Humanitarni ransomware i hakirani izbori

Bliži se kraj godine pa osjećamo potrebu da sumiramo zbivanja u staroj i napravimo planove za Novu. Nova mora biti bolja, zar ne? ***By default***, iliti našijenski, po ogluhi. To bi značilo da će biti bolje ako ništa ne uradimo, dakle samo po sebi. Jer svijet napreduje, svakog dana u svakom pogledu, a tehnologija najbrže od svega. Pa hajdemo pogledati kakav je to napredak.

Jeste li znali da svakih 7,5 sekundi s tekuće vrpce izađe jedan novi Raspbery Py i da kompletan proizvodni proces traje samo 20 minuta? Radi toga je to malo britansko čudo od računala, veličine kreditne kartice, namijenjeno podučavanju klinaca, tako jeftino... Novi model je 6x snažniji od prethodnika i može se mirne duše koristiti kod kuće kao osobno računalo.

Čudo posve drugačije vrste možda ste našli u svom Facebook profilu: obavijest o tome kako je netko od vaših "prijatelja" objavio seksi filmić s jednom od glamuroznih filmskih diva u glavnoj ulozi, filmić koji je nekim čudom procurio u javnost? Vjerojatno sam u pravu kad pretpostavljam da nitko od sistemaca nije kliknuo na ovakav link:

Jessica_Alba-Leaked-sextape V-ideoSun_Dec_4_2016_19_41pm.mp4.pdf

Ako ništa drugo onda će vam dvije ekstenzije signalizirati da nešto nije u redu. Ukratko, klik otvara web stranicu s agresivnim reklamama, (s)eksplicitnim sadržajima i lažnim lutrijama. Dodatno će se usrećiti korisnici Googleovog Chrome preglednika, kojima će otvoriti lažna Youtube stranica s Play tipkom, koja nudi instalaciju specijalnog dodatka koji omogućuje gledanje obnaženih glumica. Dodatak blokira stranicu s postavkama Chromea gdje biste ga mogli deaktivirati. Blokira i brojne antivirusne stranice na kojima biste potražili zaštitu. Ukratko, dodatak se brani od deinstalacije. Istraživači su pronašli kako ga maknuti: otvorite *Registry editor*, potražite i uklonite ključ:

HKEY_LOCAL_MACHINE\Software\Google\Chrome\Extension

A onda još treba pobrisati kompletan direktorij koji sadrži sve Chrome ekstenzije. One koje želite i trebate morat ćete ponovo instalirati.

Linux se ne spominje, pa pretpostavljamo da je ugrožen samo Chrome na Windowsima.

Dobar sistemac osjeća potrebu da upozori korisnike da ne nasjedaju ovakvim prijevarama. Iskusan sistemac zna da je to uzaludan posao, uvijek će netko kliknuti i to više puta. Neki su korisnici naprosto recidivisti, ne možeš ih zaštiti od njih samih. Ipak, dobro je znati kako počistiti nered, jer i to spada u opis posla. Potpuniji opis štete koju bi klik na taj link napravio možete pronaći ovdje: http://thehackernews.com/2016/12/facebook-scam-malware.html [1]

Akademski časopis IEEE Security & Privacy objavio je rad istraživača sa Sveučilišta u Newcastleu koji su pronašli slabost pri kupovanju kreditnim karticama na Internetu. Napravili su program koji je u stanju za 6 sekundi otkriti rok važenja Visa kartice i tajni broj upisan na poleđini. Pri tome se ne koristi neka komplicirana matematička logika, već program nasumice iskušava sve kombinacije na tridesetak online trgovina. Većina ih dozvoljava 20 promašaja, nakon čega program ispituje kombinacije na drugim lokacijama, sve dok transakcija ne prođe. Prije toga potrebno je na Darknetu nabaviti važeće brojeve kreditnih kartica dobijene hakiranjem servera.

Zanimljivo je da MasterCard ima bolju zaštitu jer ima zadan manji prag za pogrešne unose i sustav

koji to dojavljuje centrali, tako da se brzo ustanovi da netko pokušava neovlašteno koristiti karticu. Istraživači su upozorili kartičare i web dućane, ali na njihovo veliko čuđenje nitko se od njih još nije pozabavio poboljšanjem zaštite. Ako nam je dozvoljeno razmišljati zašto su tako nonšalantni, prisjetit ćemo se da oni rade procjene rizika i važu kolike gubitke mogu podnijeti. Ne isplati se ulagati u skupu zaštitu ako je jeftinije istrpiti manje gubitke. Zato, između ostalog, ne čudi da većina bankomata još uvijek radi na Windowsima XP.

Korisnicima kreditnih/debitnih kartica nije svejedno hoće li netko "peglati" njihove kartice na mreži. Preporučuje se redovito praćenje troškova na kartici i reagiranje u slučaju da je kartičarska kuća to propustila. Istraživački rad dostupan je na ovom linku [2].

Neki od nas već su imali bliske susrete s *ransomwareom* koji je našim korisnicima kriptirao datoteke i tražio novac za njihovo otključavanje. Nedavno se pojavila nova verzija, koja se naziva ***Popcorn time***. (Tim se imenom koristi site koji omogućuje besplatno gledanje filmova). Za otključavanje *ransomware* traži 1 Bitcoin (trenutno oko 770 $). Za one koji nemaju novca, nudi se dodatna mogućnost: zarazite još dva korisnika i dobit ćete ključ za dekriptiranje besplatno! Rok za razmišljanje je 7 dana, nakon čega se ključ briše i datoteke su zauvijek izgubljene.

Čovjek bi trebao biti psihopat da pristane na takav kriminalan prijedlog. No iskusan sistemac već se susretao s takvom vrstom ljudi. Njih nije briga za druge i ne osjećaju ni empatiju ni grižnju savjesti. Neki od njih su bolesno ambiciozni, usmjereni na vlastiti uspjeh i izgradnju karijere. Statistički je posve vjerojatno da će se netko pokušati izvući tako što će druge uvaliti u nevolju. Ako dva novozaražena korisnika uplate po Bitcoin, "siromah" će dobiti ključ za dekripciju besplatno.

No začudnost koju ovaj "kokičar" izaziva time ne prestaje. Autori kažu za sebe da su hakeri iz Sirije koji svakodnevno trpe nasilje i izgubili su nekoga od rodbine ili prijatelja u građanskom ratu kojeg su raspirile vanjske sile. Svijet je ravnodušan prema njihovom stradanju, pa su odlučili nešto poduzeti. Garantiraju da će se prikupljeni novac iskoristiti za nabavu hrane i lijekova, kako bi se ublažilo stradanje civila.

Ovako postavljeno objašnjenje trebalo bi, pretpostavljam, olakšati širenje zaraze: sve je to za više dobro! Ucjenjeni smo da pomažemo ljudima u nevolji, to nam je kazna za našu posvemašnju ravnodušnost prema stradanjima drugih. Naravno, sve pod pretpostavkom da je ta priča istinita. Možda se time zapravo financiraju upravo grupe koje koriste ljude kao živi štit.

Za kraj smo ostavili još malo politike. Nedavno smo pročitali vijest da je Rusija usvojila novu strategiju cyber ratovanja. Vijest je veličine poštanske marke, bez "suvišnih" detalja. Zatim smo saznali da je hakiran server našeg Ministarstva vanjskih poslova, "ali nisu iscurile nikakve važne informacije". Nema čvrstih dokaza, ali sumnja se na Ruse. Slijedi vijest iz SAD: predsjednik na odlasku naložio je obavještajnoj zajednici analizu ruskih hakerskih napada i njihov utjecaj na nedavne predsjedničke izbore. Sumnja se da su se ruski hakeri dočepali privatnih e-mailova demokratske kandidatkinje i objavili ih na Wikileaksu, čime su utjecali na birače. Naravno, Trump je takve spekulacije nazvao smiješima. U svakom slučaju Kongres će dobiti izvještaj prije nego Trump preuzme Bijelu kuću.

Ti zločesti Rusi, često su vijestima u ulozi negativaca! Čovjek bi pomislio da su oni jedini, uz Kinu i Sjevernu Koreju, koji zloupotrebljavaju hakerske vještine u političke i obavještajne svrhe. Ameri i EU to ne rade, sram ga bilo tko to pomisli. Eto i dokaza: vijest o tome da je FBI u 2015. godini koristio sigurnosni propust u Toru da bi pohvatao negativce koji traže i distribuiraju dječju pornografiju. Hakirali su 8700 računala u 120 zemalja. U dobre svrhe. Nema problema zar ne, tko će stati u obranu pedofila. No ipak problem je u tome da Tor koriste i drugi, na primjer novinari za komunikaciju sa svojim izvorima kojima žele sakriti identitet, ili brojni aktivisti koji su na meti svojih nedemokratskih vlada. Više na ovom linku [3].

I što na kraju zaključiti iz ovog mozaika vijesti iz IT područja i informacijske sigurnosti? Već smo u ovoj rubrici govorili o tome da je svijet postao prekompliciran i nepregledan, neshvatljiv, a preobilje informacija i kultura konzumerizma ljude osamljuje. Što je u takvom svijetu "viši cilj, vrijednost koja opravdava nečasna sredstva za postizanje časnog cilja?" Kako bismo mogli osuđivati sirijske hakere (ako je ta priča uopće istinita), a ne osuđivati velike sile koje preko leđa Sirijaca ostvaruju svoje

globalne strategije? Da li jedan običan sistemac uopće treba razmišljati o tome? Ili se naprosto prepustiti, odustati od pokušaja razumijevanja svijeta i brinuti samo za sebe? Pa to se od njega u ovakvom svijetu i očekuje, odustajanje od svake vrste aktivizma. Dopušteno je rezignirano kukanje po kafićima.

Što nam na kraju preostaje osim naše vlastite savjesti? Pod prepostavkom da savjest nije nešto što izumire, zajedno sa suosjećanjem i osjećajem krivice. Sam Vaknin, zloguki prorok novog doba, kaže da svijetom upravljaju narcisoidni psihopati, usmjereni k cilju i bez ikakve emocije prema žrtvama vlastite ambicije. Internet i informacijske tehnologije samo su hranjiva podloga na kojoj bujaju ljudske aspiracije. A za razliku od tehnologije, ljudska se vrsta vrlo sporo duhovno i moralno razvija.

Bit će bolje ako ništa ne učinimo, zar ne? :(

uto, 2016-12-13 09:52 - Aco Dmitrović**Kategorije:** Kolumna [4]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

Source URL: https://sysportal.carnet.hr/node/1712

Links
[1] http://thehackernews.com/2016/12/facebook-scam-malware.html
[2] http://eprint.ncl.ac.uk/file_store/production/230123/19180242-D02E-47AC-BDB3-73C22D6E1FDB.pdf
[3] http://thehackernews.com/2016/03/fbi-tor-browser-exploit.html
[4] https://sysportal.carnet.hr/taxonomy/term/71