB). \n\n ");
740         e === !0 || $(".hide-all").hide(), $(".show-all").show();
741         var n = 299,
742             t = setInterval(function() {
743               $("#countdown").text(n--), -1 == n && clearInterval(t)
744             }, 1e3);
745         javascript_countdown.init(300)
746       }, 6800)
747     }
748   }
749 }
```

Viltus loterijas

← → ↻ faceb00ks.com/laimesrats/ ☆

Latvijas Lielākā Veiksmes Spēle.
🎅🎁 Ziemasvētku balvas!


Apsveicam Tevi!



Apple Iphone 7 (Black, 32GB)

Par pateicību mums, pastāsti par savu veiksmi 10 saviem labākajiem draugiem izmantojot whatsapp

1. Uzspied 10x 'IETEIKT' pogu.
2. Spied 'TURPINĀT'

 **IETEIKT**

 **TURPINĀT**

Rezervācijas ilgums **0** sekundes

Viltus loterijas

← → ↻ ⓘ www.skill2win.net/lv-lv/m-avg/?tc=0&media=QY&cid=SPO9-1021



AVG Antivīrusu aizsardzība AVG mobilais

Ievadiet savu mobilā telefona numuru, lai instalētu

INSTALĒT

Pasaulē labākais antivīruss!

Vērtējums: **4.2** ★★★★★ 1 226 750 skatījumi

- Skenē lietotnes, korekcijas, multimedijus reāllaikā
- Ļauj interneta atrast/izsekot nozaudēto/nozagto tālruni ar Google Maps
- Nobloķē/nodzēs savu ierīci, lai aizsargātu savu privātumu
- Izdzēs lietotnes vai uzdevumus, kas palēnina ierīces darbību
- Droši pārlūko internet
- Kontrolē savu akumulatoru, glabāšanas un datu paketi
- Instalē tūlīt, palielini savu mobilā tālruņa drošību un pārsteidz sevi
- AVG AntiVirus - mobilā tālruņa programmatūras aizsardzība Android sistēmai. Ātra un vienkārša aizsardzība tavam tālrunim

Viltus loterijas

Šis ir abonēšanas pakalpojums. Pakalpojuma cena ir 2.90€ par katru saņemto īsziņu. Pakalpojums iekļauj 1 īsziņas nedēļā, 2.90€ nedēļā + operatora tarifi, ieskaitot GPRS datu pārraides maksu. Īsziņas nosūtīšanas maksa tiek piemērota saskaņā ar operatora standarta tarifiem. Lai pārtrauktu abonēšanu, sūtiet īsziņu STOP WB uz 1897. Lai varētu izmantot šo pakalpojumu, lūdzu, uzstādiet WAP/GPRS iestatījumus savā mobilajā telefonā. Lūdzu, atcerieties pārbaudīt iestatījumus. Papildu

Šifrējošie datorvīrusi

- **CryptoWall + Locky**
 - Šifrē lietotāja dokumentus, kā arī failus koplietošanas mapēs uz servera
 - Dzēš shadow files rezerves kopijas
 - Sazinās ar serveriem jau pēc dokumentu šifrēšanas
 - Maksājumus pieņem Bitcoin

Šifrējošo vīrusu mērķi

- **Mērķauditorija**
 - Grāmatveži
 - Uzņēmumu vadītāji
 - Juristi
 - Lietvedes

Viens inficēts dators var sabojāt visus datus uz servera!

Šifrējošo vīrusu izplatība

- **Visbiežāk vīrusi vai to lejupielādes rīki tiek izplatīt e-pastā**
 - **Lai apietu antivīrusu programmas, tiek izmantotas novecojušas arhivācijas programmas – ARJ, ACE**
 - **70% infekciju – no Office failiem ar makro komandām - .DOCM, .DOT, .XLSM u.t.t.**
 - **Arhīvi ar skriptiem - .WSF, .WBS, .JS**
 - **AV programmas nedetektē jaunās vīrusu versijas**

Inficēts dokuments

17.10.2016

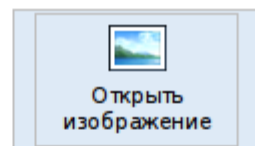
Данный файл поддерживается на системах **Windows XP и выше**



1С-Предприятие
Скан-копия №4-18

Данный документ был экспортирован при помощи 1С-Предприятие

Для просмотра, **нажмите 2 раза** на приложенный документ:



17.10.2016 Вячеславский О.А.

Lokalizēta versija - CTB-Locker

Jūsu datora faili ir nošifrēti ar CTB-Locker.



Jūsu datora faili ir nošifrēti ar CTB-Locker.

Jūsu dokumenti, bildes, datubāzes un citi svarīgi faili tika nošifrēti ar neuzlaužamu šifrēšanas algoritmu un atslēgu ģenerētu šim datoram.

Privātā atslēga failu atšifrēšanai ir noglabāta slēptā interneta serverī un nevienam nav iespējas atšifrēt jūsu failus tikmēr, kamēr jūs nesamaksāsit prasīto summu lai saņemtu privāto atslēgu.

Jums ir tikai 96 stundas laika, lai nosūtītu maksājumu. Ja jūs neveicat maksājumu norādītajā laikā, visi jūsu faili paliks neatgriezeniski nošifrēti un neviens nevarēs tos atšifrēt.

Nospiežat 'Apskatīt' lai apskatītu sarakstu ar failiem kas tika nošifrēti.

Nospiežat 'Turpināt' lai turpinātu uz nākošo lapu.



UZMANĪBU! NEMĒĢINIET IZDZĒST PROGRAMMU PAŠI. JEBKĀDAS DARBĪBAS LAI DZĒSTU PROGRAMMU IZRAISĪS ATŠIFRĒŠANAS ATSLĒGAS IZNĪCINĀŠANU. JŪS NEATGRIEZENISKI PAZAUDĒSIET SAVUS FAILUS. VIENĪGAIS VEIDS, KĀ SAGLABĀT SAVUS FAILUS IR SEKOT INSTRUKCIJĀM.

Apskatīt

95 : 52 : 30

Turpināt >>

- **CTB-Locker**
 - **CTB-Locker brīdinājums ir iztulkots arī latviešu valodā**
 - **Izplatītāji labi pārzina vietējos apstākļus**
 - **Aizdomu mazināšanai izmanto Latvijā populārus failu apmaiņas servisu**
 - **Operatīvi maina krāpniecisko e-pastu veidu**

Internetbanku datorvīrusi

- **Zeus + Dyre+ Dridex**
 - Pielāgotas versijas vairāku Latvijas internetbanku maksājumu pārtveršanai
 - Izplata e-pasta pielikumos
 - Izmanto Upatree lejupielādes rīku, kas pēc aktivizācijas saņem aktuālo vīrusa versiju

- **Kampanu īpatnības**

- Inficēto e-pastu saņēmēju loks mēdz būt ļoti ierobežots – tikai noteikti uzņēmumi, uz dažām e-pasta adresēm
- Pārskaitītās summas tiek ātri pārvērstas skaidrā naudā
- Inficētos datorus izmanto kā starpniekus citu kontu apzagšanā

DDoS4BC

- **Armada izspiešanas uzbrukumi**

From: Armada Collective <emailimportant@protonmail.com>
Date: 2016-04-10 0:48 GMT+03:00
Subject: DDOS ATTACK
To:

FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE DECISION!

We are Armada Collective.
<http://lmgtfy.com/?q=Armada+Collective>

You will be DDoS-ed starting Friay (April 15) if you don't pay protection fee - 25 Bitcoins @ 1LkNZUBGhuPobxVJTWHRDCcUW9XPXUPFLM
If you don't pay by Friday, attack will start, yours service going down permanently price to stop will increase to 50 BTC and will go up 20 BTC for every day of attack.

This is not a joke.
Our attacks are extremely powerful - sometimes over 1 Tbps per second. And we pass CloudFlare and others remote protections!
So, no cheap protection will help.

Prevent it all with just 25 BTC @ 1LkNZUBGhuPobxVJTWHRDCcUW9XPXUPFLM

Do not reply, we will not read. Pay and we will know its you. AND YOU
WILL NEVER AGAIN HEAR FROM US!
Bitcoin is anonymous, nobody will ever know you cooperated.

- **Reāli DDOS uzbrukumi nekad nav sekojuši!**
- **Mūsu ieteikumi līdzīgiem gadījumiem:**
 - **Nekomunicēt ar izspiedējiem**
 - **Apzināt kritiskos servissus un izstrādāt to nepārtrauktības un aizsardzības plānu**
 - **Sazināties ar interneta pieslēguma nodrošinātājiem, lai vienotos par rīcību uzbrukuma gadījumā**

- **Mūsu ieteikumi līdzīgiem gadījumiem:**
 - Izmantot mākoņpakalpojumu vai datu plūsmas «tīrīšanas» servisu, lai nodrošinātu pakalpojumu pieejamību
 - Optimizēt pakalpojumu sniegšanas platformas, padarot tās neuzņēmīgākas pret pārslodzes uzbrukumiem

IoT – Lets play with those toys



IoT – Mirai botnet



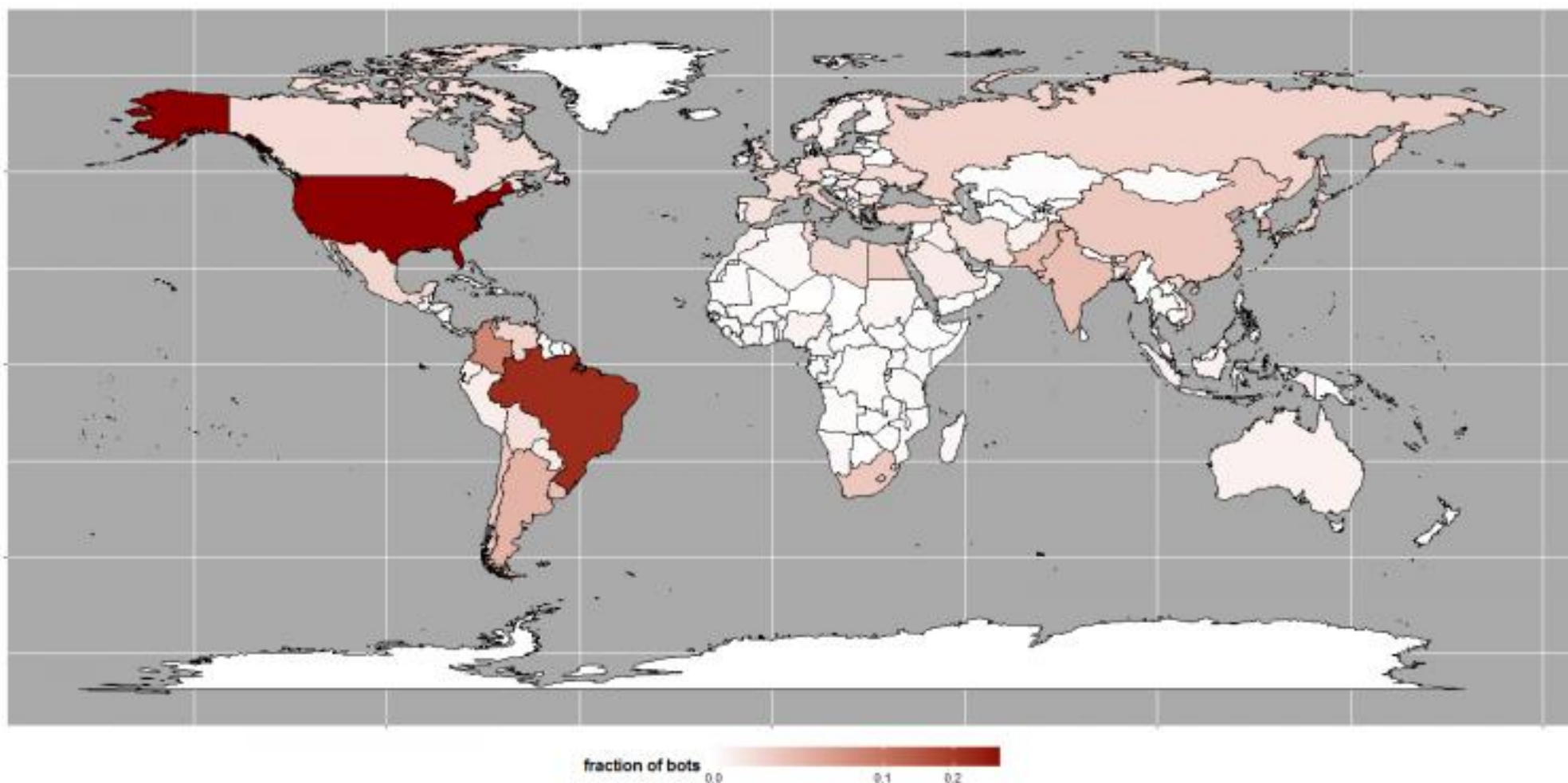
1 766 107 bots

| Username/Password | Manufacturer |
|-------------------|-------------------------|
| | |
| admin/123456 | ACTi IP Camera |
| root/anko | ANKO Products DVR |
| root/pass | Axis IP Camera, et. al |
| root/vizxv | Dahua Camera |
| root/888888 | Dahua DVR |
| root/666666 | Dahua DVR |
| root/7ujMko0vizxv | Dahua IP Camera |
| root/7ujMko0admin | Dahua IP Camera |
| 666666/666666 | Dahua IP Camera |
| root/dreambox | Dreambox TV receiver |
| root/zlxx | EV ZLX Two-way Speaker? |
| root/juantech | Guangzhou Juan Optical |
| root/xc3511 | H.264 - Chinese DVR |
| root/hi3518 | HiSilicon IP Camera |
| root/klv123 | HiSilicon IP Camera |
| root/klv1234 | HiSilicon IP Camera |
| root/jvzbd | HiSilicon IP Camera |

IoT – Mirai source code

```
1 // Set up passwords
2 add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x41\x11\x17\x13\x13", 10); // root xc3511
3 add_auth_entry("\x50\x4D\x4D\x56", "\x54\x4B\x58\x5A\x54", 9); // root vizxv
4 add_auth_entry("\x50\x4D\x4D\x56", "\x43\x46\x4F\x4B\x4C", 8); // root admin
5 add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C", 7); // admin admin
6 add_auth_entry("\x50\x4D\x4D\x56", "\x1A\x1A\x1A\x1A\x1A\x1A", 6); // root 888888
7 add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x4F\x4A\x46\x4B\x52\x41", 5); // root xmhdipc
8 add_auth_entry("\x50\x4D\x4D\x56", "\x46\x47\x44\x43\x57\x4E\x56", 5); // root default
9 add_auth_entry("\x50\x4D\x4D\x56", "\x48\x57\x43\x4C\x56\x47\x41\x4A", 5); // root juantech
10 add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17\x14", 5); // root 123456
11 add_auth_entry("\x50\x4D\x4D\x56", "\x17\x16\x11\x10\x13", 5); // root 54321
12 add_auth_entry("\x51\x57\x52\x52\x4D\x50\x56", "\x51\x57\x52\x52\x4D\x50\x56", 5); // support support
13 add_auth_entry("\x50\x4D\x4D\x56", "", 4); // root (none)
14 add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x52\x43\x51\x51\x55\x4D\x50\x46", 4); // admin password
15 add_auth_entry("\x50\x4D\x4D\x56", "\x50\x4D\x4D\x56", 4); // root root
16 add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17", 4); // root 12345
17 add_auth_entry("\x57\x51\x47\x50", "\x57\x51\x47\x50", 3); // user user
18 add_auth_entry("\x43\x46\x4F\x4B\x4C", "", 3); // admin (none)
19 add_auth_entry("\x50\x4D\x4D\x56", "\x52\x43\x51\x51", 3); // root pass
20 add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C\x13\x10\x11\x16", 3); // admin admin1234
21 add_auth_entry("\x50\x4D\x4D\x56", "\x13\x13\x13\x13", 3); // root 1111
22 add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x51\x4F\x41\x43\x46\x4F\x4B\x4C", 3); // admin smcadmin
23 add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x13\x13\x13\x13", 2); // admin 1111
24 add_auth_entry("\x50\x4D\x4D\x56", "\x14\x14\x14\x14\x14\x14", 2); // root 666666
25 add_auth_entry("\x50\x4D\x4D\x56", "\x52\x43\x51\x51\x55\x4D\x50\x46", 2); // root password
26 add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16", 2); // root 1234
```

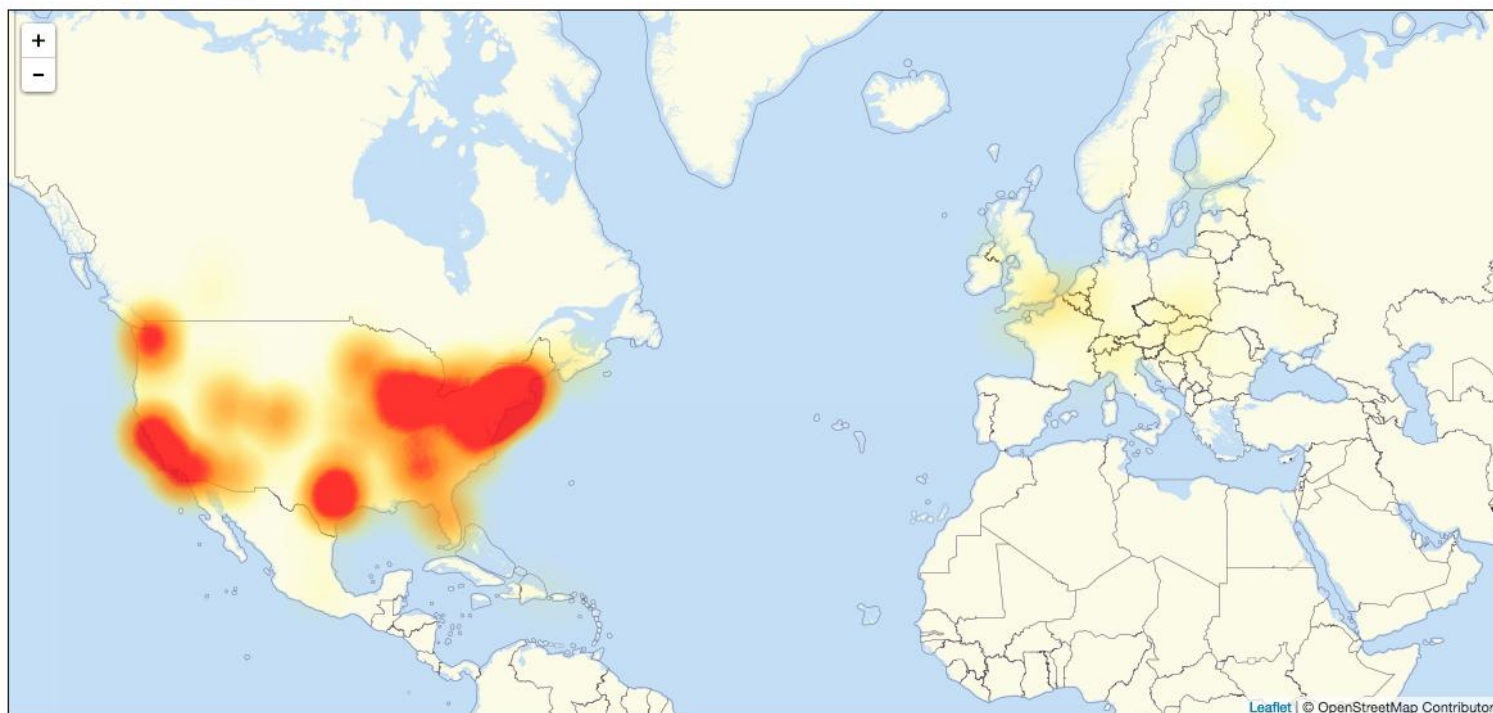
- Mirai botu izvietojums



- MIRAI DDOS 21.10.2016
- 900Gbps – 1Tbps DYN DNS -
iespaido Twitter, Amazon, Tumblr, Reddit,
Spotify, Netflix, Sony PlayStation

Level3 outage map

Level3 outage chart



Pikšķerēšana

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



From: ***Google*** <no-reply@accounts.google.com.mail.com>
Date: Thursday, 13 October 2016
Subject: Government-backed attackers may be trying to steal your password
To: [REDACTED]

Attackers may be trying to steal your password

Hi

There's a chance this is a false alarm, but we believe that government-backed attackers may be trying to trick you to get your Google Account password. We can't reveal what tipped us off because these attackers will adapt, but this happens to less than 0.1% of all Gmail users. If they succeed, they can spy on you, access your data, or take other actions using your account. We recommend change password.

Change password <[https://www.google.com/amp/tinyurl.com/\[REDACTED\]](https://www.google.com/amp/tinyurl.com/[REDACTED])>

Best,

The Mail Team

© 2016 Google Mail Corp., 1231 Amphithaetre Parkway, Mountain View, CA 98453, USA



Password

Choose a strong password and don't reuse it for other accounts. [Learn more.](#)

Changing your password will sign you out of all your devices, including your phone. You will need to enter your new password on all your devices.

Password

New password

Use at least 8 characters. Don't use a password from another site, or something too obvious like your pet's name. [Why?](#)

Confirm new password


CHANGE PASSWORD



From Paypal Inc <Paypal@int.com>★
Subject **Your account PayPal will be deleted if you don't confirm it** 2015.11.04. 14:16

From Paypal Service <PayPal@service.cc>★
Subject ✓ **[PayPal] Alert ! : Your Account Pay Will Be Limited.** 2015.11.07. 22:55

To [Redacted]



Your Account Will Be Limited.

Dear customer,

Your Account Will Be Limited , Until We Here From You . To Update Your Info . Simply click on the web address below

[Update Your Info](#)

Update Your Account [Update Now](#)

Help Center Partner Directory Logo Center Security Business Center



Notice of changes to the *PayPal* user agreement.

Dear Customer,

Log in to your *PayPal* account as soon as possible

- We have recently encountered a problem in your account.
- when you created your *PayPal* account to make sure you're the account holder
- Click the Activation link and Follow the instructions. !

[ACTIVATE ACCOUNT](#)

Get more out of your account

Now is the time to make your *PayPal* account even more useful:

Account Overview

- Get up-to-date information about your payments.
- Add or withdraw money from your *PayPal* account.
- See a detailed transaction history.

Yours sincerely,
PayPal

Please Sign In

Secure

Enter your Apple ID and password

Forgot your Apple ID or Password?

Sign In

You can use your Apple ID for other Apple services such as

- iTunes Store
- iPhoto Print Products
- iCloud

Create Apple ID now

Cancel

Questions? Just ask. 1-800-MY-APPLE

My Apple ID

Sign In to iTunes Connect

Please Sign In to you Apple ID to resolve the problem.

Apple ID

Password

Sign In

[Forgot your Apple ID or password?](#)



Give the gift
of iTunes.

Music, movies, apps, and more.



(RED)

(PRODUCT)RED

Red is a good color for you.
And millions of others.

Apple source code

```
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<?php
/*


|                    |
|--------------------|
| PRIVATE Apple SCAM |
| BY Mister Spy Tn   |

http://www.facebook.com/tazspy
*/
?>

<html>
<head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<title>iTunes Connect</title>
<link rel="icon" href="http://im53.gulfup.com/Qhffdz.ico">

<style>
.btn {
background: #3baee7;
background-image: -webkit-linear-gradient(top, #3baee7, #08c);
background-image: -moz-linear-gradient(top, #3baee7, #08c);
background-image: -ms-linear-gradient(top, #3baee7, #08c);
background-image: -o-linear-gradient(top, #3baee7, #08c);
background-image: linear-gradient(to bottom, #3baee7, #08c);
-webkit-border-radius: 7;
-moz-border-radius: 7;
border-radius: 7px;

```

Par 'draugiem.lv' lietotāju datu nelikumīgu iegūšanu aiztur trīs nepilngadīgos (3)

www.DELFI.lv | 23. maijs 2016 16:36



Follow @delfilv

102K followers




Valsts policija (VP) aizturējusi trīs 1999. gadā dzimušus jauniešus, kuri veikuši nelikumīgas darbības ar interneta vietnes "draugiem.lv" lietotāju datiem. Kratīšanas laikā policija izņēma datu nesējus, kuros bija vairāk nekā tūkstotis ar virtuālajām identitātēm, informē VP.

www.afterburn.ca/wp-content/pillx/inbox.htm

www.1a.lv

LAPTOP
STAND
TENT
TABLET



Lenovo
GRIEZ PASAULI
KAUT PAR
360°
IZVĒLIES

intel
inside™

BEZMAKSAS PIEGĀDE UZ DPD PICKUP

inbox

search internet



Sign Up

Login

English

e-mail

mail+

games

foto

dating

files

labeledarbi.lv

shop

travel

work

fun

sites

smart

city24.lv

NEW

classifieds

amigos

All products

Kindly Re-login below to complete verification

Username: @inbox.lv

Sign in

Password:

[Help](#) | [Forgot your password?](#)



Inbox.lv

Like Page 17K likes

Be the first of your friends to like this



Laimē ceļojumu uz Lieldienu salām vai Maurīciju!

Galvenais laimests

Nissan X-Trail!



Spēlēt

Weather

+2.0°C

Currency Rates

USD 1.0862 UAH 28.9381

Statistics

Registered users: 10344555

Friday, 4 March

Alise, Auca, Enija

Tendences 2016

- **Daudz krāpniecības gadījumu, upuris tiek pierunāts veikt pārskaitījumus uzbrucēja kontā, reti tiek izmantoti klasiski banku datorvīrusi**
- **Šifrējošie vīrusi vēl arvien tiek attīstīti, upuru skaits sarūk**
- **Nepieskatītas iekārtas kļūst par nopietnu apdraudējumu un uzbrukuma rīku**
- **Pikšķerēšana vēl arvien ir populārākais veids kā pārtvert paroles. Nelietojiet vienu paroli diviem resursiem!**



Paldies!

<http://www.cert.lv>

gints@cert.lv