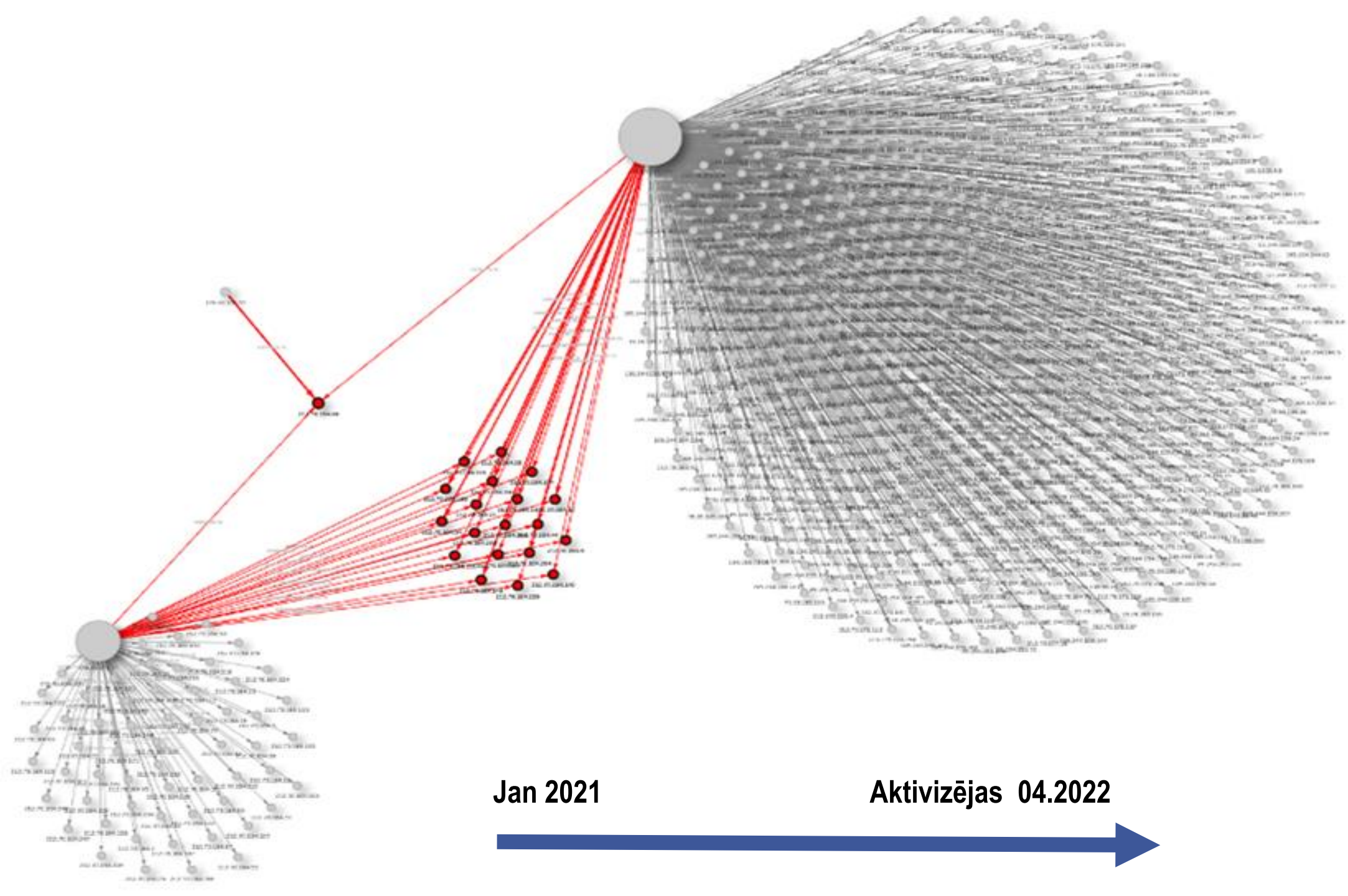
Tipiskākās kļūdas, kas noved līdz kiberincidentam

Gints Mālkalnietis

15.12.2022

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Kas notiek Latvijā?



Jan 2021

Aktivizējas 04.2022

Продолжаем наше путешествие по Латвии🇱🇻 и кладем систему авторизации для пользователей на сайте еще одной местной МФО, которая занимается выдачей кредитов населению - Banknote lv:

https://check-host.net/check-report/ba89e20k36b

👍 474 🔥 104 👏 31 ❤️ 12

🎉 6

4,9K edited 14:17

March 23

KillNet - КИБЕР АРМИЯ Z !

Не удается получить доступ к сайту

Сайт **mvd.riga.lv** неожиданно разорвал соединение.

Попробуйте сделать следующее:
Проверьте подключение к Интернету.

☝️НАШ ПРОТЕСТ В ПОДДЕРЖКУ КИРИЛЛА ФЕДОРОВА

👆"Всю ответственность за атаку берёт на себя KILLNET"

Атака на МВД ЛАТВИИ
❌https://mvd.riga.lv/
⚡https://check-host.net/check-report/81ec53bkb3e

По поводу взломов страниц писать нам
@fade_one1
@fewxxxx

6.2K edited 17:01

"Pasažieru vilciens"
@PVilciens

❌Ārēju faktoru ietekmes sadarbības partneriem dēļ nav iespējams iegādāties vilciena e-biļetes "Pasažieru vilciena" tīmekļvietnē un mobilajā lietotnē. Situācija tiek risināta.
✔️Vilciena biļeti var iegādāties kasē vai vilcienā pie konduktora kontroliera bez papildu maksas.

Translate Tweet

9:15 AM · Aug 5, 2022

🚌Благодаря нашей ддос-атаке сегодня также не работает портал покупки билетов на автобусы Литвы:

❌https://check-host.net/check-report/de342b8k82

🐻Подписывайтесь на канал NoName057(16)
🐻Вступайте в наш ддос-проект

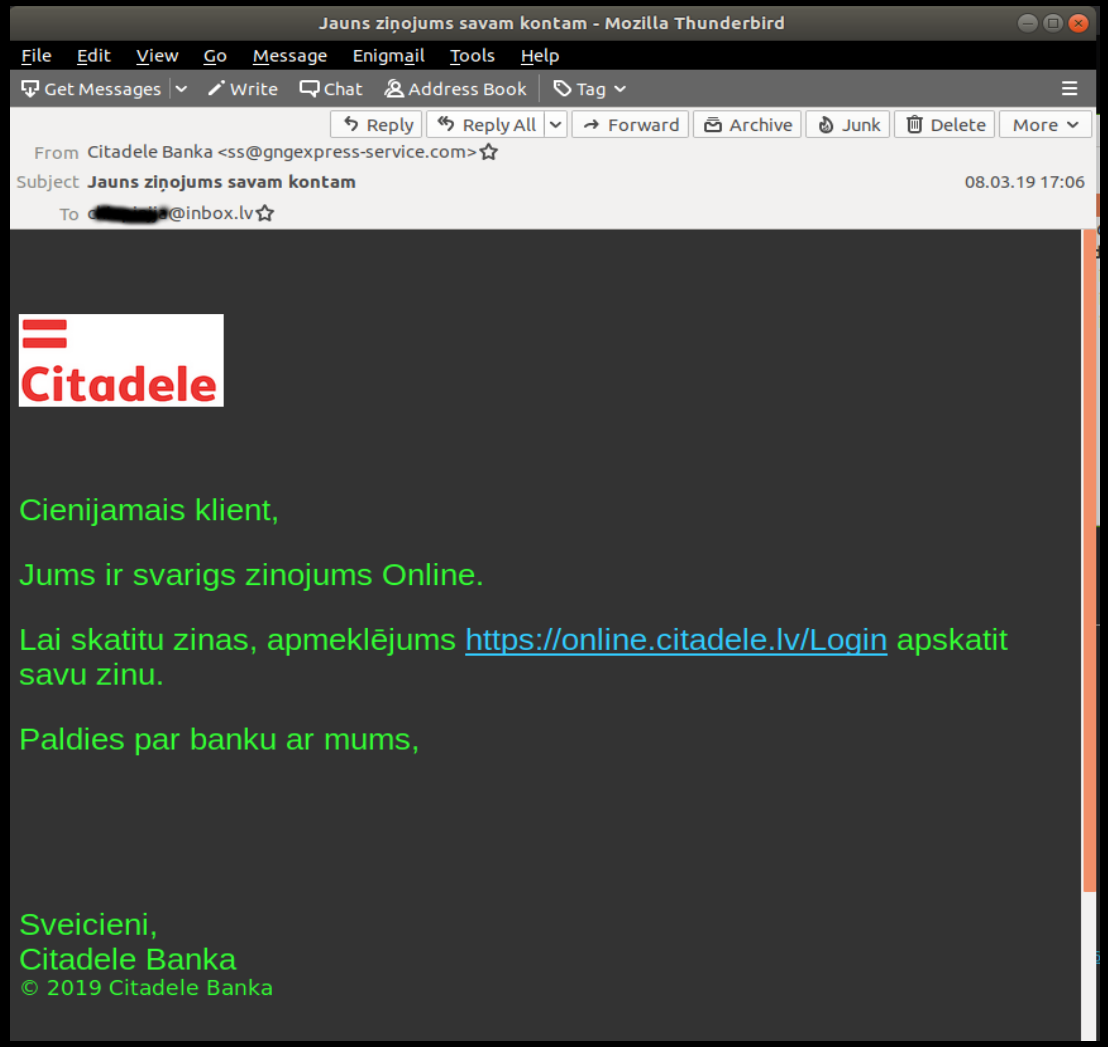
DDOS dalībnieki

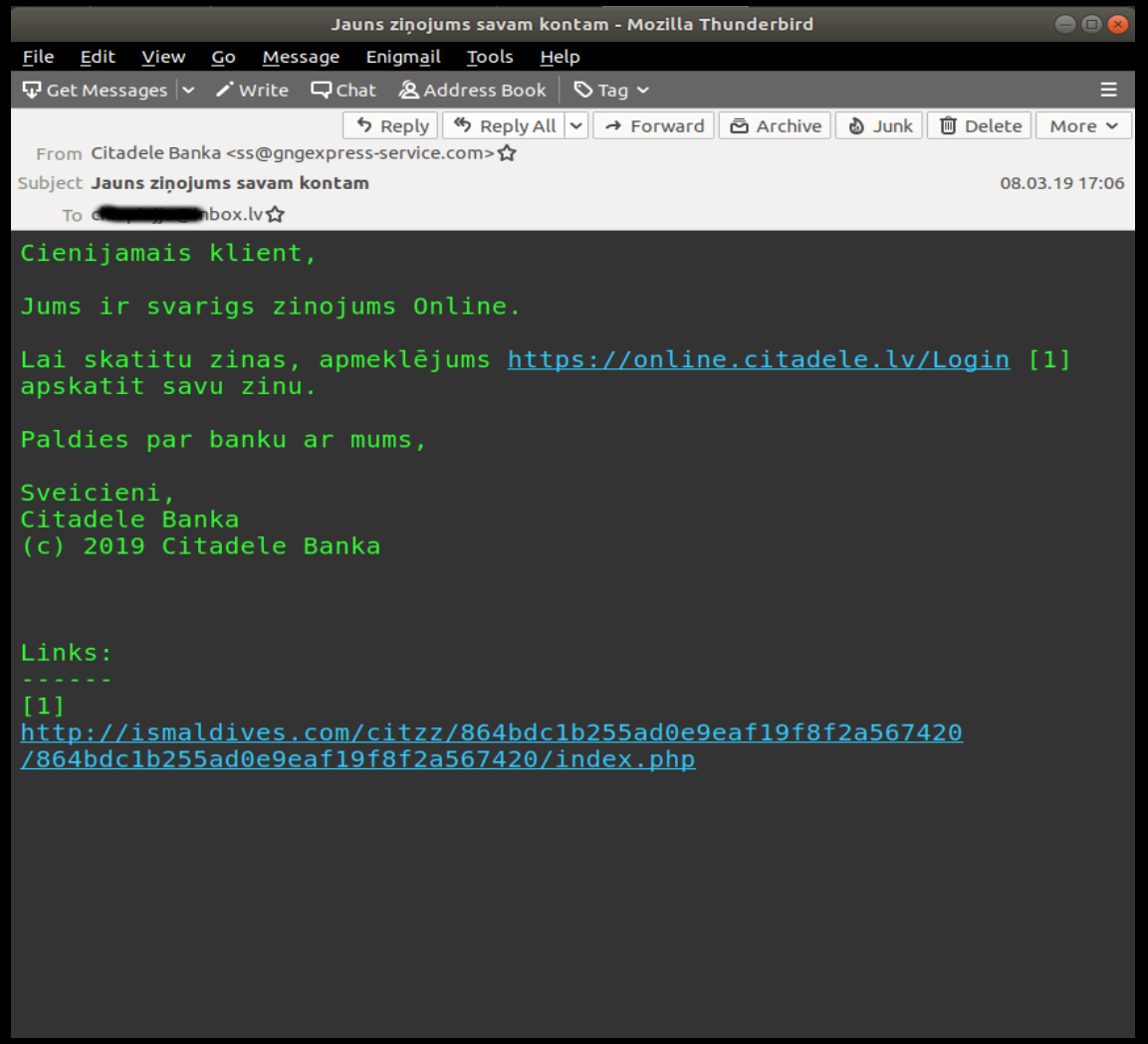
- UDP flood no atvērtiem DNS, chargen, NTP utt. servisiem. Avoti no visas pasaules, ieskaitot Latviju
- Layer 7 uzbrukumi – tiek veikti pa tiešo no datoriem un mobilajām iekārtām, daļa caur VPN, Socks Proxy
- No Latvijas aktīvi VPN serveri, kompromitēti maršrutētāji ar Socks Proxy
- Efektīvākie uzbrukumi veikti no komerciāli pieejamiem DDOS botnetiem
- Izsludināta atlīdzība aktīvākajiem DDOS veicējiem

DDOS aizsardzība

- Efektīvi darbojas IPS piedāvātie DDOS filtrācijas mehānismi, pakalpojumi ko piedāvā LVRTC, TET un citi.
- Tīmekļa vietnes var aizsargāt izmantojot Cloudflare un citus pakalpojumus, vajadzīga precīza to konfigurācija
- Iespējams lokāli bloķēt piekļuvi no zināmajiem Socks proxy, piemēram http://api.proxyscrape.com/?request=displayproxies&proxytype=socks5&timeout=10000&country=all
- Var nākties ierobežot resursa pieejamību no IP ārpus Latvijas, jāizvērtē šāda ierobežojuma ietekme uz pakalpojumu
- Ja uzbrucēji zina reālās jūsu serveru IP, var nākties tos pārcelt pie cita IPS

.lnk failu izmantošana vīrusu izpildei





http://ismaldives.com/citzz/864bdc1b255ad0e9eaf19f8f2a567

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/Logir
savu zinu.

Paldies par banku ar mums,

Sveicieni,
Citadele Banka
© 2019 Citadele Banka

[redacted]p://ismaldives.com/citzz/864bdc1b255ad0e9eaf19f8f2a567420/864bdc1b255ad0e9eaf19f8...

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.

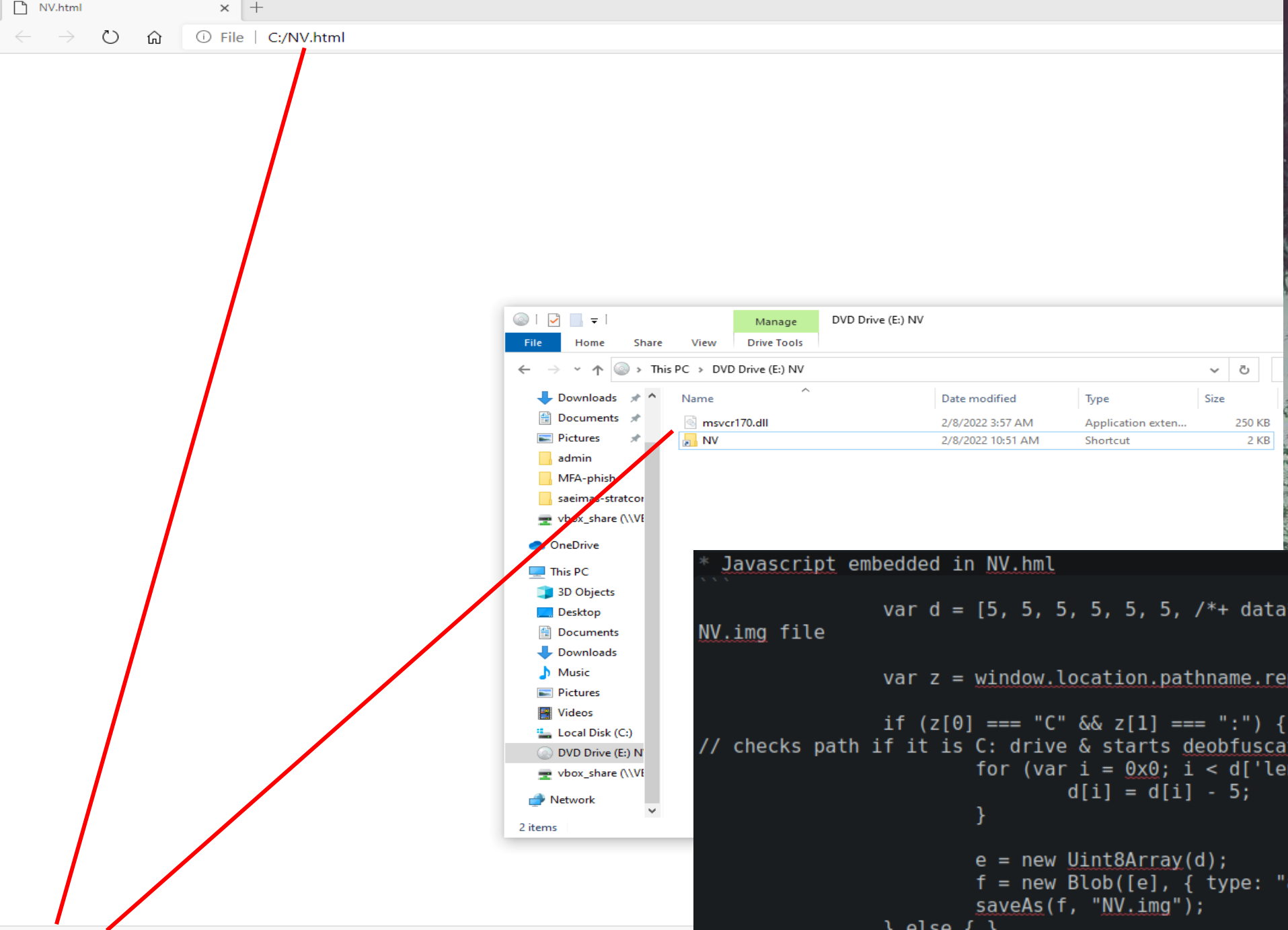
Lai skatitu zinas, apmeklējums https://online.citadele.lv/Login [1]
apskatit savu zinu.

Paldies par banku ar mums,

Sveicieni,
Citadele Banka

Links:
------
[1]
http://ismaldives.com/citzz/864bdc1b255ad0e9eaf19f8f2a567420
/864bdc1b255ad0e9eaf19f8f2a567420/index.php

http://ismaldives.com/citzz/864bdc1b255ad0e9eaf19f8f2a567



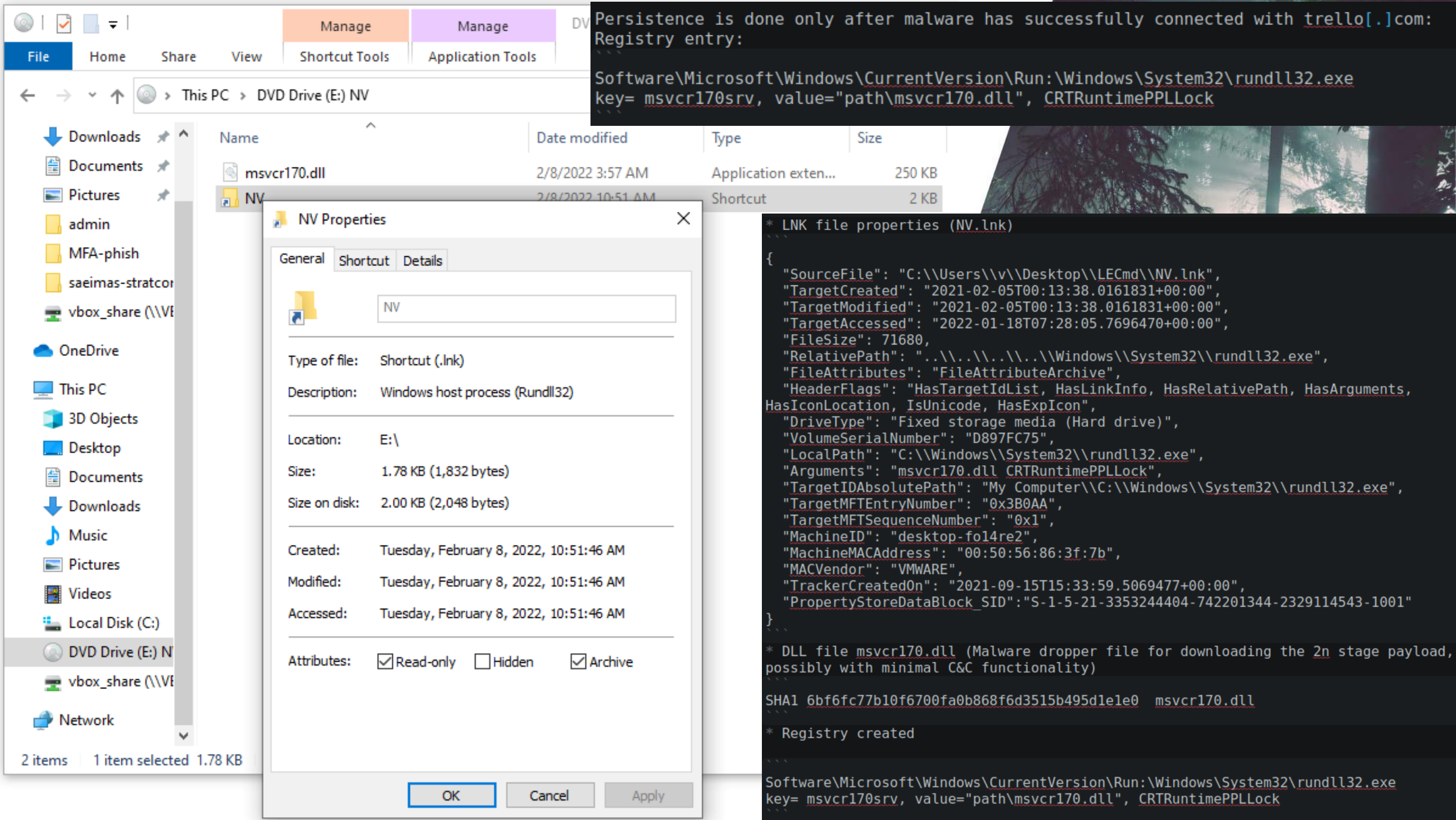
* Javascript embedded in NV.hml

```
                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 { }
```



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

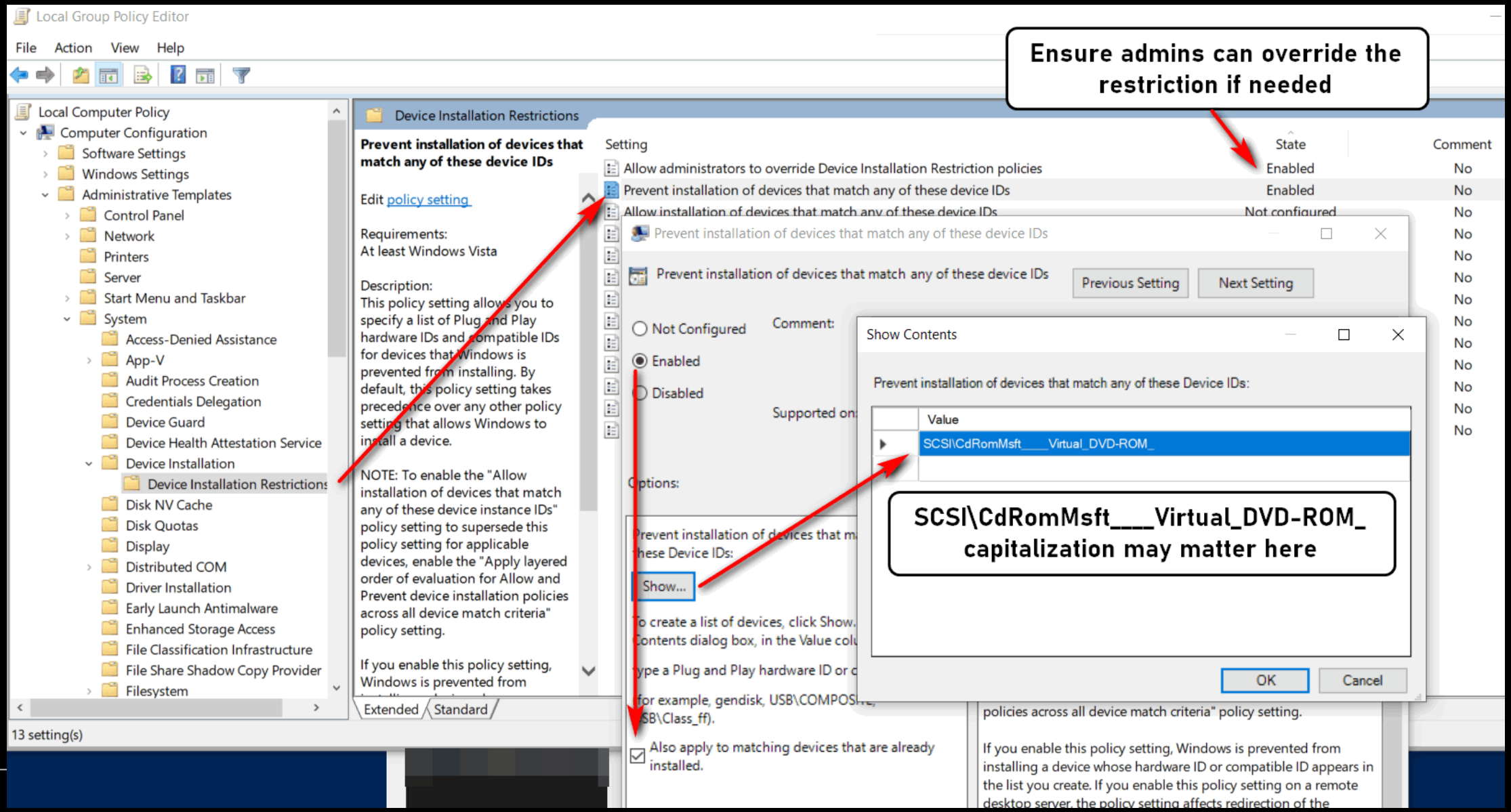
```
Software\Microsoft\Windows\CurrentVersion\Run:\Windows\System32\rundll32.exe
key= msvcr170srv, value="path\msvcr170.dll", CRTRuntimePPLLock
```

.lnk failu izmantošana vīrusu izpildei

- **.lnk faili ir būtiska Windows OS sastāvdaļa**
- **Tiek plaši izmantoti īsceļu veidošanā starp failiem**
- **.lnk failu izmantošana datorvīrusu izpildē nav jauna, bet šobrīd ir īpaši izplatīta**
- **Atslēdziet .iso, .img utt. formātu failu automātiskas pievienošanas iespējas:**

  Group Policy / Administrative Templates / System / Device Installation / Device Installation Restrictions / Prevent installation of devices that match any of these device IDs / **Enable** set: SCSI\CdRomMsft___*Virtual_DVD-ROM*

.lnk failu izmantošana vīrusu izpildei



.lnk failu izmantošana vīrusu izpildei

- **Izmantojiet AppLocker lai ierobežotu programmu izpildes iespējas no %/temp/ mapēm.**
- **Atslēdziet programmu izpildes iespējas no USB datu nesējiem**
- **Apmāciet lietotājus, par .lnk failu funkcionalitāti**

Ievainojamību meklēšana

- Ievainojamības tiek meklētas nepārtraukti
- Salīdzinot ar periodu pirms 01.2022, ievainojamību meklēšanas intensitāte valsts un pašvaldību resursos pieaugusi 7X
- Sekmīgi uzbrukumi realizēti pret mērķiem, kas nav ievērojuši labās prakses principus IKT infrastruktūras uzturēšanā
- Vairāki upuri eksponējuši internetā resursus kuriem jau sen (8-12 mēneši) bijušas zināmas ievainojamības, arī to programmatūras ražotāji brīdinājuši par uzbrukumiem
- Iekārtas pieejamas publiskā internet tīklā bez praktiskas nepieciešamības

Deadbolt izspiedējvīruss

- **Latvijā pirmie, mums zināmie, upuri 01.2022**
- **Izmanto ievainojamības QNAP tīkla datu glabātavā CVE-2021-44056,** CVE-2021-44057
- **Ievainojamā iekārta tiek izmantota citu upuru meklēšanā**
- **Šī vīrusa izplatītāji specializējas arī uz citu ražotāju tīkla datu glabātavu uzlaušanu**
- **Dati tiek bojāti uzbrukumos brīvdienu naktīs**
- **Nemaksājot datus atšifrēt nav iespējams**

Šifrējošie izspiedējvīrusi = zuduši dati

Neeksistējošas rezerves kopijas!

- **Aktuālajiem datiem kopijas tiek veidotas pārāk reti**
- **Kopijas tiek glabātas kopā ar pašiem datiem – nav atbilstošas rezerves kopiju glabāšanas infrastruktūras**
- **Nepietiekams kopēto datu apjoms, lai ātri un bez zaudējumiem atjaunotu darbu**
- **Netiek veiktas regulāras pārbaudes, lai apliecinātu kopēto datu darbaspēju**

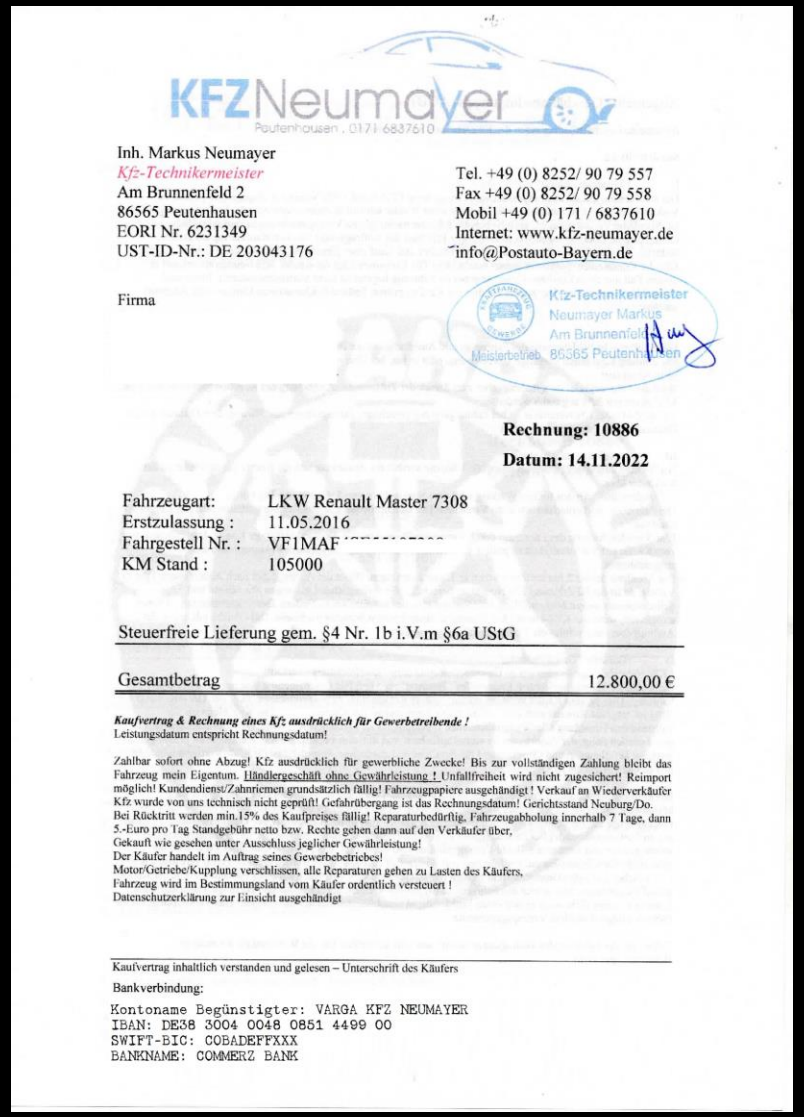
Šifrējošie izspiedējvīrusi

- **Vairums uzbrukumu veikti izmantojot RDP piekļuvi**
- **Praktiski visi veiksmīgie uzbrukumi veikti brīvdienu naktīs**
- **Uzbrucēji šifrējuši visus tīklā pieejamos datorus**
- **Izmantoti rīki kā Mimikatz un citi, lai atrastu datoros administratoru paroles vai kerberos tickets.**
- **Visbiežāk, upura lietotāja kontam bijušas vismaz lokālā administratora tiesības, atļauts atslēgt AV un mainīt ugunsmūra konfigurāciju**

Identitāes problēma

lvdpd.shop
lvdpdsafe.xyz ...

Viltoti rēķini



KFZ Neumayer
Peutenhausen , 0171 6837610

Inh. Markus Neumayer
Kfz-Technikermeister
Am Brunnenfeld 2
86565 Peutenhausen
EORI Nr. 6231349
UST-ID-Nr.: DE 203043176

Tel. +49 (0) 8252/ 90 79 557
Fax +49 (0) 8252/ 90 79 558
Mobil +49 (0) 171 / 6837610
Internet: www.kfz-neumayer.de
info@Postauto-Bayern.de

Firma

Kfz-Technikermeister
Neumayer Markus
Am Brunnenfeld
Meisterbetrieb 86565 Peutenhausen

Rechnung: 10886
Datum: 14.11.2022

Fahrzeugart:	LKW Renault Master 7308
Erstzulassung :	11.05.2016
Fahrgestell Nr. :	VF1MAF
KM Stand :	105000

Steuerfreie Lieferung gem. §4 Nr. 1b i.V.m §6a UStG

Gesamtbetrag 12.800,00 €

Kaufvertrag & Rechnung eines Kfz ausdrücklich für Gewerbetreibende !
Leistungsdatum entspricht Rechnungsdatum!

Zahlbar sofort ohne Abzug! Kfz ausdrücklich für gewerbliche Zwecke! Bis zur vollständigen Zahlung bleibt das Fahrzeug mein Eigentum. Händlergeschäft ohne Gewährleistung ! Unfallfreiheit wird nicht zugesichert! Reimport möglich! Kundendienst/Zahnriemen grundsätzlich fällig! Fahrzeugpapiere ausgehändigt ! Verkauf an Wiederverkäufer Kfz wurde von uns technisch nicht geprüft! Gefahrübergang ist das Rechnungsdatum! Gerichtsstand Neuburg/Do. Bei Rücktritt werden min.15% des Kaufpreises fällig! Reparaturbedürftig, Fahrzeugabholung innerhalb 7 Tage, dann 5.-Euro pro Tag Standgebühr netto bzw. Rechte gehen dann auf den Verkäufer über,
Gekauft wie gesehen unter Ausschluss jeglicher Gewährleistung!
Der Käufer handelt im Auftrag seines Gewerbebetriebes!
Motor/Getriebe/Kupplung verschlissen, alle Reparaturen gehen zu Lasten des Käufers,
Fahrzeug wird im Bestimmungsland vom Käufer ordentlich versteuert !
Datenschutzerklärung zur Einsicht ausgehändigt

Kaufvertrag inhaltlich verstanden und gelesen – Unterschrift des Käufers

Bankverbindung:

Kontoname Begünstigter: VARGA KFZ NEUMAYER
IBAN: DE38 3004 0048 0851 4499 00
SWIFT-BIC: COBADEFFXXX
BANKNAME: COMMERZ BANK

Zaudējumi

Latvijā ir gan veiksmīgi izkrāptas ar 6 cipariem rakstāmas summas, gan savlaicīgi apturētas tik pat lielas transakcijas
Dominē gadījumi no 10 – 150 tūkstoši EUR
Garākais CERT.LV zināmais reakcijas laiks – 11 mēneši

- ✓ Jo ātrāk izdodas atklāt krāpšanu – jo labākas iespējas atgūt naudu
- ✓ Krāpniekiem ir vienalga, kura darījumu partnera e-pastā ielauzties
- ✓ Cilvēcīgais faktors – vēl arvien labākais veids, kā atklāt krāpšanu ir apmācīti un gana aizdomīgi darbinieki!

Piegādes ķēdes aizsardzība

- Daudzas datorsistēmas ir savstarpēji saistītas vairāk nekā šķiet
- Programmatūras ražotāji izmanto savā kodā citu izstrādātāju bibliotēkas un rīkus
- Ārpakalpojumu sniedzēji savus resursus var izvietot vēl pie neskaitāmiem citiem partneriem
- Sarežģīti izsekot apjomīgu produktu atjauninašanai un to komponentu drošībai
- Liela atkarība no Google, Facebook, Amazon, Microsoft utt.
- Uzbrukumi atsevišķu komponentu izstrādātājiem pakļauj riskam simtiem citu produktu.

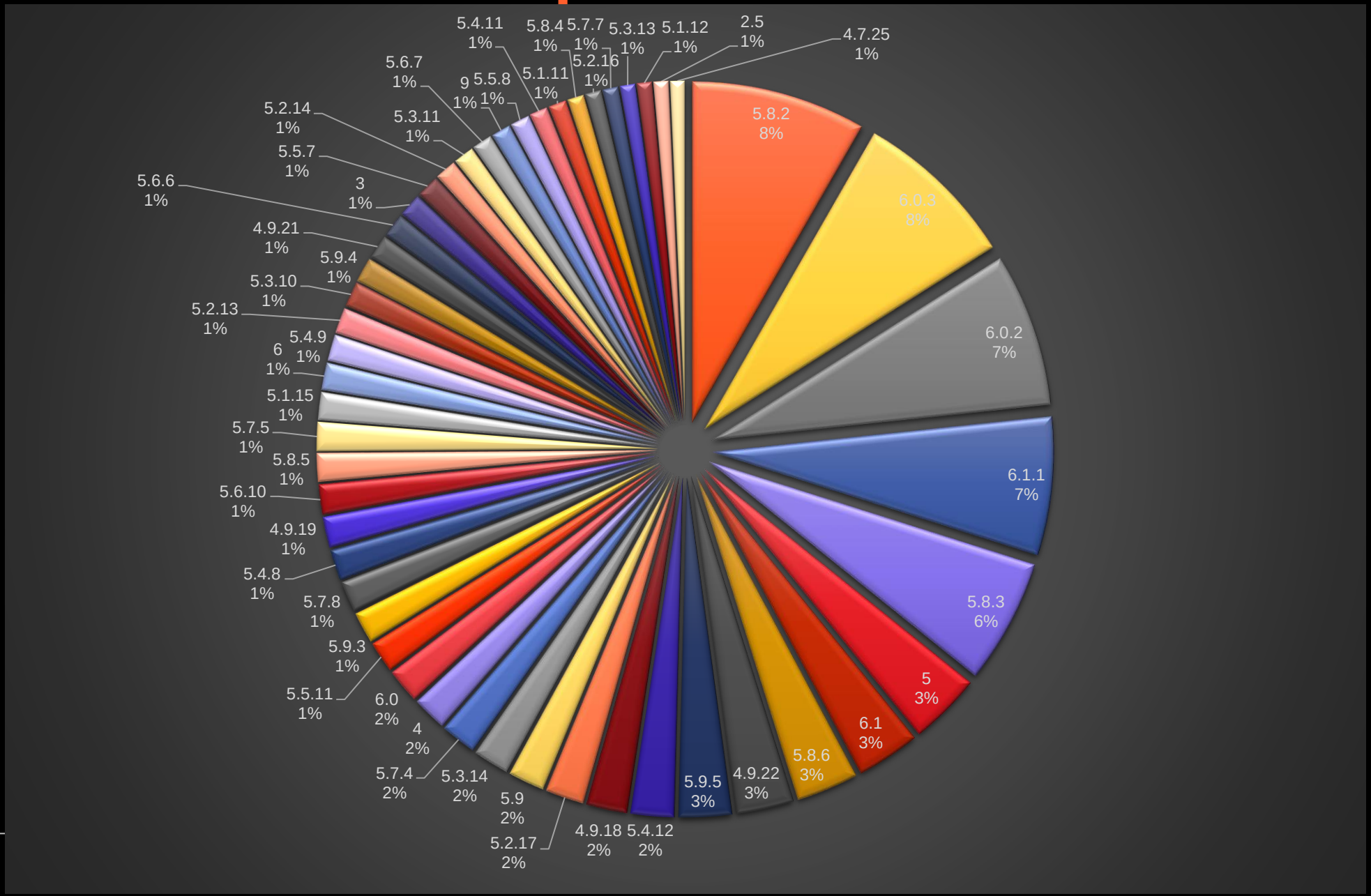
Programmatūras piegādātāja aizsardzība

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

Weblapu novecošana

- Tāpat kā programmatūra, weblapas un to CMS noveco
- Nav skaidrības kas ilgterminā atbild par uzturēšanu
- Izveidotie e-komercijas risinājumi nodrošina nelielu biznesa daļu
- Nav vēlme uzturēt sarežģītas sistēmas

Weblapu novecošana



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

RDP un citi attālinātā darba rīki

Uzņēmumi nepietiekami kontrolē attālināto piekļuvi saviem datiem

- RDP piekļuve sensitīvajiem datiem– grāmatvedībai un noliktavām
- Bez vajadzības uzstādīti TeamViewer utt. rīki
- Netiek izmantota NEKĀDA attālināta pieslēguma aizsardzība (VPN utt.)
- Netiek veikta piekļuves mēģinājumu auditēšana un kontrole
- Parole nav pietiekami droša
- Piekļuve tīklā nodrošina pārāk lielas tiesības tajā
- RDP uz nestandarta porta nepalielina drošību!

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

Paldies!

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