Dénes Tamás
matematikus-kriptográfus

email:
tdenest@freemail.hu

Kit „zsaroló vírus”?

A 20. századi atomfegyverkezés fenyegetően lebegett az emberiség feje felett. A 2001. szeptember 11-i new yorki ikertornyok elleni támadást a politikusok és a média a *„civilizált társadalmak biztonsága”* szempontjából új korszak kezdeteként emlegetik. Eme új korszak zászlójára a *„terrorizmus elleni küzdelem”* feliratot rótták. Ez alatt a zászló alatt született meg 2001. decemberében az USA történek legnagyobb hadiipari költségvetése, és ez a zászló határozza meg egész életünket Európában is. E zászlón szereplő felirat szabadította ki a palackból az orwelli NAGY TESTVÉR szellemét, ami azóta messze túlszárnyalta Orwell fantáziáját!
Alig 16 évet kellett várnunk, hogy napjainkban *„zsarolóvírus”* képében megjelenjen az „informatika történek legnagyobb kiber támadásaként” világgá kürtölt, avagy jól hangzó szalagcímként, *„minden idők legsúlyosabb vírusfertőzése”*, melyet sok szószátyár politikus és a szenzációra éhes média a *„civilizált társadalmak IT biztonsága”* szempontjából új korszak kezdeteként emleget. Eme új korszak új zászlóján a *„kiberterrorizmus elleni küzdelem”* felirat olvasható. Természetesen az „új korszak” új, még hatalmasabb IT biztonsági (hadi) költsévetéssel jár.

Sajnálatos tény, hogy a média által az emberekre zúdított információ dömping most is elfedi a jelenség mélyén lappangó lényeget. Vagyis azt, hogy ***a WannaCry zsarolóvírus (ellopott) forrása a National Security Agency (NSA), azaz az USA Nemzetbiztonsági Ügynöksége által készített kód, amely a Windows operációs rendszerekben felfedezett biztonsági rést támad.***

A **National Security Agency** (NSA, Nemzetbiztonsági Ügynökség) az Amerikai Egyesült Államok rádióelektronikai, jelhírszerzéssel foglalkozó (Signals Intelligence: SIGINT) hírszerző szervezete, a legnagyobb költségvetésű és létszámú önálló nemzetbiztonsági szolgálat. Az Amerikai Védelmi Minisztérium alárendeltségében működik. Tevékenységi körébe tartozik a külföldre irányuló rádiófelderítés tervezése, koordinálása, irányítása, beleértve az internetes forgalom ellenőrzését, valamint a hazai információbiztonság (INFOSEC) védelme, a kriptográfia, azaz a külföldi rejtjelfejtés és a hazai rejtjelzés biztonságának védelme. Az NSA az egyik főszereplője a még a hidegháborúban indult, de napjainkban is folytatott ECHELON (http://www.titoktan.hu/_raktar/_e_vilagi_gondolatok/1.GondolECHELON.htm) műveletnek is, amelynek fő tevékenysége a távközlési műholdak adatforgalmának ellenőrzése. Az NSA-nak nem tartozik a hatáskörébe az emberi erőforrásokkal folytatott hírszerzés, mint például a CIA esetében. Ezzel szemben feladata koordinálni a többi titkosszolgálat tevékenységének SIGINT elemeit. Erre a koordináló tevékenységre hozták létre az NSA igazgatója vezetésével a Central Security Service (Központi Biztonsági Szolgálat, CSS) nevű szervezetet. Az NSA igazgatója emellett a United States Cyber Command (USCYBERCOM), az Egyesült Államok Kiberhadviselési Parancsnokságának a főnöke is.

A The Shadow Brokers nevű hackercsoporttal hozzák összefüggésbe a „zsarolóvírus” támadásokat, amely csoport azt állítja, hogy az NSA-től lopott hackelési eszközöket tett közzé az interneten. Tehát a *„Minden idők legsúlyosabb vírusfertőzése”* alapját képező kódot maga az NSA állította elő, melynek nyilvánosságra kerülése sem véletlen. Az egyik alapvető kérdés, hogy az USA talán legtitkosabb működésű intézményéből hogyan „szivároghat ki”

Kit „zsaroló vírus”?

efféle információ? Vagyis az USA állampolgárok mennyire aludhatnak nyugodtan, ha a *Nemzetbiztonsági Ügynökségük így működik?*

Másrészről, természetesnek tekinthetjük, hogy egy ilyen professzionális szervezet által (lásd a keretes szöveget!) kidolgozott kód illetéktelenek kezében, kitűnő pénzszerzési forrássá válik. Azt a gyanútlan társadalom számára alapvető kérdést azonban **SENKI NEM TESZI FEL**, hogy vajon az **NSA MIRE HASZNÁLTA (vagy akarta felhasználni)** ezt az eszközt?!

Ahogy az elmúlt évtizedekben, úgy a jelen esetben is szeretnék ragaszkodni a feltett kérdésre adott szakmai válaszhoz, amely messze elkerüli a politikai PR és a média szenzáció eszközeit.

A válaszhoz észre kell venni, hogy a 2001-es és a 2017-es KORSZAKHATÁR nagy hasonlóságot mutat, különösen a politika és a nemzetbiztonsági szolgálatok összefonódása szempontjából. Ennek lényege, hogy a NAGY közös ellenség (terrorizmus, kiberterrorizmus) elleni küzdelemhez, egyre nagyobb költségvetést biztosítanak az államok a NAGY TESTVÉR program megvalósítására. Ez a védekezési stratégia tulajdonképpen a társadalom becsületesen élő 99.9%-ára tolja a védekezés nehézségeit, amikor a „biztonságra” való hivatkozással MEGZSAROLJA az állampolgárokat, és ezzel az állampolgári szabadságjogok súlyos korlátozását kényszeríti rájuk.

Miközben az NSA és a többi „fejlett ország” nemzetbiztonsági szolgálata segédkezik eme stratégia megvalósításában, „elfelejtik” tájékoztatni a társadalmat arról, hogy léteznek olyan kriptográfiai (információ biztonsági) módszerek, protokollok, amelyek lehetővé tennék az úgynevezett SZIMMETRIKUS BIZTONSÁGOT. Vagyis amikor az állampolgárok nem az állami NAGY TESTVÉR totális marionett bábuiként élnek.

Azok számára, akiket érdekel a probléma részletes kifejtése és az állampolgári szabadságjogokat tisztelő (szimmetrikus biztonság) megoldási lehetőségei, ajánlom a majdnem 10 évvel ezelőtt írt egyik tanulmányomat: http://www.titoktan.hu/_raktar/NagyTestver1.htm .
Az NSA-val kapcsolatos fenti kérdésre és egyben a „Kit zsaroló vírus?” kérdésre adandó válaszhoz, különösen ajánlom e dolgozat 9. fejezetét, amelyben ez olvasható:

A „húsevő” NAGY TESTVÉR
Az USA Szövetségi Nyomozóiroda (FBI) emberei már néhány órával a 2001. szeptember 11-i terrortámadások után telepíteni kezdték a ***Carnivore (húsevő)*** névre keresztelt Internet lehallgató rendszert az amerikai internetszolgáltatók szervereire. Hivatalosan deklarált célja a bűncselekményekkel gyanúsított személyek e-mail üzeneteinek felügyelete volt.
A Carnivore rendszer (hivatalos neve: DCS 1000) milliónyi e-mailt tud másodpercenként átnézni. A rendszert az FBI quanticoi ügynökségén Edward Hill speciális ügynök tervei alapján fejlesztették ki. A Carnivore-t a használathoz közvetlenül az Internet szolgáltató hálózatára kell kapcsolni. Ha ez megtörténik, elméletileg figyelhető minden felhasználó kommunikációja, kezdve a levelezéstől az online banki műveleteken át a webezésig.
Ez a rendszer jelentős jogi problémákat vet fel a békés, jószándékú internetezők személyiségjogainak megsértésével kapcsolatban. Az Electronic Privacy Information Center (EPIC: Elektronikus Adattitkossági Központ) alig pár hónappal a Carnivore telepítése után

Kit „zsaroló vírus”?

jelezte a nyilvánosság számára, hogy ez az email megfigyelőrendszer potenciális visszaélésekre ad lehetőséget.
Az ECHELON-nal ellentétben, a Carnivore-t már nem tudták évtizedekig titokban tartani. Az EPIC hatására az FBI már 2000. januárjában Edward Hill aláírásával nyilatkozatot adott ki, amelyben elismerte a rendszer létezését. A nyilatkozat fontosabb állításainak magyar fordítása:
„Én Edward Hill a következő nyilatkozatot teszem:
1. Az FBI speciális ügynöke vagyok 10 éve. A műszaki berendezésekre specializálódtam, beleértve az elektronikus lehallgató berendezéseket. Jártas vagyok az Internet és az Internet lehallgatására szolgáló eszközök alkalmazásában.
2. Ha engedélyezik, én vagy más technikusok üzembe helyezünk egy Carnivore nevű programot. A program az EarthLink hálózat routerére lesz telepítve. …. A router és az EarthLink hálózat egyaránt a telefonvonalakhoz kapcsolódik és a csomagkapcsolt hálózat információit továbbítja a telefonvonalakon. A Carnivore program figyeli az EarthLink-re bejövő telefon forgalmat, és regisztrálja az üzenetek aláírójának log-in nevét, vagy email azonosítóját. … A program sem az üzenet tárgyát, sem annak tartalmát nem rögzíti.
3. … Mivel a számítógép kapacitás korlátozott, a program pár percenként 8-10 millió email feldolgozását képes elvégezni.”

A 21. század információalapú társadalmának tehát kulcskérdése a hatalom és a civil társadalom közötti egyenrangú és egyenszilárdságú információbiztonság. Ennek megvalósításához vezető úton az első lépés az lenne, hogy megfogadjuk N. Wiener azon intelmét, amelyet a NAGY TESTVÉR megszületésével egyidőben fogalmazott meg:
„Az amerikai világban az információ sorsa az, hogy áru lesz. Nem az én dolgom elbírálni, hogy ez a kereskedői szemlélet erkölcsös-e vagy sem, az én dolgom az, hogy megmutassam, ha ez a szemlélet érvényesül, az az információ és a vele kapcsolatos fogalmak félreértéséhez és főleg félrekezeléséhez vezet.”
Norbert Wiener idézett gondolata tehát nem csupán az információra, hanem az információ-alapú társadalomra is igaz. A Wiener által jelzett „félreértések” és „félrekezelések” társadalmi méretekben végzetesek lehetnek, ami egyértelműen arra a következtetésre vezet, hogy A JÖVŐ BIZTONSÁGOS TÁRSADALMA NEM LEHET ÜZLETI VÁLLALKOZÁS!”

Zárszóként még egy idézet a tanulmányból:

„Egészen megdöbbentő, hogy a demokrácia és a polgári szabadságjogok paradicsomaként, a Föld többi országa számára példaképül szolgáló USA-ban, csupán egy névtelenül nyilatkozó biztonságtechnikai szakember próbálta a nyilvánosság előtt elismerni: *„A legtöbb szakmabeli, aki az USA-ban tud az ECHELON-ról és más elektronikus lehallgatási technikákról, kapcsolatban áll az NSA-val, vagy más állami ügynökséggel és ezek tanácsára nem feszegetik a témát. Eddig egyedül az Európai Unió merte hivatalosan vizsgálni ezeknek a rendszereknek a működését.”*

Budapest, 2017. május