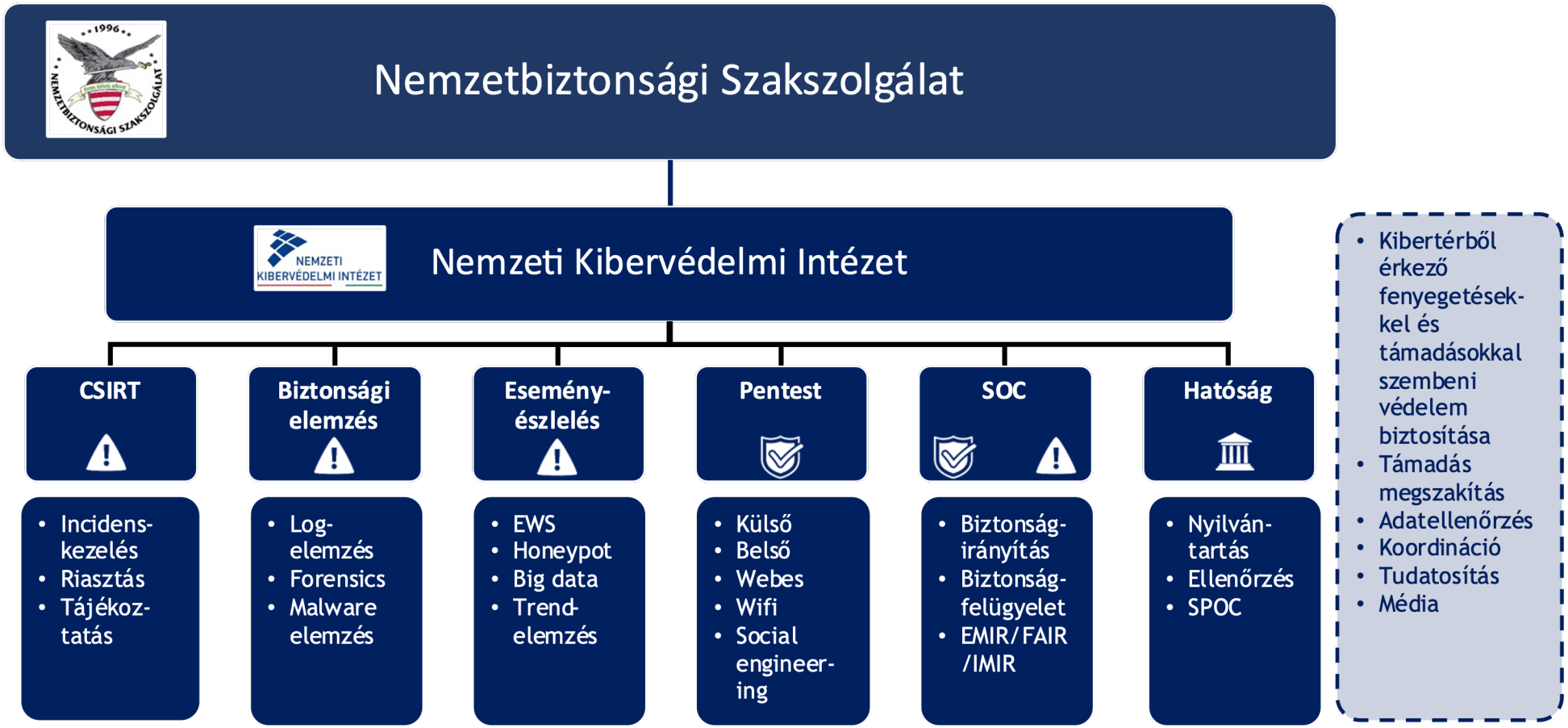
NEMZETI KIBERVÉDELMI INTÉZET

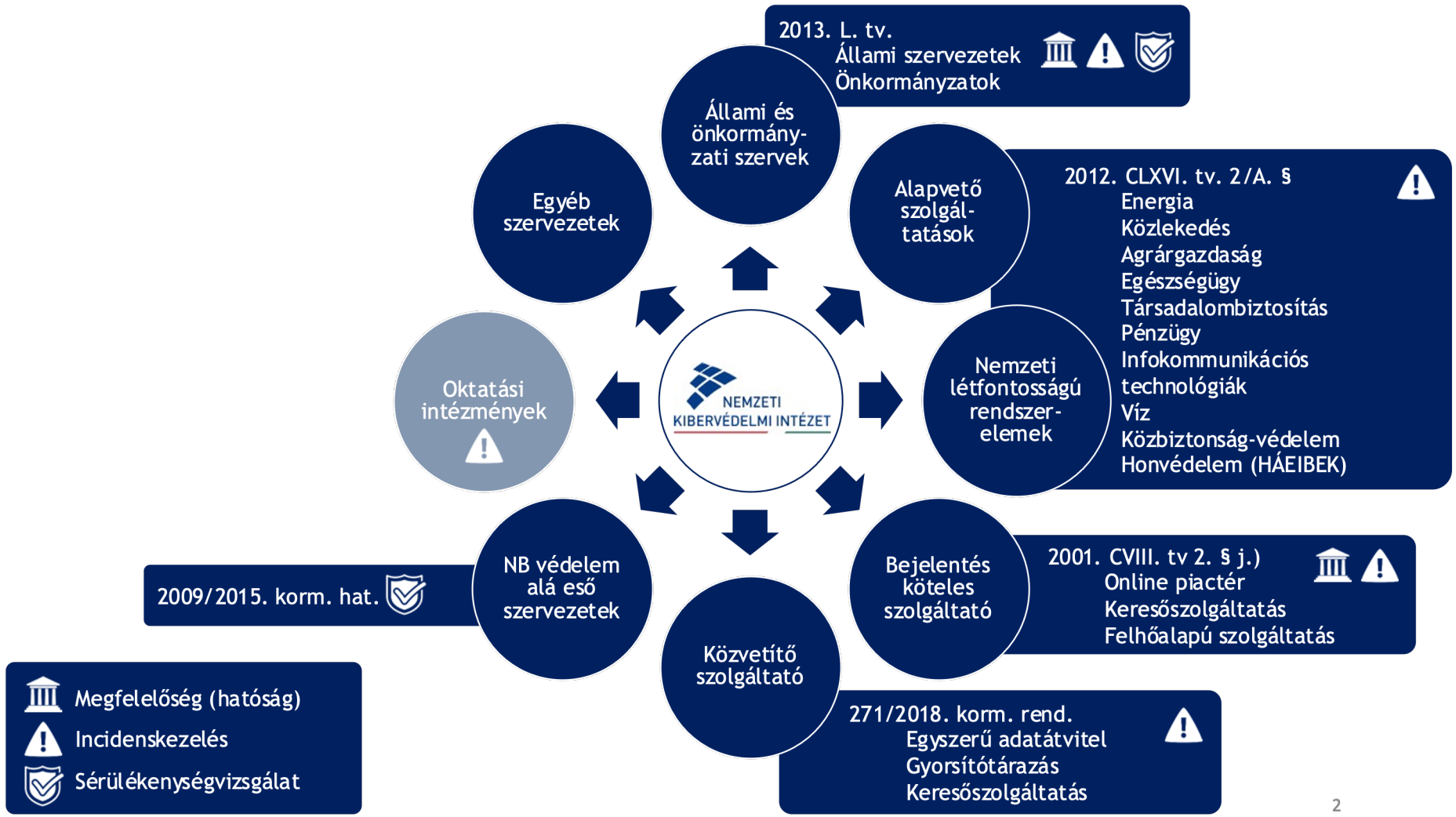
Hogyan jelentsünk be incidenst?

Marsi Tamás
EIVOK – 2022.

NKI felépítése



NKI ügyfélköre



Incidens keletkezése

1. Észlelés

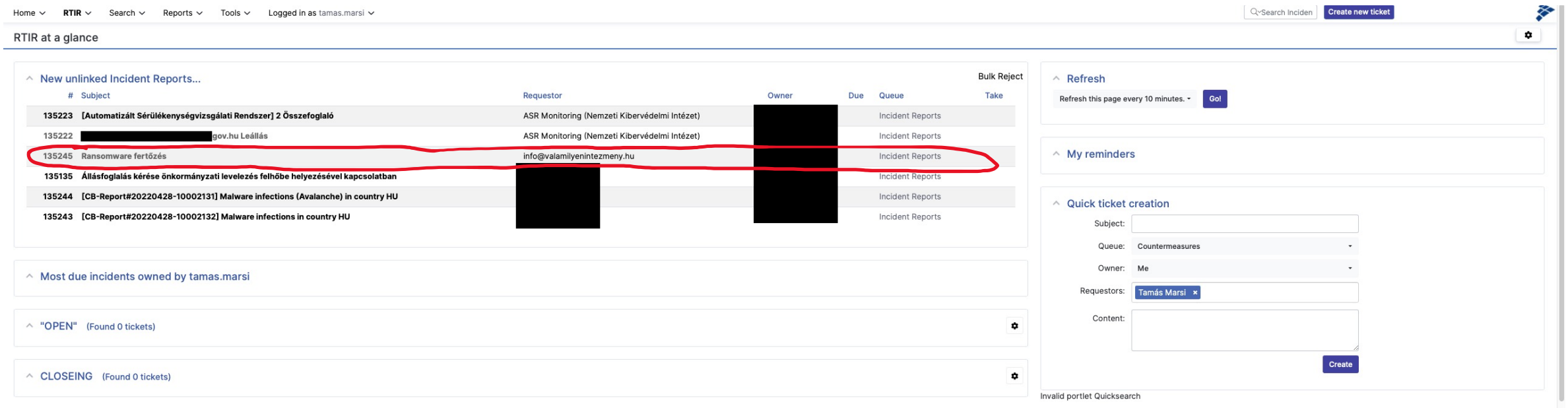
- EWS
- Honeypot
- ASR
- Biléta

2. Bejelentés

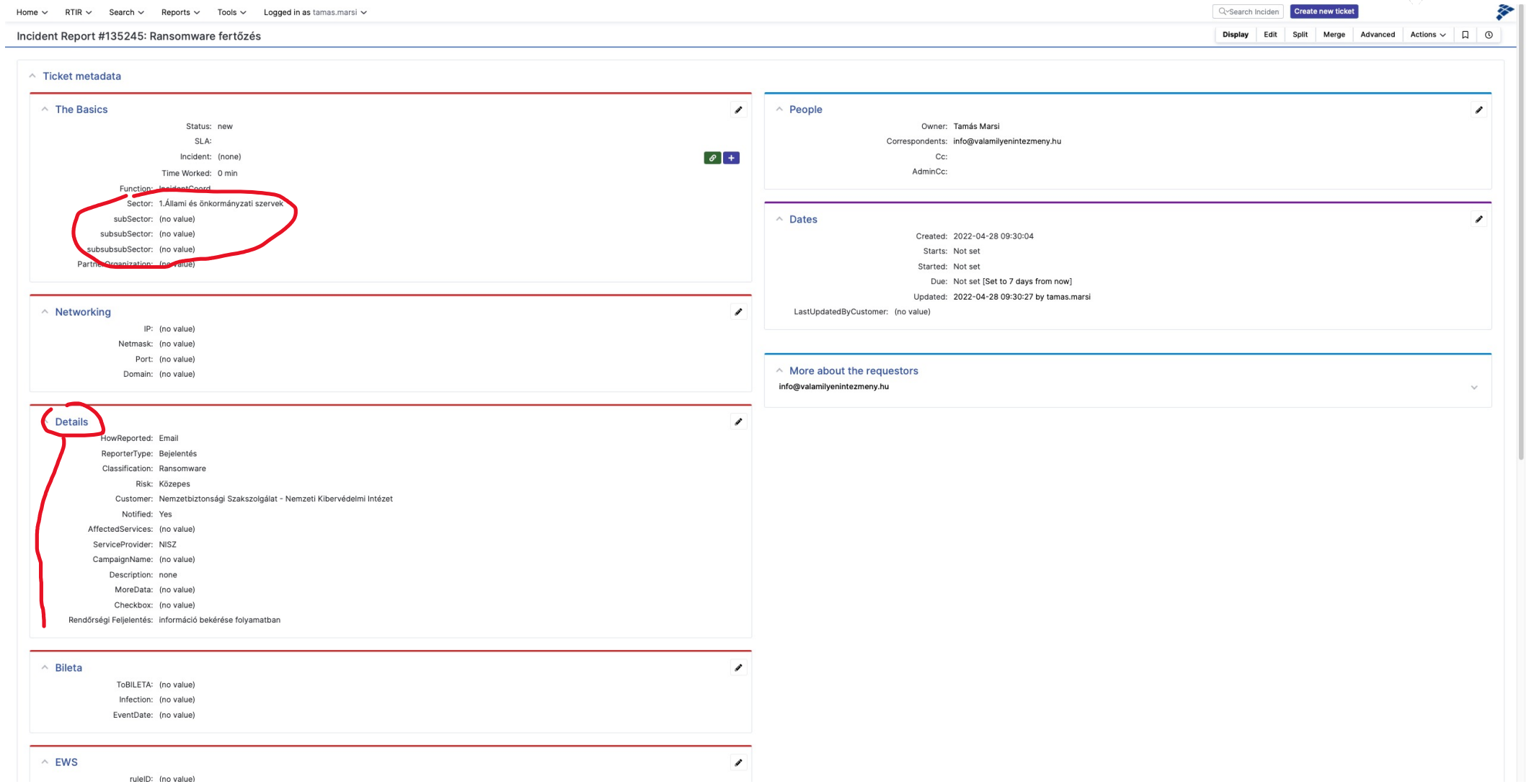
- 0-24 (készenlét)
- E-mail
- Weboldal
- Telefon

3. Jelzés

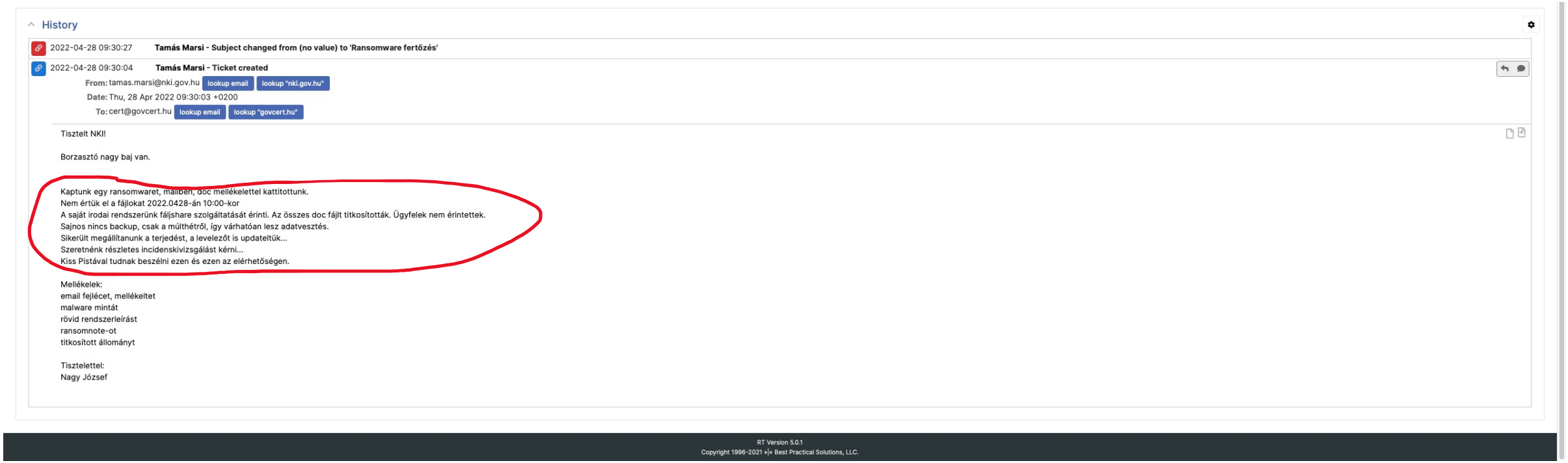
RTIR 1.


Home
RTIR
Search
Reports
Tools
Logged in as tamas.marsi
Search Inciden
Create new ticket
RTIR at a glance
New unlinked Incident Reports...
Bulk Reject
Subject Requestor Owner Due Queue Take
135223 [Automatizált Sérülékenységvizsgálati Rendszer] 2 Összefoglaló ASR Monitoring (Nemzeti Kibervédelmi Intézet) Incident Reports
135222 [redacted]gov.hu Leállás ASR Monitoring (Nemzeti Kibervédelmi Intézet) Incident Reports
135245 Ransomware fertőzés info@valamilyenintezmeny.hu Incident Reports
135135 Állásfoglalás kérése önkormányzati levelezés felhőbe helyezésével kapcsolatban Incident Reports
135244 [CB-Report#20220428-10002131] Malware infections (Avalanche) in country HU Incident Reports
135243 [CB-Report#20220428-10002132] Malware infections in country HU Incident Reports
Most due incidents owned by tamas.marsi
"OPEN" (Found 0 tickets)
CLOSEING (Found 0 tickets)
Refresh
Refresh this page every 10 minutes.
Go!
My reminders
Quick ticket creation
Subject:
Queue: Countermeasures
Owner: Me
Requestors: Tamás Marsi
Content:
Create
Invalid portlet Quicksearch

RTIR 2.


Home
RTIR
Search
Reports
Tools
Logged in as tamas.marsi
Search Inciden
Create new ticket
Incident Report #135245: Ransomware fertőzés
Display
Edit
Split
Merge
Advanced
Actions
Ticket metadata
The Basics
Status: new
SLA:
Incident: (none)
Time Worked: 0 min
Function: IncidentCoord
Sector: 1.Állami és önkormányzati szervek
subSector: (no value)
subsubSector: (no value)
subsubsubSector: (no value)
PartnerOrganization: (no value)
Networking
IP: (no value)
Netmask: (no value)
Port: (no value)
Domain: (no value)
Details
HowReported: Email
ReporterType: Bejelentés
Classification: Ransomware
Risk: Közepes
Customer: Nemzetbiztonsági Szakszolgálat - Nemzeti Kibervédelmi Intézet
Notified: Yes
AffectedServices: (no value)
ServiceProvider: NISZ
CampaignName: (no value)
Description: none
MoreData: (no value)
Checkbox: (no value)
Rendőrségi Feljelentés: információ bekérése folyamatban
Bileta
ToBILETA: (no value)
Infection: (no value)
EventDate: (no value)
EWS
ruleID: (no value)
People
Owner: Tamás Marsi
Correspondents: info@valamilyenintezmeny.hu
Cc:
AdminCc:
Dates
Created: 2022-04-28 09:30:04
Starts: Not set
Started: Not set
Due: Not set [Set to 7 days from now]
Updated: 2022-04-28 09:30:27 by tamas.marsi
LastUpdatedByCustomer: (no value)
More about the requestors
info@valamilyenintezmeny.hu

RTIR 3.



History

2022-04-28 09:30:27 **Tamás Marsi - Subject changed from (no value) to 'Ransomware fertőzés'**

2022-04-28 09:30:04 **Tamás Marsi - Ticket created**

From: tamas.marsi@nki.gov.hu lookup email lookup "nki.gov.hu"
Date: Thu, 28 Apr 2022 09:30:03 +0200
To: cert@govcert.hu lookup email lookup "govcert.hu"

Tisztelt NKI!

Borzasztó nagy baj van.

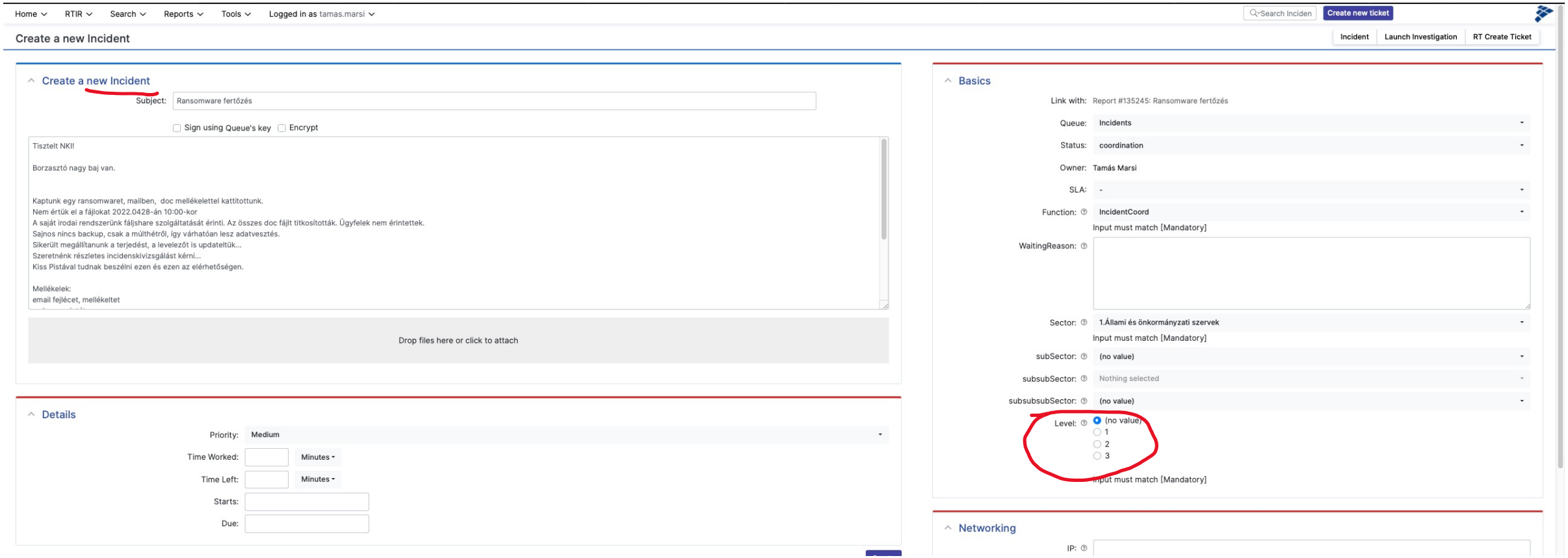
Kaptunk egy ransomwaret, mailben, doc mellékelettel kattitottunk.
Nem értük el a fájlokat 2022.0428-án 10:00-kor
A saját irodai rendszerünk fáljshare szolgáltatását érinti. Az összes doc fájlt titkosították. Ügyfelek nem érintettek.
Sajnos nincs backup, csak a múlthétről, így várhatóan lesz adatvesztés.
Sikerült megállítanunk a terjedést, a levelezőt is updateltük...
Szeretnénk részletes incidenskivizsgálást kérni...
Kiss Pistával tudnak beszélni ezen és ezen az elérhetőségen.

Mellékelek:
email fejlécet, mellékeltet
malware mintát
rövid rendszerleírást
ransomnote-ot
titkosított állományt

Tisztelettel:
Nagy József

RT Version 5.0.1
Copyright 1996-2021 »|« Best Practical Solutions, LLC.

RTIR 4.


Home
RTIR
Search
Reports
Tools
Logged in as tamas.marsi
Search Inciden
Create new ticket
Create a new Incident
Incident
Launch Investigation
RT Create Ticket
Create a new Incident
Subject:
Ransomware fertőzés
Sign using Queue's key
Encrypt
Tisztelt NKI!
Borzasztó nagy baj van.
Kaptunk egy ransomwaret, mailben, doc mellékelettel kattitottunk.
Nem értük el a fájlokat 2022.0428-án 10:00-kor
A saját irodai rendszerünk fáljshare szolgáltatását érinti. Az összes doc fájlt titkosították. Ügyfelek nem érintettek.
Sajnos nincs backup, csak a múlthétről, így várhatóan lesz adatvesztés.
Sikerült megállítanunk a terjedést, a levelezőt is updateltük...
Szeretnénk részletes incidenskivizsgálást kérni...
Kiss Pistával tudnak beszélni ezen és ezen az elérhetőségen.
Mellékelek:
email fejlécet, mellékeltet
Drop files here or click to attach
Details
Priority:
Medium
Time Worked:
Minutes
Time Left:
Minutes
Starts:
Due:
Basics
Link with:
Report #135245: Ransomware fertőzés
Queue:
Incidents
Status:
coordination
Owner:
Tamás Marsi
SLA:
-
Function:
IncidentCoord
Input must match [Mandatory]
WaitingReason:
Sector:
1.Állami és önkormányzati szervek
Input must match [Mandatory]
subSector:
(no value)
subsubSector:
Nothing selected
subsubsubSector:
(no value)
Level:
(no value)
1
2
3
Input must match [Mandatory]
Networking
IP:

RTIR 5.

Display | Edit | Split | Merge | Advanced | Actions

Ticket metadata

Incident #135246

Queue: Incidents
Status: coordination
SLA:
Owner: Tamás Marsi
Subject: Ransomware fertőzés
Priority: Medium
Time Worked: 0 min
Function: IncidentCoord
WaitingReason: (no value)
Sector: 1.Állami és önkormányzati szervek
subSector: (no value)
subsubSector: (no value)
subsubsubSector: (no value)
Level: 2

Networking

IP: (no value)
Port: (no value)
Netmask: (no value)
Domain: (no value)

Details

ReporterType: Bejelentés
Classification: Ransomware
Risk: Közepes
Customer: Nemzetbiztonsági Szakszolgálat - Nemzeti Kibervédelmi Intézet
Notified: Yes
AffectedServices: (no value)
ServiceProvider: NISZ
CampaignName: (no value)
Description: none
Resolution: (no value)
MoreData: (no value)
Checkbox: (no value)
Rendőrségi Feljelentés: információ bekérése folyamatban
Highlighted Incident: No

EWS

ruleID: (no value)

Dates

Incident Reports

135245	Ransomware fertőzés	open

(No inactive Incident Reports)

Investigations

(No active Investigations)
(No inactive Investigations)

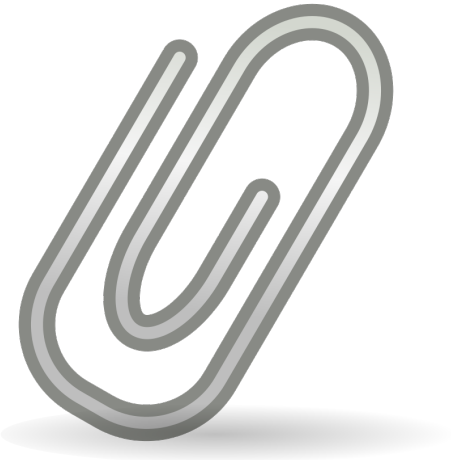
Countermeasures

(No active Countermeasures)
(No inactive Countermeasures)

Adatok

- Bejelentő személy, szervezet?
- Milyen típusú biztonsági incidens történt?
- Mit, hogyan és mikor észlelték ?
- Milyen és mekkora rendszereket, szervezeteket, ügyfélkört érint az incidens?
- Mekkora az incidens várható hatása? (Okoz-e szolgáltatás kiesést, okoz-e adatvesztést, szivárgást stb…)
- Milyen elhárító intézkedéseket tettek és milyen intézkedéseket terveznek?
- Milyen segítségre van szükségük?
- Ki az elhárításban kompetens személy?

Mellékletek

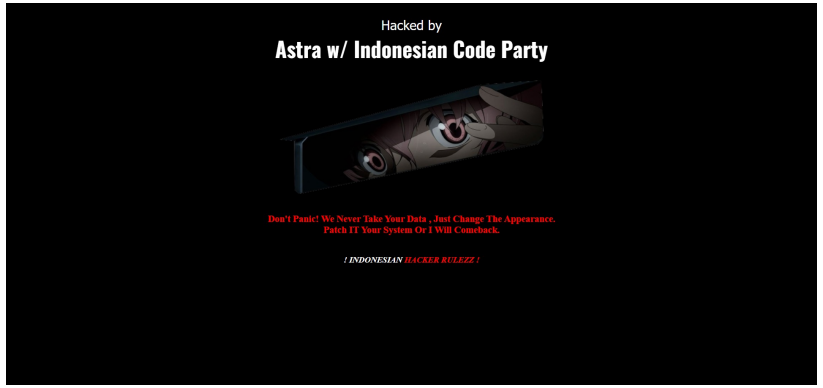


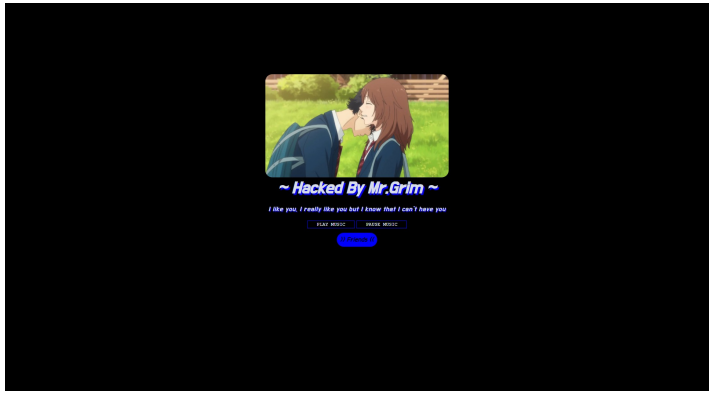
- Eseményleírás (riport), megtett intézkedésekkel
- E-mail (fejléccel, melléklettel)
- Káros kód, IoC forrása (belső IoC NEM)
- Külső forrásból származó IoC
- Rövid rendszerleírás
- Logadatok (tömörítve, értelmezve, timestamppel)
  - Tűzfal
  - IDS/IPS
  - Proxy
  - Alkalmazás
  - Endpoint

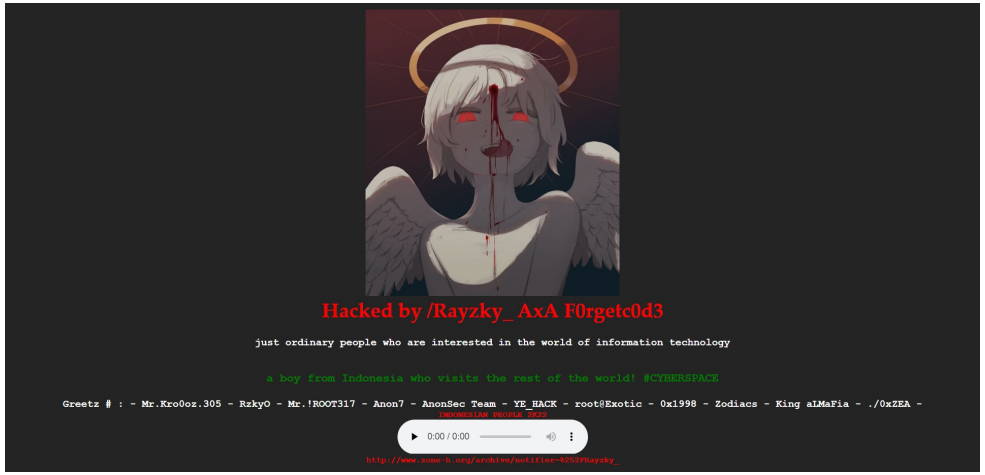
INCIDENSKEZELÉS FOLYAMATA

INCIDENSKEZELÉS FOLYAMATA

ESEMÉNY – INCIDENS?







INCIDENSKEZELÉS FOLYAMATA

ESEMÉNY – INCIDENS ?

Tisztelt Nemzeti Kibervédelmi Intézet!

Ezúton szeretném kérni, hogy történjen olyan vizsgálat, amely megvizsgálja a vakcinákat, oltott személyeket abból a szempontból, hogy tartalmaznak -e beléjük csempészett nanotechnológiai eszközöket!

https://www.bitchute.com/video/xlksP1zjNMoi/?fbclid=IwAR1SLE7Lrgb5njyDpvRoniVJDcwUu0vf8LCMvTo7cL0LNlkEw09nsQe9X4s lookup "www.bitchute.com"

A videóban említett törvények közül, melyeket országok hoznak távoli nem önkéntes elmeolvasás ellen, a Chile által hozott törvényt Kövér László is méltatta, említette a parlamentben októberben.
Azaz több ország törvényalkotói is érzékelték a veszélyt.

Szeretném kérni, hogy a vakcinák legyenek ellenőrizve, hogy vannak-e beléjük nanotechnológiai eszközök csempészve, mennyire valós veszély, tény a videóban elhangzottak.

Nemzetbiztonsági veszélynek tartom az emberiség benanózásának tervét, célját, az ilyen szándékokat. Szeretném kérni, hogy legyenek ellenőrizve ezek a vakcinák, oltott személyek is vizsgálhatók a videó szerint.

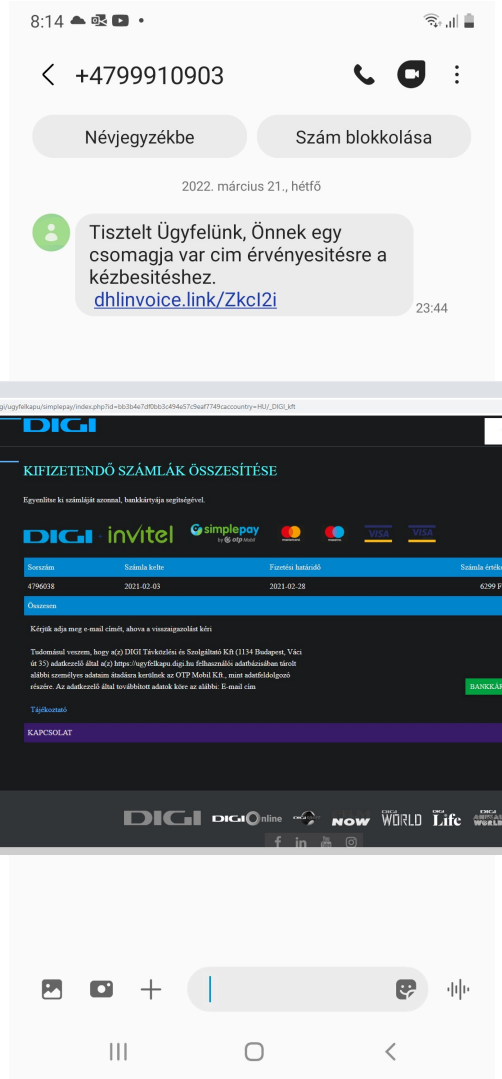
Tünde TI

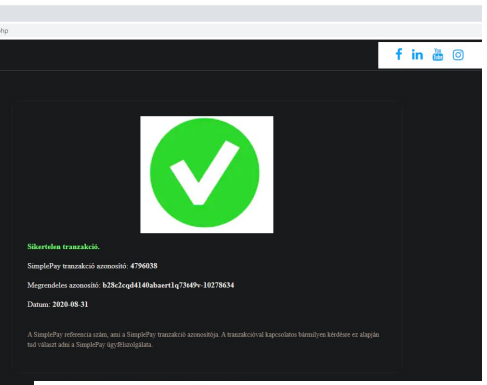
A TI közösségek (Targeted Individuals) jól ismerik hírlevelekből (pl. citizensaht.org lookup host hírlevelei) az emberiség benanózásának célját, melynek célja az egész emberiség benanózása, becsipelése, melynek végső célja az egész emberiség agyának olvasása és irányítása szimultán, azaz egyfajta teles kontrol, teljes leigázás.

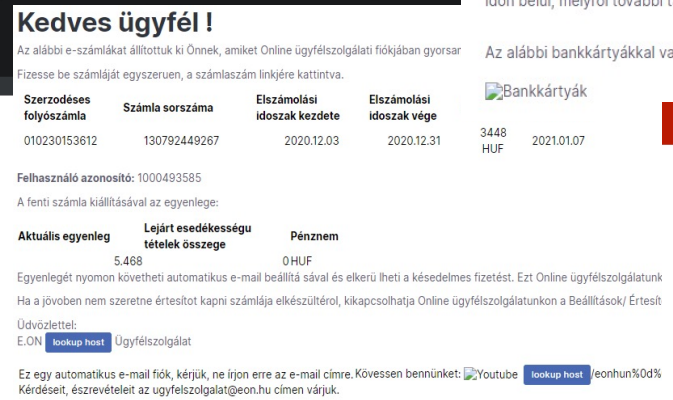
A benanózással növekszik a potenciális TI-k száma. Szélesebb értelemben véve mindenki TI (agyolvasás és kontroll alatt lévő, az alá kerülő személy).

INCIDENSKEZELÉS FOLYAMATA

ESEMÉNY – INCIDENS ?



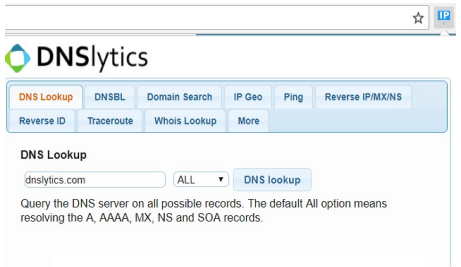


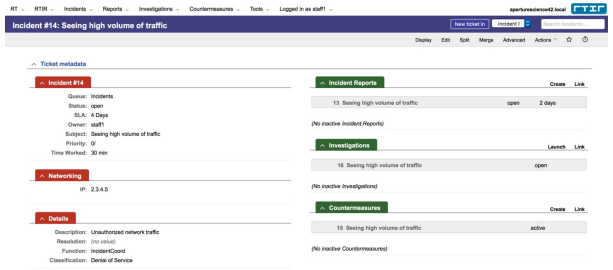


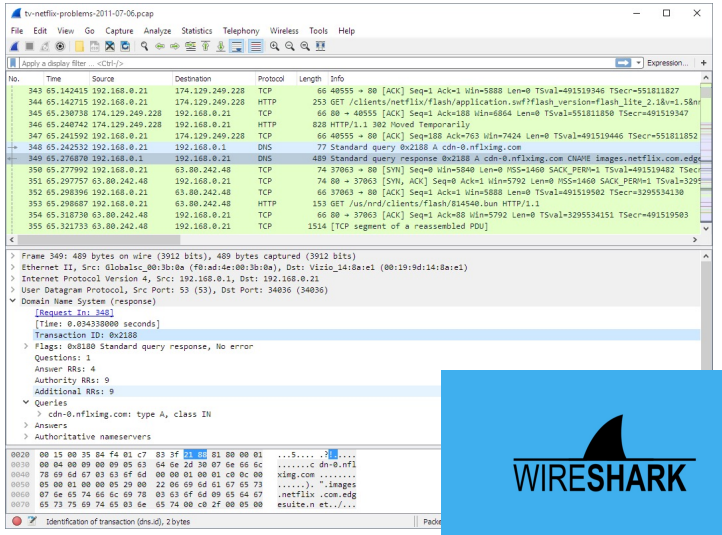
INCIDENSKEZELÉS FOLYAMATA

VIZSGÁLAT

RT | IR







WIRESHARK

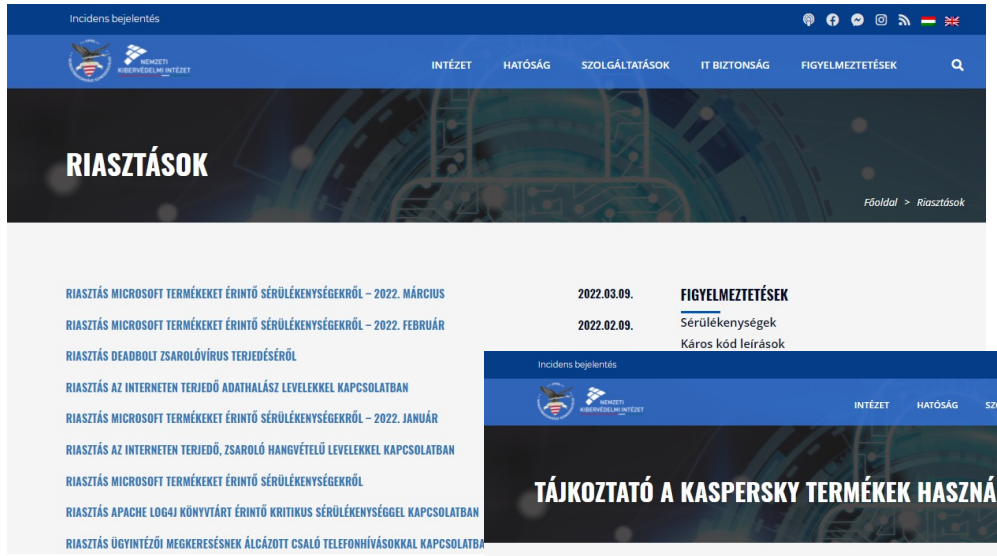
SHODAN

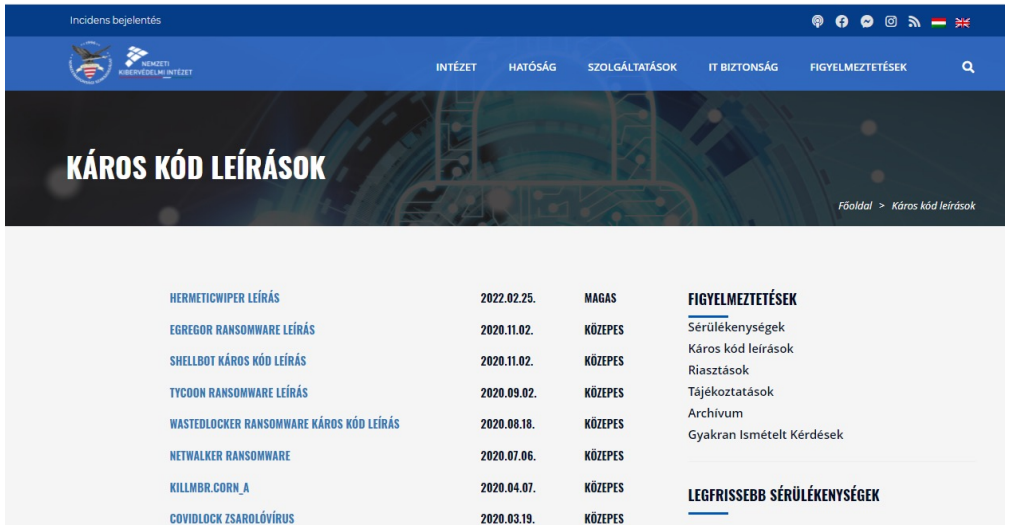
';--have i been pwned?

VIRUSTOTAL

INCIDENSKEZELÉS FOLYAMATA

FIGYELMEZTETÉSEK - TÁJÉKOZTATÓK – RIASZTÁSOK - ÁLLÁSFOGLALÁSOK





Köszönöm a figyelmet!

csirt@nki.gov.hu

Kibertámadás! Podcast

nki.gov.hu