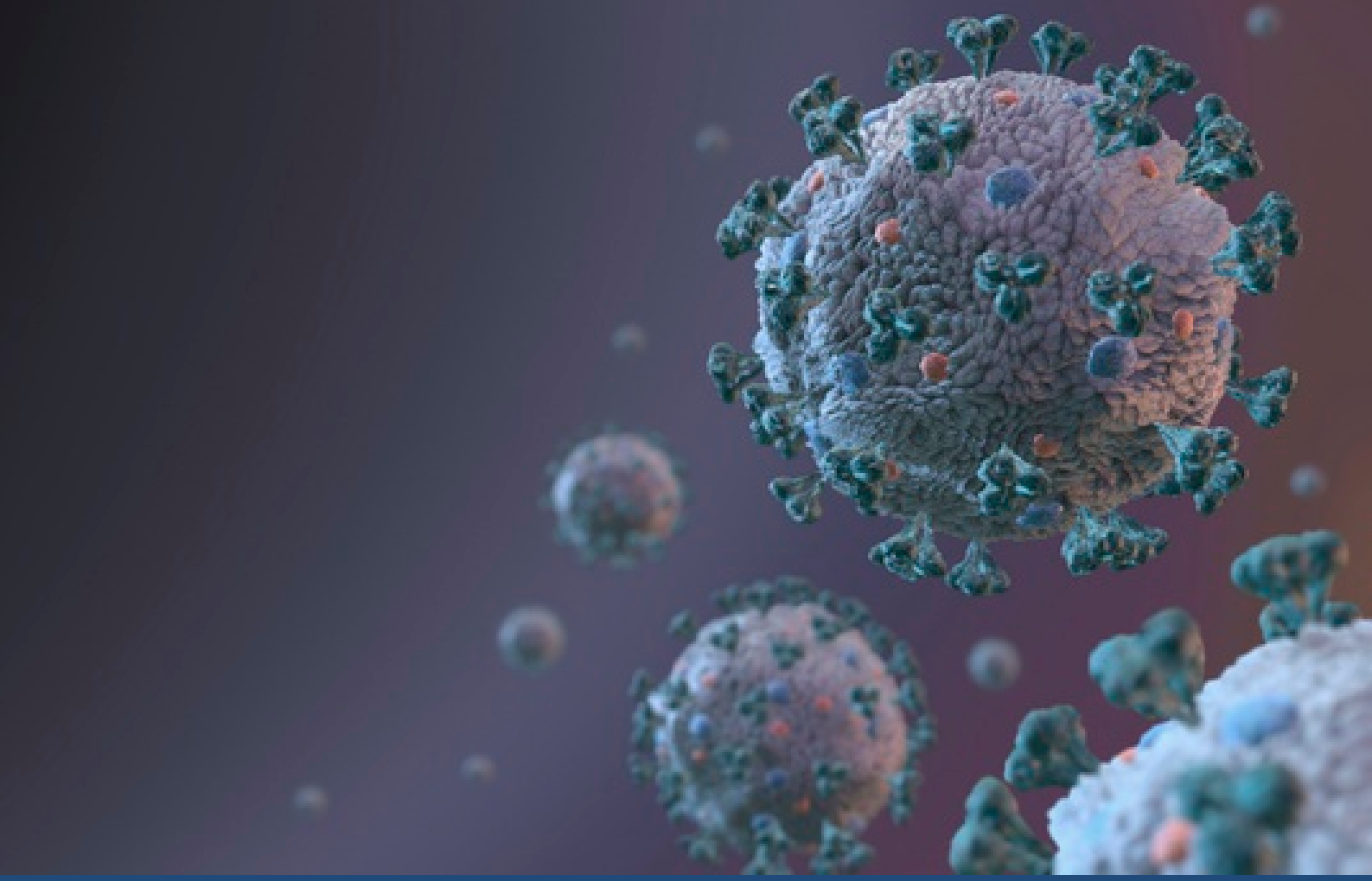


# ZLOUPOTREBA PANDEMIJE VIRUSA COVID-19 U SAJBER PROSTORU

PRIJAVITE SVAKI INCIDENT
NA NAŠEM PORTALU

SRB-CERT

# ZAŠTITA PODATAKA

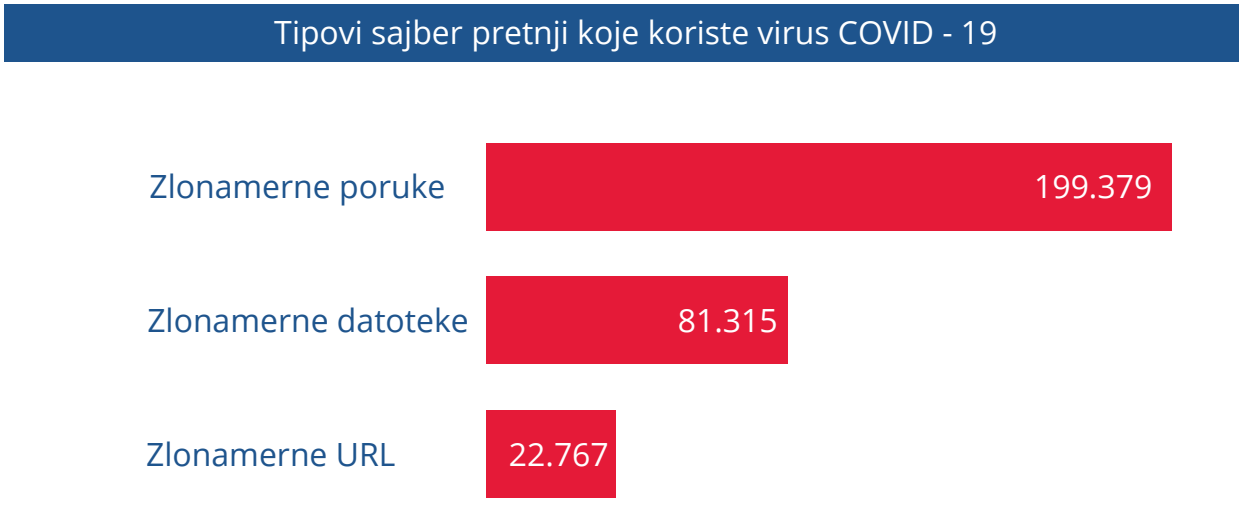
Od početka pandemije trudimo se da poštujemo zdravstvene i higijenske preporuke u cilju prevencije od virusa, a šta je sa prevencijom od sajber pretnji? Koliko sekundi traje provera poruka elektronske pošte, SMS poruka i drugih poruka koje dobijamo putem aplikacija za komunikaciju?

Sajber kriminalci koriste stanje pandemije i svakodnevno traže načine za zloupotrebu pretrage korisnika na internetu, koji žele da se informišu o savetima i vestima u vezi sa pandemijom. Sajber pretnjama smo svi podjednako izloženi, bez obzira da li internet koristimo u poslovne svrhe ili za pravovremeno i tačno informisanje.

Digitalizacija je sastavni deo svakodnevnog života u još većem obimu, pa internet koristimo za obavljanje radnih zadataka, učenje sa decom i informisanje o stanju pandemije. Sajber kriminalci iskorišćavaju stanje prilagođavanja na vanredne okolnosti života i rada, kao i borbe sa strahom od virusa i neizvesnosti, i pronalaze načine da dođu do naših podataka, koje čuvamo na prenosnim uređajima.

Jedan od načina napada su fišing kampanje koje distribuiraju maliciozni link ili dokument i za cilj imaju krađu podataka, a od korisnika se zahteva brza reakcija, najčešće samo jedan klik.

Dosadašnji podaci ukazuju da je u svetu do sada zabeleženo 300.000 jedinstvenih sajber pretnji koje zloupotrebljavaju pandemiju i manipulišu potrebom ljudi da budu informisani.




Slika 1 - Pretnje detektovane u periodu 01.januar-27.mart 2020.godine, Izvor: Micro Trend [1]

Još jedan vid zloupotrebe pandemije svakako predstavlja i masovno registrovanje lažnih internet stranica. Za vreme trajanja pandemije, značajno je povećan broj lažnih internet stranica koje koriste temu virusa COVID-19, odnosno sadrže neki od pojmova pandemije u nazivu domena ("Covid19/Coronavirus“). Pored distribucije sajber napada, ove stranice se koriste za lažnu prodaju medicinske opreme, suplemenata, lekova, vakcina i prevarom korisnika, hakeri dolaze do protivpravno stečene imovinske koristi.

[1] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains

Drugi vid zloupotrebe je masovno registrovanje lažnih internet stranica sa temom aktuelnog virusa. One se dalje koriste i za lažnu prodaju medicinske opreme, suplemenata, lekova, vakcina, a kao rezultat hakeri stiču protivpravnu imovinsku korist.

Od samog početka pandemije, a u cilju prevencije novonastalog virusa, trudimo se da poštujemo zdravstvene i higijenske preporuke. Međutim, šta je sa prevencijom kada su u pitanju sajber pretnje?

Vanredne okolnosti nastale sa pojavom korona virusa doprinele su povećanoj upotrebi interneta: virtuelne učionice, konferencijski pozivi, informisanje o stanju pandemije. Bez obzira na to u koje svrhe se internet koristi, sajber pretnjama su svi podjednako izloženi.

Prilagođavanje na vanredne uslove života i rada, takozvani sajber kriminalci planirano koriste. Dok se na jednoj strani korisnici interneta informišu, na primer, o
savetima i vestima vezanim za pandemiju, na drugoj strani sajber kriminalci svakodnevno traže nove načine za zloupotrebu aktivnosti na internetu.

Jedan od načina zloupotrebe je fišing kampanja. Naime, njom se distribuiraju maliciozni linkovi ili dokumenta s ciljem krađe podataka koju omogućava jedan korisnikov klik na link sa nazivom od interesa. Dosadašnji podaci ukazuju da je u svetu zabeleženo 300.000 jedinstvenih sajber pretnji koje zloupotrebljavaju pandemiju i manipulišu potrebom ljudi da budu informisani.

Drugi vid zloupotrebe je masovno registrovanje lažnih internet stranica sa temom aktuelnog virusa. One se dalje koriste i za lažnu prodaju medicinske opreme, suplemenata, lekova i vakcina, a kao rezultat hakeri stiču protivpravnu imovinsku korist.

## FIŠING PUTEM PORUKA ELEKTRONSKE POŠTE

Tokom pandemije je značajno povećan broj fišing kampanja koje koriste virus COVID-19 u zlonamerne svrhe.

Najčešće su ove poruke elektronske pošte na engleskom jeziku (postaju masovnije i poruke na italijanskom i portugalskom), dok sadržaj poruka varira u zavisnosti od grupe koja je meta napada (organi javne vlasti, zdravstvene ustanove, stanovnici određene države ili gradove). Naslovi poruka kao „mamac“ sadrže reč COVID-19, coronavirus (npr. 2020 Coronavirus Updates ili samo Coronavirus Updates, 2019-nCov: New confirmed cases in your city ili 2019-nCov: Coronavirus outbreak in your city (Emergency), dok je tekst poruke kreiran kao savet upućen od strane eminentnih organizacija ili kompanija (npr. Svetska zdravstvena organizacija, UNICEF, CISCO).

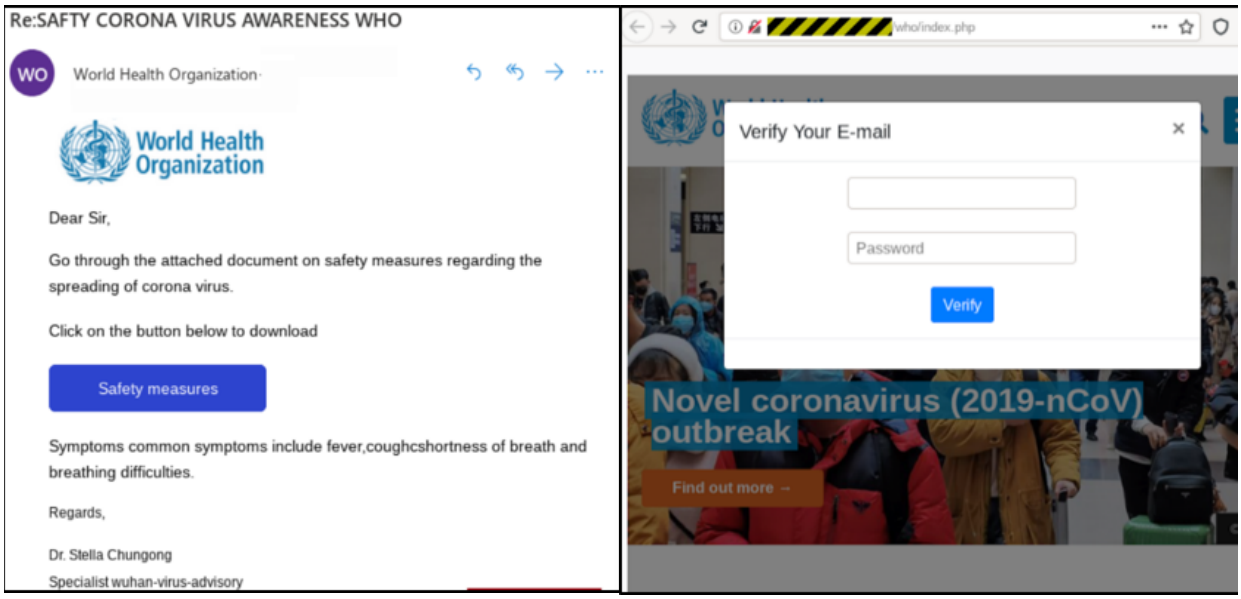
Određeni broj fišing napada ima za cilj krađu kredencijala [2], dok drugi imaju za cilj distribuciju zlonamernog softvera.

[2] Kredencijal je struktura podataka koji povezuje identitet korisnika i njegove atribute i koji se šalje verifikatoru radi provere identiteta i prava pristupa.

# KRAĐA KREDENCIJALA

Fišing napad kojim napadač namerava da dođe do kredencijala korisnika, zahteva hitnu reakciju korisnika i klik na link koji se nalazi u tekstu poruke.

Link vodi na lažnu internet stranicu koja u nazivu sadrži COVID-19, a za pristup informacijama sa stranice zahteva se unos adrese elektronske pošte i lozinke. Ove internet stranice izgledaju kao legitimne i deluju kao pouzdane, ali se zlonamerni pokušaj može utvrditi detaljnim pregledom URL-a. Unos kredencijala od strane korisnika napadaču omogućava pristup njegovoj elektronskoj pošti korisnika koja najčešće sadrži lične i poverljive podatke (npr. Izvodi sa bankovnog računa), a može iskoristiti i imenik korisnika za dalje širenje fišing napada (Slika 2).



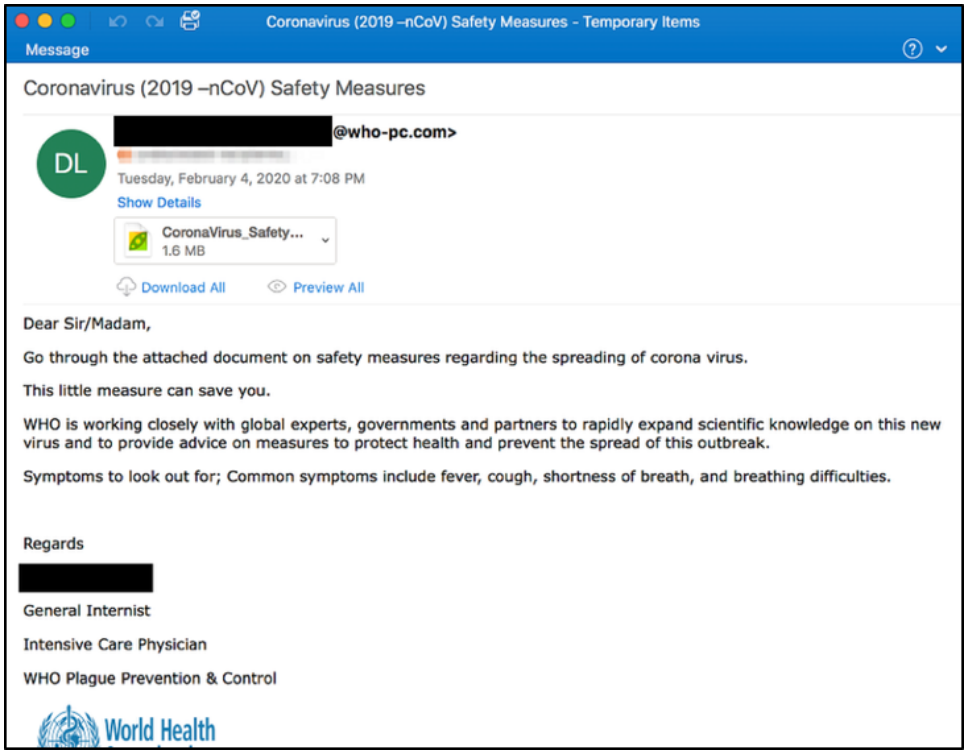

Slika 2 - Fišing koji se koristi za pribavljanje kredencijala [3]

# DISTRIBUCIJA ZLONAMERNOG SOFTVERA

Fišing napad kojim se distribuira zlonamerni softver, odnosno malver, najčešće sadrži tekst poruke kojim se zahteva otvaranje priloga.

Na osnovu statističkih podataka [4] čak 45% fišing poruka sadržalo je u prilogu AgentTesla Keylogger. Ovaj malver je distribuiran lažnim predstavljanjem u ime Svetske zdravstvene organizacije (Slika 3).

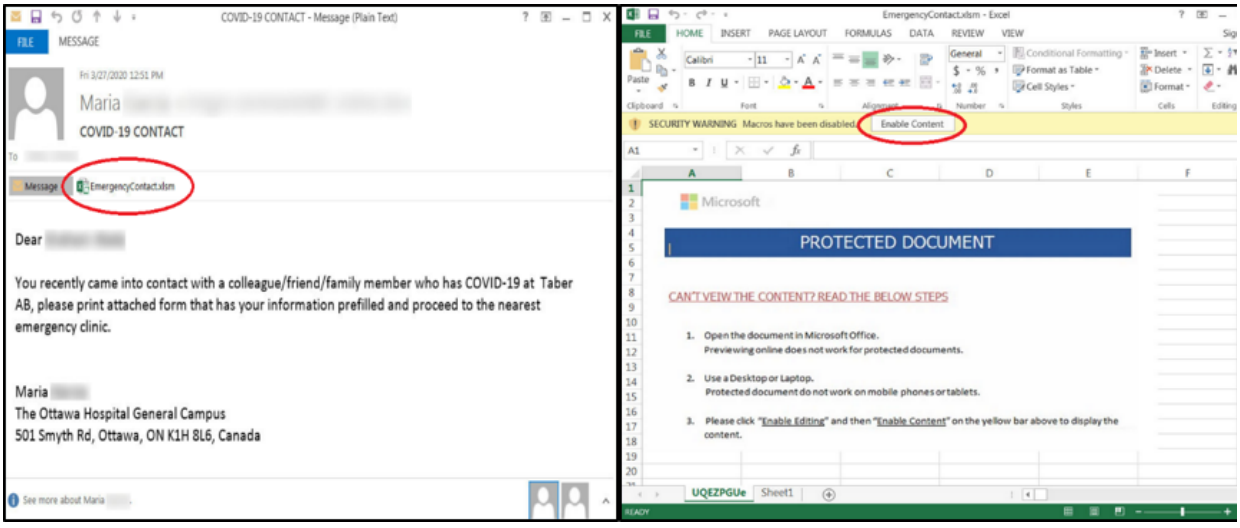
[3] https://nakedsecurity.sophos.com/2020/02/05/coronavirus-safety-measures-email-is-a-phishing-scam/
[4] https://www.group-ib.com/media/wp-content/uploads/2020/04/pic1@2x.jpg




Slika 3 - Lažno predstavljanje Svetske zdravstvene organizacije

Od primaoca poruke elektronske pošte se traži da otvori prilog za koji se tvrdi da sadrži mere zaštite od širenja korona virusa. Otvaranjem priloga instalira se malver koji napadaču omogućava da dobije sve što prevareni korisnik otkuca na tastaturi, od lozinki do sadržaja poruka elektronske pošte i tako ima mogućnost da prati sve njegove aktivnosti na mreži [5].

Jedan od najekstremnijih primera je poruka elektronske pošte kojom navodno lokalna bolnica obaveštava primaoca da je bio/bila u kontaktu sa prijateljem, rođakom ili kolegom koji je pozitivan na virus korone i traži da odštampa dokument iz priloga i odnese u najbližu bolnicu.




Slika 4 - Fišing poruka kojom se distribuira malver

[5] https://www.bbc.com/news/technology-51838468

Kada primalac otvori dokument iz priloga videće obaveštenje da je za pregled dokumenta neophodno da klikne na 'Enable Content' (Slika 4). Klikom na ovo dugme preuzima se i automatski pokreće malver, koji ubrizgava određene procese u operativni sistem primaoca, kako bi se sakrio od antivirusa i drugih bezbednosnih softvera.

# FIŠING PUTEM SMS PORUKA

Fišing napad putem SMS poruka poznat je i pod nazivom Smishing i do sada je bio korišćen u cilju pribavljanja finansijske koristi, kao navodni pošiljaoci koriste se uglavnom banke i poreske uprave.

Fišing putem SMS poruka koji kao mamac koristi COVID nema samo za cilj navođenje korisnika da izvrši određenu uplatu već se koristi i za pribavljanje kredencijala.

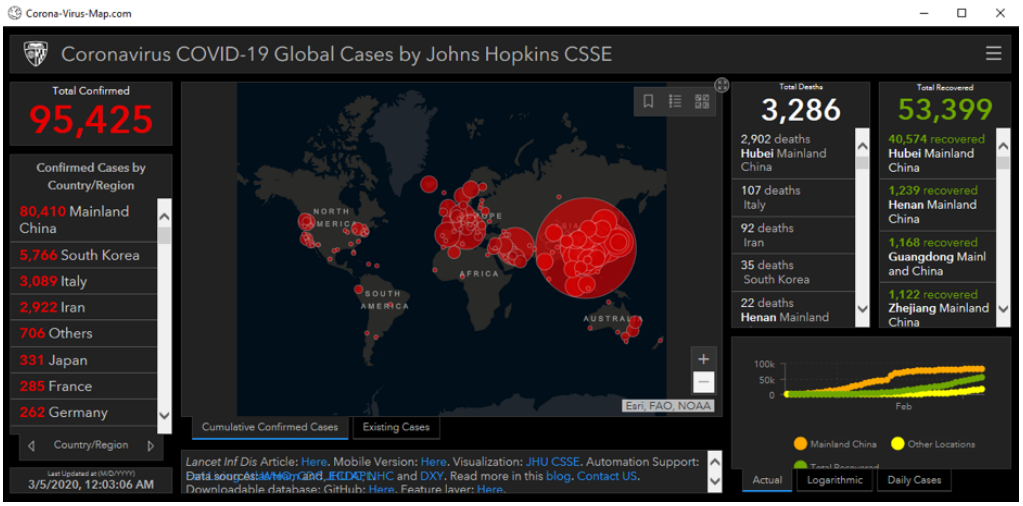
U našoj zemlji su zabeleženi fišing napadi SMS porukom koja sadrži link na kome se navodno nalazi obaveštenje Svetske zdravstvene organizacije o riziku od pandemije. Korišćena je kombinacija više jezika i pisama, što bi trebalo da izazove sumnju korisnika jer je to jedan od znakova da je reč o lažnom obaveštenju (Slika 5).


Slika 5 – Lažno obaveštenje SMS

# DISTRIBUCIJA MALVERA PUTEM WEB APLIKACIJA I RANSOMWARE KAMPANJE

## ZARAŽENE MAPE KORONA VIRUSA

Jedan od prvih primera manipulacije potrebe za informacijama o rasprostranjenosti virusa COVID-19 je kreiranje maliciozne aplikacije koja na kloniranoj mapi sveta učitanoj iz legitimnog izvora označava područja zahvaćena epidemijom (Slika 6).




Slika 6 - Aplikacija Corona-virus-Map

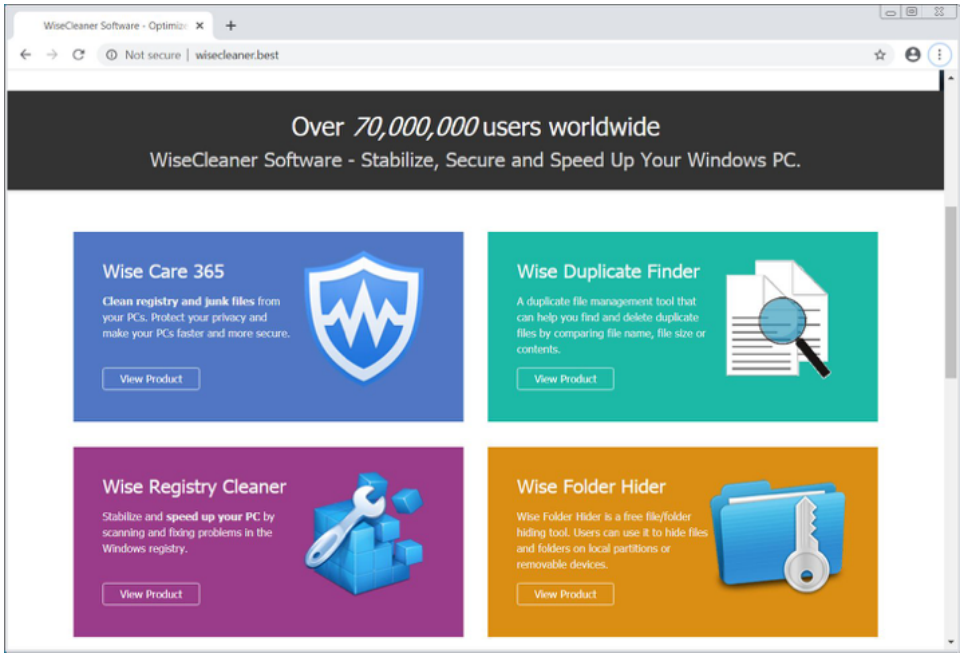
Prevareni korisnici instaliranjem mape zapravo preuzimaju na svoje računare zaraženu izvršnu datoteku Corona-virus-Map.com.exe koja sadrži trojanca AZORult. Ovaj malver krade kredencijale kao što su korisnička imena, lozinke, brojevi kreditnih kartica i druge osetljive podatke koji se čuvaju u internet pretraživaču. Ukradene informacije napadači mogu koristiti za pristup bankovnim računima, društvenim mrežama, a mogu ih čak i prodati na Dark web-u [6].


# DISTRIBUCIJA MALVERA PUTEM WEB APLIKACIJA I RANSOMWARE KAMPANJE

## ZARAŽENE MAPE KORONA VIRUSA


Za potrebe distribuiranja malvera, kreirana je internet stranica koja lažno predstavlja legitimnu stranicu WiseCleaner (Slika 7), popularne aplikacije za optimizaciju operativnog sistema. Na ovaj način su korisnicima isporučena dva malvera: CoronaVirus ransomver i trojanac Kpot.

[6] https://blog.reasonsecurity.com/2020/03/09/covid-19-info-stealer-the-map-of-threats-threat-analysis-report/




Slika 7 - WiseCleaner

Nakon što trojanac ukrade kolačiće i kredencijale za logovanje koji se čuvaju u servisima kao što su internet pretraživači, aplikacije za razmenu poruka, VPN, FTP, elektronska pošta, gejmerski nalozi i drugi, instaliraće se CoronaVirus ransomver koji zaključava podatke na računaru.

Otkupnina za otključavanje datoteka iznosi 0.008 bitkoina (oko 50 američkih dolara), ali dok korisnik razmišlja da li da plati ovaj iznos ili ne, napadač zloupotrebljava informacije pribavljene uz pomoć trojanca. Iz tog razloga se preporučuje što hitnija promena svih lozinki korišćenjem drugog nezaraženog računara [7].

Ostali malveri koji se najčešće koriste za vreme ove kampanje su trojanac Netwire Remote Access [8], modularni trojanac TrickBot [9] i mnogi drugi.

[7]https://www.bleepingcomputer.com/news/security/new-coronavirus-ransomware-acts-as-cover-for-kpot-infostealer/
[8]https://blog.malwarebytes.com/scams/2020/03/coronavirus-scams-found-and-explained/
[9] https://blog.malwarebytes.com/detections/trojan-trickbot/

# ZLOUPOTREBA KOMUNIKACIONIH PLATFORMI

U okolnostima pandemije, i preporučenim radom od kuće, povećan je broj zloupotreba online komunikacionih platformi, kao što su fišing internet stranice, koje oponašaju legitimne platforme za online učenje (na primer Google učionica), pokušaji krađe kredencijala i sl.

Platforma koja je stekla najveću popularnost je Zoom komunikaciona platforma, koju koriste mnoge obrazovne ustanove, kompanije i organi uprave i trenutno ima oko 13 miliona aktivnih korisnika mesečno. Upravo za ovu platformu je karakteristična masovna registracija novih lažnih Zoom domena kao i malicioznih Zoom izvršnih datoteka[1]. Kroz distribuciju lažnih linkova/datoteka putem četa (eng. chat) i otvaranjem istih od strane korisnika platforme, napadačima je omogućeno sprovođenje različitih malicioznih aktivnosti. Do sad su detektovane maliciozne datoteke sa nazivom "zoom-us- zoom_##########.exe" čijim pokretanjem se instaliraju neželjeni programi. Preporuka je da korisnici preuzimaju aplikaciju za pristup Zoom platformi sa zvanične internet stranice[11] kao i redovno ažuriranje platforme[12]. Predstavnici Zoom-a preporučuju automatsko generisanje meeting ID i izbegavanje opcije „personal meeting" za sastanke sa većim brojem korisnika[13].

# HIJACKING

Novi tip sajber napada koji se pojavljuje je "kidnapovanje" (eng. hijacking) DNS podešavanja rutera.

Pretraživač prikazuje poruku lažne COVID-19 aplikacije od Svetske zdravstvene organizacije, i predstavlja malver čija je svrha krađa podataka. U pretraživaču se otvara poruka koja upućuje na instalaciju COVID-19 informativne aplikacije koja navodno pripada Svetskoj zdravstvenoj organizaciji.

Ukoliko korisnik preuzme i instalira ovu lažnu aplikaciju, umesto aplikacije o COVID- 19, na korisničkom računaru će biti instaliran malver trojanac, koji prikuplja informacije od korisnika, kao što su: kolačići i istorija pretraživanja; informacije o plaćanjima; sačuvani kredencijali za logovanje; tekstualni dokumenti; forme koje se automatski popunjavaju u pretraživaču; slike ekrana korisnika i sl. Prikupljene informacije napadač može iskoristiti za dalje napade na onlajn naloge korisnika, kao što su krađa novca sa bankovnih računa, krađa identiteta ili za slanje daljih spear phishing poruka ka korisniku kako bi prikupio dodatne informacije.

Kao mere prevencije su prepoznate kreiranje jakih lozinki kao i onemogućavanje udaljenog pristupa ruterima. Ukoliko je instalirana lažna aplikacija, potrebno je promeniti DNS podešavanja rutera, skenirati uređaje, očistiti ih od malvera i promeniti sve lozinke koje su korisnici unosili dok su bili zaraženi. Prilikom promene lozinki, voditi računa da svaka lozinka bude drugačija za svaki nalog[14].

[10]https://blog.checkpoint.com/2020/03/30/covid-19-impact-cyber-criminals-target-zoom-domains/
[11] https://zoom.us/
[12] https://thehackernews.com/2020/03/zoom-video-coronavirus.html
[13] https://www.sans.org/webcasts/downloads/114670/slides
[14]https://www.bleepingcomputer.com/news/security/hackers-hijack-routers-dns-to-spread-malicious-covid-19-apps/

# PREPORUKE

Koristeći se stanjem opšteg straha, napadači se trude da tekstom poruke navedu primaoca poruke da klikne na link ili dokument iz priloga kroz lažno predstavljanje, manipulaciju emocijama, potrebe za hitnom reakcijom i na taj način dođu do podataka koji im mogu doneti novčanu ili drugu korist.

**Ako ste kliknuli na link ili dokument preduzmite sledeće korake:**

- Ako koristite službeni telefon ili laptop odmah kontaktirajte IT službu poslodavca
- Ako ste dali svoje podatke o bankovnom računu odmah obavestite banku
- Aktivirajte antivirus i kliknite na „full scan”
- Ako ste ostavili svoju lozinku, odmah promenite lozinke na svim Vašim nalozima
- Ako ste izgubili novac odmah kontaktirajte svoju banku i prijavite policiji na vtk@mup.gov.rs

- **Ne budite laka meta**

- Proverite podešavanja privatnosti na nalozima za društvene mreže i svim onlajn nalozima
- Razmišljajte o tome šta objavljujete o sebi i svojoj porodici
- Pratite šta Vaši prijatelji, porodica i kolege objavljuju o vama na društvenim mrežama, jer sve dostupne informacije mogu biti zloupotrebljene od strane napadača
- Ako primite sumnjivu poruku elektronske pošte označite je kao Spam/Junk ili je odmah izbrišite.

REPUBLIKA SRBIJA
RATEL
REGULATORNA AGENCIJA ZA ELEKTRONSKE KOMUNIKACIJE I POŠTANSKE USLUGE

#odbraniseznanjem

SRB-CERT

*Nacionalni CERT Republike Srbije ne promoviše ili favorizuje bilo koji od korišćenih javnih izvora, među kojima su i komercijalni proizvodi i usluge. Sve preporuke, analize i predlozi dati su u cilju prevencije i zaštite od bezbednosnih rizika.*