Frici, Fülöp és a hackerek

(...és lájkvadászok, adathalászok, bankkártyás csalók és egyéb szélhámosok)

Történetek az internet sötétebb oldaláról gyerekeknek és felnőtteknek.

©2019. Solymos Ákos, Minden jog fenntartva

Lektorálta: Bálint Sándor

©2019. Solymos Ákos, Minden jog fenntartva

Grafika: Ujréti Ágnes (Galantusz Grafika)

© Solymos Ákos 2019

Minden jog fenntartva, beleértve az elektronikus megjelenítés jogát, a megfilmesítést, az idegen nyelvre fordítást, a színpadra átdolgozást, a képregény formában történő megjelenést és megzenésítést. A könyv és részleteinek másolása, kinyomtatása, vagy engedély nélküli elektronikus vagy egyéb formátumú terjesztése, bármilyen formában történő sokszorosítása csak a szerző írásos engedélyével megengedett.

A történetek és a szereplők a szerző képzeletének szülöttei, a valósággal való bármilyen párhuzam a véletlen műve – de azért nem lehetetlen, hogy megtörténtek ilyen esetek másokkal.

@ @ @ TARTALOM @ @ @

©2019. Solymos Ákos, Minden jog fenntartva

Feleségemnek, Anettnek, aki nagyon régóta rágta a fülem, hogy írjak már könyvet az információbiztonságról.

©2019. Solymos Ákos, Minden jog fenntartva

1. Az igazi dark elixír

Frici reggel felébredt, és bár alig látott ki a szemén, első dolga volt, hogy ránézzen a *Clash of Clans*[1] birodalmára. Kézbe vette okostelefonját, berajzolta a feloldókódot, ami egy fordított 4-es számra hasonlított.

Sajnos éjjel eltelt az az idő, ameddig működött a pajzs, így megtámadta őt egy ismeretlen, az ő harcosainál sokkal erősebb hősökkel. Barbárok és sárkányok gyakorlatilag letarolták az összes épületet, az arany- és elixírraktárat. Elvittek sok-sok aranyat és a legértékesebb dark elixír jó részét. Frici morcosan vette tudomásul a pusztítást, de ebben a játékban ez benne van. Meghalni nem lehet, mert bár ezt-azt elvisznek, de a játék folytatódik tovább, és az erőforrások újratermelődnek. Aztán persze ő is építette már az íjászokból és varázslókból, na meg gyógyítókból álló seregét, hogy az ezüst II. ligában megtámadjon valakit, és visszaszerezze, amit tőle elvettek. Körforgás az élet.

Miután elindította az egyik rejtett Tesla-torony fejlesztését, kikászálódott az ágyból, megmosakodott és kiballagott a konyhába. Felrémlett benne, hogy az apukája mesélte, hogy már akkor, amikor ő végezte a főiskolát – és ez több mint húsz éve volt – létezett olyan kenyérpirító, ami rá volt kötve az internetre, és amikor betettek egy kenyeret pirítani, lekérdezte az időjárást egy szerverről, és rásütötte az adott időjárás jelét a kenyérre. Ha napos idő volt, napocskát, ha felhős, akkor felhőst, és így tovább. Hatalmas!

Ezen a napon felhős pirítós ugrott volna elő, de hát Friciék kenyérpirítója nem tartozott az „Internet of Things”, vagyis a

[1] A *Clash of Clans* egy okostelefonokon játszható stratégiai játék, ahol cél a bázisunk és harcosaink fejlesztése, megvédése és egyedül vagy klánokba szerveződve más játékosok javainak megszerzése. 2012-ben adták ki, azóta több mint ötvenmillióan játszanak vele a világon.

©2019. Solymos Ákos, Minden jog fenntartva

„A dolgok internete”[2] világába, ez csak egy mezei konyhagép volt. Frici, miután megkente a pirítóst vajjal, készített egy kakaót és leült, hogy megreggelizzen.

Rossz szokása volt, hogy ha egyedül volt, akkor evés közben is a telefonját nyomkodta. Ránézett az Időkép appra, hogy megnézze, milyen kint az időjárás. Jellemző módon eszébe sem jutott, hogy esetleg kisétáljon a teraszra és maga győződjön meg róla. Az olyan kőkorszaki – ahogy szokta mondani – ahogy az e-mail is.

Reggeli után megnyomta a családi laptop bekapcsoló gombját. A gépet sulikezdésre kapták a testvérével közösen. Bár sokat használta az okostelefont is, voltak dolgok, amiket sokkal jobban szeretett a nagyobb képernyős gépen nézni, például a *Minecraft*[3]-ot, meg a kedvenc vloggereinek[4] a játék végigjátszás videóit.

A gép a bekapcsolást követően a szokásosnál lassabban indult el. Frici nem tulajdonított különösebb jelentőséget a dolognak, még viccelődött is magában, hogy biztos a gép is élvezi a nyári szünetet. Hehe.

Aztán végül elindult a masina, ám egyszer csak hoppá… Egy nagy piros kép jelent meg a képernyőn furcsa angol kifejezésekkel és egy visszaszámlálóval. „Your personal files are encrypted!”, meg „you need to pay 0,55 Bitcoin (~386USD)[5]”...Miiivaaaan?

[2] *A dolgok internete* (angolul: Internet of Things, rövidítve: IoT) hálózatba kötött „intelligens/okos” eszközöket takar (Pl. okostévé, okosóra). Ez a technológia gyorsuló ütemben fejlődik, illetve terjed.
[3] A *Minecraft* egy nyílt játékterű számítógépes játék, amivel a játékosok saját világokat alakíthatnak ki. Használják számos tantárgy, például matematika oktatására is.
[4] *Vlogger* – videoblogger rövidítése
[5] „A személyes fájljaid le lettek titkosítva”, „0,55 Bitcoint (~386USD) kell fizetned.”

©2019. Solymos Ákos, Minden jog fenntartva

Frici nem értette. Sosem látott ilyet korábban, de nyolcadikos nagyfiú révén tudta, hogy mi az az USD – külföldi pénz, ami az amerikai filmekben szokott lenni. Viszont az a nagy piros képernyő... nem sok jót sejtetett. Meg az a visszaszámláló... Tisztára, mint a *CSI*[6]-ban!

De hát ez nem film volt, hanem a család által közösen használt laptop, rajta az összes családi fotó, a balatoni nyaralás képei, a családi költségvetés, ezen keresztül internetbankolt Frici apukája, és anyukája is itt tartotta féltve őrzött receptjeit, amit még a nagymama mesélt el neki. Gyorsan felkapta a telefonját, lefotózta a képernyőt, és már dobta is át Snapchaten[7] legjobb barátjának, Fülöpnek a képet. „Ez vajon mi a fene lehet...?” - morfondírozott közben.

[6] *CSI (Crime Scene Investigation) – Helyszínelők* című tévésorozat.
[7] Snapchat – azonnali üzenet- és fotóküldő mobilalkalmazás, amely bizonyos idő elteltével megsemmisíti az üzenetet.

©2019. Solymos Ákos, Minden jog fenntartva

Fülöp kissé tudálékosan, de azonnal reagált:

– Kérlek, ez egy nagyon komoly dolog. Pár napja néztük a *Híradó*t, ahol valami zenész beszélt arról, hogy zsarolóvírusok letitkosították egy csomó fájlját, köztük a frissen szerzett zenéit is. Az is valami hasonló volt. De várj, utánanézek. Google a barátunk, tudod.

Frici kezdett komolyan ideges lenni:

– Ne őrjíts meg, Fülöp!!! Letitkosítani? Az meg mi a szösz?
– Valami olyasmi, hogy csak akkor tudod újra megnyitni a fájljaidat, ha megadsz egy kódot. De ahhoz, hogy ezt megkapd, fizetni kell. Ajjaj, ez szívás… Mit ír a géped pontosan? – kérdezte Fülöp.
– Várj, beírom a fordítóba. Mia…? Hogy micsoda? Nemár… Fizessek majdnem 400 dollárt, különben 119 óra múlva törli a titkosítás visszaállító kulcsát…??? Te jó ég… Azt se tudom, az

©2019. Solymos Ákos, Minden jog fenntartva

mennyi pénz, meg különben is, honnan lenne dollárom, meg egyébként is, mi az a Bitcoin[8]…???

Frici most ijedt meg igazán. Mit fognak szólni a szülei? Az összes családi fotó, a mama receptjei… Ebből balhé lesz. Mit lehet tenni ilyenkor? El lehet sunnyogni az egészet, rákenni, hogy elromlott a gép. Áááá, ez nem jó, apáék nem hülyék, rögtön leveszik, hogy valami nem kerek. Szólni kell Apáéknak. Az a tuti.

Frici felvette a telefonját a kedvencekből kiválasztotta *Apa* nevét, és már ki is csöngött:

– Halló, halfeldolgozó – viccelődött Frici apukája, látva fia telefonszámát. – Mi újság, fiam, hogy telik a szünet?
– Baj van – mondta Frici elhaló hangon. – Valami vírus letitkosította a laptop fájljait. Azt írja, hogy ha 119 – már csak 118 – órán belül nem fizetünk 386 dollárt, akkor törli a privát kulcsot vagy mit. Ez mi lehet?
– Túl sok számítógépes videót néztél fiam, ne szórakozz velem, dolgozom éppen… – mordult fel Apa.
– Ne csináld már! Ez most komoly. Fülöp is utánanézett és ez valami zsarolóvírus! Volt a tévében is…. Meg ahogy néztem, tele van vele az internet is. Tudsz segíteni?
– Én, innen munkából? Nem hiszem. 118 óra? Még szerencse, hogy holnap szombat, és nem kell dolgozni menni. Mit fog szólni Anyád...? Te jó ég… Várj, felhívom Csuka bácsit, ő nagy tudora az ilyeneknek. Megkérem, hogy holnap ugorjon be és nézzen rá. Addig ne nyúlj semmihez!

[8] A *bitcoin* egy nyílt forráskódú digitális fizetőeszköz, amelyet 2009. január 3-án egy ismeretlen bocsátott ki, közvetlenül a 2008-as amerikai bankválság kirobbanása után. Az elnevezés vonatkozik továbbá a fizetőeszközt kezelő nyílt forráskódú szoftverre, és az azzal létrehozott elosztott hálózatra is.

©2019. Solymos Ákos, Minden jog fenntartva

Másnap délelőtt izgatottan várta Frici és családja Csuka bácsit. Csuka bácsi egy idős, de nagyon tapasztalt, nagy harcsabajszú, öreg szaki volt, aki információbiztonsági szakértőként dolgozott egy cégnél.

Csuka bácsi első kérdése így hangzott:

– Volt mentés az adatokról?

A családtagok zavartan néztek egymásra, végül Frici apukája törte meg a csendet:

– Nem, nem volt… Még nincs egyéves a gép. Még garanciális. Nem romolhat el. Vagy ha igen, akkor kijavítják – válaszolta.
– A garancia az adatokra sohasem vonatkozik. Azért mindig a használó felel – mondta Csuka bácsi. – Ha nem sikerül a fájlok visszaállítása, és nincs mentés sem, akkor örökre búcsút mondhattok a gépen lévő adatoknak és fájloknak. Azt semmiképp sem javaslom, hogy fizessetek a zsarolóknak, mert semmi garancia nincs arra, hogy tényleg működik a visszafejtő kulcs, amit küldenek. Volt már, hogy eleve rosszul volt megírva a vírus, így hiába fizetett az áldozat, még a készítő se tudta volna visszafejteni a kódolt fájlokat. Apropó: biztos érdekel, hogy miként fertőződött meg a gép. Használtok valamilyen víruskeresőt?
– Nem vettünk semmit, állítólag volt a gépen valamilyen. Bár mindig hisztizett, hogy lejárt a 30 napos próbaidő, úgyhogy letöröltem, mert nagyon idegesített. Nem kellett volna? – válaszolta bizonytalanul Apa.
– Hát nem… – mondta az öreg, és közben furcsán mozgatta nagy harcsabajszát. – Javaslom, vegyetek egyet. Sokkal olcsóbb kifizetni párezer forintot egy internetvédelmi csomagért, ami jóval többet tud, mint egy víruskereső, mint fizetni száz dollárt vagy több száz eurót a zsarolóknak. A

©2019. Solymos Ákos, Minden jog fenntartva

hekkerekről meg nem is beszélve. Meg a felbecsülhetetlen értékű adatok elvesztéséről, amit lehetetlen pótolni.
– Értem. Azt hiszem, így lesz, csak ezt most ússzuk meg! És milyen programot ajánlasz, Csuka bácsi? - kérdezte Frici.
– Válasszatok ti, én nem szeretnék ajánlani. Ha elmentek a www.virustotal.com oldalra, ott fel van sorolva majd az összes víruskereső. De vannak programtesztek a www.virusbulletin.com-on is. A lényeg, hogy valami legyen, és rendszeresen frissüljön. Egyébként nem történt tegnap valami furcsa? Nem néztetek ismeretlen weboldalakat, vagy nem jött esetleg valami furcsa e-mail?

Apa elgondolkodott:

– Furcsa e-mail nem volt. Kaptam egy levelet a DHL-től, hogy a csatolt fájlban van egy csomagértesítő, és nézzem meg.
– És vártál csomagot? – kérdezte Csuka bácsi.
– Hááát... nem vártam. Ezért is csodálkoztam és nyitottam meg a fájlt. Valami megjegyezhetetlen nevű zip-fájl volt. Rákattintottam párszor, de aztán nem történt semmi, ezért nem is foglalkoztam vele, hanem kikapcsoltam a gépet – idézte fel Apa a történteket.
– Ahhha! Itt van a kutya elesve! – kiáltott fel Csuka bácsi. – Abban a zip-fájlban volt a vírus, amit elindítottál! Soha, de soha ne nyiss meg ismeretlentől kapott e-mailt, főleg, ha bármilyen csatolmányt is tartalmaz! A csalók tipikus módszere, hogy csomagküldemény-értesítőként, vagy valamilyen tartozásra hivatkozva valamilyen számla van a levélhez csatolva. Főleg a számla veszélyes, mert azon mindenki felháborodik, és fúrja a kíváncsiság, hogy ki akar már megint valami pénzt legombolni róla. De ugyanilyenek azok a nyereményértesítések is, amelyek valami csodás összegről szólnak. A legnagyobb kérdés ilyenkor mindig az, hogy oké, hogy nyertem, de vajon játszottam-e? Mert ha nem, akkor ez átverés.

©2019. Solymos Ákos, Minden jog fenntartva

– Oké, oké, de mi lesz a mi gépünkkel? Tudsz vele valamit kezdeni? – kérdezte Apa.

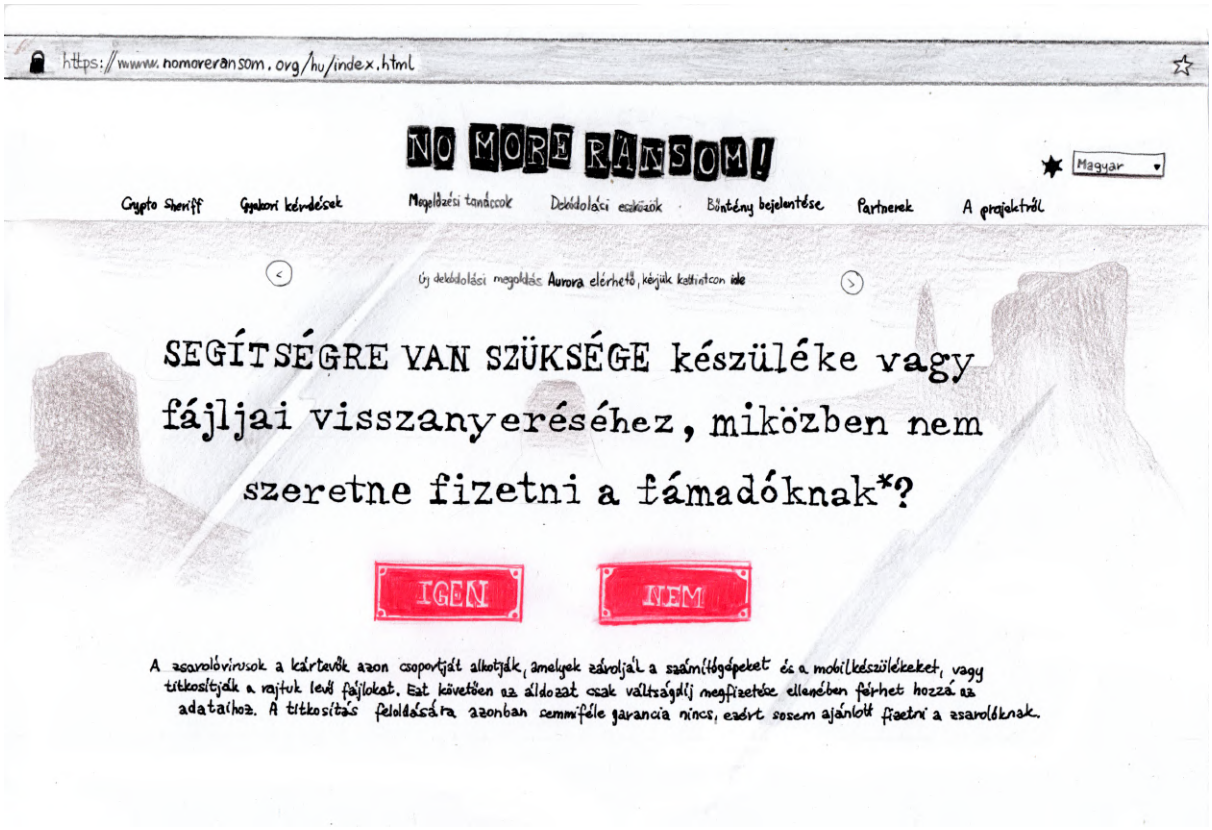
Csuka bácsi felvette a szemüvegét, és elkezdte vizsgálni a számítógép könyvtárjait és fájljait.

– Aha, itt mindjárt látok is pár letitkosított fájlt. Onnan lehet megismerni őket, hogy a CRYPTOLOCKER[9] kiterjesztést adja hozzá a fájlokhoz a vírus. Persze ez csak ez az egy, ezen kívül még sok más fajta zsarolóvírus létezik, CryptXXX, Xorist, BitCryptor – sorolta.
– Gyerekek, tudtátok, hogy az első ilyen zsarolóvírust még floppylemezen küldözgette szét az írója cégeknek, akiknek aztán egy bankszámlára kellett utalni a pénzt? Mi? Hogy nem tudjátok, mi a floppylemez…? Hm… Hát igen, kissé eljárt fölötte az idő. Olyan, mintha a számítógépen a *Mentés* ikont kinyomtatnád 3D nyomtatóval. Na, így már megvan, ugye?

Frici csodálkozva nézte, ahogy az öreg megnyitja a Chrome[10]-ot, bepötyögi a www.nomoreransom.org címet a böngészőbe. Miután betöltődött az oldal, feltöltött egy letitkosított fájlt és feszülten figyelt.

[9] *Cryptolocker* – az egyik legelterjedtebb zsarolóvírus. Letitkosítja a számítógépen/telefonon lévő fájlokat és csak váltságdíj kifizetése után oldja fel a titkosítást. De erre nincs garancia.
[10] *Chrome* – a Google által fejlesztett webböngésző program. Manapság a legnépszerűbb a világon.

©2019. Solymos Ákos, Minden jog fenntartva



Szerencsére a zsarolóvírus már ismert volt, és az oldal felkínálta a titkosítás feloldókulcsát letöltésre.
Ezek után már csak pár kattintás volt hátra, és elindult a fájlok visszaállítása. Csuka bácsi is elégedetten kortyolt bele a kávéjába, ami eddig érintetlenül gőzölgött a pohárban.
Az egész család megkönnyebbült. Frici is fellélegzett. Már épp hálálkodni akart, amikor Csuka bácsi kicsit lelohasztotta a vidám hangulatot:

– Tudnotok kell, hogy ilyen fertőzés akármikor újra előfordulhat – ha nem vagytok résen! Naponta rengeteg új variánsa jelenik meg a különböző zsarolóprogramoknak és vírusoknak, mivel ez sajnos hatalmas üzlet a rosszfiúknak. Hogy megvédjétek magatokat, pontosabban az adataitokat, az alábbiakat kell tenni: vegyetek egy internetvédelmi csomagot, de minimum egy víruskeresőt. Állítsátok be úgy, hogy rendszeresen frissüljön és hetente legalább egyszer végezzen teljes keresést az összes meghajtón a számítógépen. Legyen rendszeres mentés a gépen és a telefonokon tárolt adatokról.

©2019. Solymos Ákos, Minden jog fenntartva

Nem kell feltétlen mindenről, de ami fontos vagy akár pótolhatatlan, azokról mindenképp. A mentést ne a gép mellett tároljátok. És legfőképp legyetek óvatosak! Nem szabad ismeretlen helyről, ismeretlen feladótól származó levelek mellékleteit megnyitni. Az interneten böngészve pedig ne reflexből kattintsatok a felugró ablakokra! Mindig olvassátok el, hogy mit ír. Ha nem tudjátok, nem értitek, akkor pedig inkább a böngészőablakot csukjátok be, mintsem az ablak bármelyik részére is kattintsatok.

Miközben Csuka bácsi befejezte kis beszédét, a fájlok is visszanyerték eredeti kiterjesztésüket és a gép is már a kikapcsolás utolsó fázisánál járt.

Este Frici és családja elgondolkodva hajtotta álomra fejét. Abban mindannyian biztosak voltak, hogy az internet még számos veszélyt rejt, és ha nem figyelnek oda, és főleg, ha nincs Csuka bácsi, akkor komolyabb baj is történhetett volna. Mit tudhat vajon még az Öreg? Mi lesz, ha nem fog ráérni? Jó lenne úgy ismerni az internet sötét bugyrait, mint ő.

Aznap este Frici álmában egy öreg harcsabajszú Barbár Király harcolt a betolakodó valkűrök ellen, hogy megvédje tőlük a sok dark elixírt, amiben furcsa mód 1-esek és 0-k úszkáltak ezrével, amikből a nagyi almás pite receptjét lehetett kiolvasni: „…végy 20 dkg lisztet, 2 kg almát…”

********** Vége az első fejezetnek **********

©2019. Solymos Ákos, Minden jog fenntartva