TLP:CLEAR

TOP 10 Kiberlaikapstākļu ziņas 2025.gadā

Dace Bulte | Kiberdrošības analītiķe

CERT.LV
Kiberincidentu novēršanas institūcija

17.03.2026

CERT.LV

TLP:CLEAR

Kas ir "Kiberlaikapstākļi"?

2025 | 12 mēneši

Krāpšana

12

Ļaunatūra & ievainojamības

10 2

DDoS

1 8 2

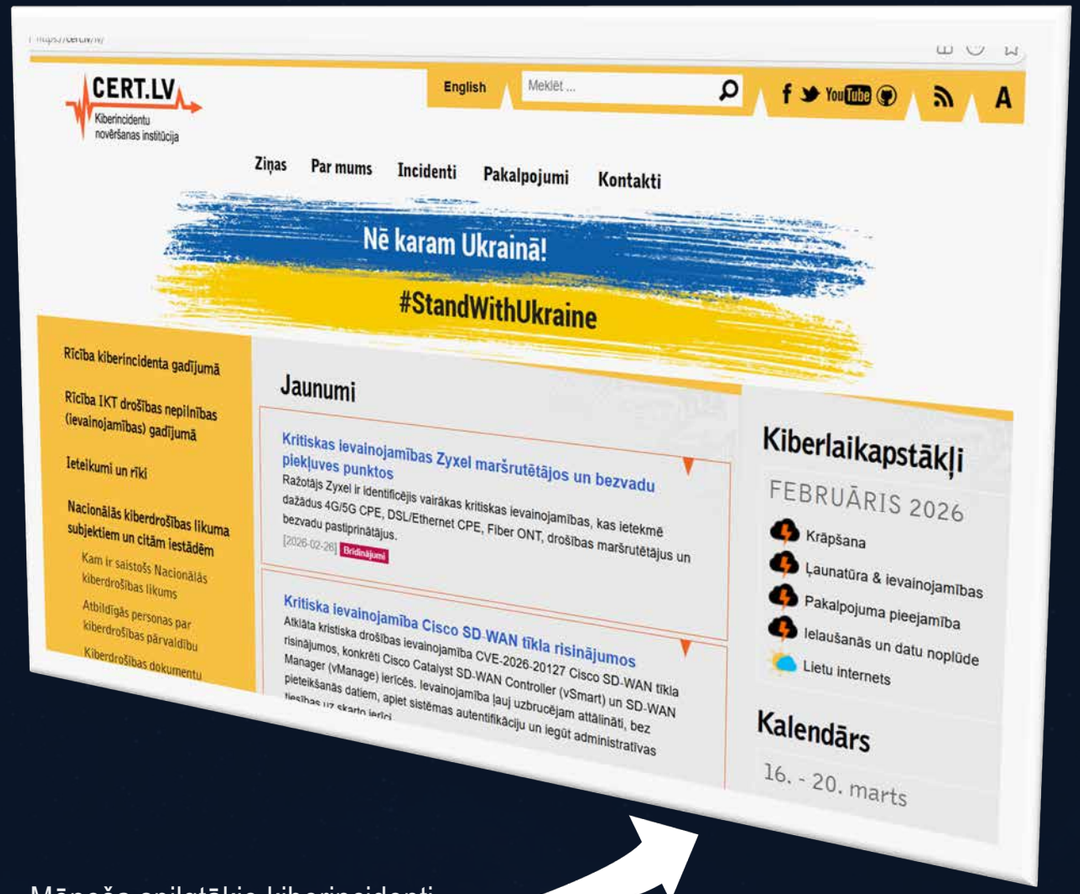
Ielaušanās un datu noplūde

3 3 6

Lietu internets (IoT)

1 9 2

Apskats «Kiberlaikapstākļi» pieejams vietnē **CERT.LV → sākumlapa / sadaļa "Ziņas"**



Mēneša spilgtākie kiberincidenti,
jaunākās ievainojamības un aktuālās kiberdrošības tendences Latvijā

CERT.LV

TLP:CLEAR

Kiberlaikapstākļi digitālajā vidē

Saule

Kibertelpā nav novēroti būtiski incidenti un uzbrukumu kampaņas

Mākoņi

Parādās apdraudējumi, kampaņas, kas vēl nav plaši izplatītas.

Lietus

Novērojama plašāka kiberaktivitāte un sociālās inženierijas uzbrukumi

Negaiss

Notiek plaša mēroga uzbrukumi ar ietekmi uz sabiedrību

CERT.LV nepārtraukti uzrauga krāpniecības kampaņas un augstu vērtē iedzīvotāju iesaisti, kuri **ziņo par incidentiem uz cert@cert.lv vai 232 304 44.**

Kaitnieciskie domēni tiek iekļauti DNS ugunsmūrī, kas pieejams bez maksas un **ik mēnesi bloķē vairāk nekā 200 000 mēģinājumu atvērt ļaunprātīgas saites**.

CERT.LV

TLP:CLEAR

TOP 10: kritēriji

Ietekmes mērogs:

cik plaši incidents skāra sabiedrību vai organizācijas.

Uzbrukuma «radošums» :

jaunas tehnikas vai interesanti sociālās inženierijas scenāriji.

Mācība:

ko mēs no šī incidenta varam iemācīties nākotnei.

CERT.LV

TLP:CLEAR

TOP 10 ?

CERT.LV

TLP:CLEAR

KIBERLAIKAPSTĀKĻI 2025 | KATEGORIJA: KRĀPŠANA TOP 10

"Slidenais ceļš" uz patvertnēm

[MARTS] Krāpnieciskā kampaņā tika izplatītas viltus īsziņas Valsts ugunsdzēsības un glābšanas dienesta vārdā ar aicinājumu nekavējoties kartē atzīmēt sev tuvāko patvertni kartē. Saite veda uz viltotu autentifikācijas lapu.

Būtiskākie riski

- Izmantota sabiedrības drošības tematika
- Imitē valsts vienotās autentifikācijas sistēmu (latvija.lv)
- Autoritatīvas iestādes vārda izmantošana

⚠ Valsts iestāžu nosaukums un krīzes tematika bieži tiek izmantota, lai palielinātu sociālās inženierijas uzbrukumu efektivitāti.
Vienmēr pārbaudiet ziņas patiesumu iestādes oficiālajos kanālos.

Uzbrukuma shēma

1. Lietotāji saņem viltus īsziņu iestādes vārda aizsegā
2. Saite uz viltotu autentifikācijas lapu
3. Krāpnieciskā vietne imitē valsts vienotās pieteikšanās sistēmu
4. Novirzīšana uz pikšķerēšanas vietni
5. Bankas datu ievade, kas nonāk krāpnieku rokās

CERT.LV

TLP:CLEAR

TOP 9 ?

CERT.LV

TLP:CLEAR

KIBERLAIKAPSTĀKĻI 2025 | KATEGORIJA: KRĀPŠANA

TOP 9

Digitālā "dūmaka ": Jūsu balss vēlēšanās ir anulēta

[JŪNIJS] Krāpnieciska kampaņa - īsziņas ar paziņojumu, ka lietotāja balsojums vēlēšanās ir anulēts. Ziņojumos iekļauta saite vai QR kods, kas novirza uz pikšķerēšanas vietni autentifikācijas vai finanšu datu iegūšanai.

Būtiskākie riski

- Sabiedriski nozīmīga tematika
- Steidzamības sajūtas radīšana
- Masveida izplatīšanās risks

Uzbrukuma secība

→ Viltus SMS par anulētu balsojumu vēlēšanās

→ Saite vai QR kods uz krāpniecisku vietni

→ Autentifikācijas vai bankas datu pieprasījums

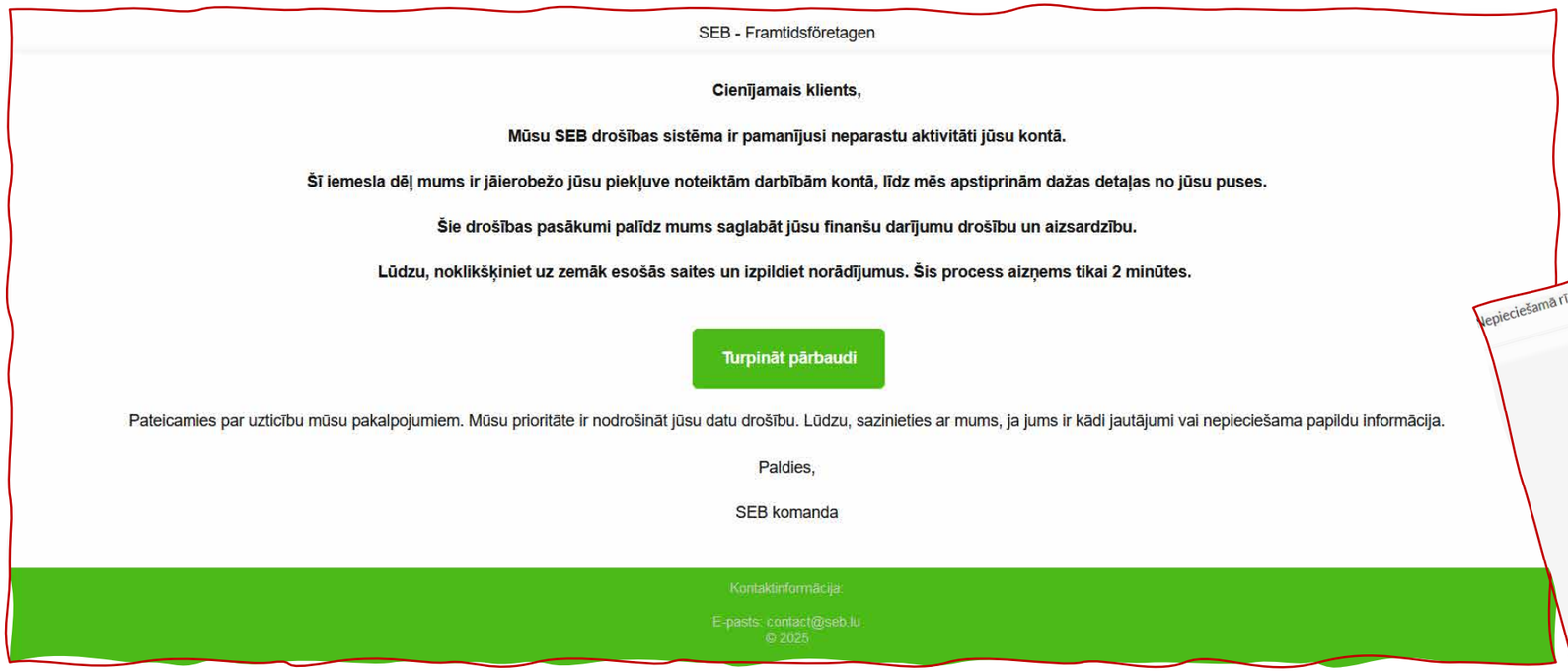
→ Sensitīvi dati nonāk krāpnieku rokās

⚠ Sabiedriski nozīmīgi notikumi bieži tiek izmantoti sociālajā inženierijā kā uzticamības un steidzamības faktori.
Pirms rīcības vienmēr pārbaudiet informāciju oficiālajos avotos un neatveriet aizdomīgas saites vai pielikumus.

CERT.LV

TLP:CLEAR

TOP 8 ?



SEB - Framtidsföretagen

Cienījamais klients,

Mūsu SEB drošības sistēma ir pamanījusi neparastu aktivitāti jūsu kontā.

Šī iemesla dēļ mums ir jāierobežo jūsu piekļuve noteiktām darbībām kontā, līdz mēs apstiprinām dažas detaļas no jūsu puses.

Šie drošības pasākumi palīdz mums saglabāt jūsu finanšu darījumu drošību un aizsardzību.

Lūdzu, noklikšķiniet uz zemāk esošās saites un izpildiet norādījumus. Šis process aizņems tikai 2 minūtes.

Turpināt pārbaudi

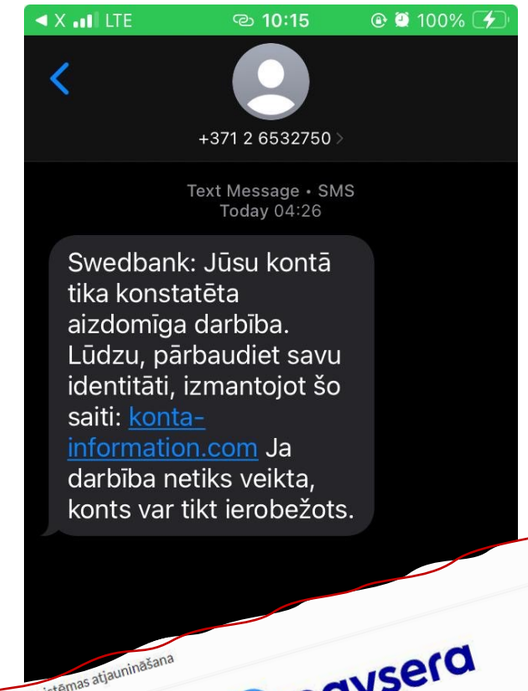
Pateicamies par uzticību mūsu pakalpojumiem. Mūsu prioritāte ir nodrošināt jūsu datu drošību. Lūdzu, sazinieties ar mums, ja jums ir kādi jautājumi vai nepieciešama papildu informācija.

Paldies,

SEB komanda

Kontaktinformācija:

E-pasts: contact@seb.lu
© 2025



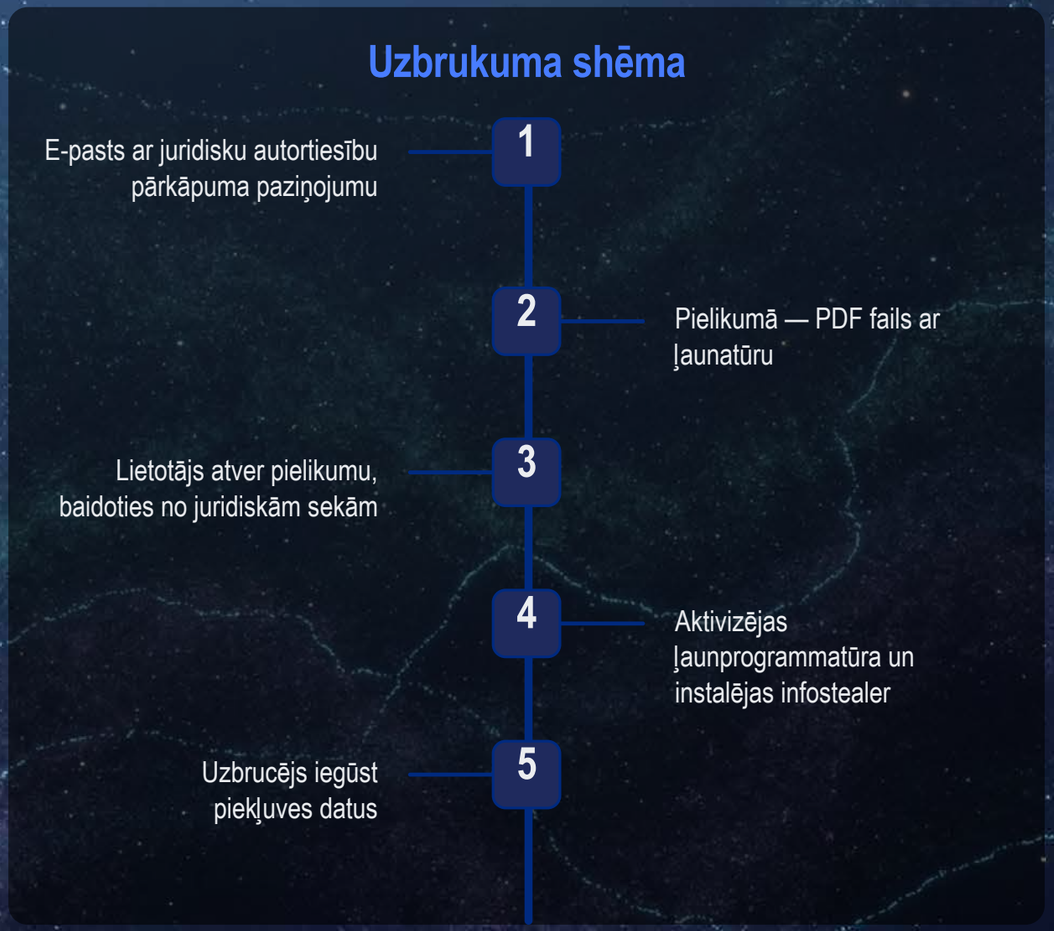
CERT.LV

TLP:CLEAR

KIBERLAIKAPSTĀKĻI 2025 | KATEGORIJA: ĻAUNATŪRA · TOP 8

Autortiesību "zibens" ar ļaunatūras pielikumu

Uzbrukuma shēma



[APRĪLIS] Krāpnieki pikšķerēšanas e-pasta vēstulēs sūtīja paziņojumus organizācijām par it kā konstatētiem **autortiesību pārkāpumiem**. Izliekoties par Latvijā zināmām juridiskām firmām, viņi apgalvoja, ka pārstāvot LTV. Ironiski - ka pielikumā PDF dokuments saturēja ļaunatūru datu zādzības nolūkos.

Mērķis – panākt, ka adresāts uzticas un nekavējoties atver pielikumu.

Būtiskākie riski

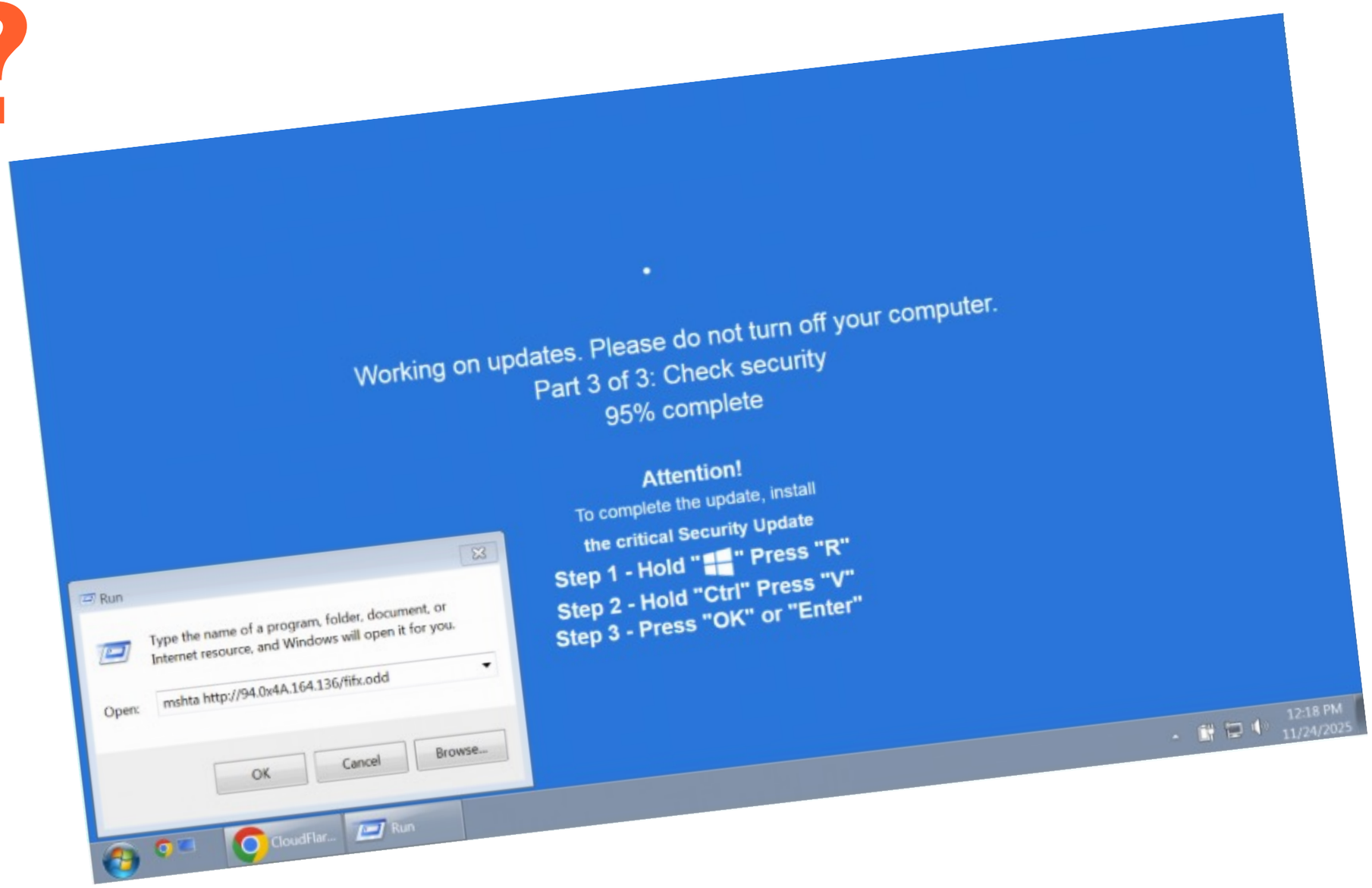
- Draudi ar tiesu vai sodu – «pēdējais brīdinājums»
- Juridiskās autoritātes izmantošana manipulācijai
- Ļaunatūras izplatīšana pielikumā
- Organizāciju mērķēšana

⚠ Steidzamība un juridiskais spiediens ir efektīvs sociālās inženierijas instruments. Pirms atvērt pielikumu — vienmēr pārbaudiet sūtītāja adresi. Ja rodas šaubas - pārbaudiet informāciju oficiālajā tīmekļvietnē.

CERT.LV

TLP:CLEAR

TOP7 ?



CERT.LV

TLP:CLEAR

KIBERLAIKAPSTĀKĻI 2025 | KATEGORIJA: ĻAUNATŪRA · TOP 7

Windows paziņojumi ClickFix "nokrišņu zonā"

[NOVEMBRIS] Kiberuzbrucēji izmantoja **viltotus Windows kļūdas vai atjaunināj uma logus**, kas aicināja lietotāju kopēt un izpildīt PowerShell vai Win+R komandu savā datorā. Šī tehnika, saukta par ClickFix, ir bīstama ar to, ka pats lietotājs kļūst par uzbrukuma izpildītāju.

Būtiskākie riski

- 🖥️ Tiek izmantota lietotāja uzticība operētājsistēmai
- ⌨️ Lietotājs pats iniciē uzbrukumu, izpildot komandu
- 🛡️ Apiet tradicionālos drošības filtrus un antivīrusus
- 🧠 Sociālās inženierijas evolūcija

ClickFix uzbrukuma plūsma

→ Viltots sistēmas kļūdas paziņojums ekrānā

→ Lietotājs tiek aicināts kopēt "labošanas" komandu

→ Lietotājs izpilda komandu PowerShell / Win+R

→ Lejupielādēta ļaunprogrammatūra

→ Sistēma kompromitēta bez trauksmes signāliem

⚠ ClickFix uzbrukumos pats lietotājs kļūst par uzbrukuma izpildes mehānismu. Nekad nekopējiet un neizpildiet komandas no nezināmiem avotiem — pat ja tā šķiet sistēmas paziņojums.

CERT.LV

TLP:CLEAR

TOP 6 ?

CERT.LV

TLP:CLEAR

KIBERLAIKAPSTĀKĻI 2025 | KATEGORIJA: KRĀPŠANA

TOP 6

"Rīta miglas" uzbrukums e-veselībai

Uzbrukuma shēma

[JŪLIJS] Krāpnieki izmantoja apmaksātus Google meklēšanas rezultātus, lai reklamētu viltus e-veselība vietnes. Apmaksātie meklēšanas rezultāti aizved uz viltus vietni, kas vizuāli ļoti atgādina īsto e-veselība, bet patiesībā ir paredzēta internetbankas piekļuves datu izkrāpšanai.

Būtiskākie riski

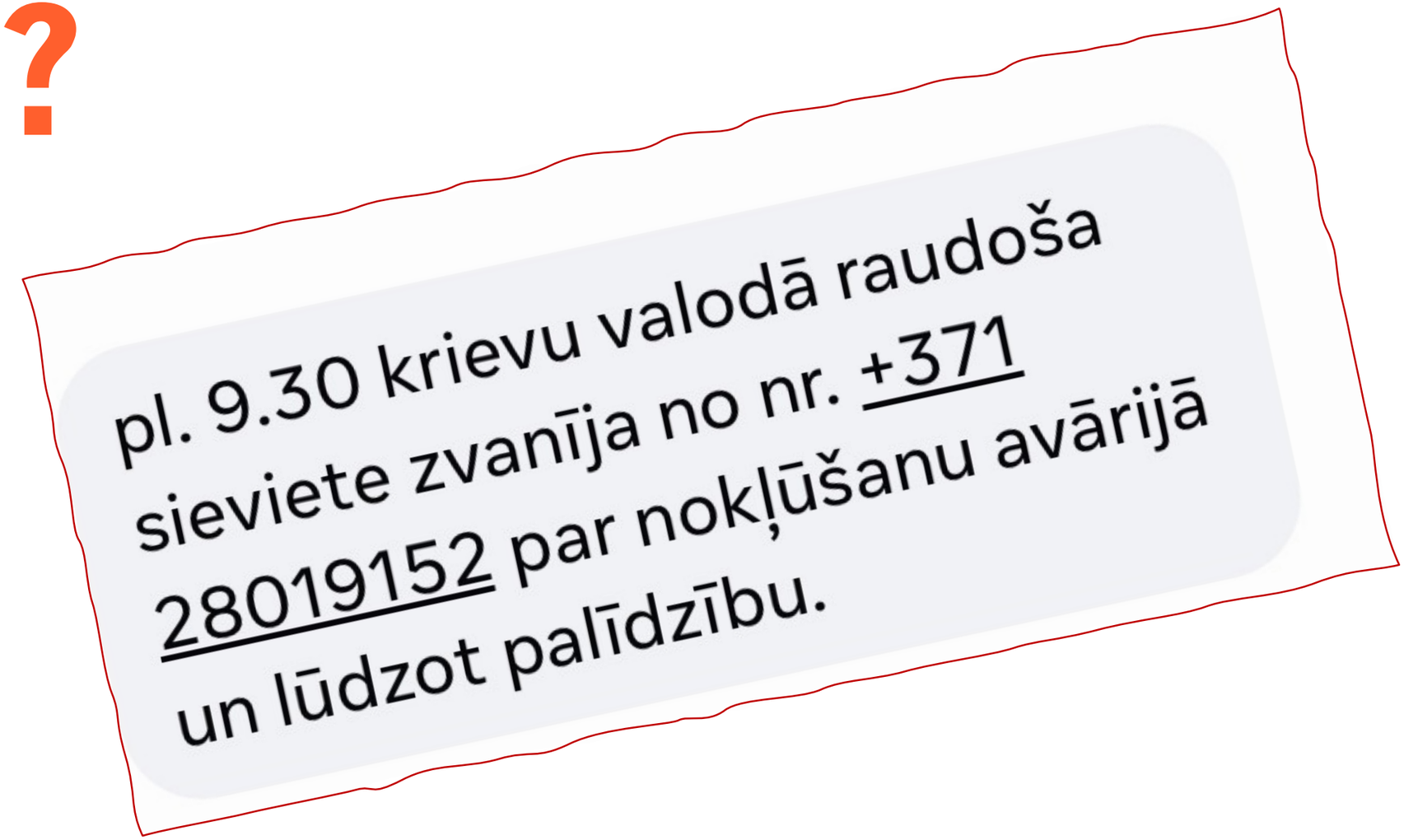
- 🏥 Izmanto sabiedrības uzticību e-veselības sistēmai
- 👥 Var skart plašu sabiedrības daļu — visus e-veselības lietotājus
- 💰 Rada tiešus finanšu zaudējumus un personas datu noplūdi

⚠ Ikdienas digitālie pakalpojumi — veselība, banka, pasts — ir biežākie krāpniecības mērķi, jo ir lielāka iespēja, ka cilvēks uzklikšķinās uz viltus saites. Pirms ievadīt datus, pārliecinieties, ka vietnes adrese un domēna nosaukums ir īsti.

CERT.LV

TLP:CLEAR

TOP 5 ?



CERT.LV

KIBERLAIKAPSTĀKĻI 2025 | KATEGORIJA: KRĀPŠANA TOP 5

TLP:CLEAR

"Lielgraudu krusa" ar dziļviltojumu zvaniem

[MAIJS] Krāpnieki izmantoja audio ierakstu ar MI ģenerētu raudošas sievietes balsi. Balss apgalvoja, ka zvana no slimnīcas pēc "negadījuma", radot emocionālu šoku. Uzbrucēji izmantoja balss klonēšanu un steidzamības sajūtu, lai panāktu maksājumu vai sensitīvas informācijas izpaušanu.

Būtiskākie riski

- 🤖 Dziļviltojumu izmantošana krāpniecībā strauji pieaug
- 😰 Spēcīga manipulācija, izmantojot paniku un uzticību tuvinieku balsij
- 🔍 Uzbrukumus grūti identificēt bez papildu verifikācijas mehānismiem

Uzbrukuma secība

→ Krāpnieks sazinās ar upuri pa telefonu

→ MI ģenerēta balss imitē tuvinieku

→ Tiek radīta steidzamības / šoka situācija

→ Upuris tiek aicināts nekavējoties pārskaitīt naudu

→ Nauda neatgriezeniski nonāk krāpniekiem

MI ģenerēts attēls

⚠ Balss vairs nav uzticams autentifikācijas faktors. Ja saņem neparastu vai satraucošu zvanu no radinieka, pārbaudi informāciju, izmantojot iepriekš atrunātu drošības frāzi vai sazinoties ar personu pa citu kanālu.

CERT.LV

TLP:CLEAR

TOP 4 ?

Microsoft

Email Deactivation Final Notice : Update below to stay active

. 2 FACTOR AUTHENTICATION EXPIRED
. EMAIL ACCOUNT OUTDATED

NOTE: COPY VALIDATION LINK BELOW AND PASTE IN BROWSER TO UPDATE EMAIL ACCOUNT

https:\\microsoftsmailuEDqQFCfqE.iparyamp.ru\EPPc9bab/#YW5uYUBhdWdzdHNrb2xhLmx2

Cienījamais lietotājs,

Šis e-pasts ir no IT servisa dienesta. Mēs vēlamies jūs informēt, ka jūsu e-pasta konts tiks atspējots tuvāko 24 stundu laikā, ja neatjaunināsiet savu informāciju. Lūdzu, ņemiet vērā, ka, lai nezaudētu piekļuvi savam e-pastam, noklikšķiniet uz zemāk esošās saites, lai saglabātu savu kontu aktīvu. Ja šīs darbības neveiksiet, jūsu konts var tikt padarīts neaktīvs un pēc tam atspējots, kas neļaus jums piekļūt savam e-pastam.

PIETEIKTIES

Ar sveicieniem
2025©. gada pasta pārskats

From: susanne.walther@orf.at <susanne.walther@orf.at>
Sent: Saturday, June 14, 2025 5:55 PM
Subject: @Info

UZMANĪBU: Šis ir ārējs e-pasts, esiet piesardzīgi, atverot pielikumus un saites.

Sveiki,

Jūsu Outlook konts drīz tiks deaktivizēts.
Lai apturētu deaktivizāciju,

noklikšķiniet šeit

Ar cieņu
IT PAKALPOJUMS

CERT.LV

KIBERLAIKAPSTĀKĻI 2025 | KATEGORIJA: IELAUŠANĀS / IZSPIEDĒJVĪRUSS TOP 4

TLP:CLEAR

Izspiedējvīrusa "negaisa fronte" Jelgavā

MI ģenerēts attēls

[JŪNIJS] Jelgavas tipogrāfija kļuva par **šifrējoša izspiedējvīrusa uzbrukuma upuri**.
Dati tika šifrēti un draudēts tos publiskot.

Uzbrukuma mehānisms

1. Piekļuves iegūšana sistēmā
2. Tiek instalēts izspiedējvīruss
3. Datu šifrēšana
4. Izpirkuma pieprasījums un draudi publiskot datus

Būtiskākie riski

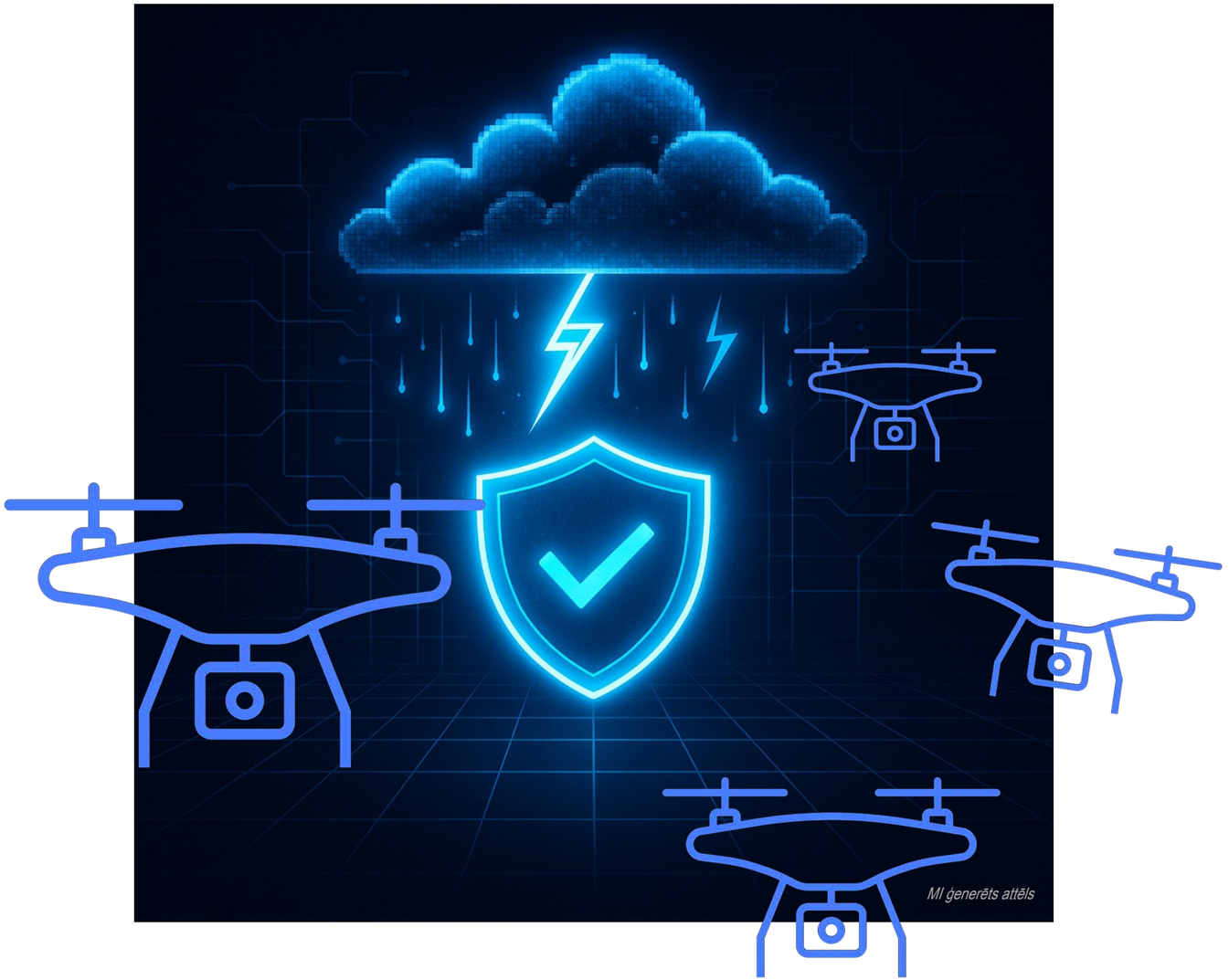
- Uzņēmuma darbības paralīze
- Datu noplūdes risks
- Būtisks finanšu zaudējumu risks

⚠ Izspiedējvīrusa uzbrukumi rada gan tehniskus, gan biznesa nepārtrauktības riskus. Lai mazinātu šos riskus, regulāri atjauniniet sistēmas un programmatūru; ieviest daudzfaktoru autentifikāciju (MFA) un apmāciet darbiniekus atpazīt pikšķerēšanu.

CERT.LV

TLP:CLEAR

TOP 3 ?



CERT.LV

KIBERLAIKAPSTĀKĻI 2025 | KATEGORIJA: DDOS UZBRUKUMS

TOP 3

TLP:CLEAR

DDoS "vētra" pēc uzvaras dronu iepirkumā

[JŪLIJS] Pēc Latvijas uzņēmuma uzvaras starptautiskās Dronu koalīcijas iepirkumā, prokremliski haktīvisti paziņoja par uzsāktiem DDoS uzbrukumiem pret vairākiem mērķiem Latvijā, tostarp vairākām pašvaldību tīmekļvietnēm un transporta nozares infrastruktūru.

Dažos gadījumos tika novēroti pakalpojumpieejamības traucējumi.

Uzbrukuma mehānisms

- Uzbrucēji mobilizē botu tīklu
- Tiek ģenerēta masīva datplūsma uz mērķa serveriem
- Serveri tiek pārslogoti
- Pakalpojumi uz laiku kļūst nepieejami

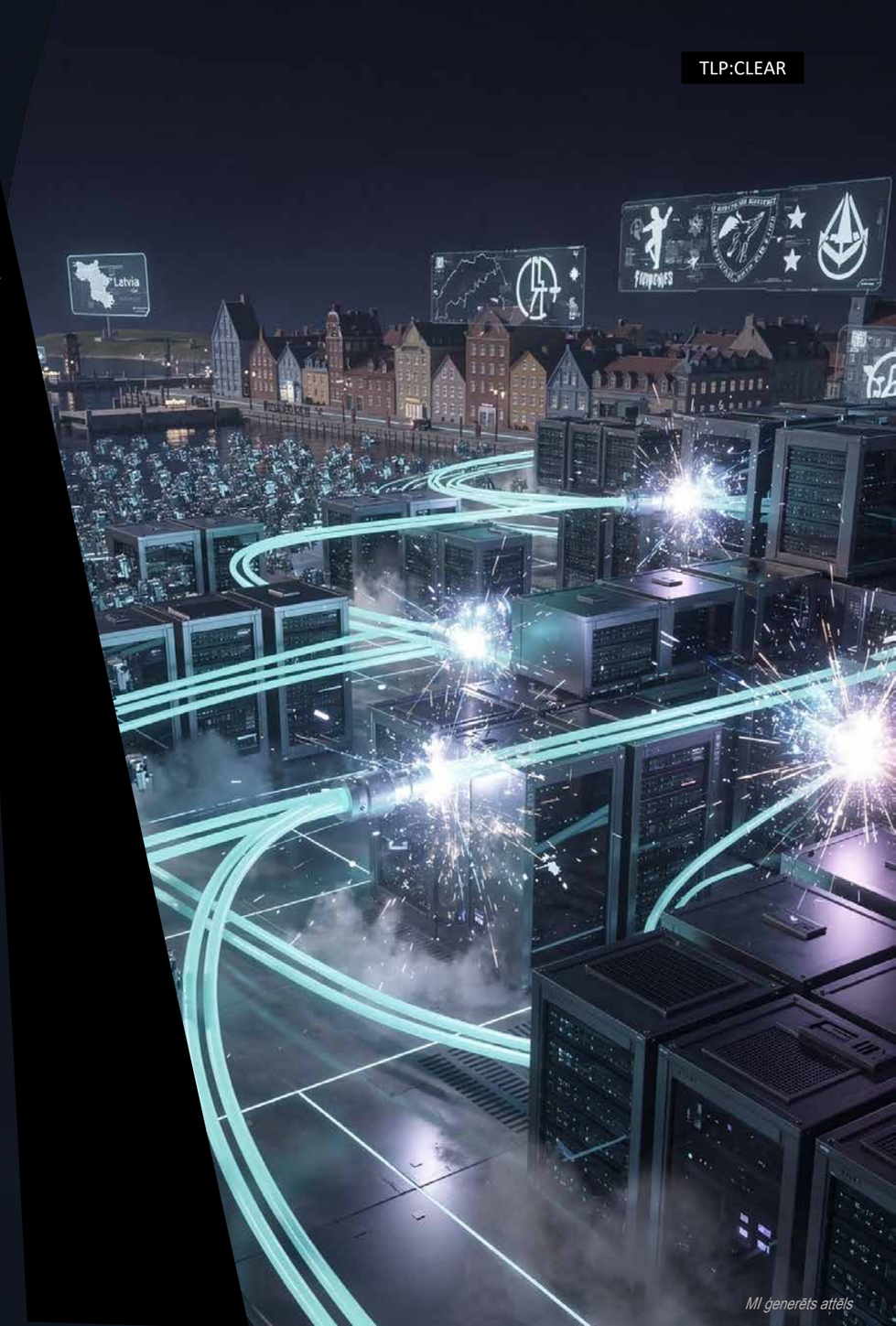
Būtiskākie riski

🌐 Ģeopolitiski motivēts uzbrukums kontekstā ar politiskiem notikumiem

🏛️ Tieša ietekme uz pakalpojumu nepieejamību

⚡ Ietekme uz sabiedrību un informācijas telpu

⚠ Kibertelpa arvien biežāk kļūst par ģeopolitisko konfliktu paplašinājumu. IKT kritiskās infrastruktūras aizsardzība ir nacionālās drošības jautājums.



MI ģenerēts attēls

CERT.LV

TLP:CLEAR

TOP 2 ?

CERT.LV

TLP:CLEAR

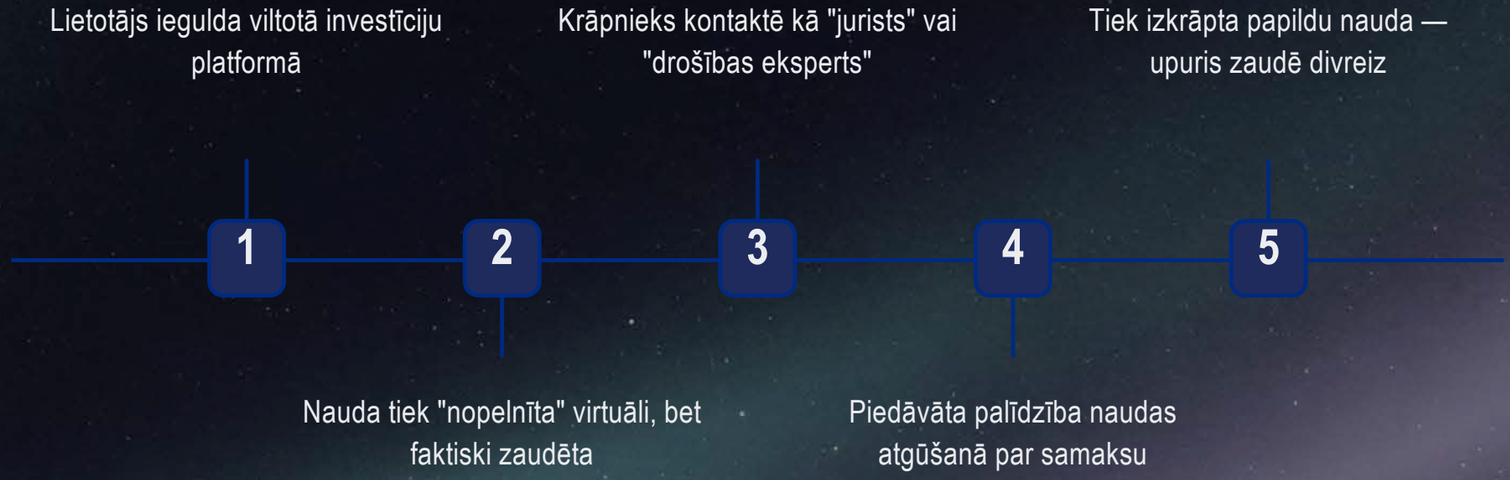
KIBERLAIKAPSTĀKĻI 2025 | KATEGORIJA: KRĀPŠANA

TOP 2

Dubultā finanšu krāpšana jeb "melnais ledus"

- Upuri sākotnēji zaudē naudu viltotās investīciju platformās — solīta augsta peļņa investīcijās vai kriptovalūtā.
- Krāpnieki fokusējās uz sabiedrībā zināmu personu vārda izmantošanu, lai veicinātu ticamību krāpnieciskiem investīciju piedāvājumiem.
- Pēc tam krāpnieki atgriežas jaunā lomā — kā "juristi", piedāvājot palīdzēt atgūt zaudēto par papildu samaksu.

Dubultās krāpšanas shēma



Būtiskākie riski

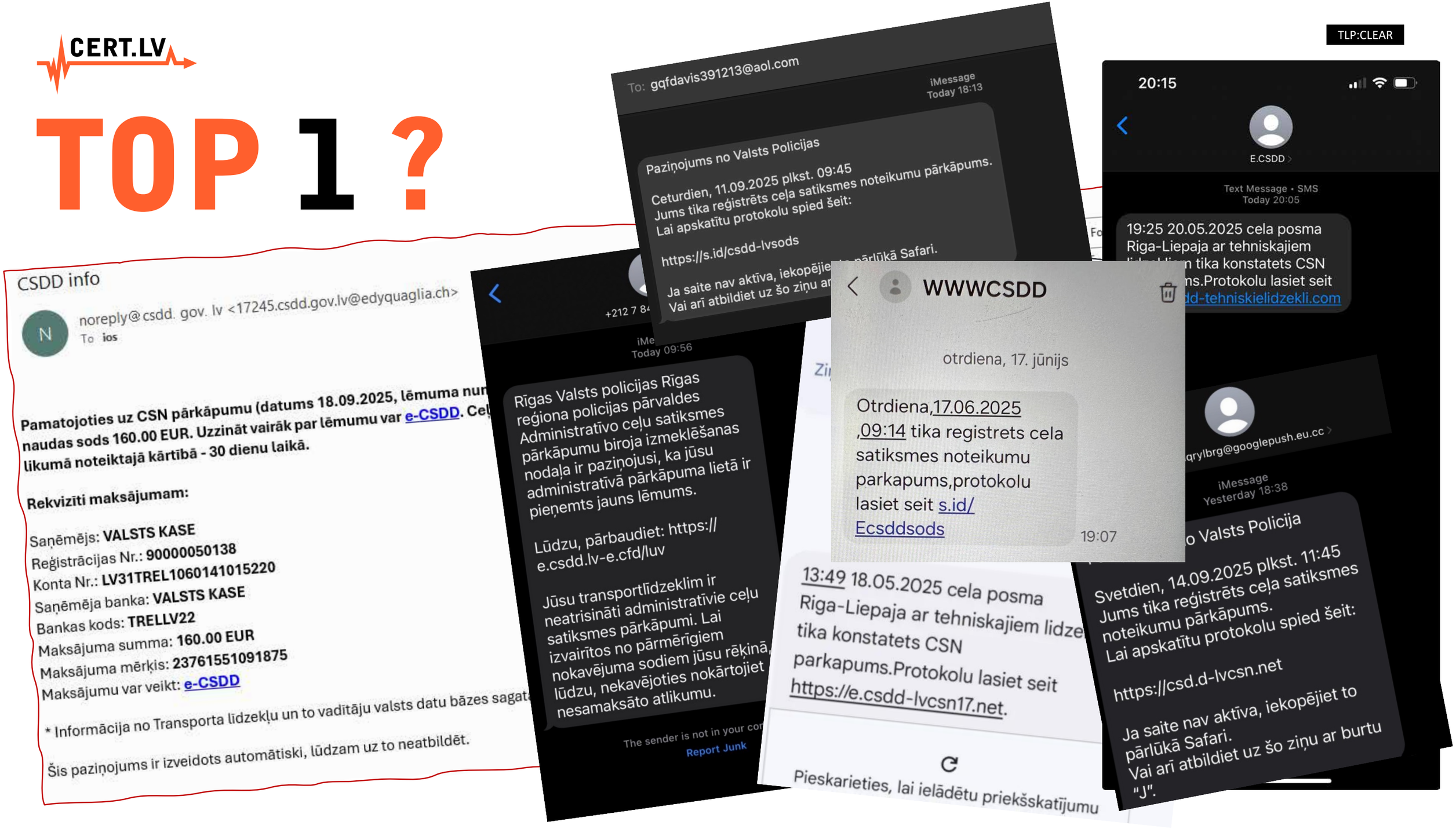
- Atkārtota upuru izmantošana
- Daudzpakāpju sociālā manipulācija
- Būtiski finanšu zaudējumi

⚠ Galvenais apdraudējums - **finanšu zaudējumi un personas datu kompromitācija**, kas var radīt ilgtermiņa ietekmi gan uz cietušajiem, gan uz finanšu sistēmas uzticamību.

CERT.LV

TLP:CLEAR

TOP 1 ?



CSDD info

noreply@csdd. gov. lv <17245.csdd.gov.lv@edyquaglia.ch>
To ios

Pamatojoties uz CSN pārkāpumu (datums 18.09.2025, lēmuma nur
naudas sods 160.00 EUR. Uzzināt vairāk par lēmumu var e-CSDD. Ce
likumā noteiktajā kārtībā - 30 dienu laikā.

Rekvizīti maksājumam:

Saņēmējs: **VALSTS KASE**
Reģistrācijas Nr.: **90000050138**
Konta Nr.: **LV31TREL1060141015220**
Saņēmēja banka: **VALSTS KASE**
Bankas kods: **TRELLV22**
Maksājuma summa: **160.00 EUR**
Maksājuma mērķis: **23761551091875**
Maksājumu var veikt: **e-CSDD**

* Informācija no Transporta līdzekļu un to vadītāju valsts datu bāzes sagat

Šis paziņojums ir izveidots automātiski, lūdzam uz to neatbildēt.

To: gqfdavis391213@aol.com
iMessage
Today 18:13

Paziņojums no Valsts Policijas

Ceturdien, 11.09.2025 plkst. 09:45
Jums tika reģistrēts ceļa satiksmes noteikumu pārkāpums.
Lai apskatītu protokolu spied šeit:

https://s.id/csdd-lvsods

Ja saite nav aktīva, iekopēji
Vai arī atbildiet uz šo ziņu ar

+212 7 84
iMe
Today 09:56

Rīgas Valsts policijas Rīgas reģiona policijas pārvaldes Administratīvo ceļu satiksmes pārkāpumu biroja izmeklēšanas nodaļa ir paziņojusi, ka jūsu administratīvā pārkāpuma lietā ir pieņemts jauns lēmums.

Lūdzu, pārbaudiet: https://e.csdd.lv-e.cfd/luv

Jūsu transportlīdzeklim ir neatrisināti administratīvie ceļu satiksmes pārkāpumi. Lai izvairītos no pārmērīgiem nokavējuma sodiem jūsu rēķinā, lūdzu, nekavējoties nokārtojiet nesamaksāto atlikumu.

The sender is not in your co
Report Junk

WWWCSDD

otrdiena, 17. jūnijs

Otrdiena,17.06.2025 ,09:14 tika registrets cela satiksmes noteikumu parkapums,protokolu lasiet seit s.id/Ecsddsods 19:07

13:49 18.05.2025 cela posma Riga-Liepaja ar tehniskajiem lidze
tika konstatets CSN parkapums.Protokolu lasiet seit https://e.csdd-lvcsn17.net.

Pieskarieties, lai ielādētu priekšskatījumu

20:15

E.CSDD

Text Message • SMS
Today 20:05

19:25 20.05.2025 cela posma Riga-Liepaja ar tehniskajiem
tika konstatets CSN
ms.Protokolu lasiet seit
dd-tehniskielidzekli.com

qrylbrg@googlepush.eu.cc

iMessage
Yesterday 18:38

o Valsts Policija

Svetdien, 14.09.2025 plkst. 11:45
Jums tika reģistrēts ceļa satiksmes noteikumu pārkāpums.
Lai apskatītu protokolu spied šeit:

https://csd.d-lvcsn.net

Ja saite nav aktīva, iekopējiet to pārlūkā Safari.
Vai arī atbildiet uz šo ziņu ar burtu "J".

CERT.LV

TLP:CLEAR

KIBERLAIKAPSTĀKĻI 2025 | KATEGORIJA: KRĀPŠANA

TOP 1

Īsziņu "sniegputenis" CSDD vārda aizsegā

Masveidīgākā krāpniecības kampaņa ar CSDD vārda izmantošanu, izsūtot viltus e-pastus un īsziņas par fiksētu ceļu satiksmes pārkāpumu vai neapmaksātu sodu.

Dominējošā krāpniecības tematika Latvijā 2025. gadā.

Būtiskākie riski

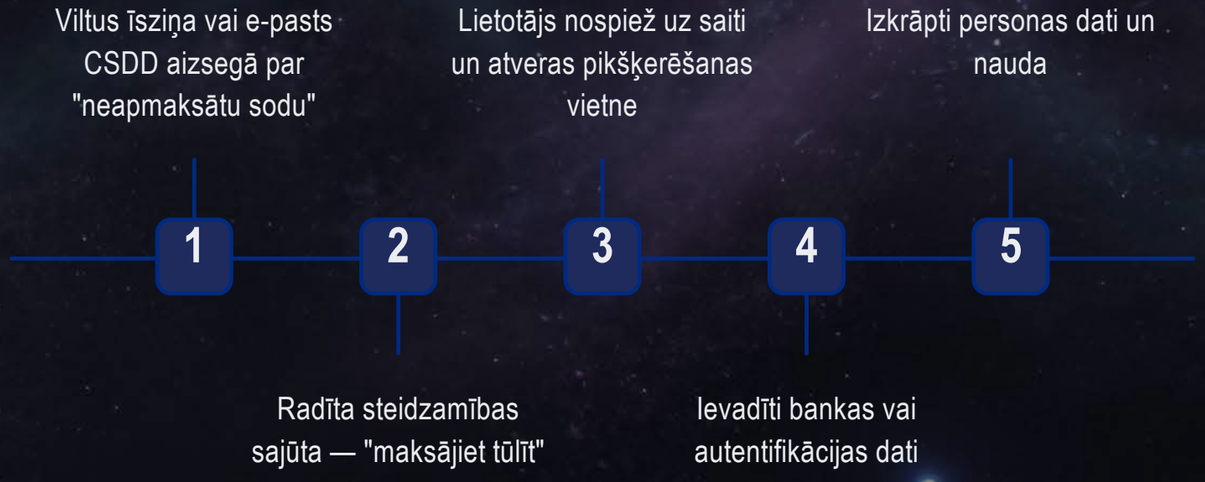
🏛️ Tiek izmantots valsts iestādes vārds un uzticamība

📊 Ļoti ticama vizuālā imitācija rada viltus drošība sajūta, nepārbaudot adresi

⚡ Steidzamība + sods = augstas iedarbības manipulācija

⚡ Autovadītāji regulāri saņem īstus paziņojumus, krāpnieki izmanto šo ieradumu

Uzbrukuma shēma



⚠ Uzticēšanās institūcijas vārdam bieži tiek izmantota kā efektīvs manipulācijas instruments. Pārbaudi ziņas autentiskumu organizācijas oficiālajā tīmekļvietnē.

CERT.LV

TLP:CLEAR

Ko 2025. gada Latvijas kiberlaikapstākļi parāda?

👤 Cilvēks ir viens no biežākajiem drošības incidentu cēloņiem

🤖 Uzbrukumu scenāriji kļūst kompleksāki un automatizētāki - MI rīki to vēl vairāk pastiprina

🌍 Kiberdraudi arvien biežāk saistīti ar ģeopolitiku un sabiedriskiem notikumiem

CERT.LV

TLP:CLEAR

3 lietas, kas jāpaņem līdzi nākamajai kibersezonai

🏋️ Lietusmētelis —
Darbinieku apmācība, testi un
laba kiberhigiēna

☂️ Lietussargs —
MFA, regulāri sistēmu un
lietotņu atjauninājumi

🏠 Drošs patvērums —
rezerves kopijas,
DNS ugunsmūris, SOC … 24/7

MI ģenerēti attēli


CERT.LV
Seko
kiberlaikapstākļiem!
VILTUS SAITES
KRĀPNIECISKI
TELEFONA NUMURI
KRĀPNIECISKAS ĪSZIŅAS
Ja pamani, ziņo SMS / WhatsApp!
232 304 44