Scareware / Sextortion / CryptoBlackmail

Tema

Primili ste sumnjivu poruku e-pošte (v. u nastavku) da…

- je vaš račun e-pošte *otet* ili *provaljen*
- je provaljeno na vaše računalo
- su preuzete vaše nedolične slike s web kamere
- ste posjetili zabranjene ili nedolične web stranice
- (ili neka slična poruka)

…i traži se od vas da platite ucjenu.

Ukratko

Nikakva reakcija s Vaše strane nije potrebna niti poželjna.

Poruku obrišite i zaboravite.

Nije se moguće potpuno zaštititi od primanja poruka ove vrste jer se šalju povremeno, s različitim tekstom, na brojne e-mail adrese s tuđih, legitimnih e-mail adresa čiji vlasnici ne znaju i u pravilu ne mogu spriječiti takvu zloupotrebu (najsličnija usporedba bi bila obično pismo – na poleđini omota se može napisati da šalje bilo tko).

ESET-ovi programi ESET Internet Security, ESET Smart Security Premium i / ili ESET Endpoint Security često prepoznaju da je riječ o neželjenim porukama i označe ih sa "[Spam]" kako bi Vas upozorili.

Opis

"Scareware" / "Sextortion" / "CryptoBlackmail" su programi i/ili e-mail kampanje koje alarmantnim upozorenjima ili obavijestima o prijetnjama imaju za cilj uplašiti korisnike, sve češće radi iznude novca ili Bitcoina. Povezan pojam: scam kampanje (kampanje prijevare). U e-porukama se od korisnika traži da uplate određen iznos kako bi izbjegli javno objavljivanje izmišljenih slika / videa izmišljenih događaja.

Najvažnije – ne morate brinuti.

U slučaju scareware / scam prijetnji / kampanja, radi se o pokušaju iznuđivanja Bitcoina na prijevaru. Činjenica da je Vaša e-adresa navedena u polju "Pošiljatelj:" ("From:") ne znači ništa; situacija s e-porukama je ista kao i s običnim pismima na kojima na poleđini možete napisati da šalje bilo tko i poslati bilo kome. U mailu može biti navedena i neka Vaša stvarna lozinka (aktualna ili jedna od onih koje ste nekada koristili) – do nje su došli na druge načine, ne "hakiranjem" Vašeg računala nego krađom podataka od onih koji su imali Vaše podatke, a nisu ih čuvali. Najčešći način je provala u nedovoljno zaštićene sustave koji imaju mnogo korisnika – ISP (teleoperateri, pružatelji internetskih usluga) su odličan cilj. U ovakvim kampanjama se jednim uspješnim napadom (koji može dugo trajati) pokradu podaci više milijuna, a ponekad i milijardi korisnika. (vidi https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html)

Što se tiče ESET-ovog programa – dakle, u slučajevima da je netko zaista i *hakirao* e-mail* sve bi se odvijalo na računalima na Internetu. ESET (kao i svi antivirusni programi) ipak štiti samo od malwarea (“*virusa*“) i to samo na računalima korisnika. ESET ne štiti računala pružatelja internetskih usluga. **Preuzimanje mail-adrese i čitanje poruka nije nemoguće niti nevjerojatno, događalo se mnogo puta i događat će se još mnogo puta. Vjerojatnost da se to dogodi Vama je mnogo veća ako koristite jednostavnu ili jednu od onih koju “svi koriste” (“qweqwe”, “admin123”, “lozinka”, …).* Obavezno napravite ono što nema veze s “*virusima*” – svakako redovito radite backup svih podataka. Više informacija o tome kako provoditi backup možete pronaći u ovom članku baze znanja: https://www.nod32.com.hr/podrska/kb10442

Ovo je dobrodošao podsjetnik da promijenite lozinke na Internetu (i radite to redovito – barem jednom godišnje, u idealnim uvjetima i češće). Ali nemojte ih promijeniti tako da kliknete na lonk u mailu u kojemu ste dobili i upozorenje! Otvorite stranicu i pregledniku (browseru) bez klikanja na link u e-poruci. Najbolje lozinke sadrže kratku rečenicu koju lako pamtite, a računalima treba mnogo vremena (godine, stoljeća) da ju pogode. Npr. lozinka “*Najbolje lozinke sadrze 1 kratku recenicu.*” je mnogo sigurnija i lakše se pamti od lozinke “N0r4!3534”.

Primitak ovakvih poruka s prijetnjama je odličan podsjednik i da pokrenete periodično skeniranje sustava računala. Preporučeni postupak možete pronaći u članku https://www.nod32.com.hr/podrska/kb10129. Obratite se eventualno svojem pružatelju usluga e-pošte (VIP/A1, T-Com, itd…) te im proslijedite poruku e-pošte koju ste dobili. U slučajevima kad takvi mailovi dolaze s računala nekog od pružatelja usluga oni mogu upozoriti korisnika i privremeno blokirati njihov račun (prijeteće e-poruke se u pravilu šalju s inficiranih računala i korisnici ne znaju da od njih stižu prijetnje). Zaražite od pružatelja usluga da Vam objasne kako su lozinke velikog broja njihovih korisnika dospjele u ruke napadačima.

E-adrese hrvatskih Abuse službi:

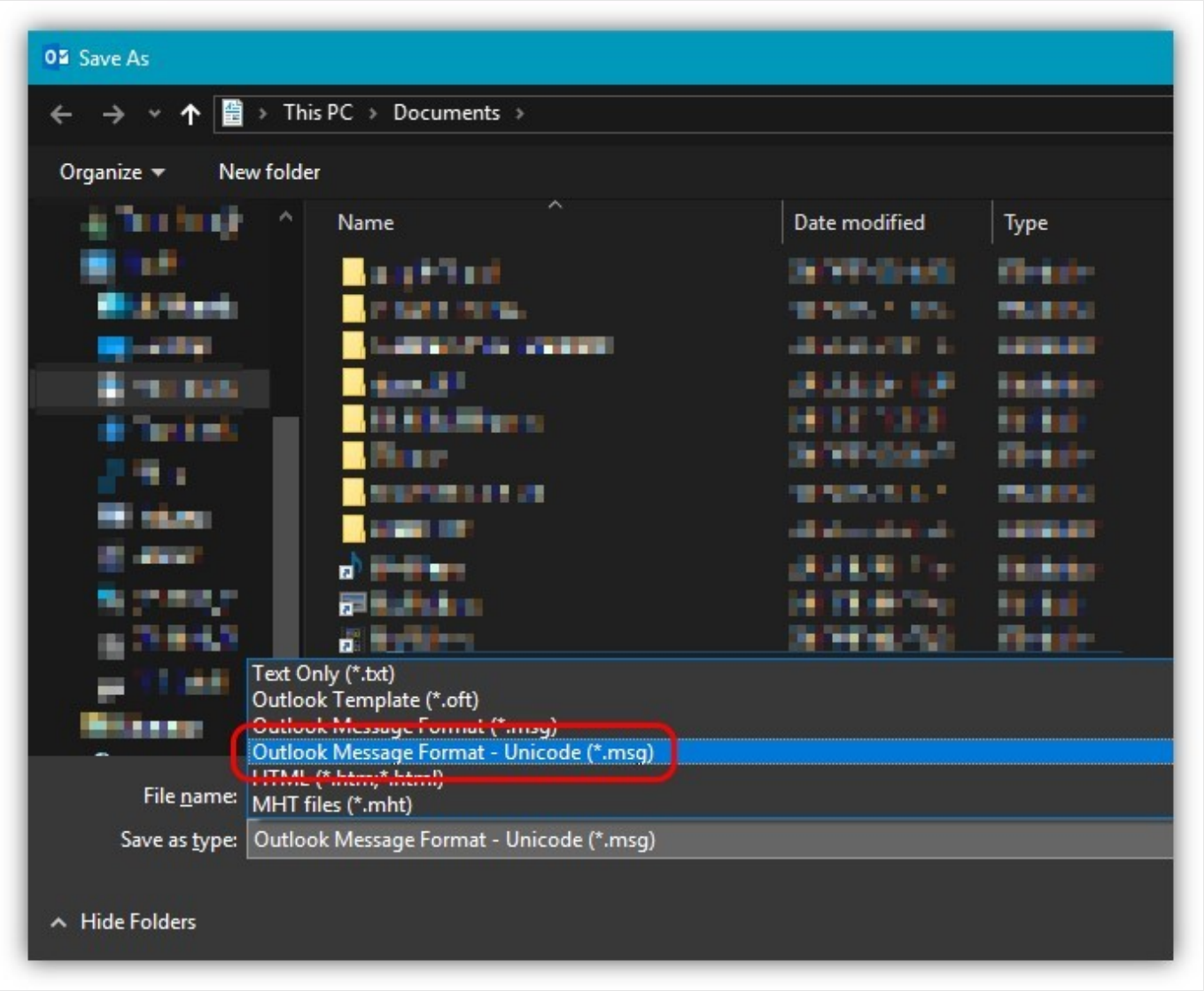
- Amis Telekom – abuse@amis.hr
- Bnet – abuse@xnet.hr
- H1 – abuse@h1telekom.hr
- Iskon – abuse@iskon.hr
- Metronet – abuse@metronet.hr
- Optima Telekom – abuse@optima-telekom.hr
- T-Com – abuse@t.ht.hr Tele2 – abuse@tele2.hr
- VIPnet / A1 – abuse@vip.hr

Ako se tako dogovorimo, sumnjivu poruku proslijedite nama, kako bismo ju analizirali.

Slanje .MSG ili .EML datoteke

Microsoft Outlook

- Ako koristite Outlook u ovome Vam može pomoći Microsoftova uputa: https://support.office.com/hr-HR/article/spremanje-poruke-u-obliku-datoteke-4821bcd4-7687-4d6d-a486-b89a291a56e2
- U koraku 2 odaberite (*.MSG), prema slici:



Mozilla Thunderbird – imate tri opcije za takvo spremanje e-poruke:

- U Thunderbird klijentu odaberite poruku, potom u meniju odaberite File > Save As > File
- Desnom tipkom kliknite na željenu poruku i iz kontekstnog menija odaberite Save As
- Jednostavno pritisnete Ctrl + S…

Dodatne informacije i linkovi na povezane članke baze znanja

Primjeri prijetećih e-poruka

1. Hello <<%RecipientAddress%>> My nickname in darknet is xxxxxxxxxx. I'll begin by saying that I hacked this mailbox (please look on 'from' in your header) more than six months ago, through it I infected your operating system with a virus (trojan) created by me and have been monitoring you for a long time. Even if you changed the password after that – it does not matter, my virus intercepted all the caching data on your computer and automatically saved access for me. I have access to all your accounts, social networks, email, browsing history. Accordingly, I have the data of all your contacts, files from your computer, photos and videos. I was most struck by the intimate content sites that you occasionally visit. You have a very wild imagination, I tell you! During your pastime and entertainment there, I took screenshot through the camera of your device, synchronizing with what you are watching.Oh my god! You are so funny and excited! I think that you do not want all your contacts to get these files, right? If you are of the same opinion, then I think that $500 is quite a fair price to destroy the dirt I created. Send the above amount on my bitcoin wallet: <<%BitcoinWallet%>> As soon as the above amount is received, I guarantee that the data will be deleted, I do not need it. Otherwise, these files and history of visiting sites will get all your contacts from your device. Also, I'll send to everyone your contact access to your email and access logs, I have carefully saved it!Since

reading this letter you have 48 hours! After your reading this message, I'll receive an automatic notification that you have seen the letter. I hope I taught you a good lesson. Do not be so nonchalant, please visit only to proven resources, and don't enter your passwords anywhere! Good luck!

2. Valjda se pitate zašto primate ovu poruku e-pošte? Bilo bi vrlo korisno za vašu privatnost ako ga niste zanemarili. Postavio sam zlonamjerni softver na web-lokaciju za odrasle (... P... 0... r... n web-lokacija) i kao što ste posjetili i gledali videozapis na koji je uređaj pogođen stavljajući spyware na uređaj. Što vas je snimilo s kamerom i snimanjem zaslona dok ste imali "zabavno vrijeme" što mi omogućuje da vidim točno ono što vidite. To je također utjecalo na smartphone putem Expl0it. Stoga nemojte misliti na jednu minutu da to možete zaobići ponovnim instaliranjem OS-a. Već ste zabilježeni. Nakon toga su zlonamjeri prikupili sve glasnike, e-poštu i društvene mreže. Pretpostavljam da ovo nije dobra vijest? No nemojte se previše brinuti, postoji način na koji možemo riješiti ovaj problem s privatnošću. Sve što trebam je Bitcoin plaćanje od £ 2.600 GBP što mislim da je fer cijena s obzirom na okolnosti. Adresa za uplatu je: <<%BitcoinWallet%>> Ako ne razumijete bitcoin, idite na YouTube i potražite "kako kupiti bitcoin" ili google za "lokalne bitcoine", to je prilično jednostavno za napraviti. Imate samo 48 sati nakon čitanja ove e-pošte za slanje plaćanja (budite upozoreni da znam kad ste otvorili i pročitali ovu poruku e-pošte, postavio sam sliku piksela koja mi omogućuje da znate kada ste točno otvorili poruku koji dan i vrijeme) Ako odlučite zanemariti ovu poruku e-pošte, nemam izbora nego proslijediti videozapis svim prikupljenim kontaktima koje imate na svom računu e-pošte, kao i postavljati na račune društvenih medija i poslati ih kao osobnu poruku svim Facebook kontaktima , i naravno da je videozapis javno dostupan na internetu, putem YouTubea i web mjesta za odrasle. s obzirom na vašu reputaciju, vrlo sumnjam da želite biti izloženi vašoj obitelji / prijateljima / suradnicima tijekom ovog trenutnog vremena. Zapravo možete ići u policiju, ali ti ljudi vjerojatno neće učiniti ništa, najznačajnije stvari koje mogu učiniti je zaključavanje novčanika i uskratit će druge ljude od mogućnosti plaćanja. Stoga razmislite dvaput prije nego što budete radili gluposti. Ako primim uplatu, svi će materijali biti uništeni i nikad više nećete čuti od mene. Ako ne dobivam sredstva iz praktički bilo kojeg razloga, kao što je nemogućnost slanja novca na novčanik na crnoj listi – će se ugled uništiti. Zato je brzo. Imajte na umu da je ovdje Bitcoin adresa za prijenos računa – <<%BitcoinWallet%>> Nemojte pokušavati stupiti u vezu sa mnom jer koristim e-poštu žrtve koja je bila sjeckana i izložena. Samo odgovorite ako ste obavijestili da ste izvršili uplatu ili imate pitanja o uplati, a zatim kliknite odgovor. Ako ne vjerujete i želite dokaz samo odgovoriti na ovu poruku e-pošte s "PROOF" i ja ću poslati videozapis na 5 vaših kontakata putem e-pošte i objaviti na Facebook zidu. U kojem ćete ga moći ukloniti jednom, ne zauvijek

3. Zahtjev za plaćanjem fakture — Pozdrav! Nažalost, imam loše vijesti za vas. Prije nekoliko mjeseci dobio sam pristup uređaju koji upotrebljavate za pretraživanje interneta. Od tada pratim vašu internetsku aktivnost. Budući da ste redoviti posjetitelj web-stranica za odrasle, mogu potvrditi da ste vi odgovorni za to. Da budem jednostavan, web-stranice koje ste posjetili pružile su mi pristup vašim podacima. Učitao sam trojanskog konja na osnovu upravljačkog programa, koji ažurira svoj potpis nekoliko puta dnevno kako bi onemogućio da ga antivirusni program otkrije. Uz to, omogućuje mi pristup vašoj kameri i mikrofonu. Nadalje, stvorio sam sigurnosnu kopiju svih podataka, uključujući fotografije, društvene mreže, razgovore i kontakte. Nedavno sam dobio sjajnu ideju da napravim video u kojem svršavate u jednom dijelu zaslona, dok se video istovremeno reproducira na drugom zaslonu. To je bilo zabavno! Budite sigurni da mogu jednostavno poslati taj video svim vašim kontaktima uz nekoliko klikova, a pretpostavljam da biste htjeli spriječiti taj scenarij. Imajući to na umu, evo mog prijedloga: Uplatite iznos od 1500 EUR na moj novčanik za Bitcoin i zaboravit ću na cijelu stvar. Također ću trajno izbrisati sve podatke i videa. Prema mom mišljenju, to je prilično skromna cijena za moj rad. Možete shvatiti kako kupiti Bitcoine pomoću tražilica poput Googlea ili Binga, budući da to nije jako teško. Moj novčanik za Bitcoin (BTC): <<%BitcoinWallet%>> Imate 48 sati vremena za odgovor, a trebali biste također imati na umu sljedeće: Nema smisla da mi odgovarate – adresa je napravljena automatski. Nema smisla ni da se žalite, s obzirom na to da se pismo, kao i moj novčanik za Bitcoin, ne može pratiti. Sve je precizno organizirano. Ako ikad otkrijem da ste nekome spomenuli bilo što u vezi s ovim pismom, video će odmah biti podijeljen, a vaši će kontakti biti prvi koji će ga primiti. Nakon toga, video će biti objavljen na internetu! P. S. Odbrojavanje će započeti kad otvorite ovo pismo (ovaj program ima ugrađeni mjerač vremena). Sretno i smirite se! Bila je to samo loša sreća, sljedeći put budite oprezni.

4. Pažnja Pretpostavljam da se pitate zašto dobro primate ovu e -poruku? Bilo bi vrlo korisno za vašu privatnost da je niste zanemarili. Davno smo na vaš telefon i elektronički uređaj stavili zlonamjerni softver/virus zvan Trojan, nadgledajući vaše aktivnosti dok varate partnera trebali ste znati da varate nekoga kome je stalo do vas nikad nije u redu. Imamo video i audio snimke koje smo napravili s vašeg telefona i drugih elektroničkih uređaja ok vas koji će uništiti sve za što ste radili. To je utjecalo i na vaš pametni telefon putem expl0ita. Stoga nemojte misliti da to možete zaobići ni minutu ponovnom instalacijom OS -a ili promjenom lozinke. Već ste snimljeni. Nakon toga naš je zlonamjerni softver prikupio kontakt vaših partnera, e -poštu prijatelja i obitelji te kontakte na društvenim mrežama. Pretpostavljam da ovo nije dobra vijest, zar ne? Ali ne brinite previše, postoji način na koji možemo riješiti ovo pitanje privatnosti. Sve što nam je potrebno je plaćanje bitcoinom u iznosu od <<%Iznos%>>, što je pošteno, s obzirom na okolnosti. Plaćanje je potrebno izvršiti na dolje navedenu bitcoin adresu: BITCOIN ADRESA ZA PLAĆANJE: <<%BitcoinWallet%>> Ako ne razumijete Bitcoin, kliknite odgovor na svoju e -poštu i odgovorite na ovu poruku, a mi ćemo vam reći kako kupiti Bitcoin. Imate samo 48 sati nakon čitanja ove e-pošte da pošaljete uplatu (upozorimo vas da znamo da ste otvorili i pročitali ovu e-poruku, stavio sam sliku piksela u nju. Što mi omogućuje da znam kada ste točno otvorili poruku koji dan i vrijeme) Ako odlučite zanemariti ovu poruku e -pošte, nećemo imati drugog izbora nego proslijediti video i zvuk svim prikupljenim kontaktima koje imate na telefonu, računu e -pošte i postaviti ih na internet. S obzirom na vašu reputaciju, jako sumnjamo da želite biti izloženi svojoj obitelji/prijateljima/suradnicima tijekom ovog trenutka. Ako primimo uplatu, sav će materijal biti

uništen i više nam se nećete javiti. Ako iz bilo kojeg razloga ne dobijemo novac, primjerice zbog nemogućnosti slanja gotovine u novčanik na crnoj listi – vaš ugled će biti narušen. Zato neka bude brzo. NAPOMENA: SJEĆAJTE SE DA PONOVNO POTVRDITE ADRESU BITCOINA S NAMA PRIJE NAVEDANJA PLAĆANJA DA IZBJEGNITE PLAĆANJE DVA PUTA. Ne pokušavajte stupiti u kontakt s nama jer koristimo e-poštu žrtve koja je hakirana i razotkrivena. Odgovorite samo tako da nas obavijestite da ste izvršili plaćanje ili imate pitanja u vezi plaćanja, a zatim kliknite odgovor.

Primjer phishinga

”Nakon uključivanja hrvatske kune u Europski tečajni mehanizam ERM II u srpnju 2020. godine kao faze koja je prethodila najavi uvođenja eura s planiranim datumom 1. siječnja 2023. godine. U (ime banke) smo započeli s pripremnim aktivnostima za konverziju nacionalne valute u euro. Molimo da ažurirate novu verziju aplikacije s (imenom banke preko koje posluje oštećeni subjekt) sukladno uputama koje se nalaze na linku ispod: <%Link%>.
S tim ćete uspješno ažurirati neophodne korake za nesmetan rad mobilne aplikacije i prilagodit je ERM II tečajnom mehanizmu.”

SOLNxxxx xsextortionx xscarewarex xucjenax mlwr xmlwr
