SECURITY DAYS

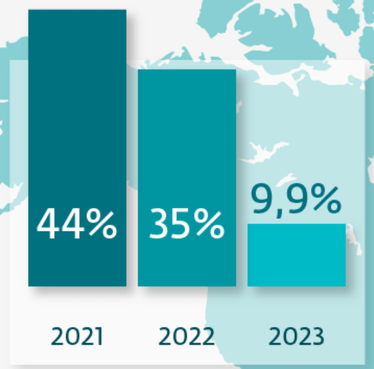
MAKE IT SMOOTH. NUO TENDENCIJŲ IKI REGLAMENTŲ

Ramūnas Liubertas - NOD Baltic vyresnysis kibernetinio saugumo inžinierius, ESET ekspertas

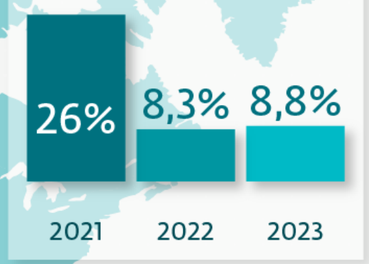
Rugsėjo 5 d. 2024
KIBERNETINIO SAUGUMO KONFERENCIJA
esd.eset.lt

TOP5 kibernetinės grėsmės Lietuvoje

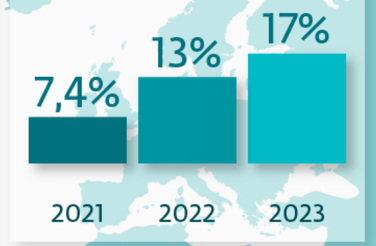
Lietuvoje plitusios kibernetinės grėsmės



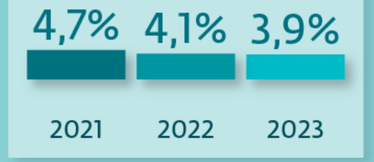
Adware
Kompiuteryje rodo nepageidaujamas reklamas, kuriose yra įrašyta kenkėjiškų programų kodų.



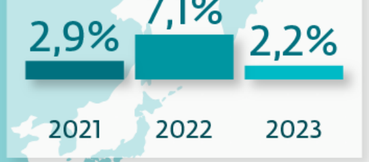
Remote connection exploits
Tinklų ir kompiuterių puolimas pasitelkiant kenkėjiškas programas per nuotolinį ryšį.



Trojan
Kenkėjiška kompiuterinė programa, skirta gauti neteisėtai prieigai prie įrenginyje esančių duomenų.



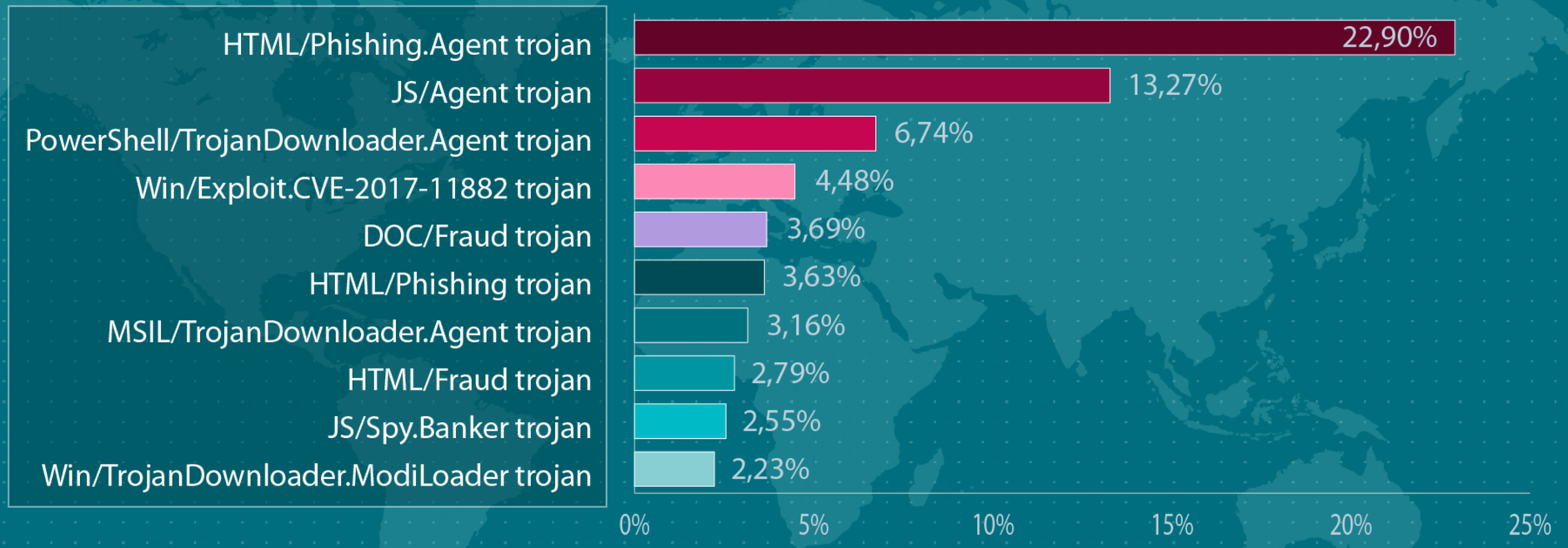
Phishing
Sukčiavimo forma, skirta išvilioti konfidencialius duomenis, kuomet pats nukentėjusysis išduoda savo asmens duomenis.



OS exploits
Išnaudoja programinės įrangos pažeidžiamumus, kad programišiams būtų suteikta prieiga per nuotolinį prisijungimą.

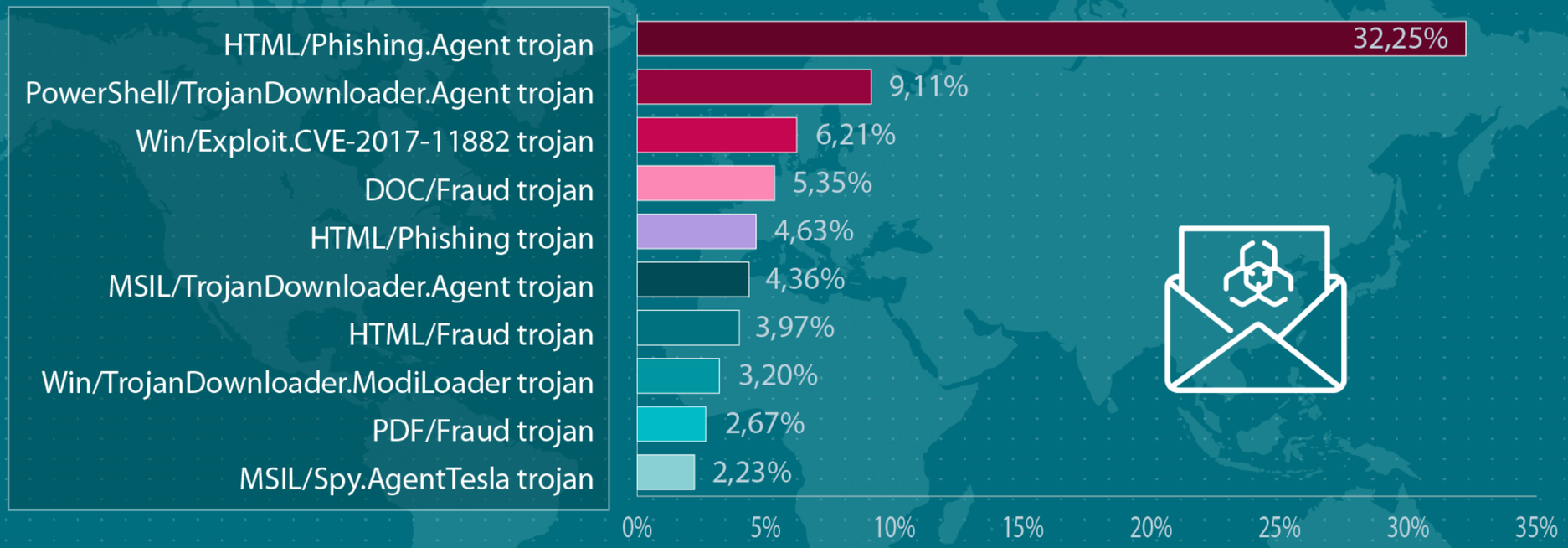
Parengta remiantis ESET telemetrijos duomenimis. Laikotarpis: 2023.01.01-2023.12.31.

Top 10 kenkėjiškų programų Lietuvoje 2024 metais



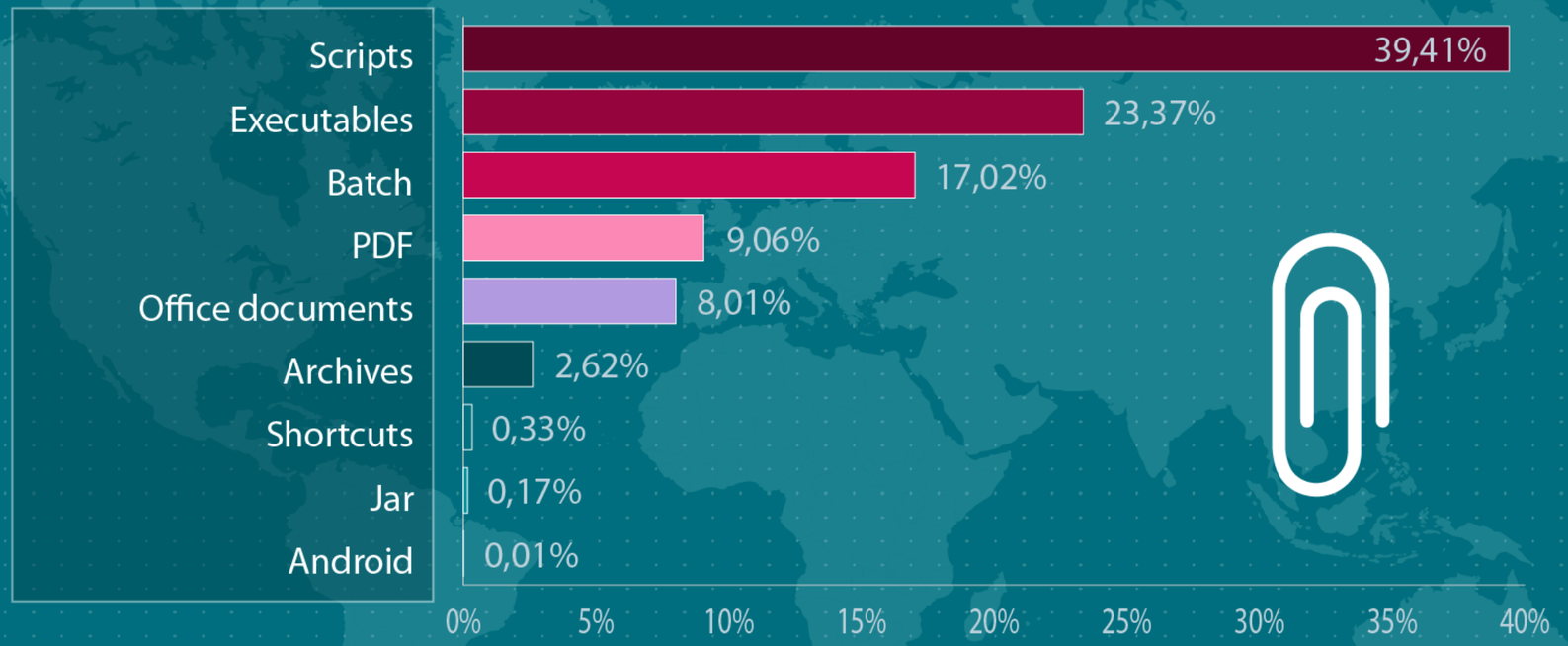
Remiantis ESET telemetrijos duomenimis, top 10 Lietuvoje 2024 metais paplitusių kenkėjiškų programų.

Top 10 grėsmių, plintančių el. paštu Lietuvoje



Remiantis ESET telemetrijos duomenimis, Top 10 grėsmių, plintančių el. paštu Lietuvoje 2024 metais.

Populiariausi kenkėjiškų prisegtukų tipai

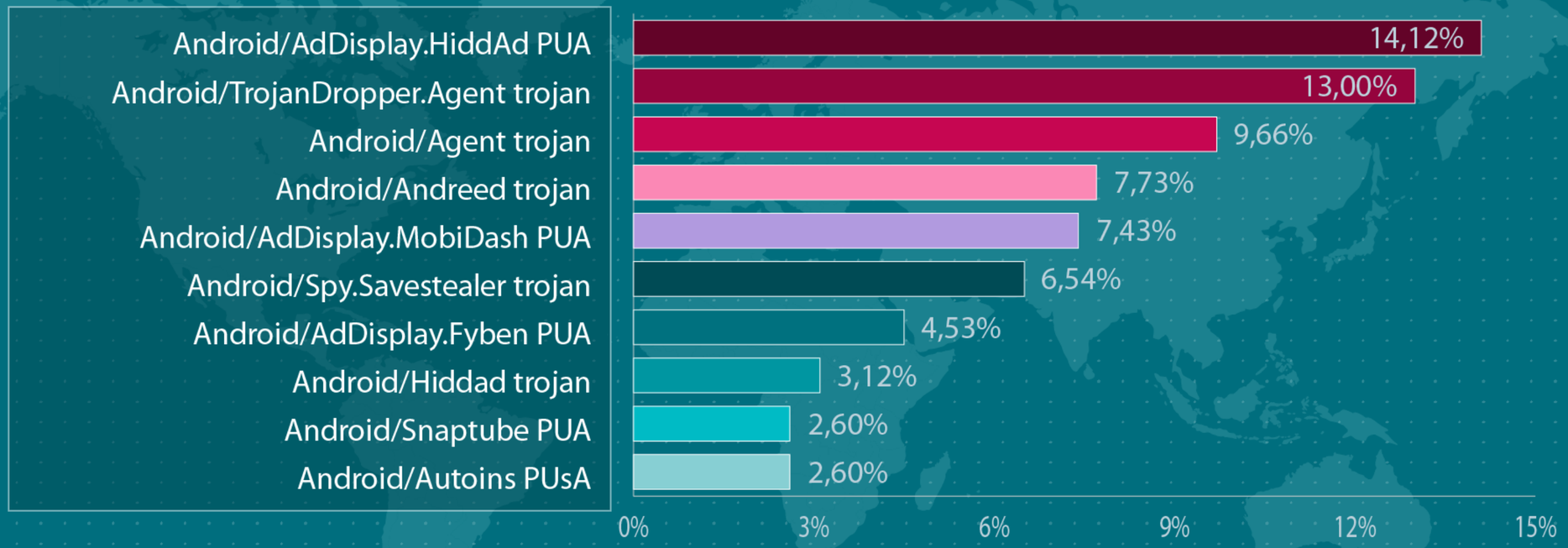


Remiantis ESET telemetrijos duomenimis, populiariausi kenkėjiškų prisegtukų tipai 2024 metais.

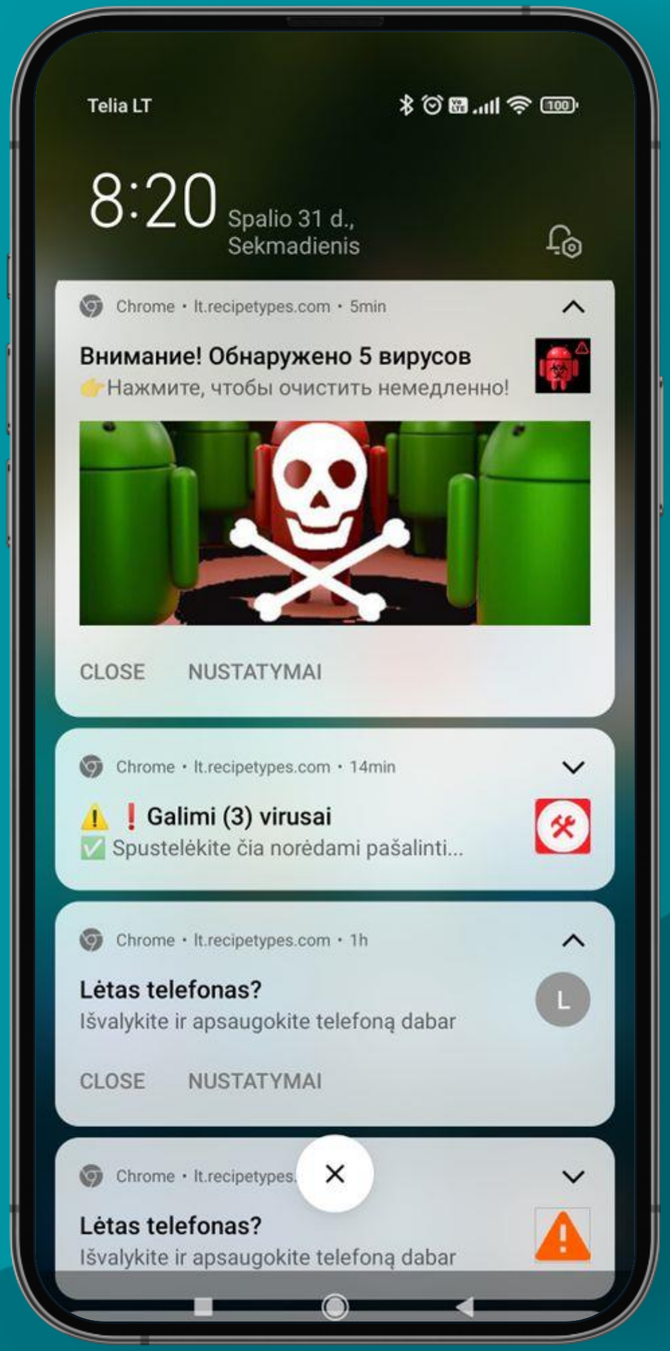
Populiariausios kenkėjiško el. laiško antraštės

- FW: sutarties dokumentas
- RE: mokejimas
- Fwd: Mokejimo patvirtinimas
- Fwd: TT payment

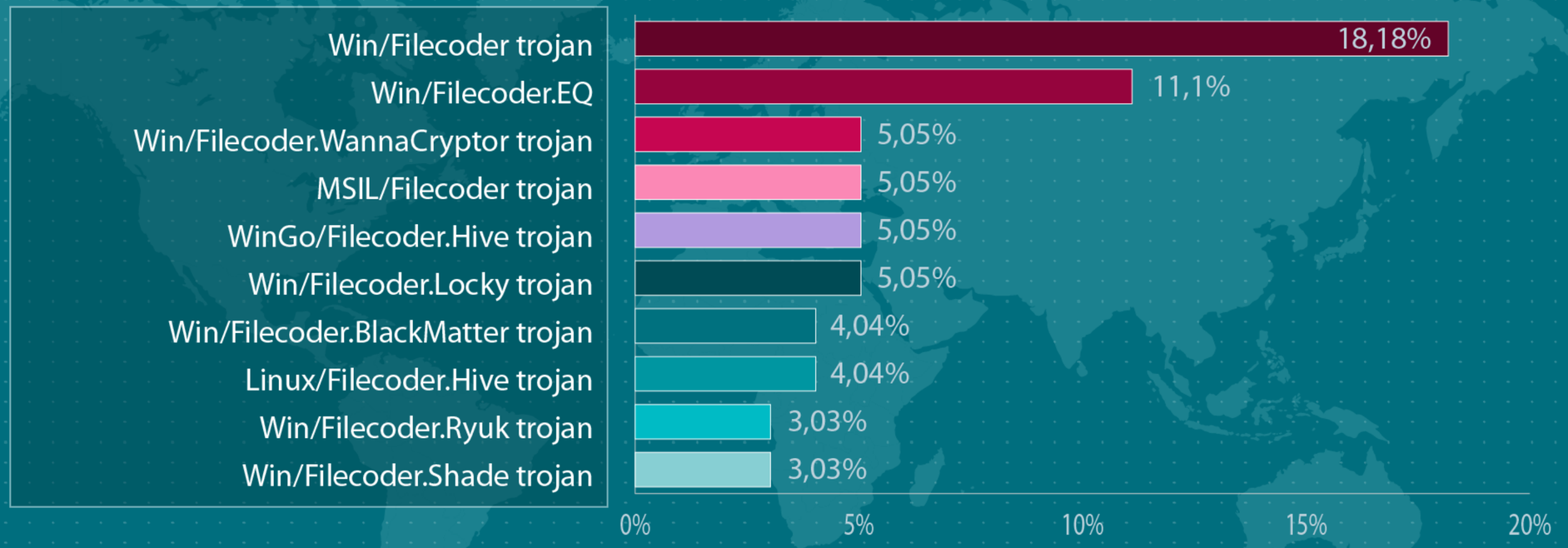
Android kenkėjiškų programų Top 10 Lietuvoje 2024 metais



Remiantis ESET telemetrijos duomenimis, top 10 Lietuvoje 2024 metais paplitusių Android kenkėjiškų programų.

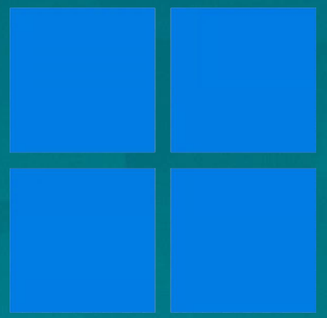


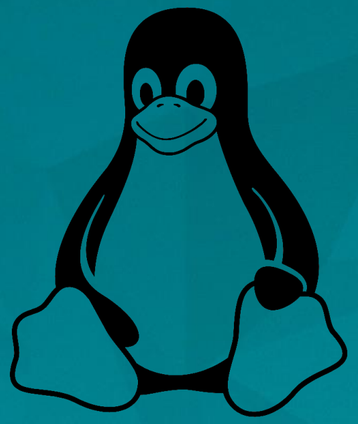
Top 10 #ransomware virusų Lietuvoje 2024 metais



Remiantis ESET telemetrijos duomenimis, top 10 Lietuvoje 2024 metais paplitusių išpirkos reikalaujančių kenkėjiškų programų programų.

Šifravimo virusai pagal operacinę sistemą





90%

5%

5%

Kibernetinių išpuolių tipai

Kibernetinių išpuolių tipai

MASINIAI

Sukčiavimo el. laiškų ar SMS siuntimas

FINANSINIAI

Prisijungimų išgavimas, lėšų pervedimo operacijos, fiktyvi bankininkystė

SLAPTAŽODŽIŲ VAGYSTĖS

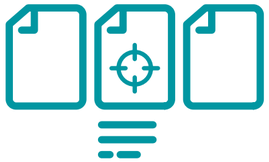
El. pašto paskyrų, prisijungimų prie sistemų

TIKSLINĖS ATAKOS

Nukreipimas į pasirinktą įmonę ar darbuotojus

Tikslinių atakų taikiniai

Interneto svetainės



Progr. įrangos pažeidžiamumai

Kompiuterinis tinklas

Atsarginės kopijos

Prieiga prie sistemų

Darbuotojai

Teisinis reglamentavimas

Teisinis reglamentavimas

DORA

Skaitmeninės veiklos atsparumo finansų sektoriuje reglamentas

(angl. Digital Operational Resilience Act)

Taikymas
2025 m. sausio 17 d.

- IRT rizikos valdymas
- Su IRT susijusių incidentų valdymas ir ataskaitų teikimas
- Skaitmeninės veiklos atsparumo testavimas
- IRT trečiųjų šalių rizikos valdymas
- Dalijimasis informacija

Teisinis reglamentavimas

TIS2 (NIS2)

Antroji ES tinklų ir
informacinių sistemų
saugumo direktyva

(angl. The second Network and Information Security Directive)

LR KSĮ įsigaliojimas
2024 m. spalio 18 d.

Požiūris į skaitmeninį saugumą

POŽIŪRIS Į SKAITMENINĮ SAUGUMĄ

1. TURTO VALDYMAS

2. TURTO APSAUGA IR INCIDENTŲ VALDYMAS

3. SLAPTAŽODŽIŲ IR PRIEGOS VALDYMAS

4. EDUKACIJA IR SAUGUMO PASLAUGOS

POŽIŪRIS Į SKAITMENINĮ SAUGUMĄ

1. TURTO VALDYMAS

- Centralizuotas valdymas
- RMM įrankiai

2. TURTO APSAUGA IR INCIDENTŲ VALDYMAS

3. SLAPTAŽODŽIŲ IR PRIEGOS VALDYMAS

4. EDUKACIJA IR SAUGUMO PASLAUGOS

POŽIŪRIS Į SKAITMENINĮ SAUGUMĄ

1. TURTO VALDYMAS

- Centralizuotas valdymas
- RMM įrankiai

2. TURTO APSAUGA IR INCIDENTŲ VALDYMAS

- Daugiasluoksnė apsauga
- XDR/SIEM/SOAR
- Pažeidžiamumų ir pataisų valdymas
- Atsarginės kopijos
- Šifravimas
- DLP

3. SLAPTAŽODŽIŲ IR PRIEGOS VALDYMAS

4. EDUKACIJA IR SAUGUMO PASLAUGOS

POŽIŪRIS Į SKAITMENINĮ SAUGUMĄ

1. TURTO VALDYMAS

- Centralizuotas valdymas
- RMM įrankiai

2. TURTO APSAUGA IR INCIDENTŲ VALDYMAS

- Daugiasluoksnė apsauga
- XDR/SIEM/SOAR
- Pažeidžiamumų ir pataisų valdymas
- Atsarginės kopijos
- Šifravimas
- DLP

3. SLAPTAŽODŽIŲ IR PRIEGOS VALDYMAS

- MFA/2FA
- PAM
- Slaptažodžių tvarkyklės

4. EDUKACIJA IR SAUGUMO PASLAUGOS

POŽIŪRIS Į SKAITMENINĮ SAUGUMĄ

1. TURTO VALDYMAS

- Centralizuotas valdymas
- RMM įrankiai

2. TURTO APSAUGA IR INCIDENTŲ VALDYMAS

- Daugiasluoksnė apsauga
- XDR/SIEM/SOAR
- Pažeidžiamumų ir pataisų valdymas
- Atsarginės kopijos
- Šifravimas
- DLP

3. SLAPTAŽODŽIŲ IR PRIEGOS VALDYMAS

- MFA/2FA
- PAM
- Slaptažodžių tvarkyklės

4. EDUKACIJA IR SAUGUMO PASLAUGOS

- DI
- Cyber mokymai
- MDR/SOC
- Pentesting
- Threat Hunting
- Threat Intelligence
- Cyber draudimas

TAKE AWAY

DORA/TIS2 direktyva

Teisinė reglamentacija – keli mėnesiai

Praktinė implementacija – nuo 1 mėn.

Digital Security
Progress. Protected.

ramunas@eset.lt

Bendraukime

www.eset.lt