direktno

'MADE IN CHINA 2025.'

# Kibernetički napadi na WHO; hakeri cijeloga svijeta u naletu na farmaceutske kompanije koje istražuju lijek za Covid-19

Mnogi su još prije nekoliko mjeseci pisali o primjeni međunarodnog prava u cyber prostoru i na globalnu pandemiju Covid-19, ali relativno je malo ispitalo povezanost između ta dva područja. Bez obzira na taj nadzor, posljednjih su tjedana zabilježeni kibernetički napadi na organizacije na prvom mjestu reakcije na pandemiju Covid-19, uključujući zlonamjerne cyber operacije protiv Svjetske zdravstvene organizacije, pružatelja lijekova, istraživačkih instituta, proizvođača lijekova, bolnica i bolničkih mreža.

19.10.2020. u 18:58

Foto: Unsplash/EPA-EFE/Wang Ye/Xinhua

TEKST SE NASTAVLJA NAKON OGLASA


Osvoji Samsung tablet – zaigraj Halloween turnir u Admiralu i pokupi spektakularne nagrade!

Sponsored by Midas

Kao odgovor na ove napade, Europska unija izdala je izjavu u kojoj "Europska unija i njezine države članice pozivaju svaku zemlju da provede dužnu skrb i poduzme odgovarajuće mjere protiv aktera koji takve aktivnosti provode s njezinog teritorija, u skladu s međunarodnim pravom".

## Borba hakera

Dok se istraživači diljem svijeta utrkuju u razvoju cjepiva protiv korona virusa, od početka ove godine špijunaža i pokušaji hakiranja usmjereni na prikupljanju obavještajnih podataka o Covid-19 diljem svijeta uzeli su maha. Prema brojnim izvješćima iz različitih relevantnih izvora, najviše od strane Kine i Rusije.

Ruski hakeri, naime, špijuniraju organizacije uključene u razvoj cjepiva u SAD-u, Kanadi i Ujedinjenom Kraljevstvu.

Do trenutka pisanja ovoga teksta, Covid-19 ubio je 1,1 milijun ljudi širom svijeta, dok je virusom zaraženo najmanje 40 milijuna.

Sada je definitivno jasno da će se za borbu protiv pandemije morati ići s više cjepiva. Zbog toga se mnogobrojne države natječu za zalihe koje bi trebale biti dostupne početkom sljedeće godine i zbog te konkurencije na površinu je izbila sebičnost nacija; primjerice, SAD u operaciji "Warp Speed" unaprijed su platile pravo na stotine milijuna doza cjepiva od domaćih i stranih tvrtki.

I druge zemlje uključile su se u utrku, poput Ujedinjenog Kraljevstva, Francuske, Indije ali, naravno i Kine.

Konkurencija je ogromna, najjače farmaceutske kompanije involvirane su u istraživanja, ogroman novac je u igri, a pritom bez da itko sa sigurnošću može reći čak niti hoće li cjepivo biti pronađeno i napokon, ako se nađe, hoće li biti dovoljno učinkovito, koliko će trajati, hoće li trebati docijepljivanje...

Tako je sredinom srpnja objavljeno zajedničko izvješće britanskog Nacionalnog centra za kibernetsku sigurnost (NCSC), američke Agencije za nacionalnu sigurnost i Odjela za nacionalnu sigurnost (NSA/CSS) te kanadskog Zavoda za sigurnosnu komunikaciju, u kojem se navodi da je tijekom 2020. godine, APT29, ruska hakerska grupa, dio ruskih obavještajnih službi, poznate pod nazivom "Vojvoda", ili "Cozy Bear", pokušala ukrasti podatke vezane uz istraživanja o liječenju te bolesti od akademskih i farmaceutskih ustanova u svijetu.

No, Rusija nije jedina koja navodno špijunira s namjerom krađe informacija i intelektualnog vlasništva u vezi s razvojem i ispitivanjem cjepiva.

## Iran u špijunskoj ekspanziji

Prema informaciji koju je još u srpnju ove godine prenio Reuters, navodno su hakeri povezani s Iranom pokušali provaliti na račune e-pošte američkog proizvođača lijekova Gilead Sciences, a koji ima potencijalno perspektivni lijek za liječenje virusa Covid-a-19.

Iran je, dakako, odbacio tu optužbu.

Prije koji mjesec (travanj 2020.), američke obavještajne službe zabilježile su da su hakeri s vezama s Iranom pokušali provaliti u Svjetsku zdravstvenu organizaciju (WHO), a istraživači izraelske obavještajne tvrtke za kibernetsku sigurnost ClearSky, potvrdili su da su web domene i poslužitelji hostinga korišteni u nedavnim pokušajima hakiranja povezani s Iranom.

Iranska misija pri Ujedinjenim narodima zanijekala je bilo kakvu umiješanost u napade uz izjavu da su kibernetičke aktivnosti kojima se Iran bavi isključivo obrambene s ciljem zaštite od daljnjih napada na iransku infrastrukturu.

Valja reći kako je infrastrukturu za hakiranje korištenu u pokušaju kompromitiranja računa elektronske pošte izvršnog direktora Gileada, ranije u cyber napadima koristila skupina osumnjičenih iranskih hakera, poznatija pod imenom "Šarmantna maca" (Charming Kitten).

Također, podsjetimo, Iran je među najpogođenijima po broju umrlih od Covida-19 na cijelom Bliskom istoku.

## Ne miruju ni u Aziji

Od kada je krenula pandemija, ni špijuni u Aziji ne miruju: FireEye, kompanija za kibernetičku sigurnost, u travnju je izvijestila da su "najranije od siječnja do travnja 2020., vijetnamski APT32 hakeri provodili kampanje upada protiv kineskih ciljeva, u svrhu prikupljanja obavještajnih podataka o krizi Covida 19".

Navodne su mete bile kinesko Ministarstvo za izvanredne situacije i općinska vlada notornog grada Wuhan, odakle je i krenuo cijeli taj horor koji je Europu i SAD, ali i ostatak svijeta bacio na koljena.

Vijetnam je pak optužio kinesku vladu da su napadi na njihov zdravstveni sustav povezani s Kinom.

I Južna Koreja aktivirala je svoje špijunske potencijale pa su tako južnokorejski hakeri "naciljali" Svjetsku zdravstvenu organizaciju i dužnosnike u Sjevernoj Koreji, Japanu i SAD-u.

Inače, APT je skraćenica od Advanced Persistent Threat, također je poznat kao OceanLotus Group, APT-C-00, SeaLotus i OceanBuffalo, prvi je put identificiran 2012. godine, kada je pokrenuo kibernetičke napade na kineske entitete, proširio se na ciljeve u Vijetnamu, ali i na Filipinima.

## Novi 'hladni' rat

Najvještiji kineski hakeri i špijuni angažirali su se na krađi američkih istraživanja u naporima da se razviju cjepiva i tretmani za korona virus. Kada je korona uzela maha, osobito u SAD-u, u svibnju je američki predsjednik **Donald Trump** najavio da će administracija poduzeti sve potrebne korake da zaustavi nalet

kibernetičke krađe i napade država koje žele osigurati prednost u borbi protiv pandemije. Posebno se referirao na Kinu i objavio da će poduzeti sve mjere u obrani protiv "kineskog virusa".

Službenik jedne europske biotehnološke tvrtke rekao je da je farmaceutska industrija "Red alert", odnosno, "Crvenu uzbunu", i poduzima dodatne mjere opreza kako bi se zaštitila od pokušaja krađe istraživanja cjepiva protiv Covid-a 19. Jedan od načina je da se podaci koji se odnose na ispitivanja cjepiva pohranjuju na tzv. "air-gapped" (sa zračnim zazorom/s procjepom za zrak), računalima koji su odspojeni s interneta.

Možemo reći da je novi hladni rat u punom jeku, ovaj puta kibernetički i još kompleksniji, jer ulozi su veliki.

Američki dužnosnici često ukazuju na kineskog predsjednika **Xi Jinpinga** i njegov plan "Made in China 2025", prema kojemu Kina planira postati svjetski lider u najvažnijim tehnologijama 21. stoljeća - umjetnoj inteligenciji, obnovljivoj energiji, kvantnom računanju, automobilima bez vozača i širokom spektru medicinskih tehnologija...

U posljednjih nekoliko godina, Ministarstvo pravosuđa USA (U.S. Department of Justice), podnijelo je prijave u više slučajeva koji uključuju kineske državljane, ili ljude za koje se sumnja da rade za Kinu, zbog krađe medicinske tehnologije.

## Kinezi u svjetskoj ekspanziji

Osim hakiranja, druga metoda koju Kinezi vrlo vješto koriste, već godinama, slanje je učenika, ili istraživača na rad u SAD, često na dulje vrijeme.

Primjerice, 2019. godine, Ministarstvo pravosuđa podiglo je optužnicu protiv kineskog para koji je deset godina radio u laboratoriju u Ohiju koji istražuje dječje bolesti, uključujući rak u djece. Optužili su ih za krađu istraživanja u tom laboratoriju, a koja su transferirali u tvrtku koju su osnovali u Kini.

Kinezi u Treći krak infiltriranja kineskih vlasti u američke znanstvene krugove, ne samo farmaceutske, tzv. je Program "Tisuću talenata" (Thousand Talents Program). Taj Program osnovala je 2008. središnja vlada Kine kako bi prepoznala i zaposlila vodeće međunarodne stručnjake za znanstvena istraživanja, inovacije i poduzetništvo. U njemu se identificiraju perspektivna istraživanja, u farmaceutskim kompanijama i sličnom sektoru, zatim najbolji studenti s američkih sveučilišta, kao i vrhunski predsjednici uprava u određenim poslovnim krugovima, od interesa za kinesku vladu; te im se nudi financiranje daljnjeg školovanja, za što se, naravno, očekuje neki oblik pristupa određenom istraživanju...

Takav svojevrsni "head-hunting", uobičajena je praksa u svijetu, no kažnjivi element pojavljuje se samo ako određena osoba pristane na bespovratno financiranje studija (ili istraživanja i sl.), od strane Kine. Zato su američki akademici, studenti, istraživači, itd. dužni američkoj vladi prijaviti ako primaju bilo takva strana sredstva.

Ta praksa je intenzivirana unazad nekoliko godina; određene osobe iz više sektora koji uključuju bolnice, medicinske centre i istraživačke institucije te farmaceutsku zajednicu, pozivaju se u Washington na informativni sastanak na kojem ih, u sklopu jednodnevnog povjerljivog informativnog rada, obučavaju kako razumjeti složenost prijetnje i koje korake poduzeti, koje službe kontaktirati u slučaju sumnje na hakerski napad i slično.

Fresenius Grupa, veliki europski zdravstveni konglomerat, bila je žrtvom hakerskog napada polovicom ove godine, pri kojemu je računalni virus zarazio najmanje jedan od IT sustava poduzeća. To pokazuje da zlonamjerni hakeri, usprkos globalnoj zdravstvenoj krizi, ne štede ni zdravstvene ustanove, odnosno, tretiraju ih kao "legitimne objekte", potpuno nezainteresirani za potencijalne ozbiljne posljedice po globalno zdravlje.

Zbog manjkavosti pravnih normi koje se odnose na špijuniranje, Sjedinjene Američke Države trebale bi surađivati sa saveznicima tijekom sljedećih tjedana, kako bi se što prije razvilo set snažnih principa specifičnih za Covid-19.

SAD i EU predložile su norme povezane s Covid-om 19, a radna skupina UN-a, kojoj je cilj razviti okvir za odgovorno ponašanje države u cyber prostoru, također je postigla napredak na ovom području. Te napore treba učiniti konkretnijim i cjelovitijim.

Pravna pitanja oko toga što predstavlja špijunažu, do kuda sežu ovlasti pojedine države i što točno uključuje suverenitet jedne države, nisu još definirana na globalnom nivou i zato hakeri koriste te rupe u sustavima...

** Dopušteno je prenošenje sadržaja uz objavu izvora i autora.*

**Tekst je nastao u okviru projekta kojeg je financijski podržala Agencija za elektroničke medije.**

Agencija za elektroničke medije
Agency for the electronic media

## VIŠE S WEBA


**Osvoji Samsung tablet – zaigraj Halloween turnir u Admiralu i pokupi spektakularne nagrade!**

**Želite li ravan trbuh za 10 dana? Svaki dan natašte...**

**Nissan X-Trail s automatskim DCT mjenjačem i 160 KS stvoren je za svaki teren. Sada u super ponudi!**

**Jedinstvena maska za lice s trostrukom antivirusnom zaštitom! Traje minimalno 7 mjeseci i sigurna za kožu!**


**Epic burgeri su stigli u McDonald's. Doživi epsku avanturu uz nove okuse.**

**TENA Pants upijajuće gaćice za pokretne osobe s inkontinencijom nose se poput običnog donjeg rublja**


**Pametna kupnja u Eurospinu! Istražite tjednu ponudu u novom katalogu.**


**U Eurospinu pronađite široki asortiman voća i povrća po 6,99 po kg/kom.**

**Iskoristite prednosti online kupnje za nova protuprovalna vrata! Proizvedeno u Hrvatskoj!**

Sponsored by Midas