Kiberuzbrukumu aktualitātes

Gints Mālkalnietis

10.12.2020

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

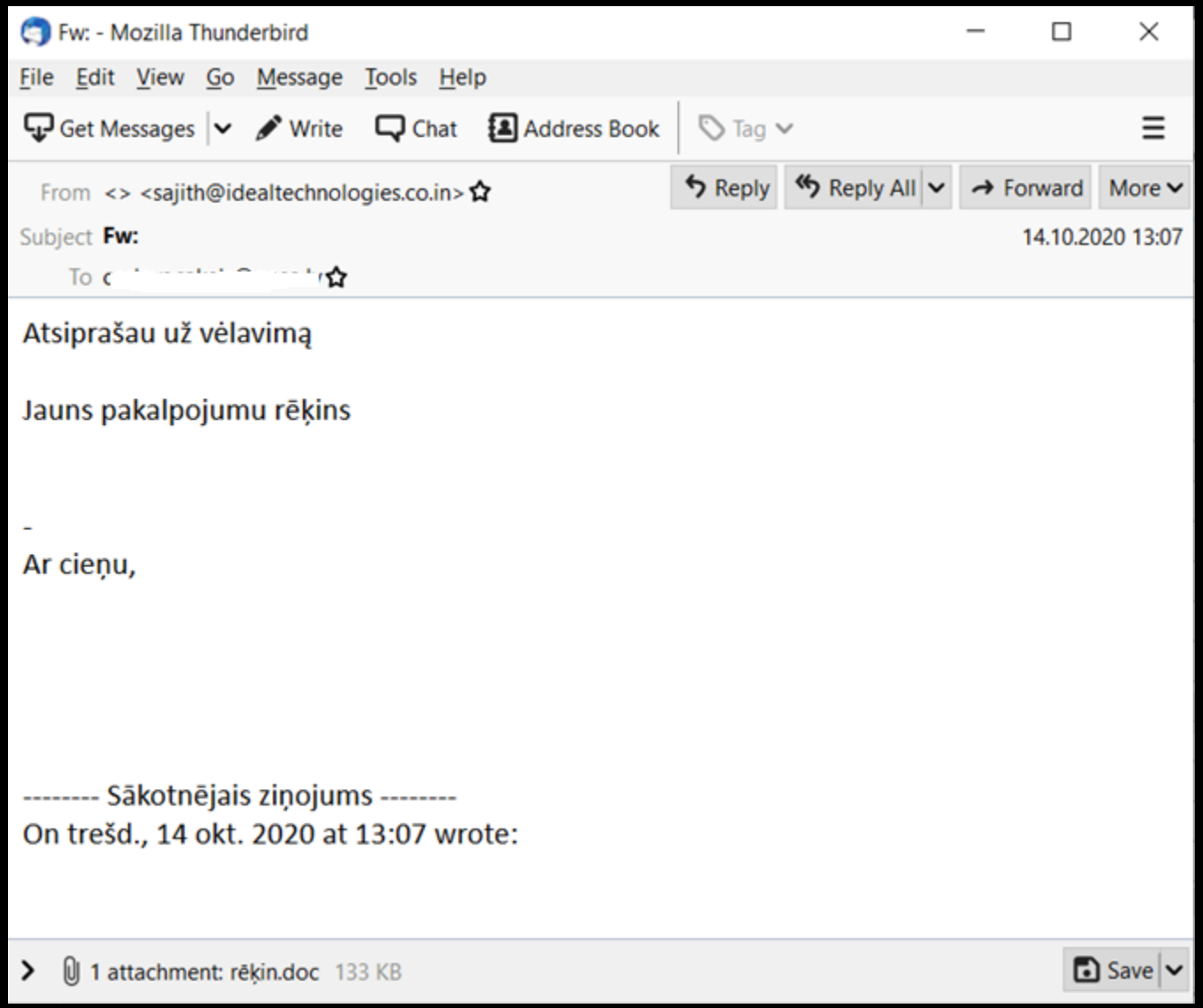
CERT.LV

Digitālā drošība šodien

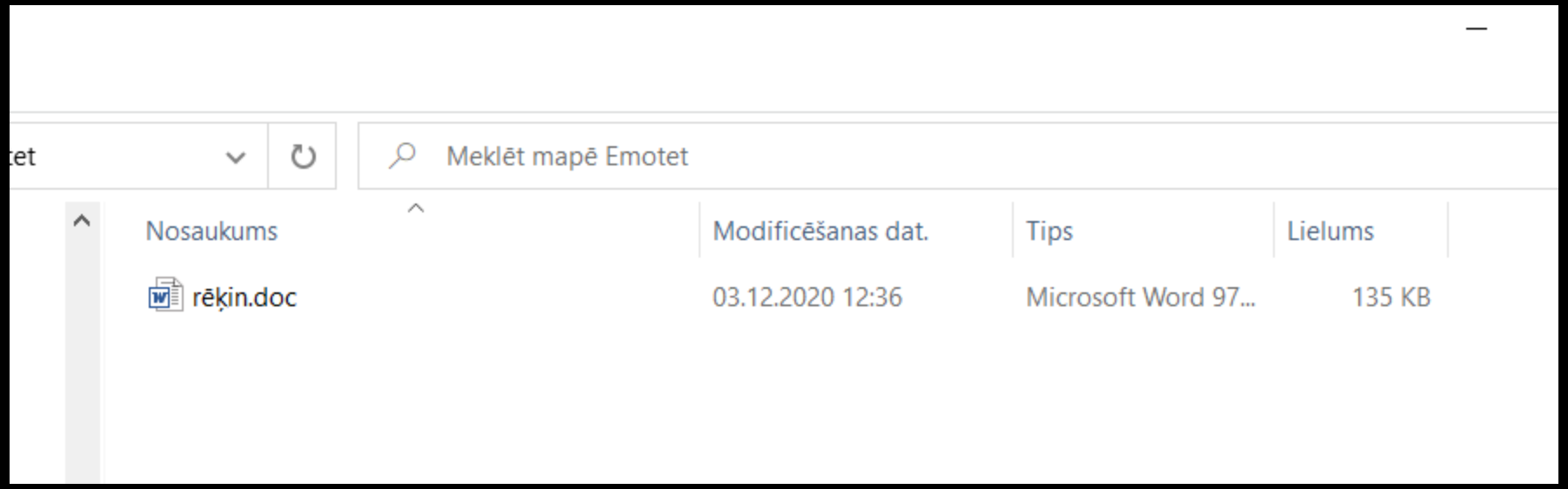
Darbs no mājām – vai kas jauns?

1. Daudzi uzņēmumi sākoties pandēmijai sākuši pastiprināti izmantot digitālos risinājumus
2. No mājām strādā un mācās daudz vairāk personu kā parasti
3. Lai nezaudētu biznesu, strauji tiek attīstīti tiešsaites veikali un citi pakalpojumi
4. Masveidā tiek izmantotas konferenču platformas
5. Pieaug portatīvo datoru tirdzniecība

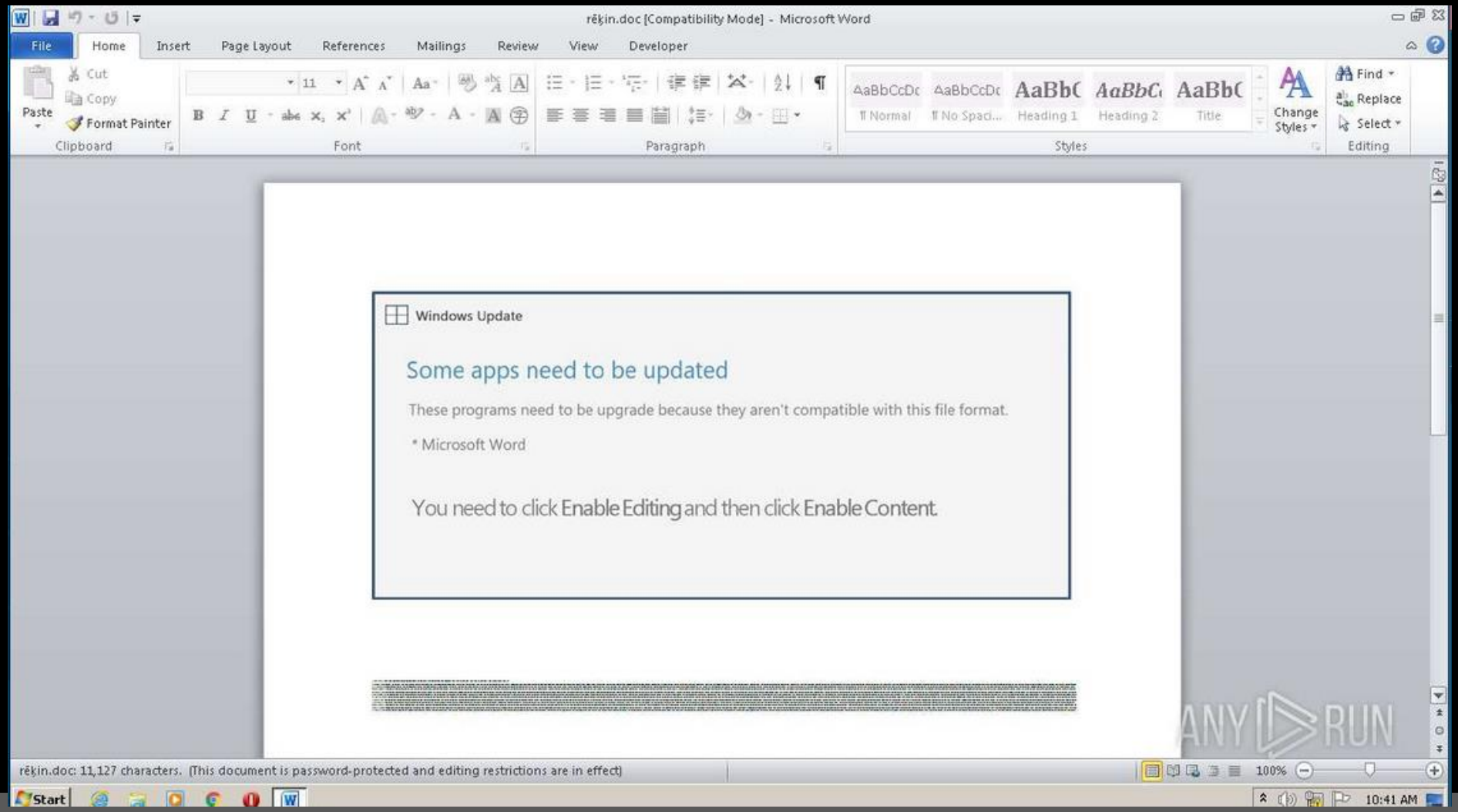
Emotet


Fw: - Mozilla Thunderbird
File Edit View Go Message Tools Help
Get Messages Write Chat Address Book Tag
From <> <sajith@idealtechnologies.co.in>
Reply Reply All Forward More
Subject Fw:
14.10.2020 13:07
To
Atsiprašau už vėlavimą
Jauns pakalpojumu rēķins
-
Ar cieņu,
-------- Sākotnējais ziņojums --------
On trešd., 14 okt. 2020 at 13:07 wrote:
1 attachment: rēķin.doc 133 KB
Save

Emotet


tet
Meklēt mapē Emotet
Nosaukums
Modificēšanas dat.
Tips
Lielums
rēķin.doc
03.12.2020 12:36
Microsoft Word 97...
135 KB

Emotet


rēķin.doc [Compatibility Mode] - Microsoft Word
File
Home
Insert
Page Layout
References
Mailings
Review
View
Developer
Paste
Cut
Copy
Format Painter
Clipboard
Font
Paragraph
Styles
Change Styles
Find
Replace
Select
Editing
Windows Update
Some apps need to be updated
These programs need to be upgrade because they aren't compatible with this file format.
* Microsoft Word
You need to click Enable Editing and then click Enable Content.
rēķin.doc: 11,127 characters. (This document is password-protected and editing restrictions are in effect)
100%
Start
10:41 AM

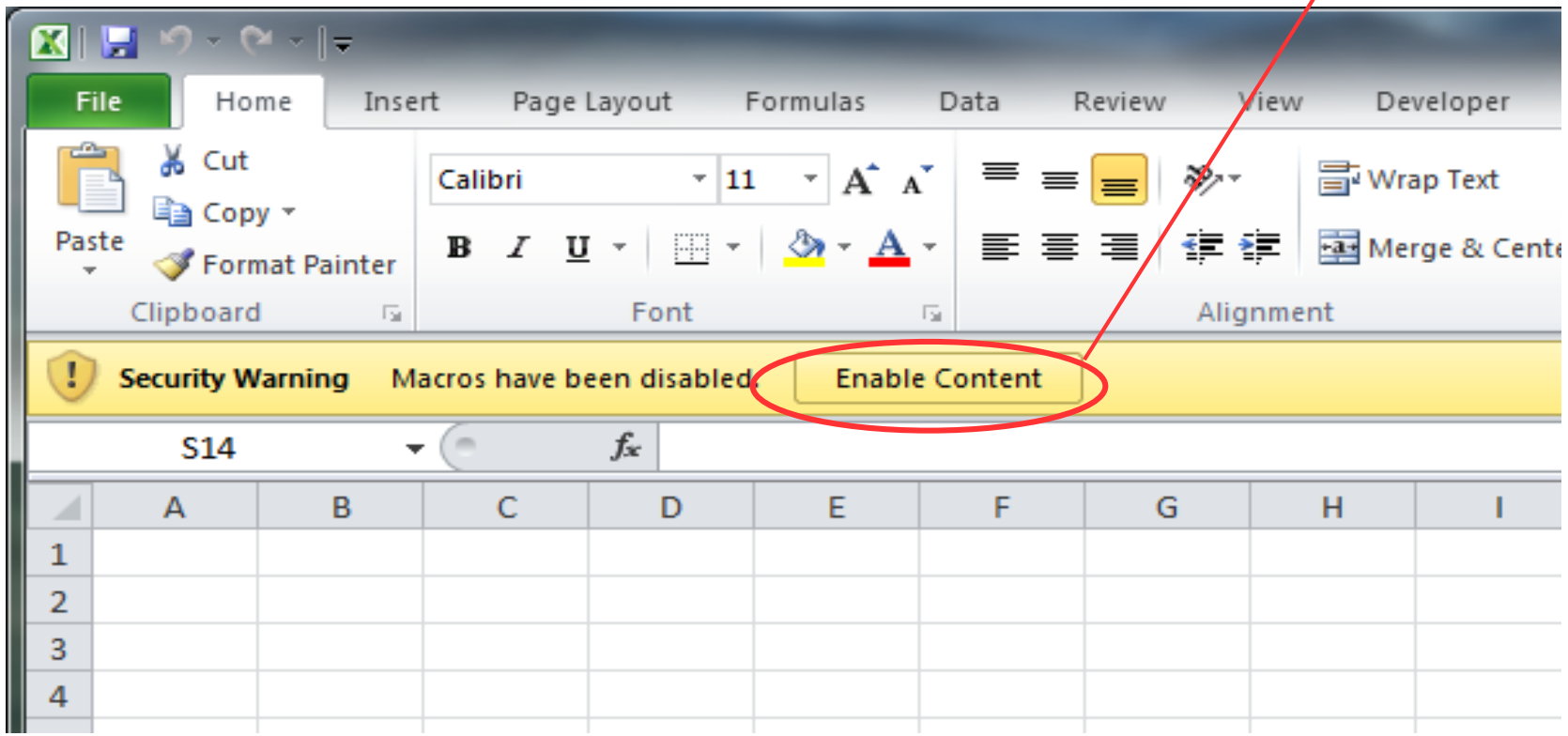
Emotet kampaņa

Aktīva 2020 gada vasarā-rudenī.
Izmanto MicrosoftOffice macro funkcijas, lai lejupielādētu un palaistu datorvīrusu.
Savāc paroles, e-pasta klientu adresu grāmatas saturu un reālas sarakstes paraugus.
Liels skaits upuru, it sevišķi būvniecības un projektēšanas uzņēmumos.
Tikai vīrusa autoru izvēle pasargā no ievērojamiem datu zudumiem, ko nodarītu datu šifrēšana!!

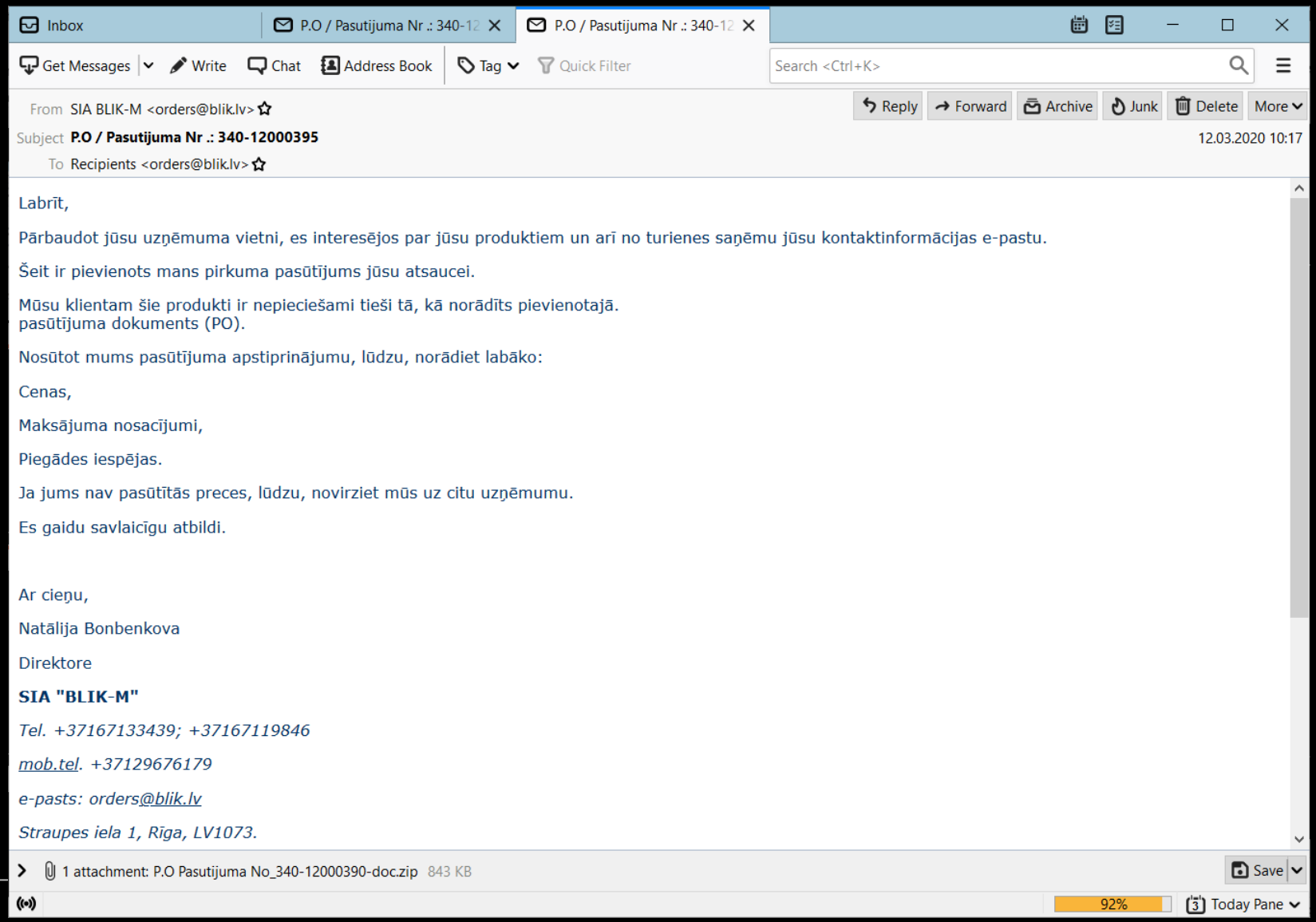
Macro un aktīvais saturs

Microsoft pēc noklusējuma ir
atspējojis automātisku Macros izpildi

Nespiežam!!!



Īsts vai viltots?



Inbox | P.O / Pasutijuma Nr .: 340-12 | P.O / Pasutijuma Nr .: 340-12

Get Messages | Write | Chat | Address Book | Tag | Quick Filter | Search <Ctrl+K>

Reply | Forward | Archive | Junk | Delete | More

From SIA BLIK-M <orders@blik.lv>

Subject **P.O / Pasutijuma Nr .: 340-12000395**

12.03.2020 10:17

To Recipients <orders@blik.lv>

Labrīt,

Pārbaudot jūsu uzņēmuma vietni, es interesējos par jūsu produktiem un arī no turienes saņēmu jūsu kontaktinformācijas e-pastu.

Šeit ir pievienots mans pirkuma pasūtījums jūsu atsaucei.

Mūsu klientam šie produkti ir nepieciešami tieši tā, kā norādīts pievienotajā.
pasūtījuma dokuments (PO).

Nosūtot mums pasūtījuma apstiprinājumu, lūdzu, norādiet labāko:

Cenas,

Maksājuma nosacījumi,

Piegādes iespējas.

Ja jums nav pasūtītās preces, lūdzu, novirziet mūs uz citu uzņēmumu.

Es gaidu savlaicīgu atbildi.

Ar cieņu,

Natālija Bonbenkova

Direktore

SIA "BLIK-M"

Tel. +37167133439; +37167119846

mob.tel. +37129676179

e-pasts: orders@blik.lv

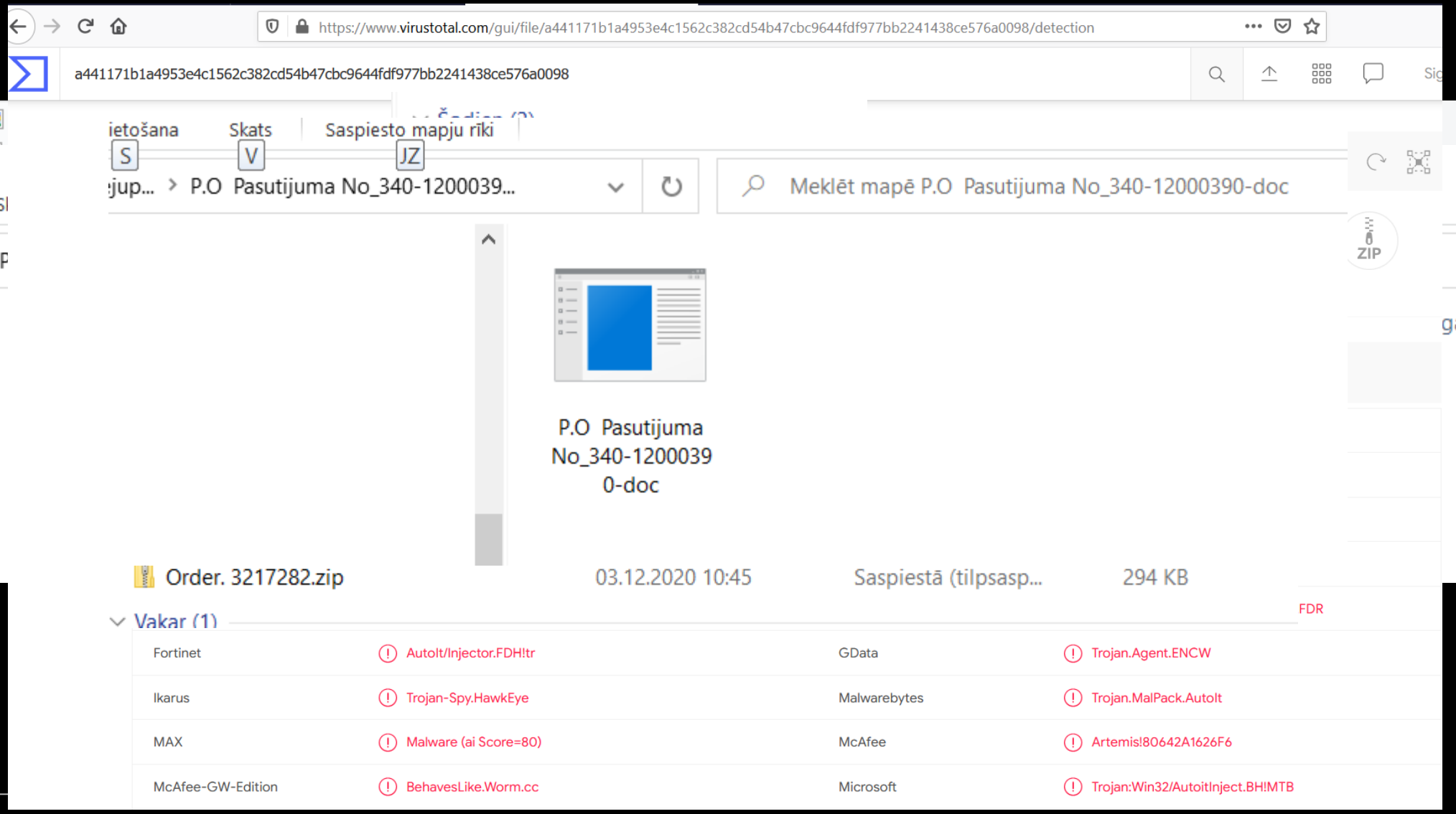
Straupes iela 1, Rīga, LV1073.

1 attachment: P.O Pasutijuma No_340-12000390-doc.zip 843 KB | Save

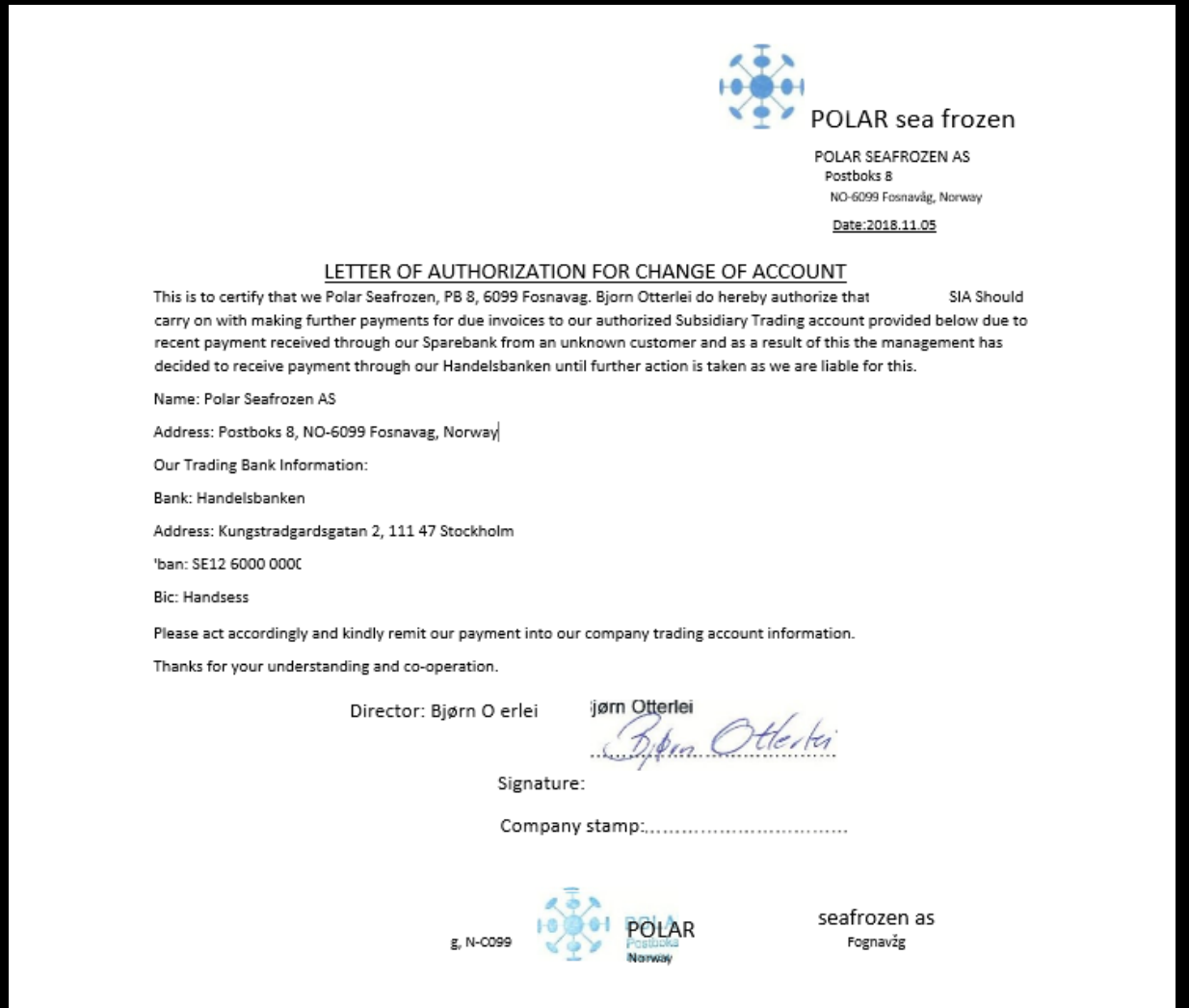
92% | Today Pane

CERT.LV

Īsts vai viltots?



Īsts vai viltots?



POLAR sea frozen

POLAR SEAFROZEN AS
Postboks 8
NO-6099 Fosnavåg, Norway

Date:2018.11.05

LETTER OF AUTHORIZATION FOR CHANGE OF ACCOUNT

This is to certify that we Polar Seafrozen, PB 8, 6099 Fosnavag. Bjorn Otterlei do hereby authorize that SIA Should carry on with making further payments for due invoices to our authorized Subsidiary Trading account provided below due to recent payment received through our Sparebank from an unknown customer and as a result of this the management has decided to receive payment through our Handelsbanken until further action is taken as we are liable for this.

Name: Polar Seafrozen AS

Address: Postboks 8, NO-6099 Fosnavag, Norway

Our Trading Bank Information:

Bank: Handelsbanken

Address: Kungstradgardsgatan 2, 111 47 Stockholm

'ban: SE12 6000 000(

Bic: Handsess

Please act accordingly and kindly remit our payment into our company trading account information.

Thanks for your understanding and co-operation.

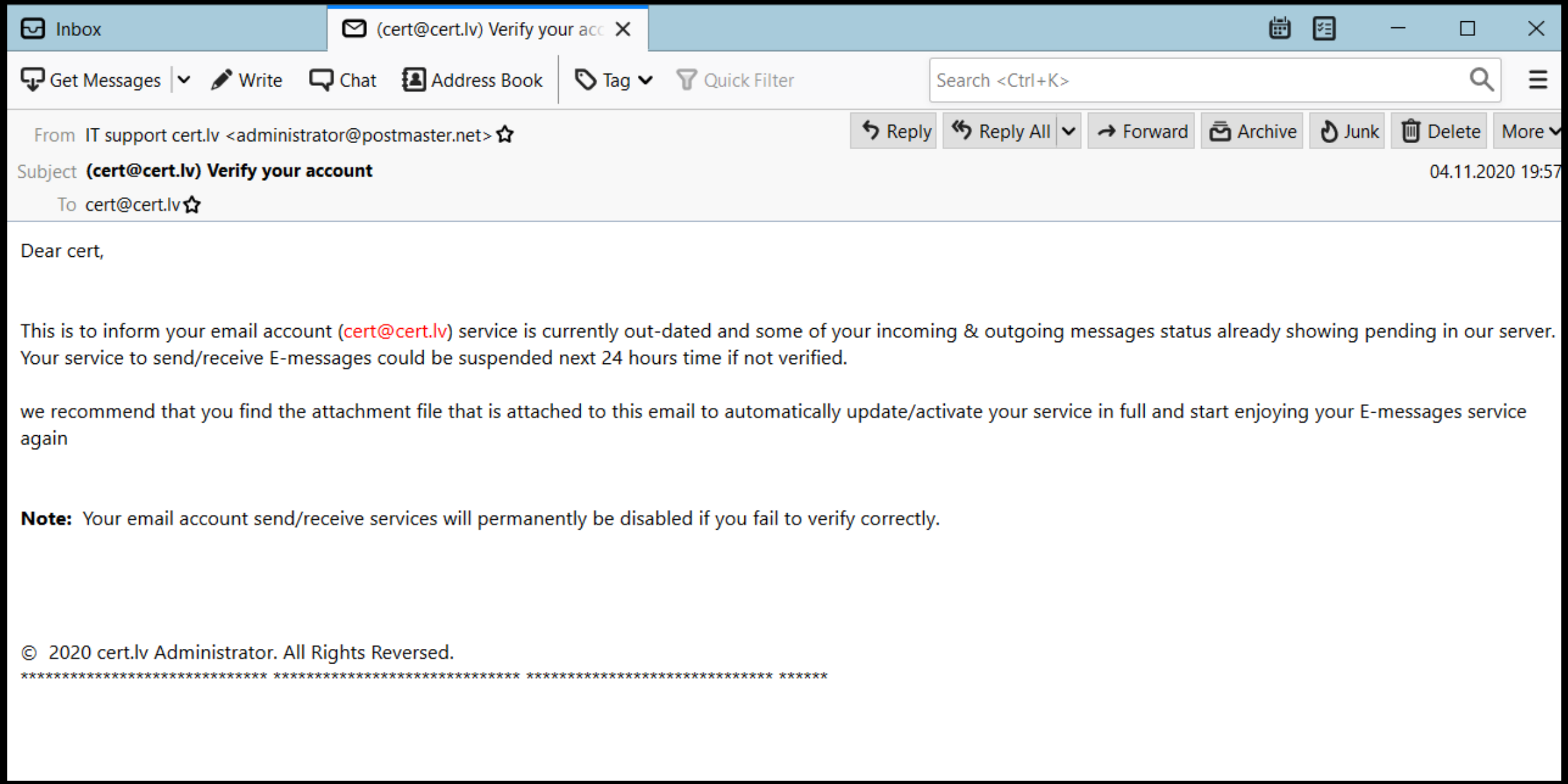
Director: Bjørn O erlei jørn Otterlei

Signature:

Company stamp:.....

g, N-0099 POLAR Norway seafrozen as Fognavåg

Īsts vai viltots?



Inbox | (cert@cert.lv) Verify your acc

Get Messages | Write | Chat | Address Book | Tag | Quick Filter | Search <Ctrl+K>

Reply | Reply All | Forward | Archive | Junk | Delete | More

From IT support cert.lv <administrator@postmaster.net>

Subject **(cert@cert.lv) Verify your account** 04.11.2020 19:57

To cert@cert.lv

Dear cert,

This is to inform your email account (cert@cert.lv) service is currently out-dated and some of your incoming & outgoing messages status already showing pending in our server. Your service to send/receive E-messages could be suspended next 24 hours time if not verified.

we recommend that you find the attachment file that is attached to this email to automatically update/activate your service in full and start enjoying your E-messages service again

Note: Your email account send/receive services will permanently be disabled if you fail to verify correctly.

© 2020 cert.lv Administrator. All Rights Reversed.

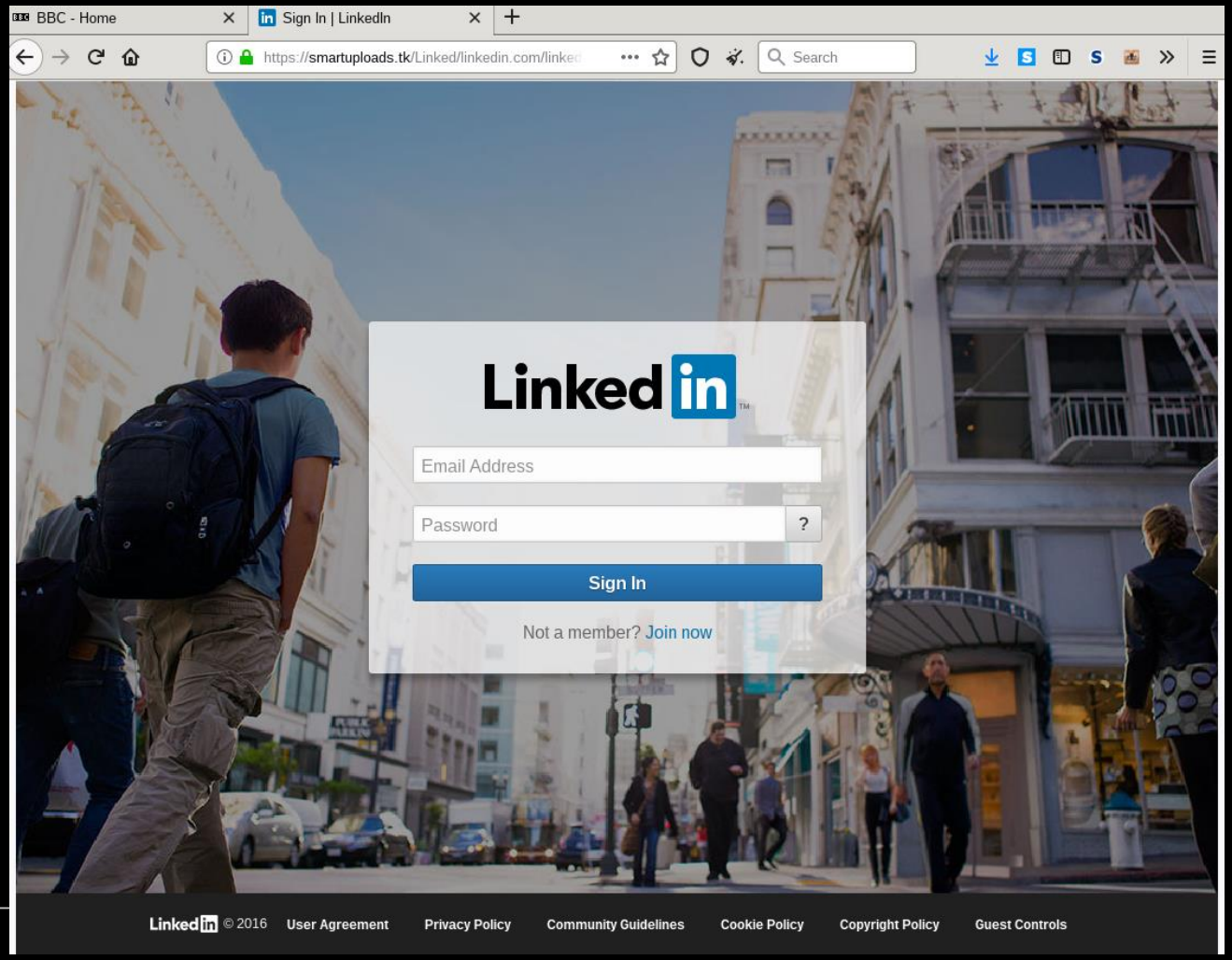
********** ********** ********** ******

Pikšķerēšana – vēl arvien darbojas!

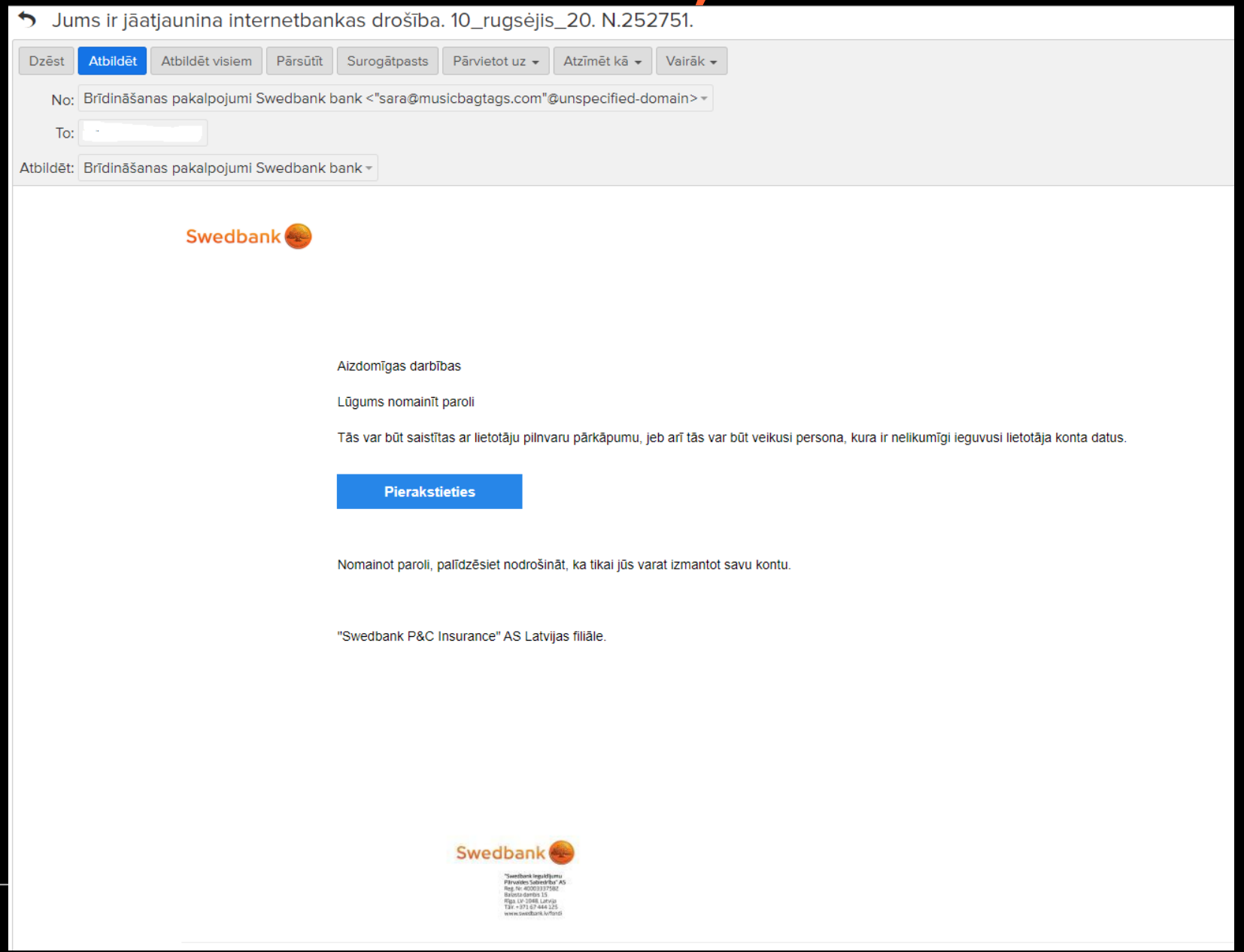
Cilvēki izmanto vienu paroli dažādiem resursiem
Vēlēšanās ātrāk iegūt pakalpojumu, neiedziļinoties detaļās
Nezina savstarpēji saistītus kontus
Piekļuve privātajam e-pastam var būt pirmais solis, lai iekļūtu uzņēmuma datortīklā!

CERT.LV

Nepārbaudām kur ievadām savus datus!



Uzbrukumi lai piekļūtu bankas kontam



Jums ir jāatjaunina internetbankas drošība. 10_rugsējis_20. N.252751.

Dzēst | Atbildēt | Atbildēt visiem | Pārsūtīt | Surogātpasts | Pārvietot uz | Atzīmēt kā | Vairāk

No: Brīdināšanas pakalpojumi Swedbank bank <"sara@musicbagtags.com"@unspecified-domain>

To:

Atbildēt: Brīdināšanas pakalpojumi Swedbank bank

Swedbank

Aizdomīgas darbības

Lūgums nomainīt paroli

Tās var būt saistītas ar lietotāju pilnvaru pārkāpumu, jeb arī tās var būt veikusi persona, kura ir nelikumīgi ieguvusi lietotāja konta datus.

Pierakstieties

Nomainot paroli, palīdzēsiet nodrošināt, ka tikai jūs varat izmantot savu kontu.

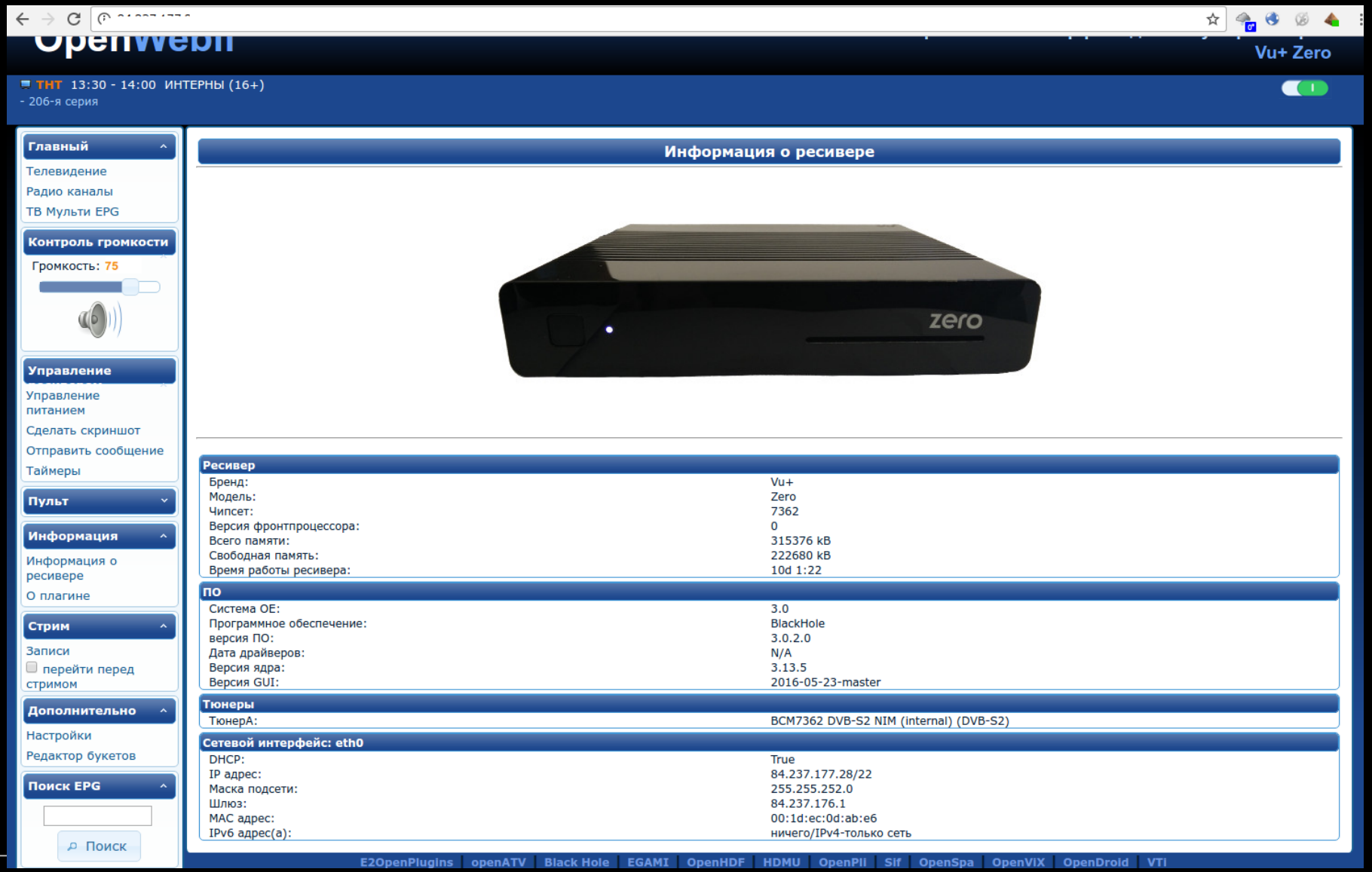
"Swedbank P&C Insurance" AS Latvijas filiāle.

Swedbank

Kā nozagt naudu?

1. Izmanto klientu ierobežotās zināšanas par bankas procedūrām
2. Klienti neizprot Smart-ID tehnoloģiju
3. Pamata dati tiek iegūti ar pikšķerēšanu un no atklātiem avotiem
4. Tiek veiktas masveida telefonzvanu kampaņas
5. Izmanto moderno tehnoloģiju ātrumu – nauda tiek izņemta no konta, pirms upuris saprot notikušo

Vai mājas datori ir drošāki?



Vai jūs ziniet cik jūsu mājās ir datori?

Ne visi datori izskatās vienādi!
Mājas datortīklos atrodas daudz neatjauninātas un neuzturētas iekārtas.
Tās var radīt datu drošības problēmas īpašniekam, darbavietai kurā tiek strādāts attālināti vai citiem interneta lietotājiem.
Sagatavojiet datorus ko lietotāji izmantos attālinātai piekļuvei darbavietai.

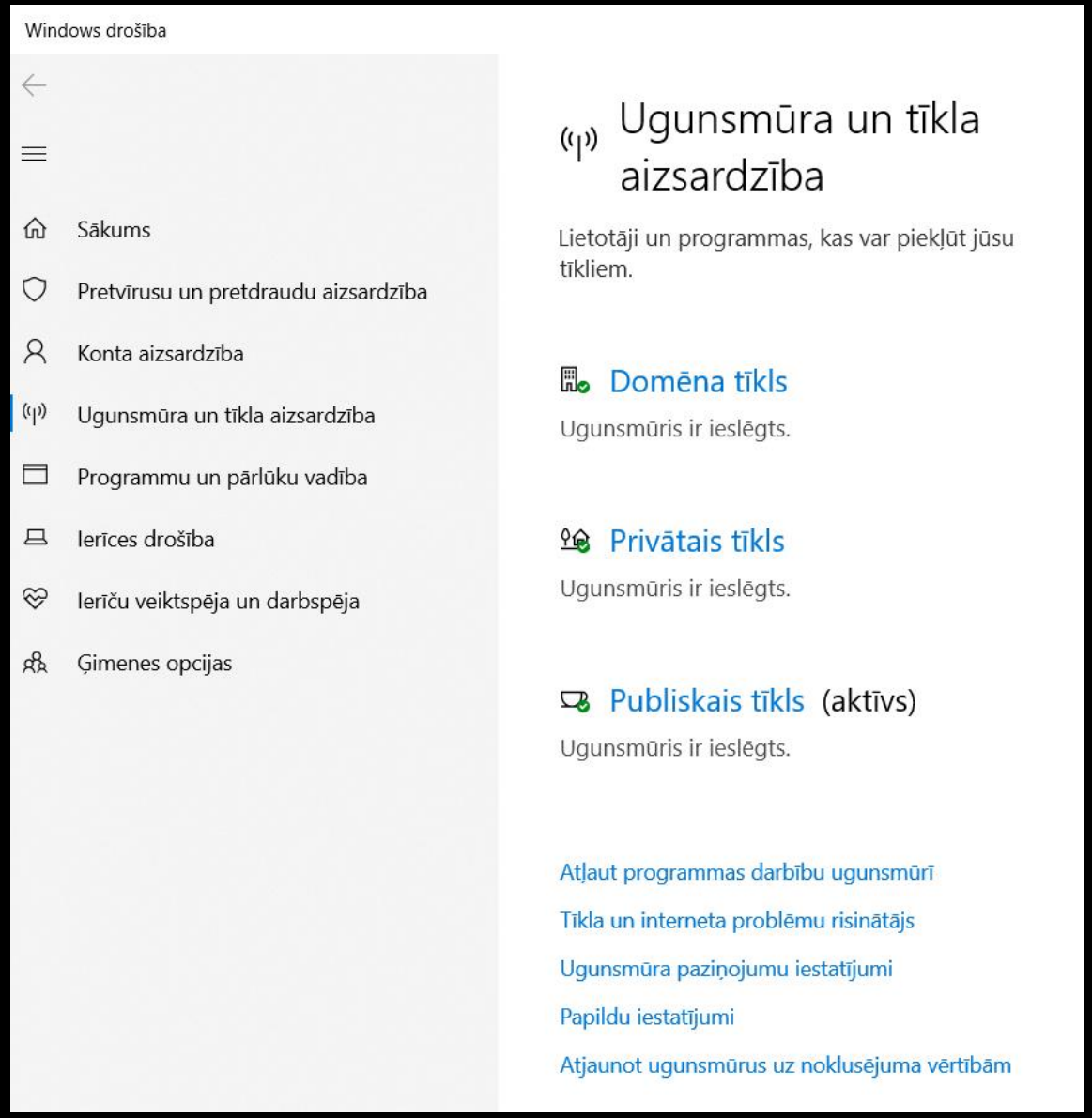
Kas vēl ir datori?

- ✓Videonovērošanas sistēmas
- ✓Satelītuztvērēji
- ✓Tīkla datu glabātavas
- ✓Multimedia serveri
- ✓Maršrutētāji
- ✓SmartTV
- ✓Smart….jebkas (pat spuldzīte)

Manā datorā nekā nav!

```
################################################################
################## YOUR FILES WERE ENCRYPTED ###################
############## AND MARKED BY EXTENSION .corona-lock ############
################################################################
--
DON'T WORRY! YOUR FILES ARE SAFE! ONLY MODIFIED :: ChaCha + AES
WE STRONGLY RECOMMEND you NOT to use any Decryption Tools.
These tools can damage your data, making recover IMPOSSIBLE.
Also we recommend you not to contact data recovery companies.
They will just contact us, buy the key and sell it to you at a higher price.
If you want to decrypt your files, you have to get RSA private key.
--
To get RSA private key you have to contact us via email to:
---------------------------->> support@covidworldcry.com <<
and send us your id: >> 1966883997 <<
--
HOW to understand that we are NOT scammers?
You can ask SUPPORT for the TEST-decryption for ONE file!
--
################################################################
################## LIST OF ENCRYPTED FILES #####################
----------------------------------------------------------------
            C:\autoexec.bat              24
            C:\install.log               45
C:\KAV\nkf1453-readme.txt                      6698
          C:\nkf1453-readme.txt      6698
C:\KAV\KES8Win\nkf1453-readme.txt  6698
```

Kāda ir pareizā atbilde?



Roboti neguļ!

Vairums zema līmeņa datoruzbrukumu tiek veikti izmantojot automatizētus rīkus.
Nav svarīgi – liels uzņēmums vai mājas dators, ja tas ir pieejams no interneta, tas būs uzbrukuma mērķis.
Mājās katram pašam ir jābūt datora administratoram, tīkla speciālistam un rezerves kopiju glabātājam!
Roboti spēj atklāt ievainojamus servisus ātrāk kā tie tiek salaboti.

Ransomware – izspiedējvīrusi

Ļoti aktīvs un augošs datorvīrusu veids.
Intensīvi tiek izplatīts meklējot piejamus RDP (remte desktop protocol) servisus un piemeklējot paroles.
Paroles var būt iepriekš iegūtas citos uzbrukumos, tādejādi apejot to sarežģītību.
Lielos datortīklos uzbrucēji pavada ilgu laiku, izpētot to struktūru un šifrējot visus sasniedzamos datorus un serverus.
Pieprasītās summas – 3000EUR un vairāk.
Šogad aktīvi izmanto «corona» paplašinājumu ☺

VPN ievainojamības

VPN servisos tiek aktīvi meklētas un izmantotas ievainojamības:

- Fortinet VPN
- Citrix "ADC" servers, Citrix network gateways
- Pulse Secure "Connect’’
- Palo Alto Networks "Global Protect" VPN servers
- F5 BIG-IP
- Moxa EDR-G902, EDR-G903
- un citi..

VPN ievainojamības

Pēc veiksmīgas piekļuves VPN tiek meklētas ievainojamības iekšējā tīkla iekārtās

- **CVE-2020-1472, Zerologon**
- **CVE-2020-1301**
- **CVE-2020-1206 utt..**

1)Nelietojiet «single sig-on»!
2)Segmentējiet tīklu, lai ierobežotu iepējas brīvi pieslēgties jebkurai tā daļai
3)Atslēdziet novecojušus un nedrošus VPN mehānismus
4)Izmantojiet daudzfaktoru autentifikācijas mehānismus
5)OPERATĪVI uzstādiet labojumus!
6)Monitorējiet VPN izmantošanu, pievēršiet uzmanību netipiskiem pieslēgumu laikiem un IP adresēm

Kāpēc uzbrukumi ir sekmīgi?

1. Vājas paroles
2. Neeksistējošs/nepietiekams monitorings
3. Nav rezerves kopiju
4. Nav veikta pietiekama piekļuves tiesību nodalīšana
5. Steiga ieviešot jaunus pakalpojumus, bez adekvātu drošības risinājumu izvēles
6. Datortīkla un tajā esošo servisu uzbūves nepārzināšana
7. Nepietiekama programmatūras versiju/atjauninājumu kontrole un ieviešana

Kāpēc vecas ievainojamības darbojas?

87.110.
TET
Added on 2020-10-29 17:57:03 GMT
Latvia, Murjani

Internetā iekārtas dzīvo ilgi!

1. Iekārtas noveco lēnāk kā programmatūra
2. Pat ļoti vecas iekārtas spēj veikt nepieciešamos uzdevumus
3. Jo zemākā OSI līmenī skatāmies – jo senākas iekārtas un protokoli tos uztur
4. «nelabot pirms saplīsis» pieeja
5. Vēlme ietaupīt naudu
6. Sarežģīta lielu sistēmu migrācija

Nemēģiniet mājās vai darbā!!

```
                    Yersinia...

          The Black Death for nowadays networks

                      by Slay & tomac

                  http://www.yersinia.net
                      yersinia@yersinia.net


          Prune your MSTP, RSTP, STP trees!!!!

Usage: yersinia [-hVGIDd] [-l logfile] [-c conffile] protocol [protocol_options]
       -V   Program version.
       -h   This help screen.
       -G   Graphical mode (GTK).
       -I   Interactive mode (ncurses).
       -D   Daemon mode.
       -d   Debug.
       -l logfile   Select logfile.
       -c conffile  Select config file.
  protocol   One of the following: cdp, dhcp, dot1q, dot1x, dtp, hsrp, isl, mpls, stp, vtp.

Try 'yersinia protocol -h' to see protocol_options help
```

Tendences

- Šifrējošie vīrusi joprojām aktuāli
- DDoS atkal ir modē
- Dažāda veida krāpšanas un izspiešanas shēmas
- Intensīvi telefona zvani lai apkrāptu banku klientus
- Jaunizveidotie internetveikali mēdz būt ar kļūdām un ievainojamībām
- Darbs no mājām rada papildus problēmas uzņēmumu datortīklu aizsardzībā