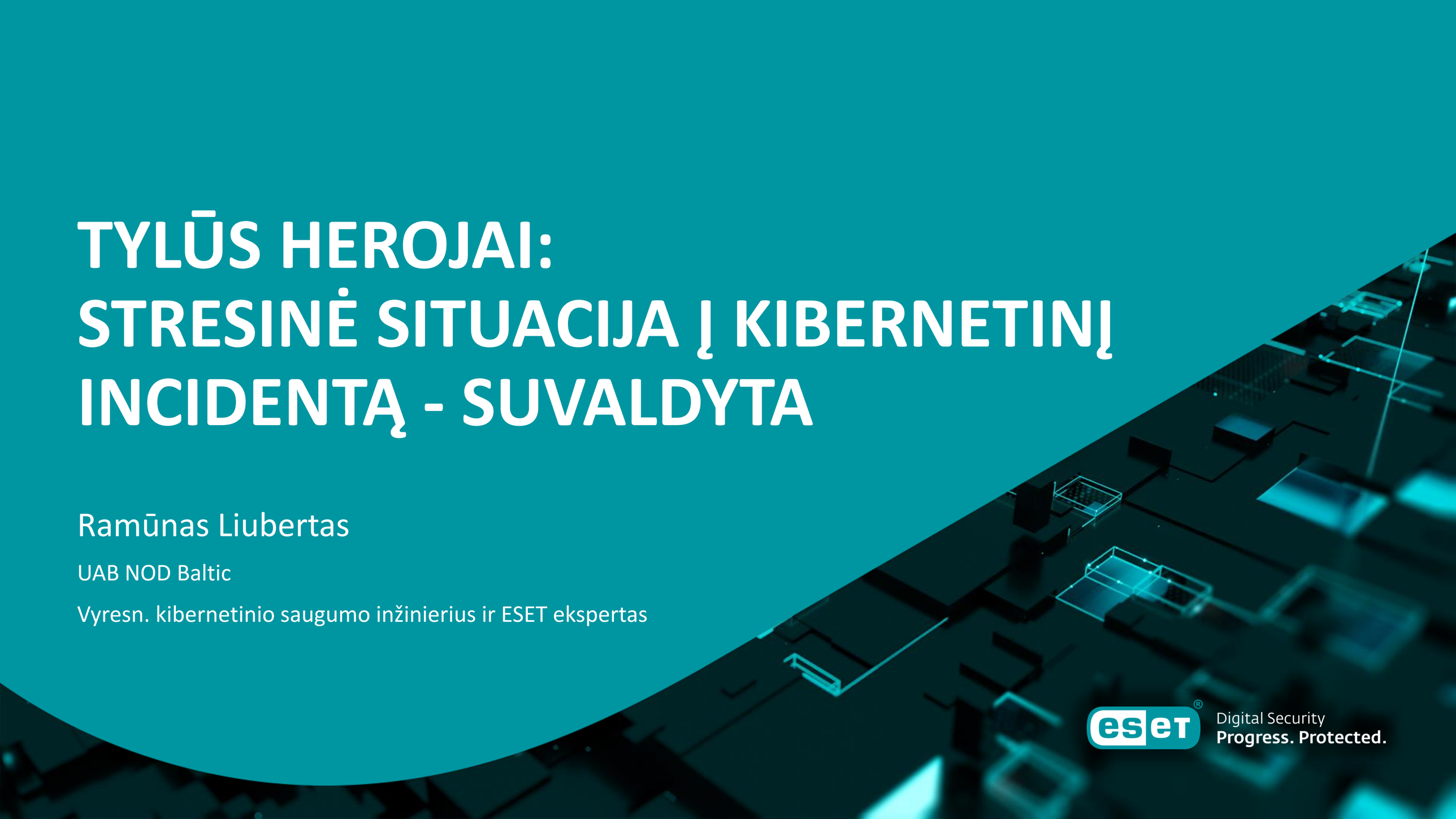
TYLŪS HEROJAI: STRESINĖ SITUACIJA Į KIBERNETINĮ INCIDENTĄ - SUVALDYTA

Ramūnas Liubertas

UAB NOD Baltic

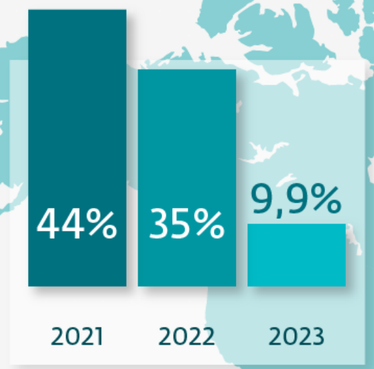
Vyresn. kibernetinio saugumo inžinierius ir ESET ekspertas



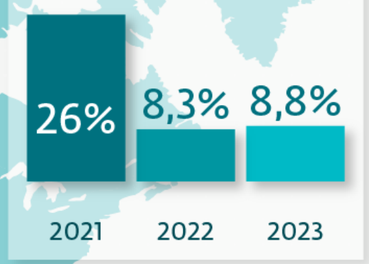
Digital Security
Progress. Protected.

TOP5 kibernetinės grėsmės Lietuvoje

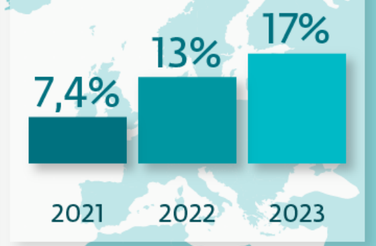
Lietuvoje plitusios kibernetinės grėsmės



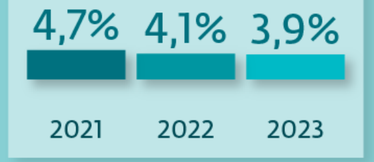
Adware
Kompiuteryje rodo nepageidaujamas reklamas, kuriose yra įrašyta kenkėjiškų programų kodų.



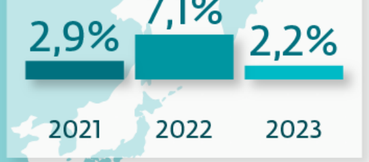
Remote connection exploits
Tinklų ir kompiuterių puolimas pasitelkiant kenkėjiškas programas per nuotolinį ryšį.



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



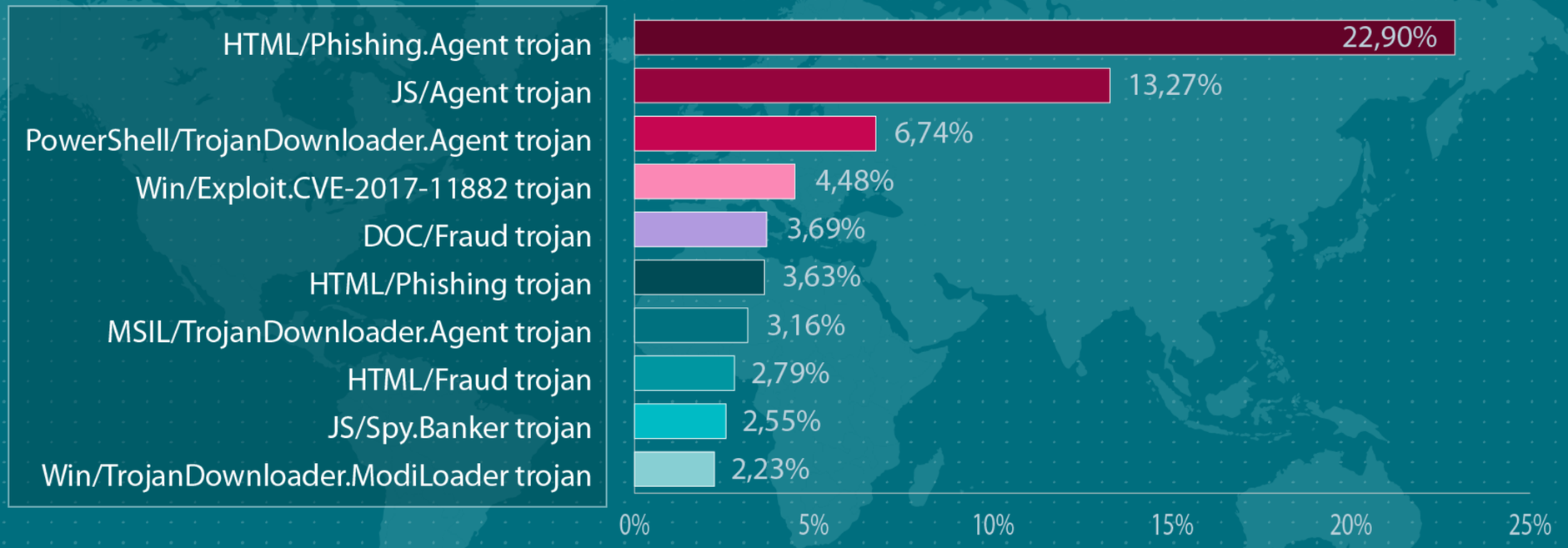
Phishing
Sukčiavimo forma, skirta išvilioti konfidencialius duomenis, kuomet pats nukentėjusysis išduoda savo asmens duomenis.



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

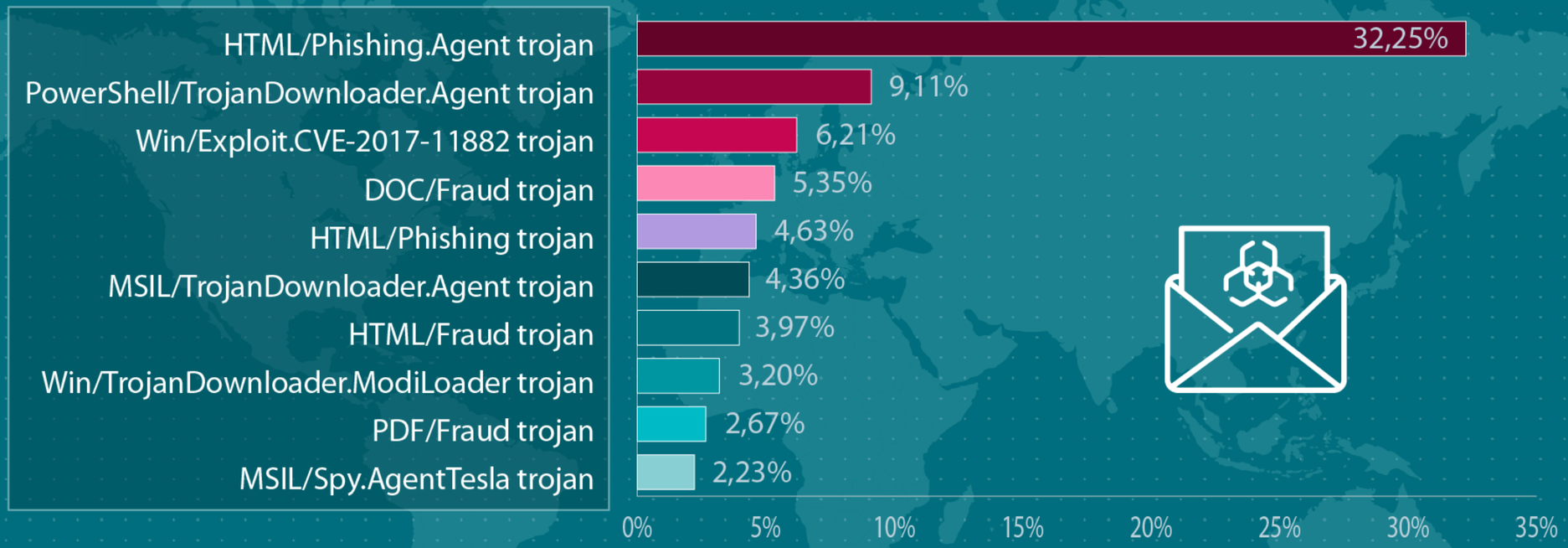
Parengta remiantis ESET telemetrijos duomenimis. Laikotarpis: 2023.01.01-2023.12.31.

Top 10 kenkėjiškų programų Lietuvoje 2024 metais



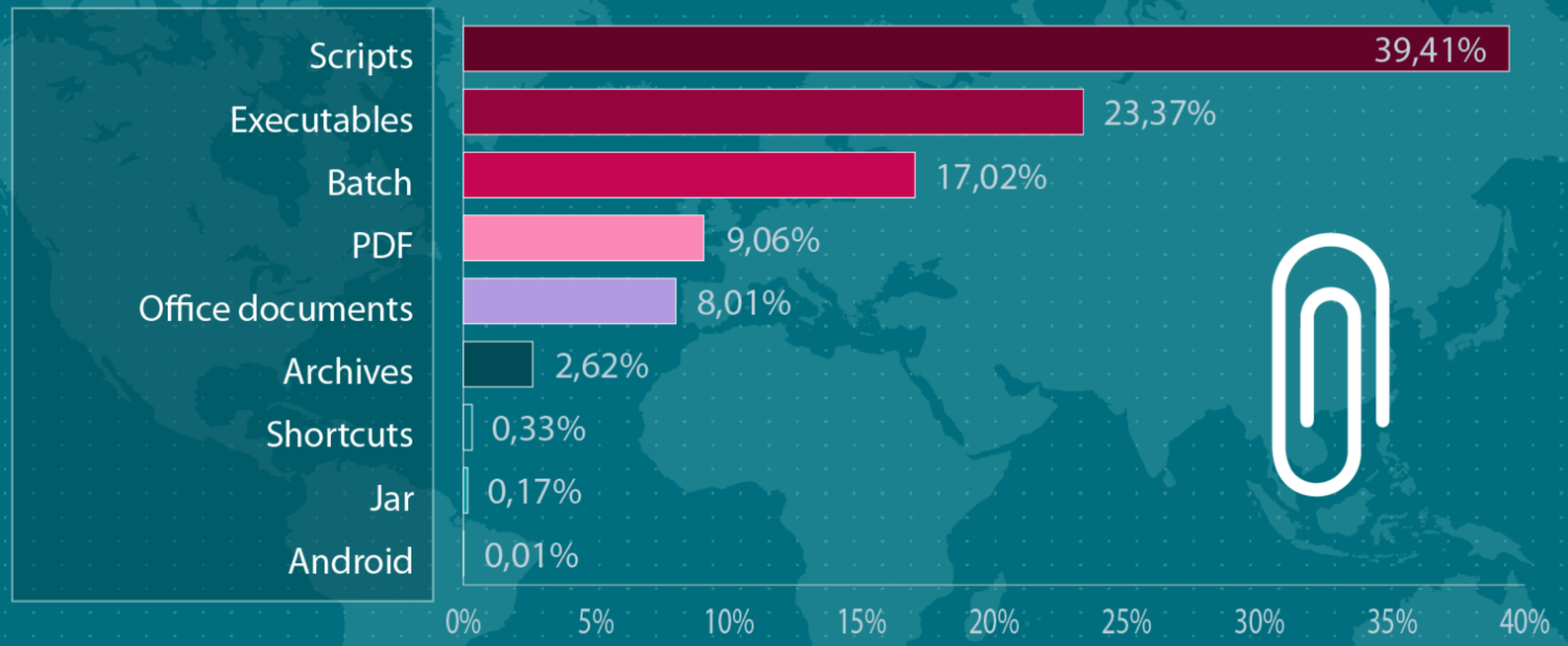
Remiantis ESET telemetrijos duomenimis, top 10 Lietuvoje 2024 metais paplitusių kenkėjiškų programų.

Top 10 grėsmių, plintančių el. paštu Lietuvoje



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

Populiariausi kenkėjiškų prisegtukų tipai

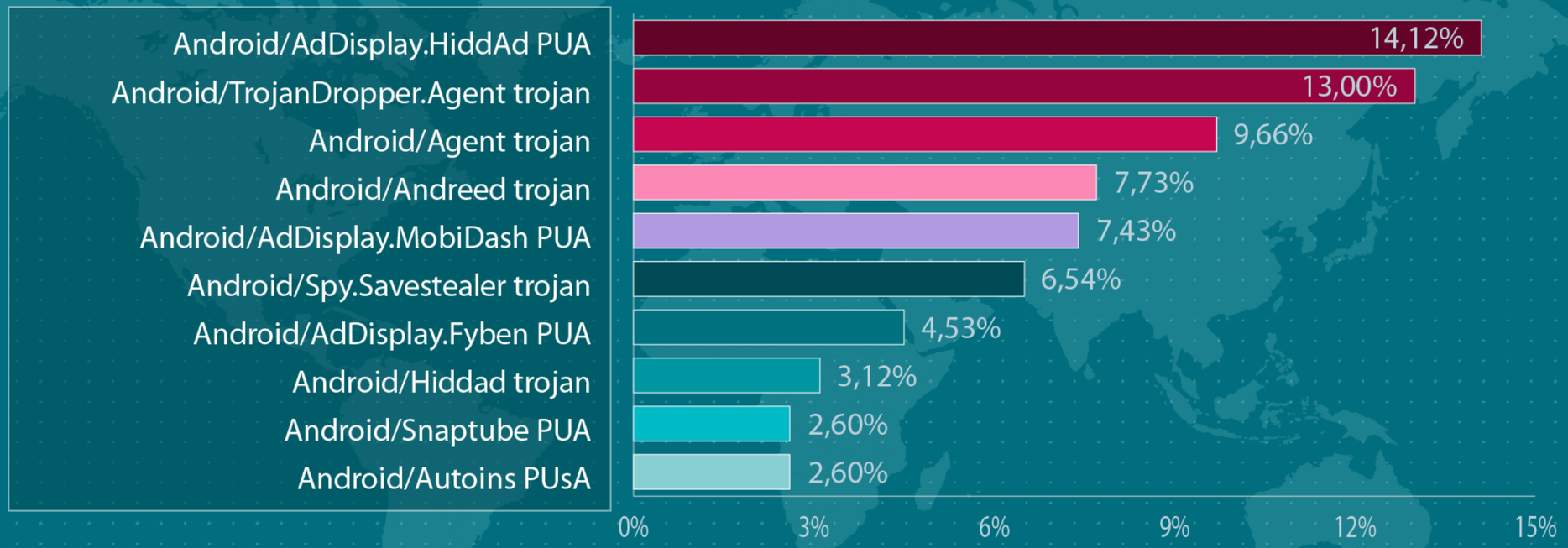


Remiantis ESET telemetrijos duomenimis, populiariausi kenkėjiškų prisegtukų tipai 2024 metais.

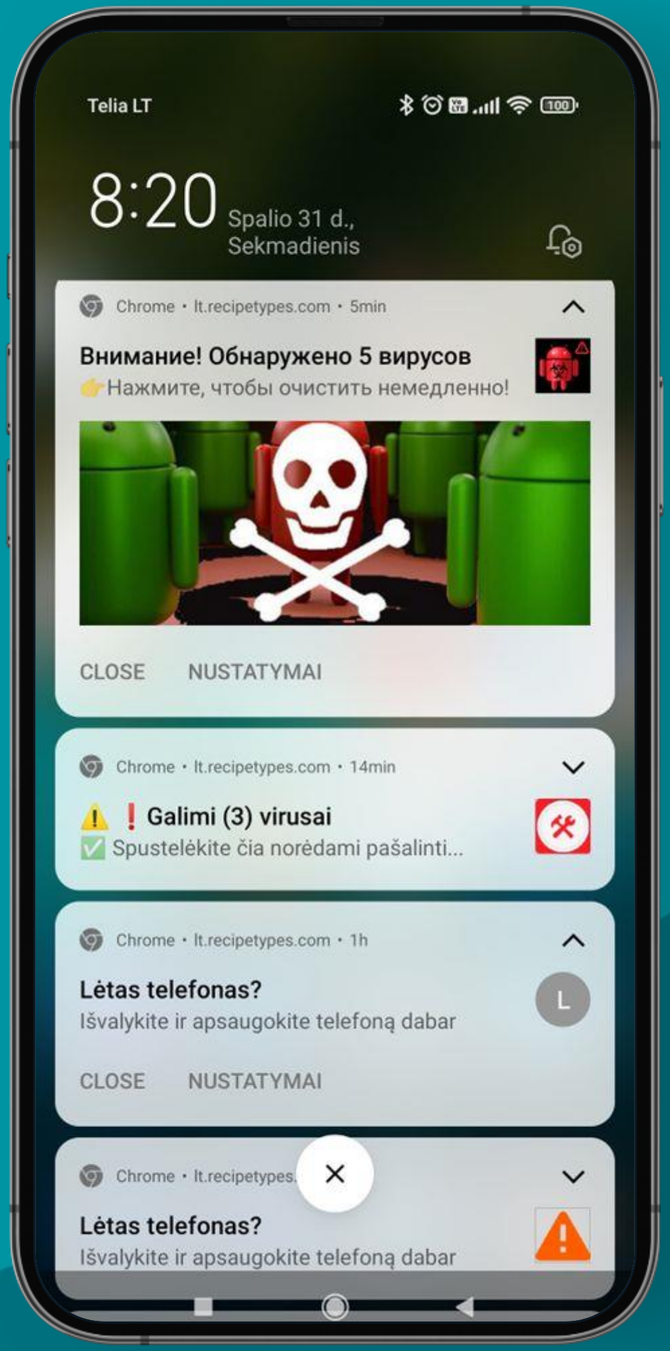
Populiariausios kenkėjiško el. laiško antraštės

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

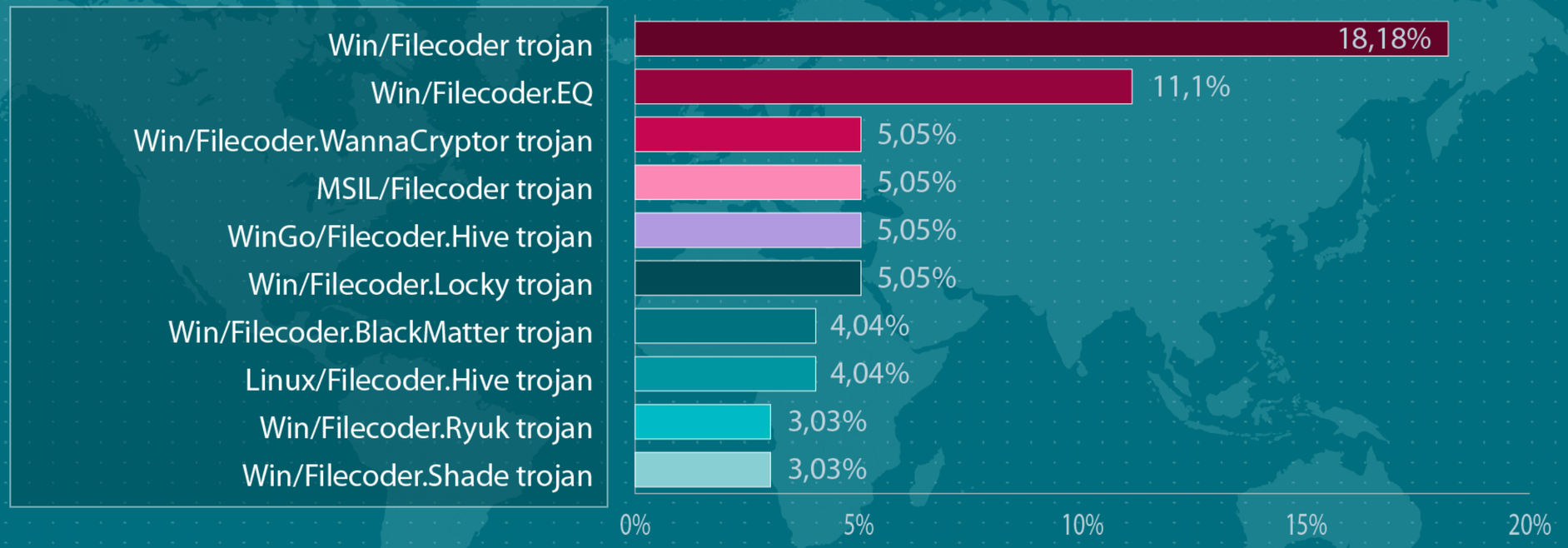
Android kenkėjiškų programų Top 10 Lietuvoje 2024 metais



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

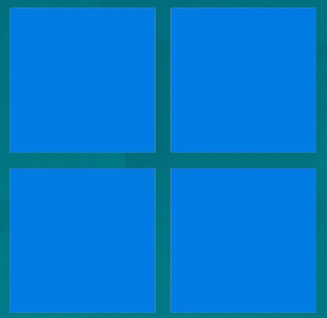


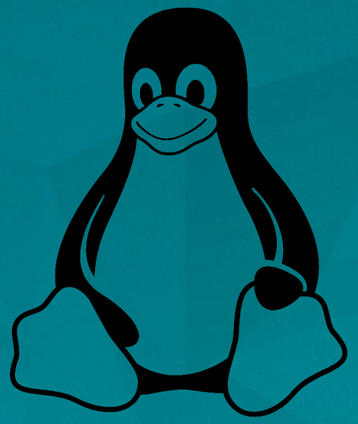
Top 10 #ransomware virusų Lietuvoje 2024 metais



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

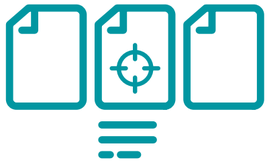
El. pašto paskyrų, prisijungimų prie sistemų

TIKSLINĖS ATAKOS

Nukreipimas į pasirinktą įmonę ar darbuotojus

Tikslinių atakų taikiniai

Interneto svetainės



Programinės įrangos pažeidžiamumai

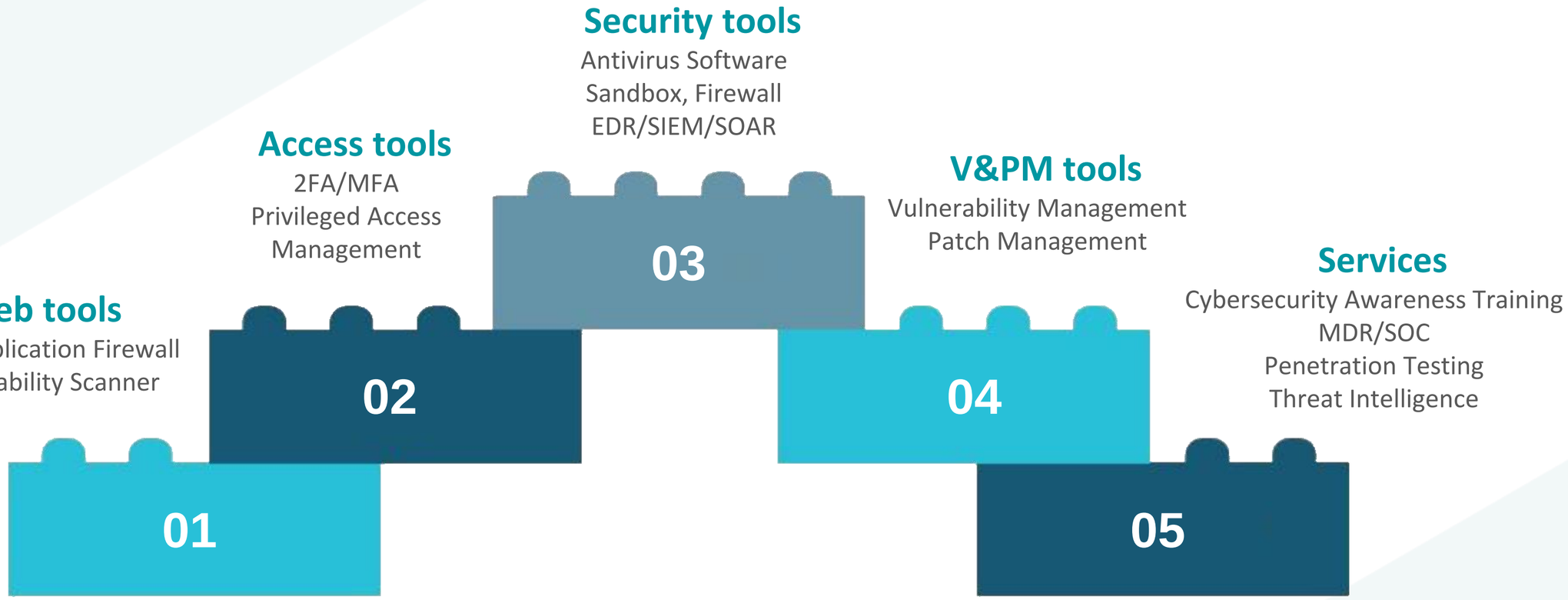
Kompiuterinis tinklas

Atsarginės kopijos

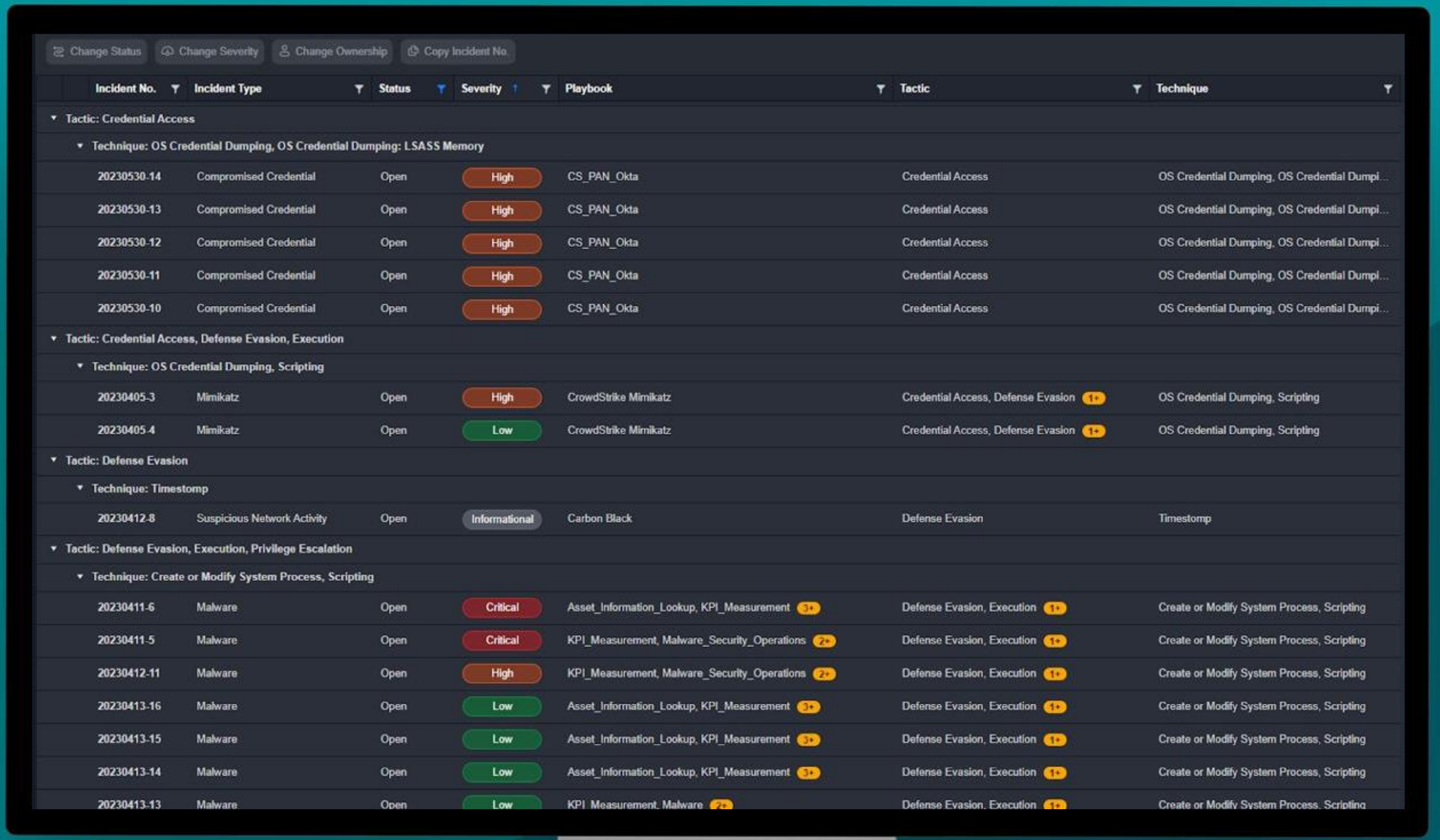
Prieiga prie sistemų

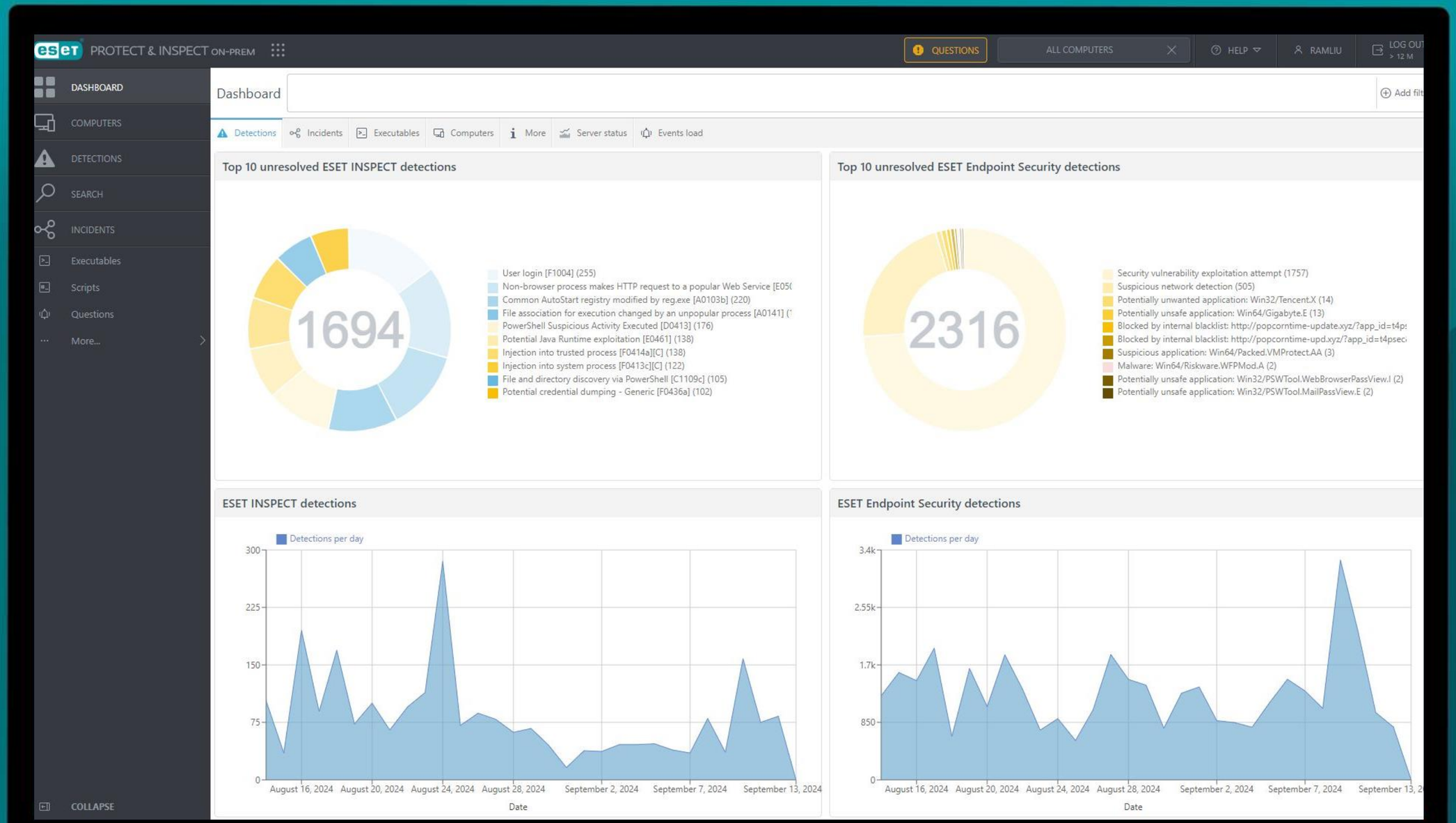
Darbuotojai

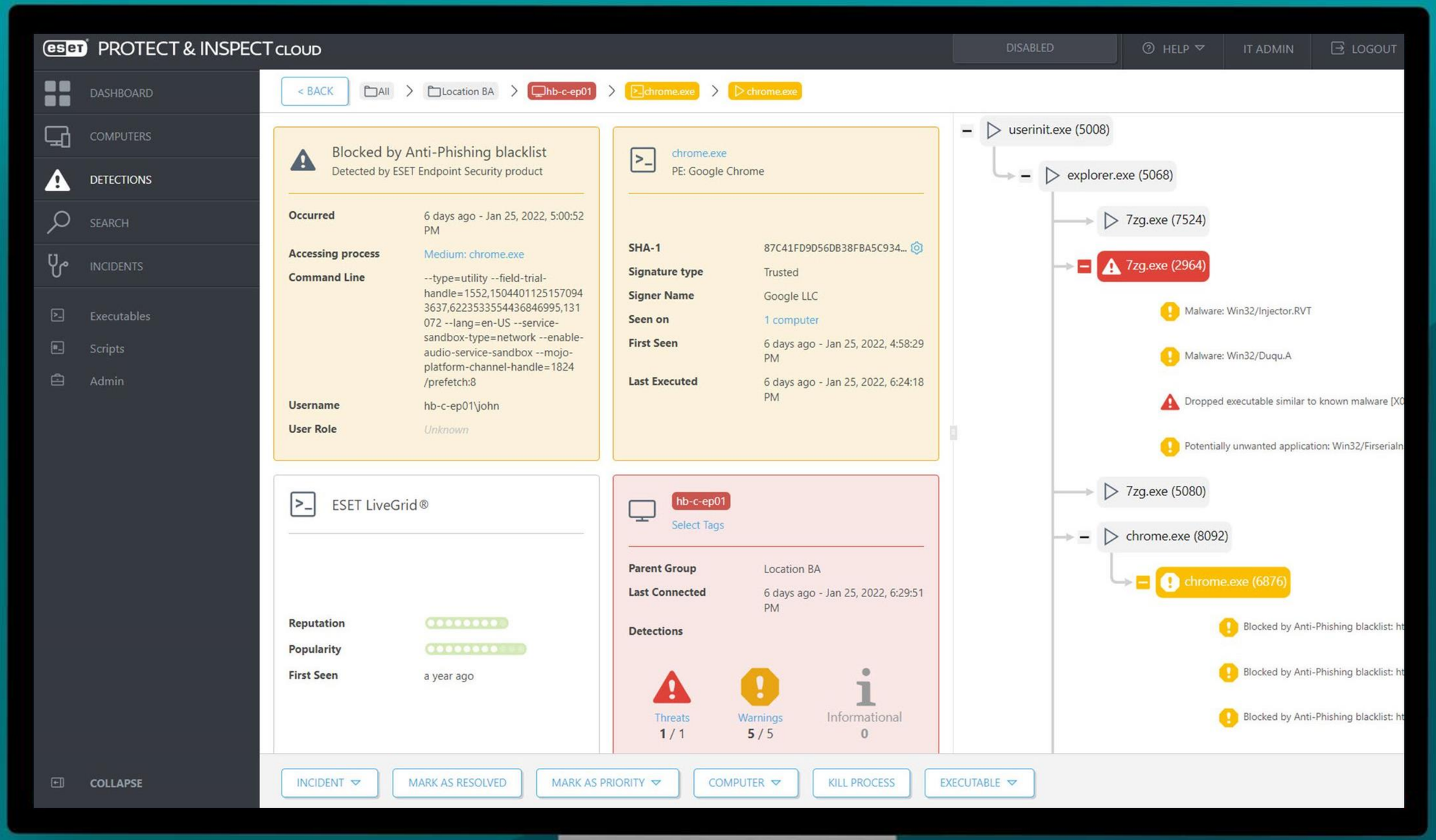
Kibernetinės saugos priemonės

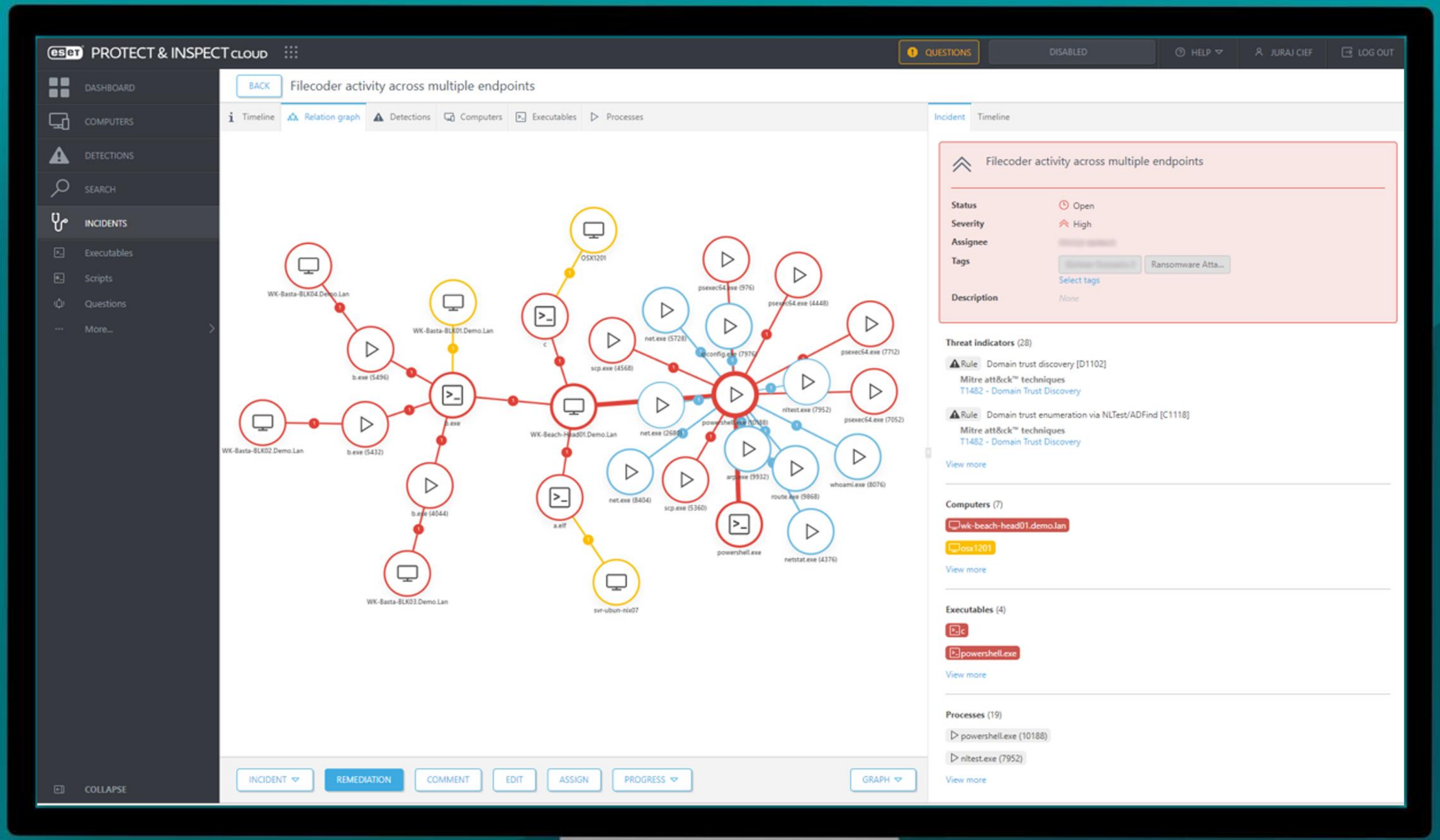


Nuo ko prasideda diena?


Change Status
Change Severity
Change Ownership
Copy Incident No.
Incident No.
Incident Type
Status
Severity
Playbook
Tactic
Technique
Tactic: Credential Access
Technique: OS Credential Dumping, OS Credential Dumping: LSASS Memory
20230530-14 Compromised Credential Open High CS_PAN_Okta Credential Access OS Credential Dumping, OS Credential Dumpi...
20230530-13 Compromised Credential Open High CS_PAN_Okta Credential Access OS Credential Dumping, OS Credential Dumpi...
20230530-12 Compromised Credential Open High CS_PAN_Okta Credential Access OS Credential Dumping, OS Credential Dumpi...
20230530-11 Compromised Credential Open High CS_PAN_Okta Credential Access OS Credential Dumping, OS Credential Dumpi...
20230530-10 Compromised Credential Open High CS_PAN_Okta Credential Access OS Credential Dumping, OS Credential Dumpi...
Tactic: Credential Access, Defense Evasion, Execution
Technique: OS Credential Dumping, Scripting
20230405-3 Mimikatz Open High CrowdStrike Mimikatz Credential Access, Defense Evasion 1+ OS Credential Dumping, Scripting
20230405-4 Mimikatz Open Low CrowdStrike Mimikatz Credential Access, Defense Evasion 1+ OS Credential Dumping, Scripting
Tactic: Defense Evasion
Technique: Timestomp
20230412-8 Suspicious Network Activity Open Informational Carbon Black Defense Evasion Timestomp
Tactic: Defense Evasion, Execution, Privilege Escalation
Technique: Create or Modify System Process, Scripting
20230411-6 Malware Open Critical Asset_Information_Lookup, KPI_Measurement 3+ Defense Evasion, Execution 1+ Create or Modify System Process, Scripting
20230411-5 Malware Open Critical KPI_Measurement, Malware_Security_Operations 2+ Defense Evasion, Execution 1+ Create or Modify System Process, Scripting
20230412-11 Malware Open High KPI_Measurement, Malware_Security_Operations 2+ Defense Evasion, Execution 1+ Create or Modify System Process, Scripting
20230413-16 Malware Open Low Asset_Information_Lookup, KPI_Measurement 3+ Defense Evasion, Execution 1+ Create or Modify System Process, Scripting
20230413-15 Malware Open Low Asset_Information_Lookup, KPI_Measurement 3+ Defense Evasion, Execution 1+ Create or Modify System Process, Scripting
20230413-14 Malware Open Low Asset_Information_Lookup, KPI_Measurement 3+ Defense Evasion, Execution 1+ Create or Modify System Process, Scripting
20230413-13 Malware Open Low KPI_Measurement, Malware 2+ Defense Evasion, Execution 1+ Create or Modify System Process, Scripting


PROTECT & INSPECT ON-PREM
QUESTIONS
ALL COMPUTERS
HELP
RAMLIU
LOG OUT
DASHBOARD
COMPUTERS
DETECTIONS
SEARCH
INCIDENTS
Executables
Scripts
Questions
More...
COLLAPSE
Dashboard
Add filt
Detections
Incidents
Executables
Computers
More
Server status
Events load
Top 10 unresolved ESET INSPECT detections
1694
User login [F1004] (255)
Non-browser process makes HTTP request to a popular Web Service [E05(
Common AutoStart registry modified by reg.exe [A0103b] (220)
File association for execution changed by an unpopular process [A0141] (
PowerShell Suspicious Activity Executed [D0413] (176)
Potential Java Runtime exploitation [E0461] (138)
Injection into trusted process [F0414a][C] (138)
Injection into system process [F0413c][C] (122)
File and directory discovery via PowerShell [C1109c] (105)
Potential credential dumping - Generic [F0436a] (102)
Top 10 unresolved ESET Endpoint Security detections
2316
Security vulnerability exploitation attempt (1757)
Suspicious network detection (505)
Potentially unwanted application: Win32/Tencent.X (14)
Potentially unsafe application: Win64/Gigabyte.E (13)
Blocked by internal blacklist: http://popcorntime-update.xyz/?app_id=t4p
Blocked by internal blacklist: http://popcorntime-upd.xyz/?app_id=t4pse
Suspicious application: Win64/Packed.VMProtect.AA (3)
Malware: Win64/Riskware.WFPMod.A (2)
Potentially unsafe application: Win32/PSWTool.WebBrowserPassView.I (2)
Potentially unsafe application: Win32/PSWTool.MailPassView.E (2)
ESET INSPECT detections
Detections per day
300
225
150
75
0
August 16, 2024
August 20, 2024
August 24, 2024
August 28, 2024
September 2, 2024
September 7, 2024
September 13, 2024
Date
ESET Endpoint Security detections
Detections per day
3.4k
2.55k
1.7k
850
0
August 16, 2024
August 20, 2024
August 24, 2024
August 28, 2024
September 2, 2024
September 7, 2024
Date


PROTECT & INSPECT CLOUD
DISABLED
HELP
IT ADMIN
LOGOUT
DASHBOARD
COMPUTERS
DETECTIONS
SEARCH
INCIDENTS
Executables
Scripts
Admin
COLLAPSE
< BACK
All
Location BA
hb-c-ep01
chrome.exe
chrome.exe
Blocked by Anti-Phishing blacklist
Detected by ESET Endpoint Security product
Occurred
6 days ago - Jan 25, 2022, 5:00:52 PM
Accessing process
Medium: chrome.exe
Command Line
--type=utility --field-trial-handle=1552,1504401125157094 3637,6223533554436846995,131 072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1824 /prefetch:8
Username
hb-c-ep01\john
User Role
Unknown
chrome.exe
PE: Google Chrome
SHA-1
87C41FD9D56DB38FBA5C934...
Signature type
Trusted
Signer Name
Google LLC
Seen on
1 computer
First Seen
6 days ago - Jan 25, 2022, 4:58:29 PM
Last Executed
6 days ago - Jan 25, 2022, 6:24:18 PM
ESET LiveGrid®
Reputation
Popularity
First Seen
a year ago
hb-c-ep01
Select Tags
Parent Group
Location BA
Last Connected
6 days ago - Jan 25, 2022, 6:29:51 PM
Detections
Threats
1 / 1
Warnings
5 / 5
Informational
0
userinit.exe (5008)
explorer.exe (5068)
7zg.exe (7524)
7zg.exe (2964)
Malware: Win32/Injector.RVT
Malware: Win32/Duqu.A
Dropped executable similar to known malware [X
Potentially unwanted application: Win32/Firserialn
7zg.exe (5080)
chrome.exe (8092)
chrome.exe (6876)
Blocked by Anti-Phishing blacklist: ht
Blocked by Anti-Phishing blacklist: ht
Blocked by Anti-Phishing blacklist: ht
INCIDENT
MARK AS RESOLVED
MARK AS PRIORITY
COMPUTER
KILL PROCESS
EXECUTABLE


PROTECT & INSPECT CLOUD
QUESTIONS
DISABLED
HELP
JURAJ CIEF
LOG OUT
DASHBOARD
COMPUTERS
DETECTIONS
SEARCH
INCIDENTS
Executables
Scripts
Questions
More...
COLLAPSE
BACK
Filecoder activity across multiple endpoints
Timeline
Relation graph
Detections
Computers
Executables
Processes
WK-Basta-BLK04.Demo.Lan
WK-Basta-BLK01.Demo.Lan
OSX1201
b.exe (5496)
c
psexec64.exe (976)
psexec64.exe (4448)
scp.exe (4568)
net.exe (5728)
psexec64.exe (7712)
nltest.exe (7952)
psexec64.exe (7052)
WK-Basta-BLK02.Demo.Lan
b.exe (5432)
b.exe
WK-Beach-Head01.Demo.Lan
net.exe (2688)
net.exe (8404)
scp.exe (5360)
whoami.exe (8076)
route.exe (9868)
b.exe (4044)
a.elf
powershell.exe
netstat.exe (4376)
WK-Basta-BLK03.Demo.Lan
svr-ubun-nix07
INCIDENT
REMEDIATION
COMMENT
EDIT
ASSIGN
PROGRESS
GRAPH
Incident
Timeline
Filecoder activity across multiple endpoints
Status
Open
Severity
High
Assignee
Tags
Ransomware Atta...
Select tags
Description
None
Threat indicators (28)
Rule
Domain trust discovery [D1102]
Mitre att&ck™ techniques
T1482 - Domain Trust Discovery
Rule
Domain trust enumeration via NLTest/ADFind [C1118]
Mitre att&ck™ techniques
T1482 - Domain Trust Discovery
View more
Computers (7)
wk-beach-head01.demo.lan
osx1201
View more
Executables (4)
c
powershell.exe
View more
Processes (19)
powershell.exe (10188)
nltest.exe (7952)
View more

Įvykis, incidentas ar įsilaužimas?

Įvykis, incidentas ar įsilaužimas?

- Duomenų srauto šuoliai
- Leidimų pakeitimai
- Atsisiunčiama trečiosios šalies programinė įranga
- Saugos nustatymų pakeitimai
- Įtartino el. laiško arba sukčiavimo bandymo pėdsakai

Įvykis, incidentas ar įsilaužimas?

- Sukčiavimo atakos
- Piktnaudžiavimas privilegijuota prieiga
- Kenkėjiškų programų atakos
- DDoS atakos
- Viešai neatskleista neskelbtina duomenų vagystė

Įvykis, incidentas ar įsilaužimas?

- Pavogti slaptažodžiai
- Kenkėjiška programa
- SQL injekcijos ataka
- DDoS ataka

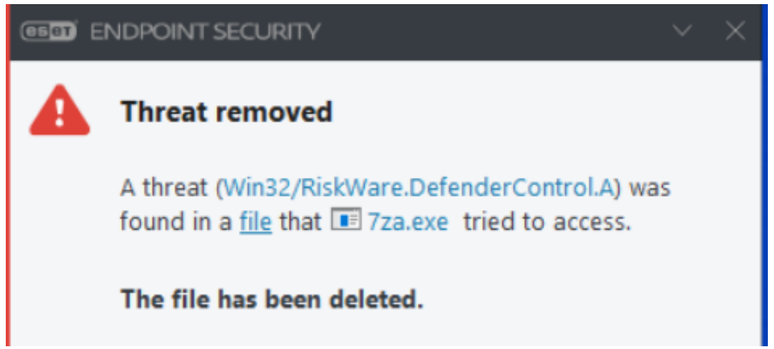
Picų vakarėlis prasideda!

Bendri įsilaužimo bruožai

Bendri įsilaužimo bruožai

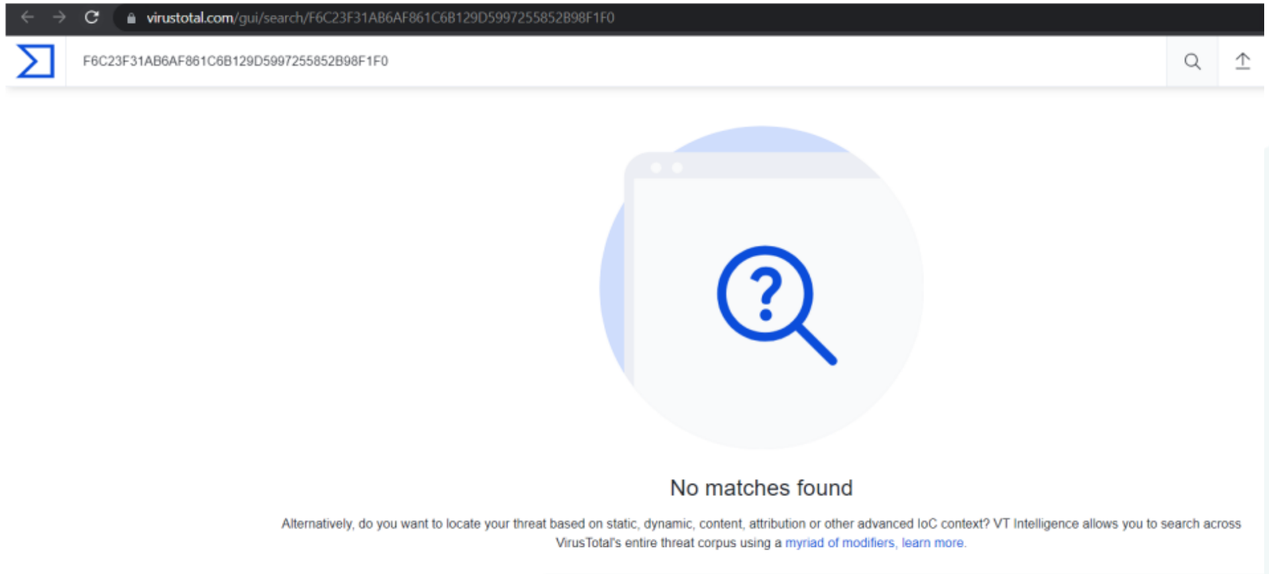
Įrenginys: BACKUP-PC
- Neturi jokios apsaugos.
- Vartotojo paskyros valdymas (UAC) yra išjungtas.

Pasirodo ir antras blokavimas – virusas turi funkciją, kuri išjungia gamyklinę „Windows defender“ apsaugą, ESET blokuoja šį veiksmą.



Failai buvo užšifruoti: Win32/Filecoder.Mimic.A (Win32/Filecoder.Medusa atmaina)
Virusas yra aptinkamas naudojant ir senesnes virusų duomenų bazes.

Failas nematytas viešai:



Bendri įsilaužimo bruožai

- Laukiantys „Windows“ atnaujinimai.

Pending Windows Updates:

Microsoft .NET Framework 4.8.1 for Windows 10 Version 22H2 for x64 (KB5011048)
2023-07 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 10 Version 22H2 for x64 (KB5028937)
2023-07 Cumulative Update for Windows 10 Version 22H2 for x64-based Systems (KB5028166)

Įjungtas pažeidžiamas SMBv1 protokolas.

Įdiegta „Windows Server 2008 R2 Standard“.

Išjungtas tinklo lygmens autentiškumo nustatymas.

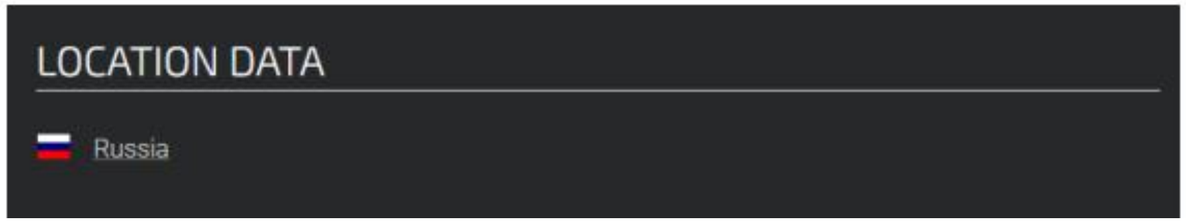
Accounts policy:

Setting	Value
Force user logoff	Never
Minimum password age (days)	1
Maximum password age (days)	42
Minimum password length	7
Length of password history maintained	24
Lockout threshold	Never
Lockout duration (minutes)	30
Lockout observation window (minutes)	30

Bendri įsilaužimo bruožai

Atakos pirminė informacija: įsilaužėlis nenustatytu būdu gavo RDP administratoriaus prisijungimus. Galėjo juos rasti nutekėjusioje DB, internete, arba naudojo „Brute-force“ ataką, kad prisijungtų prie sistemų nuotoliniu būdu.

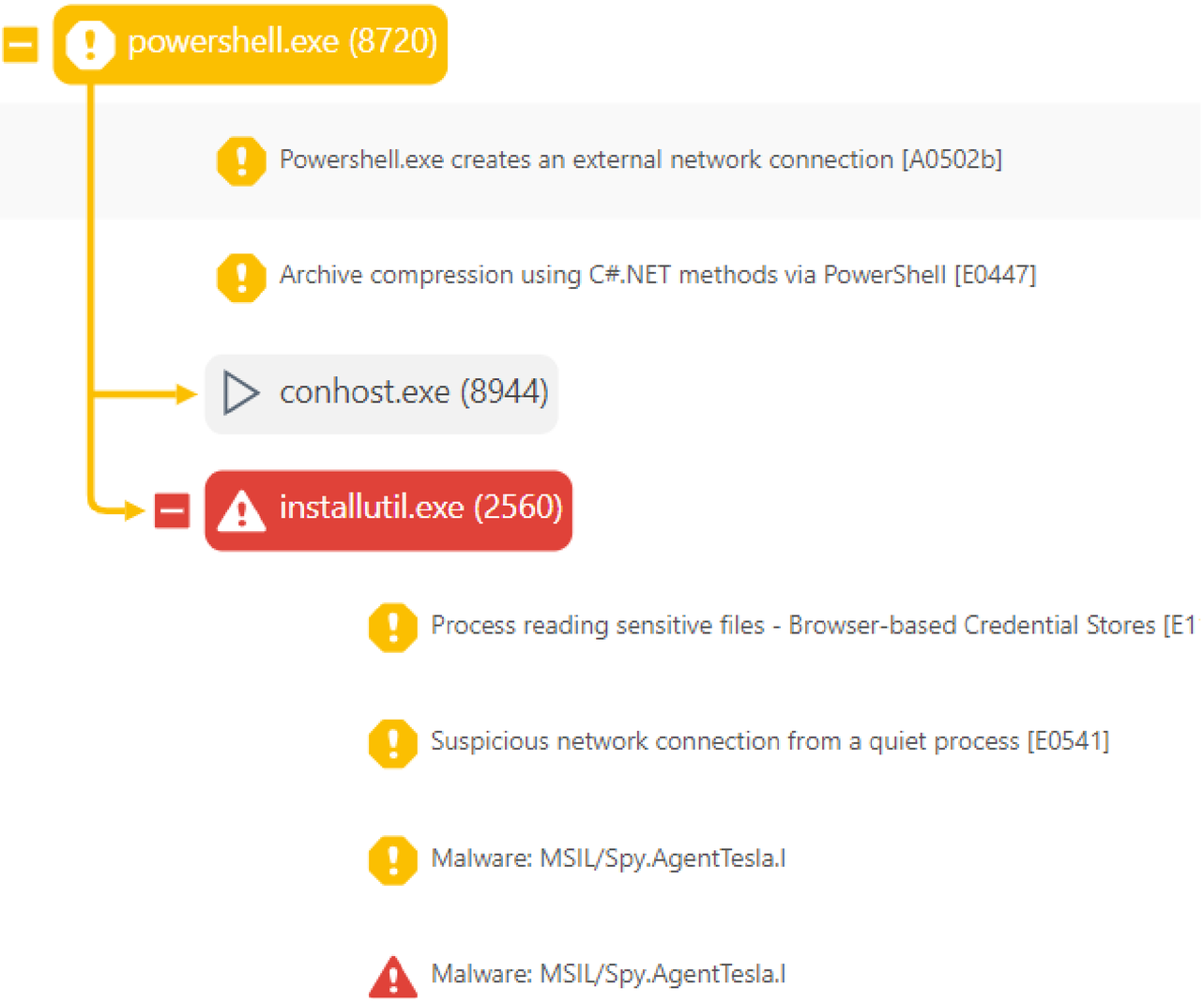
Sėkmingai prisijungė iš Rusijos IP per RDP su „Administrator“ paskyra.

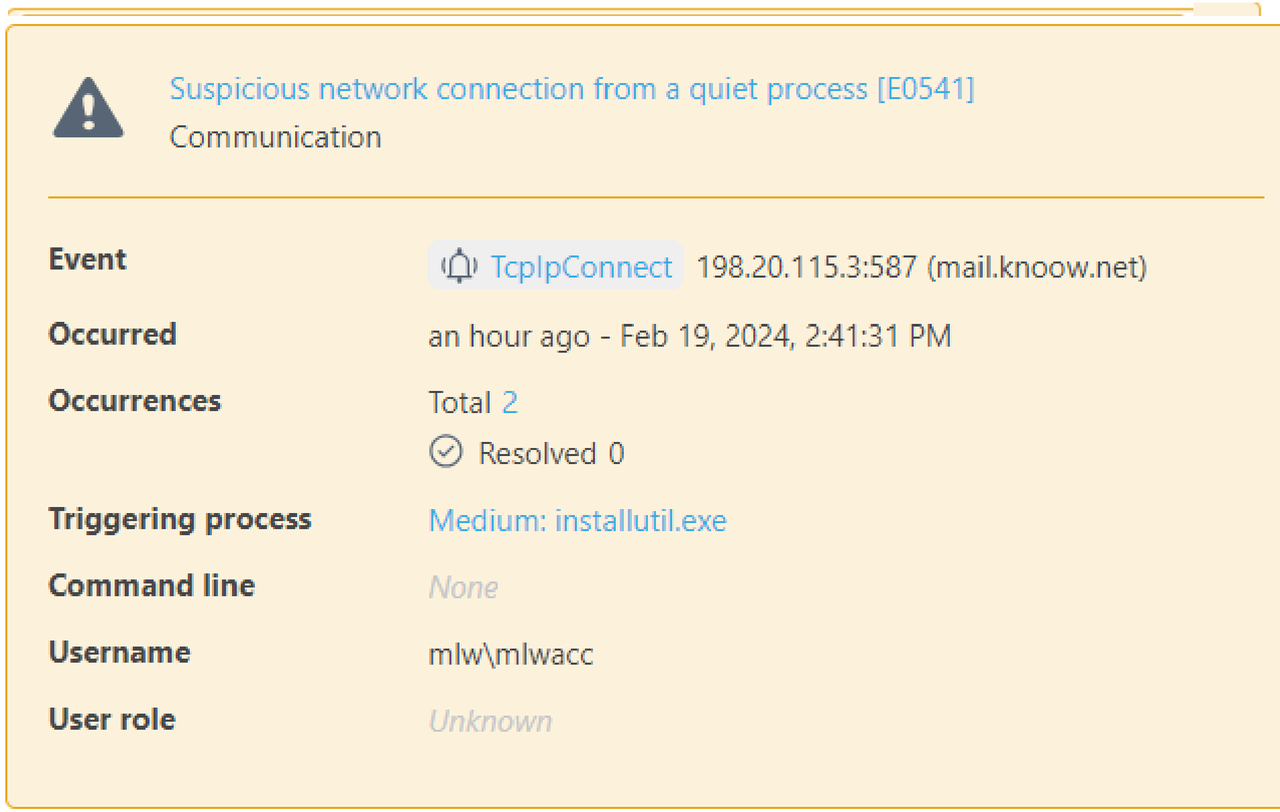


Ataka įvyko vidurnaktį: 00:27 ir kiti, panašūs blokavimo laikai.

Visi duomenys tinkle buvo pasiekiami iš bet kokio kompiuterio vidiniame tinkle.
Duomenys buvo šifruojami iš nutolusio kompiuterio.

Bendri įsilaužimo bruožai

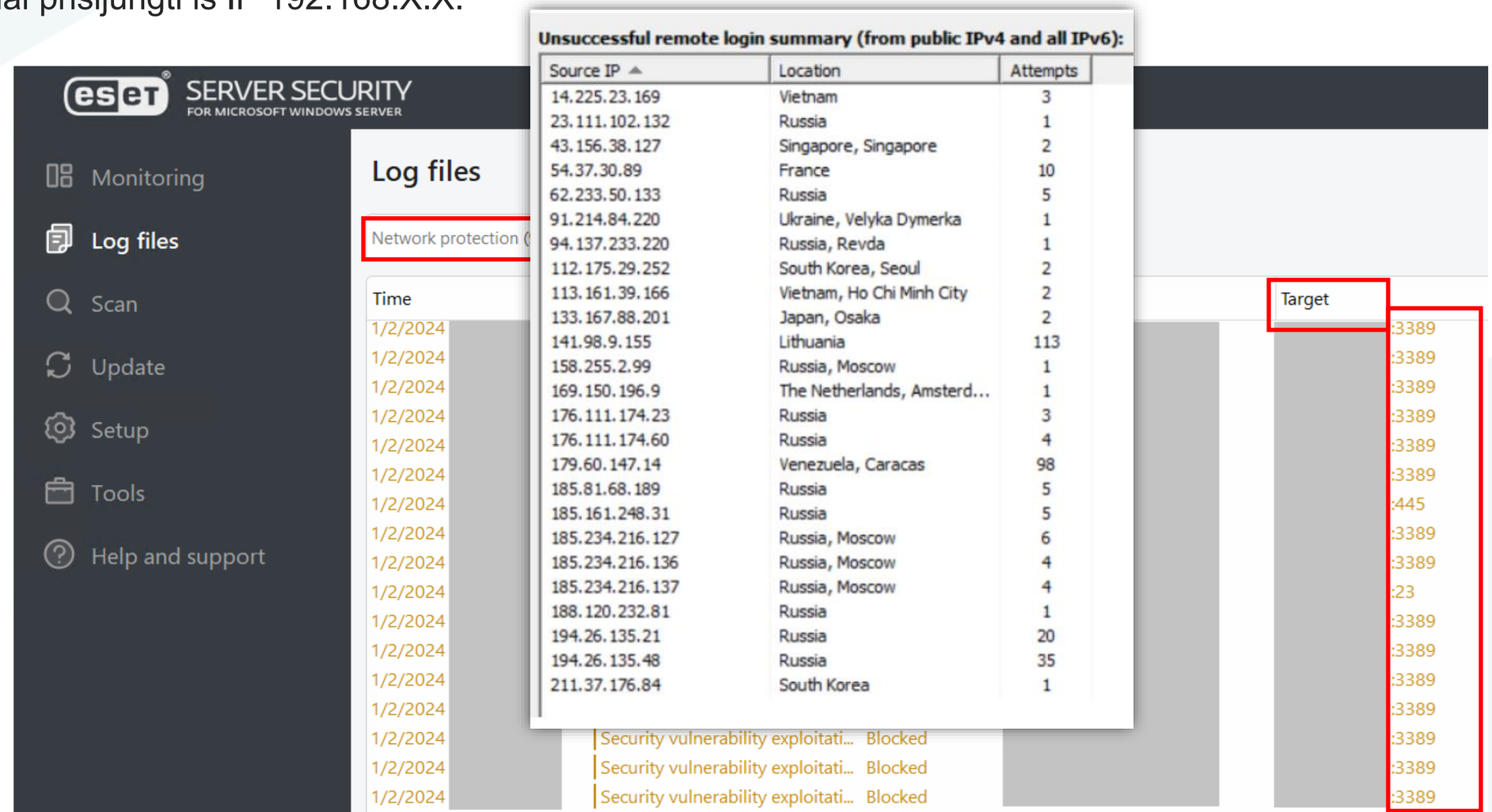




Bendri įsilaužimo bruožai

„Brute-force“ atakos buvo vykdomos iš kompiuterių, esančių vartotojo vietiniame tinkle:

- 155 nesėkmingi bandymai prisijungti iš IP 192.168.X.X.

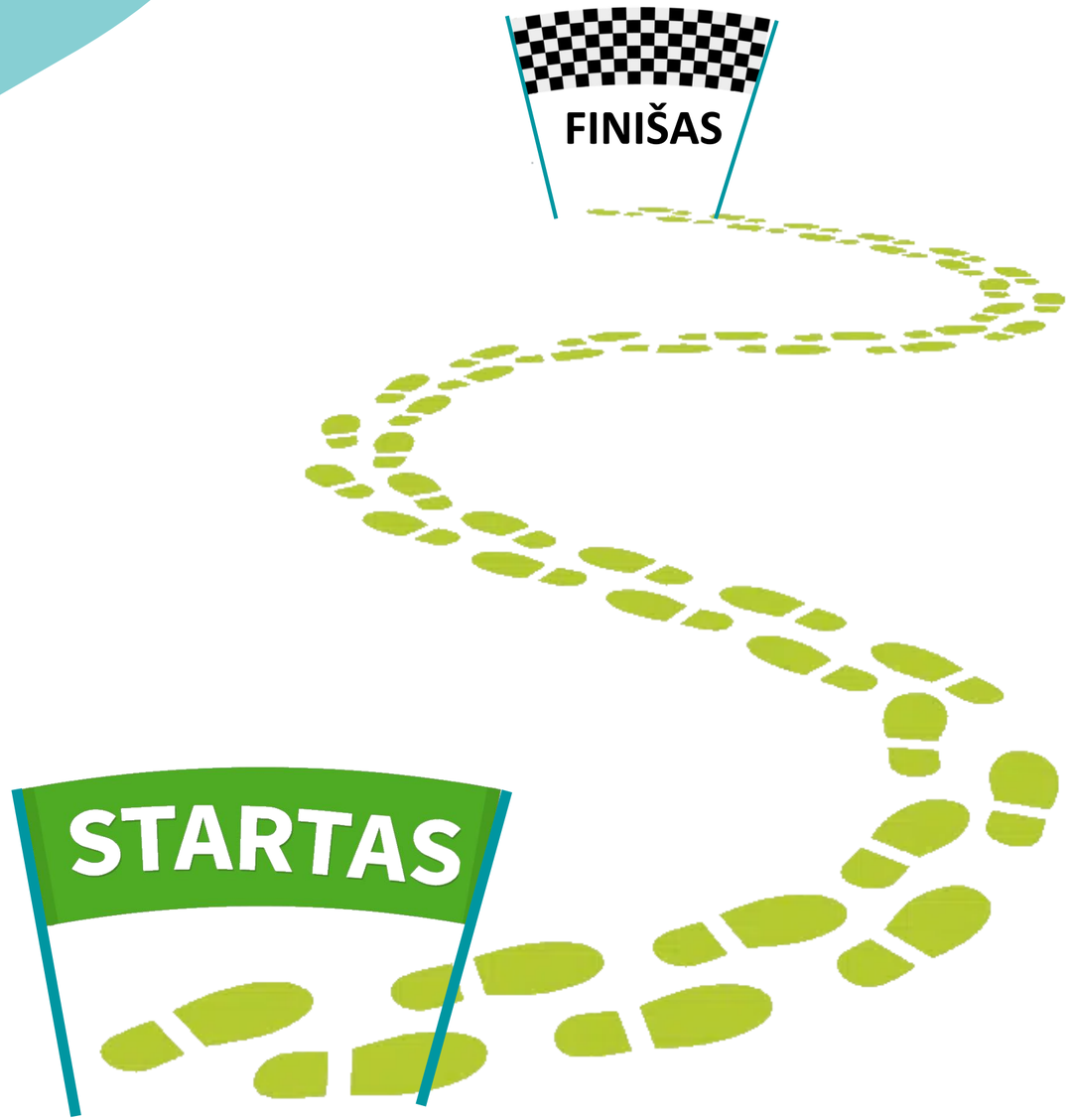


Source IP	Location	Attempts
14.225.23.169	Vietnam	3
23.111.102.132	Russia	1
43.156.38.127	Singapore, Singapore	2
54.37.30.89	France	10
62.233.50.133	Russia	5
91.214.84.220	Ukraine, Velyka Dymerka	1
94.137.233.220	Russia, Revda	1
112.175.29.252	South Korea, Seoul	2
113.161.39.166	Vietnam, Ho Chi Minh City	2
133.167.88.201	Japan, Osaka	2
141.98.9.155	Lithuania	113
158.255.2.99	Russia, Moscow	1
169.150.196.9	The Netherlands, Amsterd...	1
176.111.174.23	Russia	3
176.111.174.60	Russia	4
179.60.147.14	Venezuela, Caracas	98
185.81.68.189	Russia	5
185.161.248.31	Russia	5
185.234.216.127	Russia, Moscow	6
185.234.216.136	Russia, Moscow	4
185.234.216.137	Russia, Moscow	4
188.120.232.81	Russia	1
194.26.135.21	Russia	20
194.26.135.48	Russia	35
211.37.176.84	South Korea	1

Incidentų tyrimai – blogosios praktikos

- Interneto naršyklėse saugomi vartotojų slaptažodžiai / nesaugūs slaptažodžiai
- Nenaudojamas 2FA/MFA
- Nesaugiai atvertos nuotolinės prieigos
- Nepalaikomos/be kritinių atnaujinimų operacinės sistemos
- Netinkama saugumo produktų konfigūracija
- Pasenusios programinės įrangos naudojimas
- Nėra saugumo produkto ar saugumo strategijos
- Netikrinamos atsarginės kopijos

TAKE AWAY



Jei reikalingos konsultacijos ar trūksta kompetencijų – NOD Baltic komanda visada šalia!

Digital Security
Progress. Protected.

ramunas@eset.lt

Bendraukime

www.eset.lt