Kiberdrošības aktualitātes ģeopolitiskā saspīlējuma laikā

24.03.2022.

CERT.LV
Information Technologies Security Incident Response Institution

Apdraudējuma tendences

Apdraudējuma līmenis LV kibertelpā no janvāra vidus ir augsts.

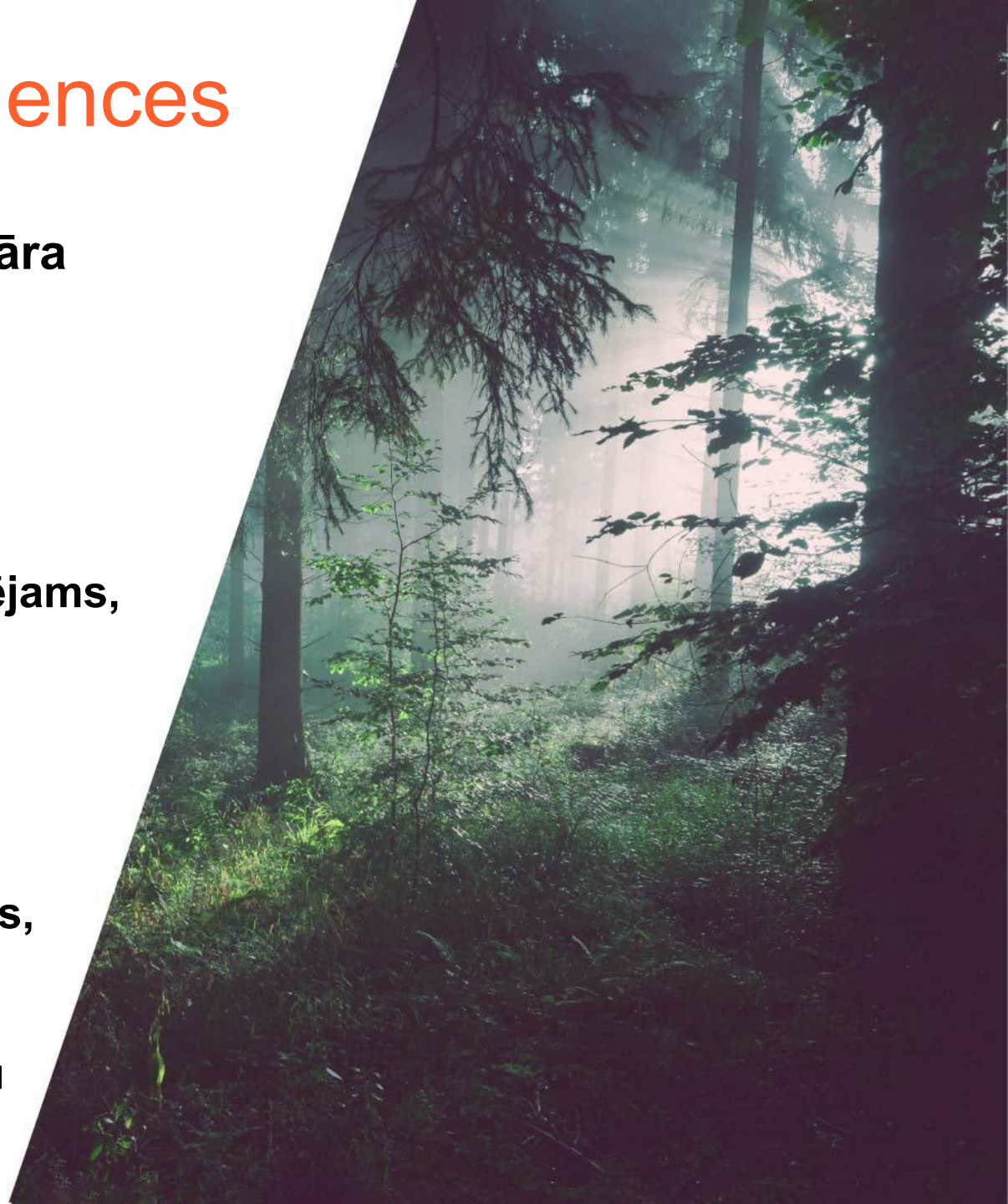
Uzbrucēja profils

- **Citas valsts atbalstītas kiberoperācijas**
- **Informācijas operācijas**
- **Finansiāli motivēti uzbrucēji, kurus, iespējams, piesedz agresora valsts**

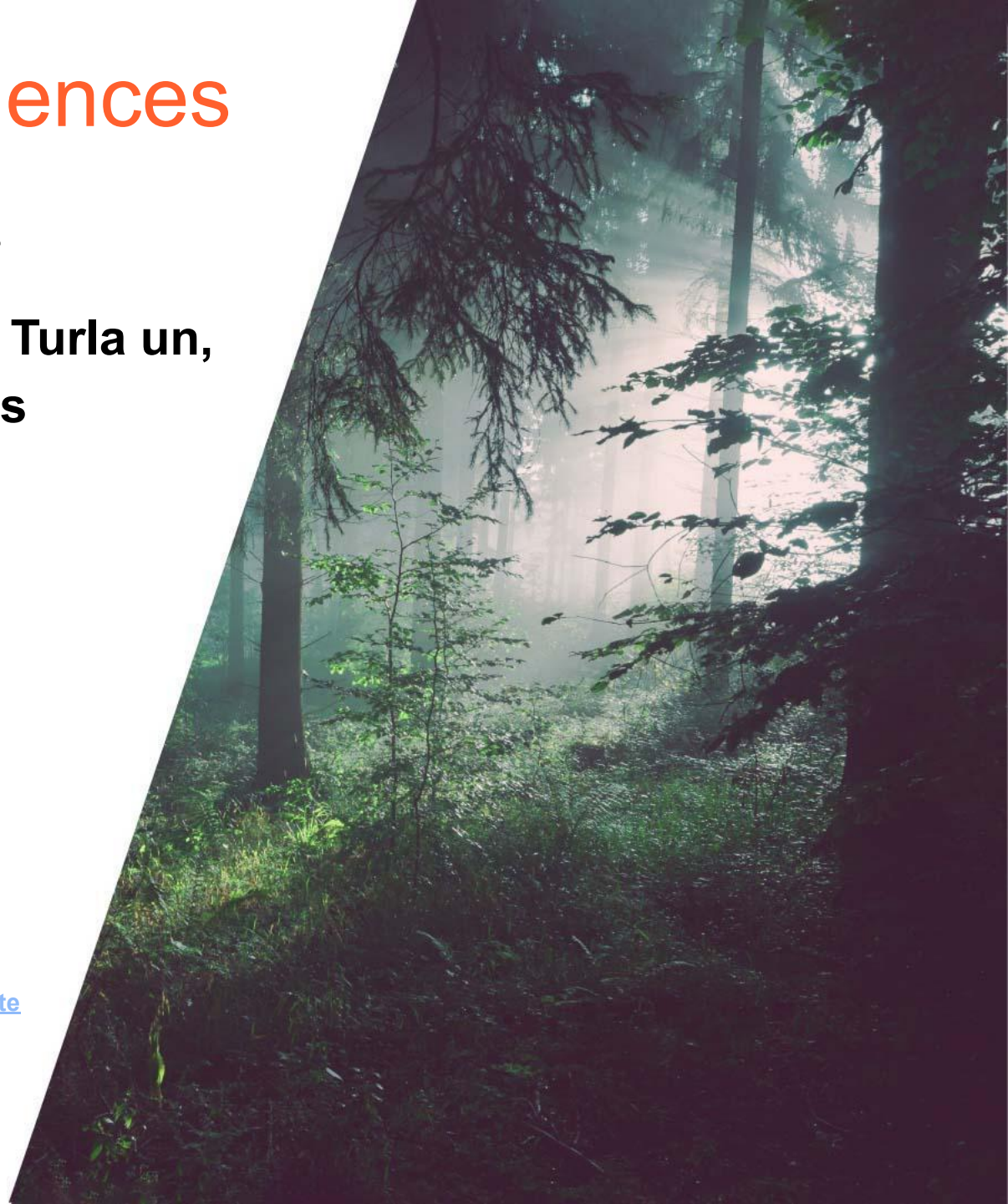
Agresors visu augstākminēto pielieto vienkopus, vienam otru papildinot.

Pielieto arī iepriekš izstrādātus mērķus/operācijas, kuros klātbūtne ir bijusi jau ilgāku laiku

Liels skaits jaunu kompromitēšanas mēģinājumu



Apdraudējuma tendences



Ar ko mums ir darīšana un kāda ir izcelsme?

Ar ausgtu ticamību NOBELIUM, Ghostwriter, Turla un, ispējams, citas RU atbalstītas kiberoperācijas

Līdz šim pret Latviju jau realizēti uzbrukumi

- **Programmatūras izstrādes un IT pakalpojumu uzņēmumi**
- **Telekomunikāciju operatori (un atsevišķi pakalpojumi)**
- **Valsts un pašvaldību iestādes**
- **Kritiskā infrastruktūra**
- **Finanšu sektors**
- **RU dezinformācijas pētnieki**

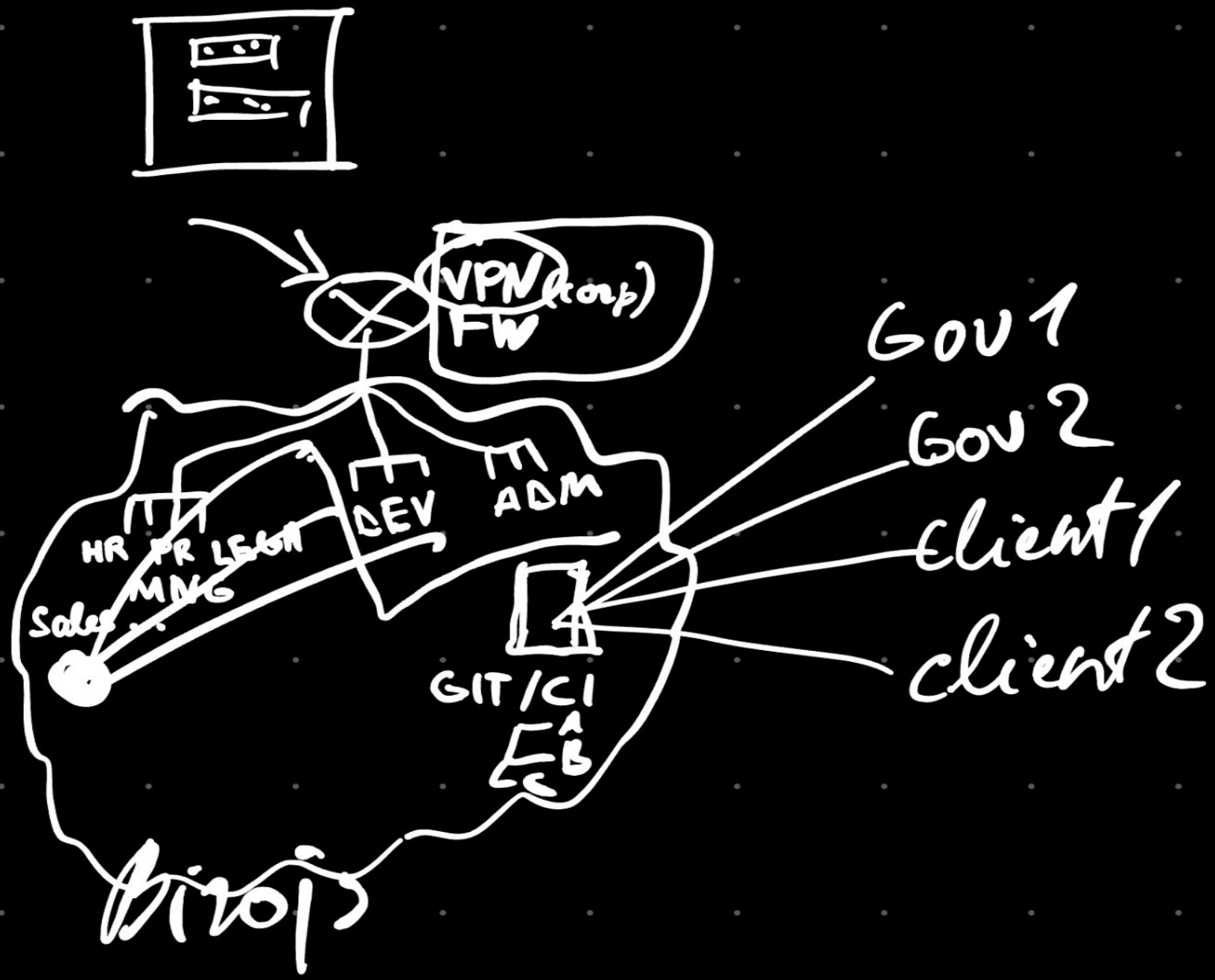
https://www.microsoft.com/security/blog/2021/11/10/the-hunt-for-nobelium-the-most-sophisticated-nation-state-attack-in-history/

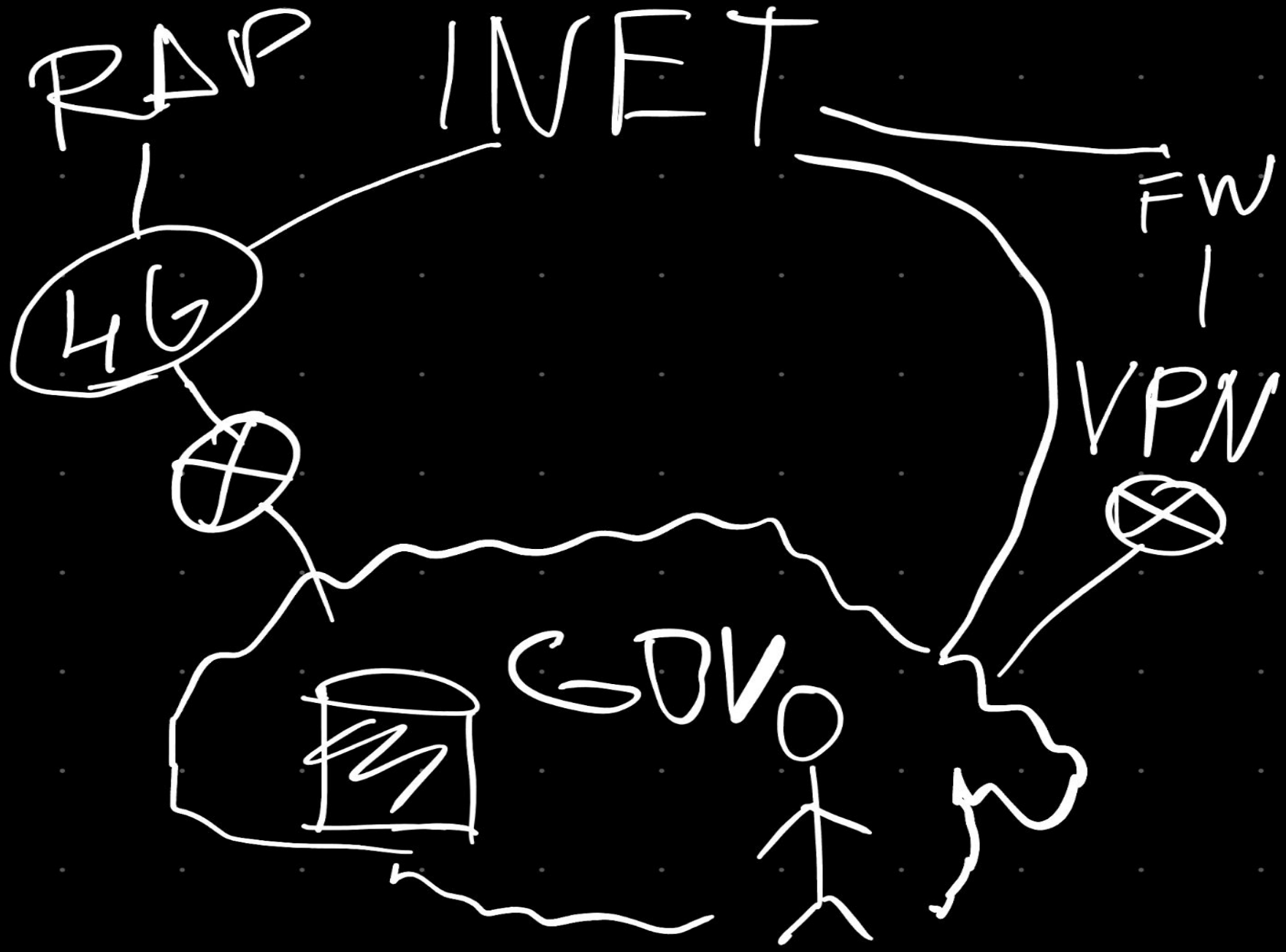
Valsts noz
- IaC
- DDoS
- app uzbr
- infrastr

auth pakalp
- bankas
- vienotā pieteikšanās

WEB
- config/GITexpose
- vuln
- CMS

Cloud
- ~~MFA~~
- ~~konta revīzija~~
- ~~auditācija~~


VPN
FW
DEV
ADM
HR
MNG
GIT/CI
Gov 1
Gov 2
client 1
client 2

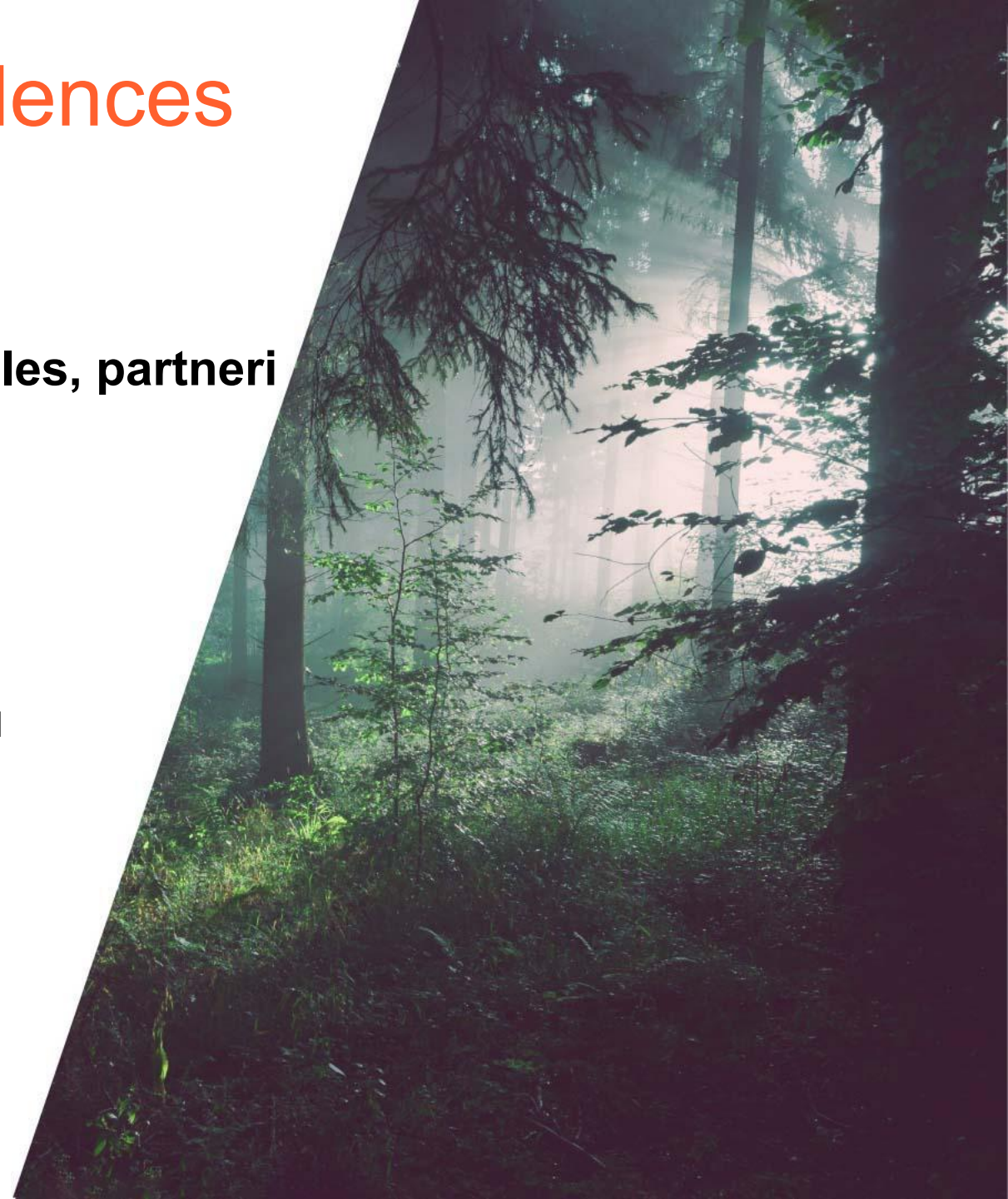

RAP
INET
FW
4G
VPN
GOV

Apdraudējuma tendences

- **VPN vārtejas, mērķis - korporatīvais tīkls**
  - **spiegošana, informācijas izgūšana**
  - **piekļuves paplašināšana - klienti, filiāles, partneri**
  - **sabotāža, destruktīvas darbības**

Kā sargāt?

- **jāmonitorē / jāierobežo pieslēgumi**
  https://www.nic.lv/lix
  vēl labāk izveidot savu balto sarakstu
- **ptch**
- **log**
- **droša konfigurācija + MFA / 2FA**



Apdraudējuma tendences

- **CMS - satura vadības sistēmas (wp,drupal)**
  - **patch**
  - **rezerves kopijas un to integritāte**
  - **attālināta žurnalēšana un monitorings**
  - **atkopšanās plāna tests**
  - **RO operāciju režīms (konteinerizēt)**
  - **No servera izejošās konekcijas (whitelist)**
  - **pieslēgumu ierobežošana admin sadaļai**

Piegādes piemēri

- SpearPhishing
  - Tematiski sagatavoti e-pasti, īsi teksti, pārsvarā angļu un latviešu valodās
  - Izsūta no jau kompromitētām iestādēm citu valstu GOV sektorā
    - ES valsts policija
    - ES valsts iestādes
    - Trešo valstu pub. sektora iestādes
  - saites uz lejuplādi leģitīmās, kompromitētās vietnēs, vai file sharing platformas
  - pielikums ar html, arhīvu, iso, .img, .xlx, xlsb, xlsx, docx, doc, utt

APT RU SunFlowerSeed

WhisperGate
- Wiper

Hermetic
- Wiper
  - Trojan.Killdisk
  - FoxBlade
- Wizard
  - Worm containing Wiper
- Ransom
  - PartyTicket
  - SonicVote

IsaacWiper
- Wiper

ACTINIUM / Gamaredon

Ghostwriter/UNC-1151/TA445
- Asylum Ambuscadec
  - SpearPhish + Attachment
    - XLS
      - Macro
      - Pcode
      - Stream.7
    - Lua/Sunseed

Sandworm
- CyclopsBlink
  - Elf executable
    - PowerPC
      - WatchGuard Firebox
      - SOHO

Delivery Methods
- GlowSpark
  - Document
    - VBA
- Discord

Get Messages | Write | Chat | Address Book | Tag

From [redacted] <[redacted]> Reply | Reply All | Forward | More

Subject **NV Absense of Ambassador of [redacted]** 2/8/22, 08:04

Dear All,

Please be guided by the Note Verbal attached.

Kind regards

[redacted]

Assistant to the Ambassador

REPÚBLICA

[redacted]

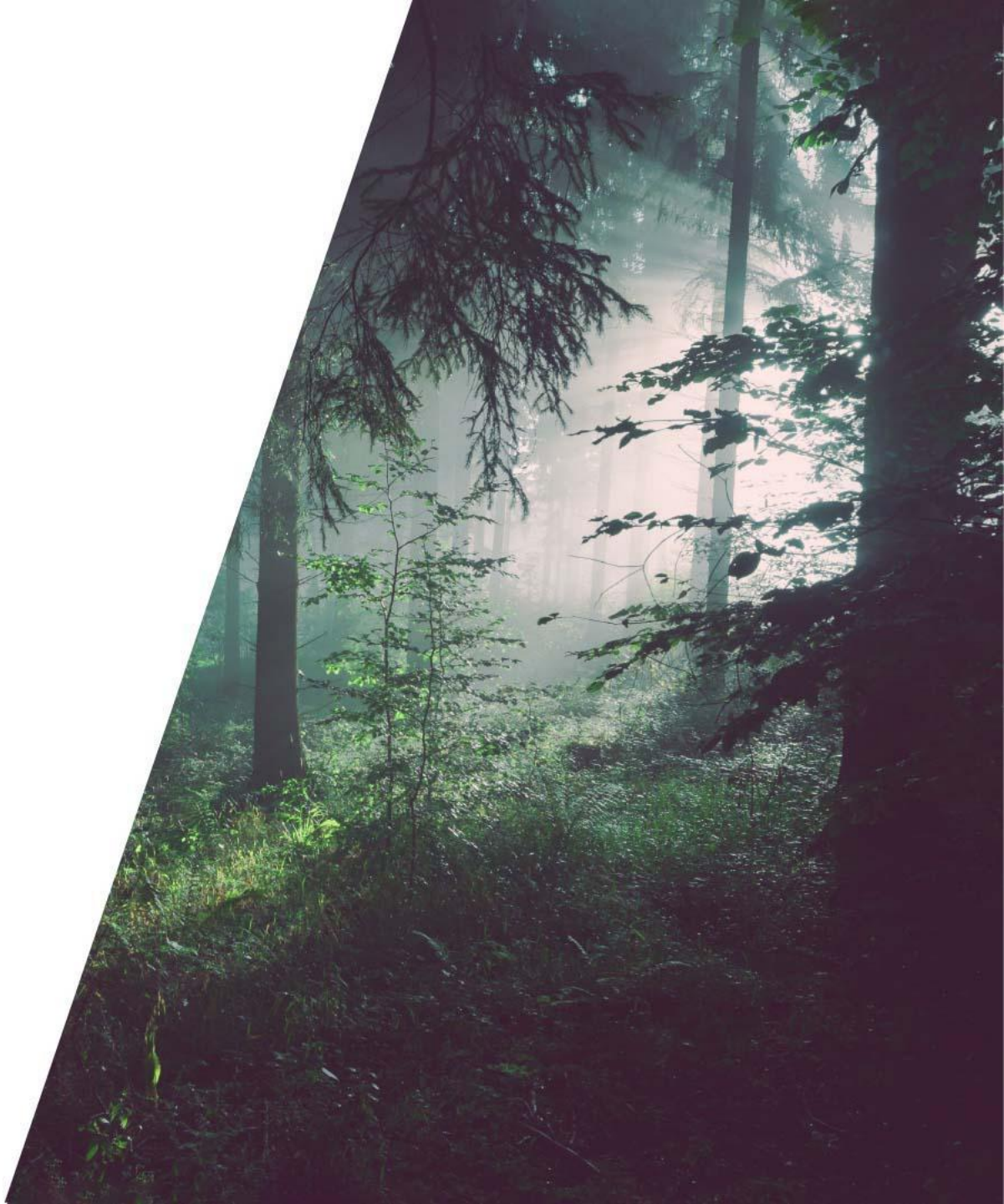
[redacted]

Por favor, tenha em consideração o ambiente antes de imprimir.

—OutlookEmoji-Inline image OWAPstImg215210465e5f30-d4cc-48b7-bc4e-aaf621620a24.png————

—OutlookEmoji-Inline image OWAPstImg663528ee95a2dc-c1b9-44e7-9ff1-a2265de7596b.png————

UNITED NATIONS OCEAN CONFERENCE LISBON



Get Messages | Write | Chat | Address Book | Tag

From [redacted]ida <cr[redacted]pt>

Reply | Reply All | Forward | More

Subject **[SPAM] 2022-0102**

2/14/22, 04:31

[redacted]da compartilhou um arquivo com você

Aqui fica o documento que [redacted]a partilhou convosco.

fatura 2022-0102 <https://login.potug[redacted]/heLPtNgz>

Este link funcionará para qualquer pessoa.

Abrir <https://login.potugal[redacted]m/heLPtNgz>

PrivacyStatement <https://login.potugal[redacted]m/heLPtNgz>

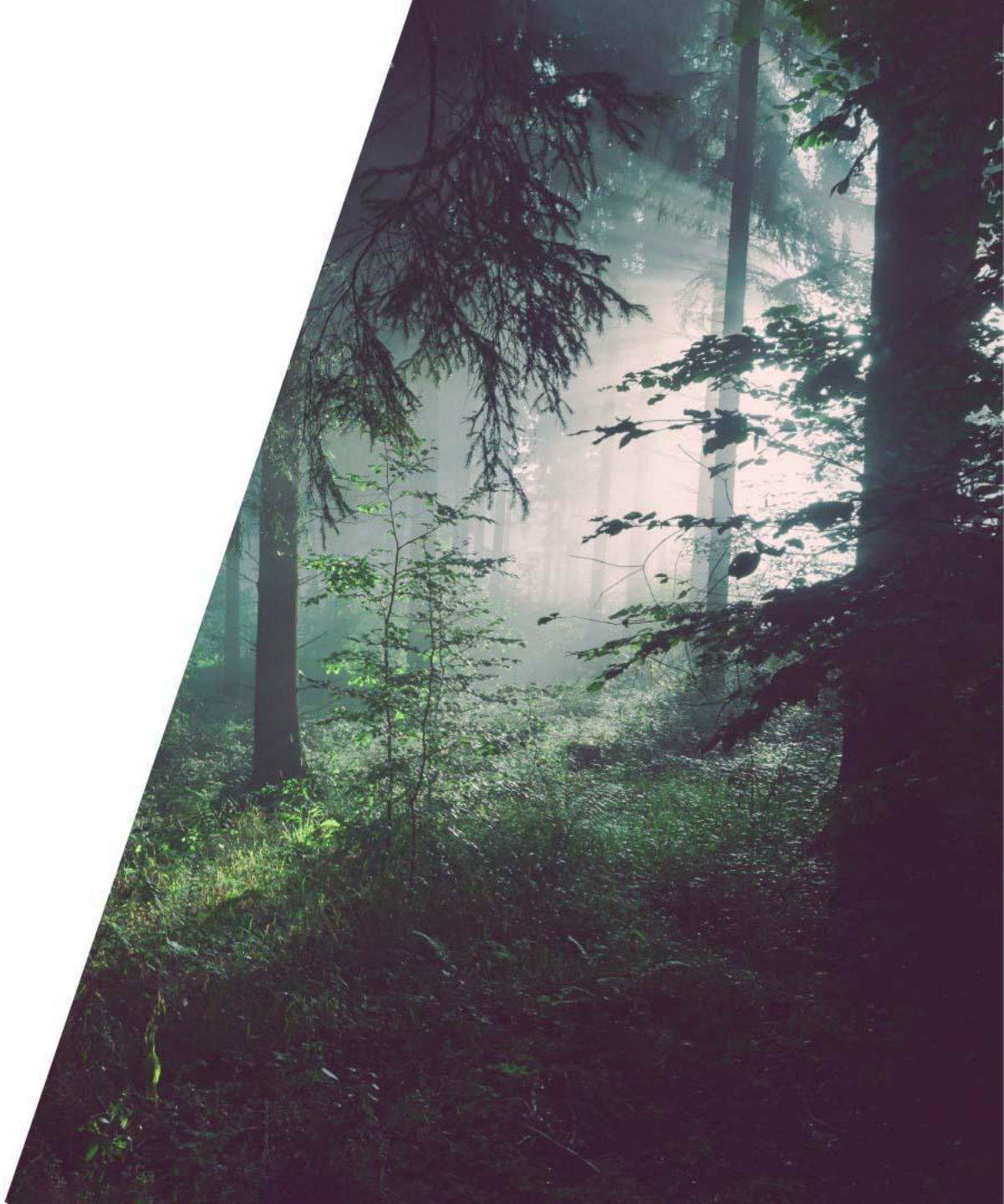
image001.png

image002.png

image003.png

image004.png

Microsoft



File Edit View Go Message Tools Help

Get Messages | Write | Chat | Address Book | Tag

From [redacted]

Reply | Reply All | Forward | More

Subject **Re: Questionnaire on [redacted] Community of Interest**

2/16/22, 09:46

To Info <Info@[redacted]

To protect your privacy, Thunderbird has blocked remote content in this message. Preferences

Šis ir ārējs e-pasts, lūdzu pievērsiet uzmanību avota autentiskumam.

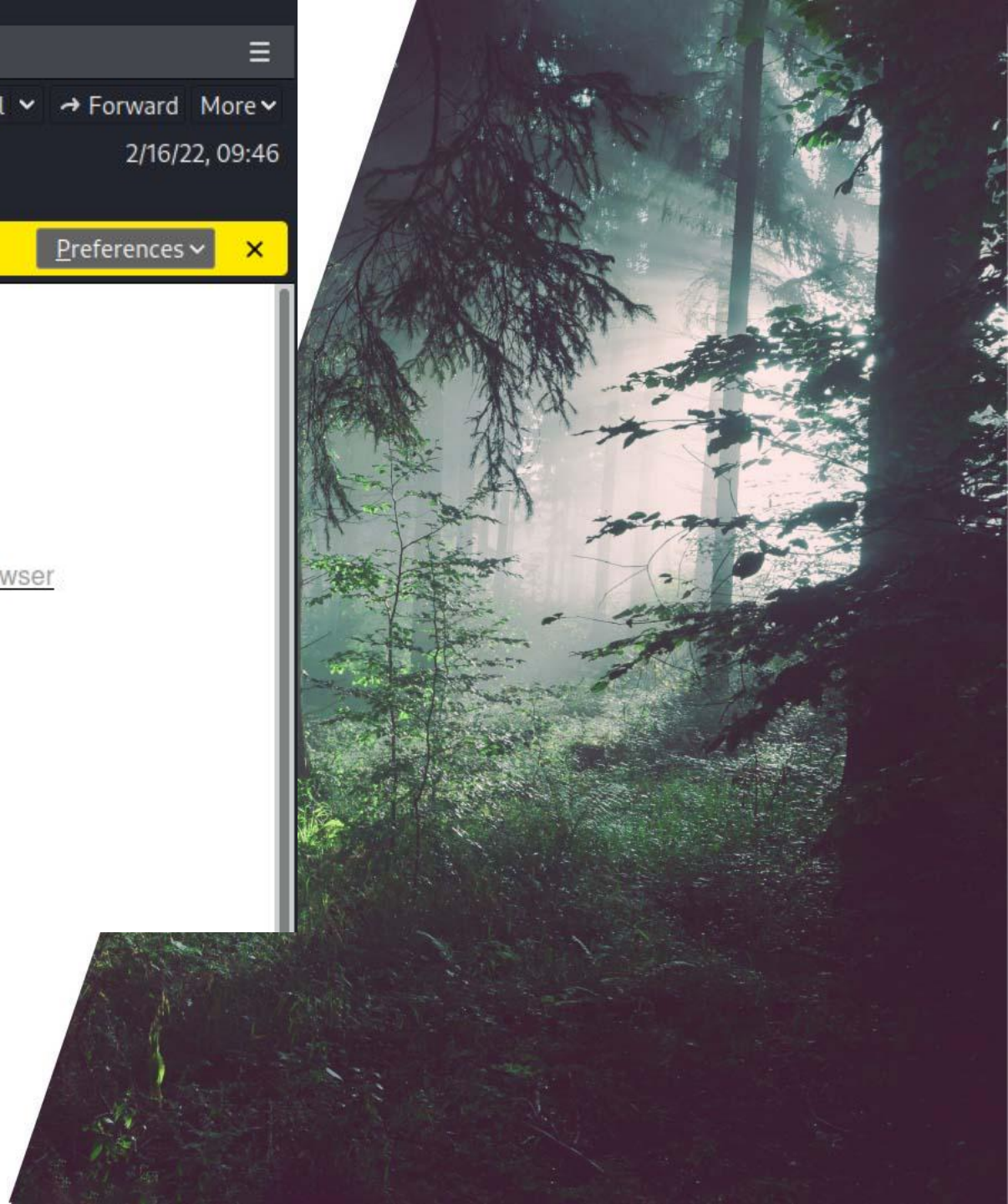
Hello!
All requested documents can be found below.

https://andre[redacted]al.cl/tlataecpe/aeruuctreiqrreuoqhiocsrnutei--

View this email in your browser

Questionnaire on [redacted] Community of Interest

[redacted] community



Get Messages | Write | Chat | Address Book | Tag

From Robert <r@gmail.com> Reply Reply All

Subject **Re: Request for SFiles**

To redacted <redacted@>

Dear

Please check these documents and inform me if we should to correct anything else.

Link: https://www./Documents/TopSecret20210127023.zip

Password for zip: @WHO1

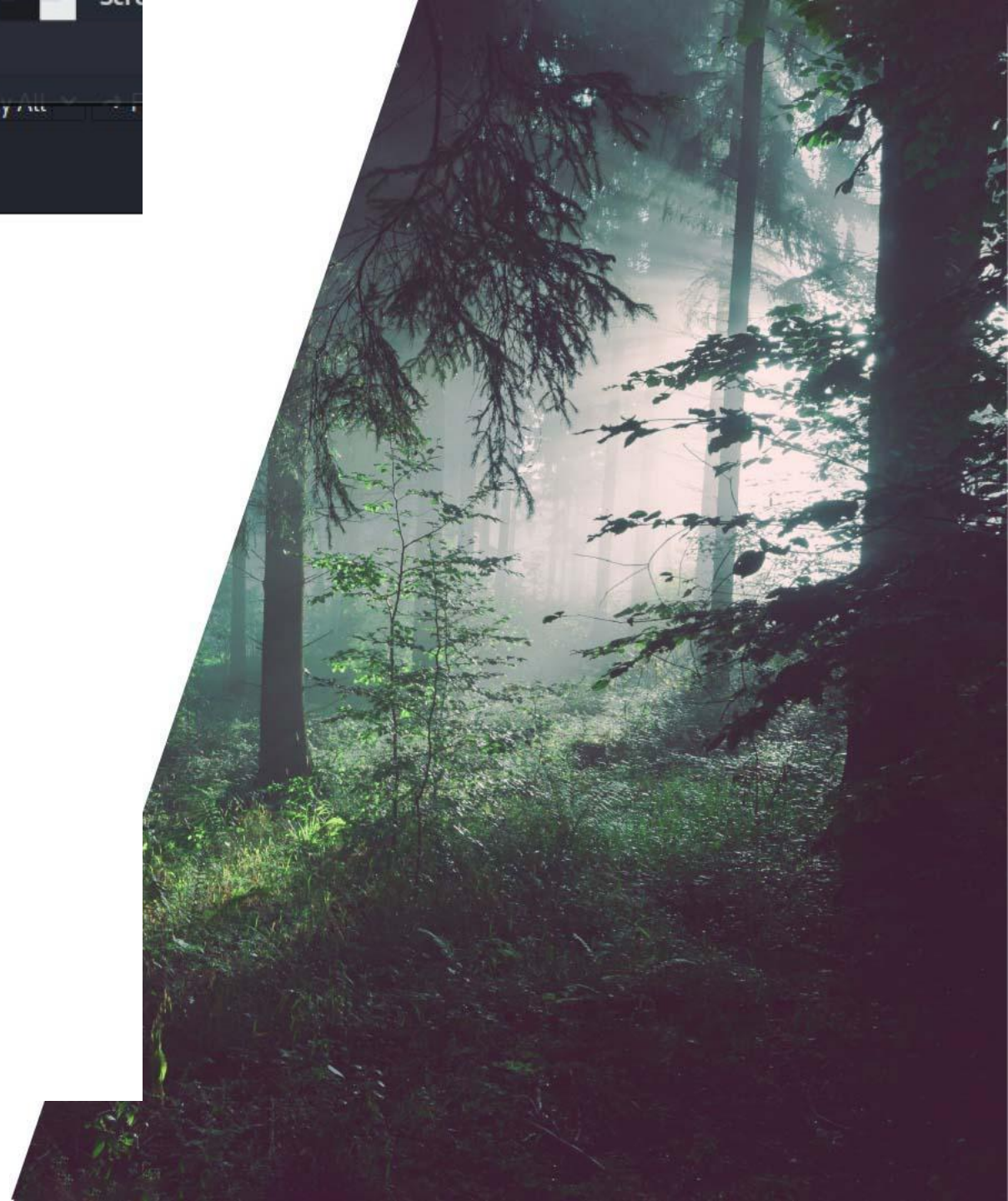
Regards...

From: >
Sent: Saturday, January 23, 2021 5:01 PM
To:
Cc:
Subject: Re: Request for SFiles

Hi

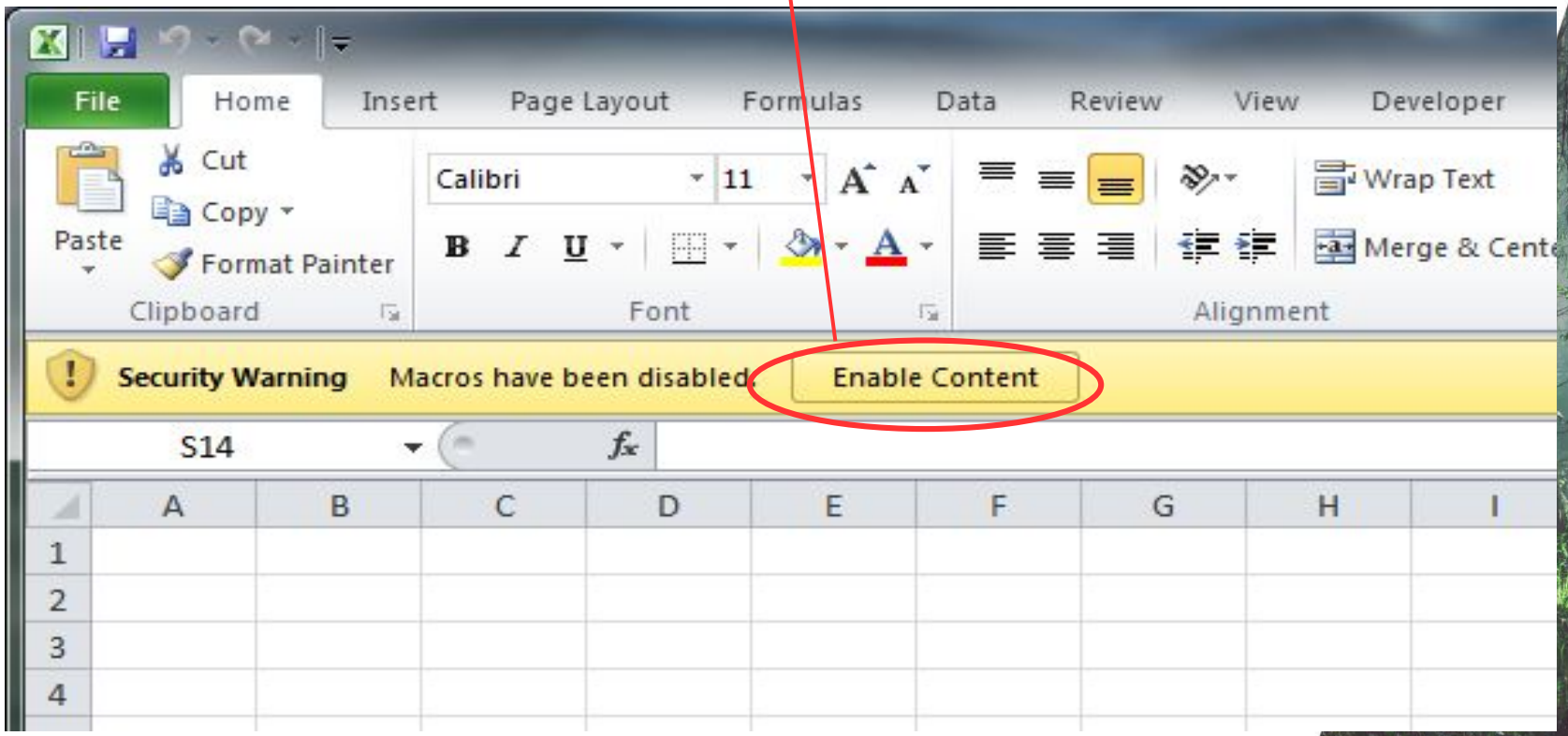
I asked about the topic, but the person who contacted me did not have any information.

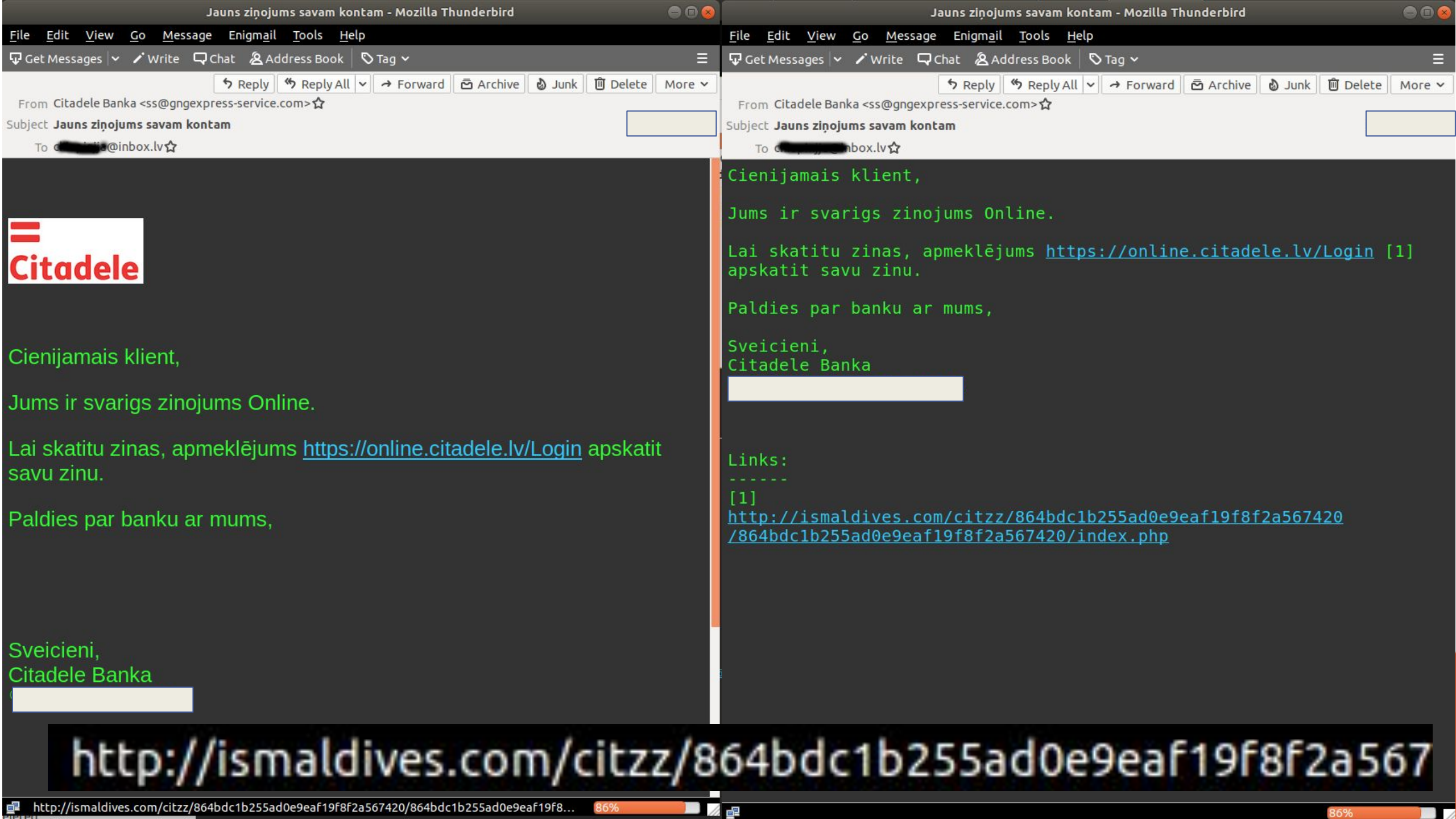
Will look forward to more info from you towards the middle of the week.



Piegādes piemēri

Jābūt atslēgtam sistēmas līmenī!!!




Jauns ziņojums savam kontam - Mozilla Thunderbird
File Edit View Go Message Enigmail Tools Help
Get Messages Write Chat Address Book Tag
Reply Reply All Forward Archive Junk Delete More
From Citadele Banka <ss@gngexpress-service.com>
Subject Jauns ziņojums savam kontam
To [redacted]@inbox.lv
Citadele
Cienijamais klient,
Jums ir svarigs zinojums Online.
Lai skatitu zinas, apmeklējums https://online.citadele.lv/Login apskatit savu zinu.
Paldies par banku ar mums,
Sveicieni,
Citadele Banka
Jauns ziņojums savam kontam - Mozilla Thunderbird
File Edit View Go Message Enigmail Tools Help
Get Messages Write Chat Address Book Tag
Reply Reply All Forward Archive Junk Delete More
From Citadele Banka <ss@gngexpress-service.com>
Subject Jauns ziņojums savam kontam
To [redacted]nbox.lv
Cienijamais klient,
Jums ir svarigs zinojums Online.
Lai skatitu zinas, apmeklējums https://online.citadele.lv/Login [1] apskatit savu zinu.
Paldies par banku ar mums,
Sveicieni,
Citadele Banka
Links:
------
[1]
http://ismaldives.com/citzz/864bdc1b255ad0e9eaf19f8f2a567420/864bdc1b255ad0e9eaf19f8f2a567420/index.php
http://ismaldives.com/citzz/864bdc1b255ad0e9eaf19f8f2a567
http://ismaldives.com/citzz/864bdc1b255ad0e9eaf19f8f2a567420/864bdc1b255ad0e9eaf19f8...
86%
86%

Piegādes piemēri

NV.html

--> javascript

--> NV.img

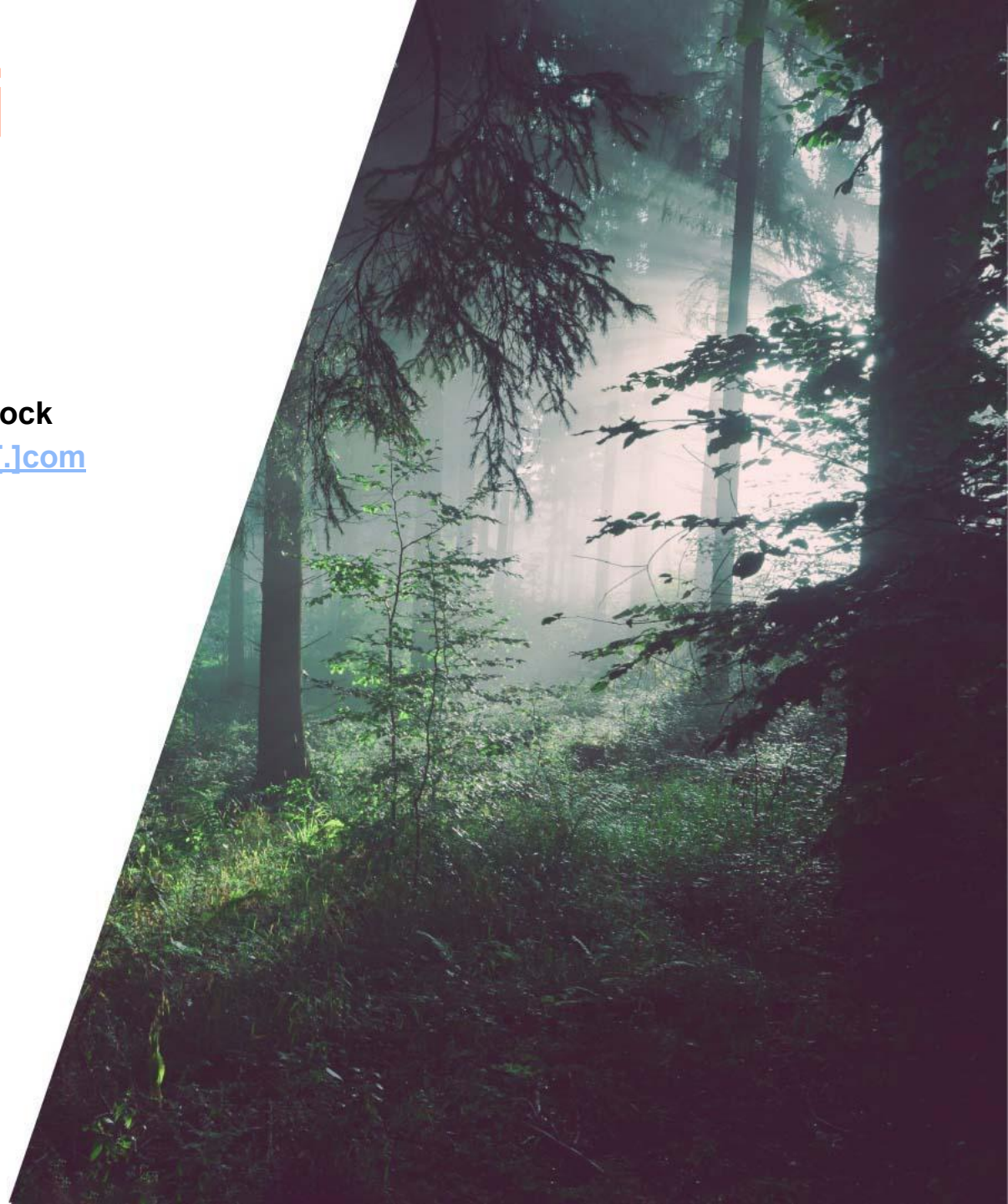
--> NV.lnk

--> rundll32.exe msvcr170.dll CRTRuntimePPLLock

--> Network connection to https://api.trello[.]com

Document.pdf.exe ←!!!?

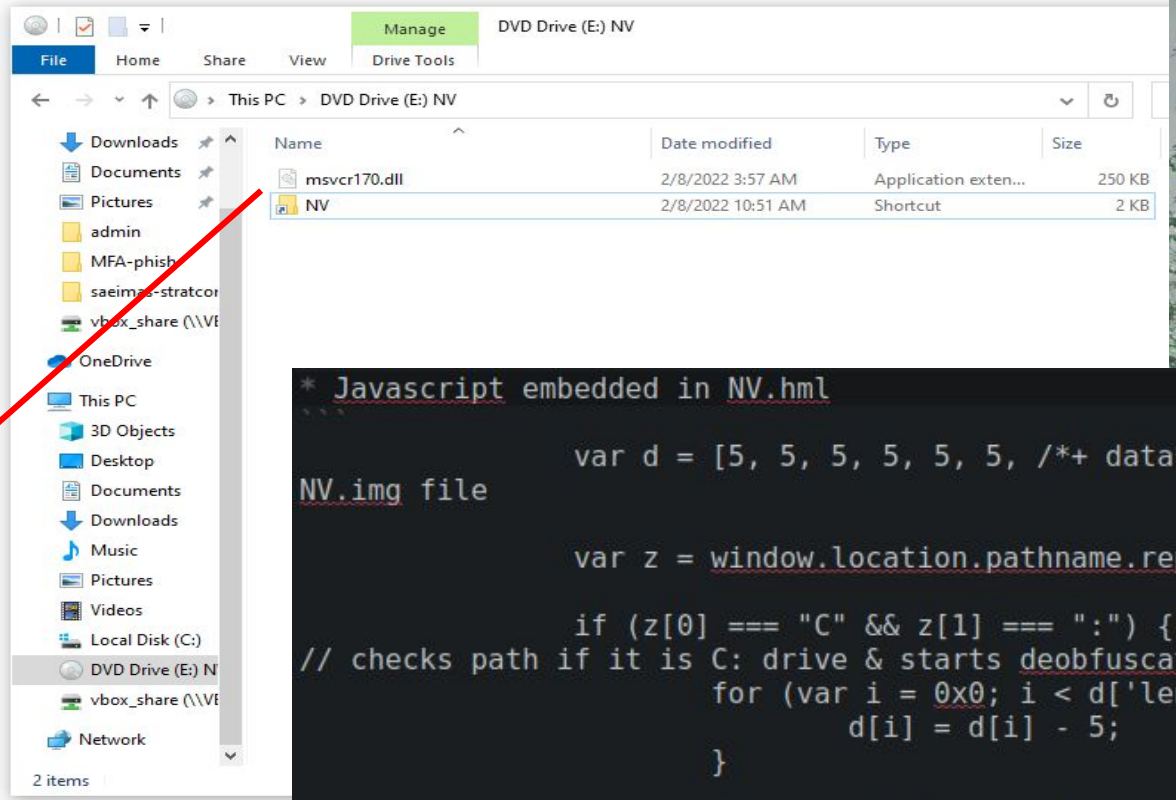
attachment: somefile.pdf.exe
attachment: somefile.zip
attachment: somefile.xlsx
attachment: somefile.xlsb
attachment: somefile.iso
attachment: somefile.img
attachment: somefile.html
attachment: somefile.hta
attachment: somefile.lnk



NV.html

File | C:/NV.html

Atverot e-pasta pielikumu…




```
* Javascript embedded in NV.hml
```

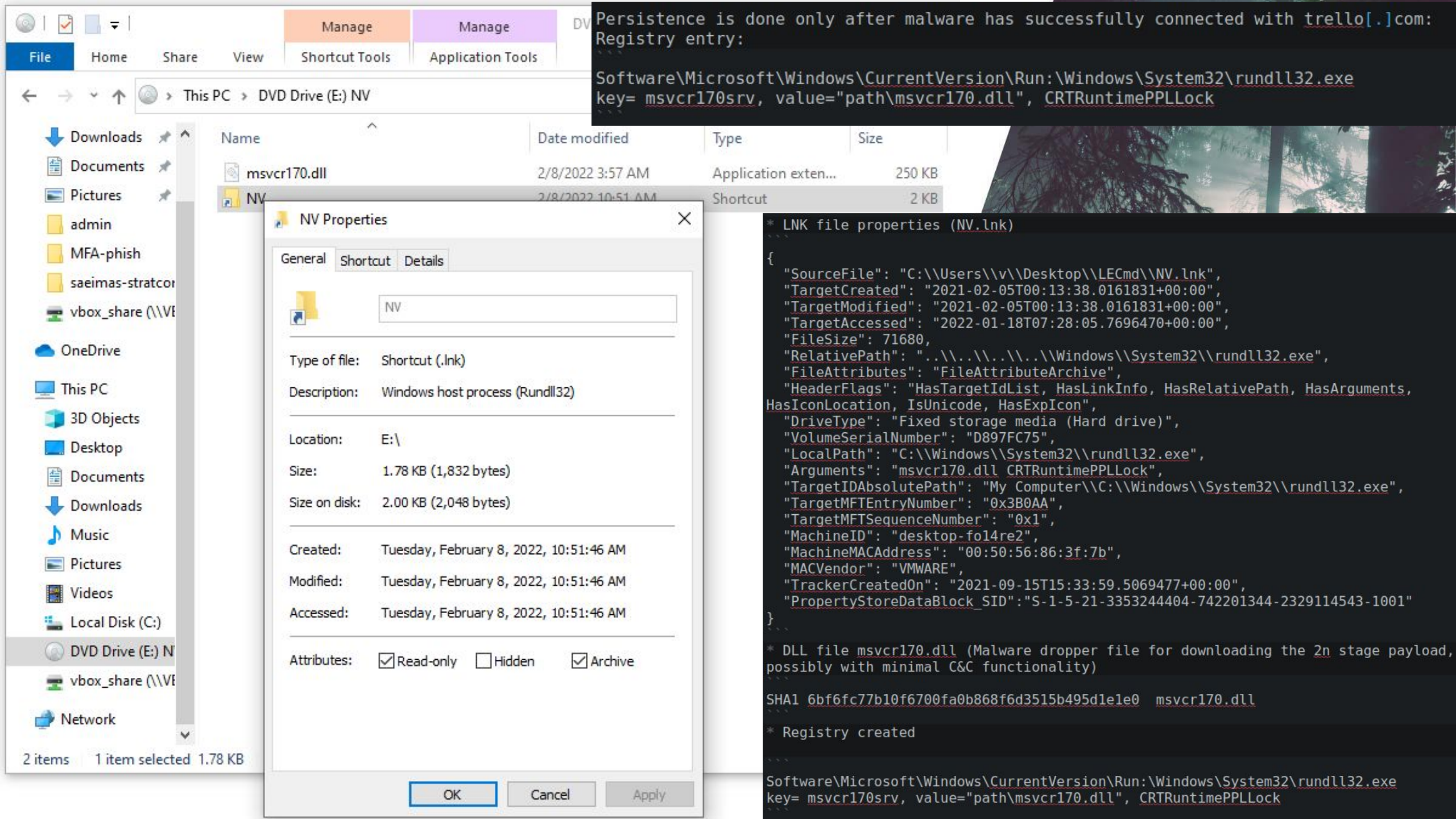
```
                var d = [5, 5, 5, 5, 5, 5, /*+ data*/]; //obfuscated (with byte[x]-5)
NV.img file

                var z = window.location.pathname.replace('/', '');

                if (z[0] === "C" && z[1] === ":") {
// checks path if it is C: drive & starts deobfuscation routine
                        for (var i = 0x0; i < d['length']; i++) {
                                d[i] = d[i] - 5;
                        }

                        e = new Uint8Array(d);
                        f = new Blob([e], { type: "application/octet-stream" });
                        saveAs(f, "NV.img");
                } else { }
```

NV.img
Open file



Persistence is done only after malware has successfully connected with trello[.]com:
Registry entry:

```
Software\Microsoft\Windows\CurrentVersion\Run:\Windows\System32\rundll32.exe
key= msvcr170srv, value="path\msvcr170.dll", CRTRuntimePPLLock
```

* LNK file properties (NV.lnk)

```
{
  "SourceFile": "C:\\Users\\v\\Desktop\\LECmd\\NV.lnk",
  "TargetCreated": "2021-02-05T00:13:38.0161831+00:00",
  "TargetModified": "2021-02-05T00:13:38.0161831+00:00",
  "TargetAccessed": "2022-01-18T07:28:05.7696470+00:00",
  "FileSize": 71680,
  "RelativePath": "..\\..\\..\\..\\Windows\\System32\\rundll32.exe",
  "FileAttributes": "FileAttributeArchive",
  "HeaderFlags": "HasTargetIdList, HasLinkInfo, HasRelativePath, HasArguments,
HasIconLocation, IsUnicode, HasExpIcon",
  "DriveType": "Fixed storage media (Hard drive)",
  "VolumeSerialNumber": "D897FC75",
  "LocalPath": "C:\\Windows\\System32\\rundll32.exe",
  "Arguments": "msvcr170.dll CRTRuntimePPLLock",
  "TargetIDAbsolutePath": "My Computer\\C:\\Windows\\System32\\rundll32.exe",
  "TargetMFTEntryNumber": "0x3B0AA",
  "TargetMFTSequenceNumber": "0x1",
  "MachineID": "desktop-fo14re2",
  "MachineMACAddress": "00:50:56:86:3f:7b",
  "MACVendor": "VMWARE",
  "TrackerCreatedOn": "2021-09-15T15:33:59.5069477+00:00",
  "PropertyStoreDataBlock_SID":"S-1-5-21-3353244404-742201344-2329114543-1001"
}
```

* DLL file msvcr170.dll (Malware dropper file for downloading the 2n stage payload, possibly with minimal C&C functionality)

```
SHA1 6bf6fc77b10f6700fa0b868f6d3515b495d1e1e0  msvcr170.dll
```

* Registry created

```
Software\Microsoft\Windows\CurrentVersion\Run:\Windows\System32\rundll32.exe
key= msvcr170srv, value="path\msvcr170.dll", CRTRuntimePPLLock
```

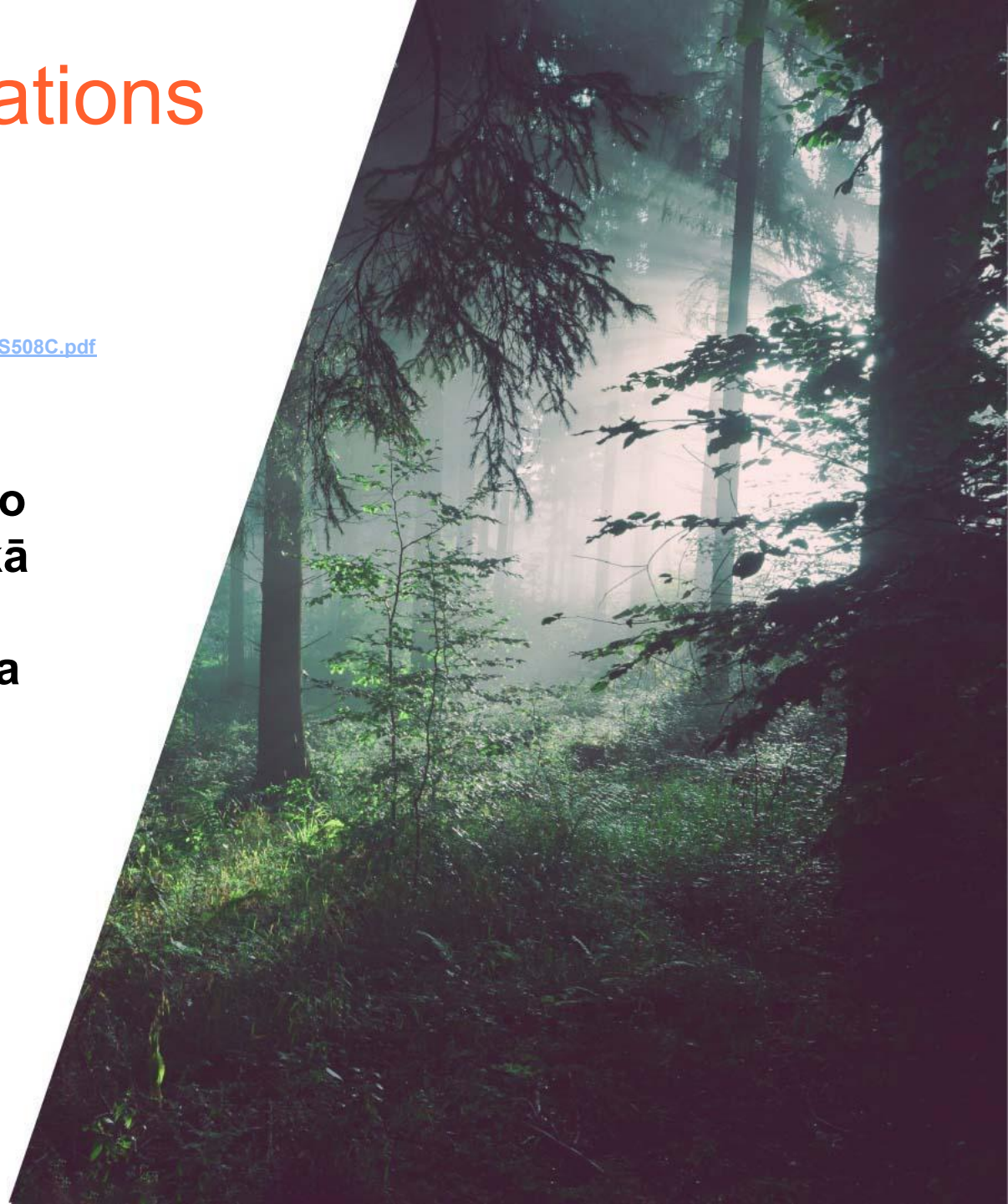
Threat hunting operations

- **Mērķa iestādēm jānodrošina spēja stradāt draudu medību režīmā**
  - **Centralizēta telemetrija no AD un darbstacijām, no standalone iekārtām, tīkla, VPN, operacionāli kritiskām komponentēm**
  - **uz laiku ierobežot starpsavienojumus**
  - **panākt segmentāciju kaut vai ar windows host firewall**

Threat hunting operations

- **Cenšamies runāt vienā valodā**
  - **Threat hunting with YARA**
    https://www.cisa.gov/uscert/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_YARA_S508C.pdf

Recepte aptuveni šāda:
1) Izveido tīkla koplietošanas disku
2) Ar GPO pievieno katrai mašīnai tīkla disku no kura paņem un izpilda Yara.exe un Yara rules kā input parametrus
3) Rezultātu ar unikālu mašīnas ID ieraksta tīkla diskā
4) Analizē rezultātus



CERT.LV

Threat hunting operations

```
rule MSG_html_file_artifacts_99{
   meta:
      score = 99
      description = "detects NOBELIUM email attachment"
      author = "CERT.LV"
      date = "12.02.2022"
   strings:
      $a1 = "application/octet-stream"
      $a2 =  /saveAs\(\S, \S+\.img\"\)/
      $a3 = "var d = [5,5"
      $a4 =
"5,5,5,5,5,5,5,5,5,5,5,6,72,73,53,53,54,6,5,37,37,37,37,37,37,37,37,37,37"
      $a5 = "d[i]=d[i] -5;"
   condition:
      (#a1 > 1) and all of them
}
```

Threat hunting operations

- **Cenšamies runāt vienā valodā**
  - **Yara** https://github.com/VirusTotal/yara/releases
  - **Loki** https://github.com/Neo23x0/Loki
  - **Threat hunting with SIEM**
    - **SysMon**
    - **EDR (Endpoint detection and response)**
    - **Security Onion**
    - **ELK & HELK stack**

https://cert.lv/lv/2022/02/cert-lv-ieteikumi-saasinoties-geopolitiskajai-situacijai-eiropa-un-pieaugot-kiberdraudiem

https://cert.lv/lv/2022/02/cert-lv-ieteikumi-saasinoties-geopolitiskajai-situacijai-eiropa-un-pieaugot-kiberdraudiem

https://cert.lv/lv/2021/03/kompromiteta-domena-atpazisana-un-atgusanas-pec-uzbrukuma

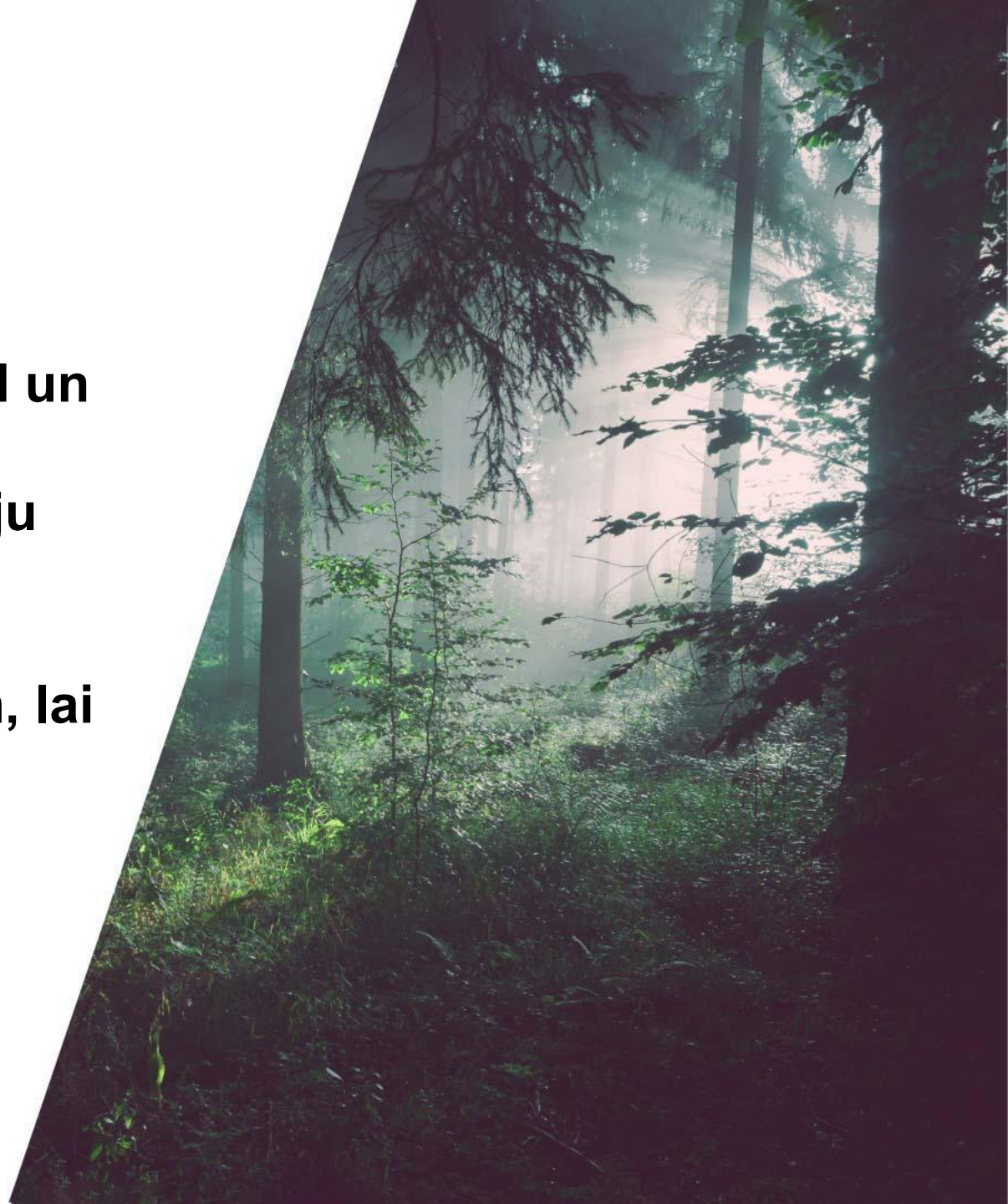
https://cert.lv/lv/2021/03/it-drosibas-incidenta-pieradijumu-materiala-iegusana-operativa-atmina

https://labs.f-secure.com/blog/attack-detection-fundamentals-discovery-and-lateral-movement-lab-5/

https://github.com/Neo23x0/Loki

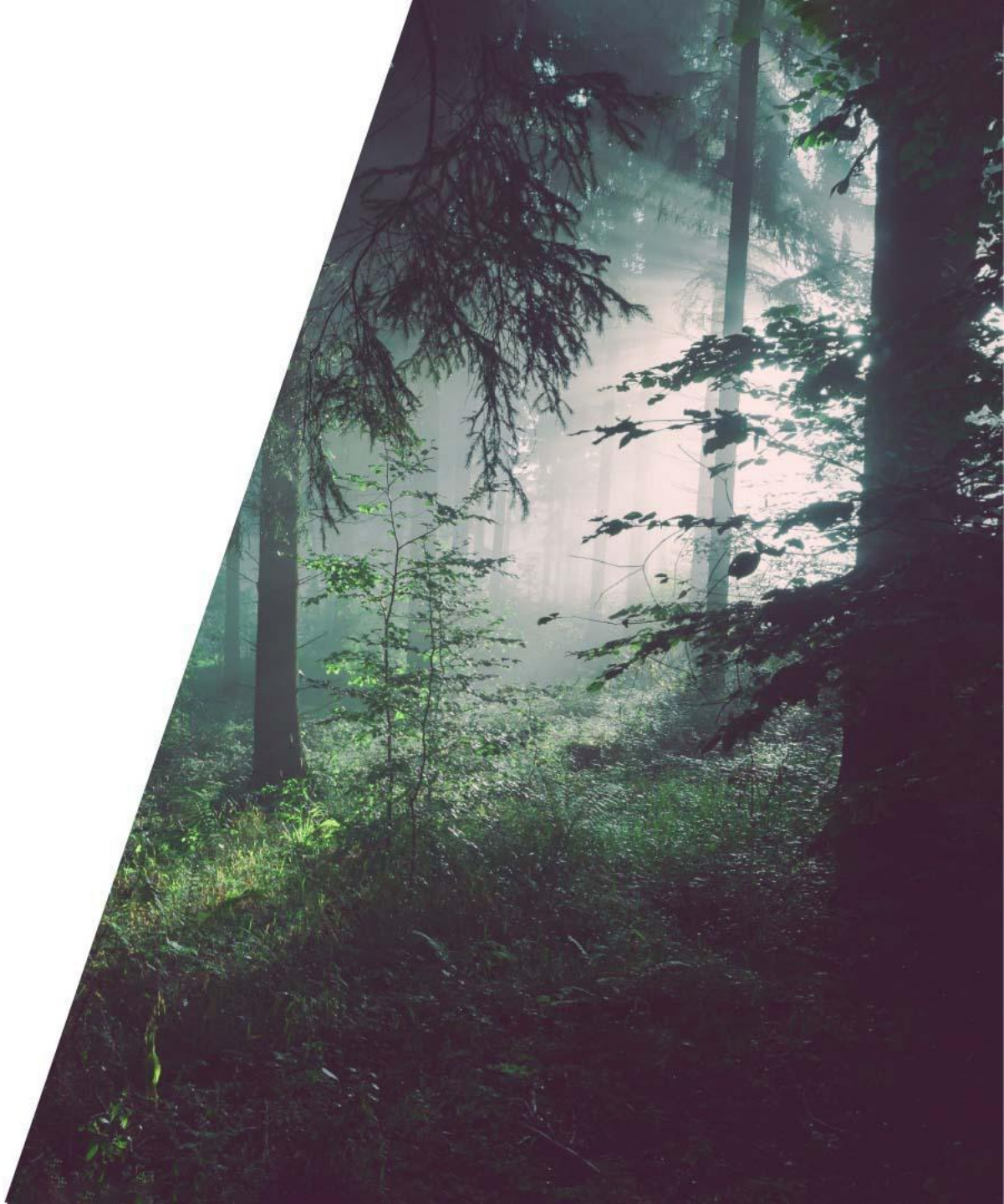
Mērķi Latvijā

- **Valsts tēla bojāšana - jābūt kaut kam redzamam**
  - **Tīmekļvietnes, Webmail, nextcloud un citi eksponētie servisi**
  - **Politiķu, valsts iestāžu, organizāciju sociālo tīklu profili, e-pasti, info noplūdes**
  - **Servisa atteices latvija.lv un citiem, lai sabiedrība sajūt**
  - **viss, kas ir .gov.lv**
  - **ikviena pašvaldība**



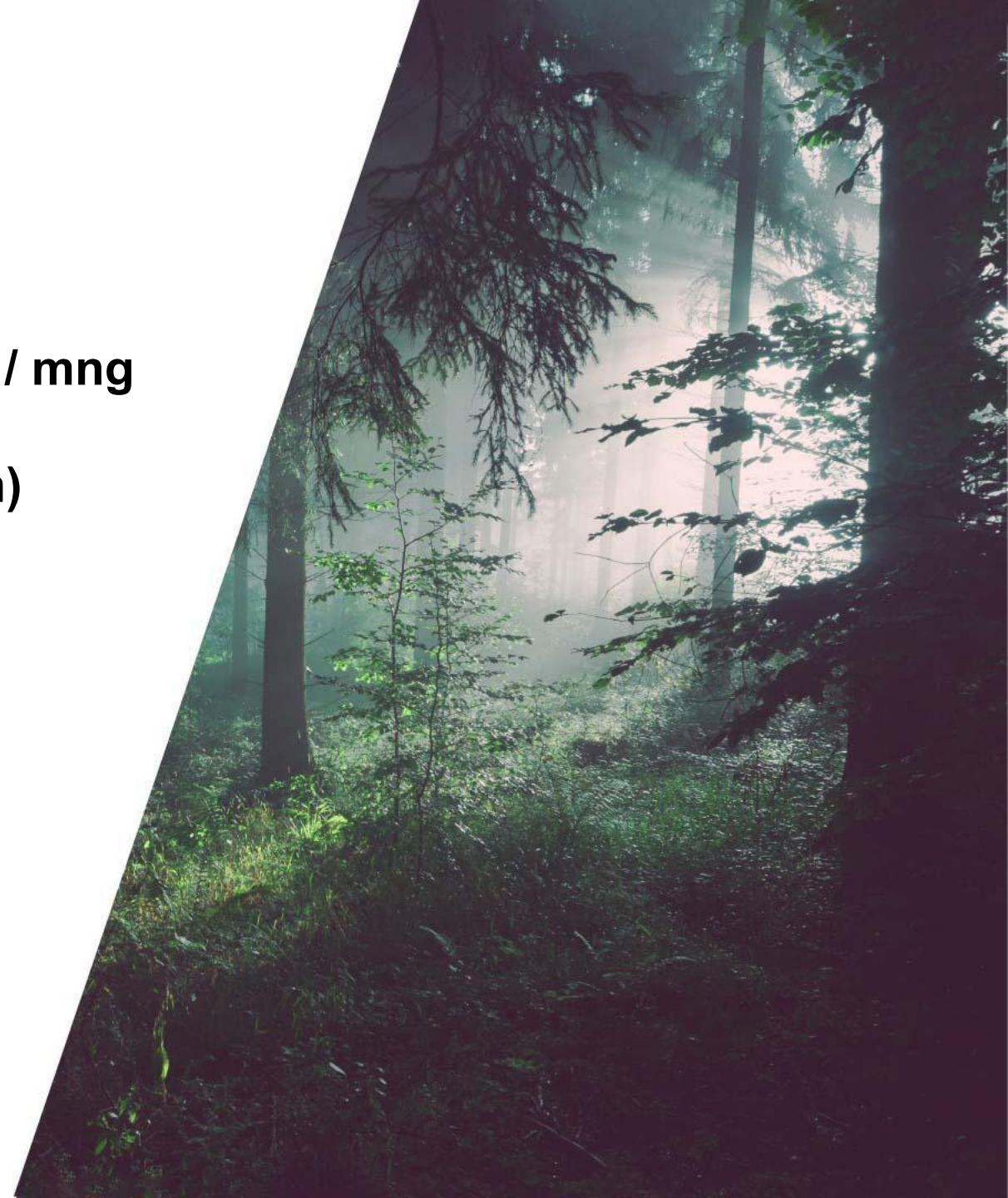
Mērķi Latvijā

- **Kritiskā infrastruktūra**



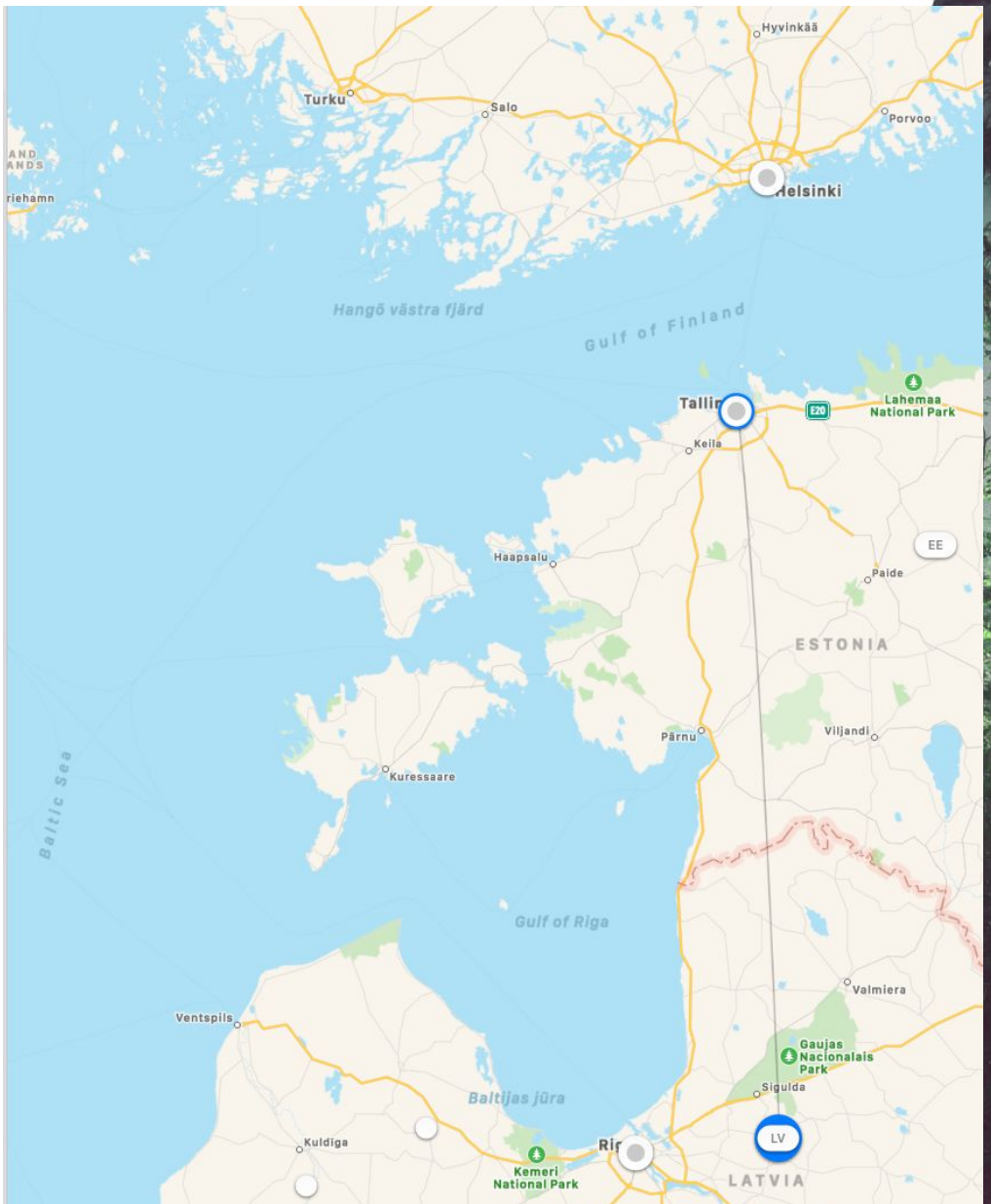
Mērķi Latvijā

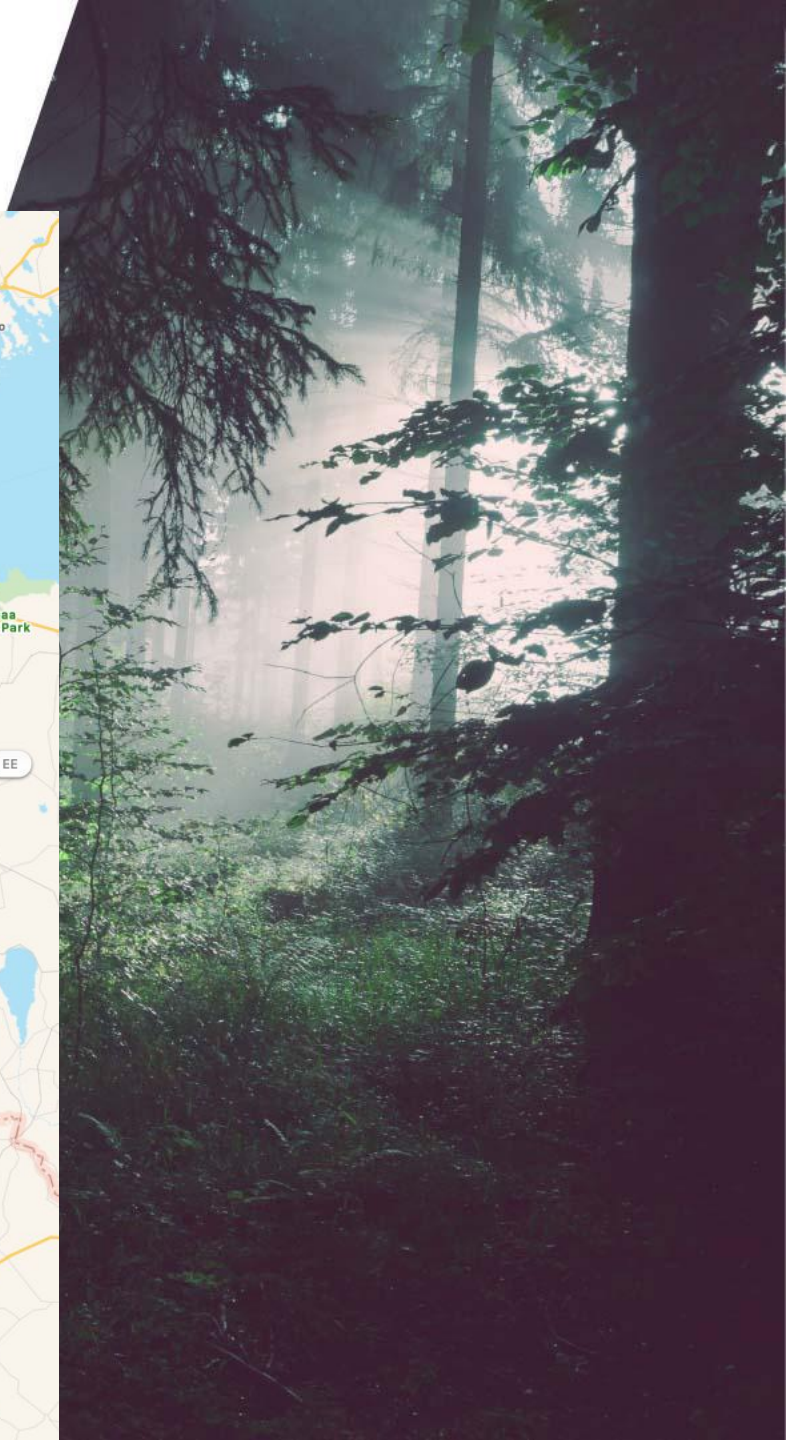
- Lielie internet operatori
  - Klientu / datu centru / publisko pakalpojumu Latvijā pret korporatīvo / mng tīklu
- IT kompānijas (ar mērķi tikt līdz klientiem)
- Glābšanas dienestu infrastruktūra
- Mediji
- Veselības aprūpes iestādes
- Valsts nozīmes datu centri
- DNS infrastruktūra
- Maršrutēšana (BGP hijack)



Mērķi Latvijā

Jādomā par darbības nepārtrauktību arī gadījumos, kad nedarbojās internet - pakalpojumi jānodrošina iekšzemē

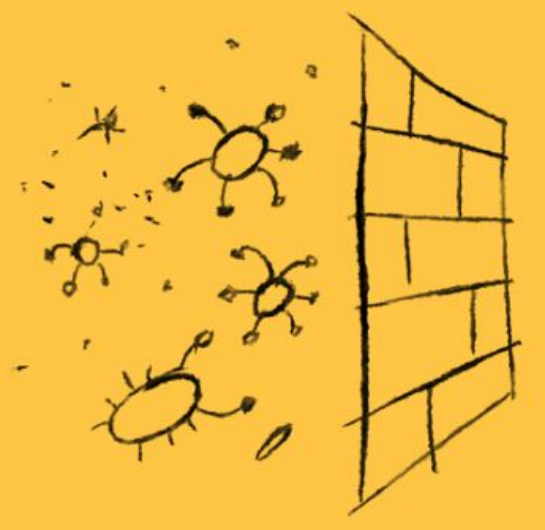




CERT.LV

DNS ugunsmūris

JUMS IR AKTĪVS



Kas tas ir?!

CERT.LV sadarbībā ar NIC (.LV domēna vārdu reģistra uzturētāju) ir izveidojuši DNS ugunsmūri - bezmaksas rīku individuālu lietotāju un organizāciju pasargāšanai no kiberapdraudējumiem, tādiem kā viltus banku lapas, krāpnieciskas tirdzniecības platformas, vīrusus izplatošas vietnes u.c.

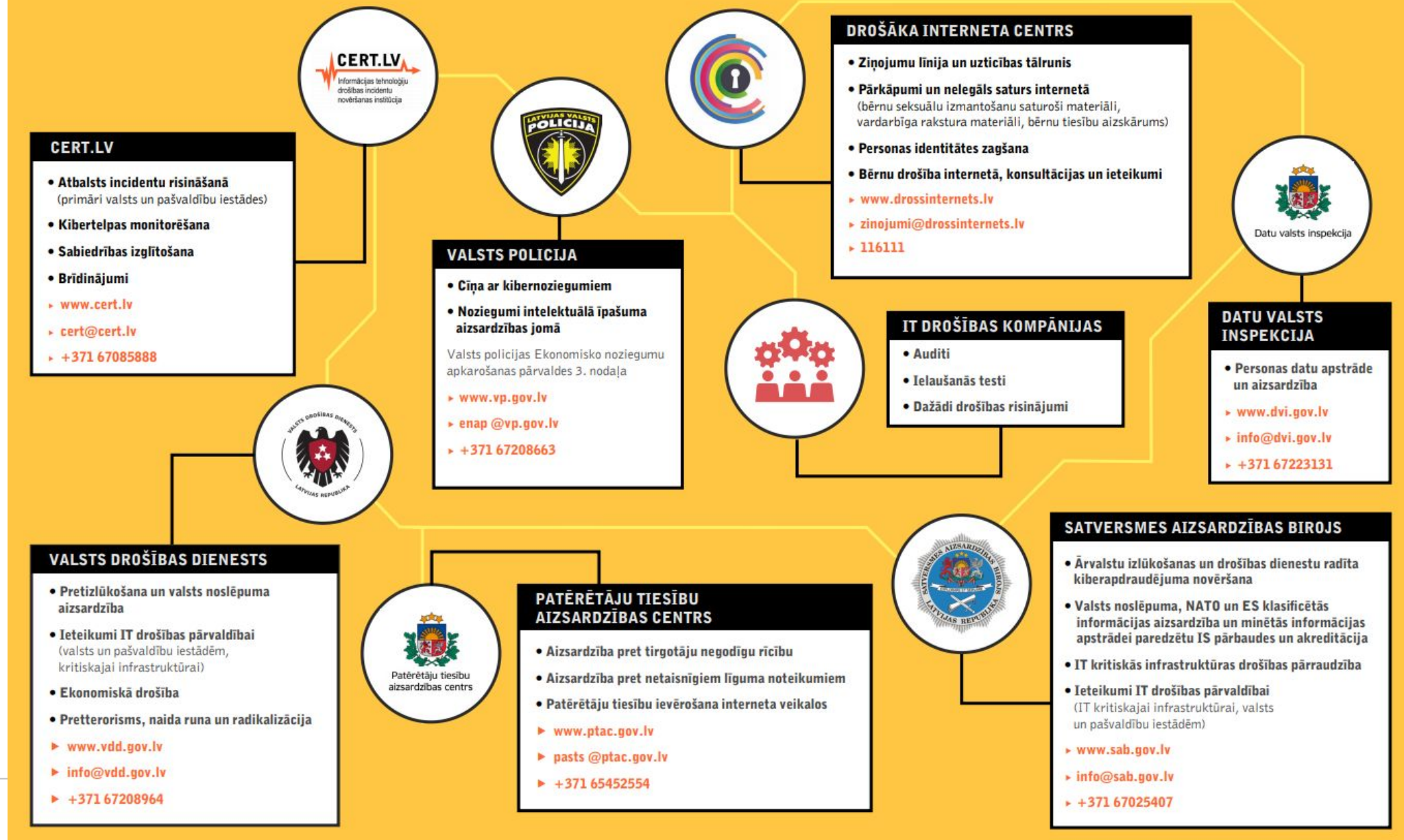
Latvijā regulāri notiek kampaņveidīgas krāpnieciskās aktivitātes – gan viltus vietnes bankas kontu, e-pasta vai sociālo tīklu piekļuves datu izkrāpšanai, gan vīrusu izplatīšanai kibertelpā. CERT.LV novēro šādas kampaņas un operatīvi ievieto šo kampaņu indikatorus ugunsmūrī, lai tā lietotājus pasargātu no identificētajiem apdraudējumiem.

Sistēma nodrošina aktīvu aizsardzību, kā piemēram, ļaunatūras lejupielādes bloķēšana, tādējādi novēršot lietotāju piekļūšanu bīstamajiem resursiem un pārvirzot tos uz brīdinājuma vietni (*landingpage*). Arī gadījumos, kad ļaunatūra jau ir inficējusi kādu iekārtu, DNS ugunsmūris sniedz iespēju ātrāk identificēt šādas iekārtas, kas sistēmu administratoriem dod iespēju operatīvi veikt seku novēršanu.

CERT.LV

ATBILDĪGĀS ORGANIZĀCIJAS LATVIJAS KIBERTELPĀ

Atbildības sfēras un kontakti: kur vērsties, ja saskaraties ar problēmu kibertelpā?



Kā pasargāties

DNS ugunsmūris - 2021. gadā gandrīz 60 000 nepieļautu incidentu
https://dnsmuris.lv/

CERT.LV Agrās brīdināšanas sistēma - sensors

CERT.LV draudu medības (pēc pamatota pieprasījuma)

Ielaušanās testi, ievainojamību un ārējā perimetra seknēšana

Kiber-higiēnas apmācības personālam

Kā pasargāties

Daudzfaktoru autentifikācija visur, kur tas iespējams NEKAVĒJOTIES!

Samaziniet savas infrastruktūras eksponētos servisus

Atjaunināt ierīces / programmatūru

Kā pasargāties

Lielāko daļu no pasākumiem jau paredz ministru kabineta noteikumu Nr.442 ievērošana!

Ikviens no mums var aizsargāt Latviju, darot savu darbu godprātīgi!

Paldies!

cert@cert.lv

certlv

certlv