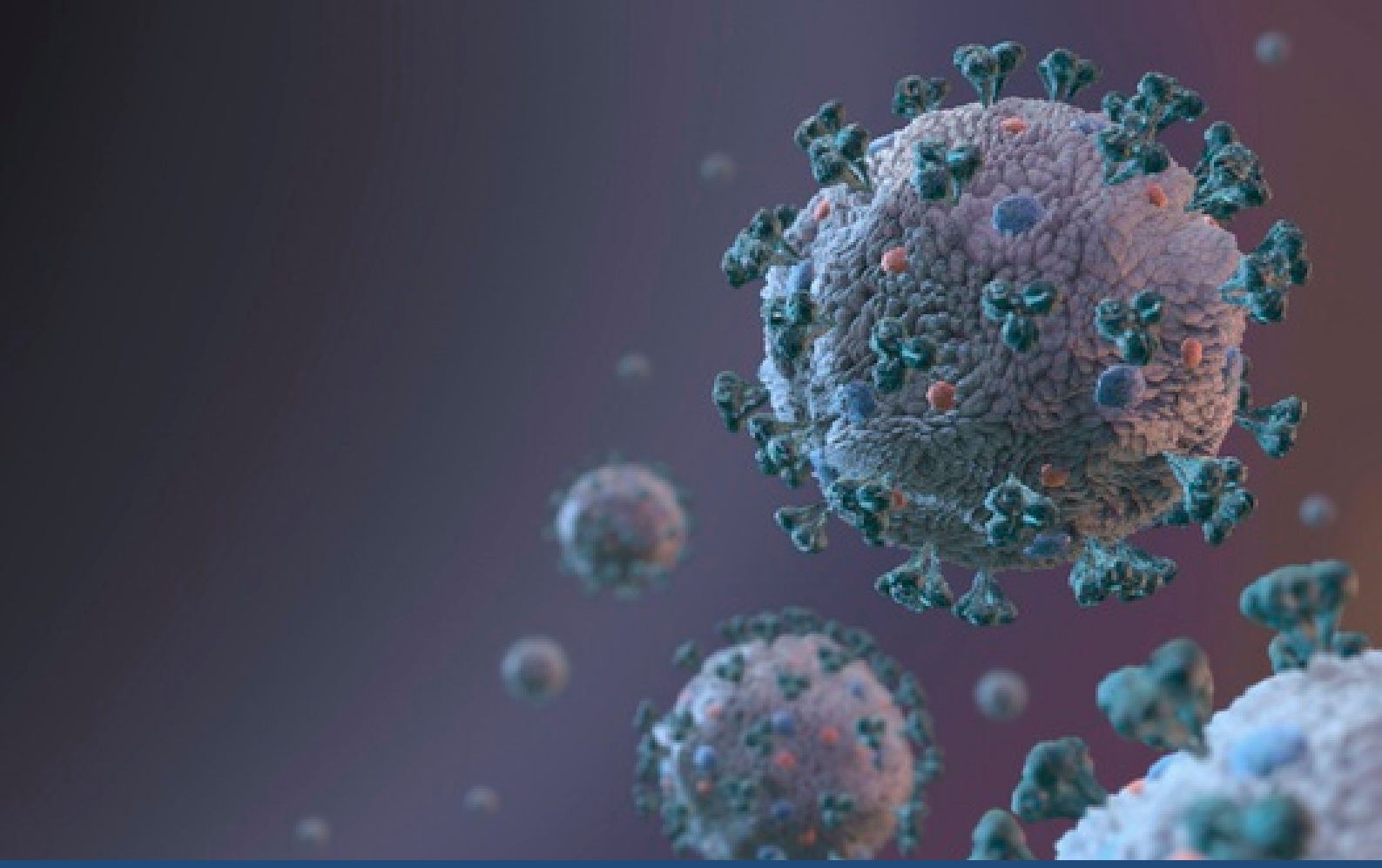


ЗЛОУПОТРЕБА ПАНДЕМИЈЕ ВИРУСА COVID-19 У САЈБЕР ПРОСТОРУ

ПРИЈАВИТЕ СВАКИ ИНЦИДЕНТ
НА НАШЕМ ПОРТАЛУ

СРБ-ЦЕРТ

ЗАШТИТА ПОДАТАКА

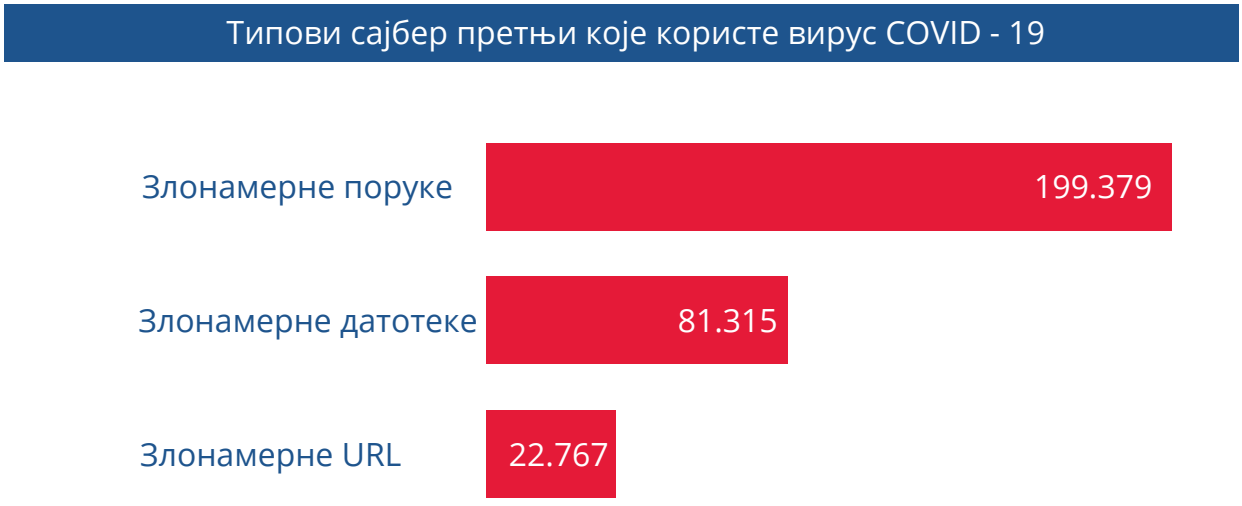
Од почетка пандемије трудимо се да поштујемо здравствене и хигијенске препоруке у циљу превенције од вируса, а шта је са превенцијом од сајбер претњи? Колико секунди траје провера порука електронске поште, СМС порука и других порука које добијамо путем апликација за комуникацију?

Сајбер криминалци користе стање пандемије и свакодневно траже начине за злоупотребу претраге корисника на интернету, који желе да се информишу о саветима и вестима у вези са пандемијом. Сајбер претњама смо сви подједнако изложени, без обзира да ли интернет користимо у пословне сврхе или за правовремено и тачно информисање.

Дигитализација је саставни део свакодневног живота у још већем обиму, па интернет користимо за обављање радних задатака, учење са децом и информисање о стању пандемије. Сајбер криминалци искоришћавају стање прилагођавања на ванредне околности живота и рада, као и борбе са страхом од вируса и неизвесности, и проналазе начине да дођу до наших података, које чувамо на преносним уређајима.

Један од начина напада су фишинг кампање које дистрибуирају малициозни линк или документ и за циљ имају крађу података, а од корисника се захтева брза реакција, најчешће само један клик.

Досадашњи подаци указују да је у свету до сада забележено 300.000 јединствених сајбер претњи које злоупотребљавају пандемију и манипулишу потребом људи да буду информисани.



Слика 1 - Претње детектоване у периоду 01.јануар-27.март 2020.године, Извор: Micro Trend [1]

Још један вид злоупотребе пандемије свакако представља и масовно регистровање лажних интернет страница. За време трајања пандемије, значајно је повећан број лажних интернет страница које користе тему вируса COVID-19, односно садрже неки од појмова пандемије у називу домена ("Covid19/Coronavirus“). Поред дистрибуције сајбер напада, ове странице се користе за лажну продају медицинске опреме, суплемената, лекова, вакцина и преваром корисника, хакери долазе до противправно стечене имовинске користи.

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

Други вид злоупотребе је масовно регистровање лажних интернет страница са темом актуелног вируса. Оне се даље користе и за лажну продају медицинске опреме, суплемената, лекова, вакцина, а као резултат хакери стичу противправну имовинску корист.

Од самог почетка пандемије, а у циљу превенције новонасталог вируса, трудимо се да поштујемо здравствене и хигијенске препоруке. Међутим, шта је са превенцијом када су у питању сајбер претње?

Ванредне околности настале са појавом корона вируса допринеле су повећаној употреби интернета: виртуелне учионице, конференцијски позиви, информисање о стању пандемије. Без обзира на то у које сврхе се интернет користи, сајбер претњама су сви подједнако изложени.

Прилагођавање на ванредне услове живота и рада, такозвани сајбер криминалци планирано користе. Док се на једној страни корисници интернета информишу, на пример, о саветима и вестима везаним за пандемију, на другој страни сајбер криминалци свакодневно траже нове начине за злоупотребу активности на интернету.

Један од начина злоупотребе је фишинг кампања. Наиме, њом се дистрибуирају малициозни линкови или документа с циљем крађе података коју омогућава један корисников клик на линк са називом од интереса. Досадашњи подаци указују да је у свету забележено 300.000 јединствених сајбер претњи које злоупотребљавају пандемију и манипулишу потребом људи да буду информисани.

Други вид злоупотребе је масовно регистровање лажних интернет страница са темом актуелног вируса. Оне се даље користе и за лажну продају медицинске опреме, суплемената, лекова и вакцина, а као резултат хакери стичу противправну имовинску корист.

ФИШИНГ ПУТЕМ ПОРУКА ЕЛЕКТРОНСКЕ ПОШТЕ

Током пандемије је значајно повећан број фишинг кампања које користе вирус COVID-19 у злонамерне сврхе.

Најчешће су ове поруке електронске поште на енглеском језику (постају масовније и поруке на италијанском и португалском), док садржај порука варира у зависности од групе која је мета напада (органи јавне власти, здравствене установе, становници одређене државе или градове). Наслови порука као „мамац“ садрже реч COVID-19, coronavirus (нпр. 2020 Coronavirus Updates или само Coronavirus Updates, 2019-nCov: New confirmed cases in your city или 2019-nCov: Coronavirus outbreak in your city (Emergency), док је текст поруке креиран као савет упућен од стране еминентних организација или компанија (нпр. Светска здравствена организација, UNICEF, CISCO).

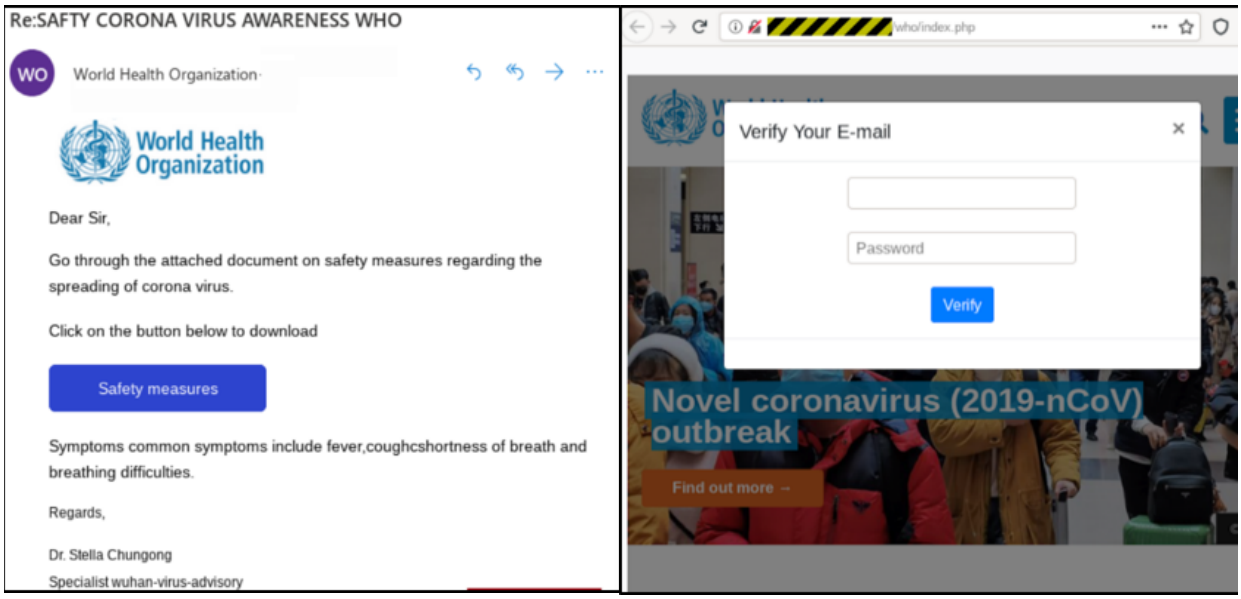
Одређени број фишинг напада има за циљ крађу креденцијала [2], док други имају за циљ дистрибуцију злонамерног софтвера.

[2] Креденцијал је структура података који повезује идентитет корисника и његове атрибуте и који се шаље верификатору ради провере идентитета и права приступа.

КРАЂА КРЕДЕНЦИЈАЛА

Фишинг напад којим нападач намерава да дође до креденцијала корисника, захтева хитну реакцију корисника и клик на линк који се налази у тексту поруке.

Линк води на лажну интернет страницу која у називу садржи COVID-19, а за приступ информацијама са странице захтева се унос адресе електронске поште и лозинке. Ове интернет странице изгледају као легитимне и делују као поуздане, али се злонамерни покушај може утврдити детаљним прегледом URL-а. Унос креденцијала од стране корисника нападачу омогућава приступ његовој електронској пошти корисникакоја најчешће садржи личне и поверљиве податке (нпр. Изводи са банковног рачуна), а може искористити и именик корисника за даље ширење фишинг напада (Слика 2).



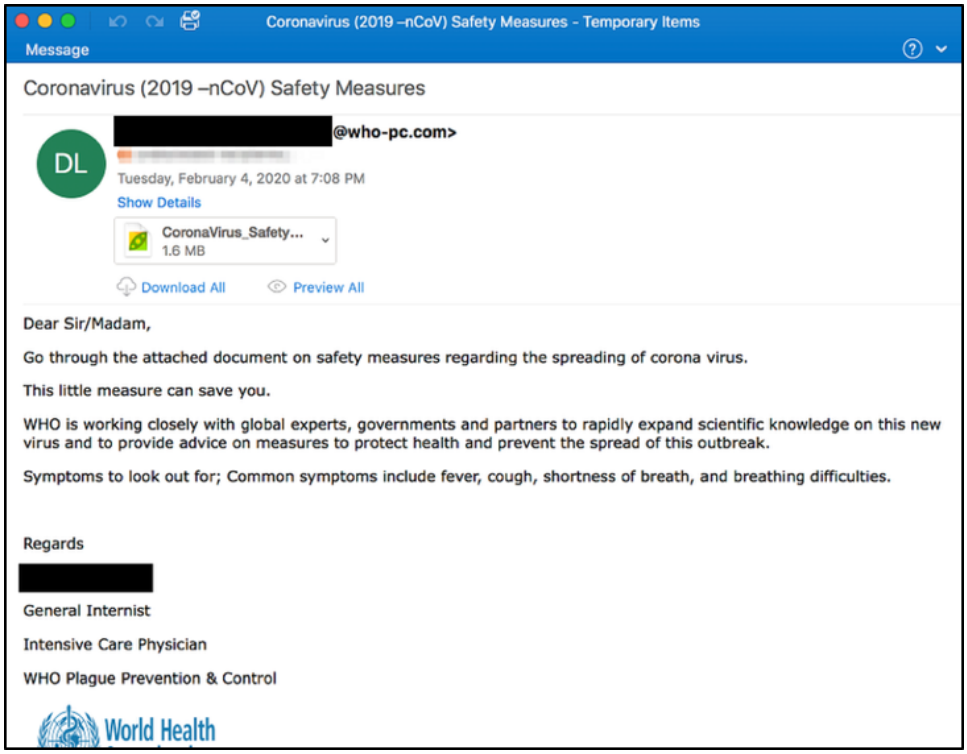
Слика 2 - Фишинг који се користи за прибављање креденцијала [3]

ДИСТРИБУЦИЈА ЗЛОНАМЕРНОГ СОФТВЕРА

Фишинг напад којим се дистрибуира злонамерни софтвер, односно малвер, најчешће садржи текст поруке којим се захтева отварање прилога.

На основу статистичких података [4] чак 45% фишинг порука садржало је у прилогу AgentTesla Keylogger. Овај малвер је дистрибуиран лажним представљањем у име Светске здравствене организације (Слика 3).

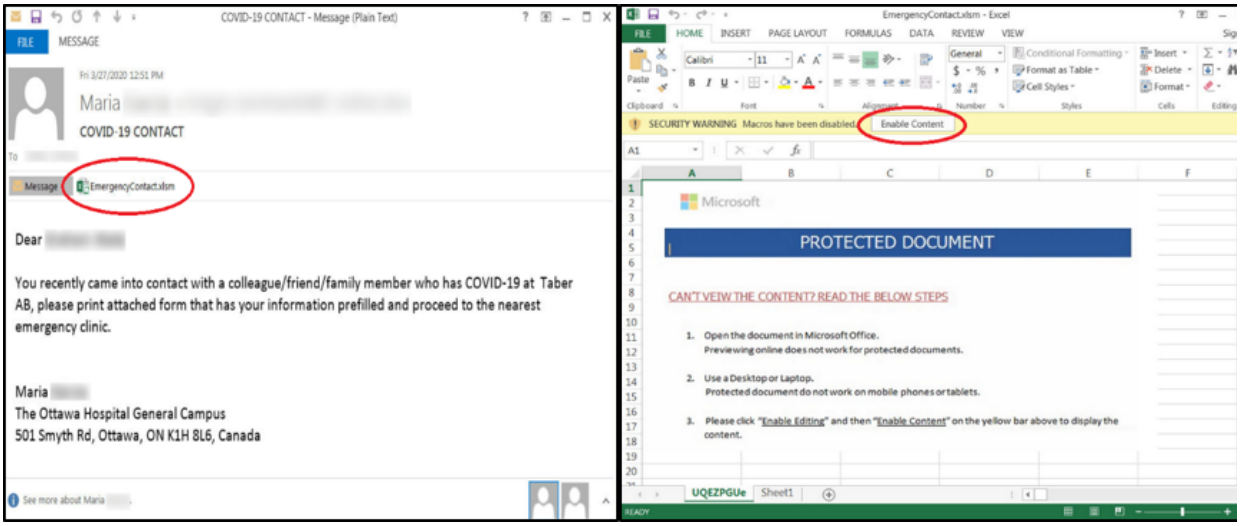
[3] https://nakedsecurity.sophos.com/2020/02/05/coronavirus-safety-measures-email-is-a-phishing-scam/
[4] https://www.group-ib.com/media/wp-content/uploads/2020/04/pic1@2x.jpg



Слика 3 - Лажно представљање Светске здравствене организације

Од примаоца поруке електронске поште се тражи да отвори прилог за који се тврди да садржи мере заштите од ширења корона вируса. Отварањем прилога инсталира се малвер који нападачу омогућава да добије све што преварени корисник откуца на тастатури, од лозинки до садржаја порука електронске поште и тако има могућност да прати све његове активности на мрежи [5].

Један од најекстремнијих примера је порука електронске поште којом наводно локална болница обавештава примаоца да је био/била у контакту са пријатељем, рођаком или колегом који је позитиван на вирус короне и тражи да одштампа документ из прилога и однесе у најближу болницу.



Слика 4 - Фишинг порука којом се дистрибуира малвер

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

Када прималац отвори документ из прилога видеће обавештење да је за преглед документа неопходно да кликне на 'Enable Content' (Слика 4). Кликом на ово дугме преузима се и аутоматски покреће малвер, који убризгава одређене процесе у оперативни систем примаоца, како би се сакрио од антивируса и других безбедносних софтвера.

ФИШИНГ ПУТЕМ СМС ПОРУКА

Фишинг напад путем СМС порука познат је и под називом Smishing и до сада је био коришћен у циљу прибављања финансијске користи, као наводни пошиљаоци користе се углавном банке и пореске управе.

Фишинг путем СМС порука који као мамац користи COVID нема само за циљ навођење корисника да изврши одређену уплату већ се користи и за прибављање креденцијала.

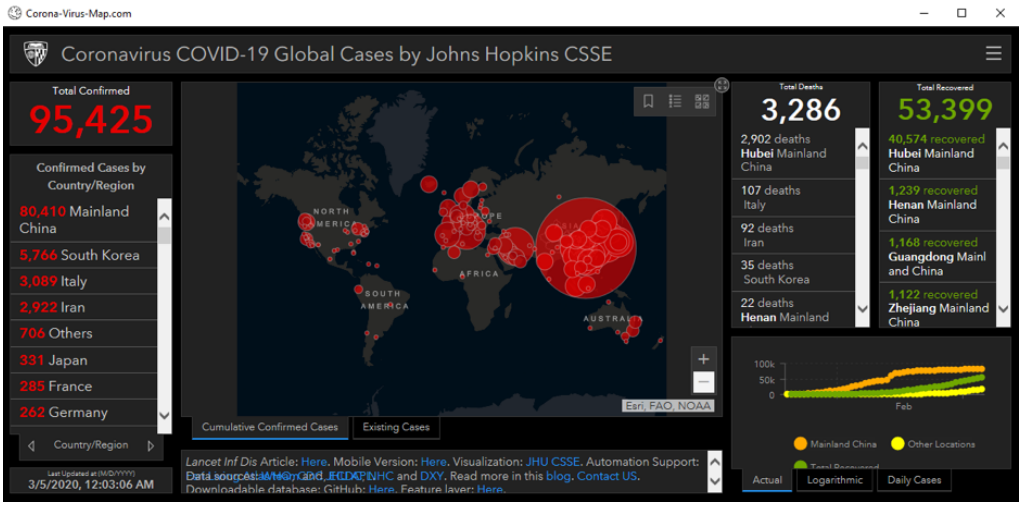
У нашој земљи су забележени фишинг напади СМС поруком која садржи линк на коме се наводно налази обавештење Светске здравствене организације о ризику од пандемије. Коришћена је комбинација више језика и писама, што би требало да изазове сумњу корисника јер је то један од знакова да је реч о лажном обавештењу (Слика 5).

Слика 5 – Лажно обавештење СМС

ДИСТРИБУЦИЈА МАЛВЕРА ПУТЕМ ВЕБ АПЛИКАЦИЈА И РАНСОМВЕР КАМПАЊЕ

ЗАРАЖЕНЕ МАПЕ КОРОНА ВИРУСА

Један од првих примера манипулације потребе за информацијама о распрострањености вируса COVID-19 је креирање малициозне апликације која на клонираној мапи света учитаној из легитимног извора означава подручја захваћена епидемијом (Слика 6).



Слика 6 - Апликација Corona-virus-Map

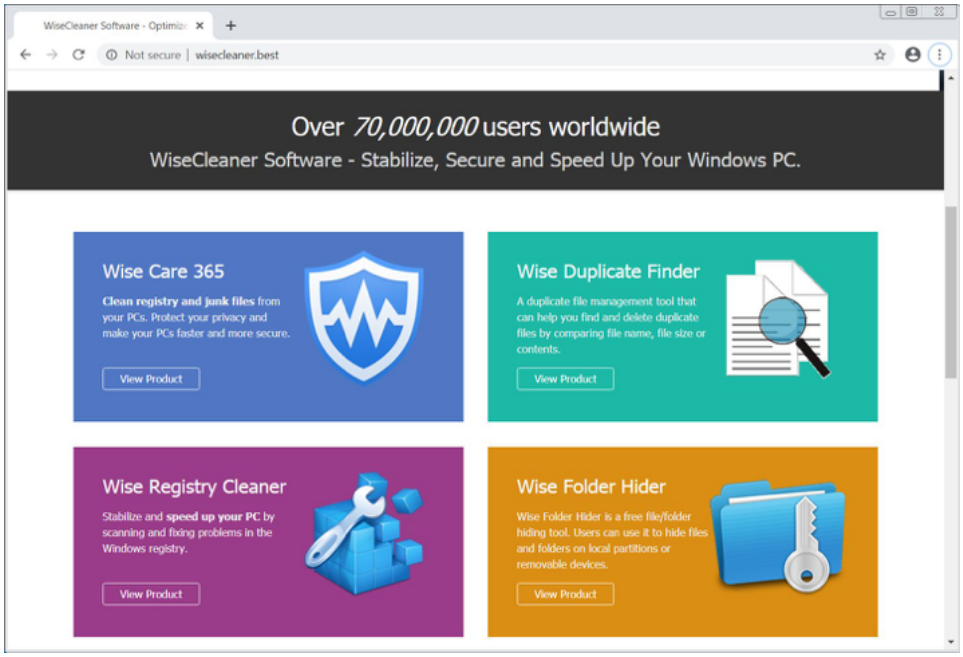
Преварени корисници инсталирањем мапе заправо преузимају на своје рачунаре заражену извршну датотеку Corona-virus-Map.com.exe која садржи тројанца AZORult. Овај малвер краде креденцијале као што су корисничка имена, лозинке, бројеви кредитних картица и друге осетљиве податке који се чувају у интернет претраживачу. Украдене информације нападачи могу користити за приступ банковним рачунима, друштвеним мрежама, а могу их чак и продати на Dark web-у [6].

ДИСТРИБУЦИЈА МАЛВЕРА ПУТЕМ ВЕБ АПЛИКАЦИЈА И РАНСОМВЕР КАМПАЊЕ

ЗАРАЖЕНЕ МАПЕ КОРОНА ВИРУСА

За потребе дистрибуирања малвера, креирана је интернет страница која лажно представља легитимну страницу WiseCleaner (Слика 7), популарне апликације за оптимизацију оперативног система. На овај начин су корисницима испоручена два малвера: CoronaVirus рансомвер и тројанац Kpot.

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



Слика 7 - WiseCleaner

Након што тројанац украде колачиће и креденцијале за логовање који се чувају у сервисима као што су интернет претраживачи, апликације за размену порука, VPN, FTP, електронска пошта, гејмерски налози и други, инсталираће се CoronaVirus рансомвер који закључава податке на рачунару.

Откупнина за откључавање датотека износи 0.008 биткоина (око 50 америчких долара), али док корисник размишља да ли да плати овај износ или не, нападач злоупотребљава информације прибављене уз помоћ тројанца. Из тог разлога се препоручује што хитнија промена свих лозинки коришћењем другог незараженог рачунара [7].

Остали малвери који се најчешће користе за време ове кампање су тројанац Netwire Remote Access [8], модуларни тројанац TrickBot [9] и многи други.

[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/

ЗЛОУПОТРЕБА КОМУНИКАЦИОНИХ ПЛАТФОРМИ

У околностима пандемије, и препорученим радом од куће, повећан је број злоупотреба онлајн комуникационих платформи, као што су фишинг интернет странице, које опонашају легитимне платформе за онлајн учење (на пример Google учионица), покушаји крађе креденцијала и сл.

Платформа која је стекла највећу популарност је Zoom комуникациона платформа, коју користе многе образовне установе, компаније и органи управе и тренутно има око 13 милиона активних корисника месечно. Управо за ову платформу је карактеристична масовна регистрација нових лажних Zoom домена као и малициозних Zoom извршних датотека[1]. Кроз дистрибуцију лажних линкова/датотека путем чета (енг. chat) и отварањем истих од стране корисника платформе, нападачима је омогућено спровођење различитих малициозних активности. До сад су детектоване малициозне датотеке са називом "zoom-us-zoom_##########.exe" чијим покретањем се инсталирају нежељени програми. Препорука је да корисници преузимају апликацију за приступ Zoom платформи са званичне интернет странице[11] као и редовно ажурирање платформе[12]. Представници Zoom-а препоручују аутоматско генерисање meeting ID и избегавање опције „personal meeting" за састанке са већим бројем корисника[13].

HIJACKING

Нови тип сајбер напада који се појављује је "киднаповање" (eng. hijacking) DNS подешавања рутера.

Претраживач приказује поруку лажне COVID-19 апликације од Светске здравствене организације, и представља малвер чија је сврха крађа података. У претраживачу се отвара порука која упућује на инсталацију COVID-19 информативне апликације која наводно припада Светској здравственој организацији.

Уколико корисник преузме и инсталира ову лажну апликацију, уместо апликације о COVID-19, на корисничком рачунару ће бити инсталиран малвер тројанац, који прикупља информације од корисника, као што су: колачићи и историја претраживања; информације о плаћањима; сачувани креденцијали за логовање; текстуални документи; форме које се аутоматски попуњавају у претраживачу; слике екрана корисника и сл. Прикупљене информације нападач може искористити за даље нападе на онлајн налоге корисника, као што су крађа новца са банковних рачуна, крађа идентитета или за слање даљих spear phishing порука ка кориснику како би прикупио додатне информације.

Као мере превенције су препознате креирање јаких лозинки као и онемогућавање удаљеног приступа рутерима. Уколико је инсталирана лажна апликација, потребно је променити DNS подешавања рутера, скенирати уређаје, очистити их од малвера и променити све лозинке које су корисници уносили док су били заражени. Приликом промене лозинки, водити рачуна да свака лозинка буде другачија за сваки налог[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/

ПРЕПОРУКЕ

Користећи се стањем општег страха, нападачи се труде да текстом поруке наведу примаоца поруке да кликне на линк или документ из прилога кроз лажно представљање, манипулацију емоцијама, потребе за хитном реакцијом и на тај начин дођу до података који им могу донети новчану или другу корист.

Ако сте кликнули на линк или документ предузмите следеће кораке:

- Ако користите службени телефон или лаптоп одмах контактирајте IT службу послодавца
- Ако сте дали своје податке о банковном рачуну одмах обавестите банку
- Активирајте антивирус и кликните на „full scan”
- Ако сте оставили своју лозинку, одмах промените лозинке на свим Вашим налозима
- Ако сте изгубили новац одмах контактирајте своју банку и пријавите полицији на vtk@mup.gov.rs

- **Не будите лака мета**

- Проверите подешавања приватности на налозима за друштвене мреже и свим онлајн налозима
- Размишљајте о томе шта објављујете о себи и својој породици
- Пратите шта Ваши пријатељи, породица и колеге објављују о вама на друштвеним мрежама, јер све доступне информације могу бити злоупотребљене од стране нападача
- Ако примите сумњиву поруку електронске поште означите је као Spam/Junk или је одмах избришите.

РЕПУБЛИКА СРБИЈА
РАТЕЛ
РЕГУЛАТОРНА АГЕНЦИЈА ЗА ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ И ПОШТАНСКЕ УСЛУГЕ

#odbraniseznanjem

СРБ-ЦЕРТ

Национални ЦЕРТ Републике Србије не промовише или фаворизује било који од коришћених јавних извора, међу којима су и комерцијални производи и услуге. Све препоруке, анализе и предлози дати су у циљу превенције и заштите од безбедносних ризика.