2023 gads Latvijas kibertelpā

Gints Mālkalnietis

12.12.2023

Aizsargrīki kļūst par uzbrukuma mērķi

- Fortinet: CVE-2022-42475, CVE-2023-27997, CVE-2023-33308
- Cisco: CVE-2023-20109,CVE-2023-20189, CVE-2023-20032
- OpenVPN: CVE-2023-46850
- F5: CVE-2023-46748, CVE-2023-46747, CVE-2023-44487
- Juniper: CVE-2023-36847, CVE-2023-36844, CVE-2023-28962
- Zyxel: CVE-2023-33010, CVE-2023-33009, CVE-2023-22920

DDOS uzbrukumi

- DDOSIA un citi speciāli rīki
- Liels budžets, par uzbrukumiem tiešām maksā kriptovalūtu
- Mērķus izvēlas atbilstoši politiskām aktualitātēm
- IP ierobežojumus apiet izmantojot TOR un dažādus proxy
- Uzbrukumi aplikāciju līmenī, izmanto vietnēs identificētas ievainojamības, parasti meklēšanas rīkos
- Ilgākie uzbrukumi ilgst 2-3 diennaktis

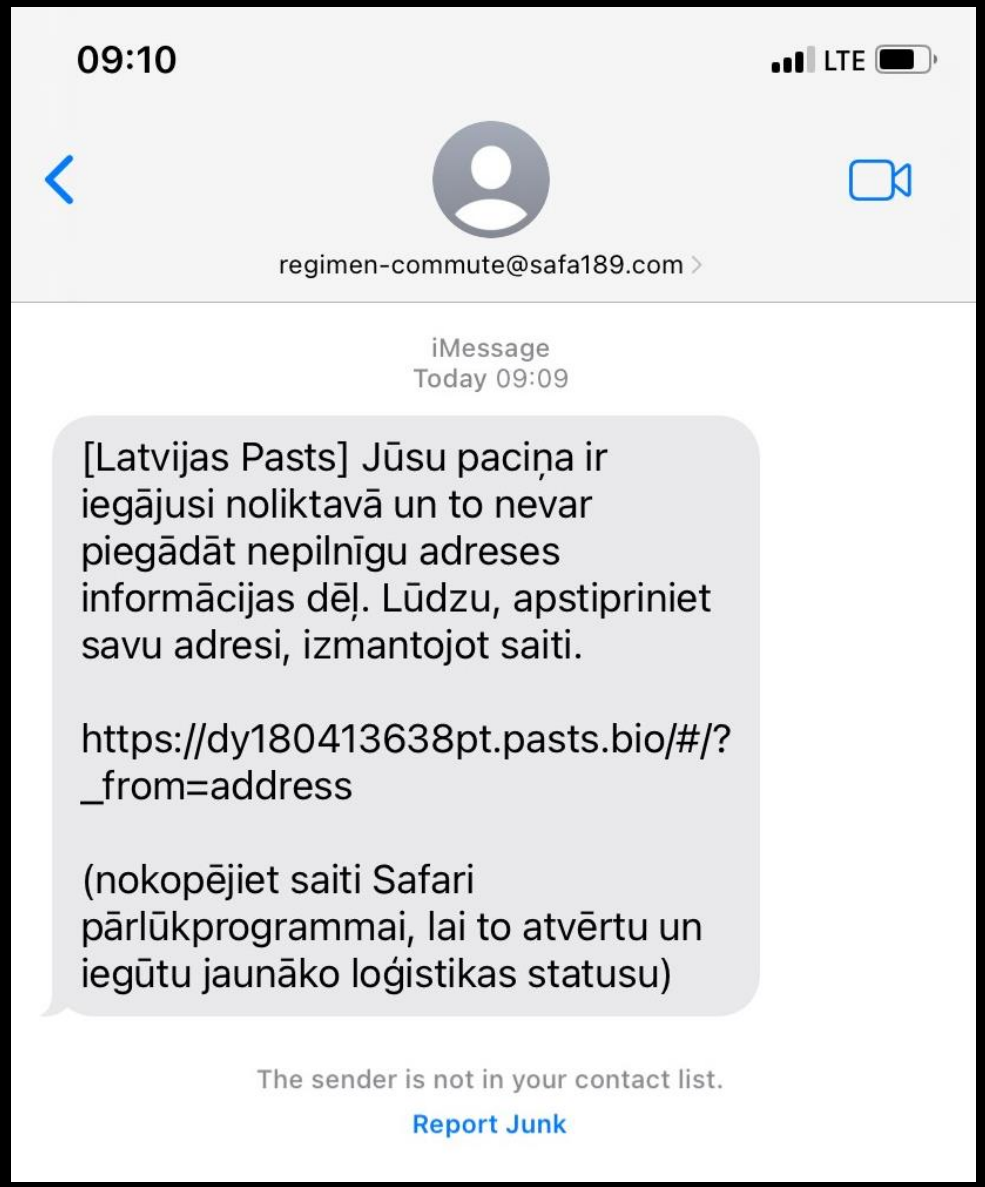
Bīstamie pastnieki

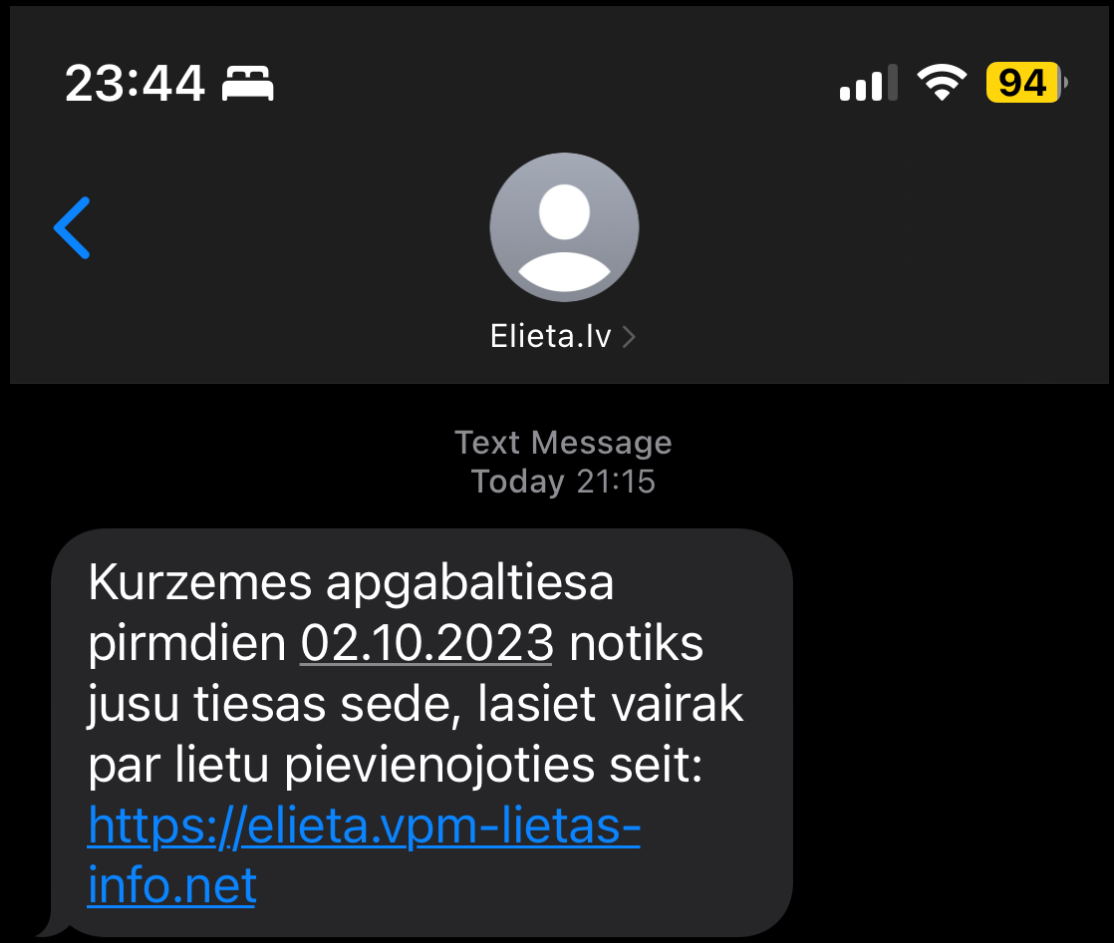
- Microsoft Exchange: CVE-2022-41082, CVE-2023-21529, CVE-2023-21707, CVE-2023-21709, CVE-2023-32031, CVE-2023-38185
- Barracuda: CVE-2023-2868
- Microsoft Outlook: CVE-2023-23397, CVE-2023-33131, CVE-2023-35311
- Mozilla Thunderbird: CVE-2023-4863, CVE-2023-5217

Uzbrukumi mobilajiem telefoniem

- AppleIOS:CVE-2023-23526, CVE-2023-28204, CVE-2023-28205, CVE-2023-28206, CVE-2023-32373, CVE-2023-32409, CVE-2023-32434, CVE-2023-32435, CVE-2023-41993, CVE-2023-42917
- Android:CVE-2023-20963, CVE-2023-20965, CVE-2023-35681, CVE-2023-21250, CVE-2023-20946

Uzbrukumi mobilajiem telefoniem





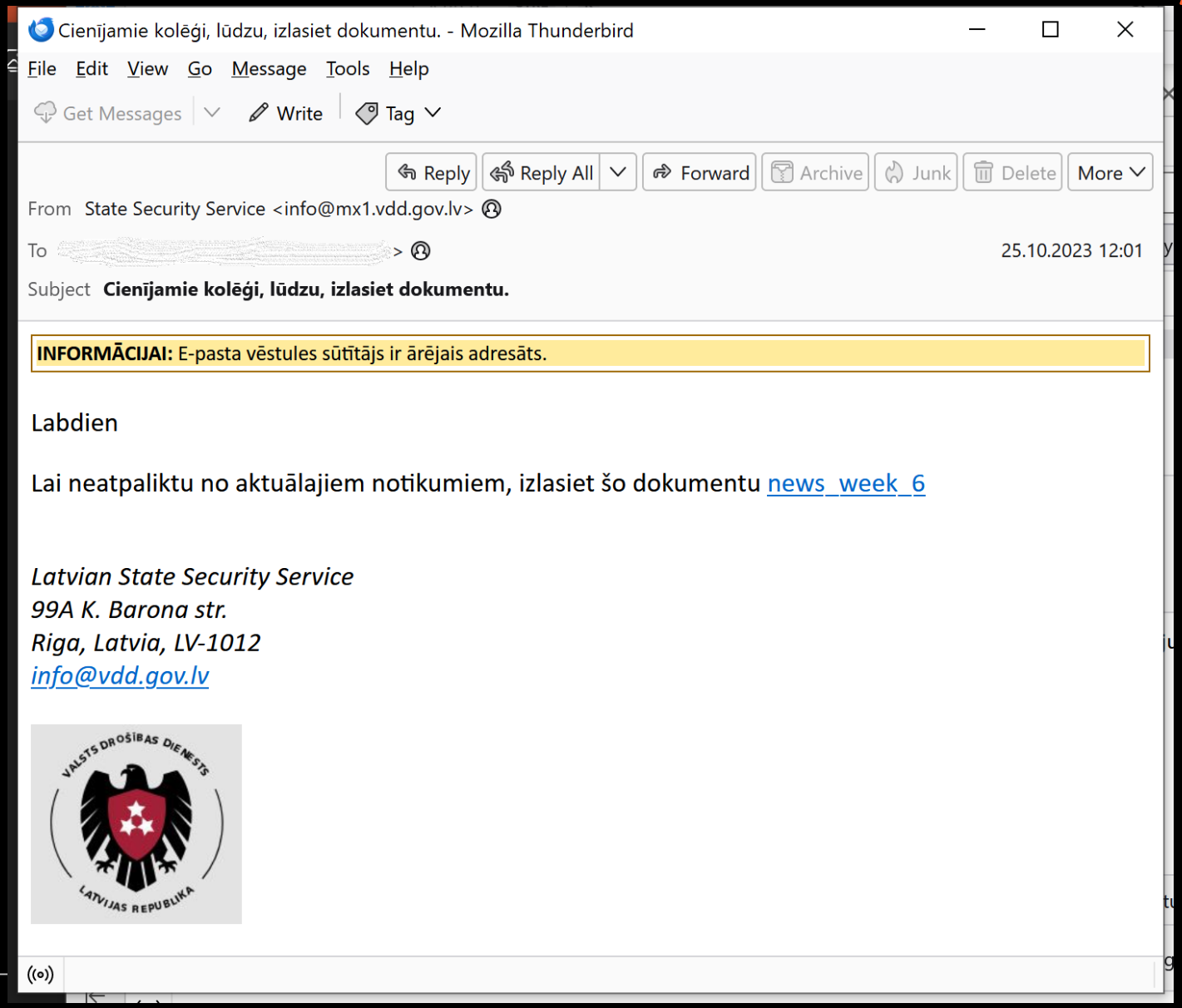
Lai izspiestu lielu naudu, tiks lietotas visas metodes!

- Ja ir iespējams nozagt lielāku naudu, uzbrucēji izmantos visus līdzekļus!
- Viltotas SMS – to identifikatorus ir iespējams viegli mainīt, bet cilvēki tām uzticas
- Balss zvani izliekoties par kolēģi
- Balss viltošana izmantojot jaunākas MI metodes ir kļuvusi pavisam vienkārša
- Viltoti (deepfake) video
- Viltoti datu pārraides kabeļi ar keyloger funkciju

Uzbrucēji pievērš uzmanību detaļām!

- E-pasta programmu izmantotie fonti ļauj noslēpt īsto sūtītāju
- Mobilo tālruņu pārlūkprogrammas nerāda pilnu adresi
- Pikšķerēšanas lapas tiek aizsargātas ar kodu
- FB/Instagram izplatītas pikšķerēšanas pārbauda vai tiek atvērtas no šiem tīkliem
- DMARC, DKIM, SPF ieviešanas kļūdas
- IP adrešu ierobežojumi

Uzbrucēji pievērš uzmanību detaļām!



«Caurie» izstrādātāji

- Sekmīgam uzbrukumam vajag atrast vājāko ķēdes elementu, nevis uzbrukt labi aizsargātai datorsistēmai!
- Ērtības labad resursu uzturētāji labprātīgi ievieš dažādus «backdoor»

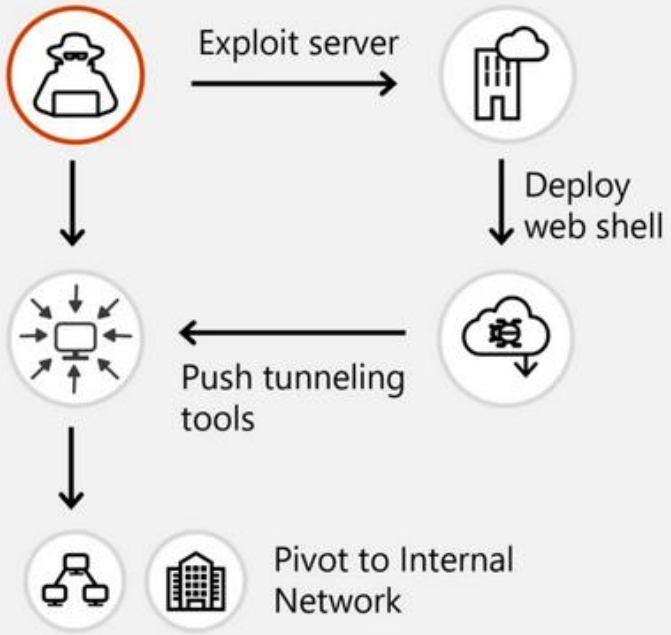
«Caurie» izstrādātāji

- Izstrādātājam papildus izveidots lietotāja konts ar augstām tiesībām
- IP adrese izstrādātāja tīklā, no kuras var piekļūt serveriem bez VPN savienojuma
- Piekļuve sistēmu «backend» serveriem bez pilnvērtīgas darbību izsekojamības un žurnalēšanas
- Iespēja pieslēgties sistēmām bez saskaņošanas ar to turētāju
- Izstrādātājiem izsniegtas domēna administratora tiesības
- Uz izstrādātāju kontiem neattiecas uzņēmumā pieņemtās paroļu izveides politikas
- Atļauts izmantot novecojušas/neuzturētas OS un programmu versijas
- Nepietiekami nodalīta izstrādes un produkcijas vide

CERT.LV

DEV-0586

Initial access



Lateral movement

- Credential access via process dumping
- Interactive reverse shell via netcat/GOST
- Command execution via Impacket
- Disable antivirus and wipe logs

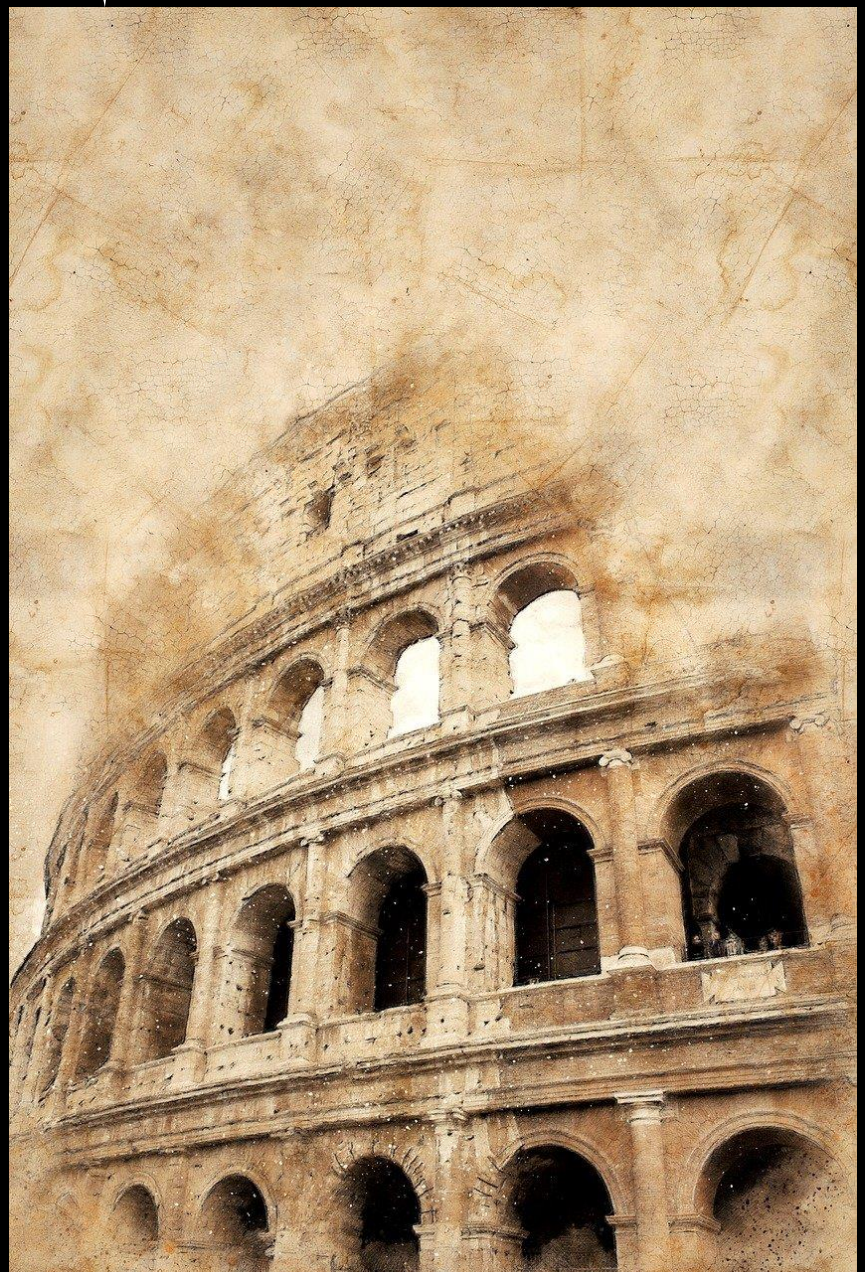
Action on objectives

- Exfiltrate data
- Deploy destructive payloads
- Leak data / targeted information operations

Vai zināms, kas notika iekšējā tīklā?

- Piekļuve uzņēmuma iekšējam tīklam sākas no publiski pieejama webservera
- Serveros tiek uzstādīti rīki administratoru ievadīto paroļu un komandu pārtveršanai un saglabāšanai
- Vadība un datu nodošana cau Ngrok TCP tuneļiem un Ghost Shell
- Darbības datortīklā pamatā tiek veiktas izmantojot esošo Windows OS programmu un rīku iespējas – LOTL - Living Off the Land Attacks

Vēstures nastas problēmas



- Jebkura IT sistēma ir ar ierobežotu dzīves ciklu
- Jauni projekti aizēno senos
- NEVIENAM negribās «lāpīt» 10+ gadus vecas vietnes
- Veidojot jaunu interneta resursu, jādomā arī par tā uzturēšanu, un likvidēšanu!
- Nevajag «pamest» vecas interneta lapas, ja tās nevaram uzturēt – labāk izslēgt!

Parolēm nav nākotnes!

Cilvēki lieto nedrošas paroles!

Ar parolēm aizsargāto kontu ir pārāk daudz, tāpēc:

- Izmanto īsas paroles
- Izmanto paroles, kas ir viegli uzminamas
- Izmanto vienu paroli vairākiem resursiem

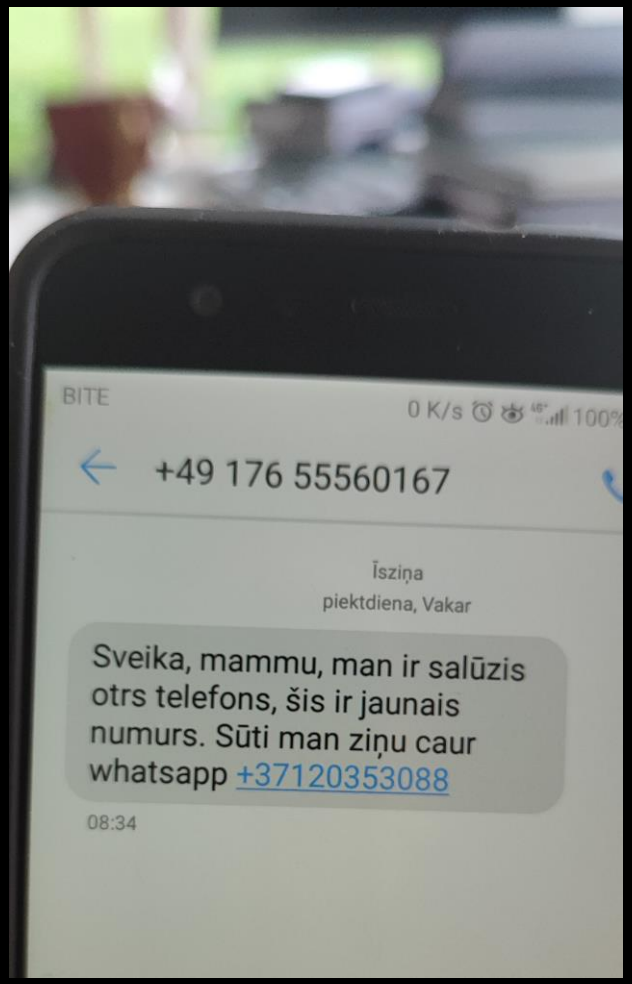
Nelieto papildus autentifikācijas rīkus, pat ja tie pieejami

- SW kodu ģeneratori (Google autentifikators utt.)
- Autentifikācijas aplikācijas (Smart ID utt.)
- SMS kodi

Praktiski visi kompromitētie e-pasta un sociālo tīklu konti nav izmantojuši S2FA!

Kas vajadzīgs sekmīgam uzbrukumam?

- Neparasta situācija
- Steiga
- Nogurums
- Neuzmanība
- Mazs telefona ekrāns
- Esošo procedūru nepārzināšana
- Veiksmīga sagadīšanās



Nepieciešama aizsardzība dziļumā

Perimetra aizsardzība jau sen nav pietiekama!

IDS/EDR vajag ne tikai uzstādīt bet arī konfigurēt, katru dienu uzmanīt un sekot līdzi rezultātiem!

Lielu tīklu aizsardzībai bez ML/AI risinājumiem neiztikt!

Tehniskie ierobežojumi un metodes jāpapildina ar regulāru apmācību!

Jāmācās aizsargāt arī savu bērnu un dzīvesvietā uzstādītos IT risinājumus

Jāpārtrauc drošības upurēšana ērtībai!

Paldies!

https://www.cert.lv
gints@cert.lv
Gints Mālkalnietis