digitaltech EDIH

A kiberbiztonság alapjai

Számítógép felhasználók számára

Dr. Koczka Ferenc, koczka.ferenc@inf.elte.hu

A DigitalTech EDIH 2.0 c. projekt megvalósulását a Közigazgatási és Területfejlesztési Minisztérium támogatta.

Co-funded by the European Union

Miről lesz szó?

- A nigériai csalás
- OSINT
- Bankszámlaszám változása
- Adásvétel az interneten
- Banki csalók
- Távmenedzsment
- Tanúsítványok
- A Darknet

- A támadók motivációi
- Becsapós levelek
- Facebook piactér
- Zsaroló levelek
- Zsarolóvírusok
- Valótlan ajánlat
- Adat megszerzése, kicsalása
- Hamis számla
- Kártékony programok
- Célzott támadások
- Egyéb

- Távozó dolgozók
- Adatok mentése
- Titkosított adattárolás
- Selejtezett eszközök törlése
- Redundáns eszközök
- Vírus- és kártevővédelem
- Tűzfalak
- IDS, IPS és SIEM



A nigériai királyi család

"A nigériai csalás az egyik legismertebb internetes bűncselekmény, amelyet 419-es átverésnek is neveznek (ez a száma a visszaéléseket büntető nigériai törvénykönyv vonatkozó paragrafusának). A nigériai csalás legkorábbi verzióját az 1830-as években regisztrálták."

- Az elektronikus korszak elején csaló faxokat küldtek.
- Ma számos más országban alkalmazzák, és e-mailben terjesztik.
- Könnyű felismerni: valószínűtlen történetek, nyelvi problémák, melyek a mesterséges intelligencia és a gépi fordítók következtében egyre kevésbé jellemzőek.
- Figyelembe veszik az aktuális politikai/gazdasági/vallási eseményeket: Covid19, természeti katasztrófák, felfedezések, halálesetek révén igyekeznek aktualitást adni.
- A levelek nagy százaléka csaló levél. Szűrni meglehetősen nehézkes.



!!444!!! Csatlakozz a Körhöz!

A fene se gondolta volna, hogy így néz ki egy, a vagyonától elzárt nigériai herceg!

Király András
BŰNÜGY · 2017 december 31., 12:17

Ha nem ez az első napja az interneten, akkor már biztosan hallott a nigériai levelekről, tán már kapott is párat. Ezek azok a levelek, amelyekben egy bizonyos nigériai herceg arra panaszkodik, hogy elzárták mesés vagyonától, de ha a levél címzettje átutal egy kisebb, vagy ha lehet, nagyobb összeget, akkor a herceg busásan megjutalmazza majd, amint hozzáfér végre a vagyonához.
Bár nyilvánvaló átverésről van szó, az emberben mégiscsak él egy kép az állítólagos hercegről. Nem tudom, hogy önökben milyen kép élt, az enyémben biztosan nem ilyen:

Michael Neu, a Louisianában elfogott nigériai csaló. Fotó: Slidell PD - public domain



Példák

Hon B Samte — 2020. September 17. 13:15
(No Subject)
To: undisclosed-recipients:;, Bcc: Ferenc Koczka
Details

A nevem Samte, kapcsolatba lépek Önnel, mert van valami nagyon komoly és fontos előny, amelyet szeretnék megosztani veletek, várom a válaszát. Barr. Samte/My name is Mr. Samte, I am contacting you because there is something very serious and important to benefit which i want to share with you, I am waiting for your reply. Barr. Samte

lizzy Raphael — 2019. July 10. 19:00
Üdvözlet Lizzy Raphael asszonynak
To: undisclosed-recipients:;, Bcc: Ferenc Koczka,
Reply-To: lizzyraphael6@gmail.com
Details

Üdvözlet Lizzy Raphael asszonynak

Az általam olvasott jó profiljaim alapján kapcsolatba lépek veled, és jó okok miatt keresek egy ingatlanot, amelyet megvásárolhatok az Ön országában, amikor meg akartam jönni
ország befektetési céllal, bár nem találkoztam veled korábban, de úgy vélem, hogy az embernek meg kell kockáztatnia, hogy néha sikerüljön az életben.

A nevem Lizzy Raphael asszony. A késő férjem a Szudán Szövetségi Kormányával folytatott nyersolajjal foglalkozik, és a Bentiu Oil zóna városában és a Felső-Fülöp-szigeteken egy személyes Olajvállalkozás van. Nílus városa. Amit fizikailag megtapasztaltam, nem szeretném újra megtapasztalni az életemben, mivel Salva Kiir úr újabb polgári etnikai háborúja okozott.
és a lázadó vezetője, Riek Machar, az Egyesült Nemzetek menedéktáborában voltam Csádban, hogy megmentsem az életemet és a kis lányom életét.

Bár nem tudom, hogyan fogod érezni a javaslatomat, de az igazság az, hogy a szomszédos országunkba csatoltam Csádba, ahol most menekültként élek.
Elmenekültem a kis lányommal, amikor a lázadók a házunkba buknak, és megölték a férjemet, mint az ország egyik nagy olajforgalmazóját, azóta azóta futok.

Elhagytam az országomat, és a szomszédos országunkba költöztem Csádba a kis tűzszünet miatt, amit az amerikai államtitkár, John Kerry és az Egyesült Nemzetek Etiópiában (Addisz-Abeba), az elnökünk közötti koordinált szembesült békemegbeszélési megállapodás miatt tettünk. Salva Kiir és a lázadó vezetője Riek Machar, hogy állítsa le ezt a háborút.

Azt szeretném kérni a bizalommal való partnerségedet, hogy a késő férjem által a Bankban letétbe helyezett 8 millió dollárt fektetnéd be, mert az életem már nem biztonságos az országunkban, hiszen a lázadók az ország minden olajipari vállalkozásának családjait keresik megölni, mondván, hogy ők azok, akik szárazak az országban.

A teljes alap 20% -át felajánlom a segítségedre, miközben partne
az Ön országában való befektetésért fogok együttműködni.
Ha megkapom a választ.

Azt várom, hogy meghallgassak téged, hogy részleteket adjak neke
Szeretettel

capitals info — 2020. September 1. 23:51
Gratulálok Győztes / Winner.!!!
To: undisclosed-recipients:;, Bcc: tom@ektf.hu
Details

Gratulálok Győztes / Winner.!!!

A te E-mail cím nemrég nyerte € 150,000.00 (százötven ezer euró) ban Uplift Nemzetközi Jótékonysági lottó programot. Hivatkozási száma: Sp / 229 / 0-01 / 07 / 5-02 / ES. Szerencsés No: 9/11/13/24/40.

További információ és támogatás érintkezés a lenti.

CAPITAL CLAIM AGENCY
Mr. John Carlos.
Email: infoassets@aol.com
Tel: +34-604-206-030 (Beszélj csak angol)

Vel az Ön teljes nevét, címét, életkor, foglalkozás, telefonszámok

Küldje el Válasz az e-mailre: infoassets@aol.com

Megjegyzés: Ez egy nemzetközi lottó programot. Ezt az üzenetet automatikusan fordította angolról magyarra.

Gratulálok!!!

Congratulations Winner. !!!

Your email address has just won € 150,000.00 (One Hundred and Fifty Thousand Euros) in the Uplift International Charity Lottery Program. Reference No: Sp / 229 / 0-01 / 07 / 5-02 / ES. Lucky No: 9/11/13/24/40.

For more information and claim procedure contact below.

CAPITAL CLAIM AGENCY
Mr. John Carlos.
Email: infoassets@aol.com
Tel: +34-604-206-030

Your full name, address, age, occupation, phone numbers

Submit Reply to Email: infoassets@aol.com

Congratulations!!!

George Luis — 2020. August 3. 14:31
Re: Nagyon Sürgős?
To: undisclosed-recipients:;,
Reply-To: lougeorge196@gmail.com

Dr. Monika Norbert — 2020. August 22. 0:18
Fizetési értesítő levél
To: undisclosed-recipients:;,
Reply-To: rconsultant81@gmail.com

Fizetési értesítő levél

Arra a levélre hivatkozom, amelyet a ház címére írtam, de nem hallottam rólad, és úgy döntöttem, hogy ismét e-mailen küldöm Önnek, hogy tájékoztassam Önöket, örömmel hirdetjük Önnek az Arcus Alapítvány jóléti támogatási rendszerének felhívását. Ez egy online nyereményjáték nemzetközi program, amelyet 2020 áprilisában tartanak az Amerikai Egyesült Államokban az Európai Unió Közszolgálati Szövetségével együttműködésben.

Az online e-mail fiókját az Arcus Alapítvány jóléti támogatási rendszere választotta ki $ 850,000,00 dolláros szerencsés nyertesnek. Az Ön pénzeszközeit vízum-betéti kártyába töltötték, amely segítségével bármilyen nehézség nélkül felveheti pénzét az ország bármely bankjáról.

További információ / pontosítás és vízumbetéti kártya átadása Önnek regisztrált expressz futárszolgálaton keresztül; kérjük, vegye fel a kapcsolatot a fizetési övezeti koordinátorunkkal a következő e-mail címen. E-mail kapcsolat: (peter.udoma012@gmail.com) Kapcsolattartó: Úr. Peter Domasky.

Üdvözlettel,
Dr. Monika Norbert

Mr. Maki — 2019. July 17. 16:44
.
To: undisclosed-recipients:;, Bcc: Ferenc Koczka,
Reply-To: mta816489@gmail.com
Details

--
Dear Friend.

My name is:Mr. Tangza Maki, a banker in one of the banks in my country Burkina Faso in African.I Hoped that you will not expose or betray this trust and confident that I am about to repose on you for the mutual benefit of our both families.I need your urgent assistance in transferring the sum into your account.The money has been dormant for years in our Bank here without anybody coming for it. I want to release the money to you as the nearest person to our deceased customer (the owner of the account) who died along with his supposed

ügyfelemmel, akinek a neve Dr. László, aki szívrohamban halt meg. 6800
not interested,i will be waiting for your reply immediately,

Antonette Gross
Antonette-től
To: antonettegross8@daum.net

Helló, szerettem.

Köszöntök titeket a mi Urunk Jézus Kris
veled. Mindazonáltal alázatosan kérem,
Antonette Gross asszony az Amerikai Eg
aki egyszer 2002-ben dolgozott a németo
meghalt, londoni nagykövetségen dolgoz

25 évig házasodtunk gyermek nélkül, mi
döntöttem, hogy nem vallok újból házass
férjem életben volt, letétbe helyezte a 10
amerikai dollár) összegét egy bankkal itt
őrizetében van. Az utóbbi időben az orvo
nem tartom a következő négy hónapot.

Miután ismertem az állapotomat, úgy dö
szervezetnek vagy a jó embernek adomá
módon.

Szeretném, ha ezt a pénzt használná temp
és más rászorulók számára. Vettem ezt a
ezt a pénzt. Továbbá, a férjem rokonai ne
problémát, és azt akarták, hogy halottak
gyermekünk. Ezek az emberek nem érde
hogy kapcsolatba lépek veled, és adomán
jótékonysági munkákhoz használd.

Amint megkapom a választ, az Egyesült
kapcsolatba lépek a Bankkal. Felhatalma
pénz jelenlegi kedvezményezettjét. Azt i

Bármilyen késedelem a válaszban, adhat
a célra. Kérem, győződjön meg róla, hog
említettem.

Köszönöm és megmaradt.

A húgod az Úrban

- ChatGPT: Write a letter in Hungarian on behalf of a woman in distress who has $100,000 and would like to find an investor in Hungary.
- Fordító példa

A támadók három fő célja



Személyes és bizalmas adatok ellopása



Valamilyen aktivitás elérése



A számítógép irányításának átvétele



A domain névről

A számítógépes kommunikáció IP címek alapján működik, de helyettük inkább neveket használunk.

- Példa egy IP címre: 212.92.23.213
- Egy teljes cím több részből áll, amelyeket ponttal választanak el egymástól.
- A tulajdonosaik az utolsó két tagból álló részt vásárolják meg és a regisztrációt évente meg is újítják.
- Magyarországon a www.domain.hu oldalon lehet ellenőrizni, egy név foglaltságát és a tulajdonosát (GDPR). D
- Egyéb domain nevek pl. a https://www.domain.com/ oldalon kérdezhetők le. D

- Egy domain és adatainak lekérdezése, megtévesztő domain regisztrálása: gyeqep.hu D

- A qov.hu és uni-esztehazy.hu története.
- freenom.com: ingyenes domain nevek regisztrálása.

www.	facebook.com
fileserver.iroda.	agrialanc.hu
www.	facebook.com
www.	ugyfelkapu.gov.hu
saját hatáskör	domain név
eon.pay.hungary.	chachais.com
www.	uni-esztehazy.hu
om.	qov.hu
www.	qyeqep.hu

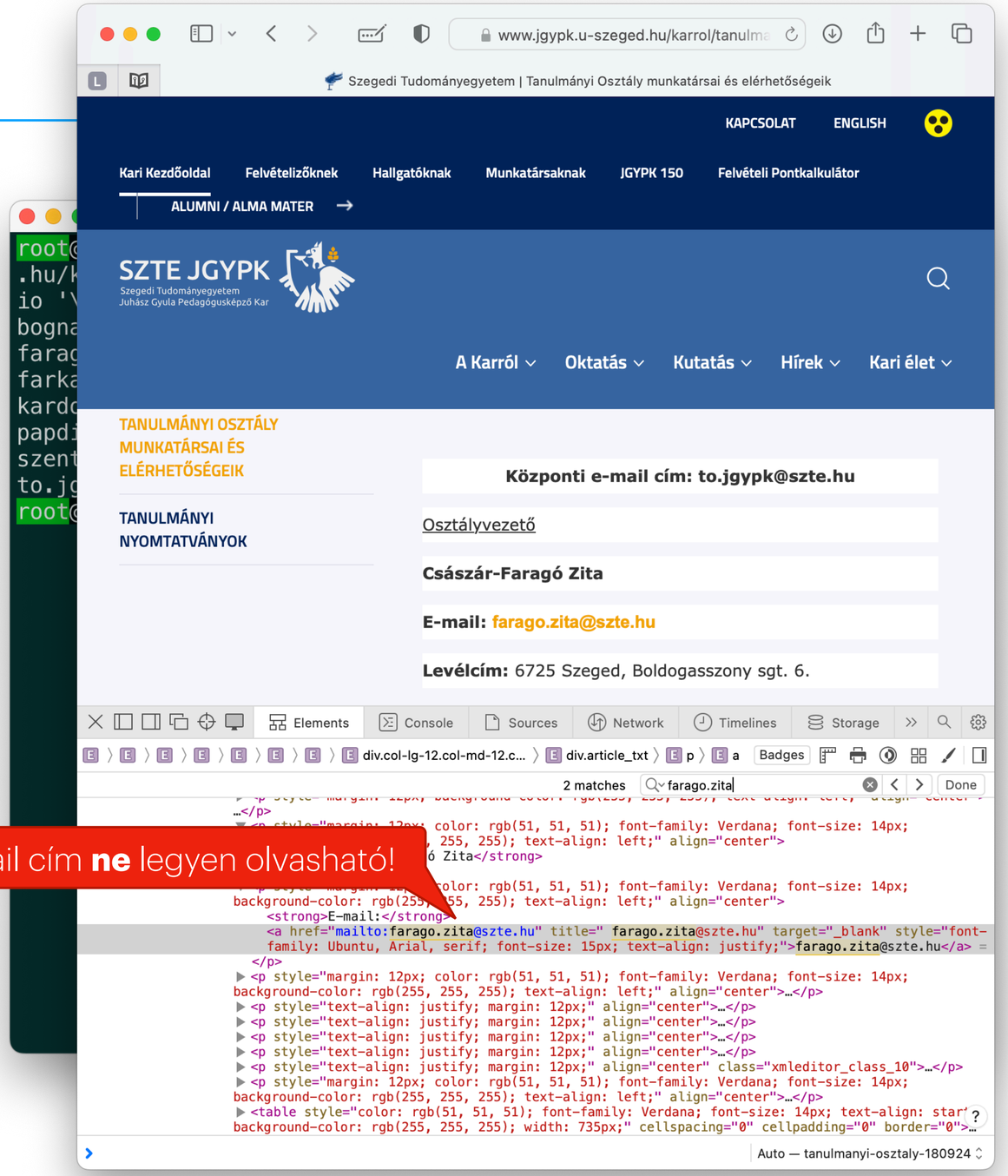
Phishing

Hogyan találnak meg minket?

- Az e-mail címeket különböző forrásokból gyűjtik, vagy komplett listákat vásárolnak meg.
- Ne szerepeljen az e-mail címünk nyilvános forrásban, mert onnan nagyon könnyű azokat összegyűjteni!
- Weboldalak forrásában ne szerepeljenek az e-mail címek!
- wget --quiet 'http://www.jgypk.u-szeged.hu/karrol/tanulmanyi-osztaly/tanulmanyi-osztaly-180924' -O - | grep -EiEio '\b[A-Z0-9._%+-]+@[A-Z0-9.-]+\.[A-Z]{2,4}\b' | sort | uniq

D

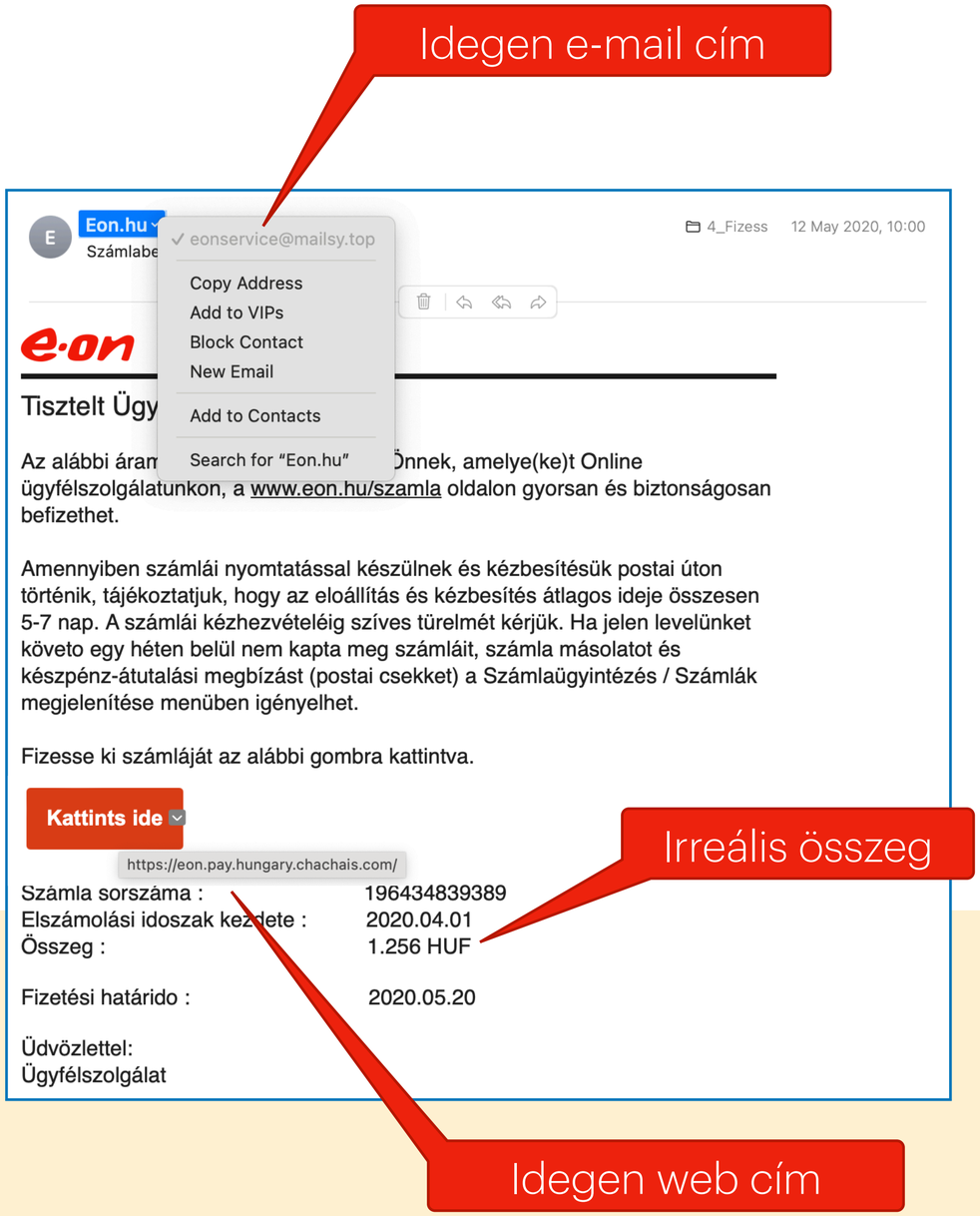
- Ne használjuk a céges e-mail címet magáncélra és fordítva!
- Ne használjunk személyes címeket, inkább pozícióra utalókat! A sales@, meo@ típusú címek megkönnyítik a a személycseréket + GDPR megfelelőség!



Hamis számlák

Tipikus csalási forma a hamis számlák küldése, amelyet a figyelmetlen felhasználó esetleg kifizet.

- Sokkal könnyebb megtéveszteni azokat, akik ügymenetében valóban megjelennek ilyen számlák.
- Gyakran rövid határidő áll rendelkezésre.
- Ismeretlen, a feladóhoz nem köthető e-mail cím.
- Az összeg eltér a szokásos számla összegtől.
- Az oldalon belül elhelyezett link a szolgáltatóhoz nem köthető oldalra mutat:



eon.pay.hungary.chachais.com

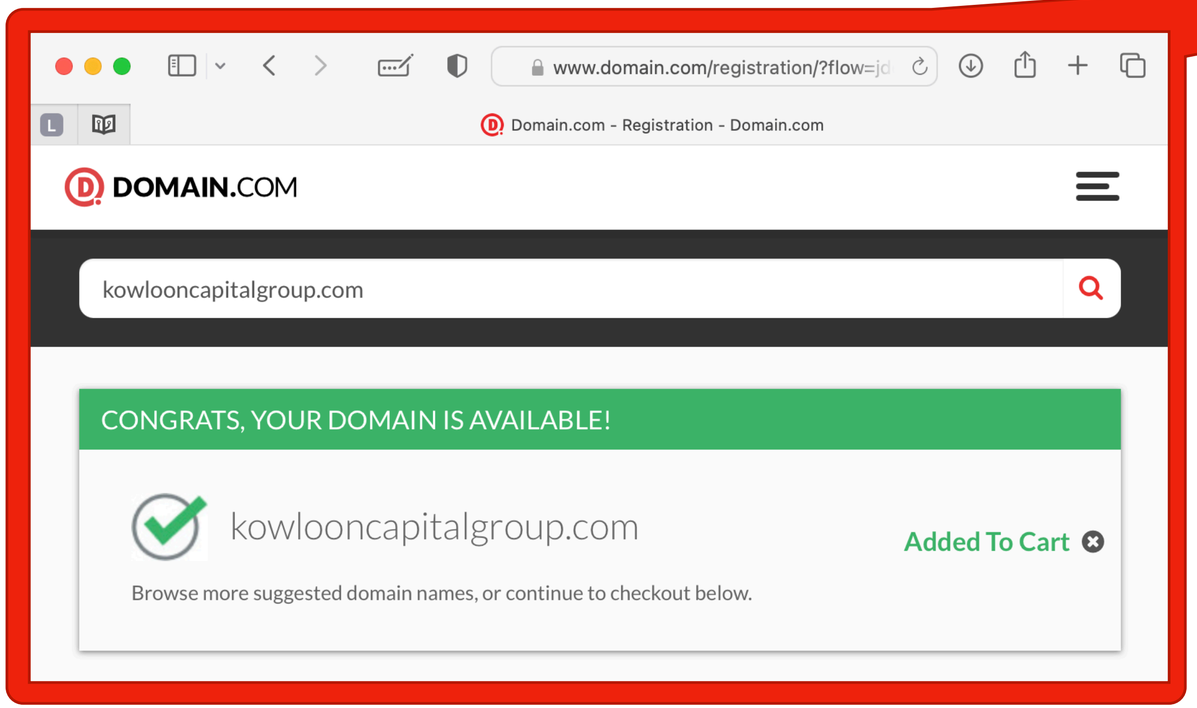
- **Az EON nemigen rendelkezik .com-os címmel.**
- **A chachais.com nemigen lehet az EON domainje.**

A domaint megelőző rész megtévesztési céllal tartalmazza az EON-ra és a fizetésre utaló szavakat, ezt a csaló adja meg!

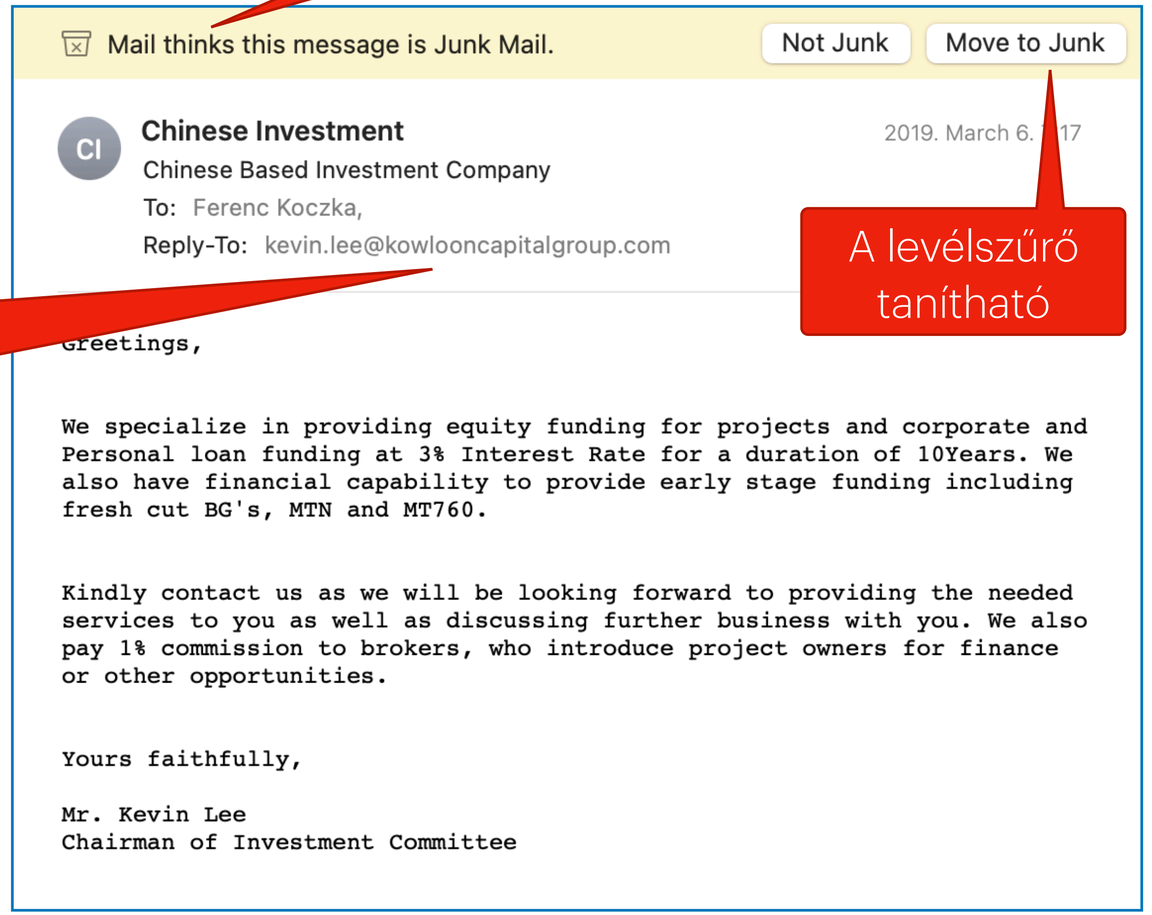
Phishing

Hogyan védekezzünk?

- A levelező programok jelezhetik, ha egy levél problémás.
- Ellenőrizhetjük a küldő domain nevét.
- Gondolkodjunk józan ésszel! Sajnos mindenkinél máshol szólal meg a vészcsengő, nincsenek szerencsék, csodák.



Figyelmeztetés kéretlen tartalomra

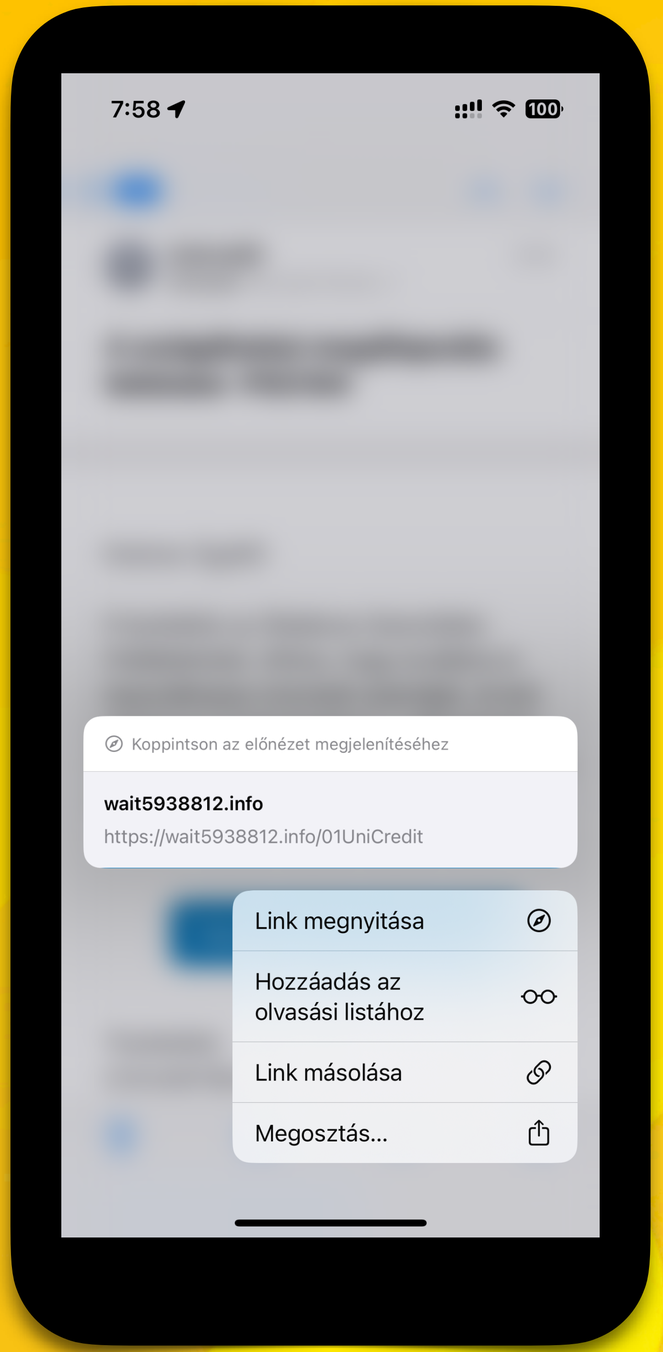


A levélszűrő tanítható

Phishing

Hogyan védekezzünk?





Co-funded by the European Union

További példák

EU Business Register
EU Business Register 2019/2020
To: Ferenc Koczka,
Reply-To: EU Business Register

4_Fizess 28 September 2019, 02:50

Hello,

In order to have your company inserted in the EU Business Register for 2019/2020, please print, complete and submit the attached form (PDF file) to the following address:

EU BUSINESS REGISTER
P.O. BOX 34
3700 AA ZEIST
THE NETHERLANDS

Fax: +31 205 248 107

You can also scan the completed form and attach it in a reply to this email.

Updating is free of charge.



Company Data Control

EU BUSINESS REGISTER

Dear Company,

We are compiling information for the EU BUSINESS REGISTER. We wish to be able to inform other EU companies about **your activities.** In order to list your company on the Internet for EU Businesses, just fill in and return the form. Any additional material of **your company** that can make your profile up to date is very welcome.

We thank you for your cooperation.

To update your company profile, please print, complete and return this form. ***(Updating is free of charge)*** Only sign if you want to place an insertion.

Please fill in the form completely, and return it to:
Eu Business Register
P.O.BOX 34
3700 AA - ZEIST
THE NETHERLANDS

Industry in which your company is working
Specify branch

A Division A: Agricultural
Specify branch

B Division B: Mining
Specify branch

Division C: Construction

Please fill in your company details:

Company name

This register are not related to any organization or institution of the European Union or Commission.



Magyar Posta

Kedves ügyfél,

Csomagja a szállításra vár. Kérjük, erősítse meg a fizetést (299,99 Ft) az alábbi linken, az online hitelesítést a következő 14 napon belül kell elvégezni:

Kattints ide
https://japonspostes.blogspot.com/?m=0

Segítség

Telenor.hu
Notification : Your electronic invoice is ready to pay
To: Ferenc Koczka

4_Fizess 11 January 2019, 20:39

Kedves info !

Tájékoztatjuk, hogy elektronikus számlája elkészült és megtekintheto.

Kérjük, látogasson el a MyTelenor oldalára!

Számla adatai:	
Telenor azonosító:	7037025446
Számlázási azonosító:	33238100
Számlaszám:	100189089742
Összeg:	**4 536 Ft**
Fizetési határido:	**2018.01.13**
Számla típusa:	havi számla

Fizesse ki egyszeruen és kényelmesen a számláját az interneten keresztül:
Számla befizetése

Ez a levél kizárólag értesítésként szolgál, kérjük, ne válaszoljon rá.

Reference to the Microsoft Edinburgh 2019 Product Award held on 28th January 2019 were your E-mail address emerged among one of the winners in the 3rd Category, please find attached details of your award and respond soonest for the processing of your claims.

Derrick McCourt.
Regional Director,
Microsoft Edinburgh, Scotland & Wales at Microsoft UK.



Microsoft

MICROSOFT CORPORATION
Customer Service
Edinburgh Regional Office
Waverley Gate 2-4 Waterloo Place
Edinburgh EH1 3EG United Kingdom.

RE: PRODUCT AWARD NOTIFICATION.

We are aware that this notification will come to you as a surprise but please find time to read it carefully as we congratulate you over your success on the following official publication of results from our ongoing Online Raffle Draws as Organized by Microsoft Corporation, foundation for software products and the consortium of software promotion companies i.e. The Intel Group, Toshiba, Dell Computers and other International Companies which was tagged Microsoft Edinburgh 2019 Product Award. This programme is held every year around the world with this aim of encouraging this use of Microsoft Products and other software for computer Literacy worldwide. We do believe that your emergence for the 3rd Category Prize award of (£870,000.00) as drawn against your E-mail address from the result of our online e-mail beta draws held on 28th January 2019 here in Edinburgh United Kingdom will help and promote your active patronage to Microsoft and FSP Products.

We wish to formally announce to you that you have successfully passed the requirements, satisfactory obligation, verification and satisfactory report test as conducted for all our online winners. A winning cheque of £870,000.00 (Eight Hundred And Seventy Thousand Great British Pounds Sterling Only)in your name and A Brand New 2019 Matte Black Surface Laptop(2) which was consequently staked to be won by the 3rd Category will be sent to you from Microsoft Edinburgh Regional Office here in the United Kingdom. We hereby advise you to establish an immediate contact Via E' mail with the MS-FSP Europe Payment processing Unit of Microsoft Edinburgh United Kingdom with the following details to avoid unnecessary delay and complications in releasing your payment to you.

PAYMENT RELEASE FORM.
(1). Residential Address:
(2). Telephone/Fax Number:

locomotivgrill.com
Domain Notification for locomotivgrill.com : This is your Final Notice of Domain Listi...
To: Ferenc Koczka

4_Fizess 7 August 2019, 11:45

Details

Attention: Important Notice , DOMAIN SERVICE NOTICE
Domain Name: locomotivgrill.com

ATT: Ferenc Koczka
locomotivgrill.com
Response Requested By
8 - Aug - 2019

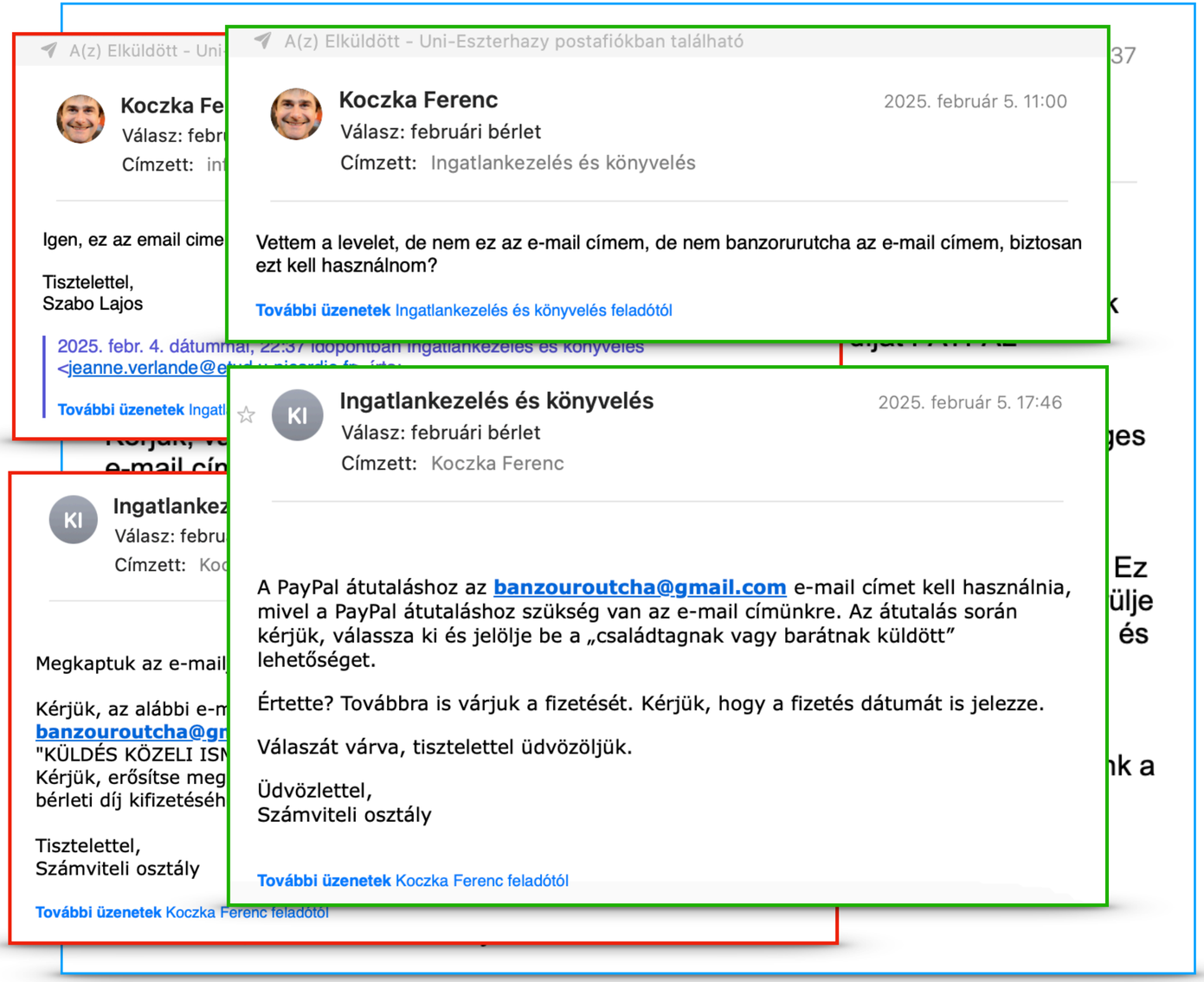
PART I: REVIEW NOTICE

Attn: Ferenc Koczka
As a courtesy to domain name holders, we are sending you this notification for your business Domain name search engine registration. This letter is to inform you that it's time to send in your registration.

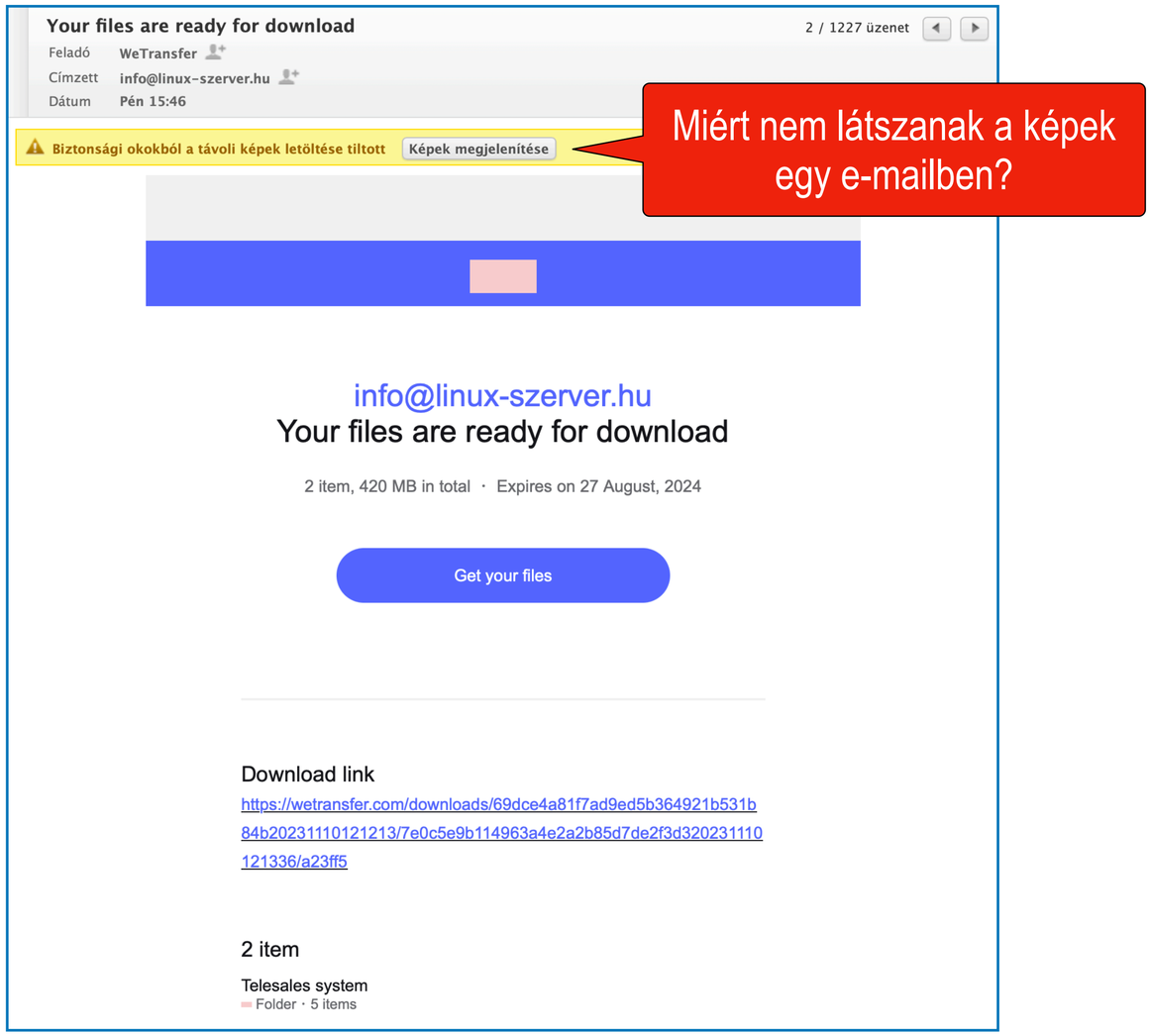
Failure to complete your Domain name search engine registration by the expiration date may result in

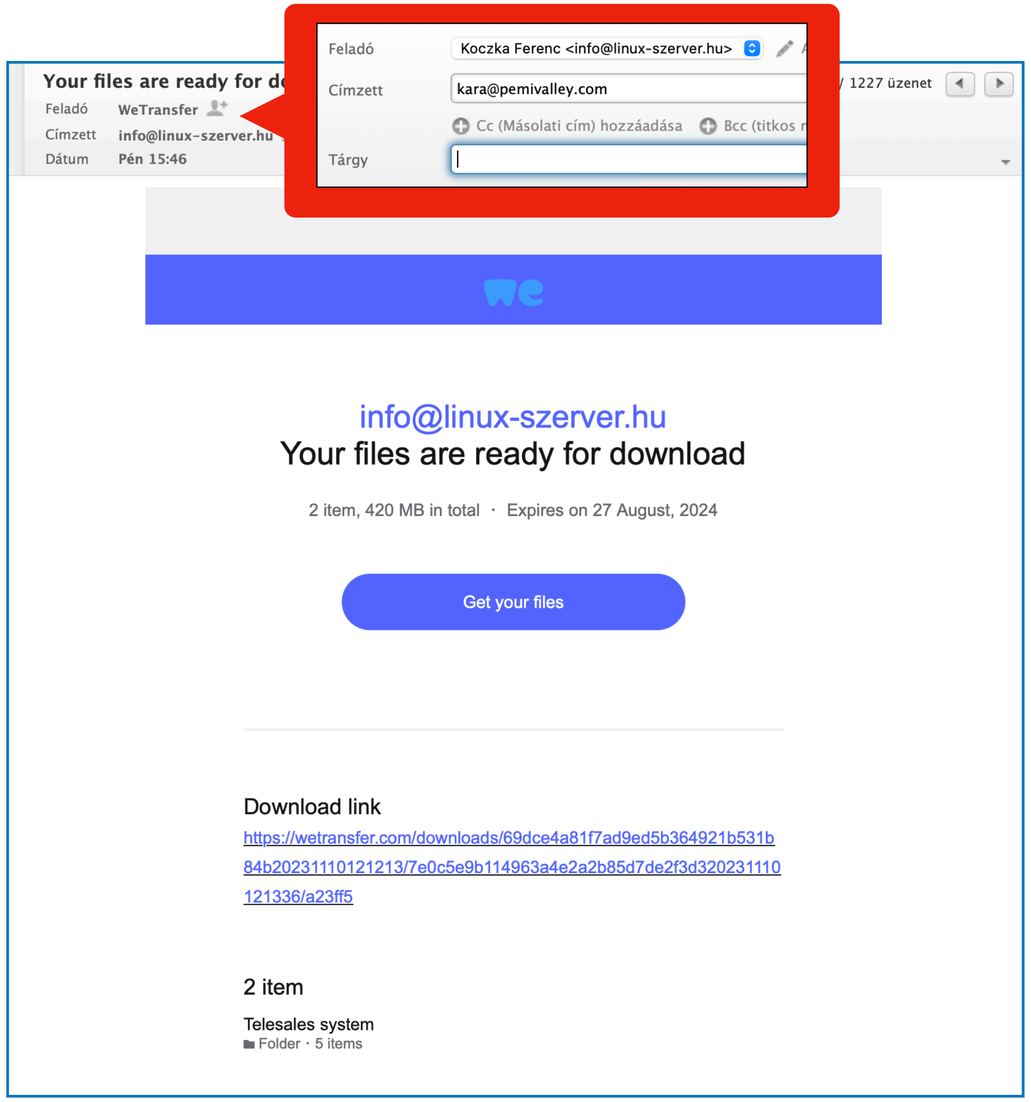
Paypal csalások

- Nincsenek hamis linkek, a támadók egy meglevő szerződés vagy vásárlás fizetési linkjét irányítanák át a saját bankszámlájukra.



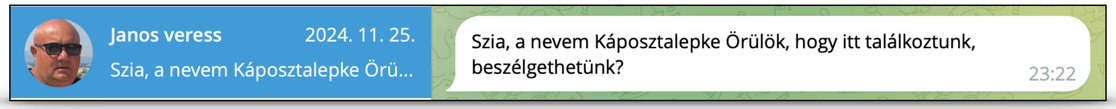
Visszajelzés a támadónak: képek a levelekben

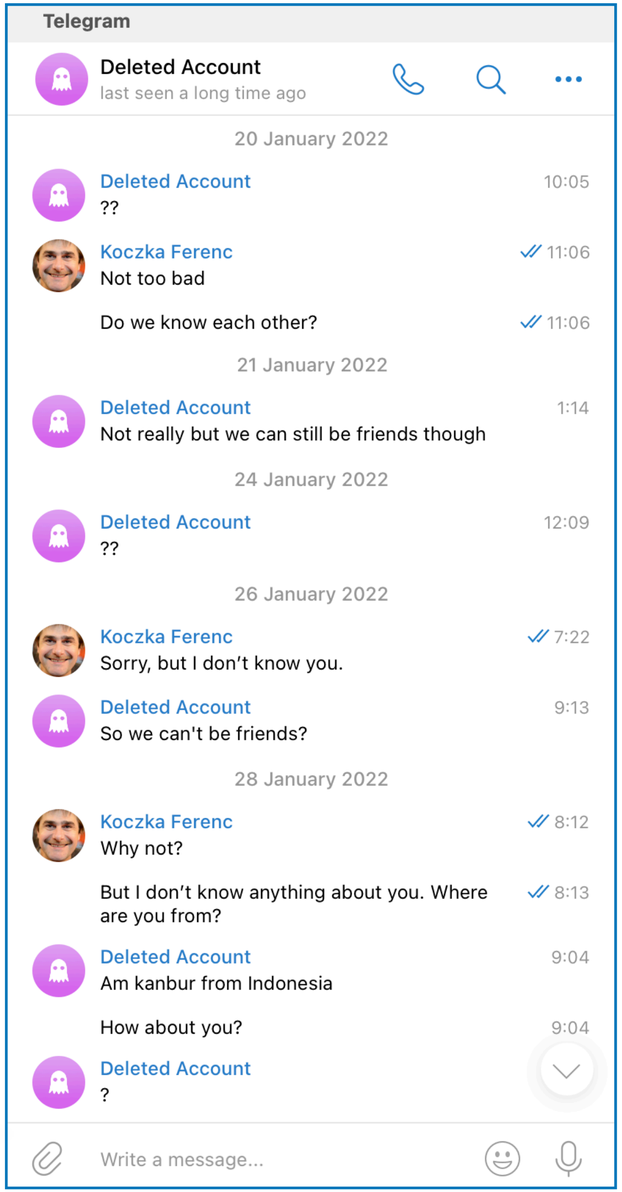


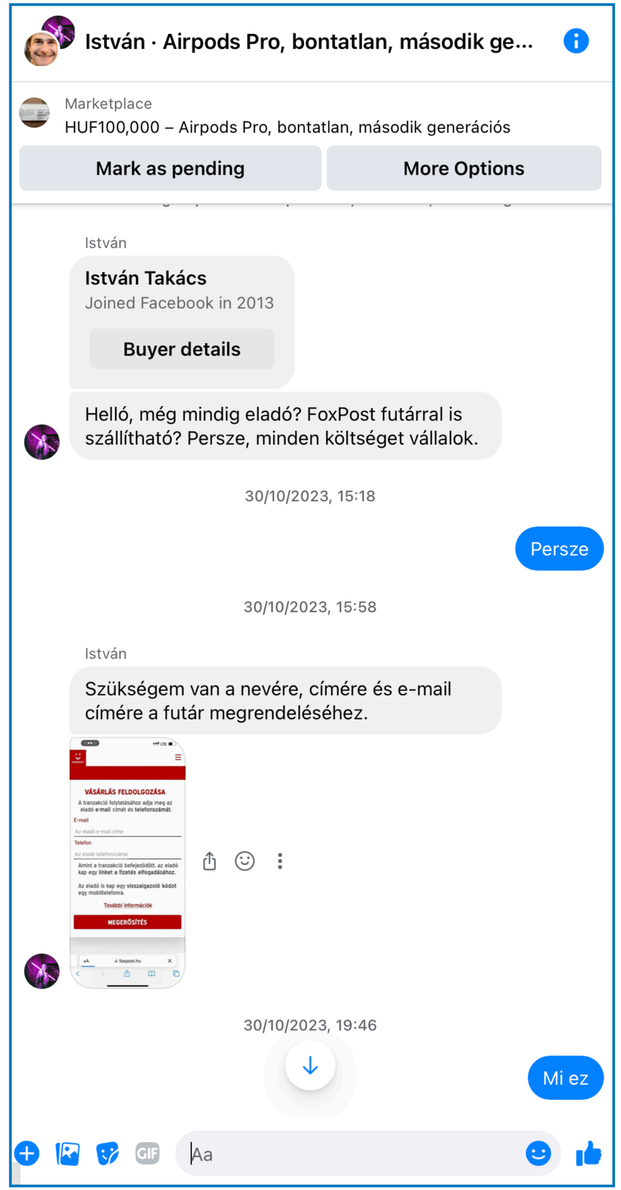


Egyéb csatornák

- Mik az azonnali üzenetküldők, és miért jobb az egyik, mint a másik?
- A támadók az azonnali üzenetküldő szoftvereket (Skype, Messenger, Telegram stb.) is felhasználják, hogy kapcsolatba lépjenek velünk.
- A profilunk áttekintésével sok információt szerezhetnek rólunk, így sokkal hihetőbb történetet adhatnak elő. (Vallás, állatvédelem, politikai irányultság stb.)
- Itt már célként jelenik meg az anyagi haszonszerzés.
- Facebook apróhirdetés trükkje. D







SMS-ek

tegnap 21:37

Szia apa, az alabbi szam az uj szamom. Az régi telefonom elromlott. Tudsz nekem küldeni egy üzenetet WhastApp,-on? +36702069055 // ezt kaptam már másodszor, hol tudom bejelenteni? Elsőre majdnem besétáltam.

iMessage

10:01

122

+36 70 700 9267

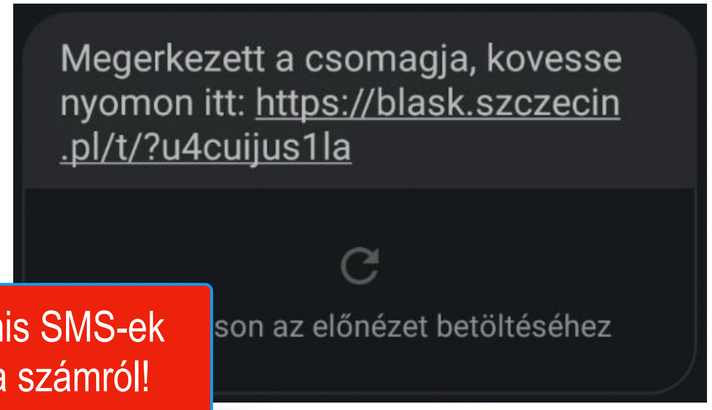
Szöveges üzenet
aug. 16., P 14:29

A csomagot leállították a meg nem fizetett vámok miatt: jii.li/GqSni

ma 10:00

Kedves Vásárlónk! Megrendelésed átvehető boltunkban! aqua.hu

DHL: A csomagját nem sikerült kézbesíteni. 3,99 eurós vámdíjat kell fizetni. Kérjük, fizesse ki, mielőtt a csomagot visszaküldi a feladónak dhlritardi.com



valós és hamis SMS-ek ugyanarról a számról!

8:44

119

+33 6 17 34 00 95

Szöveges üzenet
2023. febr. 21. 15:35

Netflix : Legutobbi befizetését elutasitottak,kérjük, er sitse meg fizetési adatait, különben fiokjat felfüggesztjük: https://hongria-azen-net-flix.com/

8:4

119

+36 30 555 5412

A magyar telefonszám semmit sem jelent!

Szöveges üzenet
dec. 10., V 9:28

4550 Ft-os kesedelmes fizetese van, tekintse meg a HU8202731 szamu szabalysertesi aktajat: https://hu-rendorsegi.net

8:57

119

ipbgxvp10734@aa.guge888.net

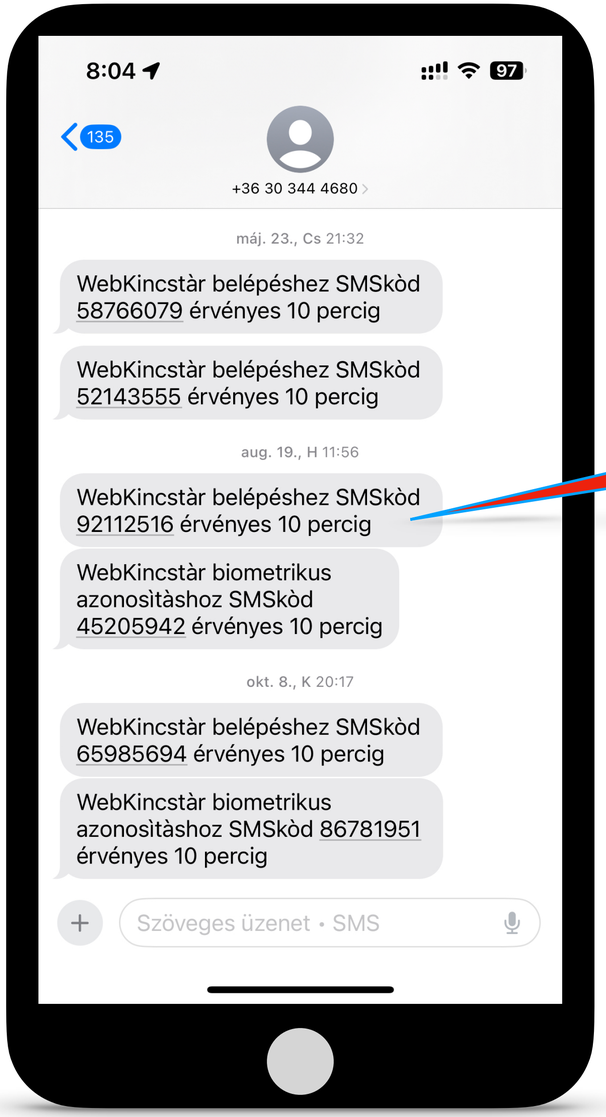
iMessage
máj. 13., H 16:13

Küldemenyenek kezbesitese megszakadt, mert a csomagon hianyzott az utcaszam. Kerem frissitsen: http://s.mrw.so/aVQ2f

A küldő nem szerepel az Ön kontaktlistájában.

Kéretlen üzenet jelentése

SMS kódok megosztása

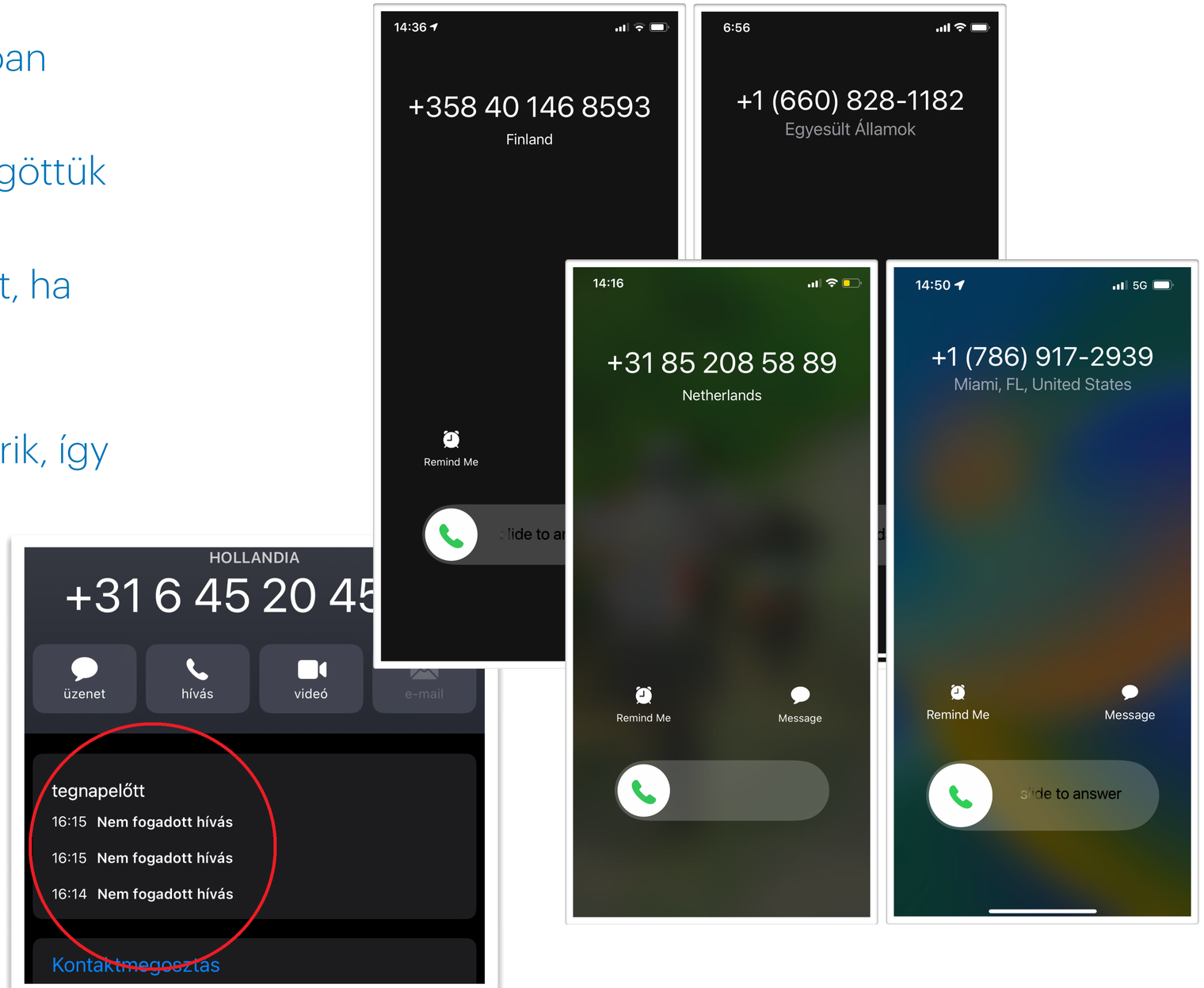


Soha, senkivel ne osszuk meg az üzenetekben kapott kódokat!



Ismeretlen telefonhívások

- Rendszerint külföldi számok, de várhatóan hazaiak is megjelennek majd. (Asterix)
- Emelt díjas szolgáltatások állhatnak mögöttük (*wangiri* - visszahívásos csalás).
- Soha ne hívjuk vissza ezeket a számokat, ha lehet, válasszunk más utat a kapcsolatfelvételre!
- A magyar szolgáltatók egy részüket szűrik, így ezek általában nem járnak sikerrel.



Feltörhetik a telefonomat?

- Zerodium **D**





Nyilvános töltők

- Mi egyáltalán a probléma?
- https://hak5.org/products/omg-cable



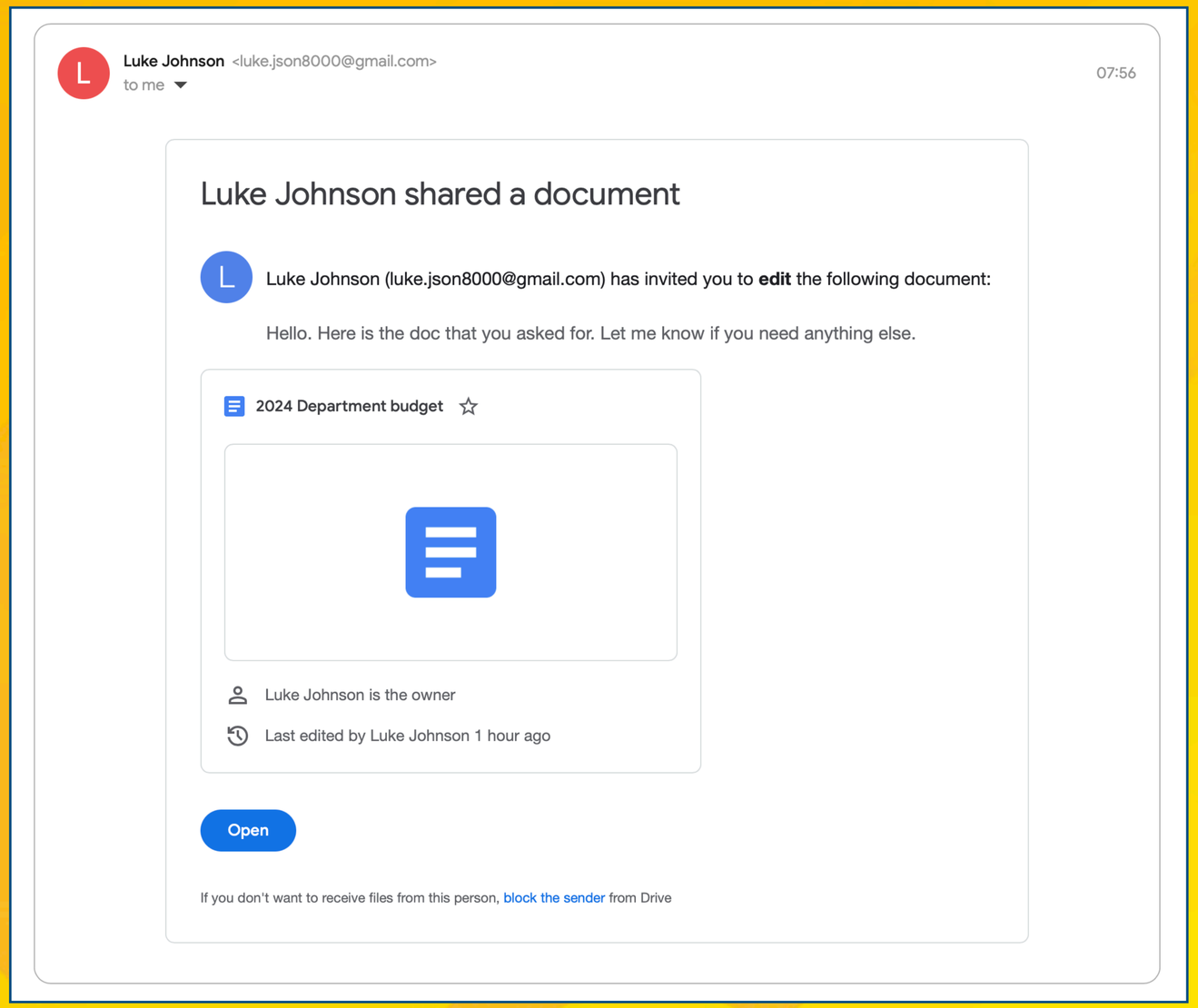
Shoulder peeking

- Nem gyakori probléma, de érdemes ismerni.



Google Phishing Quiz

https://phishingquiz.withgoogle.com/



Co-funded by the European Union

Bankszámlaszám változás

Co-funded by the
European Union



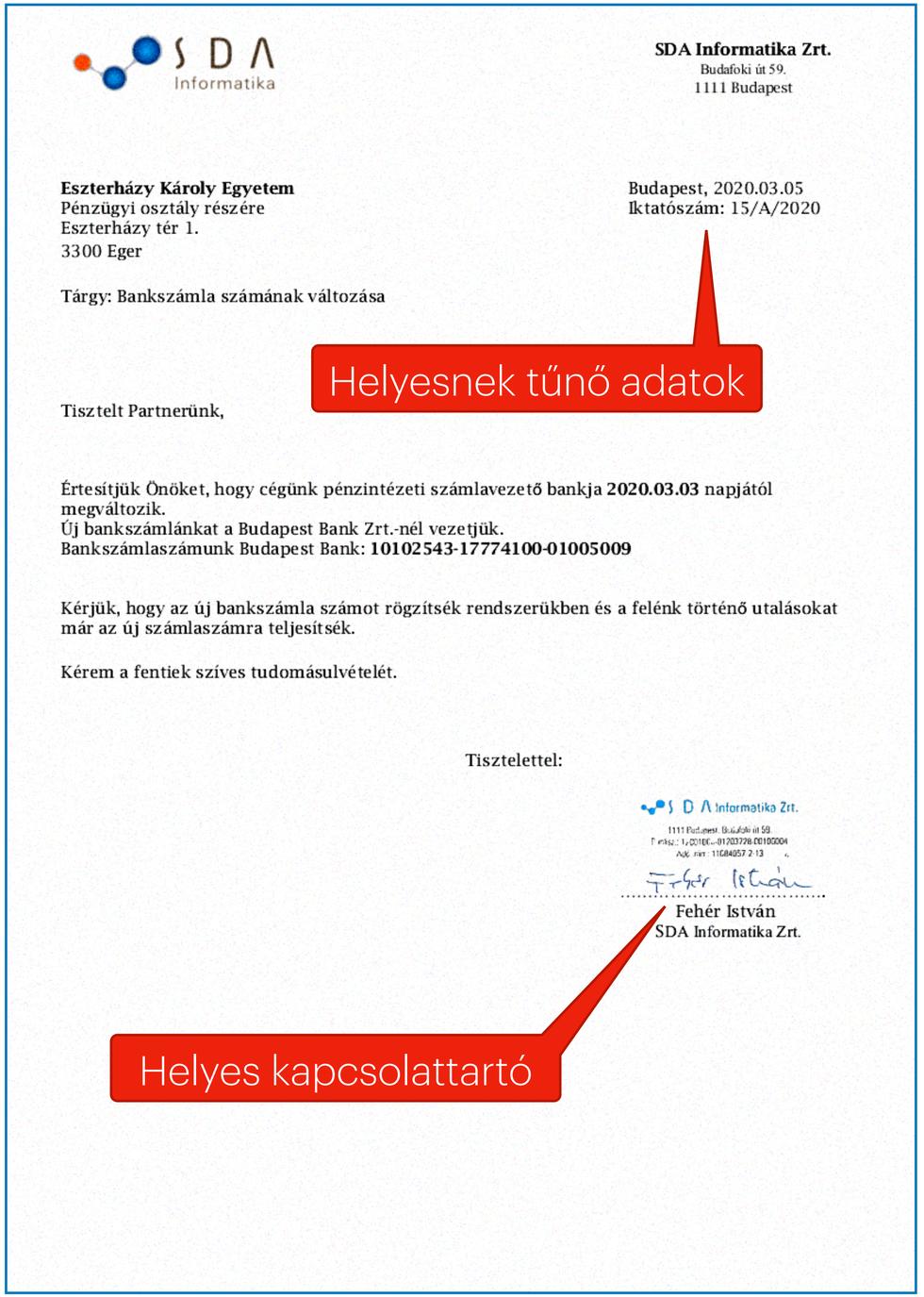
Célzott támadások

A támadó előzetes információ gyűjtés után bankszámla változásról küld levelet, vagy indít telefonhívást.

- A támadó nyílt információgyűjtéssel (OSINT) előzetesen feltérképezi a célpont üzleti/kommunikációs kapcsolatait.
- Megpróbálja rávenni az ügyintézőt arra, hogy a pénzügyi rendszerében változtassa meg a cég bankszámlaszámát. Ezt követően a kifizetések a támadó számlájára kerülnek.



- Bankszámlaszám változáskor azonnal csörögnie kell a vészcsengőnek! Ilyen esetekben különösen óvatosan kell eljárni! Független csatornán meg kell győződni az információ valódiságáról!



SDA Informatika

SDA Informatika Zrt.
Budafoki út 59.
1111 Budapest

Eszterházy Károly Egyetem
Pénzügyi osztály részére
Eszterházy tér 1.
3300 Eger

Budapest, 2020.03.05
Iktatószám: 15/A/2020

Tárgy: Bankszámla számának változása

Helyesnek tűnő adatok

Tisztelt Partnerünk,

Értesítjük Önöket, hogy cégünk pénzintézeti számlavezető bankja **2020.03.03** napjától megváltozik.
Új bankszámlánkat a Budapest Bank Zrt.-nél vezetjük.
Bankszámlaszámunk Budapest Bank: **10102543-17774100-01005009**

Kérjük, hogy az új bankszámla számot rögzítsék rendszerükben és a felénk történő utalásokat már az új számlaszámra teljesítsék.

Kérem a fentiek szíves tudomásulvételét.

Tisztelettel:

SDA Informatika Zrt.
1111 Budapest, Budafoki út 59.
Fehér István
SDA Informatika Zrt.

Helyes kapcsolattartó



Üvegzseb

Az üvegzseb programok, a kötelező nyilvánosság a kiberbiztonság szempontjából gyengítő tényező.

- Az aláírások közzétételével könnyen állíthatók elő hitelesnek tűnő iratok.



Google hack

- csík lászló filetype:pdf
- anyós site:https://media.ekonyv.hu/shared/product filetype:epub

anyós filetype:epub site:https://media.ekonyv.hu/shared/product

Összes | Képek | Videók | Hírek | Rövid videók | Könyvek | Web | Egyebek | Eszközök

Ekonyv.hu
https://media.ekonyv.hu › shared › product

Az anyós

Az **anyós** a Magyarországon A válással berobbanó Moa Herngren nagysikerű családidráma-trilógiájának második darabja. „Minden karakterem emberi, közel sem ...

Ekonyv.hu
https://media.ekonyv.hu › shared › product

A Baljós Anyós

K.B. Rottring. Stanley Steel. A Baljós **Anyós**. (Részlet). Excalibur Könyvkiadó. K.B. Rottring. &. Stanley Steel: A Baljós **Anyós**. Kiadja: Az Excalibur Könyvkiadó.

Ekonyv.hu
https://media.ekonyv.hu › shared › product

Anyósom, a drága - részlet

– Mindig is nehéz természet volt – jegyezte meg lemondóan a férjem az édesanyjáról egy **anyós**-meny vita után. – Azt hittem, ha unokája születik, majd ...

Ekonyv.hu
https://media.ekonyv.hu › shared › product

Az igazi

... **Anyós**, rosszízű szó! Ez a nő, férjem anyja, a legfinomabb emberi teremtések egyike volt, akit ismertem. Mikor apósom meghalt, s ez a gazdag, előkelő asszony ...

Ekonyv.hu
https://media.ekonyv.hu › shared › product

Minden napra egy sztori

... **anyós** is maradéktalanul elégedett legyen a nyílászárókkal, a lépcsővel, a fűtéssel, a konyhával, a kamrával, a nappalival, a fürdővel, leveszi dolgozó ...

ekonyv.hu
https://media.ekonyv.hu › shared › product

Anyák és kamionsofőrök – részlet

... **anyós** mellett. Hallgass rám, mondta. És anya hallgatott rá. Csakhogy aztán apa is bekeményített, hogy neki ott van az otthona és kész. Magyarán, külön éltek ...

Célzott támadások



Co-funded by the
European Union



Célzott támadások

A támadó előzetes információgyűjtés után küld valódinak tűnő, helyes adatokat tartalmazó levelet.

- A támadó nyílt információgyűjtéssel (OSINT) előzetesen feltérképezi a célpont üzleti/kommunikációs kapcsolatait.
- Valódinak tűnő számlát küld, melyet a pénzügy esetleg kifizet.



- Mindig ellenőrizni kell a levél valódiságát és a bankszámlaszámot!

Feladó: ISD DUNAFERR Zrt. [mailto:finance@isd-dunaferr.hu]
Küldve: 2017. május 25., csütörtök 12:44
Címzett: logiszti[redacted]
Tárgy: Rendelés visszaigazolása: 5847395902

ISD DUNAFERR

ISD DUNAFERR DUNAI VASMŰ
ZÁRTKÖRŰEN MŰKÖDŐ RÉSZVÉNYTÁRSASÁG
Cím: 2400 Dunaújváros, Vasmű tér 1–3.
Levélcím: 2401 Dunaújváros, Pf. 110
Telefon: +36 (25) 998-602, Fax: +36 (25) 999-190

Tisztelt [redacted]

Az ISD DUNAFERR Zrt. elektronikus számlalevelet állított ki önnőknek mellékletben megtalálható!

Kérjük hogy a számla ellenértékét szíveskedjenek kiegyenlíteni hogy 2017.05.25.-ig átutalni hogy könyvelésre kerülhessen, a lentiekben megjelölt szállítási időpont akadálymentes foglalása érdekében!

Tervezett szállítási időpont 2017.05.26. 13:30 -16:30 ig bezárólag érkeznek a szerelvények!

ISD DUNAFERR Zrt.
Tóth Imre
Telefon: +36 (25) 998-602
Értékesítő

ISD DUNAFERR DUNAI VASMŰ ZÁRTKÖRŰEN MŰKÖDŐ RÉSZVÉNYTÁRSASÁG

ISD DUNAFERR

Előlegszámla

Kibocsátó
ISD DUNAFERR Zrt.
2400 Dunaújváros, Vasmű tér 1-3
Tel.: +36 (25) 998 602 Fax: +36 (25) 999 190
Adószám: 11102539-4-07
Számlavezető: OTP Bank Nyrt.
Bankszámla: 11773353-01654808-00000000
Web:www.dunaferr.hu

Vevő
[redacted]

Tárgy: A szállítás várható ideje: 2017.05.26.

Fizetési mód	Teljesítés	Kelt	Fizetési határidő	Sorszám
Átutalás	2017.05.25.	2017.05.25.	2017.05.25.	536617/2017

Megnevezés	Mennyiség	Egységár Ft	Nettó össz. Ft
M.H. Bordás betonacél átm.: 10 mm-12 fm Minőség: B 60-50 (7.44 kg / szál) 360 szál / köteg	13 392 kg	105	1 406 160,00

Kártékony kód

Co-funded by the
European Union

Kártékony kód - kettős kiterjesztés



A támadó célja, hogy a felhasználót rávegye egy kártékony szoftver elindítására.

- Leggyakrabban e-mail mellékletként érkezik.
- A melléklet gyakran kettős kiterjesztéssel rendelkezik.
- Különösen veszélyesek az .iso és a .zip fájlok.
- Kártékony kódot tartalmazhatnak a .docx és az .xlsx fájlok is.



- Soha, de soha ne nyissunk meg idegen forrásból származó mellékletet!
- Különösen fontos a melléklet kiterjesztésének ellenőrzése!

Akár valódinak látszó feladó



Kettős kiterjesztés a fájlnévben



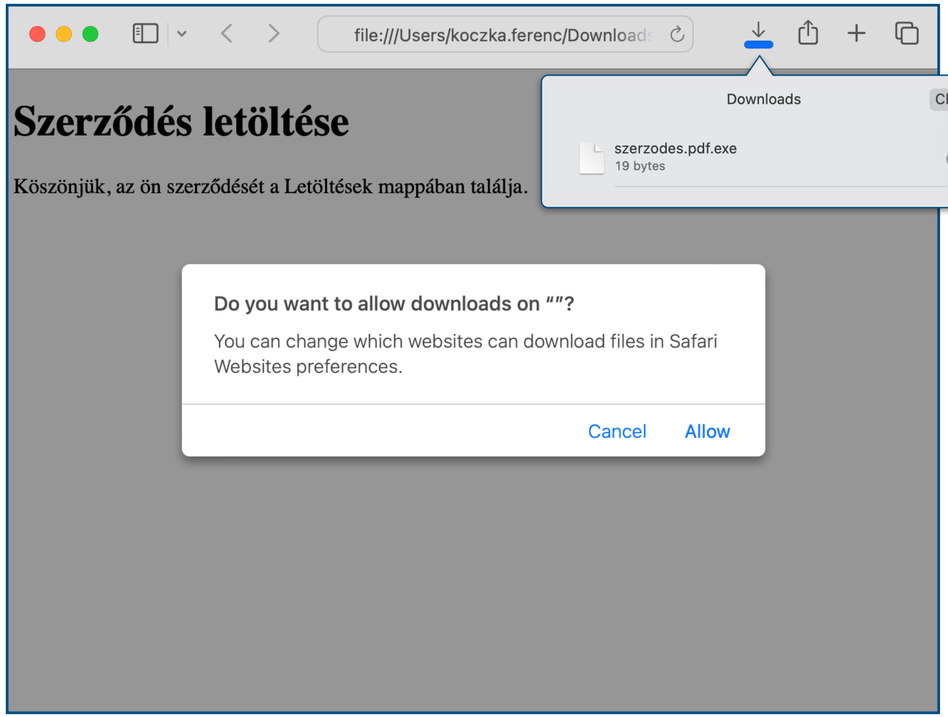
HTML Smuggling



A támadó egy preparált weboldalt készít, amely automatikusan letölt egy fájlt a felhasználó gépére.

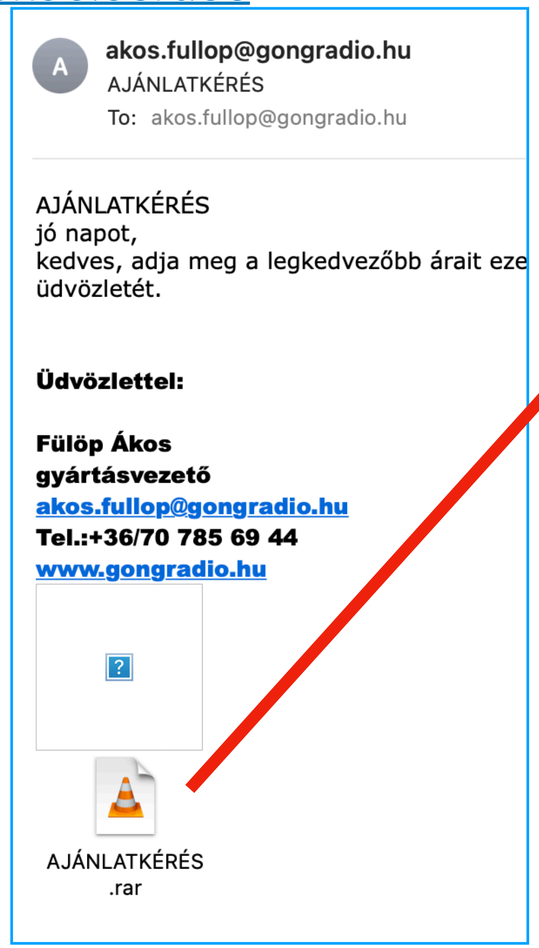
A támadók könnyen készítenek olyan weboldalt, vagy módosítanak más, feltört oldalakat, hogy egy fájl letölthető legyen a felhasználó közreműködése nélkül is.

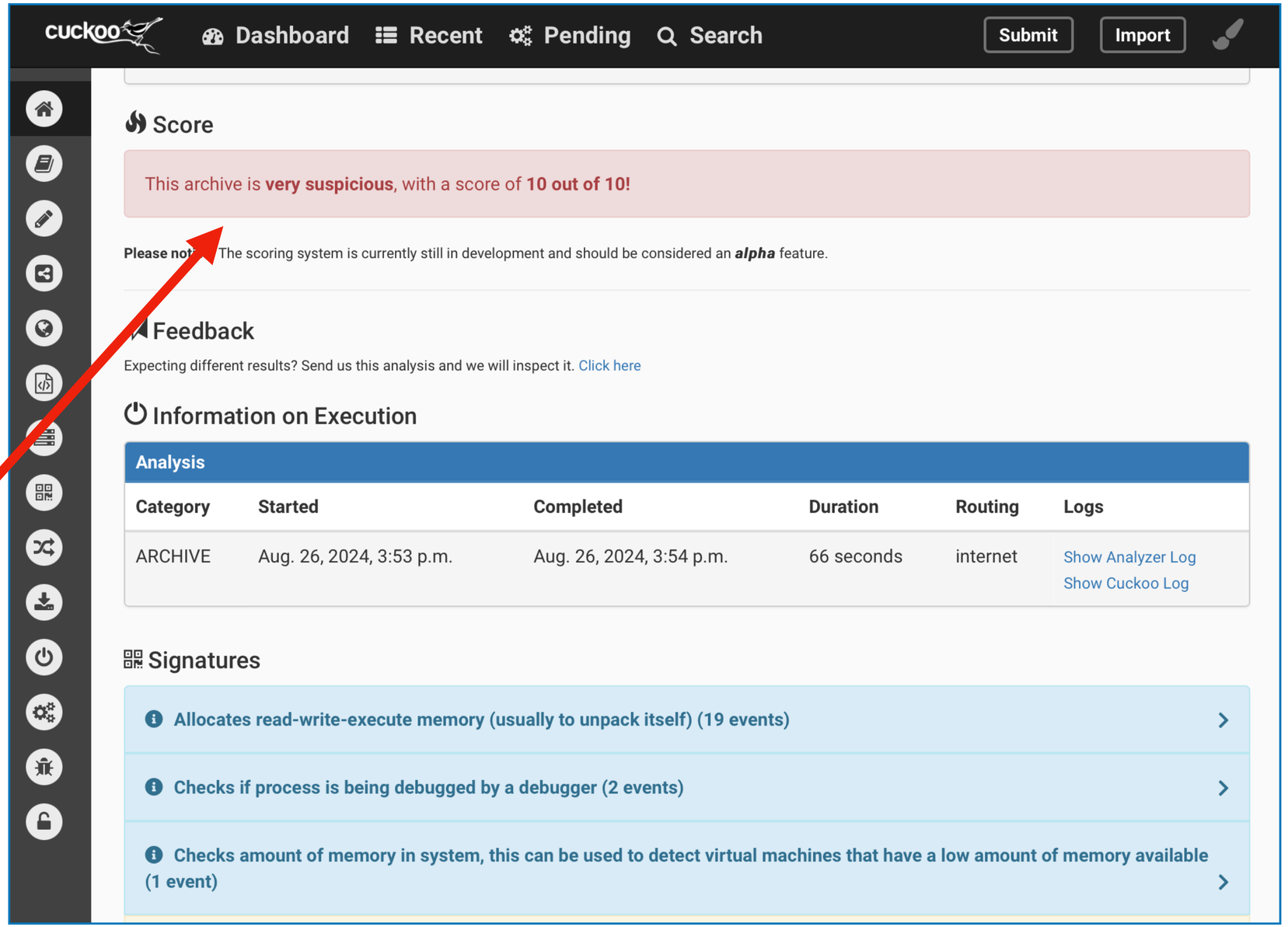
```
<!DOCTYPE html>
<html lang="hu">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Dokumentum letöltése</title>
</head>
<body>
    <h1>Szerződés letöltése</h1>
    <p>Köszönjük, az ön szerződését a Letöltések mappában találja.</p>
    <script>
        // echo "Ez egy káros kód" | base64
        let content = "data:application/octet-stream; base64,RXogZWd5IGvDoXJvcyBrw7NkCg==";
        let downloadlink = document.createElement("a");
        downloadlink.href=content;
        downloadlink.download = "szerzodes.pdf.exe";
        downloadlink.click();
    </script>
</body>
</html>
```



Valóban kártékony a melléklet?

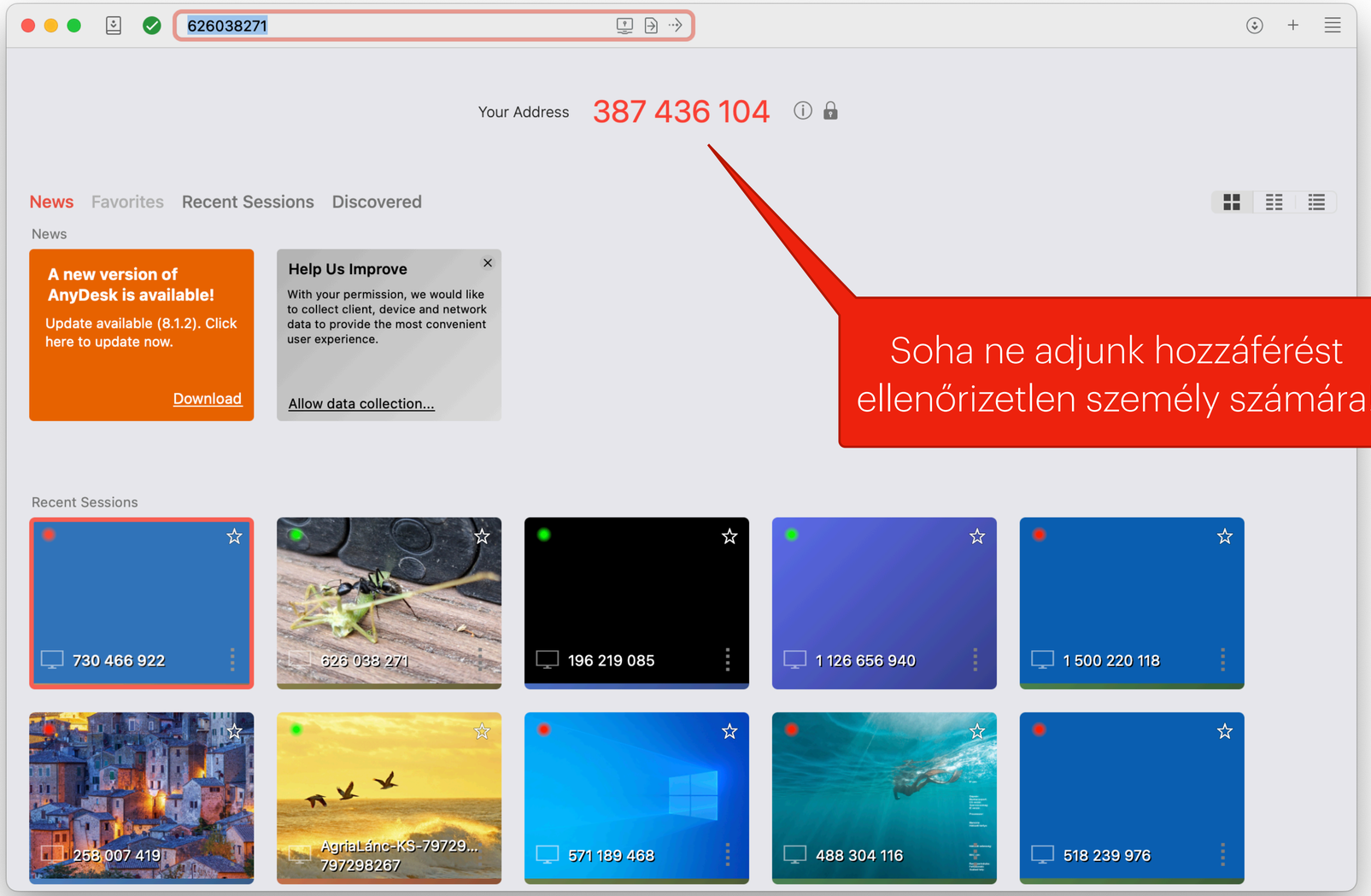
- akos.fullop@gongradio.hu
- https://cuckoo.cert.ee





Távvezérlés: Anydesk, Teamviewer

- Csalók előszeretettel telepítenek távoli hozzáférést lehetővé tevő programokat a számítógépünkre.
- Telefonos megtévesztés során védelmi szoftverként mutatják be.
- Mindig győződjünk meg a hozzáférést kérő személyének azonosságáról!
- Ne telepítsünk semmilyen alkalmazást, ha akár a gyanúja is felmerül annak, hogy csalás áldozatai lehetünk!

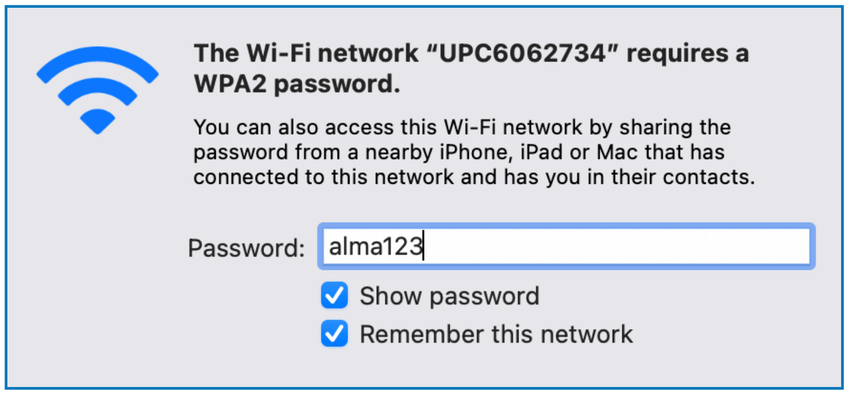


Titkosított adatforgalom

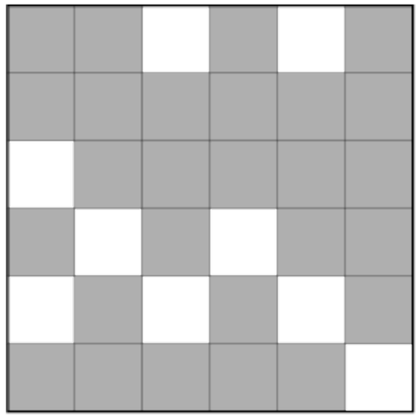
Co-funded by the
European Union

Azonosítás és titkosított adatforgalom

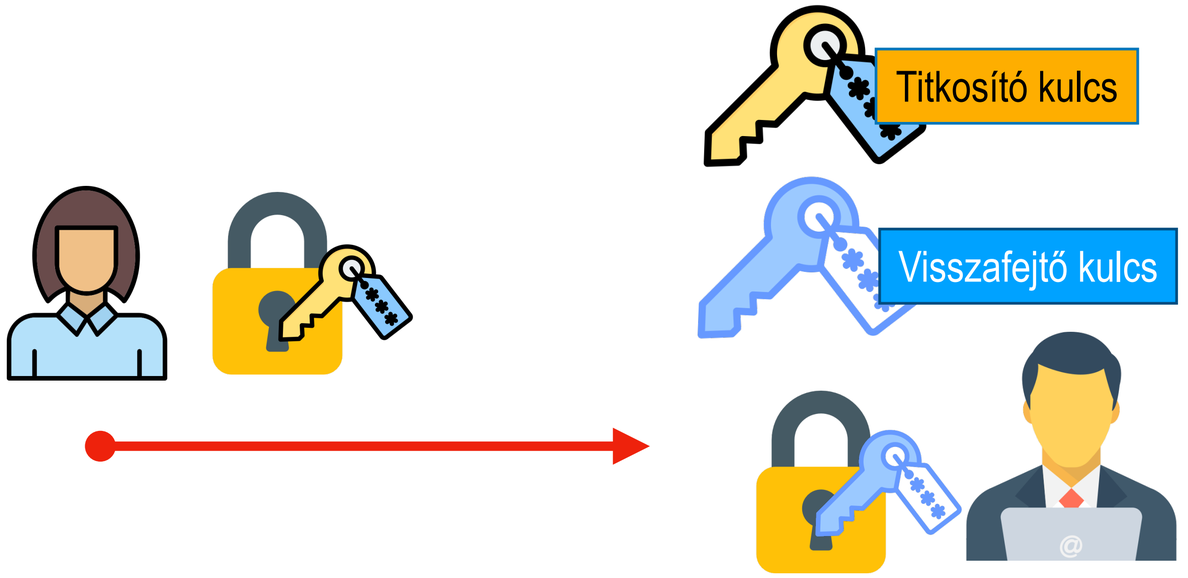
- Szolgáltatások használatához azonosítás szükséges még akkor is, ha a rendszer nem kér jelszót!
- Csak a titkosítás nyújthat megfelelő védelmet az interneten küldött és a számítógépeinken tárolt adatok védelmére!
- Kétféle titkosítás:
  - szimmetrikus kulcsú (WiFi, Sándor Mátyás).
  - Publikus - privát kulcson alapuló.



E	J	E	U	S	T
Y	G	L	É	Á	N
Á	E	Y	S	É	S
C	N	V	D	Í	B
O	E	R	M	M	R
N	E	Ű	N	R	Á

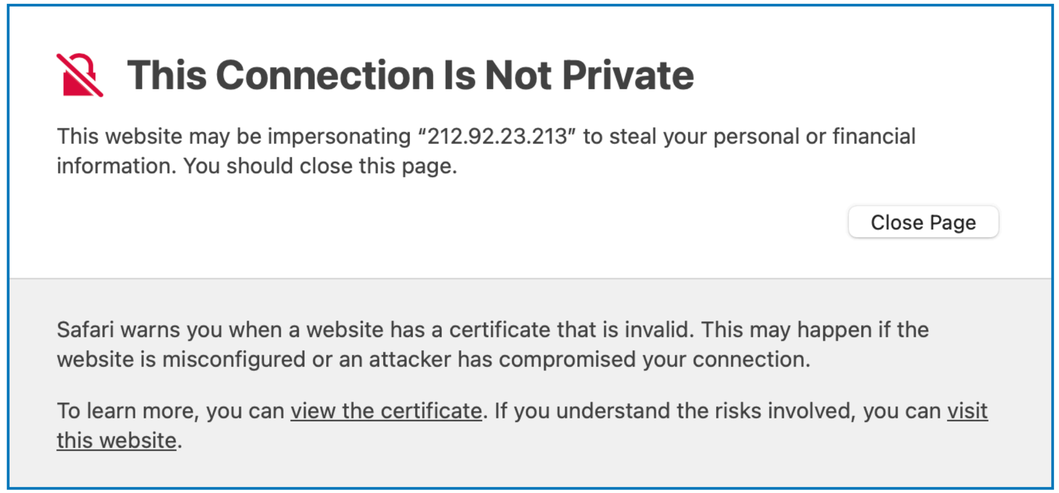


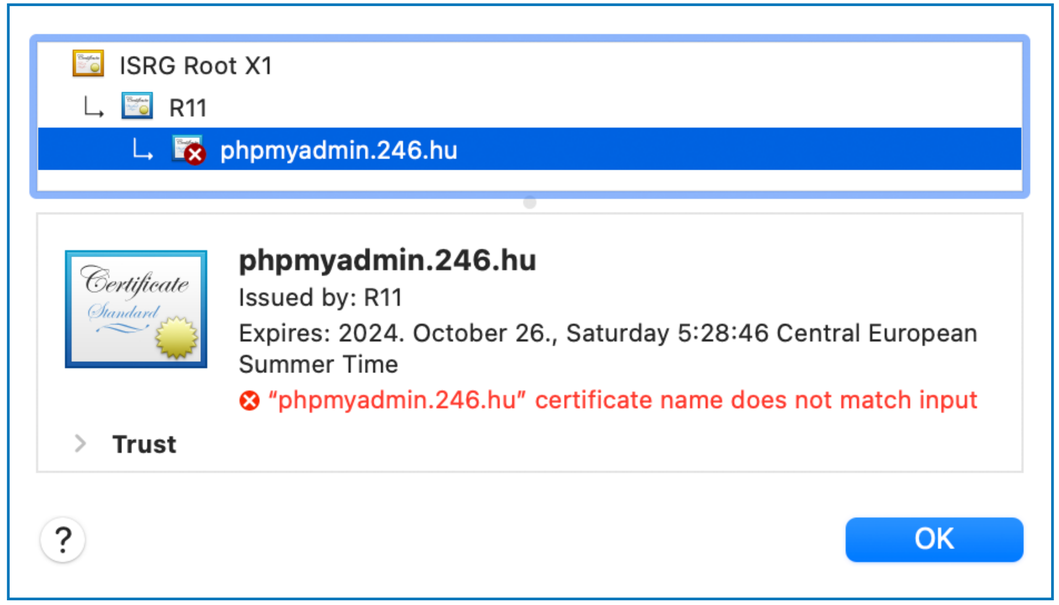
D

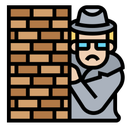


Megtévesztő weboldalak és a tanúsítványok

- http:// és https://. D
- A https kapcsolat egyúttal titkosítást is jelent!
- Bármelyik weboldal könnyűszerrel lemásolható!
  - wget -r -p -k -E https://www.kh.hu D
  - Forrás átírása “**Ingyen hitel**”
- Egy oldal hitelességét a tanúsítvány bizonyít**hat**ja.
- https://www.dp.hu D
- Tipikus példái a banki weboldalak.

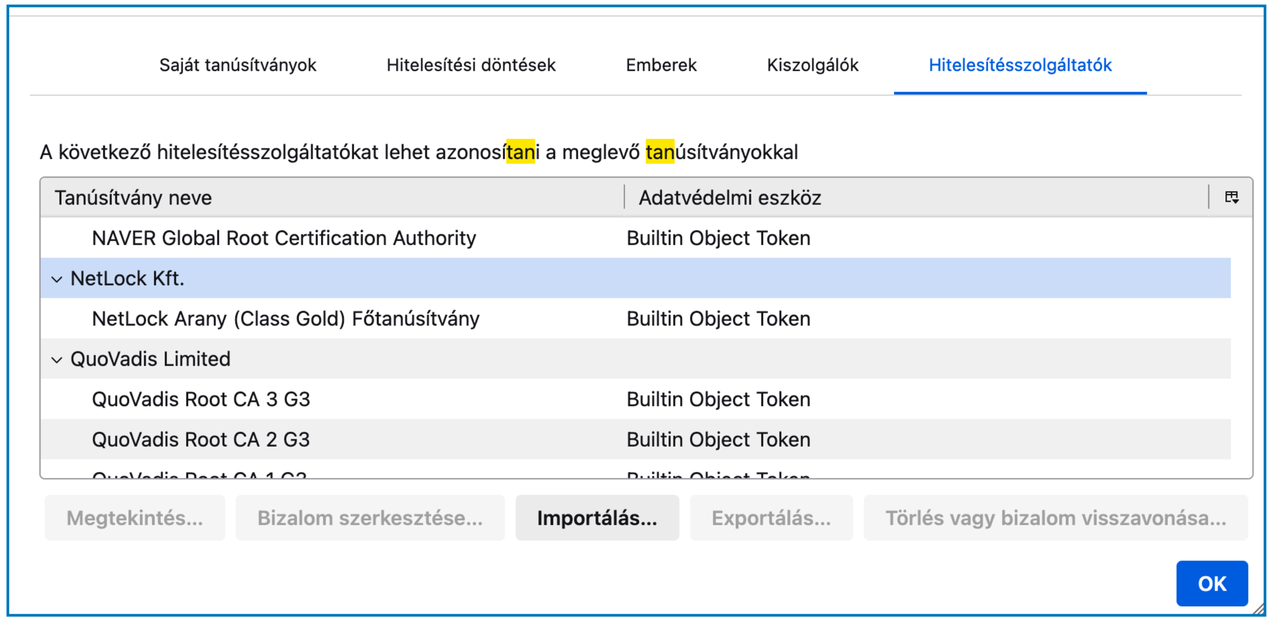


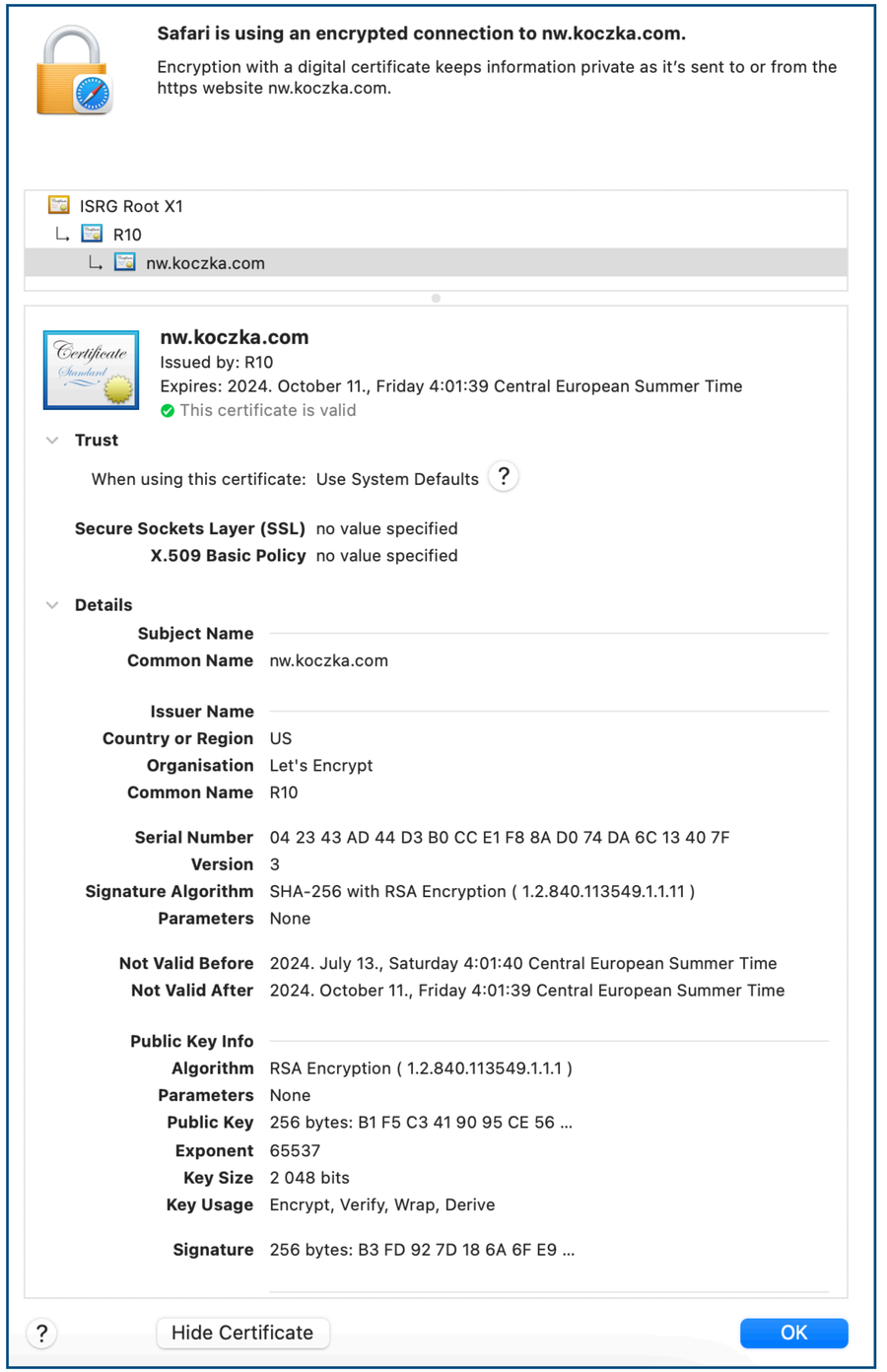




Hogyan működik egy tanúsítvány?

- A böngésző tanúsítványai.
- Saját tanúsítvány használata: lehetséges veszélyforrás!
- Ingyenes és vásárolt tanúsítványok. D
- Magyar tanúsítvány szolgáltatók: Netlock Kft., Microsec Kft.
- A Letsencrypt: R10







A védekezés elemei

- A feladó címének és domainjének ellenőrzése minden olyan levél esetében, amely valamilyen számlát, kérést stb. tartalmaz.
- Figyeljünk a kettős domain nevekre, pl.
- Különös tekintettel kell lenni a “hasonló” domain nevekre: *eon.pay.hungary.chachais.com*
- Weboldalak esetén ellenőrizzük a tanúsítvány kiállítóját és érvényességét!
- A Letsencrypt tanúsítványok csak a titkosítást garantálják!
- Saját domainre bárki készíthet helyes tanúsítványt!

Támadók és motivációik

Co-funded by the
European Union



Államilag támogatott Hackerek

Cél: Politikai, gazdasági vagy katonai előnyök szerzése.

Módszerek: Kémkedés, kritikus infrastruktúrák elleni támadások, propaganda terjesztése.

Példa: APT (Advanced Persistent Threat) csoportok, pl. Fancy Bear (APT28).

Észtország elleni támadás (2007): Az egyik első nagyobb léptékű állami támogatású kibertámadás során orosz hackerek több kormányzati, pénzügyi és egyéb webhelyet tettek (DDoS) támadásokkal működésképtelenné,
részben válaszul a szovjet Vörös Hadsereg emlékművének eltávolítására.

Sony Pictures feltörése (2014): Az Egyesült Államok kormánya Észak-Koreát tette felelőssé azért a támadásért, amely során hackerek megszerezték és nyilvánosságra hozták a Sony belső dokumentumait és filmjeit Is megsemmisítették a vállalat IT infrastruktúráját. A támadást az Észak-Koreáról szóló "The Interview" című film vetítése váltotta ki.

Stuxnet (2010): Az USA és Izrael által fejlesztett Stuxnet féreg célzott támadást indított az iráni nukleáris program ellen, a Natanz urándúsító üzem centrifugáinak tönkretételére. Ez volt az első ismert eset, amikor egy kártevő fizikailag károsította ipari berendezéseket.

NotPetya (2017): Az orosz katonai hírszerzés, a GRU által indított támadás célja az ukrán kritikus infrastruktúra tönkretétele volt. A NotPetya támadás, amely egy olyan ransomware-nek álcázott kártékony szoftver volt, melynek célja az IT rendszerek használhatatlanná tétele, gyorsan elterjedt, több milliárd dolláros kárt okozva a gazdaságban és az egészségügyben.



SolarWinds (2020): Az USA állítása szerint az orosz hírszerzés (SVR) állt a támadás mögött, amely során a SolarWinds Orion nevű termékének frissítésébe kártékony kódot juttattak, amelyet több ezer ügyfél töltött le és futtatott le a rendszerében. A kártevő több mint fél éven át maradt rejtve és lappangott többek között az amerikai kormányzati szervek és nagyvállalatok rendszereiben is.



Szervezett bűnözői csoportok

Cél: Széleskörű bűncselekmények elkövetése anyagi haszonszerzés céljából.

Módszerek: Kémkedés, kritikus infrastruktúrák elleni támadások, propaganda terjesztése.

Támadási formák: Tipikusan zsarolóvírusok, adatlopás, banki lopás, bankkártya adatok ellopása, csalás, botnet támadások.

Példák: APT (Advanced Persistent Threat) csoportok, pl. Fancy Bear (APT28).

- DarkSide és a Colonial Pipeline támadás (2021): zsarolóvírus-támadás, mely során egy DarkSide nevű csoport zsarolóvírussal támadta meg az USA keleti partját üzemanyaggal ellátó Colonial Pipeline rendszereit. A támadás jelentős üzemanyaghiányt okozott, és a cég kénytelen volt 4,4 millió dollárt fizetni váltságdíjként a visszaállítás érdekében.





Belső munkatársak

Cél: Személyes haszonszerzés vagy elégedetlenség kifejezése.

Módszerek: Belső információk ellopása, rendszerhibák kihasználása.

Példa: Cég alkalmazottai, akik elégedetlenek a munkakörülményekkel vagy anyagi haszonra vágynak. A távozó dolgozók rendszerint elviszik magukkal azokat az adatokat, amelyekhez hozzáférnek, a legnagyobb károkat a szellemi termékekkel, ügyféllistákkal okozzák. Magyarországon alig ismertek jogi következmények.

Védekezés:

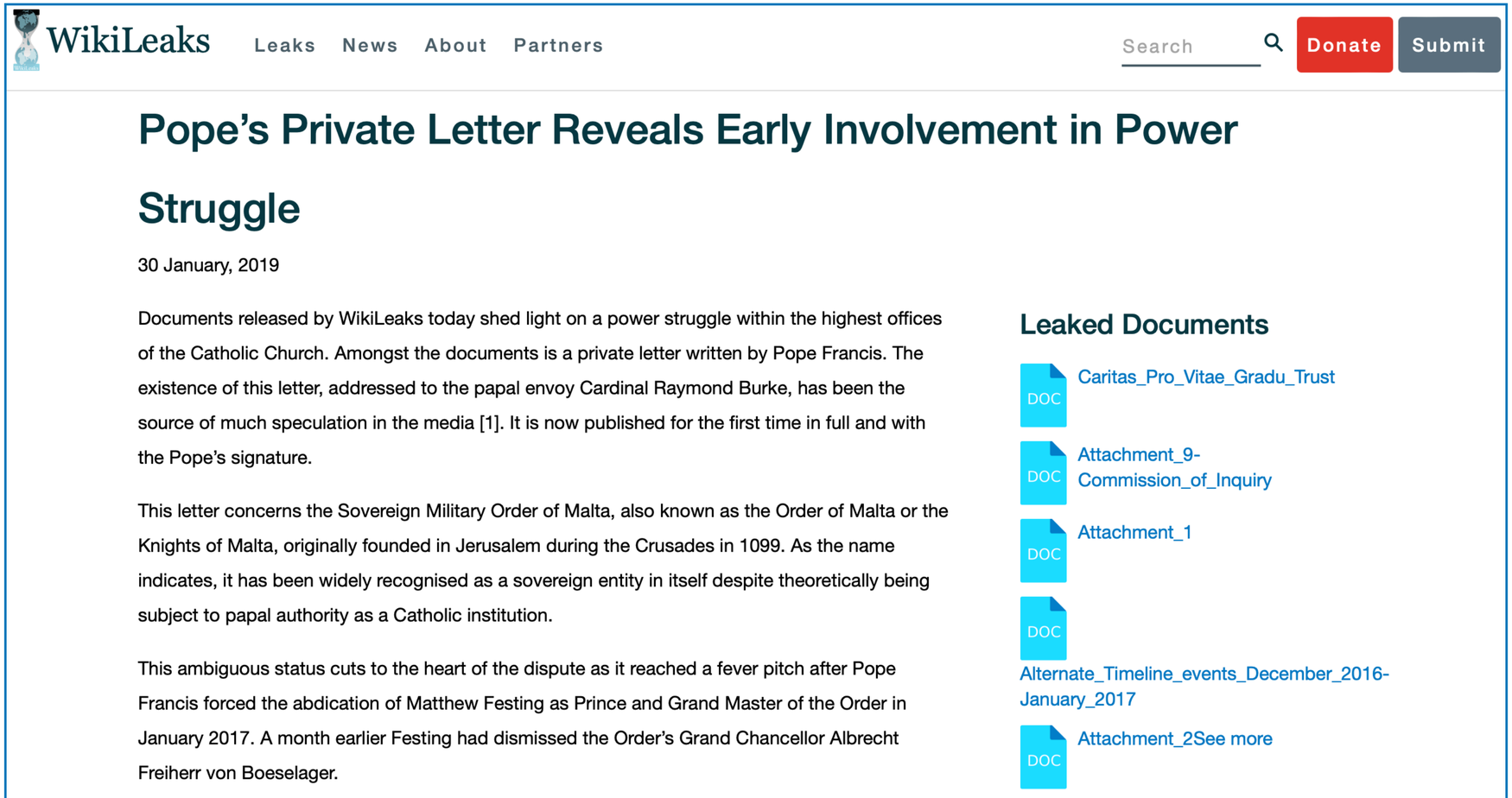
- Rendszeres és ellenőrzött adatmentés.
- Szigorú és minimalizált hozzáférés szabályozás.
- Rendszernaplók létrehozása és folyamatos ellenőrzése.
- Távozó munkatársak szabályos kiléptetése.

Hacktivisták

Cél: Politikai vagy társadalmi változás előidézése.

Módszerek: Weboldalak feltörése, szolgáltatásmegtagadásos támadások (DDoS), adatlopás és közzététel.

Példa: Anonymous, Julian Assange (WikiLeaks), Edward Snowden.





Hackerek

Cél: Rendszerek biztonságának tesztelése

- Etikus hackerek: céljuk a rendszerek tesztelése és a hibák feltárása. Biztonsági szakértők, akik legálisan dolgoznak cégeknek vagy kormányzati szerveknek.
- Szürke kalapos hackerek: illegálisan tesztelnek rendszereket és a megtalált sebezhetőségért pénzt kérnek a rendszer tulajdonosától. (BKV: https://444.hu/2017/07/20/18-eves-fiatal-jelezte-a-bkk-nak-hogy-50-forintert-tudott-berletet-venni-de-koszonet-helyett-inkabb-feljelentettek)
- Fekete kalapos hackerek: fő céljuk a haszonszerzés, az illegális tesztelés során fellelt sérülékenységeket a versenytársaknak vagy a Darkneten próbálják értékesíteni. (https://zerodium.com/program.html)

Módszerek: Penetrációs tesztelés, sebezhetőségek feltárása.

Példa: APT (Advanced Persistent Threat) csoportok, pl. Fancy Bear (APT28).



Script kiddies

Cél: Szórakozás, hírnévszerzés, tapasztalatszerzés. Célpontjaik elsősorban weblapok.

Módszerek: Előre elkészített programok és eszközök használata, nem rendelkeznek technikai ismeretekkel.

Példa: Kezdő hackerek, akik mások által írt eszközöket használnak.

Védekezés:

- Szoftverek és webalkalmazások rendszeres frissítése.
- A Wordpress és más CMS rendszerek.
- https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=wordpress



Search Results

There are **9311** CVE Records that match your search.

Name	Description
CVE-2024-5341	The The Plus Addons for Elementor Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'size' attribute of the Hea g Title all versio d includin .5.4 to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor- access ve, to in t web scr in pa that will execute whenever a user accesses an injected page.
CVE-2024-5327	The PowerPack Addons for Elementor (Free Widgets, Extensions and Templates) plugin for WordPress is vulnerable to DOM-Based Stored Cross-Site ipting v ‘pp_animated_gradient_bg_color’ parameter in all versions up to, and including, 2.7.19 due to insufficient input sanitization and ou escapin ak t possi th icated ckers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2024-5326	The Post Grid Gutenberg Blocks and WordPress Blog Plugin – PostX plugin for WordPress is vulnerable to unauthorized modification of data due missin y check on _pre callback' function in all versions up to, and including, 4.1.2. This makes it possible for authenticated attackers, with Contributor-level access and above, to change ary n affected si ca sed to enable new user registration and set the default role for new users to Administrator.
CVE-2024-5229	The Primary Addon for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Pricing Table widget in all versions up to, an 1.5.5 due to in input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web ecute whenever a user accesses an injected page.
CVE-2024-5223	The Post Grid Gutenberg Blocks and WordPress Blog Plugin – PostX plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's file uploading feature in all versions up to, and including, 4.1.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2024-5220	The ND Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's upload feature in all versions up to, and including, 7.5 due to insufficient input sanitization and output This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2024-5218	The Reviews and Rating – Google Reviews plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's file upload feature in all versions up to, and including, 5.2 due to insuffi t sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an

D

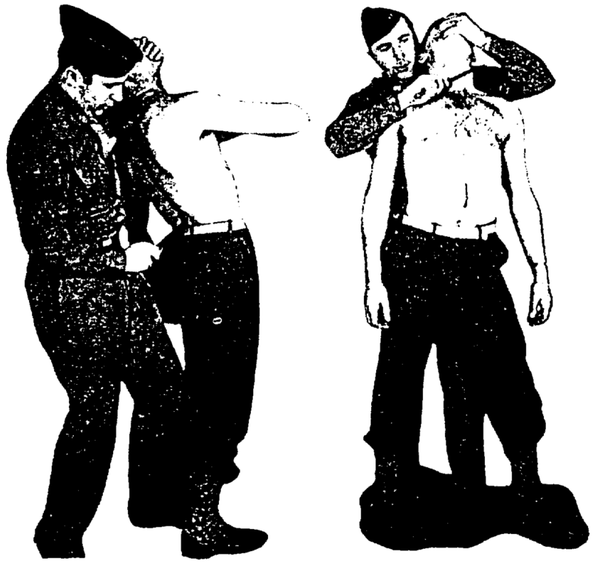
Illegális tartalmak publikálása feltört weboldalakon

Kill or get killed

http://3yryua3n3eu3i4gih2iopzph.wpengine.netdna-cdn.com/wp-content/uploads/2016/07/pdf/Kill_or_Get_Killed.pdf

for which there is no defense if the victim is taken by surprise. It is not unlikely that it will be used again, since many individuals, in all armies during World War II, received training in it, just as they received training in methods of strangulation.

In killing an enemy sentry, all factors regarding the approach and initial attack, described for use with a rear strangle, apply. The approach from the rear is naturally a noiseless one. At the time of rising, a few feet in the rear of the victim, the knife should be taken either from the sheath where it has been during the crawl, or from the teeth where it may have been carried. The attack is launched from a distance of



KILLING AN ENEMY SENTRY

This is the best method of surprise knife attack taught in the Armed Forces. Approach from the rear, grasp the nose and mouth with the left hand to prevent outcry, and thrust the knife into the kidney area, as shown at the left. After a short interval, withdraw the knife and cut the throat.

Inspire Magazine

https://www.oodaloop.com/wp-content/uploads/2014/03/Inspire-12.pdf

HINT

- You can use air from SCUBA cylinders.
- You can also use other fuels instead of propane, e.g. hydrogen, methane or acetylene.
- These fuels give better results, if security measures allow you to buy.


Tire Barometer

2. This tire barometer can measure up to 11 bars. We will use it in our procedure.


Regulator 2

3. The meter on the right measures a maximum of 25 atmospheres - almost equivalent to 25 bars, while the meter on the left measures a maximum of 2.5 atmospheres - almost equivalent to 2.5 bars.


Tire Barometer 2

4. This tire barometer can measure a maximum of 16 bars.

DID YOU KNOW?

that you can mix the two gases in the SCUBA Cylinder? An air cylinder can sustain more than 12 Cooking Gas Cylinders of 25-liters. BUT do not forget the balloon principle.

CAR BOMB PREPARATION:

1 - Mixing the Gases:

- Discharge gas from the Cooking Gas Cylinder until only 9 bars are left in it.
- Note: to be sure of the required amount, you have to measure the pressure after every few moment of releasing the gas. Use a barometer suitable for the cooking gas cylinder.
- Note: If you do not have the suitable barometer, there is a simple way to measure the pressure by a tire barometer (fig 1.1)
- Take a normal cooking gas regulator and cut its connecting nut off. Use a hacksaw to cut at the yellow mark. (fig 1.2)
- Take a tire's inner tube and cut the valve stem off, in such its lower part fits the nut. (fig 1.3
- Fit the valve stem into the nut precisely.
- Apply epoxy from the outside to provide a strong adhesion between the valve stem and the nut and prevent the gas from leaking. Also apply a little of epoxy inside - Do not block the hole. Now the nut is ready to use with the tire barometer and the Cooking Gas Cylinder. (fig 1.4


1.1. Tire Barometer

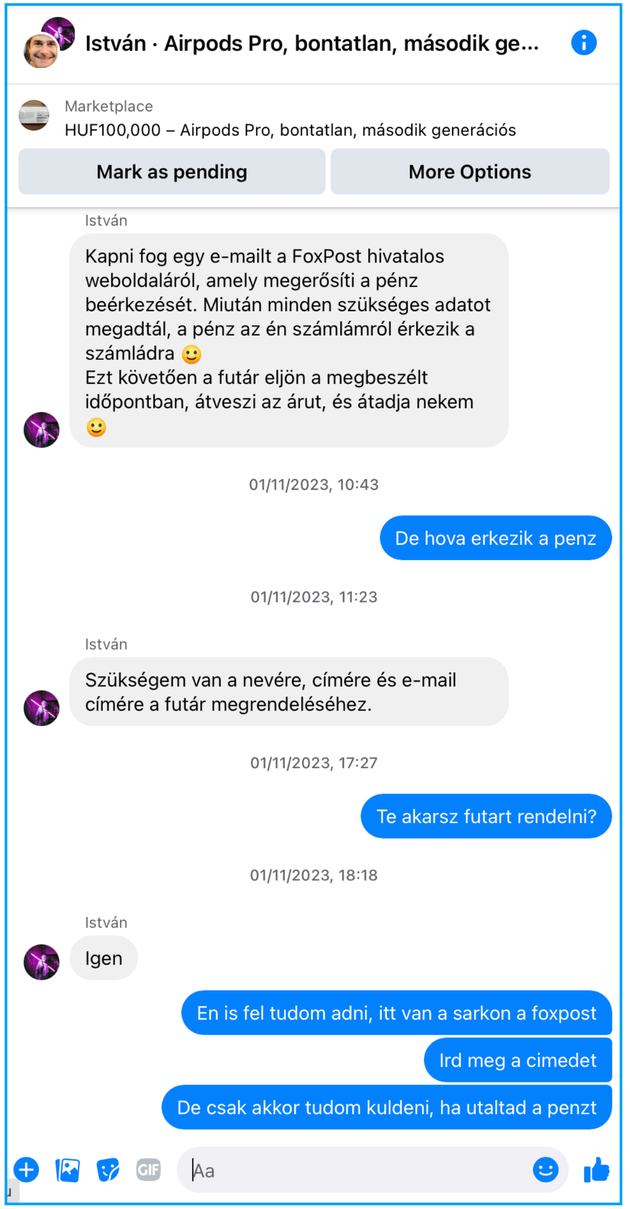

1.2. Cooking Gas Regulator


1.3. Nut and Valve


1.4. Final Result

Webshopok, piacterek

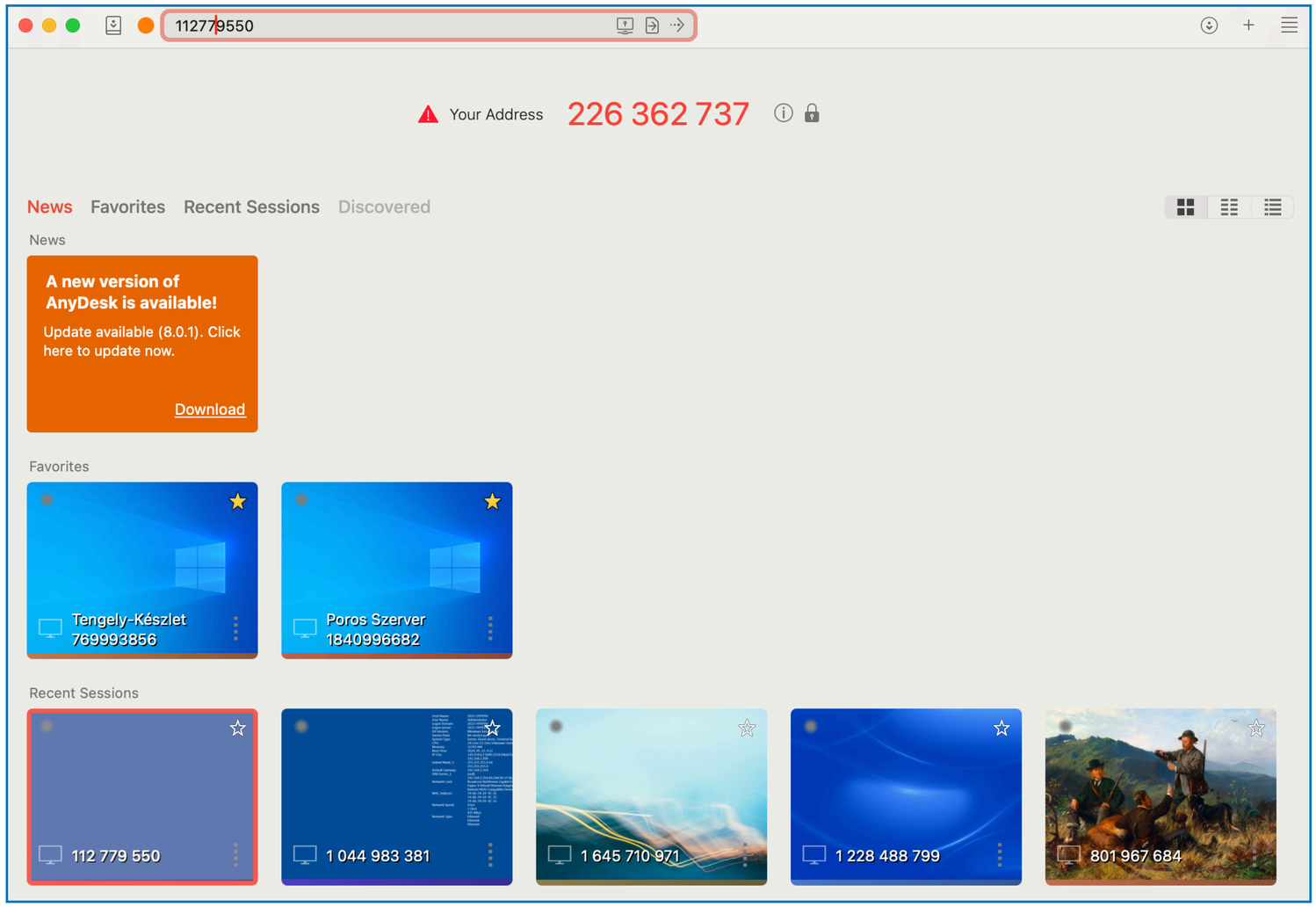
- Csaló webshopok
- Facebook piactér és chat
- Használt autókhoz kötődő csalások (https://totalcar.hu/magazin/kozelet/2017/02/07/sorozatcsalo_a_finn_kardiologus/)
- Gyanakodjunk, ha:
  - Túl szép, hogy igaz legyen: ismert márkákat, drága munkavédelmi termékeket, szoftver licensz kódokat különlegesen olcsón árulnak.
  - Ha a weblap gyenge minőségű.
  - Ha kétesek a fizetési lehetőségek.
  - Sürgetés: már csak néhány darab érhető el.
  - A domain név gyanús, vagy nemrég regisztrálták.
- Kép eredetiségének ellenőrzése.



Banki csalások

A támadó banki munkatársnak adja ki magát, rendszerint telefonhívás során próbálja meg rávenni a felhasználót, hogy a gépén a banki alkalmazásba beléphessen.

- Nem csak bankszámlákat, hanem más, pl. szép kártya vagy állampapír számlákat is támadnak.
- Az internetes telefonszolgáltatók bármilyen hívószámot kijelezhetnek.
- Tipikus elem, hogy nem a banki hozzáférés kódját, hanem más kódot kérnek: Anydesk, Teamviever vagy más távoli vezérlésre alkalmas szoftver telepítésére veszik rá a felhasználót, amit vírusvédelemnek vagy banki biztonsági szoftvernek neveznek.



Álhírek



A sajtó esete a szír repülővel

BOTRÁNY!
A SZÍR ELNÖK TITOKBAN BUDAPESTRE MENEKÜLT!
AZ ILLETÉKESEK TAGADNAK!

- Céljuk elsősorban politikai befolyásolás, gazdasági haszon vagy a társadalmi megosztás.
- Clickbait oldalak.
- https://alhirvadasz.hu/
- Google képkereső használata egy kép eredetijének, vagy további példányainak megkereséséhez.
- A szír repülőgép eredetije egy 2012-es videóból származik:
  - A hír: https://szmsz.press/2024/12/08/magyar-hang-titokzatos-szir-repulo-erkezett-ferihegyre/
  - https://globoplay.globo.com/v/2183074/
  - https://www.mako.co.il/news-world/arab/Article-d5e91dc0a9e4a31004.htm



Kártékony szoftverek



Co-funded by the
European Union

Kártékony szoftverek



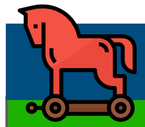
Vírusok

Programok, amelyek képesek önmaguk reprodukálására — ennek gyakori formája, hogy egy fertőzött fájlt megnyitásakor, a vírusprogram további, később megnyitott a fájlokba vagy programokba is beágyazódik.



Férgek

Önállóan terjedő programok, amely a hálózati kapcsolatokon keresztül vagy adathordozók cseréjével képesek más számítógépekbe is átjutni, esetenként akár emberi közreműködés nélkül is.



Trójai falovak

Programok, melyek gyakran valamilyen hasznosnak tűnő alkalmazás formájában kerülnek a gépre, de különböző károkat okozó rejtett kódot tartalmaznak: például adatokat lophatnak vagy hátsó ajtókat (backdoor) nyithatnak a rendszeren.



Kémprogramok

Olyan programok, melyek titokban információkat gyűjtenek a felhasználóról vagy a rendszeréről: tipikusan jelszavakat, e-maileket, pénzügyi adatokat keresnek meg és továbbítják a támadónak.



Reklámprogramok

Reklámokat jelenítenek meg a felhasználó számítógépén, vagy a böngésző felugró ablakaiban. Bár az adware önmagában nem feltétlenül ártalmas, gyakran erőforrásokat használ és zavarja a felhasználót.



Rootkit

Olyan szoftver, amelyek lehetővé teszi egy támadó számára, hogy a behatolást követően rejtve maradjon és fenn tudja tartani a teljes hozzáférését. Egy sikeres betörést követően a támadók gyakran telepítenek ilyet.



Zsarolóprogram

Olyan kártevő, amely titkosítja a felhasználó fájljait, és váltságdíjat követel a visszafejtési kulcsért. Gyakran komoly kárt okoz, mert minden fájlt használhatatlanná tesz, amelyhez hozzáfér.



Botnet

Fertőzött számítógépekből álló hálózat, amelyeket egy támadó távolról irányíthat, és így használják szolgáltatásmegtagadásos támadásokra, kéretlen levelek küldésére, vagy egyéb illegális tevékenységekre.

Vírusok

- A legrégebbi kártékony programok, eleinte mágneslemezeken terjedtek. 1982-ben írta egy középiskolás diák az Egyesült Államokban.





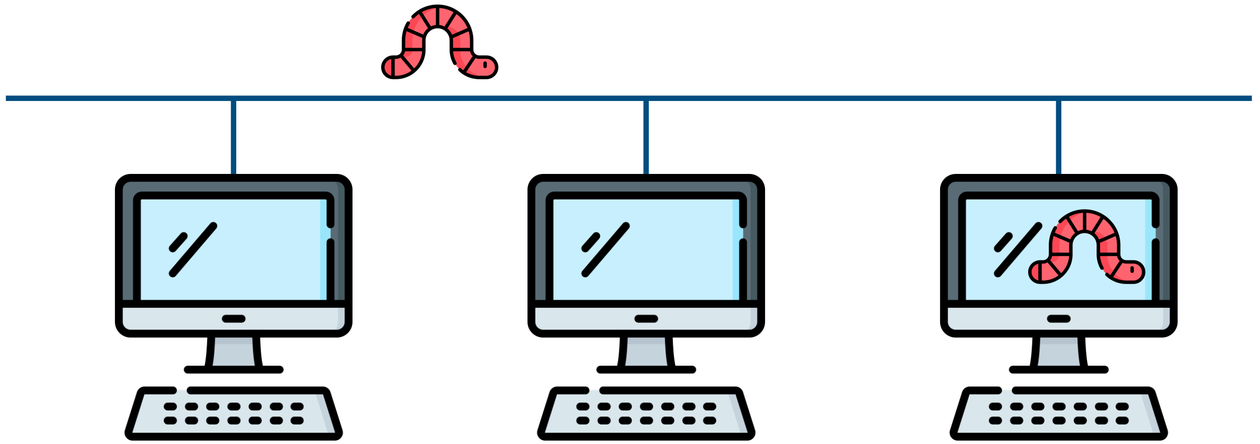
- A legváltozatosabb károkozási műveleteket hajtják végre (verseléstől a törlésig).
- Védekezés vírusvédelmi rendszerekkel.
- MAC-re és Linuxra tényleg nem kell vírusvédelem?
- Miért nincs iPhone-ra?





Férgek

- Olyan szoftverek, amelyek önállóan terjedni képesek a hálózaton belül.
- Kihasználják az egyes gépek sebezhetőségeit.
- Céljuk szintén a károkozás.
- WannaCry (2017): Ez egy zsarolóprogram-féreg, amely a hálózati sebezhetőségeket kihasználva terjedt el világszerte. A Windows rendszereket célozta, és több mint 200 000 gépet fertőzött meg több mint 150 országban.
- A frissítések fontosságáról.



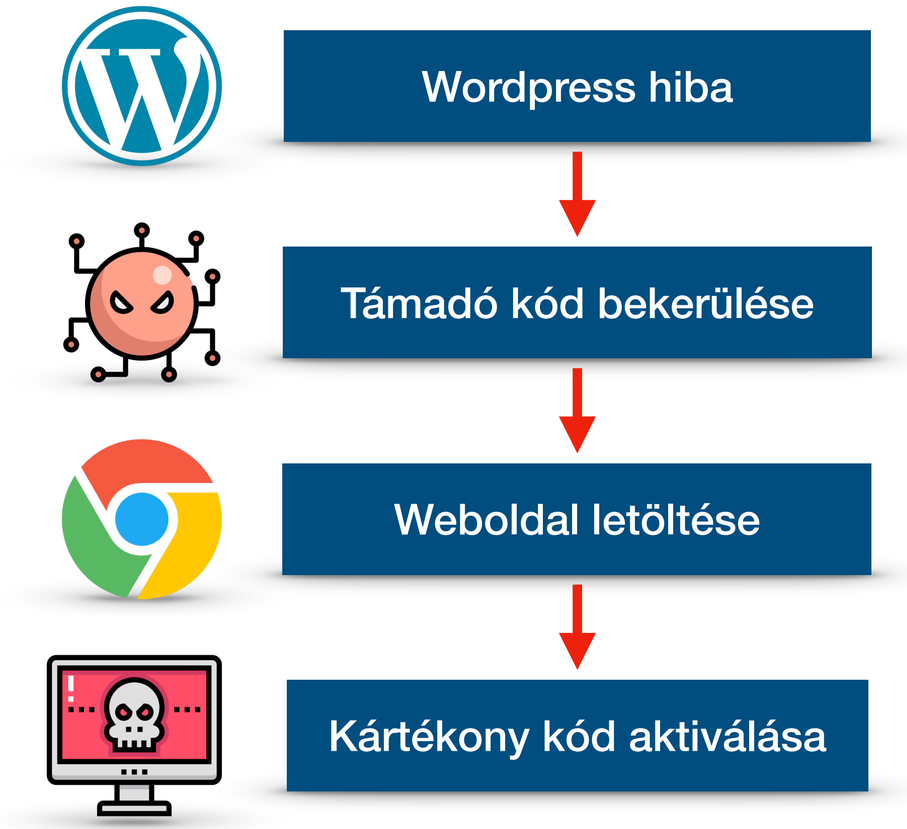


Trójai falovak

- Ártalmatlan vagy hasznos programoknak álcázzák magukat, de valójában rosszindulatú tevékenységeket hajtanak végre, miután telepítették őket.
- Tipikusan mobilokon fordulnak elő.
- Nem képesek önállóan terjedni, mint például a férgek vagy a vírusok.
- Nem másolják magukat.
- Óvatosan a böngészők bővítményeivel!
- Trójai sztori az AIDS-szel.
- Zsarolóvírusok is ebbe a kategóriába tartozhatnak.
- Védekezés: ne indítsunk el ismeretlen forrásból származó programokat!

Kémprogramok (spyWare)

- titokban figyelik és gyűjtik a felhasználók adatait és tevékenységeit a számítógépen vagy más eszközön.
- Tipikus célok:
  - Böngésző előzmények
  - Tárolt jelszavak
  - Bankkártya adatok
  - E-mailek, címjegyzék, jelszavak
  - Alkalmazások használata
- Tipikusan fertőzött weboldalakról vagy e-mail mellékletből kerülnek be
- Hamis böngésző frissítéseknek álcázzák magukat
- shop.hak5.org: OMG kábel és szoftveres változataik.
- Zero Day sérülékenységek





Reklámprogramok - Adware

- Hirdetéseket jelenítenek meg, gyakran ingyenes szoftverekbe ágyazva. (Itt az ingyenes programhoz való hozzáférésért cserébe kell hirdetéseket olvasni.)
- Egyes változatai ártalmatlanok, mások komoly zavaró tényezők lehetnek, sőt, néha rosszindulatú tevékenységeket is végezhetnek.
- Példa: https://angol-magyar-szotar.hu/

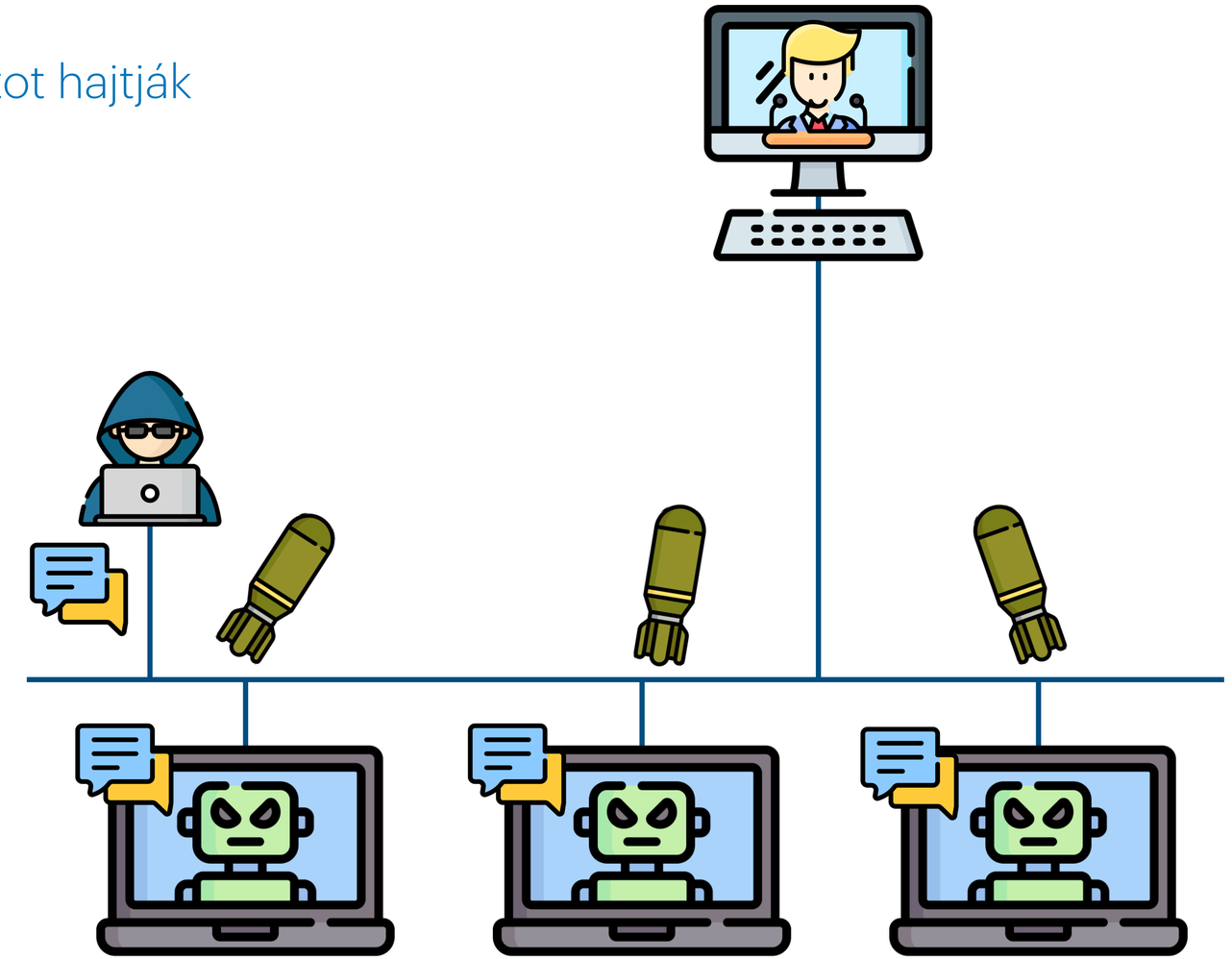


Rootkitek

- Olyan rosszindulatú szoftverek vagy eszközök, amelyeket arra terveztek, hogy a megtámadott számítógépen teljes hozzáférést biztosítsanak a támadóknak.
- Hátsó ajtó.
- Ha egyszer egy támadó megszerezte a kontrolt, valószínűleg ilyet telepít.
- Önállóan nem detektálhatók, a rendszer egyes részeit cserélik le.
- Frissítetlen számítógépekbe, vagy felhasználói interakcióval kerülnek be a gépekre.
- Csak a rendszer teljes újratelepítésével szabadulhatunk meg tőlük.

Botnet

- Számítógépekre olyan programok települnek, melyeket a támadó irányít.
- Adott jelre a gépek a meghatározott feladatot hajtják végre
- Torrent áruház crack-jei.



Zsarolóvírusok

Hogyan védekezzünk?

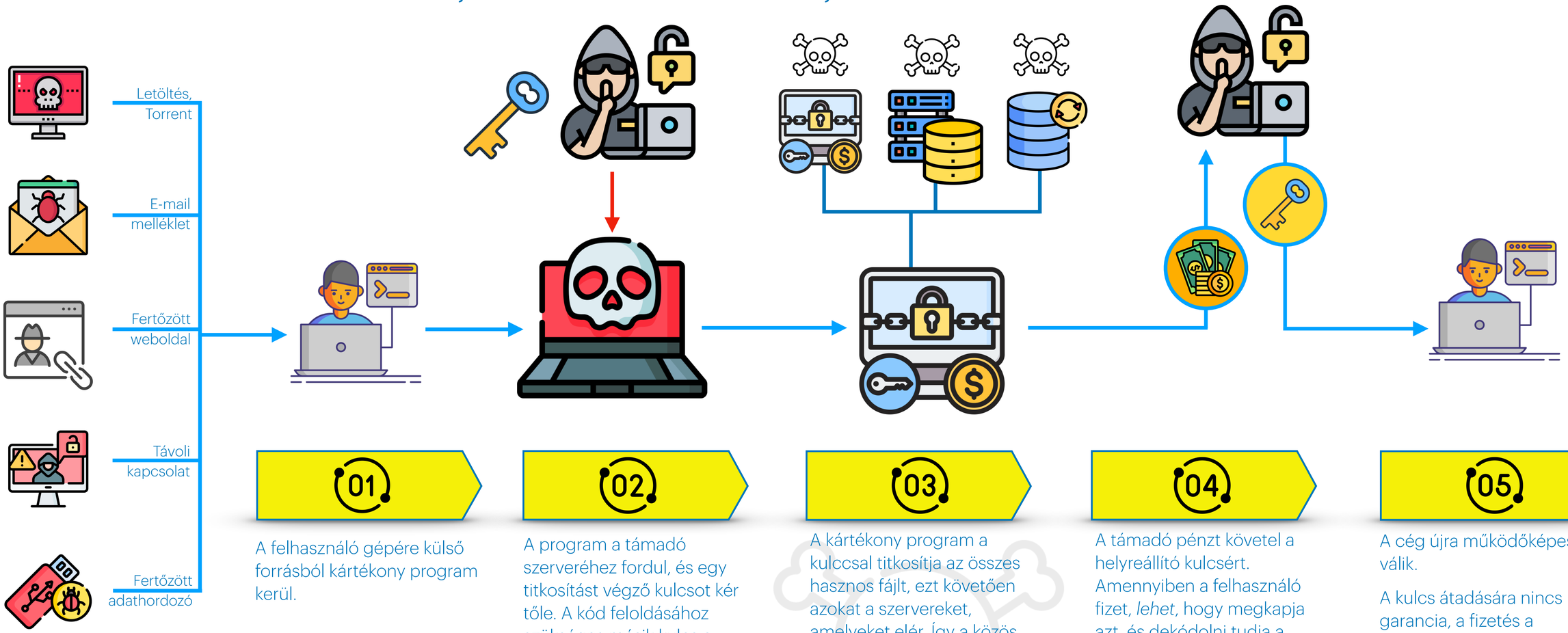
- Ha a titkosítási folyamat végbement, akkor csak a mentés segít.
- A mentő berendezések ne legyenek állandó kapcsolatban a géppel (eltávolítható merevlemez, távoli “húzó” mentési eljárás)
- A vírusvédelmi rendszerek tapasztalataim szerint ez ellen nem hatásosak.
- Ha nincs mentés, esetleg meg lehet próbálni a fizetést:
  - Magas ár.
  - Rendszerint Bitcoinban kell fizetni.
  - Semmilyen garancia nincs a helyreállító kulcs megküldésére.
- A folyamat legtöbbször e-mail mellékletre kattintással indul el.
- A titkosítási folyamat lassú, ha észrevesszük, hogy fájlok kiterjesztése megváltozik, azonnal áramtalanítsunk mindent, ne csak a gépet, hanem a szervereket is. Ezzel a titkosítási folyamat leáll.





Zsarolóvírusok

Az informatikai biztonság alapvető eleme a titkosítás. Az erős titkosítási módszereket használják ki a zsarolóvírusok terjesztői.



01

A felhasználó gépére külső forrásból kártékony program kerül.

02

A program a támadó szerveréhez fordul, és egy titkosítást végző kulcsot kér tőle. A kód feloldásához szükséges másik kulcs a támadónál marad.

03

A kártékony program a kulccsal titkosítja az összes hasznos fájlt, ezt követően azokat a szervereket, amelyeket elér. Így a közös fájlszervereket, mentéseket. A folyamat végén az IT infrastruktúra használhatatlan lesz.

04

A támadó pénzt követel a helyreállító kulcsért. Amennyiben a felhasználó fizet, *lehet*, hogy megkapja azt, és dekódolni tudja a fájljait.

05

A cég újra működőképessé válik.

A kulcs átadására nincs garancia, a fizetés a tevékenység folytatására ösztönöz.

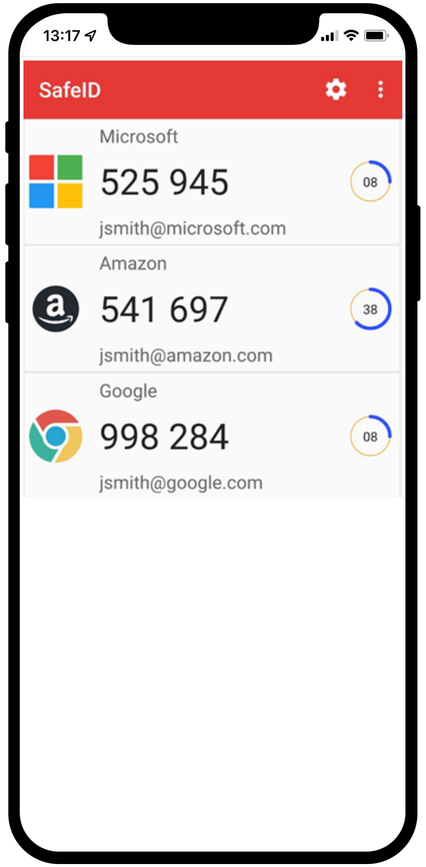
Azonosítás és jelszavak

Co-funded by the
European Union

Jelszavak

- A jelszavakkal kapcsolatos problémák kifejezetten gyakoriak.
- Jelszavak ismétlődése, erőssége, cseréje, feltörhetősége
- A haveIbeenpwned
- Titkosítatlan jelszó
- Többszörös használat
- A gyenge jelszavakat a támadók átveszik és megváltoztatják
- Többfaktoros és többlépcsős azonosítás
- Biometria, kártya, token, mobil
- Jelszó generálás

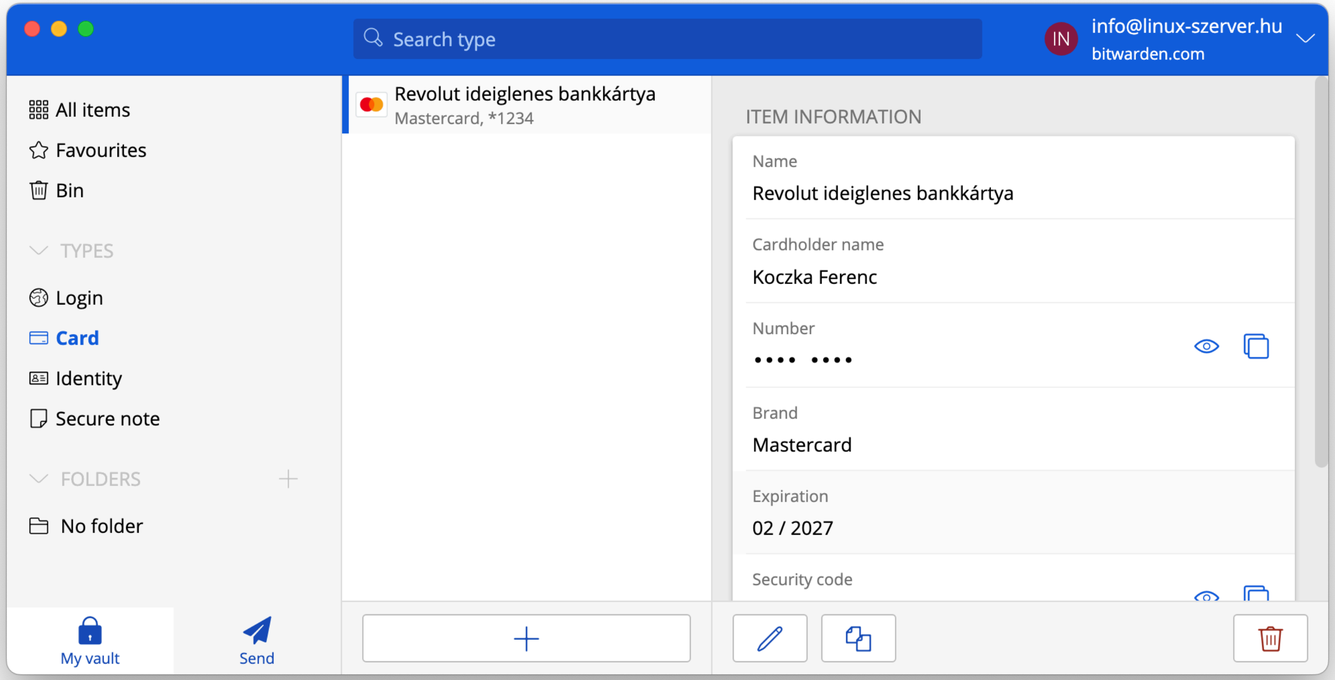


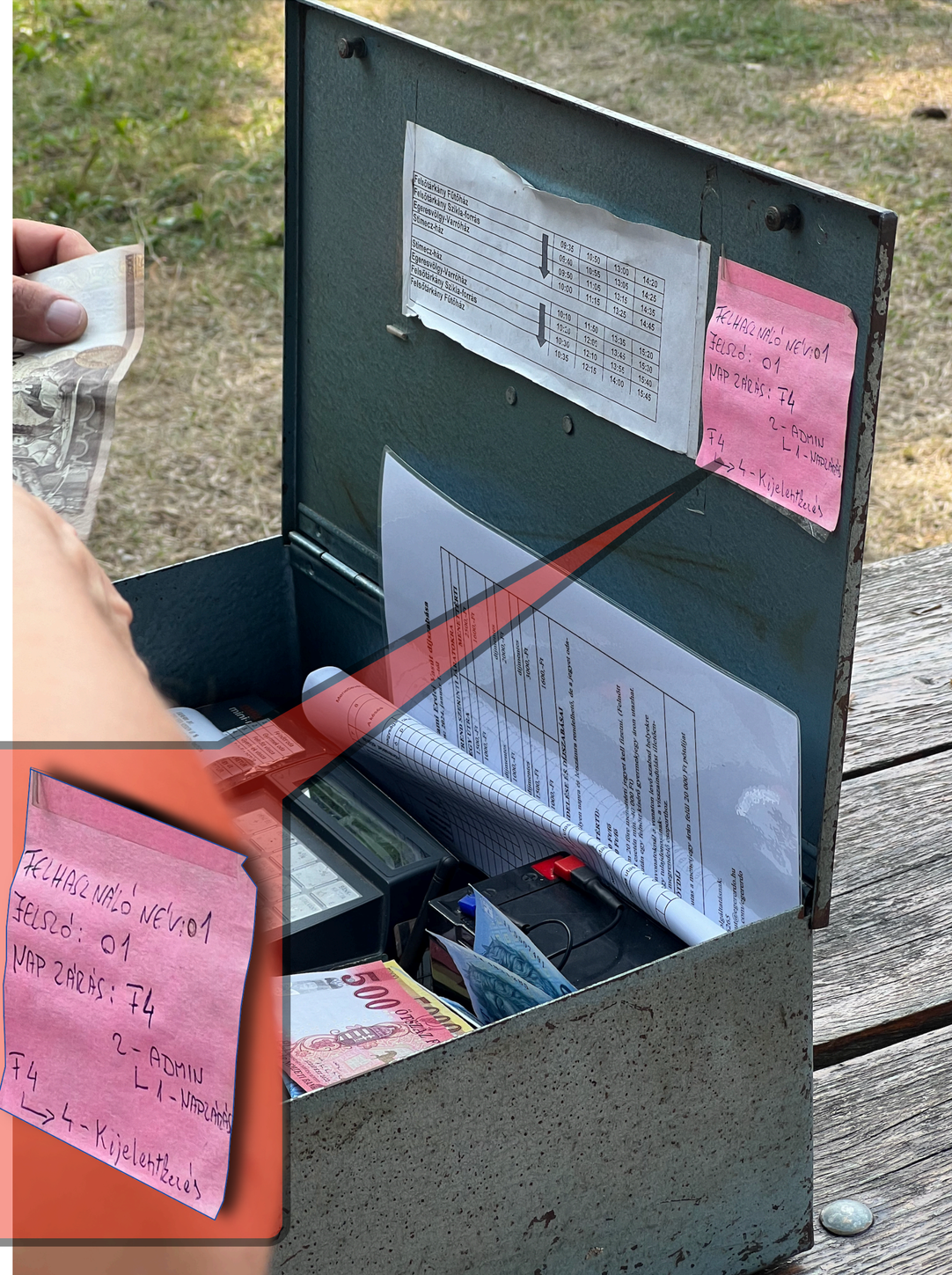




Hogyan jegyezzem meg?

- A jelszavak megjegyzése problémát jelent.
- Ha felírjuk, azt el kell zárni!
- Jelszószéfek alkalmazásának lehetősége. Ingyenes változat a Bitwarden.



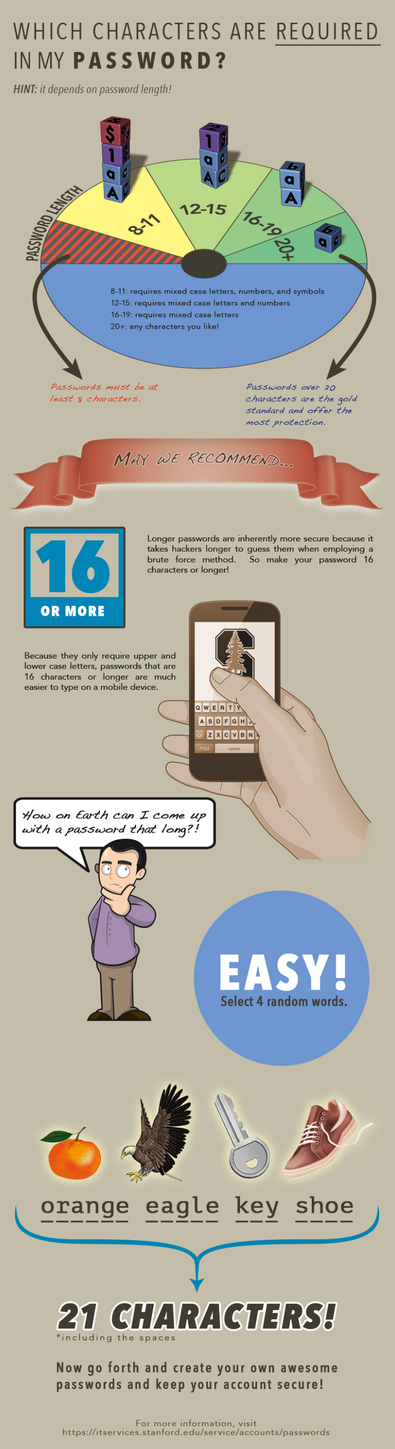


Jelszavak

Az ideális jelszó

- Hossza ..... 12 karakter
- Karakterei ..... kis- és nagybetűk, számok, írásjelek
- Cseréjének gyakorisága ..... 3 havonta
- Felhasználásának száma: 1

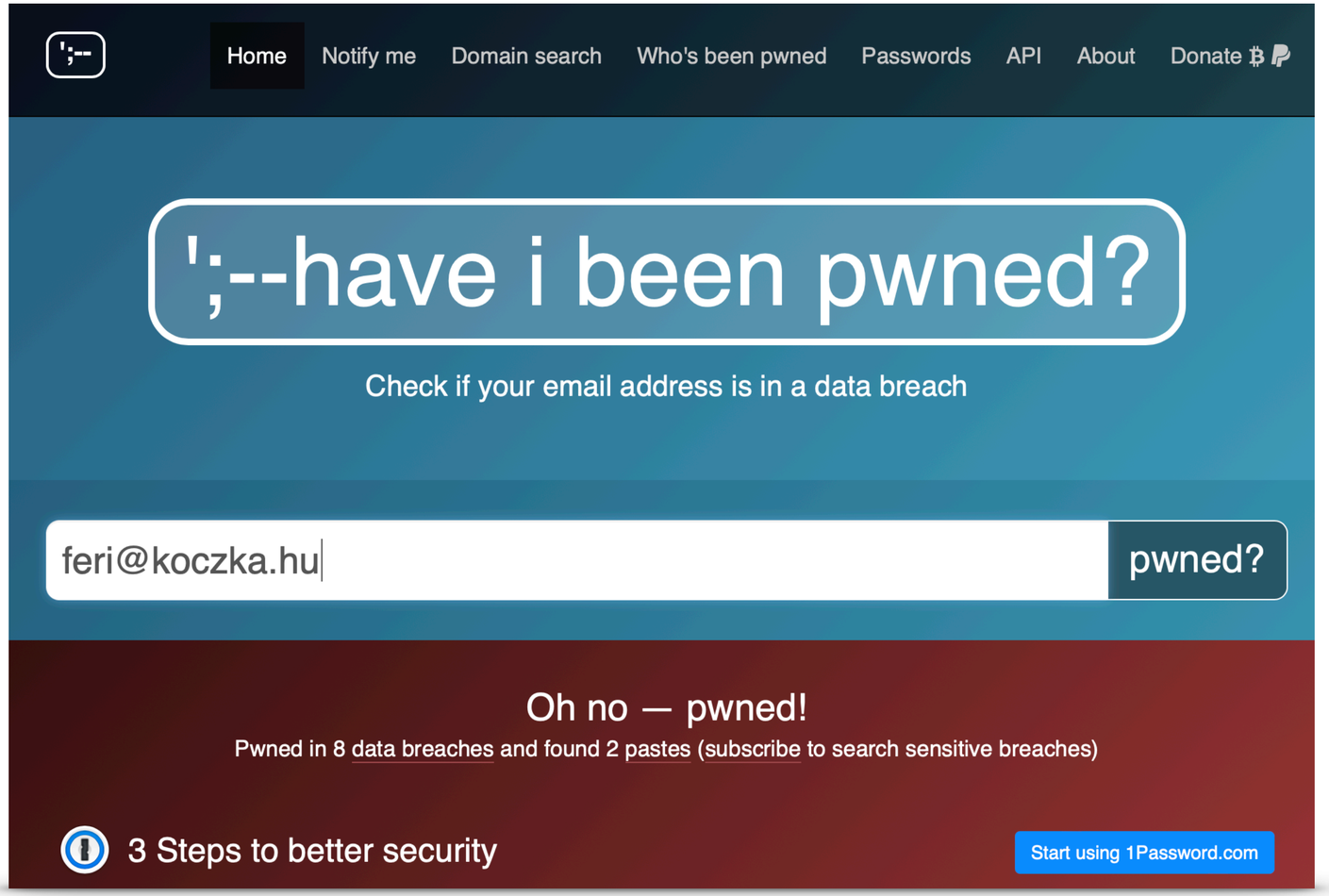
- https://uit.stanford.edu/service/accounts/passwords/quickguide





haveibeenpwned.com

- Különféle forrásból származó e-mail cím és jelszó adatbázis
- Több, mint 14 milliárd bejegyzést tartalmaz
- Találat esetén azonosítható a forrás. D



804	14,115,481,441	115,796	228,889,153
pwned websites	pwned accounts	pastes	paste accounts



Jelszavak feltörése

NTLM passwords	Jelszó hossza					
Futási idő	4	5	6	7	8	9
Default mask	~0s	~0s	~0s	23s	18m 35s	12h 41m
Teljes névtér	~0s	3s	2m 14s	3h 39s	Nem mértem	Nem mértem
Own mask 1	~0s	2s	5s	2m 34s	1h 54m	3d 5h
Own mask 2	~0s	~0s	19s	5m 40s	4h 8m	Nem mértem
Own mask 3	~0s	1s	19s	3m 13s	2h 18m	3d 21h

SHA1 passwords	Jelszó hossza				
	4	5	6	7	8
lehetséges variációk	$2{,}40\times10^{7}$	$1{,}68\times10^{09}$	$1{,}18\times10^{11}$	$1{,}02\times10^{12}$	$4{,}18\times10^{13}$
Futási idő	~0s	~2s	1m 6s	10m 55s	7h 24m
Találatok	2	11	21	22	414

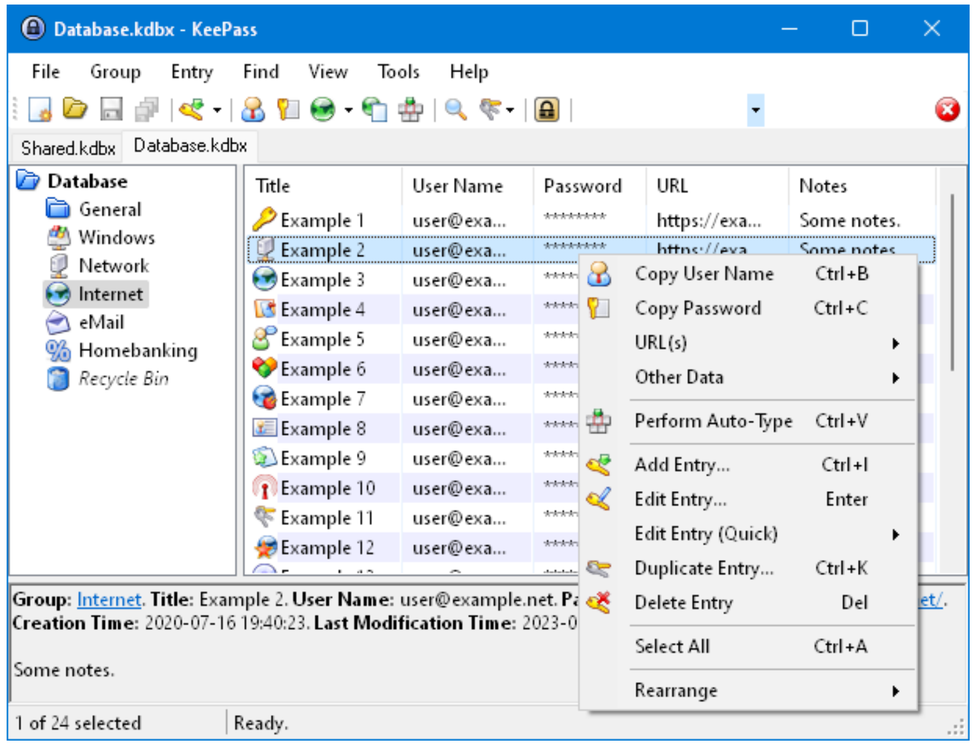


Jelszavak

```
root@fw.linux-szerver.hu:/var/log#
```

A jelszavak

- Ideális esetben minden alkalommal más jelszót kellene használnunk.
- Ez csak jelszómenedzserekkel valósítható meg, ami szintén bizalmi kérdés.



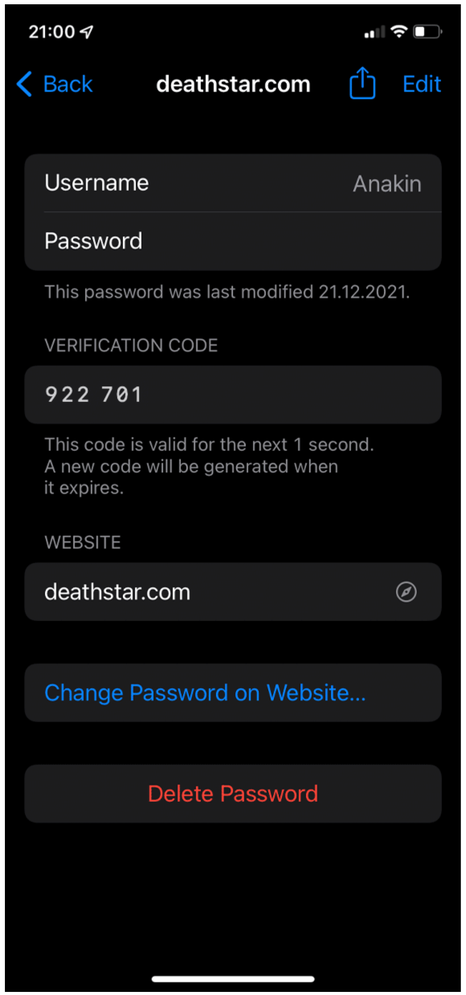


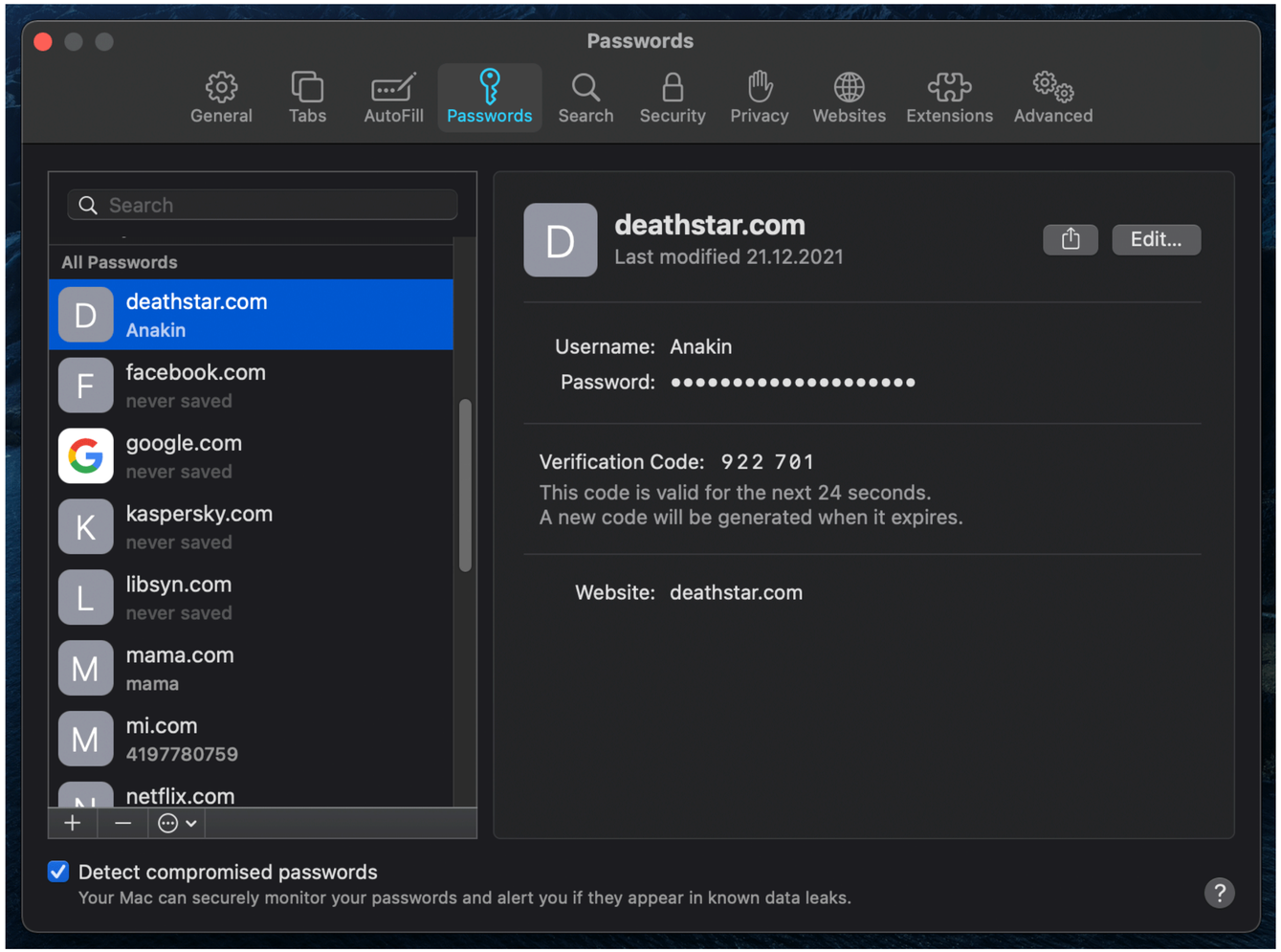
Which password managers have already hacked?
- https://password-managers.bestreviews.net/faq/which-password-managers-have-been-hacked/



A böngészők tárolják a jelszavainkat és egyéb adatainkat

- A böngészők titkosítás nélkül tárolják a jelszavainkat.
- Egyébként a böngészési előzményeket is.
- És a letöltött weboldal elemeket is.
- A privát mód némiképp segíthet ezen, de a védelem csak részleges.

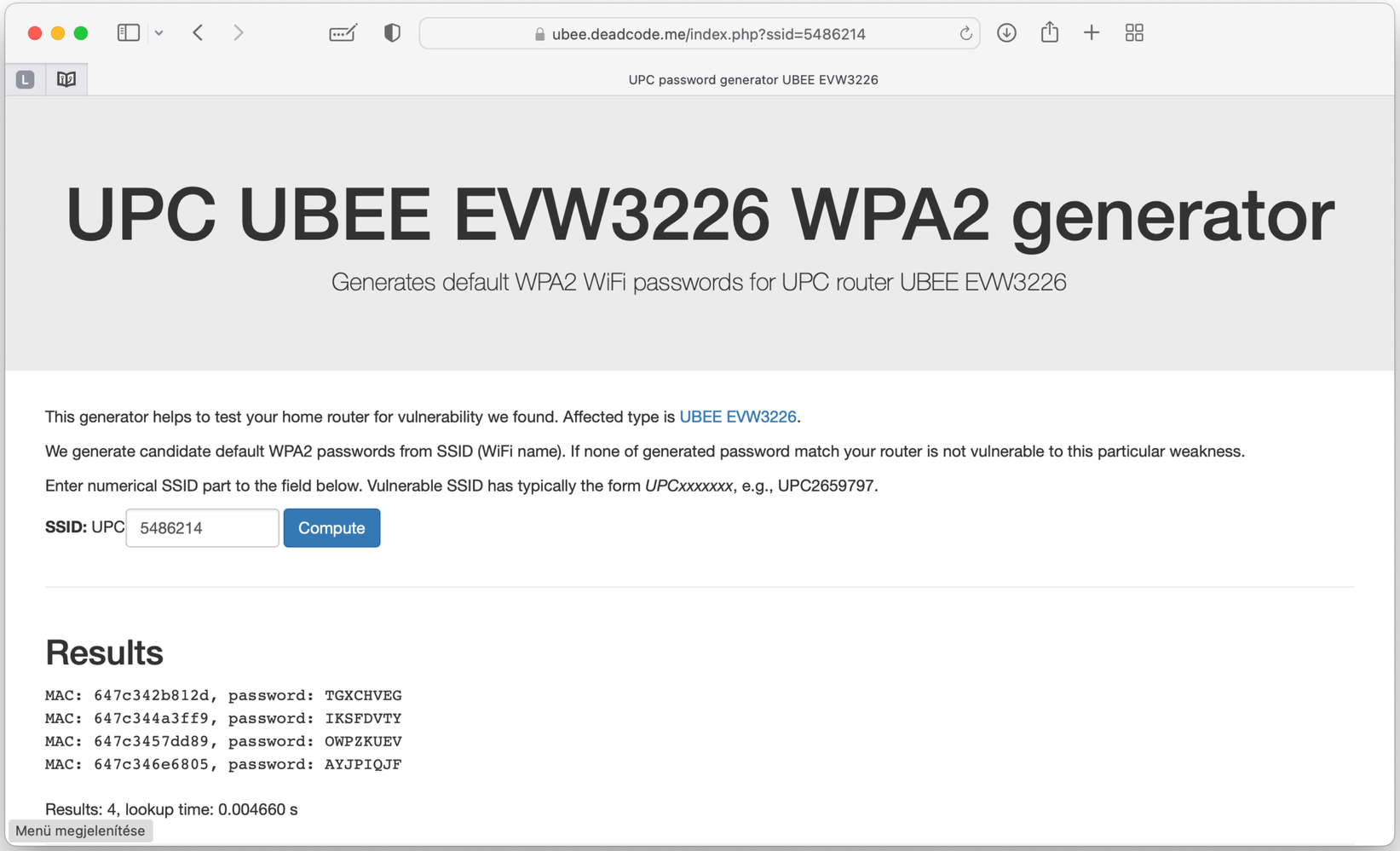






Kiszámítható jelszavak

- Egyes esetekben a rosszul megtervezett eszközök jelszavai kiszámíthatók.



Titkosítás, Titkosítás, Titkosítás!

index BAJNOKOK LIGÁJA

EUR 384,26 Ft ▼ USD 353,38 Ft ▼ GBP 451,44 Ft ▼
BUX 68 826 Ft ▼ OTP 17 655 Ft ▼ MOL 2 800 Ft ▼
12 °C 27 °C

BELFÖLD BRFK PENDRIVE ADATVÉDELEM ADAT

Elhagyott a BRFK egy pendrive-ot az összes munkatársuk személyes adatával

ZED

2019.07.12. 19:14

A Nemzeti Adatvédelmi és Információszabadság Hatóság 5 millió forintra bírságolta a Budapesti Rendőr-főkapitányságot, olvasható a hatóság határozatában,

UGYANIS ELVESZÍTETTEK EGY 4 GB-OS PENDRIVE-OT, AMIN MEGTALÁLHATÓ VOLT A BRFK TELJES NEVESÍTETT SZEMÉLYZETI ÁLLOMÁNYTÁBLÁJA, SZÜLETÉSI NÉV, SZÜLETÉSI IDŐ, ANYJA NEVE, TAJ SZÁM, BEOSZTÁS, MUNKAKÖR.

A főkapitányság munkatársa még januárban vitte magával a pendrive-ot egy értekezletre. Az adathordozót a kulcskarikájára fűzte, a kulcsot pedig magával vitte a szállodai szobájába. Másnap kijelentkezett a szállodából, majd egy rövid gyorsétteremi kitérő után visszatért a budapesti szolgálati helyére, ekkor vette észre:

> **NINCS MEG A PENDRIVE.**

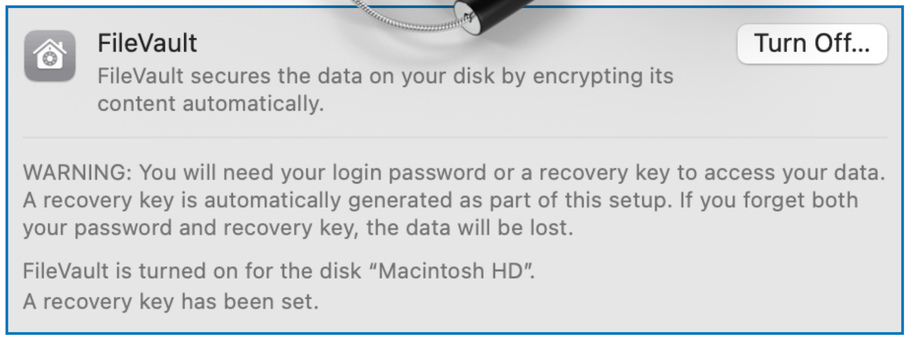
Még aznap jelentette az elöljárójának, hogy nyoma veszett az adathordozónak. Rögtön megindult a telefonálgatás az eltűnt pendrive után, felhívták a szállodát és a gyorsétteremet is, azonban mindhiába.

A pórul járt rendőr a személyes adatokat tartalmazó dokumentumokat nem a szolgálati, hanem magáncélra használt adathordozóra másolta át, és nem alkalmazott semmilyen biztonsági intézkedést a tárolt adatokkal kapcsolatban, ezért vele szemben fegyelmi eljárás indult. A pendrive azóta sem került elő.

Titkosított adathordozók

- Az elvesztett informatikai eszközök tartalmához a megtalálók hozzáférhetnek, ami nagyobb kár, mint az eszköz értéke. Ezért azokat az adathordozók, amelyeket a cég telephelyéről ki szabad vinni, titkosítani kell.
- Hardveres megoldás: titkosított pendrive.
- Windows Pro változatban: Bitlocker.
- Apple gépeken: fileVault.
- Általános felhasználásra: VeraCrypt.



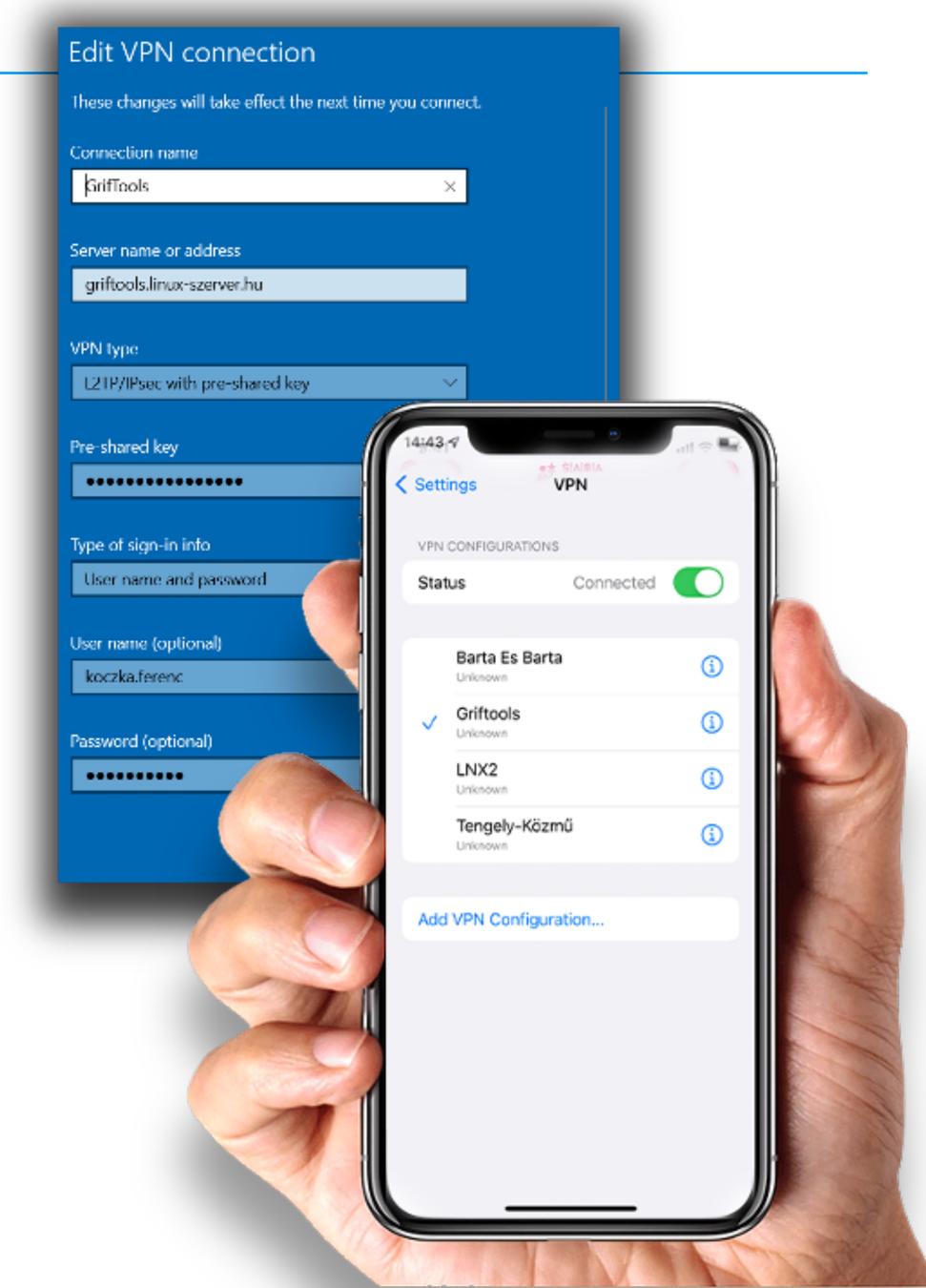


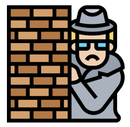


VPN

- Biztonságos kapcsolat a külső munkatársak és a cég belső hálózata közt.
- A mai routereken egyszerűen beállíthatók és nyomon követhetők.
- Mi is kapcsolódhatunk pl. az ExpressVPN-nel.







BYOD (Bring Your Own Device)

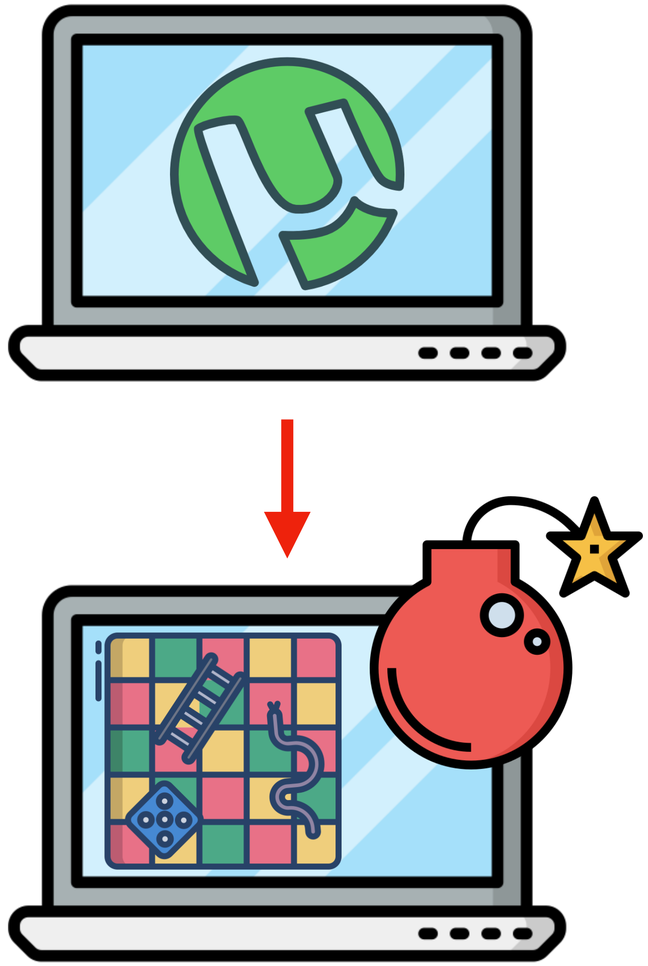


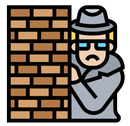
A munkatárs a saját eszközét használja a céges feladatok ellátására.

- A saját tulajdonú informatikai berendezéseken nem érvényesíthetők a céges biztonsági előírások.
- Gyakran a családtagok is ezt a gépet használják akár játékra is.
- A gépen levő kártevők bekerülhetnek a céges informatikai rendszerbe/ hálózatba.
- Különösen veszélyes, ha a a gépen torrent áruházból származó feltört (crackelt) programok működnek. Miközben a crack kiiktatja az adott program másolásvédelmét, megfertőzi a számítógépet is.
- Nem jellemző az otthoni hálózati eszközök frissítése.



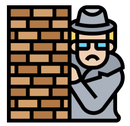
- Amennyiben lehetséges, a munkatársak használjanak céges tulajdonú, korlátozott hozzáférésű számítógépet és mobilnet kapcsolatot!





Frissítések

- Minden program hibás.
- A hibák javításai újabb hibákat hoznak.
- Nem biztos, hogy mindent javítani fognak: kivezetett szoftverek.
- Elavult rendszerek frissítése?
- CNC gépek frissítése?



Fizikai védelem

- Fizikai hozzáférés.
- Tűzvédelem.
- Lopás elleni védelem.
- Adathordozók ellopásának lehetősége.
- Saját adathordozóról indítás után könnyű lehet a hozzáférés megszerzése — titkosított adathordozó követelménye.



Adatok mentése

- Munkaállomások és szerverek mentése
- Kritikus számítógépek RAID diszkjei
- Ideális környezetben a munkaállomások nem tartalmaznak adatokat.
- Egyes esetekben (Abevjava) ez nehezen elkerülhető.
- A mentéseket titkosított adathordozón illik tárolni.
- Több változatot, mérföldköveket célszerű tárolni.
- Off-line mentések szerepe.
- A mentések kiszivárgása a teljes adatvagyon kiszivárgását jelenti!





Távozó munkatársak

- Hozzáférések megszüntetése:
  - E-mail (törölhető? személyes adatok?)
  - VPN kapcsolat
  - Fájlszerver
  - Telefonszám
  - Vezeték nélküli hálózati hozzáférések (vállalti megoldás, vagy közös jelszóhasználat?)
- Az informatikai szabályzat kell, hogy tartalmazza a szükséges eljárást.

Selejtezett eszközök

- A selejtezés során az adathordozók tartalmának törléséről gondoskodni kell!
- Az egyszerű törlés nem elégséges.
- Lemágnesező berendezések is elérhetők.
- Homok utcai számítógépek :-)

https://kiber.blog.hu/2021/02/26/adatok_a_szemetdombrol_tobbezer_egeszsegugyi_es_beteg_adat_vegezte_egy_hulladek_kontenerben

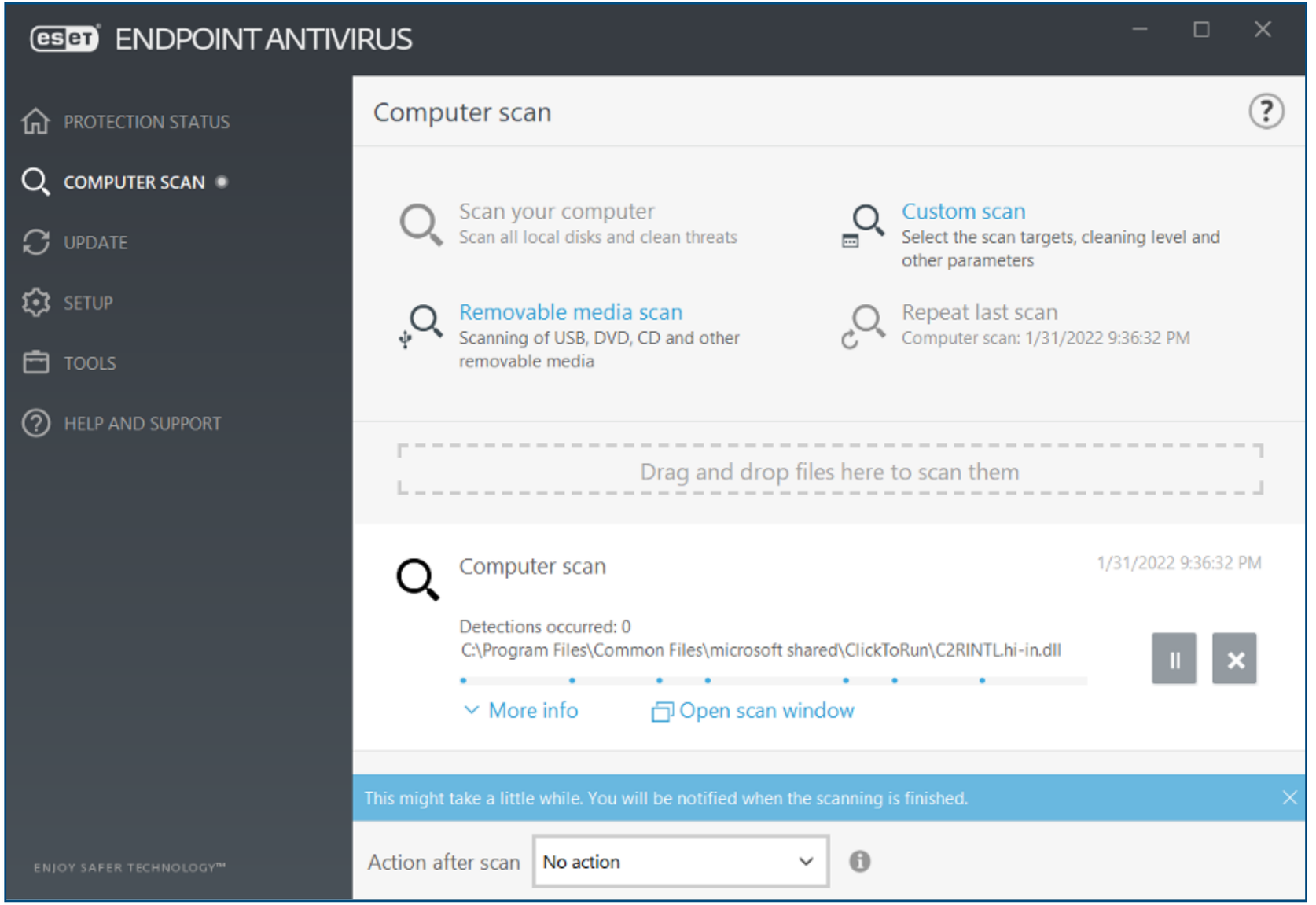


Védelmi eszközök

Co-funded by the
European Union

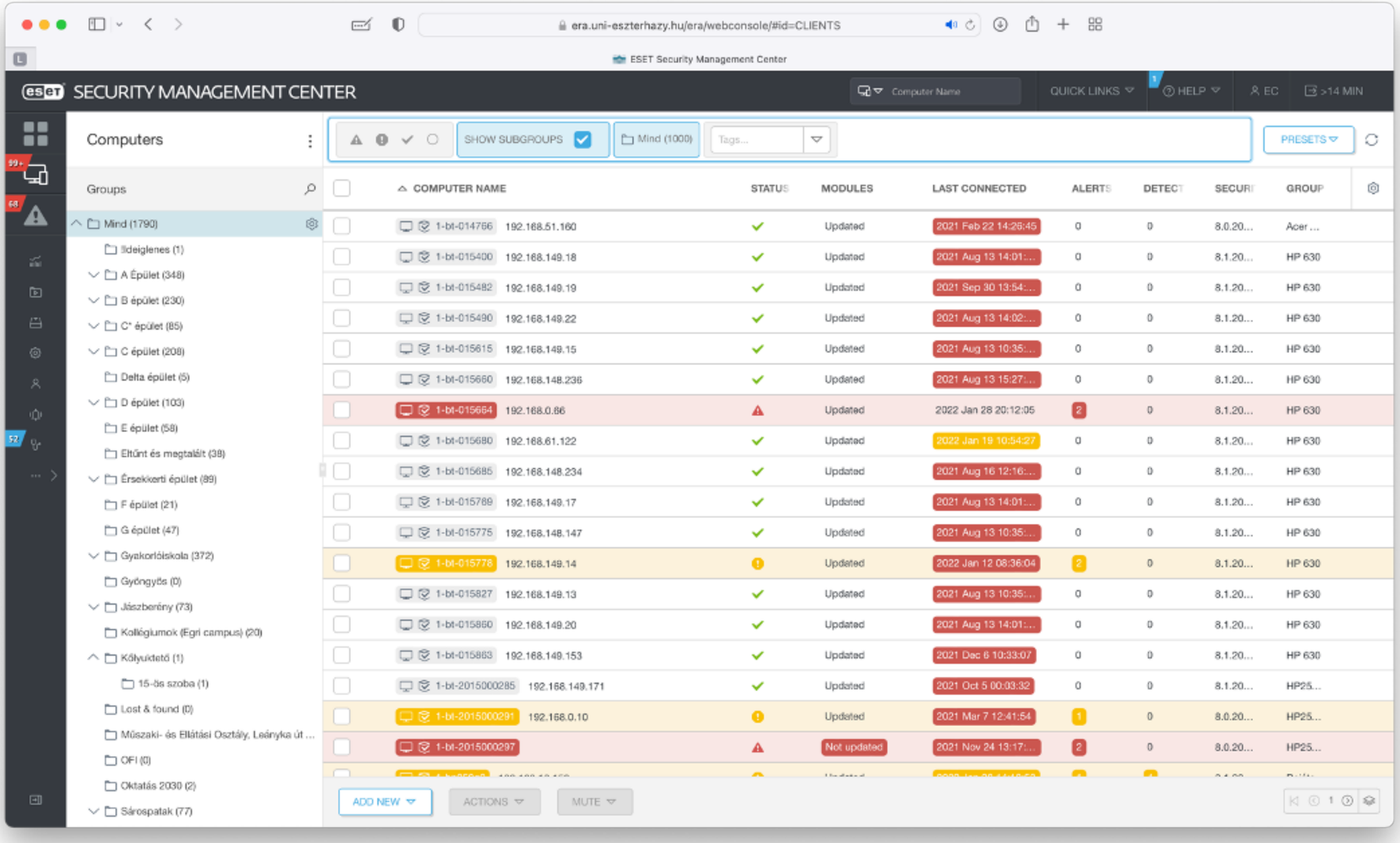
Kombinált vírusvédelmi rendszerek

- Vírusirtó a fájlrendszer valós idejű védelmére
- Kémprogram-ellenes modul
- Tömörített fájlok
- Kártevők eltávolítása
- Behatolás érzékelés
- Rootkit-felismerő modul
- Hálózatvédelem
- E-mail kliens védelem
- Tűzfal modul
- Szülői felügyelet
- Bankkártyás fizetés védelem



Centralizált vírusvédelmi rendszerek

- Egyes vírusvédelmi rendszerek nyilvántartják a hálózat gépeit és azok állapotát.
- Jelezhetik a sérülékenységeket, a védelem hiányát és a hardver változásait is.



Támadó és védelmi eszközök?

- shodan.io:
  city:eger product:"Hikvision IP Camera”

D

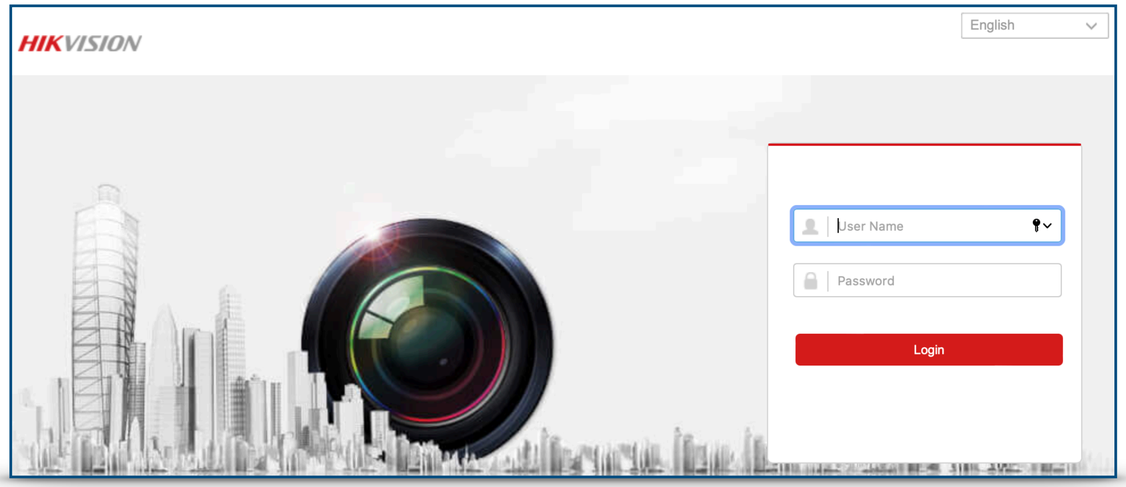
- http://176.63.94.161/

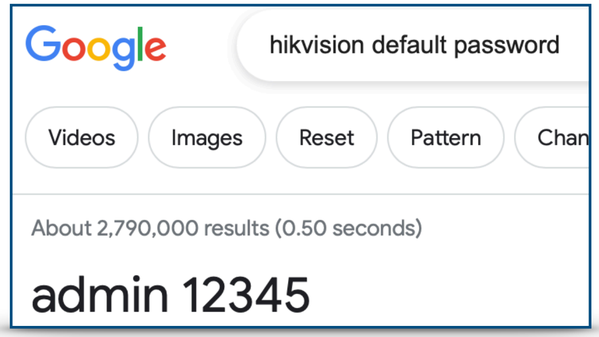
index

176.63.94.161
business-176-63-94-161.business.broadband.hu
Vodafone Hungary Ltd.
Hungary, Eger

```
HTTP/1.1 200 OK
Date: Fri, 09 Jun 2023 04:57:38 GMT
Server: App-webs/
ETag: "892-746-550a95c4"
Content-Length: 1862
Content-Type: text/html
Connection: close
Last-Modified: Thu, 19 Mar 2015 09:24:20 GMT


Hikvision IP Camera:
  Web Version: 3.1.3.150324
  Plugin Version: 3.0.5.38
  Activ...
```

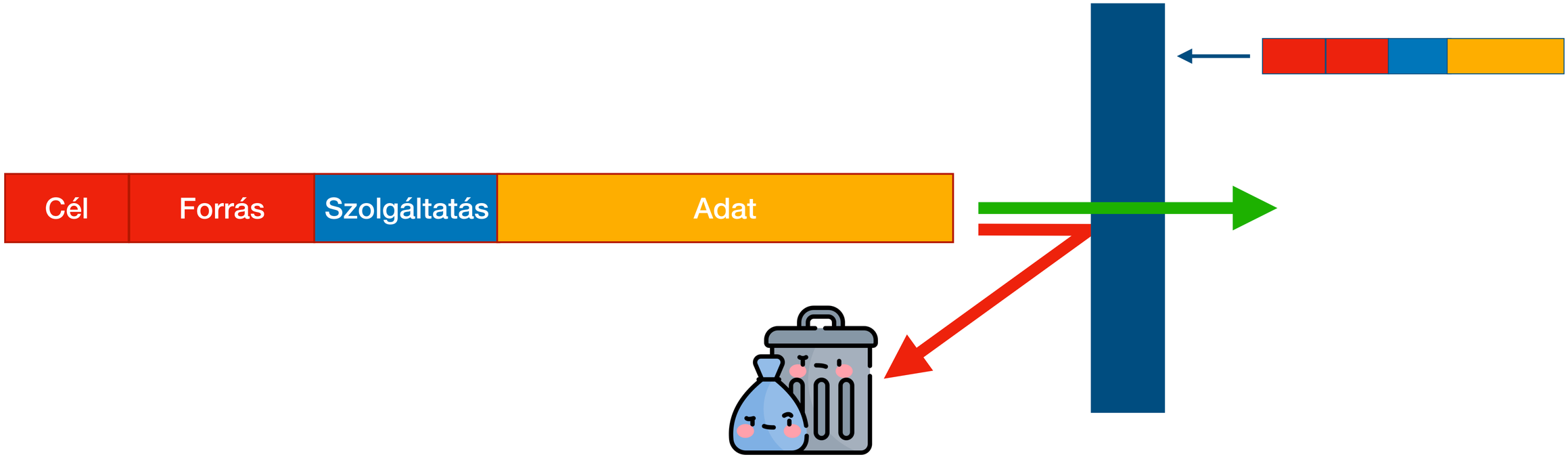




Tűzfalak

- A hálózati forgalom korlátozását szolgálják.
- Működhetnek a munkaállomáson és a központi eszközként is.
- Belső forgalom is korlátozható.
- Mikrotik demo. D







Wazuh

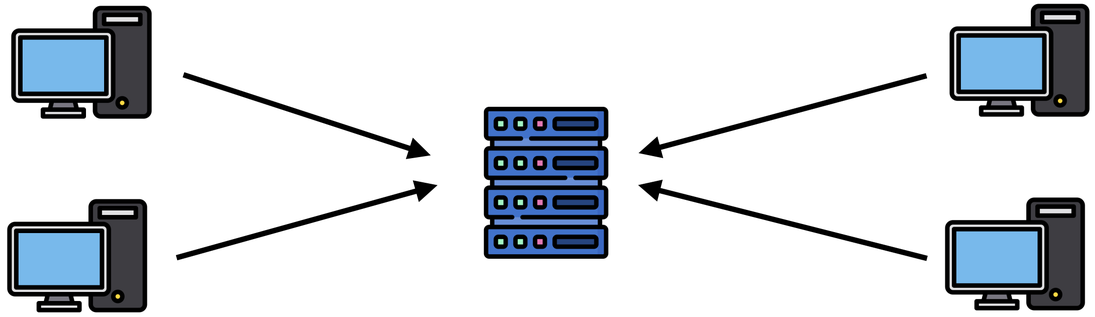
- Biztonsági események rögzítése:
  - Napi ellenőrzést feltételez
  - mitre.org azonosító, alkalmazott taktika azonosítása
  - biztonsági szabványok, keretrendszerek kapcsolódásai (pl. NIST 800-53)
  - Felhasználói aktivitás
- Javaslatot ad konfigurációs hibák javítására
- Munkaállomások és szerverek sérülékenységeinek detektálása
- Fájlrendszer változásainak detektálása

D

D

D

D





Wazuh

- Konfigurációs hibák azonosítása **D**

ID ↑	Title	Target	Result
19000	Ensure mounting of cramfs filesystems is disabled.	**Command:** modprobe -n -v cramfs	Passed
19001	Ensure mounting of freevxfs filesystems is disabled.	**Command:** /sbin/modprobe -n -v freevxfs	Passed
19002	Ensure mounting of jffs2 filesystems is disabled.	**Command:** /sbin/modprobe -n -v jffs2	Passed
19003	Ensure mounting of hfs filesystems is disabled.	**Command:** /sbin/modprobe -n -v hfs	Passed
19004	Ensure mounting of hfsplus filesystems is disabled.	**Command:** /sbin/modprobe -n -v hfsplus	Passed
19005	Ensure mounting of squashfs filesystems is disabled.	**Command:** /sbin/modprobe -n -v squashfs	Failed

Rationale

Removing support for unneeded filesystem types reduces the local attack surface of the system. If this filesystem type is not needed, disable it.

Wazuh

- Biztonsági események **D**

Security Alerts

Time ↓	Technique(s)	Tactic(s)	Description	Level	Rule ID
Apr 19, 2024 @ 13:47:34.821			The CVE-2024-2961 that affected locales was solved due to a package removal/update or a system upgrade	3	23502
Apr 19, 2024 @ 13:47:34.811			The CVE-2024-2961 that affected libc6 was solved due to a package removal/update or a system upgrade	3	23502
Apr 19, 2024 @ 13:47:34.801			The CVE-2024-2961 that affected libc-bin was solved due to a package removal/update or a system upgrade	3	23502
Apr 19, 2024 @ 12:55:26.710			New dpkg (Debian Package) installed.	7	2902
Apr 19, 2024 @ 12:55:24.719			Dpkg (Debian Package) half configured.	7	2904

Wazuh

- Sérülékenységek **D**

Vulnerabilities (98)

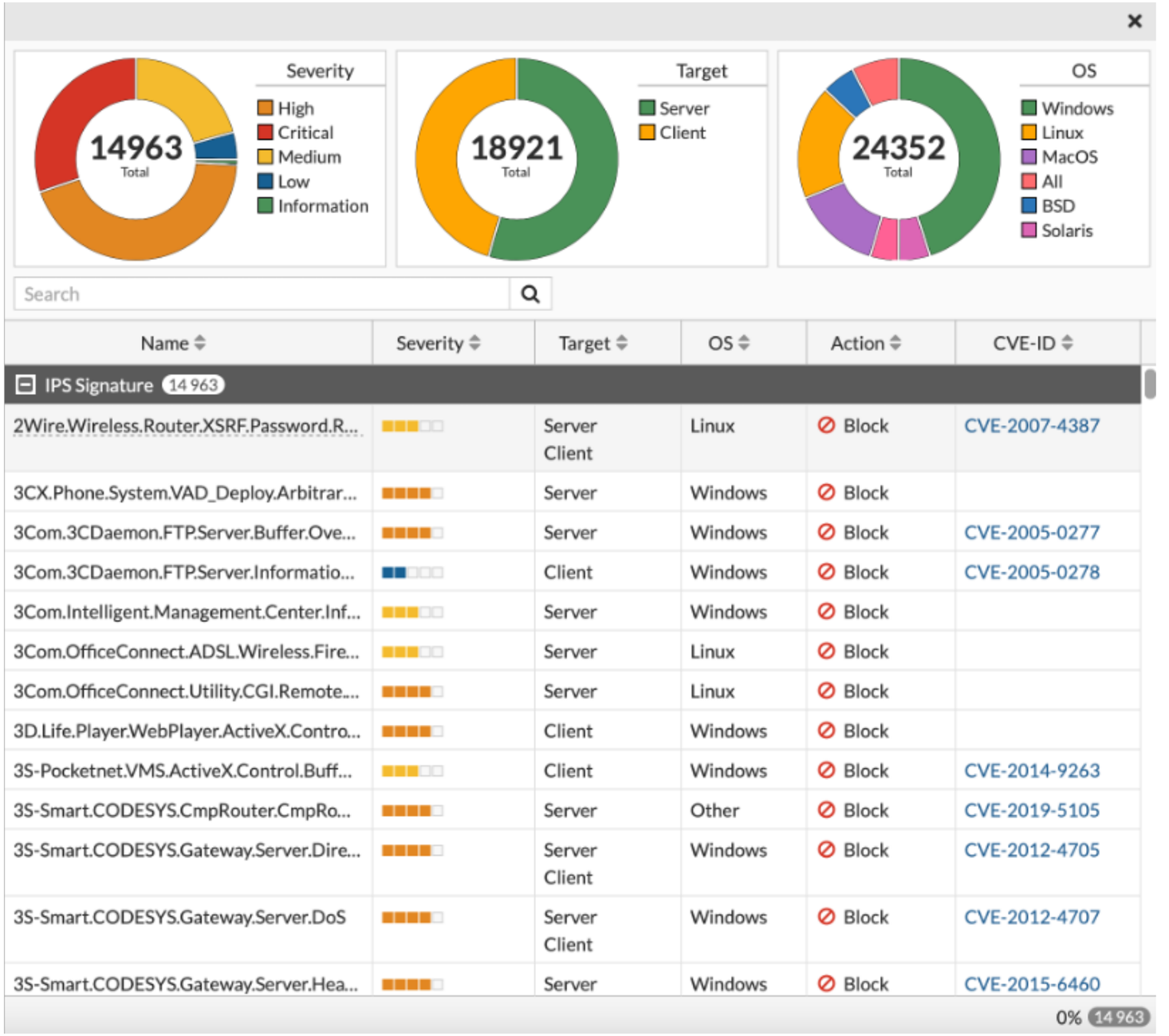
Refresh Export formatted

Search WQL

Name	Version	Architecture	Severity	CVE	CVSS2 Score	CVSS3 Score	Detection Time
apparmor	3.0.4-2ubuntu...	amd64	Critical	CVE-2016-1585	7.5	9.8	Dec 24, 2023 @ 22:05:27.000
apport	2.20.11-0ubun...	all	Low	CVE-2022-286...	0	0	Jul 29, 2023 @ 18:39:37.000
binutils	2.38-4ubuntu2.6	amd64	Medium	CVE-2022-480...	0	5.5	Mar 22, 2024 @ 20:52:15.000
binutils-common	2.38-4ubuntu2.6	amd64	Medium	CVE-2022-480...	0	5.5	Mar 22, 2024 @ 20:52:15.000
binutils-x86-64-linux-gnu	2.38-4ubuntu2.6	amd64	Medium	CVE-2022-480...	0	5.5	Mar 22, 2024 @ 20:52:15.000

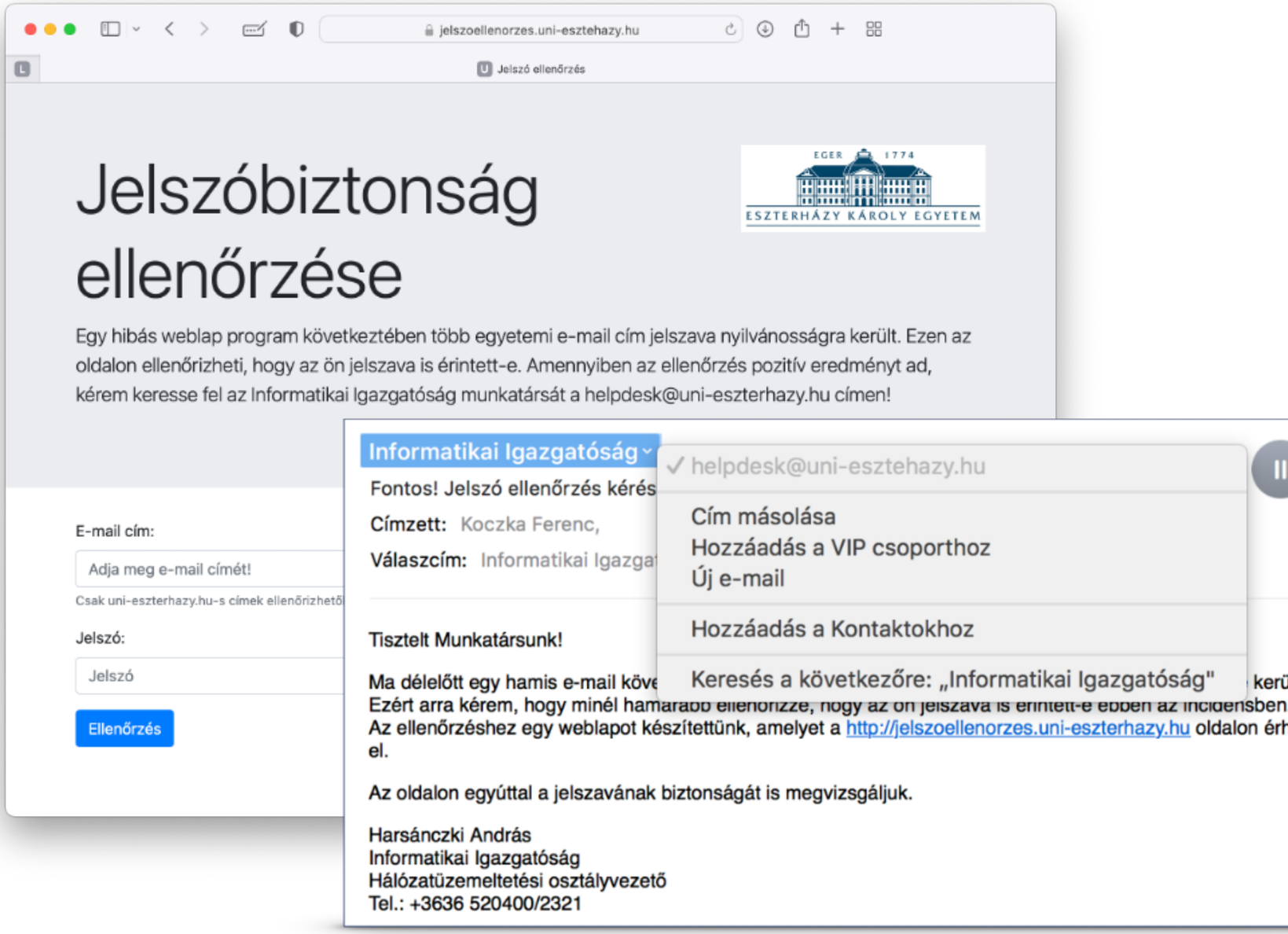
IDS/IPS

- IDS: (Intruder Detection System): az átfolyó forgalom folyamatos monitorozása.
- IPS: (Intrusion Prevention System): az átfolyó forgalom folyamatos monitorozása, kártékony adat esetén a forgalom megszakítása.



Munkatársak tesztelése

- A munkatársak “éberségének” ellenőrzése általunk küldött hamis levelekkel is ellenőrizhető.
- A kollégák együttműködésével a kényes helyzetek felismerhetők és megfelelően kezelhetők.
- A mérés során 304/1200 jelszót adtak meg.

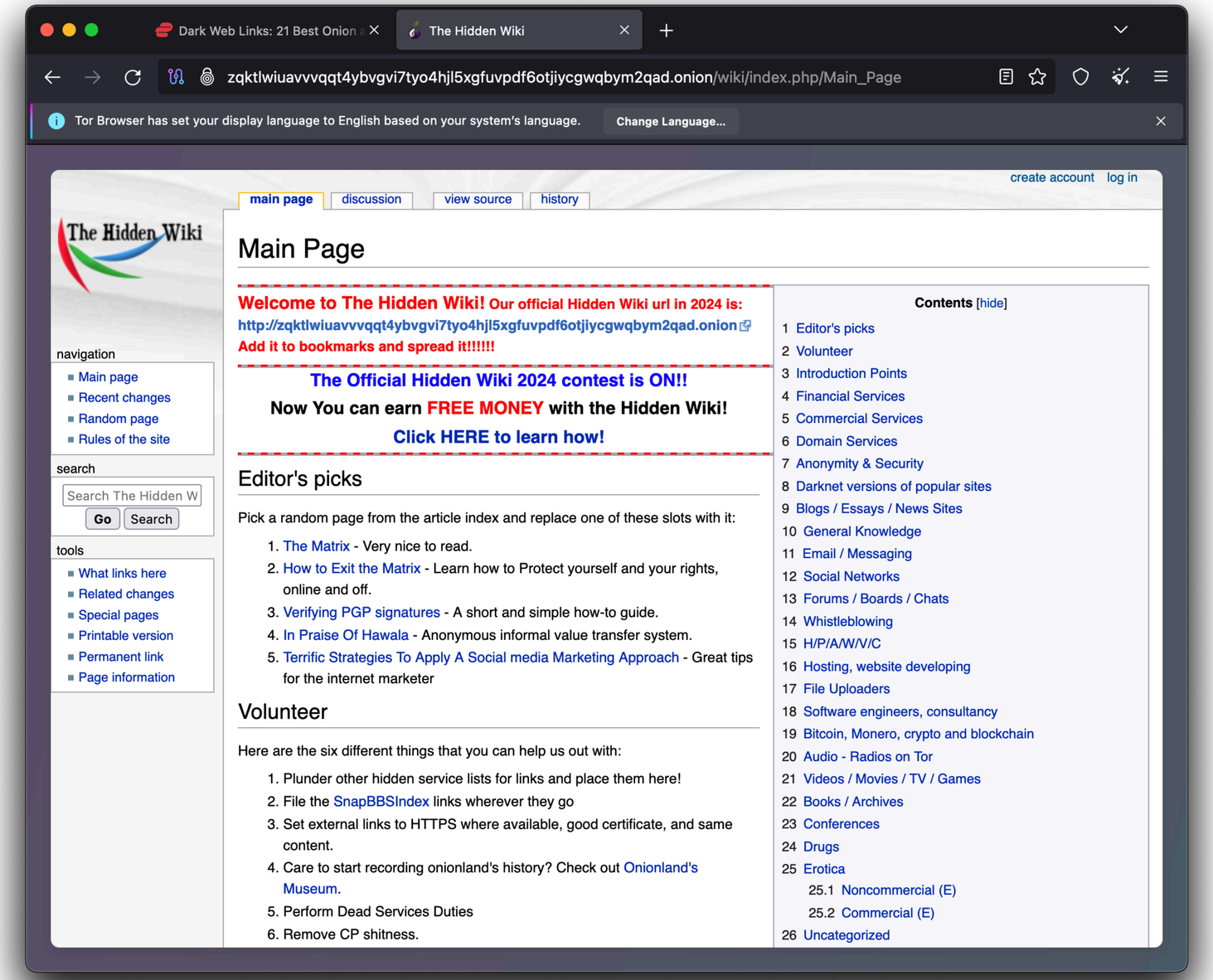


A Darknetről

Co-funded by the
European Union

Darknetről

- A Darknet alternatív hálózat az Interneten belül.
- Speciális böngésző kell a használatához, ez a TOR.
- Nyom nélkül tekinthetők meg weboldalak a használatával, cserében a böngészés sokkal lassabb lesz.
- A Darknet belső hálózatán .onion domaint használnak, a webhelyek nevei nem értelmesek.
- Szűrhető: flaticons
- Hidden Wiki: http://zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion/ D



Az Eszterházy Károly Egyetemen működött a sötét web legnagyobb drogáruháza



DEZSŐ ANDRÁS
KÖVETÉS

2019.07.27. 07:05

Ajánlom 6,9 E

Aki jelszavakat akar óbégatni, azt zavarja a független média. Aki gondolkodni akar, nem élhet nélküle.

TÁMOGASS TE IS!

> *Még ez év elején olyan jelzést kaptunk a német kábítószerellenes szolgálattól, hogy egy kábítószer ügy nyomára bukkantak, s találtak egy miskolci telefonszámot. Arra kértek minket, hogy próbáljuk lenyomozni ezt a szálat*

- így kezdődött az a történet, amelyet Hollósi György őrnagy, az ORFK kábítószer bűnözés elleni alosztály munkatársa mesélt el 1992 decemberében az Új Hírnök nevű újságnak. Az ügy kezdeti szakaszában még a rendőrök sem gondolták volna, hogy a telefonszámon keresztül egy nemzetközi drogügyletre bukkannak, ahol az egyik legnagyobb magyar vállalat, a BorsodChem az érintett. Mint a kábítószer előállítója.

BEST OF MINDEKÖZBEN

Vaddisznók pusztítottak el közel 7 millió forint értékű kokaint egy olasz erdőben

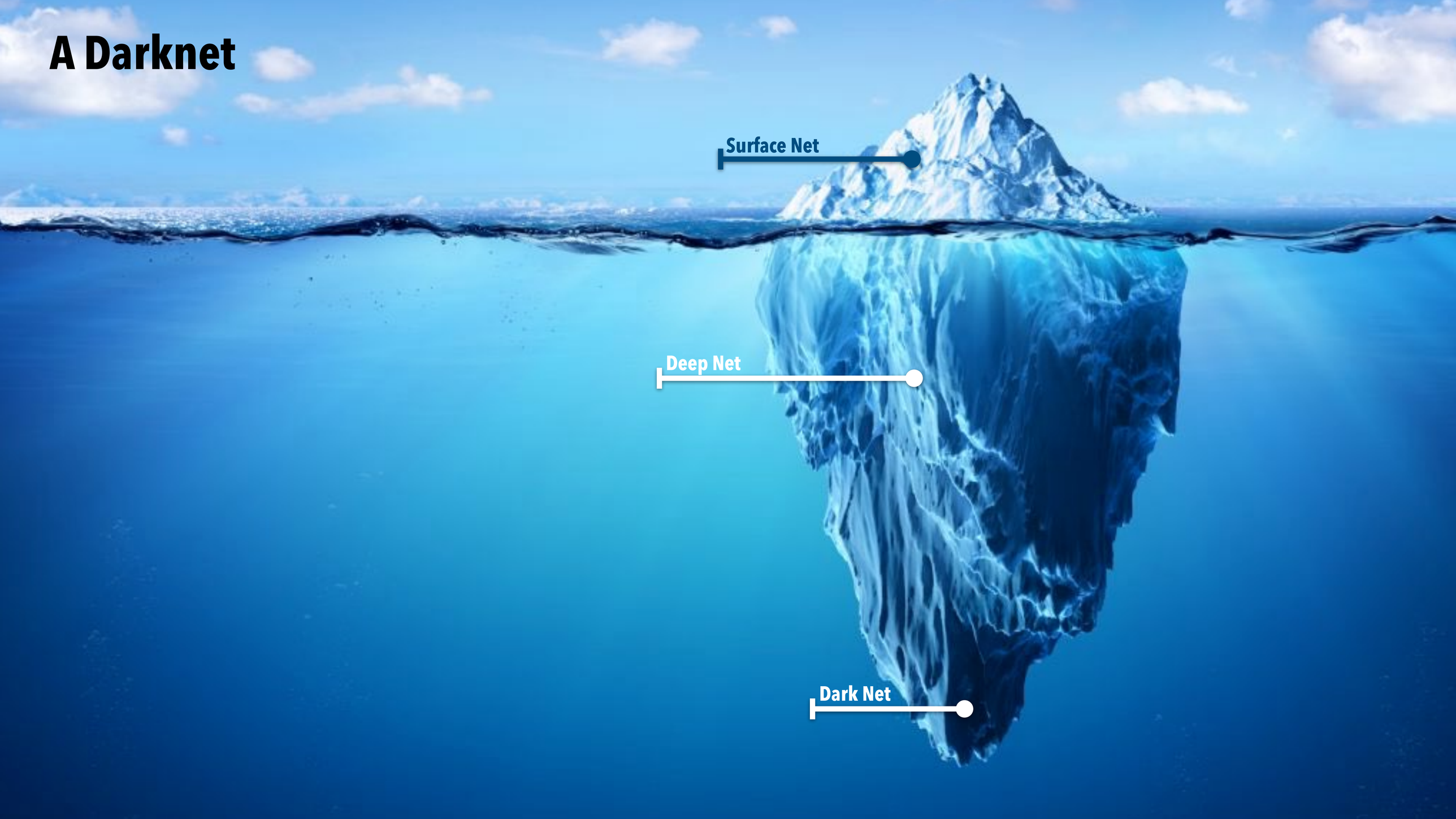
Indexnek nevezte el a rendőrség Bambi és Lövész kölykeinek egyikét

A Joker legőrültebb jeleneteit soha nem fogjuk látni

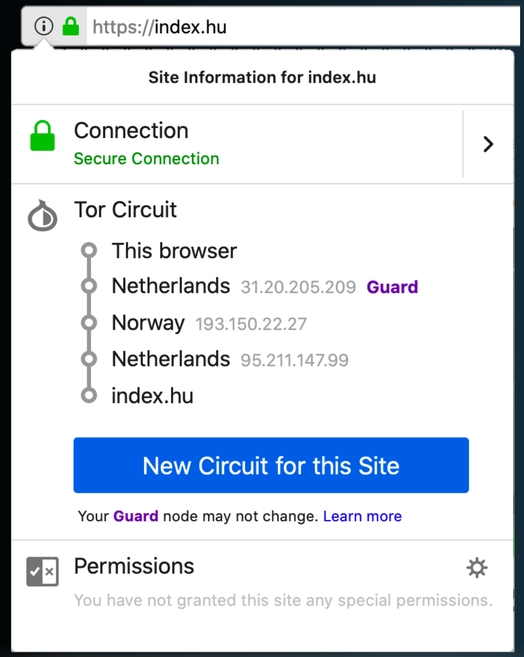
MINDEKÖZBEN

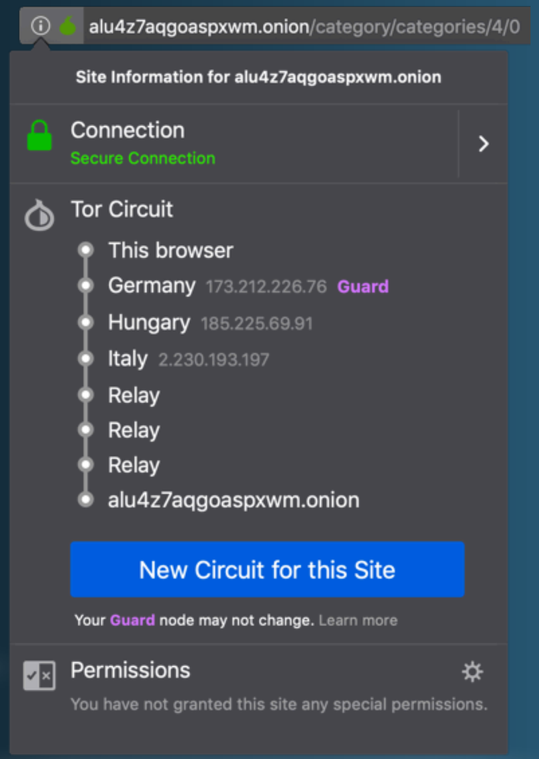
JUHÁSZ EDINA 1 ÓRÁJA

A Darknet

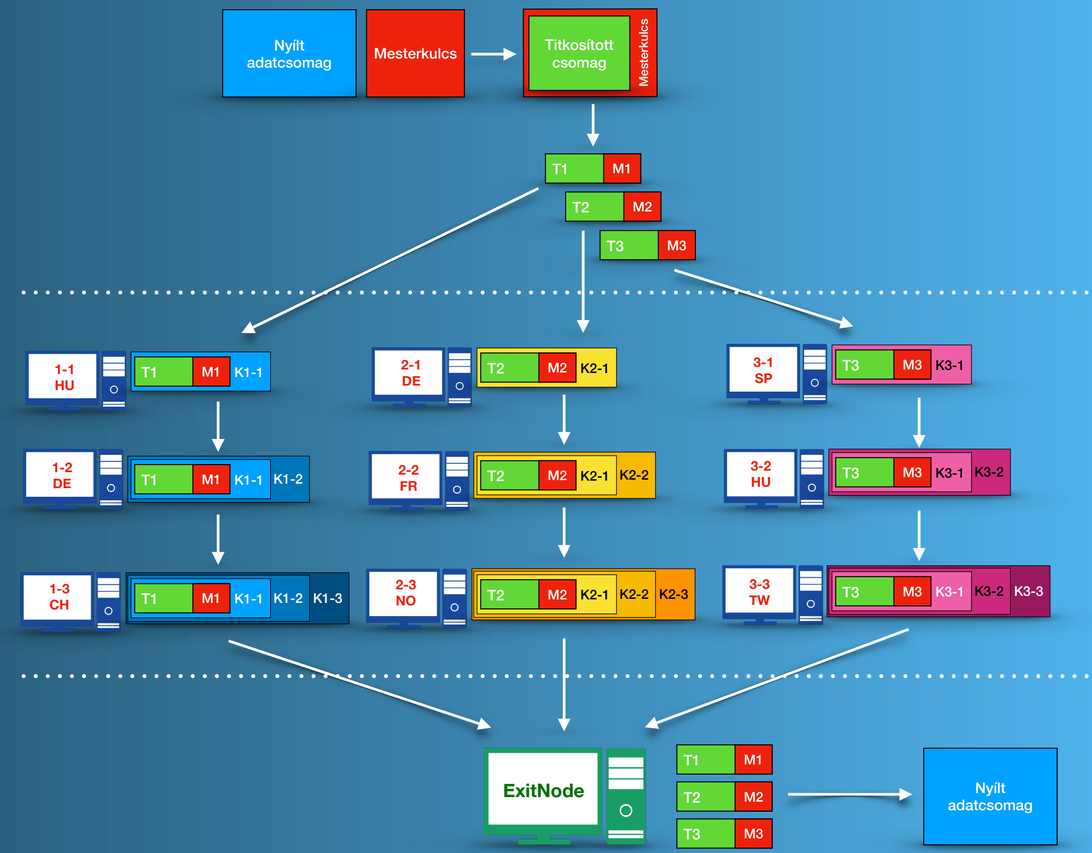





https://index.hu
Site Information for index.hu
Connection
Secure Connection
Tor Circuit
This browser
Netherlands 31.20.205.209 Guard
Norway 193.150.22.27
Netherlands 95.211.147.99
index.hu
New Circuit for this Site
Your Guard node may not change. Learn more
Permissions
You have not granted this site any special permissions.


alu4z7aqgoaspxwm.onion/category/categories/4/0
Site Information for alu4z7aqgoaspxwm.onion
Connection
Secure Connection
Tor Circuit
This browser
Germany 173.212.226.76 Guard
Hungary 185.225.69.91
Italy 2.230.193.197
Relay
Relay
Relay
alu4z7aqgoaspxwm.onion
New Circuit for this Site
Your Guard node may not change. Learn more
Permissions
You have not granted this site any special permissions.


koczka.ferenc — root@ns: /var/log/apache2/access — ssh backup4 — 106×12
[root@ns:/var/log/apache2/access# tail -n 1 -f www.246.hu-access.log
54.36.149.13 - - [17/Nov/2019:20:06:48 +0100] "GET /robots.txt HTTP/1.1" 200 455 "-" "Mozilla/5.0 (compatible; AhrefsBot/6.1; +http://ahrefs.com/robot/)"
185.220.100.255 - - [17/Nov/2019:20:07:25 +0100] "GET /statpages/images/help128.jpg HTTP/1.1" 200 4342 "-" "Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101 Firefox/68.0"
23.129.64.154 - - [17/Nov/2019:20:07:28 +0100] "GET /statpages/images/help128.jpg HTTP/1.1" 200 4342 "-" "Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101 Firefox/68.0"
89.144.12.17 - - [17/Nov/2019:20:07:31 +0100] "GET /statpages/images/help128.jpg HTTP/1.1" 200 4342 "-" "Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101 Firefox/68.0"


Nyílt adatcsomag
Mesterkulcs
Titkosított csomag
Mesterkulcs
T1 M1
T2 M2
T3 M3
1-1 HU
T1 M1 K1-1
2-1 DE
T2 M2 K2-1
3-1 SP
T3 M3 K3-1
1-2 DE
T1 M1 K1-1 K1-2
2-2 FR
T2 M2 K2-1 K2-2
3-2 HU
T3 M3 K3-1 K3-2
1-3 CH
T1 M1 K1-1 K1-2 K1-3
2-3 NO
T2 M2 K2-1 K2-2 K2-3
3-3 TW
T3 M3 K3-1 K3-2 K3-3
ExitNode
T1 M1
T2 M2
T3 M3
Nyílt adatcsomag

El vannak rejtve?

hu.hostadvice.com/tools/whois/#http://

hostadvice. HUF HU

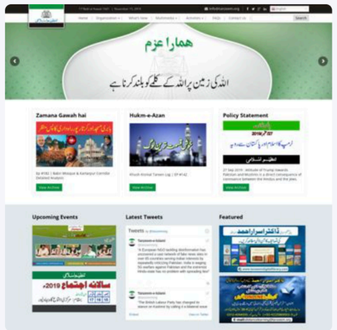
Ön itt van épp: HostAdvice › Eszközök › Tudja meg, hogy mely tárhelyszolgáltatóknál üzemelnek egyes weboldalak

http://tanzeem.org

Hostolva: HostGator

HostGator

Látogatton el a(z) HostGator weboldalára



Tárhelyszolgáltató:
HostGator

IP:
108.167.140.94

Sites hosted on this ip:
91

Földrajzi hely:
Egyesült Államok

Domain:
Kattintson ide

Névszerverek:
ns8331.hostgator.com, ns8332.hostgator.com.

CMS:
WordPress

Webszerver:
Apache

Programnyelv:
PHP

Ossza meg ezt az ingyenes eszközt:

HostAdvice.com
https://ent.siteintelgroup.com

HostAdvice.com
http://tanzeem.org

hu.hostadvice.com/tools/whois/#https://

hostadvice. HUF HU

Ön itt van épp: HostAdvice › Eszközök › Tudja meg, hogy mely tárhelyszolgáltatóknál üzemelnek egyes weboldalak

https://ent.siteintelgroup.com/Conventional/jihadist-gives-manual-for-silent-killing.html el van rejtve a CloudFlare

CLOUDFLARE

mögött Sajnálatosan, lehetetlen elmondani, ki adja a hostingot ehhez a weboldalhoz, mivel ez el van rejtve a CloudFlare proxy mögött. Nincs olyan eszköz az interneten, ami képes lenne megmondani website-hoz tartózó hosting szolgáltató nevét.



Tárhelyszolgáltató:
CloudFlare

CDN:
CloudFlare

Földrajzi hely:
Egyesült Államok

Domain:
Kattintson ide

Névszerverek:
piotr.ns.cloudflare.com, rosa.ns.cloudflare.com.

Ossza meg ezt az ingyenes eszközt:

Látogatton el a(z) CloudFlare weboldalára

Check another website

24/7 HostAdvice Support

Törvénysértő tartalmak





Make your weapons at home - Files for 3D printer
Item # 19720 - Other Listings / Other - SwagQuality (1122)

Views: 6843 / **Sales:** 137
Quantity left: Unlimited *(Unlimited automatic items)*

Buy Price
USD 3.30
(0.000379 BTC)



3D-Printed GUN Blueprints (LIBERATOR ®) v 1.0
Item # 44875 - Guides & Tutorials / Security & Anonymity - MIT (1275)

Views: 534 / **Sales:** 4
Quantity left: Unlimited *(Unlimited automatic items)*

Buy Price
USD 3.99
(0.000457 BTC)

BROWSE CATEGORIES

Fraud	4286
Drugs & Chemicals	38413
Guides & Tutorials	2642
Counterfeit Items	2790
Clothing	650
Electronics	23
Jewelry	497
Money	561
Other	175
Fake IDs	884
Digital Products	6475
Jewels & Gold	751
Carded Items	291
Services	647
Other Listings	374
Software & Malware	529
Security & Hosting	238



Kronos – powerful electric lock pick gun kit for emergency door opening, incl. pick needles set
Item # 40983 - Carded Items / Other - MayansMC (13)

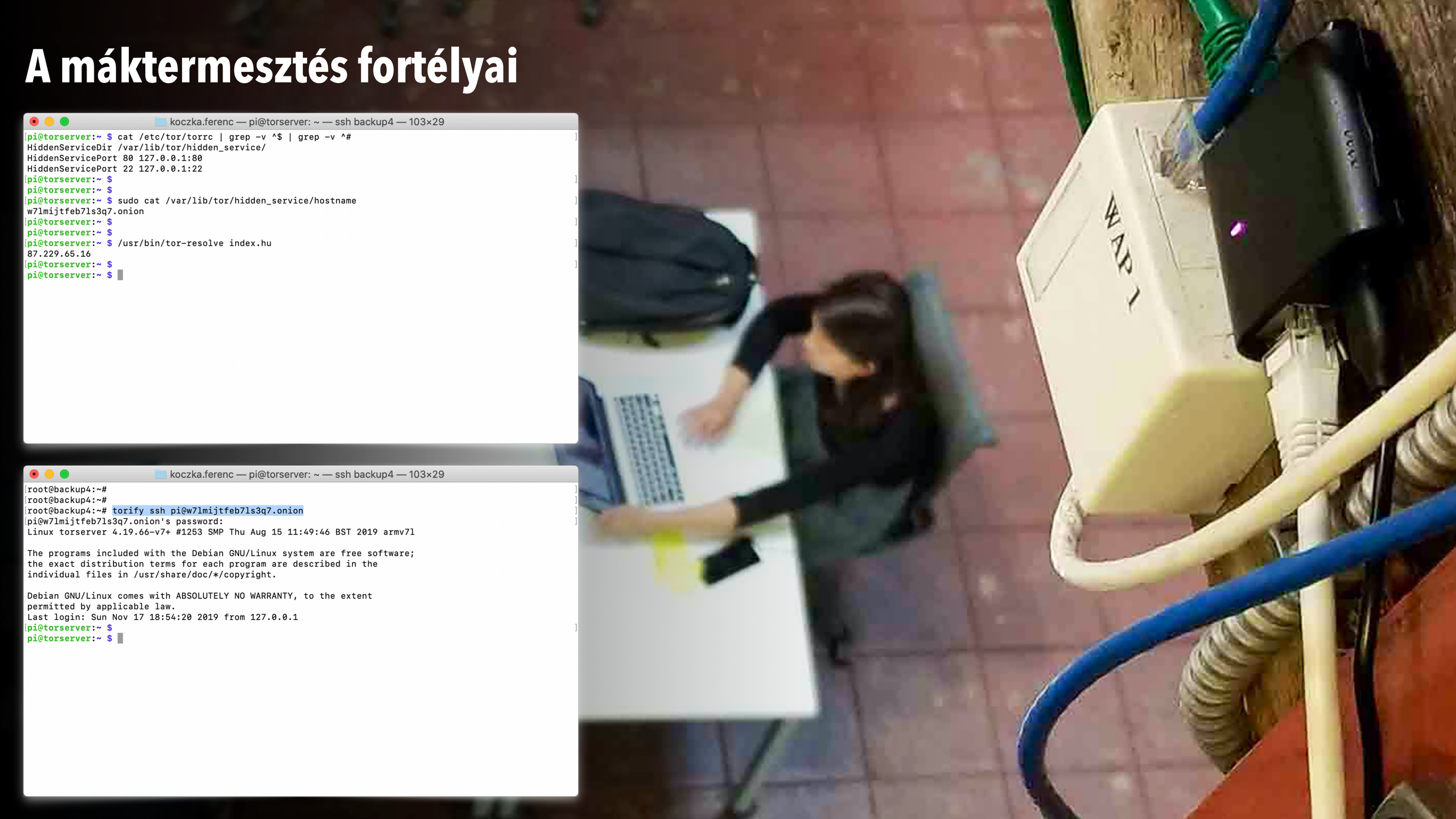
Views: 562 / **Sales:** 0
Quantity left: Unlimited

Buy Price
USD 275.47
(0.031581 BTC)





A máktermesztés fortélyai



koczka.ferenc — pi@torserver: ~ — ssh backup4 — 103×29

```
pi@torserver:~ $ cat /etc/tor/torrc | grep -v ^$ | grep -v ^#
HiddenServiceDir /var/lib/tor/hidden_service/
HiddenServicePort 80 127.0.0.1:80
HiddenServicePort 22 127.0.0.1:22
pi@torserver:~ $
pi@torserver:~ $
pi@torserver:~ $ sudo cat /var/lib/tor/hidden_service/hostname
w7lmijtfeb7ls3q7.onion
pi@torserver:~ $
pi@torserver:~ $
pi@torserver:~ $ /usr/bin/tor-resolve index.hu
87.229.65.16
pi@torserver:~ $
pi@torserver:~ $
```

koczka.ferenc — pi@torserver: ~ — ssh backup4 — 103×29

```
root@backup4:~#
root@backup4:~#
root@backup4:~# torify ssh pi@w7lmijtfeb7ls3q7.onion
pi@w7lmijtfeb7ls3q7.onion's password:
Linux torserver 4.19.66-v7+ #1253 SMP Thu Aug 15 11:49:46 BST 2019 armv7l

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Nov 17 18:54:20 2019 from 127.0.0.1
pi@torserver:~ $
pi@torserver:~ $
```

R.I.P. Welcome to Video

Dream Market

OutLaw

Evolution

Hansa

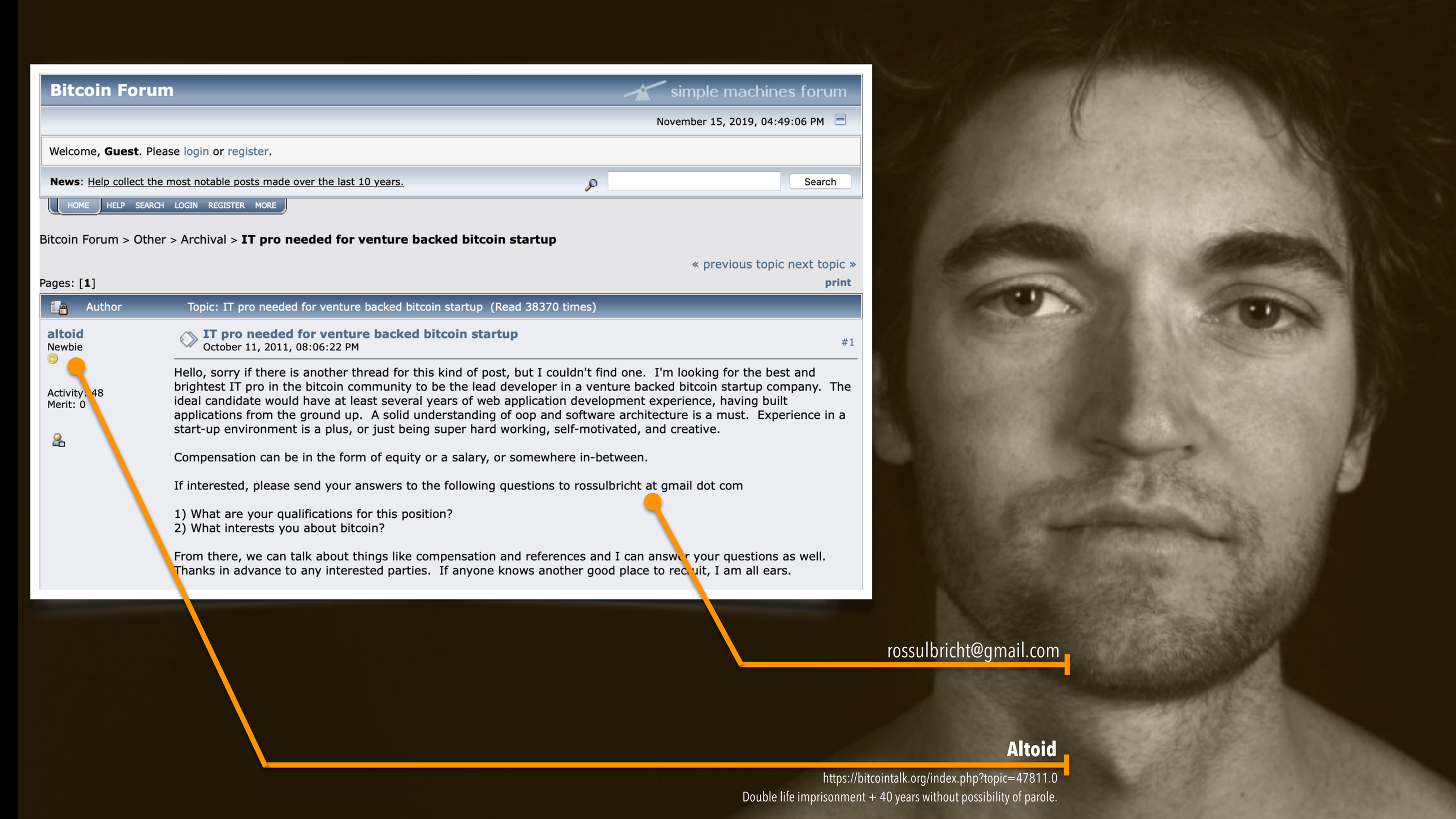
AlphaBay

Wall Street

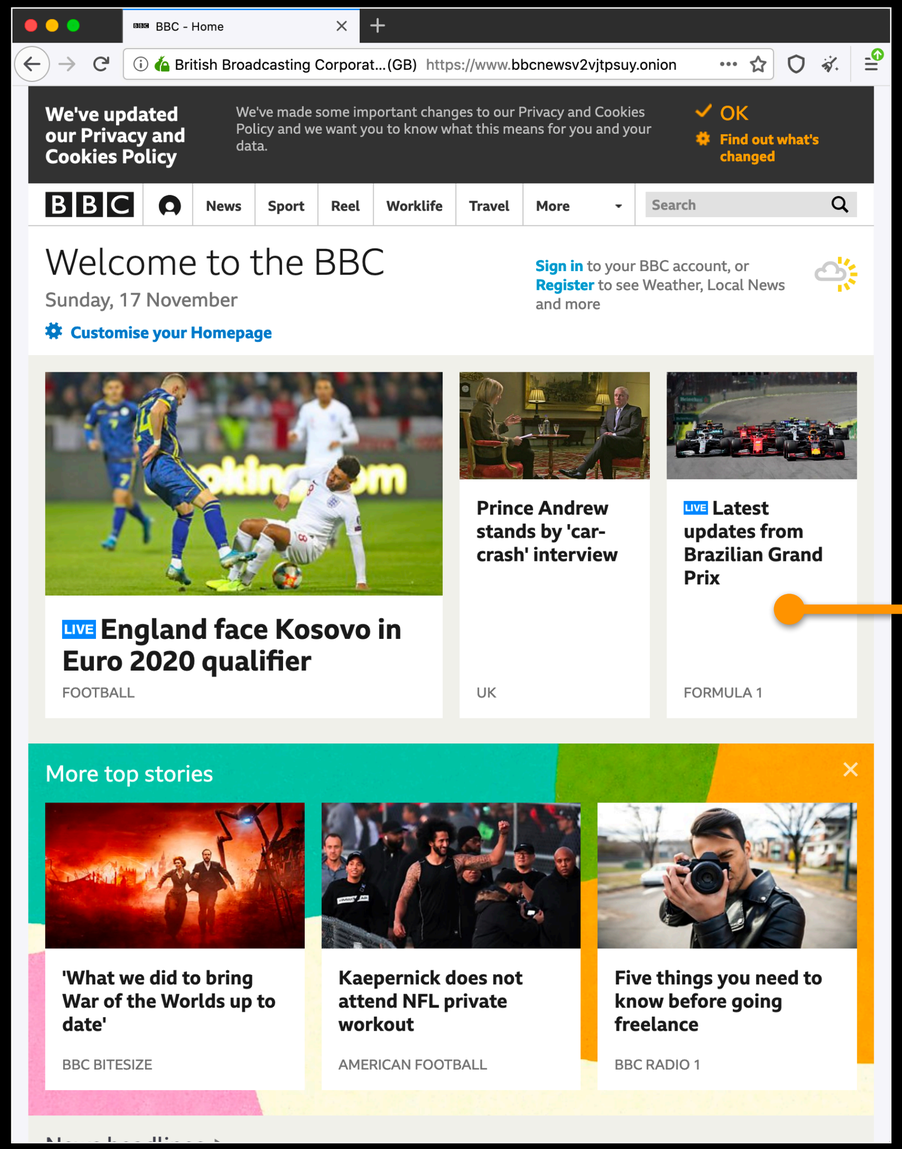
Grams Search

“Az IRS bűnüldözési szervei lekövették a darkweb bitcoinfizetéseit, így eljutottak egy darknetes szerver helyszínéhez Dél-Koreában. Ezután beazonosítottak egy Son álnevű embert, és hamarosan megtalálták a weboldal fizikai elhelyezkedését. A tranzakciók mögött álló felhasználókat is lebuktatták.
Az elkövető, Son, a dél-koreai törvények értelmében csak 18 hónap börtönbüntetést kapott.”




Bitcoin Forum
simple machines forum
November 15, 2019, 04:49:06 PM
Welcome, Guest. Please login or register.
News: Help collect the most notable posts made over the last 10 years.
Search
HOME HELP SEARCH LOGIN REGISTER MORE
Bitcoin Forum > Other > Archival > IT pro needed for venture backed bitcoin startup
« previous topic next topic »
Pages: [1]
print
Author
Topic: IT pro needed for venture backed bitcoin startup (Read 38370 times)
altoid
Newbie
Activity: 48
Merit: 0
IT pro needed for venture backed bitcoin startup
October 11, 2011, 08:06:22 PM
#1
Hello, sorry if there is another thread for this kind of post, but I couldn't find one. I'm looking for the best and brightest IT pro in the bitcoin community to be the lead developer in a venture backed bitcoin startup company. The ideal candidate would have at least several years of web application development experience, having built applications from the ground up. A solid understanding of oop and software architecture is a must. Experience in a start-up environment is a plus, or just being super hard working, self-motivated, and creative.
Compensation can be in the form of equity or a salary, or somewhere in-between.
If interested, please send your answers to the following questions to rossulbricht at gmail dot com
1) What are your qualifications for this position?
2) What interests you about bitcoin?
From there, we can talk about things like compensation and references and I can answer your questions as well.
Thanks in advance to any interested parties. If anyone knows another good place to recruit, I am all ears.
rossulbricht@gmail.com
Altoid
https://bitcointalk.org/index.php?topic=47811.0
Double life imprisonment + 40 years without possibility of parole.

Adott értékrendhez illeszkedő tartalmak védelme

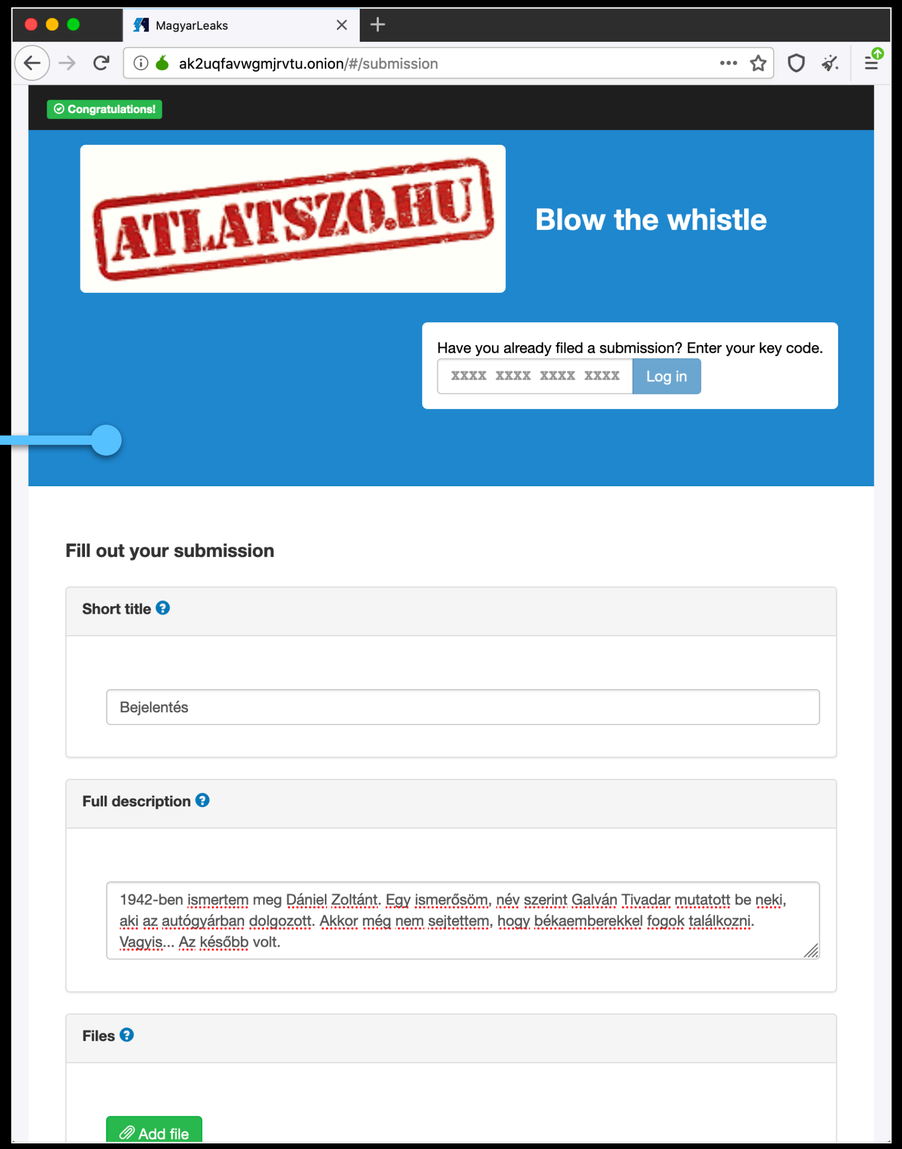


Átlátszó

http://ak2uqfavwgmjrvtu.onion/

BBC News

https://www.bbcnewsv2vjtpsuy.onion/



Alternatívák



FreeNet

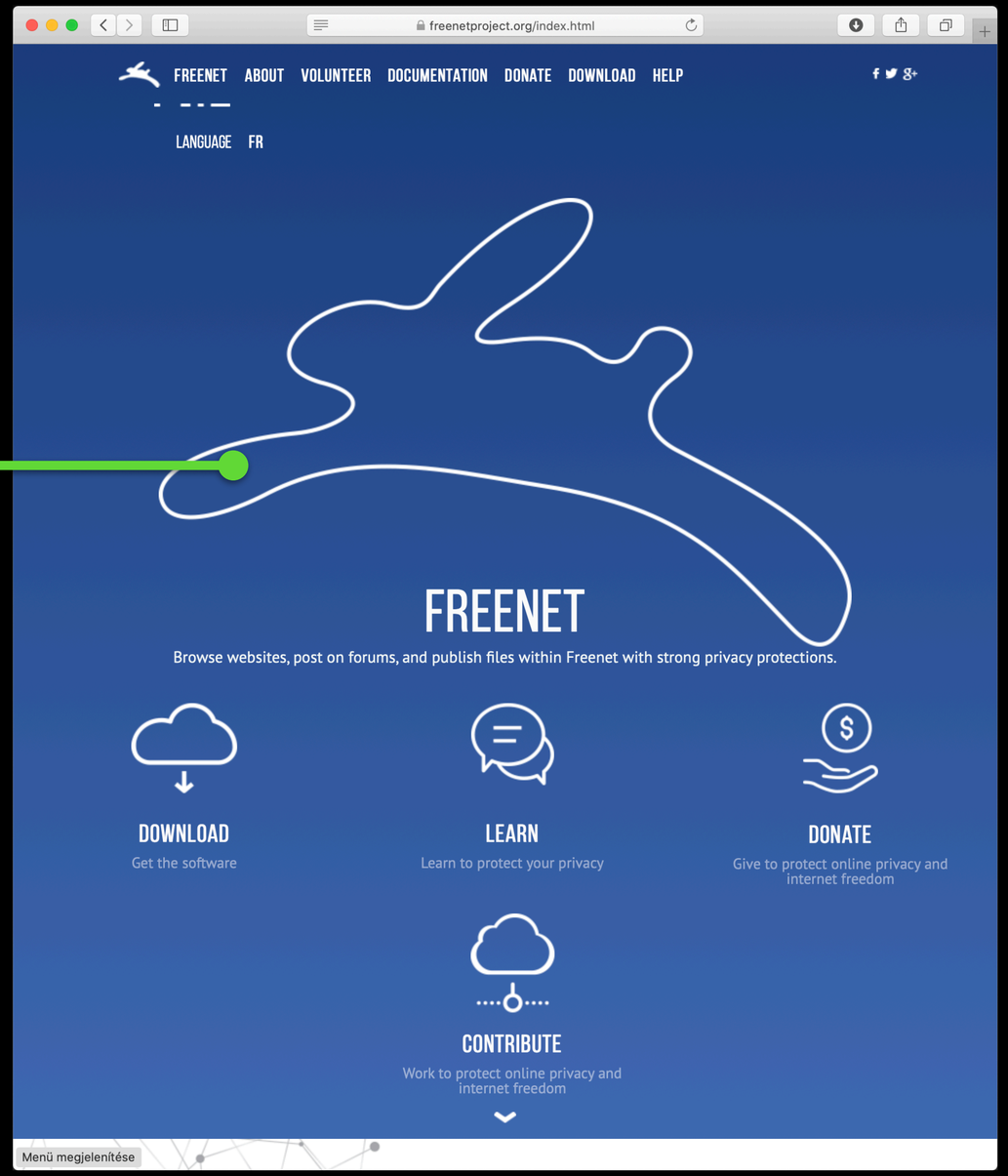
https://freenetproject.org

I2P

https://geti2p.net

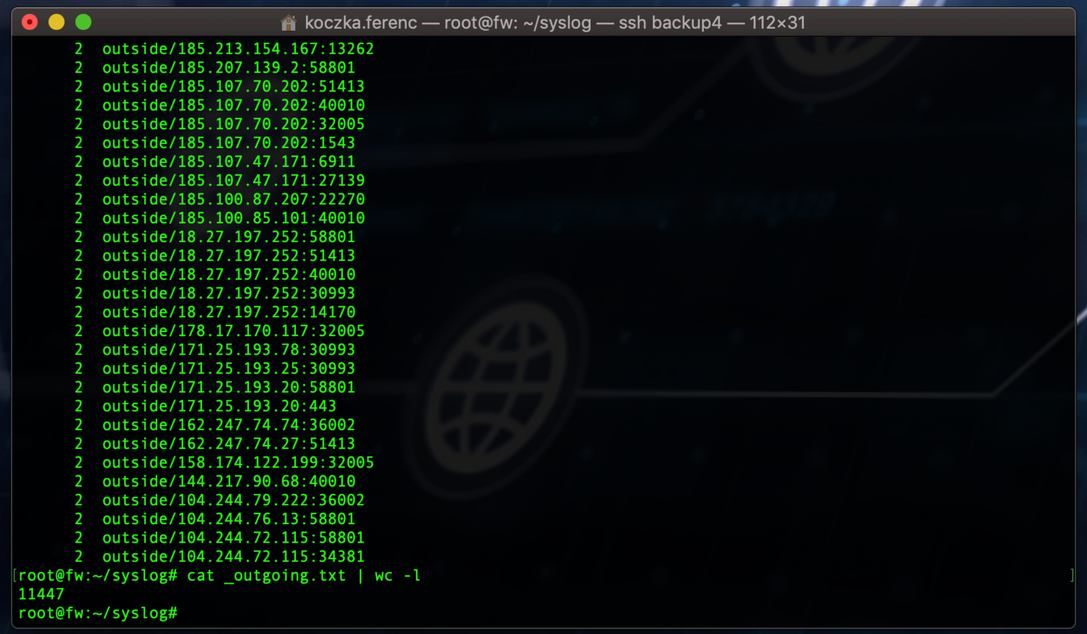
VPN szolgáltatók

https://expressvpn.com



Darknet forgalom

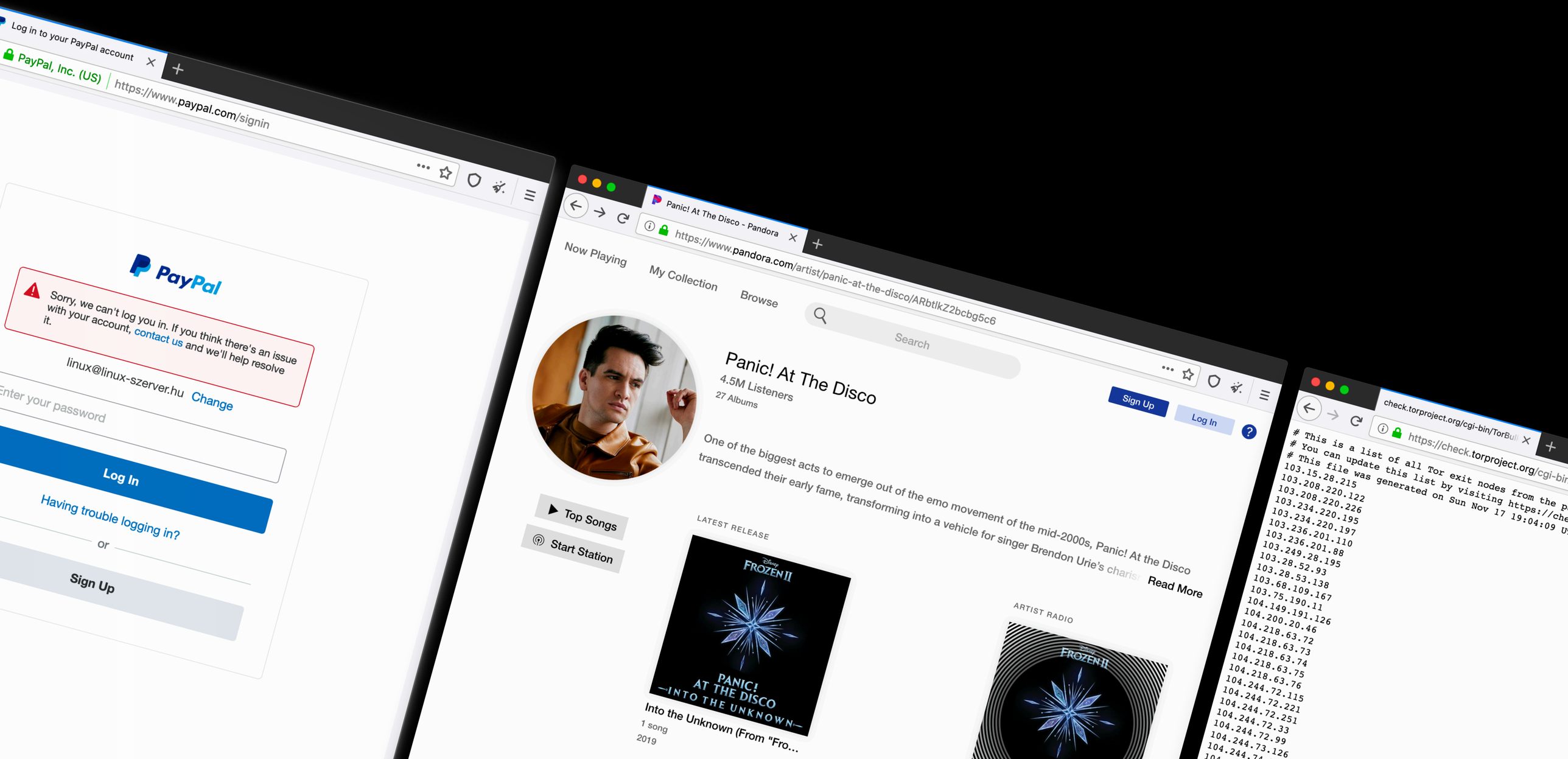
Domain és RDP?



Num	Segment	IP	Port	HostName
48 966	DMZ_PUBLIC_GROUP2	193.225.35.220	22	3(NXDOMAIN)
34 690	DMZ_SERVER	193.225.32.55	22	docker.uni-eszterhazy.hu.
34 629	DMZ_SERVER	193.225.32.57	22	www.oktatas2030.hu.
34 596	DMZ_SERVER	193.225.32.56	22	grafana.uni-eszterhazy.hu.
33 773	inside	193.225.33.45	22	ugyfelkapu.uni-eszterhazy.hu.
32 775	inside	193.225.33.32	22	d317-02.szt.ektf.hu.
30 710	DMZ_SERVER	193.225.32.17	22	aquila.ektf.hu.
29 902	DMZ_OFI1	193.225.32.140	22	3(NXDOMAIN)
28 459	inside	193.225.33.33	22	d318-01.szt.ektf.hu.
26 245	DMZ_SERVER	193.225.32.58	22	sztr.komplexalapprogram.hu.
24 007	DMZ_SERVER	193.225.32.4	22	tavoktatas.ektf.hu.
23 298	DMZ_PUBLIC_GROUP2	193.225.35.220	80	3(NXDOMAIN)
20 551	DMZ_SERVER	193.225.32.9	80	gin.ektf.hu.
20 388	inside	193.225.33.16	22	dorado.ektf.hu.
19 981	inside	193.225.34.31	22	bzs.host.ektf.hu.
19 846	DMZ_SERVER	193.225.32.39	22	columbo.ektf.hu.
19 696	DMZ_SERVER	193.225.32.59	22	3(NXDOMAIN)
19 598	DMZ_SERVER	193.225.32.19	22	insomnia.ektf.hu.
19 579	DMZ_SERVER	193.225.32.16	22	taurus.ektf.hu.
19 570	inside	193.225.33.29	22	3(NXDOMAIN)
19 134	DMZ_SERVER	193.225.32.86	22	hr.nkp.uni-eszterhazy.hu.
18 765	DMZ_SERVER	193.225.32.87	22	hrrep.nkp.uni-eszterhazy.hu.
18 161	DMZ_SERVER	193.225.32.5	80	trevor.ektf.hu.
16 662	DMZ_SERVER	193.225.32.41	80	gemini3.uni-eszterhazy.hu.
16 052	DMZ_OFI1	193.225.32.140	80	3(NXDOMAIN)
15 006	inside	193.225.33.43	22	iot-blade.uni-eszterhazy.hu.
14 480	DMZ_OFI1	193.225.32.131	80	3(NXDOMAIN)
14 373	DMZ_SERVER	193.225.32.5	22	trevor.ektf.hu.
14 302	DMZ_SERVER	193.225.32.21	80	smtp.uni-eszterhazy.hu.
12 166	DMZ_SERVER	193.225.32.189	80	ibmtest.ektf.hu.
12 119	DMZ_SERVER	193.225.32.11	80	gemini.ektf.hu.
10 524	DMZ_SERVER	193.225.32.17	80	aquila.ektf.hu.

Darab	Port	Protocol
600 606	22	ssh
515 661	80	http
5 252	53	domain
1 748	443	https
166	465	smtps
108	993	imaps
100	8080	http-alt
58	25	smtp
38	137	netbios-ns
34	587	submission
22	23	telnet
20	143	imap2
18	3389	rdp
14	3390	rdp?
2	21	ftp

Tiltsuk?


Log in to your PayPal account
PayPal, Inc. (US)
https://www.paypal.com/signin
PayPal
Sorry, we can't log you in. If you think there's an issue with your account, contact us and we'll help resolve it.
linux@linux-szerver.hu Change
Enter your password
Log In
Having trouble logging in?
or
Sign Up
Panic! At The Disco - Pandora
https://www.pandora.com/artist/panic-at-the-disco/ARbtlkZ2bcbg5c6
Now Playing
My Collection
Browse
Search
Sign Up
Log In
Panic! At The Disco
4.5M Listeners
27 Albums
One of the biggest acts to emerge out of the emo movement of the mid-2000s, Panic! At the Disco transcended their early fame, transforming into a vehicle for singer Brendon Urie's charis
Read More
Top Songs
Start Station
LATEST RELEASE
FROZEN II
PANIC! AT THE DISCO
—INTO THE UNKNOWN—
Into the Unknown (From "Fro...
1 song
2019
ARTIST RADIO
FROZEN II
check.torproject.org/cgi-bin/TorBul
https://check.torproject.org/cgi-bin
This is a list of all Tor exit nodes from the p
You can update this list by visiting https://che
This file was generated on Sun Nov 17 19:04:09 U
103.15.28.215
103.208.220.122
103.208.220.226
103.234.220.195
103.234.220.197
103.236.201.110
103.236.201.88
103.249.28.195
103.28.52.93
103.28.53.138
103.68.109.167
103.75.190.11
104.149.191.126
104.200.20.46
104.218.63.72
104.218.63.73
104.218.63.74
104.218.63.75
104.218.63.76
104.244.72.115
104.244.72.221
104.244.72.251
104.244.72.33
104.244.72.99
104.244.73.126

Engedjük

Forgalom
A nyílt nethez képest nem számottevő.

Malware
A forgalom növekedése jelezheti a fertőzött gépek számának növekedését.
Nincs számottevő rdp forgalom.

Anonim böngészés
Érdemes támogatni? Pro és kontra.

Mások példái
Az én buborékomban általános az engedélyezés.

Tudjuk egyáltalán felügyelni?
Sok alternatív megoldás van, az SSH tunnel, VPN szolgáltatók számos lehetőséget adnak.

Inkább legyen kontroll
Érdemes engedélyezni és felügyelni, ezzel felkészülni egy esetleges esemény kezelésére.

Tiltsuk

Bejövő forgalom
A források jó eséllyel támadók.

Anonim böngészés
Ezeket máshol végezzék, a munkakör ellátásához nem szükséges.
*Leaks oldalak ne legyenek elérhetők védett hálózatból.

Darknet szerverek
Ezeket ne nálunk üzemeltessék.
Ne legyen értelme rejtett szervereket elhelyezni a hálózatban.

Felelősség
Probléma esetén felmerül a felelősség kérdése.

Szabályzás
2013 évi L. törvény, 41/2015 BM rendelet, Létfontosságú rendszerekre vonatkozó szabályzások.

Segíti munkánkat, ha kitölti elégedettségi kérdőívünket.

Köszönöm a figyelmet!

Kérdés esetén forduljon hozzánk bizalommal!
info@digitaltechedih.hu

Co-funded by the European Union

A DigitalTech EDIH 2.0 c. projekt megvalósulását a Közigazgatási és Területfejlesztési Minisztérium támogatta.