



NEMZETI KIBERVÉDELMI INTÉZET



Hogyan jelentsünk be incidenst?

Marsi Tamás
EIVOK – 2022.



NKI felépítése



Nemzetbiztonsági Szakszolgálat



Nemzeti Kibervédelmi Intézet

CSIRT



- Incidens-kezelés
- Riasztás
- Tájékoztatás

Biztonsági elemzés



- Log-elemzés
- Forensics
- Malware elemzés

Esemény-észlelés



- EWS
- Honeypot
- Big data
- Trend-elemzés

Pentest



- Külső
- Belső
- Webes
- Wifi
- Social engineering

SOC



- Biztonság-irányítás
- Biztonság-felügyelet
- EMIR/ FAIR /IMIR

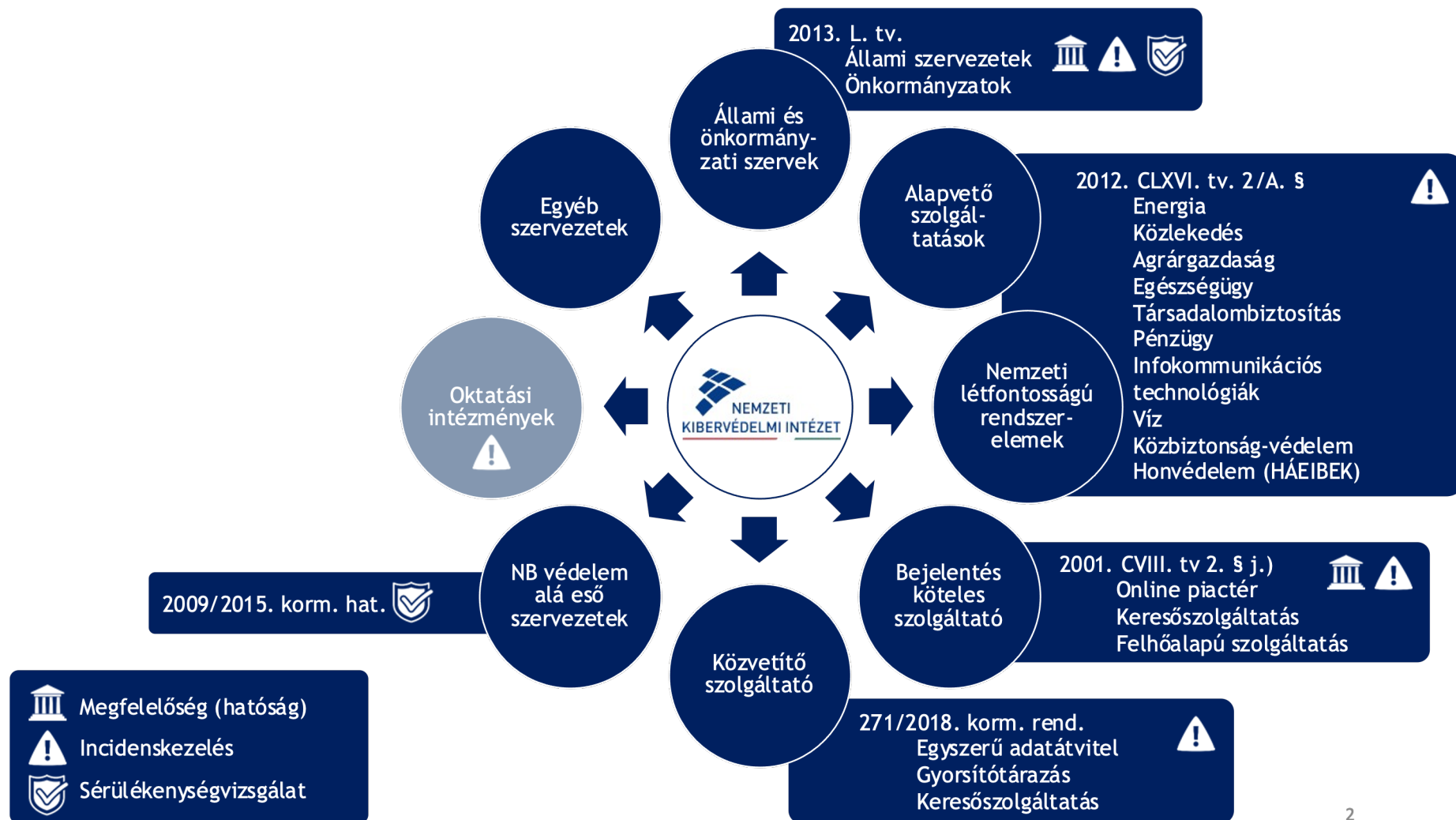
Hatóság



- Nyilvántartás
- Ellenőrzés
- SPOC

- Kibertérből érkező fenyegetésekkel és támadásokkal szembeni védelem biztosítása
- Támadás megszakítás
- Adatellenőrzés
- Koordináció
- Tudatosítás
- Média

NKI ügyfélköre





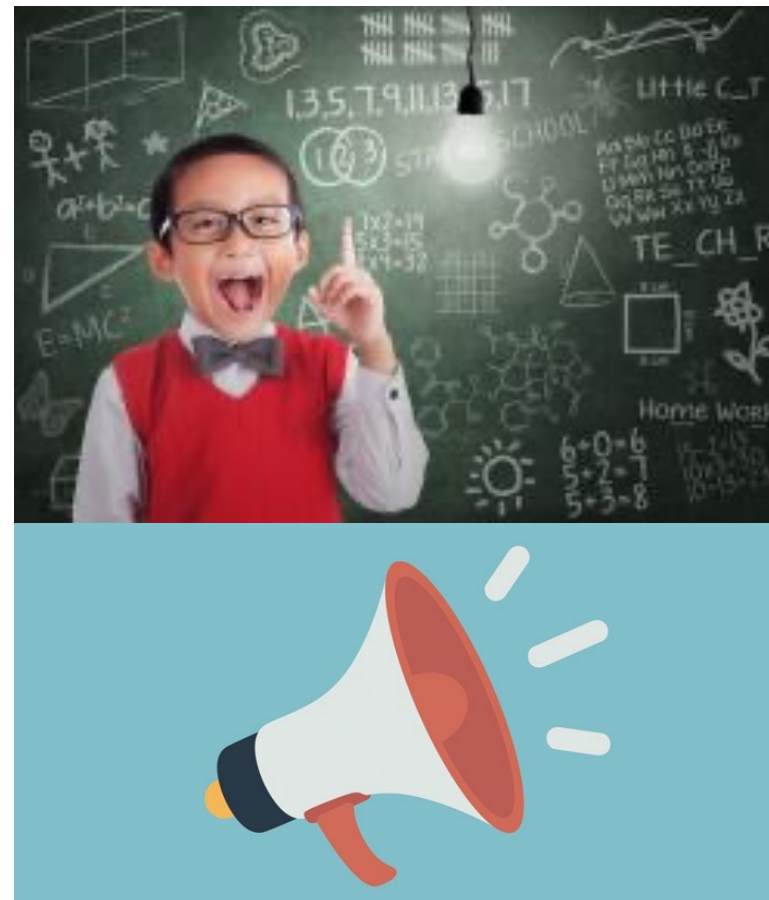
1. Észlelés

- 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](#) ▾

[Create new ticket](#)

RTIR at a glance

^ New unlinked Incident Reports...

#	Subject	Requestor	Owner	Due	Queue	Bulk Reject Take
135223	[Automatizált Sérülékenységvizsgálati Rendszer] 2 Összefoglaló	ASR Monitoring (Nemzeti Kibervédelmi Intézet)			Incident Reports	
135222	gov.hu Leállítás	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)

^ CLOSING (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 ▾

Q Search Incident 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)
Partner Organization: (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 Bejelentés: 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 ransomware-t, mámben, doc mellékelettel kattitottunk.

Nem értük el a fájlokat 2022.04.28-án 10:00-kor

A saját irodai rendszerünk fájlshare 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 fejléceket, mellékeltet

malware mintát

rövid rendszerleírást

ransomnote-ot

titkosított állományt

Tisztelettel:

Nagy József



RTIR 4.



Home ▾ RTIR ▾ Search ▾ Reports ▾ Tools ▾ Logged in as **tamas.marsi** ▾

Q-Search Incident Create new ticket

Incident Launch Investigation RT Create Ticket

Create a new Incident

^ Create a new Incident

Subject: Ransomware fertőzés

☐ Sign using Queue's key ☐ Encrypt

Tisztelt NKII!

Borzasztó nagy baj van.

Kaptunk egy ransomware-t, mailben, doc mellékelettel kattitottunk.
Nem értük el a fájlokat 2022.0428-án 10:00-kor
A saját irodai rendszerünk fájlshare szolgáltatását érinti. Az összes doc fájlt titkosították. Ügyfelek nem érintettek.
Sajnos nincs backup, csak a múltétéről, így várhatóan lesz adatvesztés.
Sikerült megállítanunk a terjedést, a levelezőt is updateltük...
Szeretnénk részletes incidenskövizsgálást 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

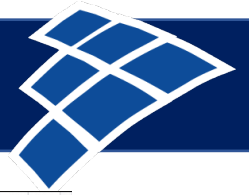
Input must match [Mandatory]

^ 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

^ Incident Reports

135245 Ransomware fertőzés

open

(No inactive Incident Reports)

^ Investigations

(No active Investigations)

(No inactive Investigations)

^ Countermeasures

(No active Countermeasures)

(No inactive Countermeasures)

^ Networking

IP: (no value)

Port: (no value)

Netmask: (no value)

Domain: (no value)

^ Detail

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



- 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?

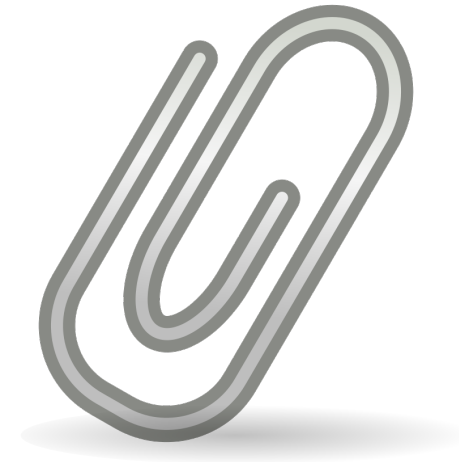




Mellékletek

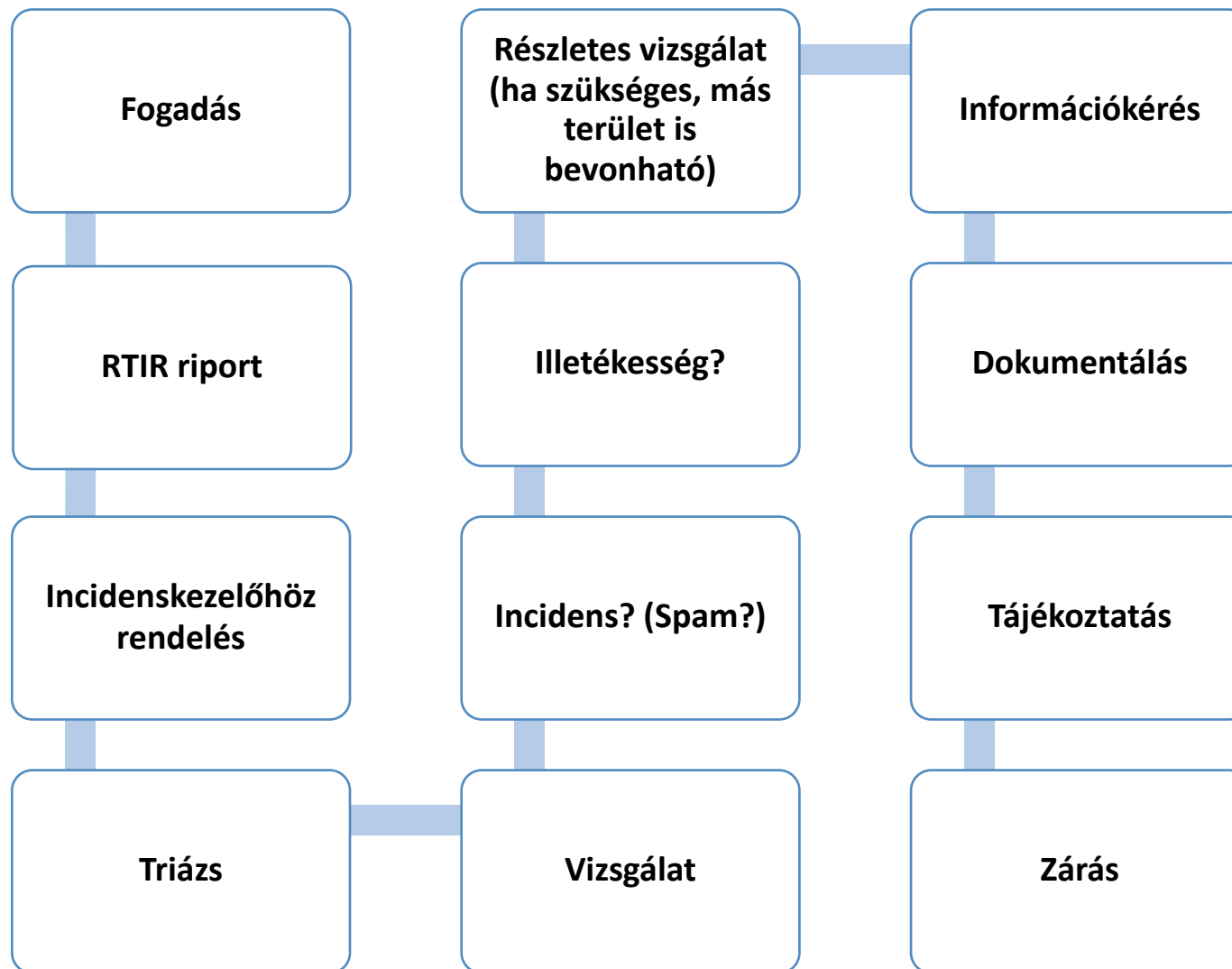


- Eseményleírás (riport), megtett intézkedésekkel
- E-mail (fejléccel, melléklettel)
- Káros kód, IoC forrása (belső IoC NEM)
- Külső forrásból származó IoC
- Rövid rendszerleírás
- Logadatok (tömörítve, értelmezve, timestamppeel)
 - Tűzfal
 - IDS/IPS
 - Proxy
 - Alkalmazás
 - Endpoint





INCIDENSKEZELÉS FOLYAMATA

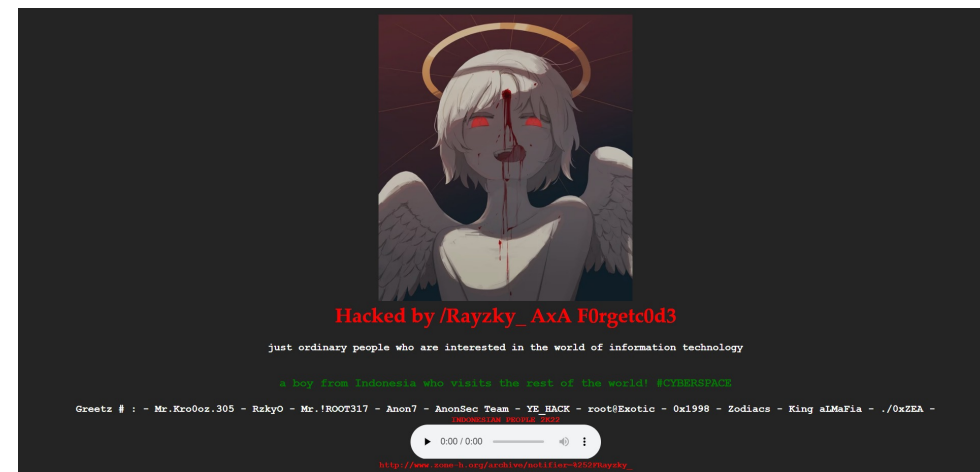
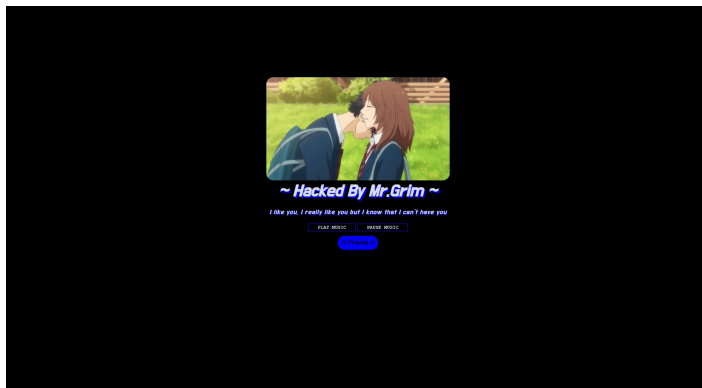




INCIDENSKEZELÉS FOLYAMATA



ESEMÉNY – INCIDENTS?





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 csempésztett nanotechnológiai eszközöket!

<https://www.bitchute.com/video/xlksP1zjNMoi/?fbclid=IwAR1SLE7Lrgb5njdPvRoniVJDcwUu0vf8LCMvTo7cL0LNikEw09nsQe9X4s> [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 benanóztatásának 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 benanóztatásának célját, melynek célja az egész emberiség benanóztatása, becsipelése, melynek végső célja az egész emberiség agyának olvasása és irányítása szimultán, azaz egyfajta teljes kontroll, teljes leigázás.

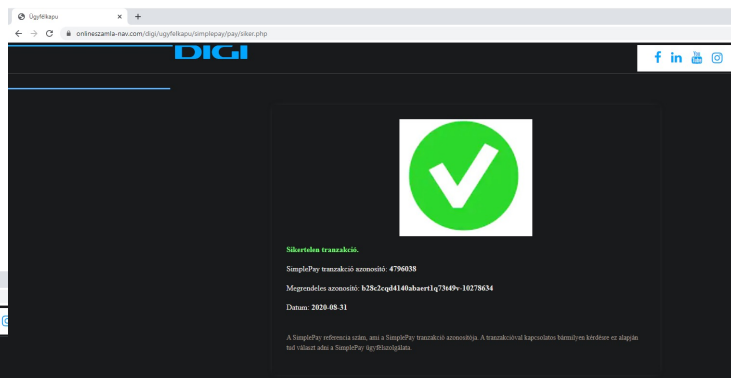
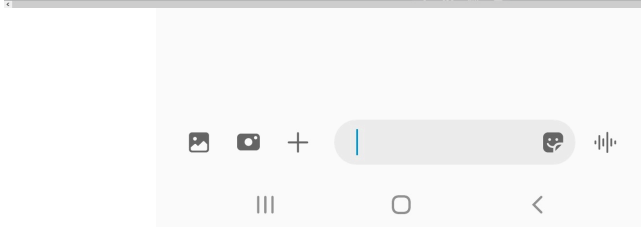
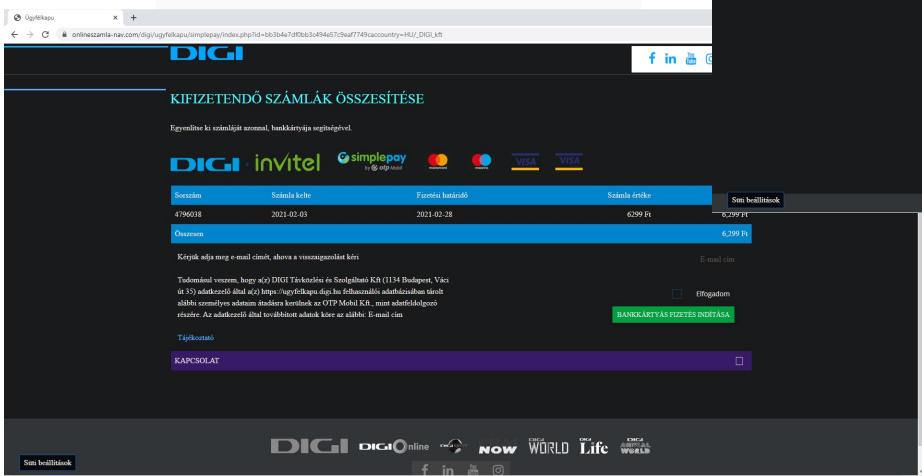
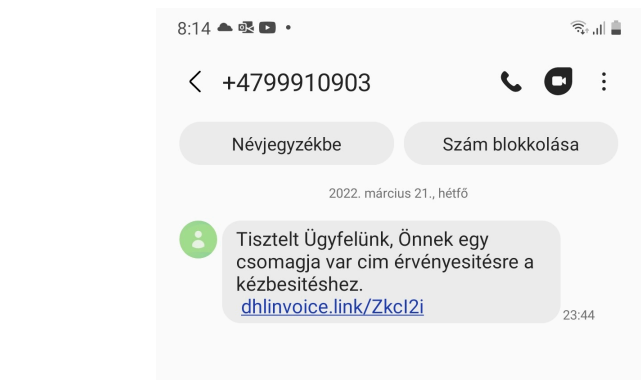
A benanóztatással növekszik a potenciális TI-k száma. Szélesebb értelemben véve mindenki TI (agyolvasás és kontroll alatt lévő, az alá kerülő személy).



INCIDENSKEZELÉS FOLYAMATA



ESEMÉNY – INCIDENS ?



Kedves ügyfél !

Az alábbi e-számlákat állítottuk ki Önnek, amiket Online ügyfélszolgálati fiókjában gyorsan Fizesse be számláját egyszerűen, a számlaszám linkjére kattintva.

Szerződéses folyószámla	Számla sorszáma	Elszámolási időszak kezdete	Elszámolási időszak vége
010230153612	130792449267	2020.12.03	2020.12.31

Felhasználó azonosító: 1000493585

A fenti számla kiállításával az egyenlege:

Aktuális egyenleg	Lejárt esedékességi tételek összege	Pénznem
5.468	0 HUF	

Egyenlegét nyomon követheti automatikus e-mail beállításával és elérheti a késedelmes fizetést. Ezt Online ügyfélszolgálatunk

Ha a jövőben nem szeretne értesítést kapni számlája elkészültéről, kikapcsolhatja Online ügyfélszolgálatunkon a Beállítások/Értesít

Üdvözléssel:

E.ON [lookup host](#) [Ügyfélszolgálat](#)

Ez egy automatikus e-mail fiók, kérjük, ne írjon erre az e-mail címre. Kövessen bennünket: [Youtube](#) [lookup host](#) [feonhun%0d%](#)

Kérdéseit, észrevételeit az ugyfelszolgalat@eon.hu címen várjuk.

Tisztelt **Ügyfelünk!**

Csomagküldemény

Értesítjük, hogy csomagküldeményt adtak fel Önnek.

Emlékeztetőül a Magyar Posta tájékoztatta, hogy az Ön szállítási száma: HU / 2938456 továbbra is várja az utasításait.

Erosítse meg a szállítási költség (805,28 HUF) kifizetését és a megrendelés szállítási címét az alábbi linkre kattintva:

kapja meg a Csomagomat

Házhoz szállítás* esetén a kézbesítő indulásáról vagy a küldemény átvételi pontra (Posta, MOL, Coop, Csomagautomata) történő érkezéséről újabb üzenetet küldünk Önnek.

*A házhoz szállítással kért küldeményeket két egymást követő munkanap kíséreljük meg kézbesíteni 8:00 és 17:00 óra között. Amennyiben sikertelen mindkét kézbesítés, ezt követően a postán veheti át a csomagot a feladó által megjelölt őrzési időn belül, melyről további tájékoztatást küldünk.

Az alábbi bankkártyákkal van lehetősége a szolgáltatás igénybevételére:



Csomag Z 257 2077 179

Csomag státusz: Kiadásra vár (-ig 2022-03-29)

Csomag száma

Feladó	csomagtika.hu https://www.csomagtika.hu/
Rendelési szám	83945-547262
Utánvétel	0.00 HUF
Átvevőhely/futár neve	Budapest 1033, Akác köz 5
Átvevőhely címe	Illa Akác Akác köz 5 Budapest
Nyitvatartás	H-P 06:30-19:00 Sz 07:00-13:00 2022.04.15 zárv 2022.04.18 zárv
Kártyás fizetés	Igen

Részletek

2022-03-18 14:17:31	Elektronikus adatok fogadása a csomaghoz. Várjuk az áru átadását a feladótól szállítóra.
2022-03-18 14:25:11	Csomag bevételezése az alábbi feladóhelyen: Budapest 1139, Petneházy utca 16-18. fsz.47.
2022-03-21 15:04:08	A csomag bevételezése az alábbi depóban: Budapest, Ezred utca 1-3 B/11
2022-03-22 13:11:08	A csomag átvételre kéri az átvételhez Budapest 1033, Akác köz 5

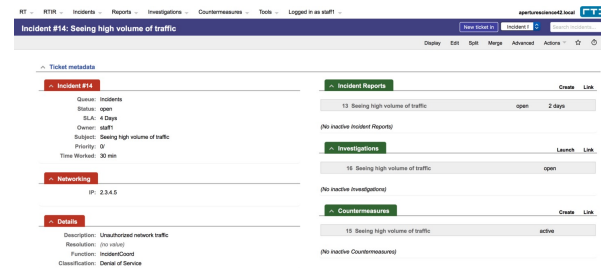
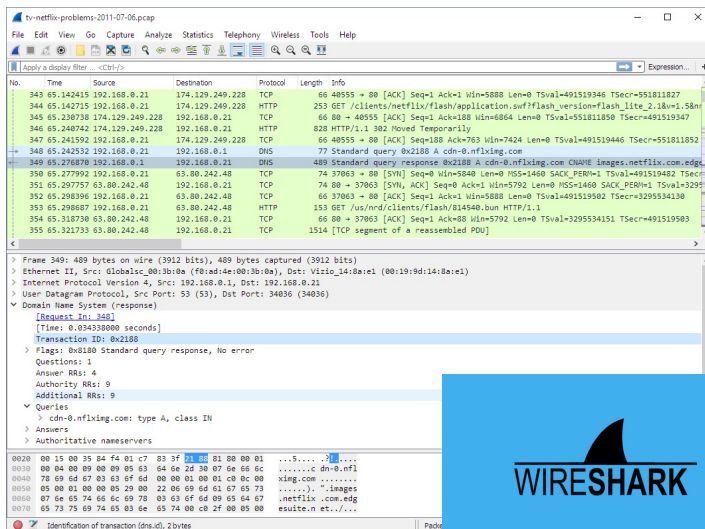
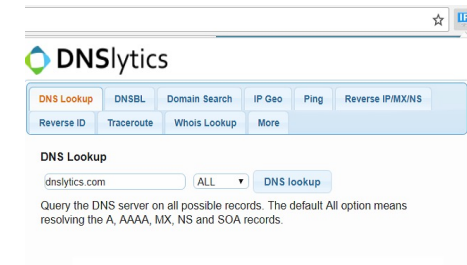


INCIDENSKEZELÉS FOLYAMATA



VIZSGÁLAT

» RT | I R «



'--have i been pwned?



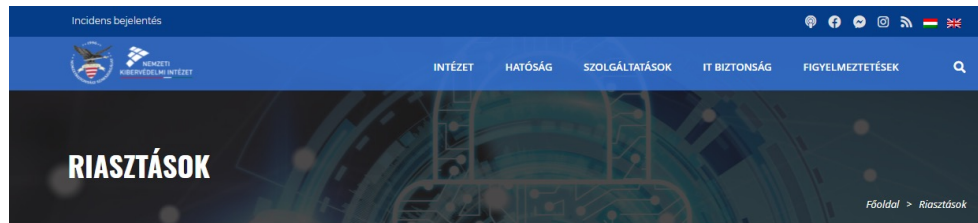
WIRESHARK



INCIDENSKEZELÉS FOLYAMATA

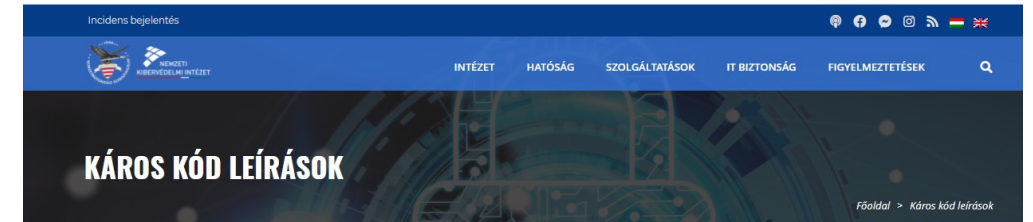


FIGYELMEZTETÉSEK - TÁJÉKOZTATÓK – RIASZTÁSOK - ÁLLÁSFOGLALÁSOK



RIASZTÁS MICROSOFT TERMÉKEKET ÉRINTŐ SÉRÜLÉKENYSÉGEKRŐL – 2022. MÁRCIUS
RIASZTÁS MICROSOFT TERMÉKEKET ÉRINTŐ SÉRÜLÉKENYSÉGEKRŐL – 2022. FEBRUÁR
RIASZTÁS DEADBOLT ZSAROLÓVÍRUS TERJEDÉSÉRŐL
RIASZTÁS AZ INTERNETEN TERJEDŐ ADATHALÁSZ LEVELEKKEL KAPCSOLATBAN
RIASZTÁS MICROSOFT TERMÉKEKET ÉRINTŐ SÉRÜLÉKENYSÉGEKRŐL – 2022. JANUÁR
RIASZTÁS AZ INTERNETEN TERJEDŐ, ZSAROLÓ HANGVÉTELŐ LEVELEKKEL KAPCSOLATBAN
RIASZTÁS MICROSOFT TERMÉKEKET ÉRINTŐ SÉRÜLÉKENYSÉGEKRŐL
RIASZTÁS APACHE LOG4J KÖNYVTÁR ÉRINTŐ KRITIKUS SÉRÜLÉKENYSÉGGEL KAPCSOLATBAN
RIASZTÁS ÜGYINTÉZŐI MEGKERESÉSNEK ÁLCÁZOTT CSALÓ TELEFONHÍVÁSOKKAL KAPCSOLATBAN

2022.03.09. FIGYELMEZTETÉSEK
2022.02.09. SÉRÜLÉKENYSÉGEK
Káros kód leírások



HERMETICWIPER LEÍRÁS	2022.02.25.	MAGAS	FIGYELMEZTETÉSEK
EGREGOR RANSOMWARE LEÍRÁS	2020.11.02.	KÖZEPES	Sérülékenységek
SHELLBOT KÁROS KÓD LEÍRÁS	2020.11.02.	KÖZEPES	Káros kód leírások
TYCOON RANSOMWARE LEÍRÁS	2020.09.02.	KÖZEPES	Riasztások
WASTEDLOCKER RANSOMWARE KÁROS KÓD LEÍRÁS	2020.08.18.	KÖZEPES	Tájékoztatások
NETWALKER RANSOMWARE	2020.07.06.	KÖZEPES	Archívum
KILLMBR.CORN_A	2020.04.07.	KÖZEPES	Gyakran Ismételt Kérdések
COVIDLOCK ZSAROLÓVÍRUS	2020.03.19.	KÖZEPES	LEGFRISSEBB SÉRÜLÉKENYSÉGEK



NEMZETI KIBERVÉDELMI INTÉZET



Köszönöm a figyelmet!

csirt@nki.gov.hu

Kibertámadás! Podcast

nki.gov.hu