Cybersecurity
Progress. Protected.

2026 M. KIBERNETINIO SAUGUMO TENDENCIJOS: KAIP APSISAUGOTI?

Lukas Apynis

Baltimax vyresnysis kibernetinio saugumo inžinierius ir ESET ekspertas

Populiariausios kibernetinės grėsmės pasaulyje 2025 metais

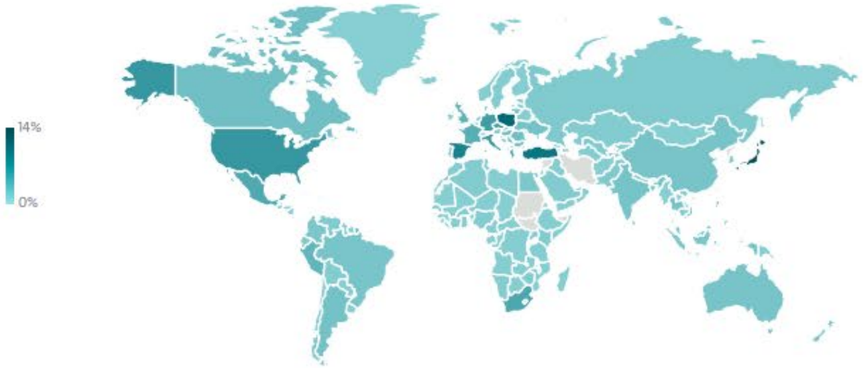
Cybersecurity
Progress. Protected.

ESET Threat Report

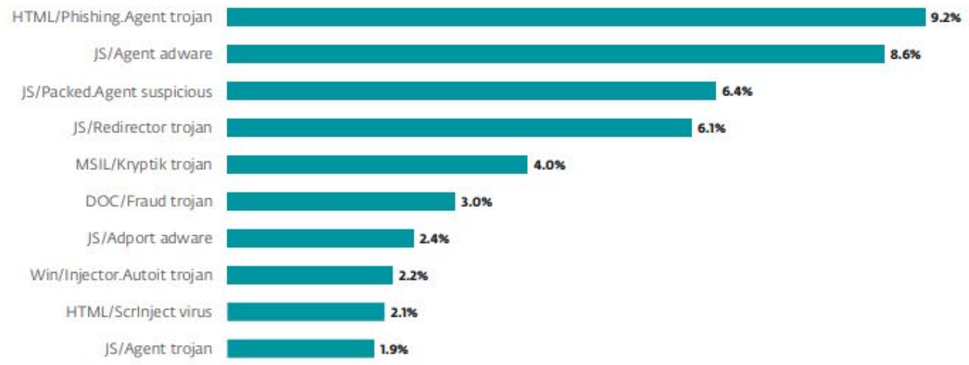
2025 m. duomenys

All threats

Overall threat detection trend in H1 2025 and H2 2025, seven-day moving average



Geographic distribution of malware detections in H2 2025

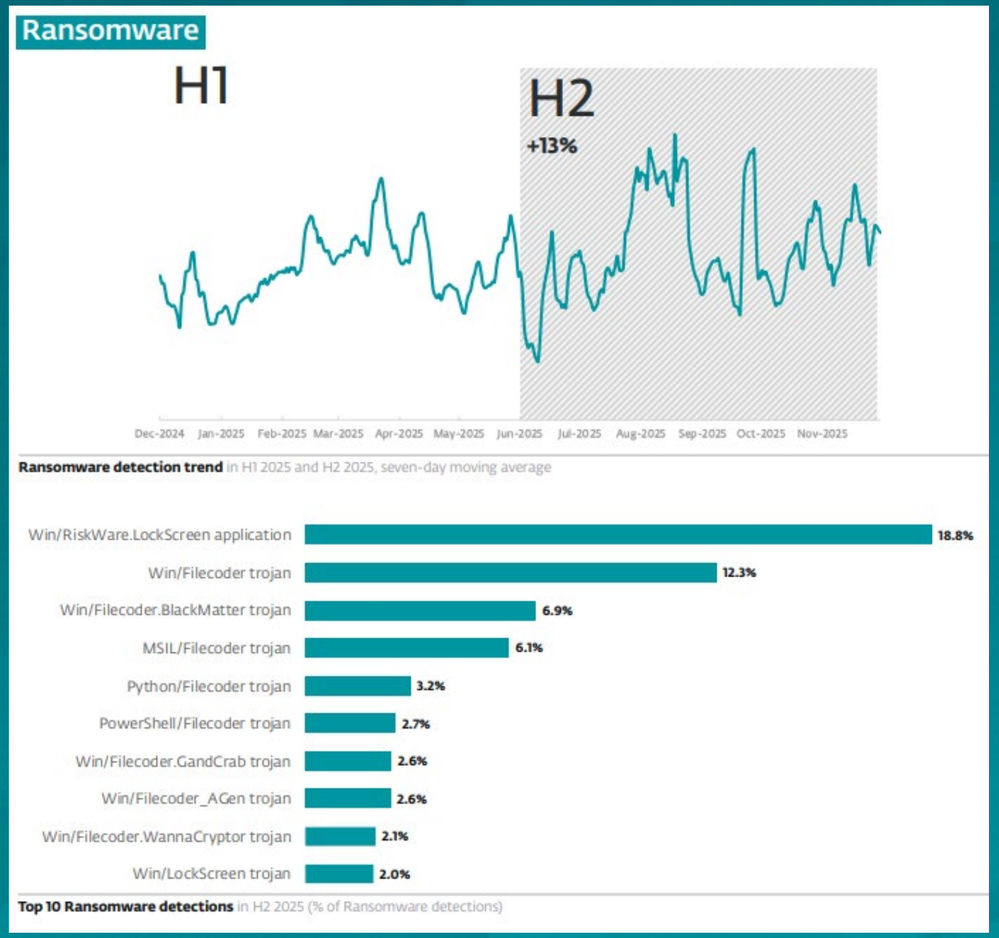


Top 10 malware detections in H2 2025 (% of malware detections)

eset® Cybersecurity
Progress. Protected.

ESET Threat Report

2025 m. duomenys



Cybersecurity
Progress. Protected.

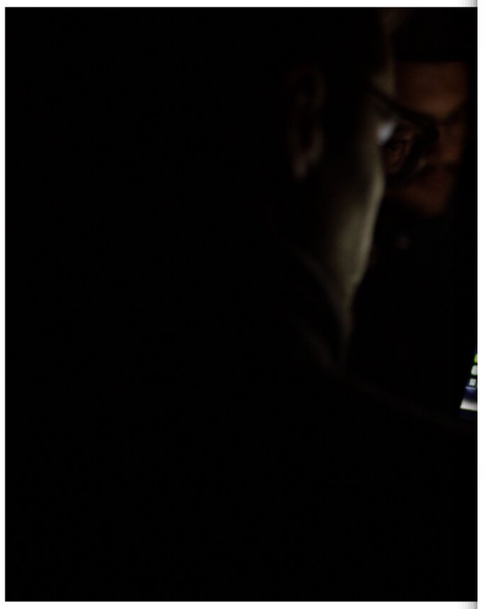
Kokia buvo situacija Lietuvoje 2025 metais?

Cybersecurity
Progress. Protected.

Mokslas ir IT 2025.08.12 14:08

„Creditinfo“ patyrus kiberr
tūkst. Lietuvos vartotojų du

LRT.lt
2025.08.12 14:08



Programišiai | J. Stacevičiaus / LRT nuotr.

Liepos 25 d. buvo išplatinta žinia, kad
informacijos bendrovė „Creditinfo“ pa
kibernetinę ataką. Tuomet įmonė teig
nepaveikė. Tačiau *15min* duomenimis,
buvo nutekinta.

LOGIN KONFERENCIJA Technologijos Verslas Progresas Finansinės techn

LOGIN › PROGRESAS › KIBERNETINIS SAUGUMAS

„RackRay“ patyrė kibernetinio saugu
patarė, kaip elgtis nukentėjusiems

„LOGIN“ žurnalistė **Rusnė Valatkaitė**

Delfi

**Bendrovė „RackRay“ savo klientams
pirmadienį patyrė kibernetinio saugu**

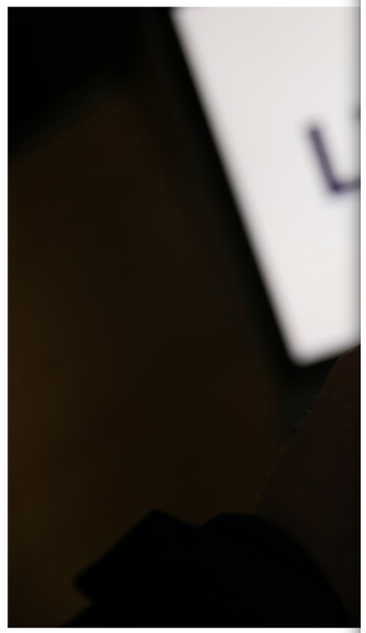
Bendrovės klientai sulaukė elektroninio laišk
kibernetinio saugumo **incidentas** paveikė „R
debesijos paslaugų teikimą.

„Mūsų techninis skyrius nustatė, kad nuo 202
paveikta „Cloudstack“ viešosios debesijos pl
incidento analizę, paaiškėjo, kad incidento su
atsarginių kopijų ir virtualiuose serveriuose e

Tavo LRT 2025.03.04 09:03

LRT.lt patyrė kiberr
nesutrikdyta 10

LRT.lt
2025.03.04 09:03



Portalas LRT.lt | D. Umbraso / LRT nuotr.

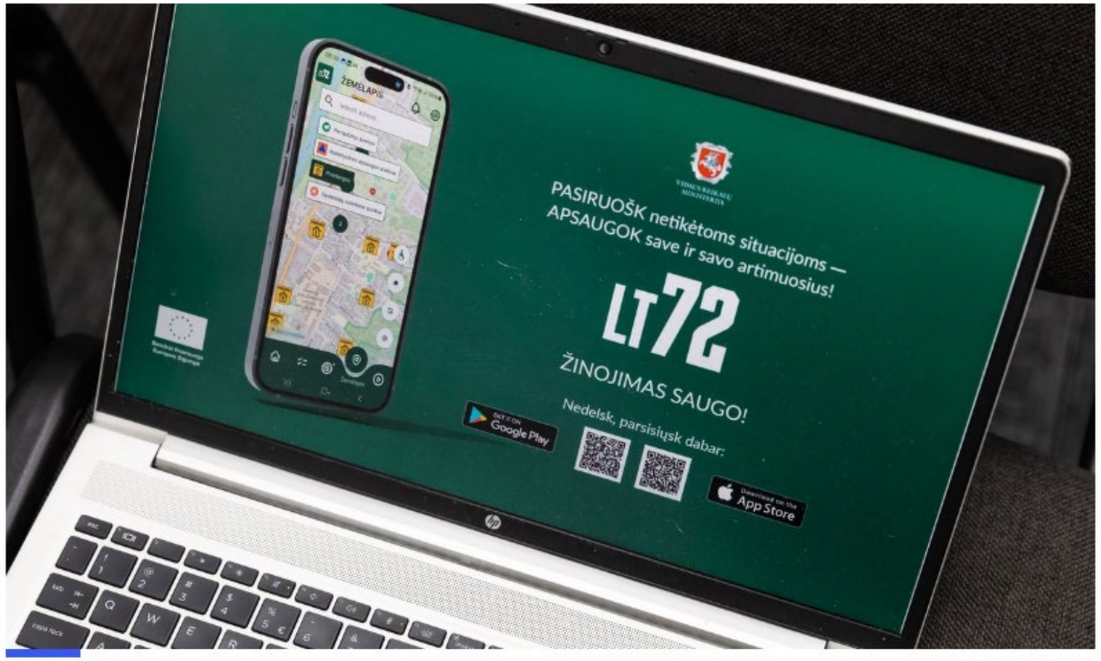
Portalas LRT.lt nuo sekmad
kibernetinę ataką, kurios ti
portalo darbą.

Delfi Naujienos TV Verslas Sportas Veidai Laisvalaikis RU Projektai Kita Mano Delf

Delfi › Dienos naujienos › Lietuvoje 2025.03.22 12:50

Pasirengimo ekstremaliosioms situacijos interneto svetainėje įvykdytas kibernetinis incidentas

Delfi



LT72

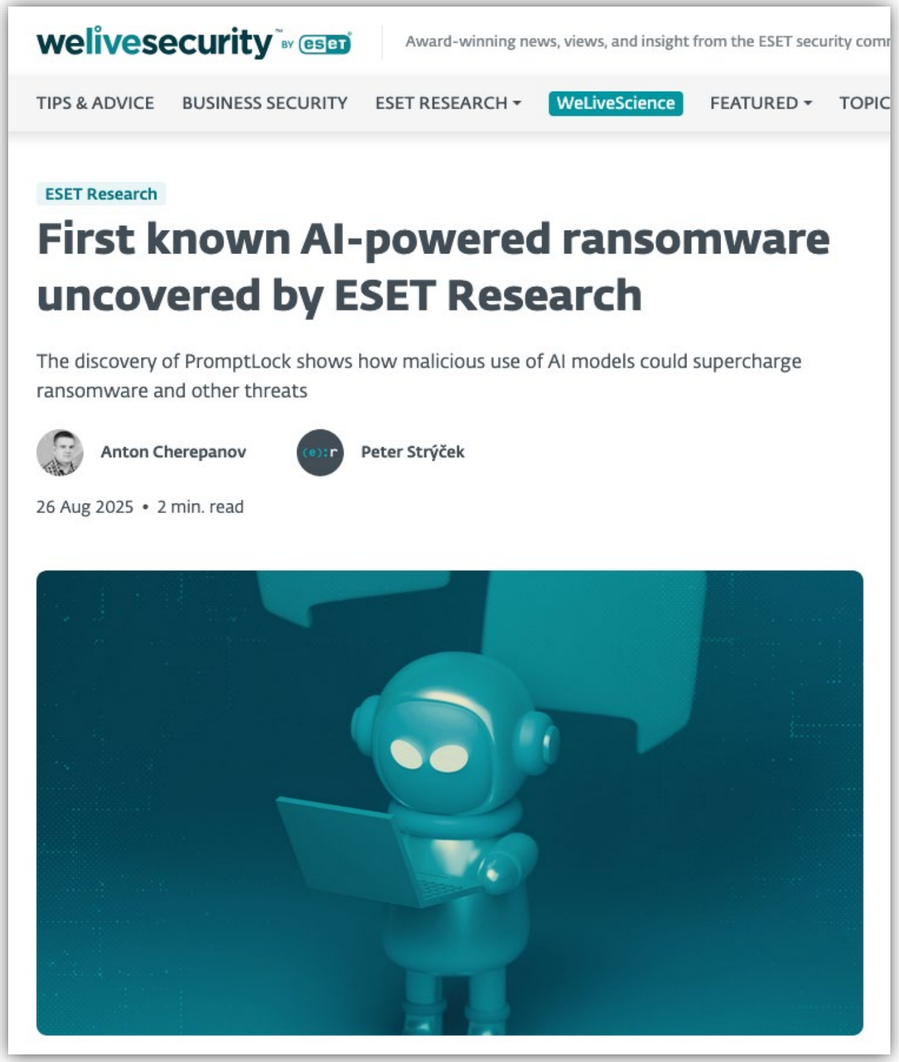
FOTO: DAINIUS LABUTIS | ELTA

Priešgaisrinės apsaugos ir gelbėjimo departamentas informuoja, kad įvyko kibernetinis incidentas interneto svetainėje LT72.

2025 metais pasitvirtinusios globalios prognozės

Cybersecurity
Progress. Protected.

Failų šifravimo atakos pasitelkiant DI



Šaltinis: https://www.welivesecurity.com/en/ransomware/first-known-ai-powered-ransomware-uncovered-eset-research/

Kibernetinio saugumo įstatymas

LIETUVOS RESPUBLIKOS
KRAŠTO APSAUGOS MINISTERIJA

Paieška...

Ministerija | Gynybos politika | Veiklos sritys

Pagrindinis / Kibernetinio saugumo įstatymas

Kibernetinio saugumo įstatymas

2024 m. spalio 18 d. įsigaliojo **atnaujintas Kibernetinio saugumo įstatymas** (toliau – Kibernetinio saugumo įstatymas).

Kibernetinio saugumo įstatymu įgyvendinami **šie Europos Sąjungos teisės aktai**:

- **TIS 2 direktyva**;
- **Kibernetinio saugumo aktas**;
- Europos Parlamento ir Tarybos reglamentas, kuriuo įsteigiamas **Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras** ir **Nacionalinių koordinavimo centrų tinklas**.

Į **Kibernetinio saugumo įstatymą** perkeltos **TIS 2 direktyvos nuostatos** sustiprins **kibernetinio saugumo valdysenos modelį** Lietuvoje.

ESET XDR

Cybersecurity
Progress. Protected.

Doom įvykių seka

Everything is fine

Day 1

Everything is fine

Beginning

Everything is fine

Day 2

Everything is fine

Everything is fine

Day 3

Everything is fine

Everything is…

…ON FIRE!!!

Day 4

Doom įvykių seka

Everything is…

…ON FIRE!!!

Everything is fine

Everything is fine

Everything is fine

Everything is fine

Day 1

Day 2

Day 3

Day 4

Beginning

Initial Access

Discovery

Tool Ingress Transfer

Command and Control

Execution

Lateral Movement

Evasion

Active Scanning

Command and Scripting

Credential Theft

IMPACT

Files Encrypted

Doom įvykių seka

Everything is…

…ON FIRE!!!

Day 1 | Day 2 | Day 3 | Day 4

Beginning

Initial Access

IMPACT
Files Encrypted

Dvi dienas buvo blokuojama daugybė veiksmų

Threat Name – Day 1	Count
Suspicious	5
URL/Urlik.AAF	1
URL/Urlik.C	1
URL/Urlik.E	1
Win64/GenKryptik.GTKR	1
Win64/Kryptik.EEY	5
Win64/Kryptik.EFH	1
Renamed PowerShell Execution [D0411]	19
Total	34

Threat Name – Day 2	Count
Hash blocked by ESET LiveGuard	2
Generik.GXUDDTG	2
MSIL/HackTool.SharpShares.A	1
MSIL/Riskware.BloodHound.D	6
MSIL/Riskware.Rubeus.A	3
Suspicious	14
Win32/GenCBL.EQQ	2
Win32/Rozena.SA	2
Win64/CobaltStrike.Agent.B	2
Win64/CobaltStrike.Artifact.Z	1
Win64/CobaltStrike.Beacon.A	2
Win64/GenKryptik.GTCZ	2
Win64/GenKryptik.GTOS	2
Win64/Kryptik.EEY	2
Win64/Kryptik.EFH	7
Win64/Kryptik.EFK	5
Win64/Kryptik.EFP	2
Renamed PowerShell Execution [D0411]	4
Total	62

Doom įvykių seka

Everything is…

…ON FIRE!!!

Day 1 | Day 2 | Day 3 | Day 4

Beginning

Initial Access

Discovery

Execution

Tool Ingress Transfer

IMPACT
Files Encrypted

Doom įvykių seka

Everything is…

…ON FIRE!!!

Day 1 Day 2 Day 3 Day 4

Beginning

Initial Access

Discovery

Execution

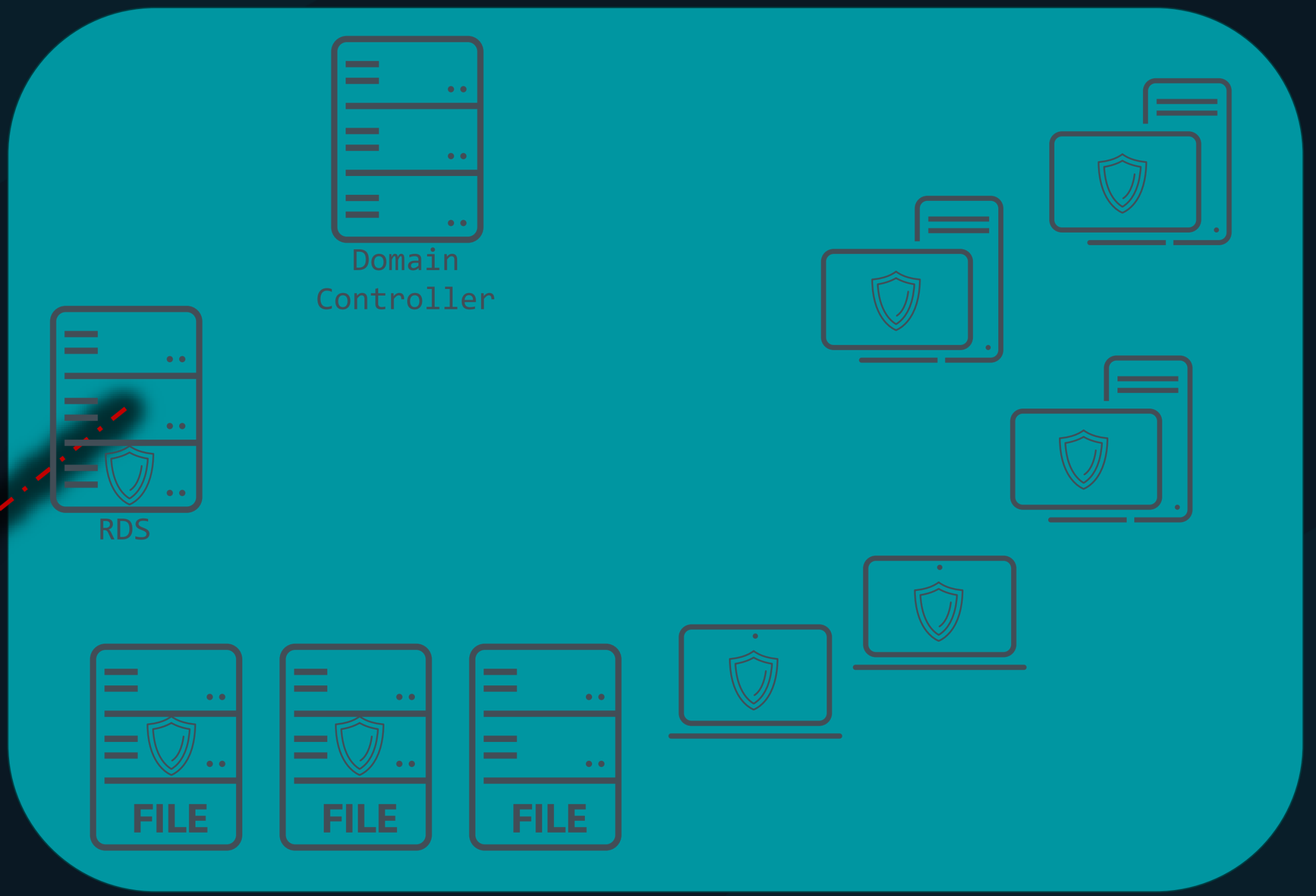
Tool Ingress Transfer

IMPACT
Files Encrypted

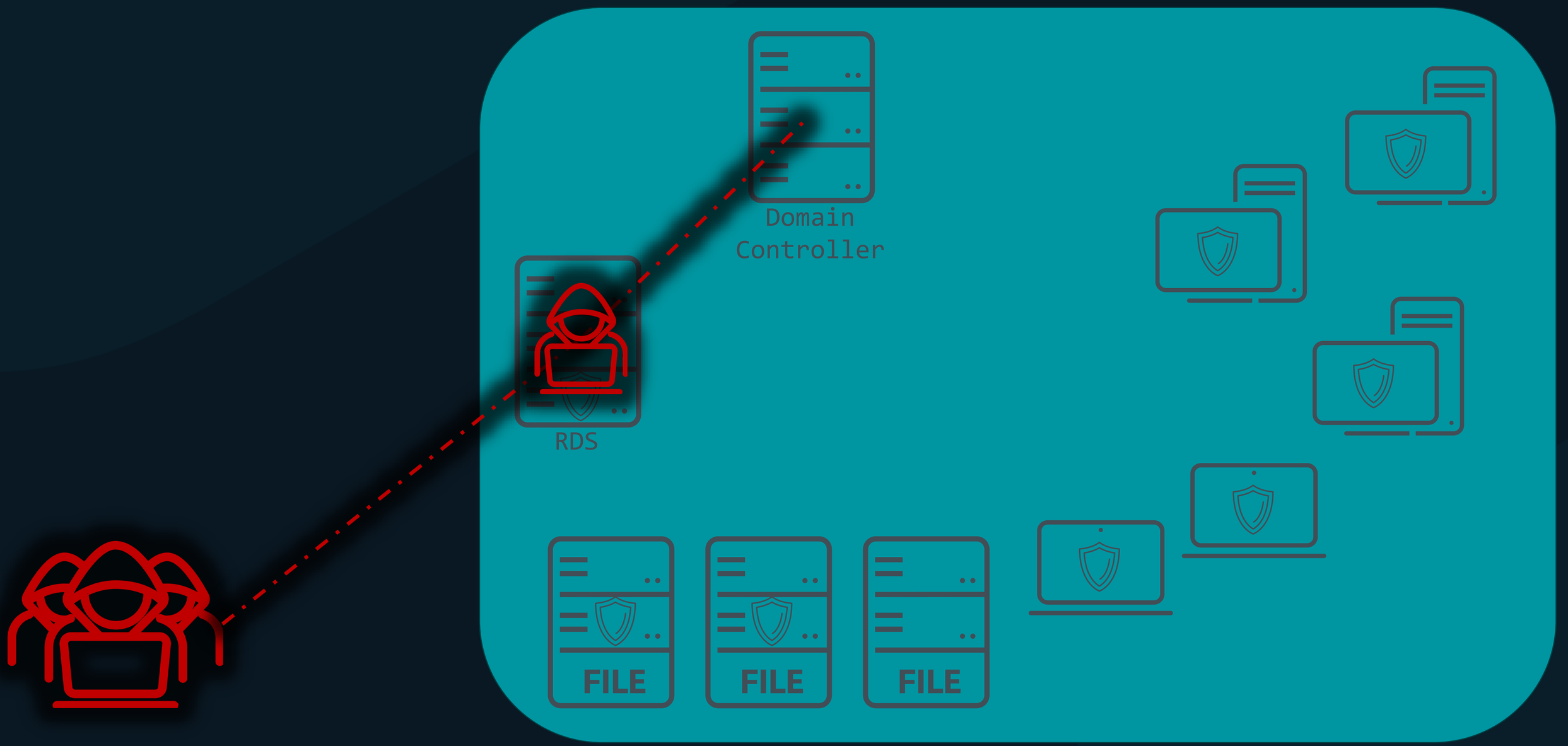
Jei visi jų įrankiai buvo blokuojami, kaip jiems pavyko apeiti ESET ir paleisti išpirkos reikalaujančią programą?

- Jiems nepavyko
- Jie atidarė PDF failą pavadinimu „Company Passwords.PDF“
- Pasirinko kitus įrenginius ir per RDP prisijungė prie neapsaugoto serverio
- Taip pat per RDP prisijungė prie 127.0.0.1

Kaip tai įvyko

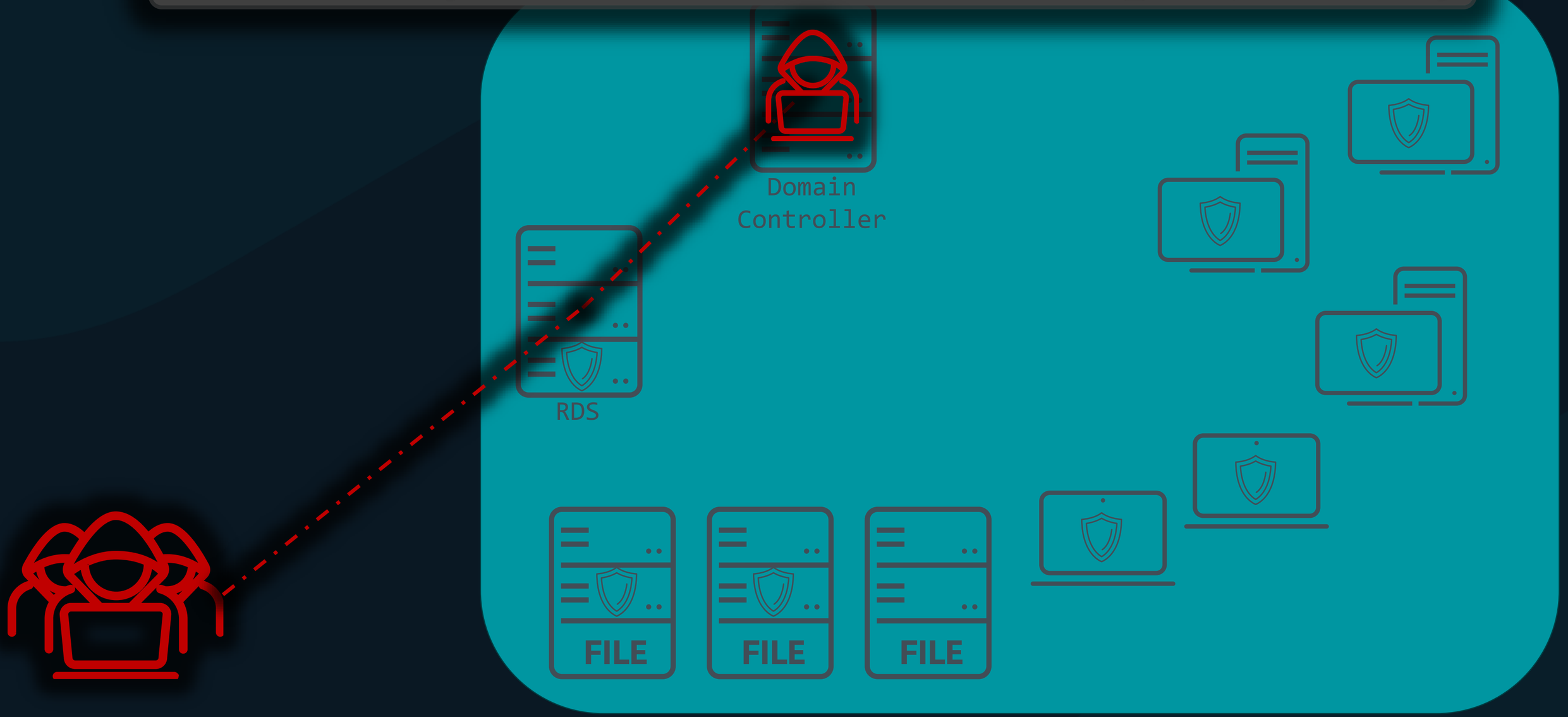


Kaip tai įvyko



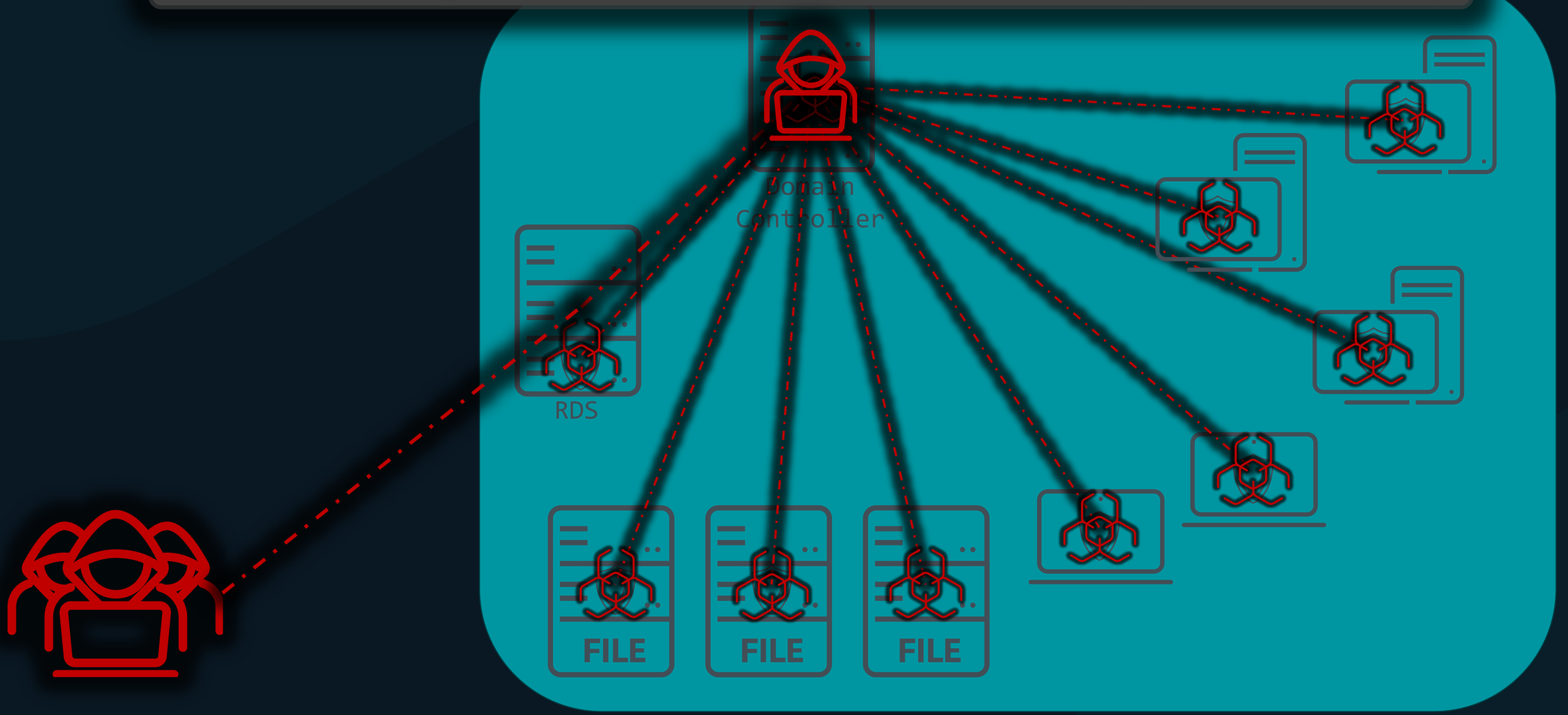
Kaip tai įvyko

```
WMI:> %WINDIR%\syswow64\rundll32.exe c:\windows\COMPANY_c.dll,VisibleEntry
```



Kaip tai įvyko

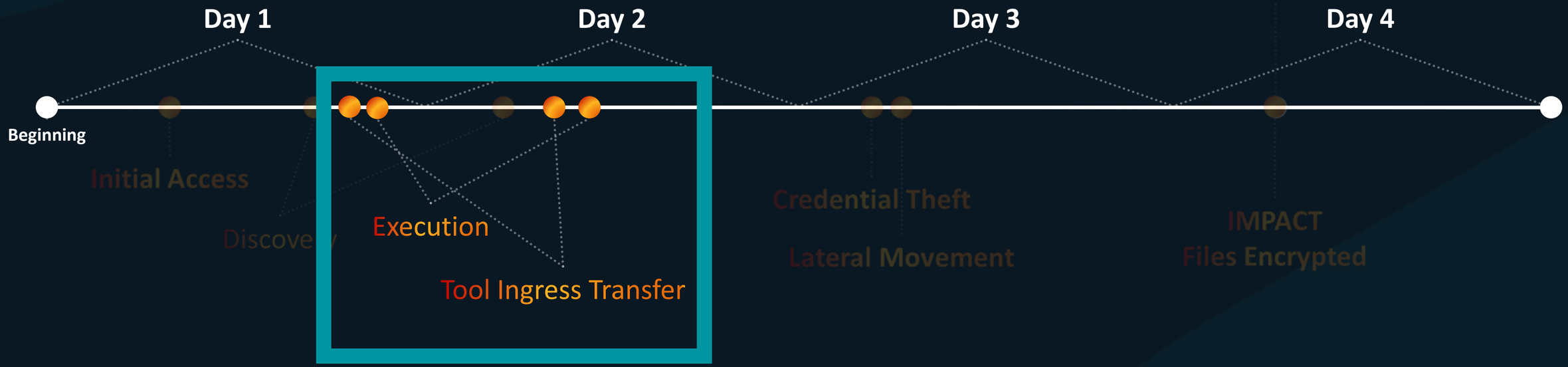
```
WMI:> %WINDIR%\syswow64\rundll32.exe c:\windows\COMPANY_c.dll,VisibleEntry
```



Doom įvykių seka

Everything is...

...ON FIRE!!!



Išmoktos pamokos

- 2FA/MFA būtų užblokavęs pradinę prieigą
- Numatytasis EDR/XDR taisyklių rinkinys ir antivirusinė apsauga yra pakankamai galingi, kad sustabdytų užpuoliką
- Jei sistemą stebėtų tikri ekspertai, ši ataka būtų sustabdyta jau pirmą dieną
- Užtikrinus, kad ESET būtų įdiegtas visuose įrenginiuose, būtų buvę lengviau užkirsti kelią incidentui

Išbandykite ESET XDR

Kreipkitės į Baltimax partnerį

TELECENTRAS

Cybersecurity
Progress. Protected.

Klausimai?

Cybersecurity
Progress. Protected.

lukas@baltimax.com
www.eset.lt