Hoidu koroonaviirust ärakasutavatest pettustest

6 aastat tagasi - 19.03.2020 Autor: AM

Sogases vees on alati neid, kes tulevad segadusest kasu lõikama. Praegu levib massiliselt pettusi, mis seotud kroonaviirusega ja mis aitavad ka paanikat õhutada, võttes terve mõistusega asjadele lähenemise kaotanud inimestelt raha ära. ESET kirjeldab mõnesid enamlevinud juhtumeid.

Alates pahavaraga nakatunud meilidest kuni võltsannetusteni - need on ühed sagedaseimad pettused, millega tuleb rahvatervise kriisi ajal arvestada.

Koroonaviiruse 2019 (COVID-19) puhang – mis on kuulutatud ametlikult pandeemiaks – on põhjustanud ülemaailmset ebakindlust, põhjustades seisakuid, reisikeelde, paanilist ostlemist ja finantsturgude ebastabiilsust.

Ka petturid on seda kõike märganud. Hädaolukorrad pakuvad kurjategijatele häid võimalusi käivitada rünnakuid ning kasutada ära murelikku õhkkonda. Seni enam kui 4000 surma põhjustanud ja jätkuvalt leviva haiguse taustal pole petturid aega raisanud ning on aktiivselt kasutanud ära inimeste hirmu, ilmutamata kübetki kaastunnet.

Mõned küberkurjategijad on arvamusel, et nende jõulukingitused on saabunud sobival ajal: murelik elanikkond, riskirühmas olevad haavatavad inimesed, defitsiit teatud kaupade nõudluses ja suurel hulgal valeteavet sotsiaalmeedias – kõik see võrdub tohutu võimalusega petta inimesi just siis, kui nad on kõige vastuvõtlikumad.

Pettused esinevad erinevates vormides ja turvatarkvara tootja ESET uurimisrühm toob välja paar näidet taktikatest, mida on viimasel ajal kasutatud.

Kuritahtlikud uudised

Maailma Terviseorganisatsiooni (WHO), kui peamist teabeallikat haiguspuhangu ajal, on kasutatud rünnakutes enim imiteeritud asutusena. Allpool toodud näites pakuvad petturid olulist teavet viiruse kohta, lootes, et potentsiaalsed ohvrid klõpsavad pahatahtlikel linkidel. Tavaliselt võivad nimetatud lingid installida pahavara, varastada isiklikku teavet või proovida murda sisselogimistunnuseid ja

salasõnu.



Joonis 1. E-kiri Maailma Terviseorganisatsioonist.

WHO on teadlik, et petturid kasutavad nende nime, seetõttu on WHO avaldanud oma veebilehel näiteid nende tavapärasest suhtlusstiilist ning jagab teavet oma tegevuse kohta ametlikes e-kirjades. Üks olulisemaid punkte on selline:

“Veendu, et saatja e-posti aadress oleks näiteks selline “‘person@who.int”. Kui pärast “@” sümbolit on midagi muud peale “who.int”, pole saatjaks WHO. WHO ei saada sõnumeid aadressidelt, mis lõppevad näiteks nii: „@ who.com”, „@ who.org” või „@ who-safety.org”. ”

Organisatsioon soovitab kontrollida ka e-kirjade linkide URL-e ning veenduda, et kogu veebisisu alguses on https://www.who.int/, mitte mõni muu domeen. Kahtluse korral sisesta aadress otse oma brauserisse.

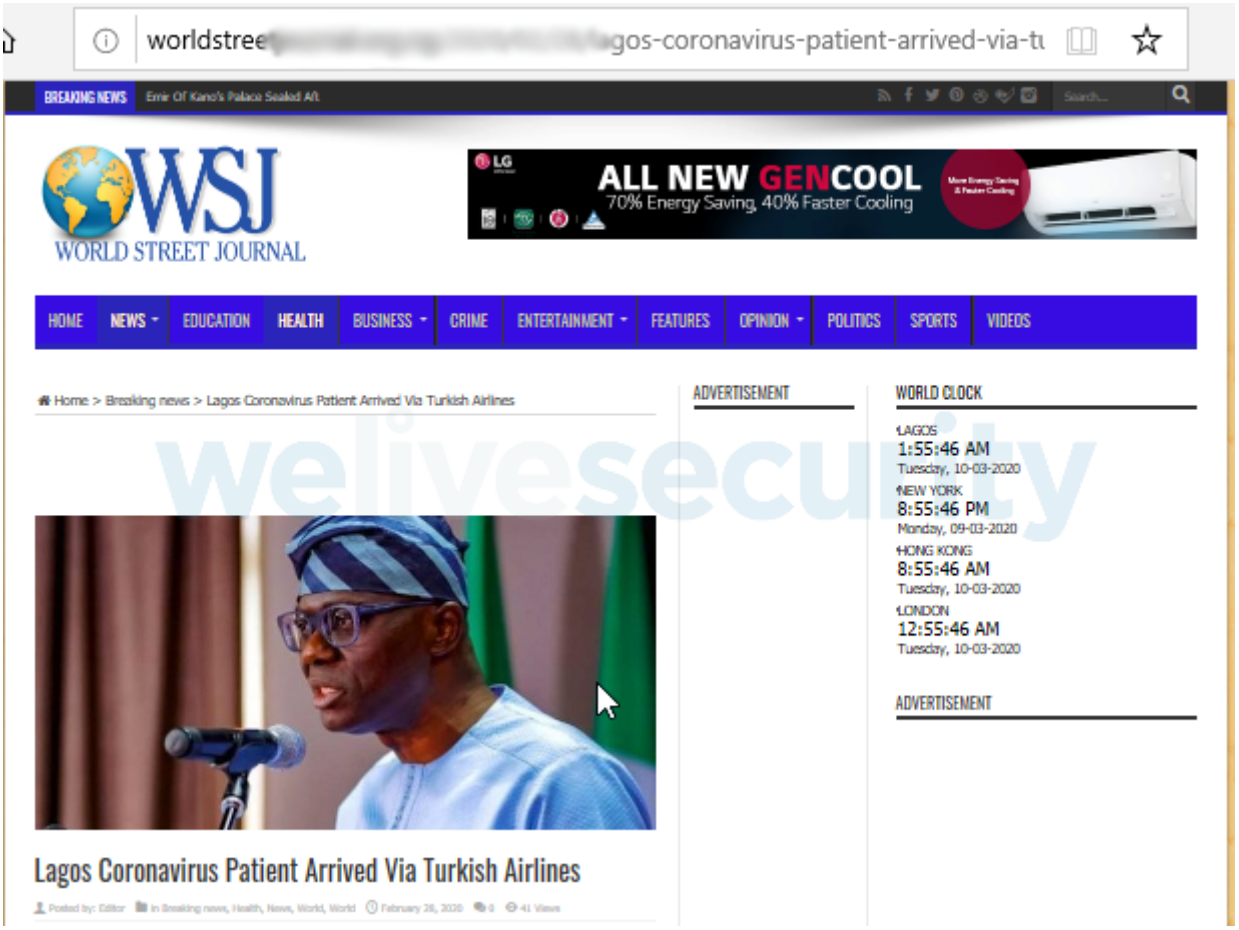
Oluline on meeles pidada, et WHO pole alustanud e-kirjade saatmist inimestele, kes pole mõnda nende teenust tellinud. Kaalu WHO saitide kasutamist või oma riiklike tervishoiuasutuse veebilehtede külastamist, näiteks Ameerika Ühendriikide Haiguste Tõrje ja Ennetamise Keskuse (Center for Disease Control and Prevention) (CDC) või Ühendkuningriigi Riiklikku Tervishoiuteenistuse (

National Health Service) veebilehtede kasutamist.

Rahuldamaks oma igapäevast meediatarbimist, võib päris uudiseid leida ka tavaolukorras kasutatavatest usaldusväärsetest allikatest. Soovimatud e-kirjade lingid pole ainulaadsed ning ei sisalda uusi uudiseid.

Järgmise näite puhul üritab allpool toodud andmepüügisait imiteerida Wall Street Journalit (WSJ) ning edastab väidetavalt kõige viimaseid uudiseid COVID-19 kohta. Oleme redigeerinud arusaadavatel põhjustel mõnda URL-i, ent pane tähele, et veebileht algab sõnaga “worldstreet” ja ka veebilehe sõnastus sisaldab fraasi “world street”.

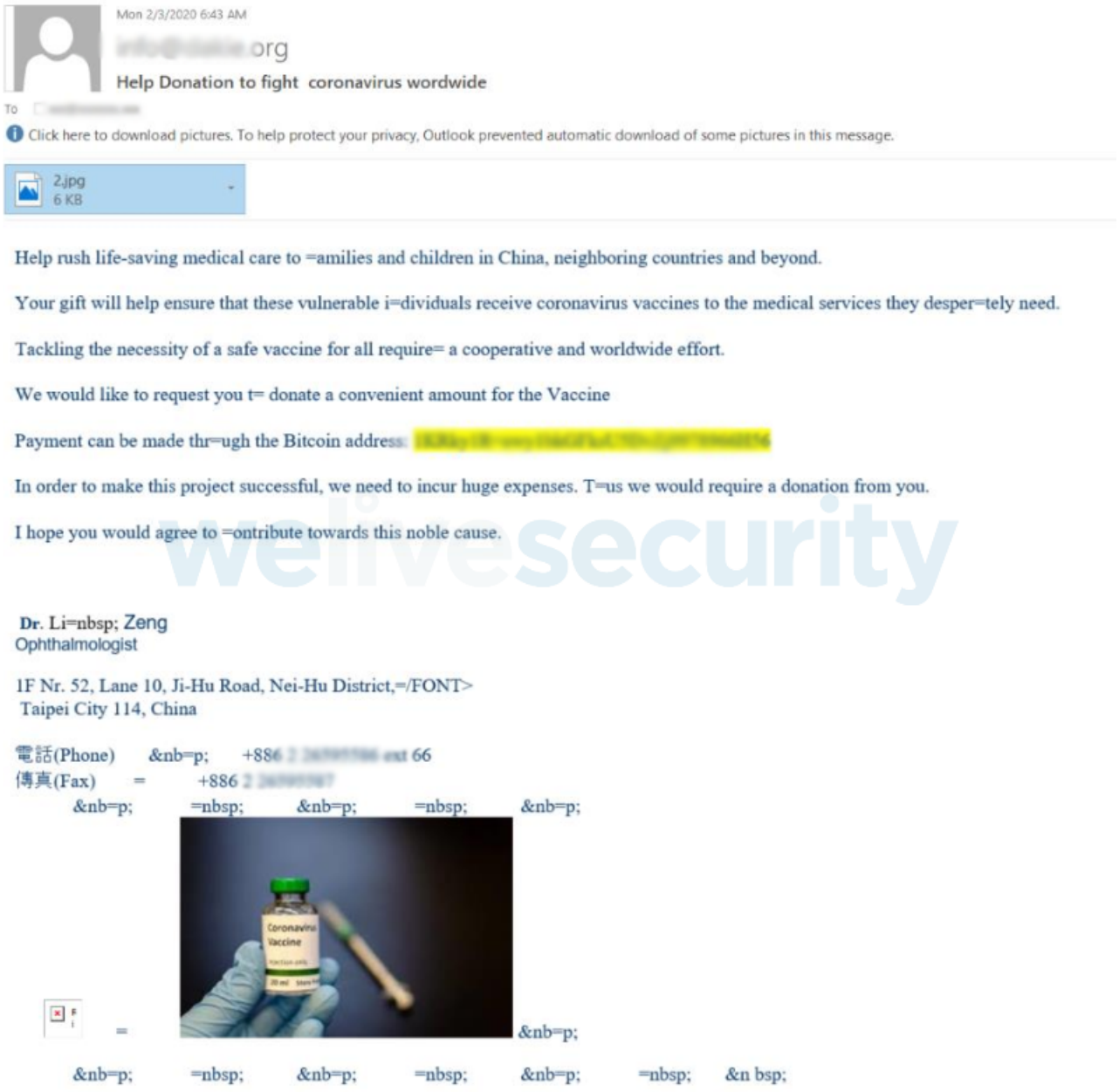
Sellegipoolest on WSJ-i brändiga visuaalse kooskõla kaudu üritatud petta kasutajat mõtlema, et tegemist on Wall Street Journaliga. Veebilehel kuvatav reklaam teenib kurjategijatele raha, seda ka juhul, kui kasutaja isikuandmed jäävad puutumata.



Joonis 2. Reaalsusest kaugel.

Heategevuse ärakasutamine

Üks levinud pettuste tüüp koputab inimeste südametele, üritades koguda rahastust Hiina laste vaktsiini rahastamiseks. Antud artikli kirjutamise ajal ei ole vaktsiini leiutatud ja eeldatakse, et avalikkus saab vaktsiini kasutada alles järgmisel aastal.



Joonis 3. Võlts-heategevus.

Antud näite huvitav asjaolu on, et kurjategija on olemasoleva rünnaku struktuuri ära vahetanud COVID-19 sisu vastu. ESET avaldas 2019. aastal info seksväljapressimise rünnaku kohta, millega üritati ohvritelt raha välja pressida.

Koroonaviiruse teemalisi e-kirju saavatel inimestel palutakse saata ründajatele bitcoine. Vaatamata sellele, et antud tehnika kasutamine on efektiivne ainult

murdosa kasutajate jaoks, võib see globaalses mastaabis olla kurjategijatele rahaliselt vägagi atraktiivne.

Maskipaanika õhutamine

Seda tüüpi pettuste korral saadavad petturid rämpspostitusi, mis panevad inimesi uskuma, et ilma maskita ei ole nad viiruse eest kaitstud ja pakuvad maskide tellimist. Selle tulemusel avaldavad ohvrid petturitele tahtmatult ka oma isiklikku ja rahalist teavet.



Joonis 4. Petturite näomaskide pakkumised.

Nagu võis ka eeldada, näitab Google Trends, et terminite “kätepuhastusvahendid” ja “näomaskid” otsingumaht on saavutamas enneolematut taset. Kuna nõudlus ületab pakkumist, on ründajad üha enam võtnud sihtmärgiks inimesi, kes soovivad soetada kaitsevahendeid. Sky News i andmetel peteti ainuüksi veebruaris Ühendkuningriigis näomaskide

“müümisega” inimestelt välja 800 000 naela (üks miljon USA dollarit).

Näomaske on väga piiratud koguses, seega ole ettevaatlik ja osta ainult usaldusväärselt müüjalt, keda usaldad tavapäraste tellimuse (ja krediitkaardiandmete jagamisel) tegemisel.

Kokkuvõtteks - selliseid näiteid on palju

Need on vaid mõned näited selle kohta, kuidas küberkurjategijad üritavad kasutada ära viirusepuhangust tulenevat olukorda. See on sobiv aeg omandada või tuletada meelde nii eraisikutele kui ka ettevõtetele levinumaid viise, kuidas kasutatakse ära inimeste emotsioone suurte sündmuste ja hädaolukordade ajal.

On äärmiselt oluline olla valvas, tuvastada ja ignoreerida küberkurjategijate tooteid ja pettuste või libauudistega seotud küberhäireid. Siin on mõned põhitõed, mis aitavad kaasa sinu turvalisusele:

- Väldi tundmatute allikate ning e-kirjade linkide klõpsamist või failide allalaadimist ning veendu, et kiri on autentne isegi usaldusväärse allika puhul.
- Ignoreeri teateid, milles küsitakse sinu isiklikku teavet. Vajadusel kontrolli sõnumi sisu saatjaga või näiliselt esindatava organisatsiooniga üle ning tee seda läbi muu suhtlusvahendi.
- Eriti ettevaatlik tuleb olla e-kirjade suhtes, mis lisavad ärevustunnet ja kutsuvad sind üles tegutsema või pakuvad COVID-19 vaktsiini või ravimeid.
- Ole ettevaatlik võlts heategevusorganisatsioonide ja ühisrahastuskampaaniate osas.
- Kasuta mainekat ning mitmekihilist turvatarkvara, mis sisaldab kaitset andmepüügi vastu.

https://blog.eset.ee/et/2020/03/19/beware-scams-exploiting-coronavirus-fears/

- Uudised

- Turvalisus

Pilt

worldstree[illegible]gos-coronavirus-patient-arrived-via-tu

BREAKING NEWS Emir Of Kano's Palace Soaked Aft

WSJ
WORLD STREET JOURNAL

LG
ALL NEW GENCOOL
70% Energy Saving, 40% Faster Cooling

HOME | NEWS | EDUCATION | HEALTH | BUSINESS | CRIME | ENTERTAINMENT | FEATURES | OPINION | POLITICS | SPORTS | VIDEOS

Home > Breaking news > Lagos Coronavirus Patient Arrived Via Turkish Airlines

welivesecurity



Lagos Coronavirus Patient Arrived Via Turkish Airlines

Posted by: Editor In Breaking news, Health, News, World, World February 28, 2020 0 41 Views

ADVERTISEMENT

WORLD CLOCK

LAGOS
1:55:46 AM
Tuesday, 10-03-2020

NEW YORK
8:55:46 PM
Monday, 09-03-2020

HONG KONG
8:55:46 AM
Tuesday, 10-03-2020

LONDON
12:55:46 AM
Tuesday, 10-03-2020

ADVERTISEMENT