М-р Јован Петрезанов[1]

ВЛИЈАНИЕТО НА ПАНДЕМИЈАТА ПРЕДИЗВИКАНА ОД ВИРУСОТ КОВИД-19 ВРЗ КОМПЈУТЕРСКИОТ КРИМИНАЛ

1.02 Прегледна научна статија
УДК 343.9:004.7(497.7)
616.98:578.834-036.21(100)

Апстракт

Компјутерскиот криминал е еден од најголемите, најактивните и најкомплексните форми на криминал на глобално ниво. Со оглед на тоа што станува збор за вид на криминал што е неразделно поврзан со технологијата, компјутерскиот криминал се развива и бележи сериозно комплексни форми со развојот на технологијата, но и со други влијанија, како што е сегашната пандемија предизвикана од вирусот КОВИД-19. Иако навидум под контрола, и по повеќе од три години, пандемијата предизвикана од вирусот КОВИД-19 сè уште е актуелна, а вирусот продолжува да мутира во нови соеви, да се шири и да зема жртви глобално.

КОВИД-19 го потресе модерното човештво од корен: ограничена беше слободата на движењето, слободата на пазарот и претприемништвото, правната сигурност на граѓаните, здравствените системи беа пред колапс, ограничени беа некои од основните права на работниците (здравствените работници не земаа одмор), а во првите месеци од пандемијата не функционираа ниту образовниот, ниту правосудниот систем. При вакви околности, додека сиот тој сообраќај се намалуваше, интернет-сообраќајот од ден на ден стана сè погуст, а тоа донесе толкав број незгоди и жртви колкав што човештвото одамна не памети. Се чини дека здравствената пандемија со себе донесе уште едно зло – сајбер пандемија.

Несомнено е дека оваа проблематика не е доволно проучена, а истовремено зема сè поголем замав. Благодарејќи на научните истражувања и општествениот дијалог, може полесно да се подигне свеста кај луѓето за препознавање, реагирање, спречување и закрепнување од компјутерски злосторства.

Клучни зборови: компјутерски криминал, пандемија, малициозен софтвер, компјутерски напад, последици.

Несакани ефекти од начините на справување со пандемијата предизвикана од вирусот КОВИД-19

Благодарејќи на дигиталната трансформација што светот ја доживува во последната деценија, а особено со започнувањето на пандемијата предизвикана од вирусот КОВИД-19, криминалците успешно прават секакви напори за да ги пронајдат и да ги злоупотребат слабостите во онлајн системите, мрежите и инфраструктурата. Ова има огромно економско

[1] Авторот е адвокат, магистер по кривично право и правен консултант за менаџмент на меѓународни, комерцијални и компјутерски договори.

и социјално влијание врз владите, бизнисите и поединците ширум светот на тој начин што се користат нови технологии за приспособување и унапредување на компјутерските напади и мрежна соработка помеѓу сторителите, најчесто преку фишингот и разните видови малициозни софтвери.

Бидејќи глобалното изолирање во 2020 година стана универзална стратегија за контрола на пандемијата, социјалното дистанцирање предизвика огромно потпирање на алтернативите на интернет-просторот. И покрај ефикасноста за работа на далечина и онлајн интеракции, алтернативите на ваквиот простор отвориј нови предизвици за компјутерската безбедност. Хакерите ги искористија глобалниот страв и вознемиреноста на популацијата, така што ги зачестија и ги усовршија нападите врз компјутерските системи, а тоа предизвика влијание врз интегритетот на податоците, приватноста и дигиталното однесување.

Со цел да се прикаже присуството на компјутерскиот криминал во нашето општество во последните години, а по поднесено барање до Министерството за внатрешни работи на Република Северна Македонија, подолу се прикажани податоци за регистрирани кривични дела и сторители за периодот од 2019 година, па сè до јуни 2023 година, одделно по периоди.

ТАБЕЛАРЕН ПРИКАЗ НА ОДРЕДЕНИ РЕГИСТРИРАНИ КРИВИЧНИ ДЕЛА И СТОРИТЕЛИ ВО ВРСКА СО КОМПЈУТЕРСКИ КРИМИНАЛ ЗА ПЕРИОД ОД 2019 ДО ЈУНИ 2023 ГОДИНА

Законска квалификација од КЗ на РСМ	2019 година		2020 година		2021 година		2022 година		јануари - јуни 2023 година	
	кривични дела	сторители	кривични дела	сторители	кривични дела	сторители	кривични дела	сторители	кривични дела	сторители
Злоупотреба на лични податоци чл.149 ст.2	19	10	1	1	9	4	14	17	16	6
Повреда на авторско право и сродни права чл.157 ст.2	-	-	-	-	-	-	-	-	-	-
Производство и дистрибуција на детска порнографија чл.193 - а	6	5	2	-	4	5	5	2	6	4
Намамување на обљуба или друго полово дејствие на дете кое не наполнило 14 години чл.193 - б	-	-	2	2	2	1	3	1	1	1
Оштетување и неовластено навлегување во компјутерски систем чл.251	65	37	85	33	71	30	138	82	56	32
Правење и внесување на компјутерски вируси чл. 251 - а	-	-	-	-	-	-	1	-	-	-
Компјутерска измама чл.251 - б	12	9	3	-	6	5	6	3	12	7
Ширење на расистички и ксенофобичен материјал по пат на компјутерски систем чл.394 - г	27	26	16	16	30	30	51	51	21	19
Тероризам чл.394-б ст.2 и ст.3	-	-	-	-	-	-	4	4	1	1
Компјутерски фалсификат чл.379 - а	3	3	1	1	-	-	-	-	-	-

**Извор: Официјална електронска евиденција на МВР и АИКР.*

Видно од овие статистички податоци, најголем број од регистрираните кривични дела се однесуваат на *оштетување и неовластено навлегување во компјутерски систем*, при што во 2019 година биле регистрирани 65 кривични дела и 37 сторители – бројки што оттогаш постепено растат низ текот на годините, за во 2022 година да достигнат двојно повеќе, односно алармантни 138 кривични дела и 82 сторители. Бројките за првата половина на 2023 година исто така не се оптимистични, бидејќи за само шест месеци биле регистрирани 56 кривични дела и дури 32 сторители.

Ширењето расистички и ксенофобичен материјал по пат на компјутерски систем исто така е сè повеќе присутно. Во 2019 година биле регистрирани 27 кривични дела и 26 сторители, со благо намалување во 2020 година, кога имало 16 кривични дела и исто толку сторители. Меѓутоа, овие бројки значително растат во 2021 година, а таа тенденција продолжува во 2022 година и достигнува 51 регистрирано кривично дело и исто толку

сторители. Се чини дека во 2023 година, барем досега, не се бележи пораст во споредба со 2022 година бидејќи во првите шест месеци од годината се регистрирани 21 кривично дело и 19 сторители.

Злоупотребата на лични податоци преку навлегување во компјутерски информатички систем е едно од најчестите кривични дела во светски размери. Во 2019 година биле регистрирани 19 вакви кривични дела и 10 сторители. Иако овие бројки во 2020 година драстично опаднале на само едно регистрирано кривично дело и еден сторител, сепак во следните години е забележан постојан раст. Имено, во 2021 година биле регистрирани 9 кривични дела и 4 сторители, во 2022 година 14 кривични дела и дури 17 сторители, за во оваа 2023 година, во првата половина да бидат регистрирани дури 16 кривични дела и 6 сторители. Интересен е фактот што во 2022 година бројот на сторители е поголем од бројот на сторени дела, што значи дека некои од овие дела се извршени од страна на повеќе сторители, организирано.

Иако од 2019 година па наваму не се регистрирани кривични дела за *компјутерски фалсификат* и *повреда на авторско право и сродни права*, а било регистрирано само едно дело во 2022 година за *правење и внесување компјутерски вируси*, можеби е умно оптимизмот да се стави страна бидејќи тоа не значи дека вакви дела не се сторени – засега знаеме само дека не се регистрирани. Тука се поставува прашањето дали жртвите на компјутерскиот криминал се свесни дека се жртви на компјутерски криминал?

Од вестите што ја бранувааа македонската јавност во 2022 година можеше да се забележи дека компјутерскиот криминал станува сè поприсутен, а не беа поштедени ниту органите на извршната власт. Имено, во септември 2022 година бил извршен напад врз електронскиот систем на Министерството за земјоделство, шумарство и водостопанство, при што напаѓачите успеале да дешифрираат податоци од документи и за нив барале откуп.[2] Иако главните системи и бази не биле нападнати и оштетени, од превентивни причини тие морало да бидат исклучени со лимитиран пристап до нив, а редовниот работен процес во министерството бил блокиран. Речиси истовремено под удар биле и веб-страниците на Владата и на Министерството за образование и наука, каде што хакерите ги пробиле безбедносните филтри и прикачиле линкови за препродавање облека, патики и чанти.

Од ова може да се заклучи дека недоволното инвестирање во сајбер безбедноста и заштитата на компјутерските системи, македонските веб-страници ги прави лесна мета за напаѓачите. По ваквите случувања, Македонската агенција за електронски комуникации и Националниот центар за одговор на компјутерски инциденти МКД-ЦИРТ им препорачале на организациите од јавниот, владиниот и приватниот сектор да извршат безбедносна процена на своите системи и услуги и да имплементираат и да применуваат превентивни мерки и процедури за заштита од сајбер напади и инциденти.

Чести форми на компјутерски криминал за време на пандемијата предизвикана од вирусот КОВИД-19

[2] https://www.slobodnaevropa.mk/a/зачестените-сајбер-напади-на-државни-сајтови-го-вклучуваат-црвениот-аларм-/32093026.html (Пристапено на: 09.06.2023).

Според Генералниот секретаријат на Интерпол[3] во објавениот глобален извештај за компјутерски закани за КОВИД-19 од 2020 година, злонамерните домени, фишингот, онлајн измамите и малициозните софтвери се најчести форми на регистриран напад.

Се чини дека веродостојноста на овие податоци уште повеќе се зајакнува кога статистичките податоци ќе се споредат со податоци од други извори. „Статиста“[4] е водечки глобален снабдувач на податоци за пазарот и за потрошувачите. Според статистиките на „Статиста“, најголем број жртви на фишинг измами од 2018 година наваму е забележан во 2021 година, приближно 324 илјади. Во 2022 година, најчестиот вид сајбер криминал бил исто така фишингот, со замав од приближно 300 илјади поединци како жртви на фишинг, како и незанемарливи 59 илјади случаи на случаи на кражба на лични податоци.

Меѓу најтаргетираните индустрии од страна на сајбер криминалците се здравствените, финансиските, производствените и образовните институции. Во 2022 година, 85 отсто од анкетираните светски организации изјавиле дека наишле на масовни напади на фишинг, а три од четири биле цел на измами. Над четири од десет светски организации што доживеале фишинг напади претрпеле повреда на податоци на клиенти.[5]

На светско ниво, според „Статиста“[6], најчесто пријавените видови сајбер криминал во 2022 година по бројот на засегнати лица се фишингот, кражбата на лични податоци, измамите при онлајн купувањето, изнудата, лажната техничка поддршка, лажните инвестиции, кражбата на идентитет, измамата со лажен идентитет и кражбата на кредитни картички и чекови.

Се чини дека овие податоци неслучајно се такви. Анонимноста, глобалната неограниченост и лукративноста се главни двигатели што придонесуваат хакерите да се охрабрат и да започнат со сторување на овие дела. Знаејќи дека најголемиот дел од популацијата секојдневно поминува часови на интернет преку разни лични уреди чија сајбер безбедност веројатно не е на завидно ниво, најдобрата појдовна точка за хакерите е да навлезат во личните уреди, најчесто преку фишинг пораки, електронска пошта, па дури и телефонски повици. Овде се поставува прашањето дали обичниот граѓанин не е доволно едуциран за опасноста што може да го снајде и дали неговата финансиска состојба дозволува превентивно да дејствува кон заштита на својот уред, т. е. да купи антивирус, антималвер или друг вид безбедносни софтвери? Тешко е да се најде категоричен одговор на овие прашања, но, исто така, и тешко е да се занемарат.

Онлајн ризици

Нападите врз сајбер безбедноста за време на пандемијата имаат различни степени на влијанија врз поединци, организации, влади, групи, па и цели општества. Очигледно беше

---

[3] Global Landscape on Covid-19 Cyberthreat, Interpol General Secretariat https://www.google.com/url?sa=i&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=0CAIQw7AJahcKEwjI_dW5oryBAxUAAAAAHQAAAAAQAg&url=https%3A%2F%2Fwww.interpol.int%2Fcontent%2Fdownload%2F15217%2Ffile%2FGlobal%2520landscape%2520on%2520COVID-19%2520cyberthreat.pdf&psig=AOvVaw1_UeaX8GxmkTaALM9Yk3BB&ust=1695405108117149&opi=89978449 (Пристапено на: 04.11.2023).

[4] https://www.statista.com/register/basic/advice-email/?svid=519428217942 (Пристапено на: 22.08.2023).

[5] https://www.statista.com/statistics/1376249/cyber-attack-global-firms-by-type/ (Пристапено на: 22.08.2023).

[6] https://www.statista.com/statistics/184083/commonly-reported-types-of-cyber-crime-global/ (Пристапено на: 22.08.2023).

дека порастот на онлајн трансакциите ќе отвори нови патишта за хакирање и други малициозни сајбер настани насочени кон ранливите системи од комерцијална вредност, користејќи фишинг е-пошта како алатка за ширење малициозен софтвер, а социјалниот инженеринг како тактика да се намамат или да се манипулираат лица самите да ги дадат своите лични информации преку интернет за одредена легална цел, а всушност потоа се користат за криминални цели.

Како што беснееше пандемијата, онлајн услугите станаа широко прифатена алтернатива на активностите на работниот простор. Тоа, исто така, значеше дека би се зголемиле изложеноста и ризикот од кражба на несоодветно заштитени доверливи податоци преку интернет. Лошо или недоволно обезбедената работа од домашните системи беа најранливите и најпогодените цели за работење на далечина. Во својата книга „Компјутерска безбедност во пандемијата со КОВИД-19“[7], Кенет Окрифор објаснува дека инцидентите на пресретнување чувствителни податоци што се пренесуваат преку небезбедни телекомуникациски канали и слабо заштитени терминали за работење на далечина станаа гориво за лажни банкарски трансакции, неовластени процени, предност за откуп и арсенал за идни сајбер криминали.

Така, на 24 април 2020 година, јапонската компанија за игри, Нинтендо, откри дека хакерите незаконски стекнале неовластен пристап до 160 000 нејзини кориснички сметки, бројка што подоцна се зголеми за дополнителни 140 000 во јуни 2020 година[8]. Хакирањето, односно кражбата на овие „онлајн идентитети“ се случи среде пандемијата предизвикана од вирусот КОВИД-19, кога имало пораст на продажбата на „Nintendo Switch“, бидејќи луѓето се обидуваа да се забавуваат со игри додека беа во карантин. Овој податок е фрапантен и многу говори за неукоста или, можеби, и за незаинтересираноста и игнорантниот однос на луѓето кон нивните лични податоци на интернет. При нападите врз Нинтендо, хакерите го компромитирале наследниот систем за интеграција на „Nintendo Network ID“ („ННИД“) за да добијат пристап до профилите на Нинтендо. ННИД управува со сметките на старите платформи за игри „Нинтендо 3-ДС“. Откако хакерите добиле пристап до личните информации, вклучувајќи ги родендените и адресите на е-поштата на корисниците, Нинтендо подоцна ја идентификувал предизвиканата штета од хакирањето на сметките, а тоа е неможноста на системот да ги спречи корисниците да ја задржат истата лозинка. Како итно ублажување на влијанијата на сајбер криминалот, компанијата беше принудена да издаде извинување и советување за ресетирање лозинка до своите корисници и дека ќе осигури безбедност за да избегне повторување сличен настан во иднина.

Во зависност од природата и чувствителноста на украдените корпоративни податоци, губењето на трговските тајни го загрози опстанокот на засегнатите организации. Во здравствениот сектор, губењето или неовластеното менување на медицинската документација на пациентите ги изложи пациентите на ризици од погрешна дијагноза и погрешно препишување, па и двете имаа долгорочна тенденција да резултираат со смртни случаи.

Далекосежни влијанија имаше и во многу други сектори, вклучувајќи ги и владините сектори, финансиските институции, образованието (пропуштање настава),

[7] Okreafor, Kenneth (2021) “Cybersecurity in the Covid-19 Pandemic”, CRC Press.

[8] https://www.forbes.com/sites/daveywinder/2020/06/12/300000-nintendo-users-hacked-what-gamers-need-to-know-switch-gamers-account-passwords/amp/ (Пристапено на: 08.08.2023).

малопродажбата, е-трговијата и угостителството. Хакирањето на Твитер[9] од 15 јули 2020 година беше очигледно напад без преседан врз приватноста, довербата и безбедноста, надополнет со лошите механизми за контрола на пристап во услови на ранливи вработени во социјалниот инженеринг.

Тешкотиите за пристап до податоци за време на пандемијата предизвикана од вирусот КОВИД-19 покренаа важни прашања. Според својата природа одредени видови сајбер закани, особено откупниот софтвер, одбивањето на услугата и дејството на вирусот, може да предизвикаат огромно влијание врз дигиталните системи. Бавните или недостапните мрежи, кои произлегоа како резултат на безбедносните напади, станаа кошмар за услужните организации што се потпираа на брзата достапност на податоци во моментот кога имаат потреба за пристап до тие податоци во своето бизнис-работење.

Сите погоре наведени примери резултирале со загуби, на еден или друг начин. Малициозниот софтвер за откуп (англ. Ransomware) е криминален деловен модел што чува вредни датотеки, податоци или информации за откуп. На жртвите на напад со откупни софтвери може сериозно да им се деградираат операциите или целосно да се исклучат. Така, секојпат кога жртвите покажуваат неподготвеност да платат откуп, *Ransomware* резултира со загуба на податоци, големи трошоци и прекин на услугите, како за правни, така и за физички лица.

Угледот на една организација е негувано богатство и затоа ништо не може да биде толку штетно колку скандалот што следува по сајбер криминал, особено инциденти од висок профил што вклучуваат повеќе закани и хакирања. Окрифор прави терцијарен поглед на последиците. Прво, тоа дава првичен впечаток на неподготвеност и лоша култура на сајбер безбедност, што може да влијае врз нивото на доверба на клиентите, кои со доверба ѝ ги довериле своите податоци на организацијата. Второ, тоа покренува сомневања за внатрешна соработка што ги става брендот, производите, услугите и угледот на организацијата во голем ризик и потенцијално влијае врз нејзината пазарна конкурентност. Трето, судските спорови и истрагите што следуваат по сајбер криминал може да бидат скандалозни и потенцијално да откријат скриени тајни, а тоа дополнително може да го намали кредибилитетот на организацијата.[10]

Инцидентот на Твитер од 15 јули 2020 година[11], каде што беа хакирани повеќе кориснички сметки од висок профил на Џо Бајден, Бил Гејтс, Барак Обама, Илон Маск и 127 други, создаде сомнеж во главите на милиони негови глобални клиенти, доведе до речиси инстант опаѓање на покровителството на гигантот за микроблогирање и социјалните мрежи и предизвика пад од 4 % на акциите на Твитер на американската берза во рок од само неколку часа по инцидентот. Нарушувањето на безбедноста на Твитер, кое на хакерите им овозможи да упаднат во сметките на влијателни лидери, технолошки магнати и деловни директори, ја разниша довербата во платформата што политичарите и извршните директори ја користат за да комуницираат со јавноста, а особено ги покрена прашањата за „дослух на инсајдери“.

Покрај нефинансиските, логистичките и оперативните проблеми, сајбер нападот речиси секогаш доаѓа со големи финансиски загуби. Ваквите економски загуби обично се шират меѓу трошоците за извршување на операциите за одговор и обновување инциденти

[9] https://www.bbc.com/news/technology-53445090.amp (Пристапено на: 09.08.2023).

[10] Okreafor, Kenneth (2021) “Cybersecurity in the Covid-19 Pandemic”, CRC Press.
[11] https://en.m.wikipedia.org/wiki/2020_Twitter_account_hijacking (Пристапено на: 23.08.2023).

со сајбер безбедност, загубата поради намалениот приход како резултат на повлекувањето на покровителството од страна на клиентите и трошоците настанати од вредноста на украдените информации или вредноста на оштетените податоци.

Безбедносни мерки и препораки

Според американскиот Центар за интернет безбедност[12], длабинската одбрана (англ. Defense in Depth – „DiD“) е пристап за безбедност на информации во кој низа безбедносни механизми и контроли се смислено поставени низ компјутерската мрежа за да се заштитат доверливоста, интегритетот и достапноста на мрежата и податоците во неа. Иако ниту едно поединечно ублажување не може да ги запре сите сајбер закани, тие заедно обезбедуваат ублажување против широк спектар на закани, активирајќи алтернативен механизам во случај претходниот механизам да не успее. Кога е успешен, овој пристап значително ја зајакнува мрежната безбедност против многу видови напади. Оваа ефективна стратегија ги вклучува (засега) најдобрите безбедносни практики, алатки и политики, и тоа:

- Заштитните ѕидови (англ. Firewalls) се софтверски или хардверски уреди што го контролираат мрежниот сообраќај преку давање или негирање пристап на интернет-сообраќајот;
- Системи за спречување или откривање упади (IDS/IPS) – IDS праќа предупредување кога е откриен злонамерен мрежен сообраќај, додека, пак, IPS се обидува да спречи и да предупреди идентификувана злонамерна активност на мрежата или работната станица на корисникот;
- Софтверите за откривање и одговор на т.н. „крајна точка“ (EDR) се наоѓаат на системот на клиентот (на пр. лаптоп или мобилен телефон на корисникот) и обезбедуваат антивирусна заштита, предупредување, откривање, анализа, тријажа на закани и способности за разузнавање закани;
- Мрежната сегментација е практика на поделба на мрежата на повеќе подмрежи дизајнирани за деловни потреби. На пример, ова често вклучува постоење подмрежи за директори, финансии, операции и човечки ресурси. Во зависност од потребното ниво на безбедност, овие мрежи можно е да не може директно да комуницираат меѓу себе;
- Принципот на „најмала привилегија“ подразбира контроли само за да им се додели пристап на корисниците, системите и процесите до ресурсите (мрежи, системи и датотеки) што се апсолутно неопходни за извршување на нивната доделена функција;
- Силните лозинки се критичен механизам за автентикација во безбедноста на информациите. Ова значи дека лозинката може да подразбира користење повеќекратна автентикација за која било сметка со вредност, користење фраза со повеќе зборови и користење лозинки што не се повторуваат, односно кои не се користени претходно од истиот корисник;

[12] https://www.cisecurity.org/insights/spotlight/cybersecurity-spotlight-defense-in-depth-did (Пристапено на: 12.08.2023).

- Ажурирања: ова е процес на примена на ажурирања оперативен систем, софтвер, хардвер или приклучок за решавање идентификувани пропусти и унапредување на самиот оперативен систем, хардвер или приклучок.[13]

Окрифор вели дека движечка сила во сајбер безбедноста по пандемијата предизвикана од вирусот КОВИД-19 ќе биде спојот на машинско учење со проширена информатичко-технолошка рамка што ќе инкорпорира вештачка интелигенција. Со предвидлива аналитика, столбот на вештачката интелигенција подразбира детектирање предвидливи закани, приспособување на безбедносни филтри и системи за предупредување управувани од вештачката интелигенција и интелигентни мрежи што самите ќе може да закрепнат доколку претрпат напад. Со вештачката интелигенција, можностите за сајбер безбедноста се сметаат за целосно неограничени.[14]

Со вештачката интелигенција ќе има помал акцент на системите за сајбер безбедност засновани врз однесување, а наместо тоа, фокусот ќе се префрли на сложени системи што може подобро да ги заштитат податоците и да предвидат инциденти со загуба на податоци пред да се случат. Затоа, Окрифор смета дека следната генерација сајбер безбедност во вештачката интелигенција ќе го затвори јазот помеѓу човековата интерпретација на безбедносните предупредувања и способностите за откривање и одговор на сајбер напади, а тоа нема да остави простор за човечки грешки што се распространети во денешните неисправни парадигми за сајбер безбедност. Алгоритмите за машинско учење дизајнирани да анализираат сложени агрегати на податоци ќе помогнат во предвидување и неутрализирање на сајбер измамите каде што луѓето се измамени од измамници преку лажно претставување.[15]

Пандемијата предизвикана од вирусот КОВИД-19, несомнено, го забрза процесот на преобликување на компјутерскиот криминалот и на сајбер безбедноста. Нè научи дека подготовката е клучна за успешно ограничување на ризиците поврзани со сајбер нападите и компјутерскиот криминал воопшто. Спремноста за брзо реагирање при непредвидени настани помага да се намали влијанието на сајбер нападите. Компаниите што биле фатени неподготвени и во невнимание ќе мора брзо да ја проценат нивната изложеност на сајбер закани и приоритетно да ја зајакнат сајбер безбедноста преку инвестирање во соодветна технологија, квалификувани професионалци од областа на сајбер безбедноста и квалитетна едукација на вработените. Корпоративните компјутерски уреди и системи, особено оние што дозволуваат далечински пристап до доверливи и лични податоци, мора да бидат соодветно заштитени. Реалноста е дека компаниите треба да го променат својот изглед од „ако“ бидат нападнати во „кога“ и да сфатат дека последиците од нарушувањето на приватноста на податоците или откупниот софтвер може да бидат финансиски погубни. Исто така, треба да се запомни дека финансиската добивка не е единствениот мотив зад сајбер нападите. Дополнителна закана претставува хактивизмот и неговата цел да ја нарушат бизнис-репутацијата.

На индивидуално ниво, едукацијата на поединецот, се чини, е клучен фактор за сузбивање на компјутерскиот криминал: користење антивирус, подигнување на свеста кај вработените во однос на тоа како да може подобро да ги препознаваат компјутерските

[13] https://www.cisecurity.org/insights/spotlight/cybersecurity-spotlight-defense-in-depth-did (Пристапено на: 12.08.2023).
[14] Okreafor, Kenneth (2021) “Cybersecurity in the Covid-19 Pandemic”, CRC Press.
[15] Ibid.

напади, да препознаат фишинг е-пошта, како и да користат ВПН (виртуелна приватна мрежа), кога тоа е целисходно.

Идентификацијата и анализата на различните облици на сајбер криминалот се одвиваат низ развивање безбедносни мерки и процедури за заштита од сајбер напади, опфаќаат цел процес на собирање, анализа и презентација пред истражните органи на колку што е можно повеќе докази за идентификација на сторителите, а честопати се јавува и потреба од реконструкција на криминалните активности. За да се постигне ова, неопходно е државата да поседува компјутерски форензичари и експерти што би биле најмалку на исто техничко ниво со сторителите на делата.

Со цел конечна правна разрешница и примена на репресивни мерки, нужно е детално проучување и анализа на законските акти, со особен осврт на прашањето кои се причините и мотивите за вршење сајбер криминал и следење на трендовите во оваа област. Сајбер безбедноста е динамично поле што бара континуирано приспособување и внимателност. Затоа, препознавајќи ги лекциите научени од ерата на пандемијата предизвикана од вирусот КОВИД-19, може да ја зајакнеме колективната свест и одбрана, да создадеме побезбеден дигитален екосистем за сите и со тоа да се намали стапката на компјутерски криминал глобално.

ИЗВОРИ И КОРИСТЕНА ЛИТЕРАТУРА:

Global Landscape on Covid-19 Cyberthreat, Interpol General Secretariat https://www.google.com/url?sa=i&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=0CAIQw7AJahcKEwjI_dW5oryBAxUAAAAAHQAAAAAQAg&url=https%3A%2F%2Fwww.interpol.int%2Fcontent%2Fdownload%2F15217%2Ffile%2FGlobal%2520landscape%2520on%2520COVID-19%2520cyberthreat.pdf&psig=AOvVaw1_UeaX8GxmkTaALM9Yk3BB&ust=1695405108117149&opi=89978449 (Пристапено на 04.11.2023)

https://en.m.wikipedia.org/wiki/2020_Twitter_account_hijacking (Пристапено на: 23.08.2023)

https://www.bbc.com/news/technology-53445090.amp (Пристапено на: 09.08.2023)

https://www.cisecurity.org/insights/spotlight/cybersecurity-spotlight-defense-in-depth-did (Пристапено на: 12.08.2023)

https://www.forbes.com/sites/daveywinder/2020/06/12/300000-nintendo-users-hacked-what-gamers-need-to-know-switch-gamers-account-passwords/amp/ (Пристапено на: 08.08.2023)

https://www.slobodnaevropa.mk/a/зачестените-сајбер-напади-на-државни-сајтови-го-вклучуваат-црвениот-аларм-/32093026.html (Пристапено на 09.06.2023)

https://www.statista.com/register/basic/advice-email/?svid=519428217942 (Пристапено на 22.08.2023)

https://www.statista.com/statistics/1376249/cyber-attack-global-firms-by-type/ (Пристапено на 22.08.2023)

https://www.statista.com/statistics/184083/commonly-reported-types-of-cyber-crime-global/ (Пристапено на 22.08.2023)

Okreafor, Kenneth (2021) “Cybersecurity in the Covid-19 Pandemic”, CRC Press

Jovan Petrezanov, LL.M.[16]

THE IMPACT OF THE COVID-19 PANDEMIC ON CYBERERCRIME

Abstract

Computer crime is one of the largest, most active and most complex forms of crime globally. Considering that it is a type of crime that is inseparably connected with technology, computer crime develops and takes seriously complex forms with the development of technology, but also with other influences, such as the current Covid-19 pandemic. Although seemingly under control, it has been more than three years and yet Covid-19 is still a pandemic, the virus continues to mutate into new strains and to spread and claim victims globally.

Covid-19 has shaken modern humanity to its core: the freedom of movement, freedom of the market and entrepreneurship, legal security of citizens, and healthcare systems were on the verge of collapse, some of the basic rights of workers were restricted (healthcare workers did not take vacation), and in the first months of the pandemic, neither the education nor the justice system functioned. Under such circumstances, while all that traffic was decreasing, the internet traffic became more and more dense day by day, which brought such a number of accidents and victims as humanity has not witnessed for a long time. It seems that the health pandemic has brought along another evil – the cyber pandemic.

There is no doubt that this problem has not been sufficiently studied, and at the same time it is gaining momentum. Thanks to scientific research and social dialogue, people's awareness of recognizing, responding to, preventing and recovering from computer crimes can be more easily improved.

Key Terms: Computer Crime, Pandemic, Malware, Computer Attack, Consequences.

[16] The author is a lawyer, master of criminal law and a legal consultant for management of international commercial and IT contracts.