# Celosvětový skandál Izraelského špionážního programu Pegasus: JE I VÁŠ TELEFON “24-HODINOVÝM SLEDOVACÍM ZAŘÍZENÍM”?

- CZ24 News | 24. září 2021
Hackerské útoky byly odhaleny v nové zprávě laboratoře Citizen Lab na Torontské univerzitě, která se intenzivně zabývá studiem programu Pegasus a příbuzných neblahých moderních jevů.

Jak píše Guardian, Pegasus je “pravděpodobně nejvýkonnější špionážní software, jaký byl kdy vyvinut” a dokáže z mobilního telefonu udělat “24hodinové sledovací zařízení” – sbírá zprávy, hesla, fotografie, vyhledávání na internetu a další data a přebírá kontrolu nad kamerou a mikrofonem.

To vše lze provést pomocí technologie “zero-click”, což znamená, že k infikování telefonu není třeba kliknout na napadený odkaz ani udělat nic jiného.

Jako by bahrajnští bojovníci za lidská práva neměli v království, kde se mučí, dost starostí už před úplným zrušením práva na soukromí.

Přesto je zpráva Občanské laboratoře jen nejnovější epizodou dystopického sci-fi thrilleru, který v současnosti na Zemi prožíváme.

V červenci projekt Pegasus – konsorcium 17 médií spolupracujících s Amnesty International a pařížskou nevládní organizací Forbidden Stories – odhalil uniklý seznam více než 50 000 čísel chytrých telefonů z celého světa. Většina čísel byla soustředěna v zemích, o nichž je známo, že byly klienty NSO, což naznačuje, že seznam byl kompilací potenciálních cílů sledování.

Deník The Washington Post, jeden z přidružených deníků, vysvětlil, že u 37 z uvedených telefonů bylo dosud potvrzeno, že se staly cílem pokusu nebo úspěšného hackerského útoku špionážního softwaru Pegasus. Mezi majiteli telefonů byli novináři, aktivisté a “dvě ženy z nejbližšího okolí saúdského publicisty” Džamála Chášakdžího, který byl 2. října 2018 zavražděn agenty saúdského státu.

Přesně den před vraždou společnost Citizen Lab s “vysokou mírou jistoty” varovala, že telefon Omara Abdulazize, saúdského kritika v Kanadě, byl infikován programem Pegasus. Ukázalo se, že Abdulaziz byl blízkým přítelem a častým Khashoggiho dopisovatelem.

A přestože představitelé NSO hlasitě popírají, že by se kdy podíleli na jakémkoli pochybení, seznam náhod pokračuje.

Více než 15 000 z 50 000 telefonních čísel bylo například v Mexiku, které se v roce 2011 stalo prvním mezinárodním klientským pokusným králíkem NSO. Při úvahách o osudu mexického reportéra na volné noze Cecilia Pinedy, který byl zastřelen v houpací síti poté, co se jeho číslo dvakrát objevilo na nechvalně proslulém seznamu, deník Washington Post přihodil výhradu: “Není jasné, jakou roli, pokud vůbec nějakou, hrála schopnost programu Pegasus geolokace svých cílů v reálném čase, která přispěla k jeho vraždě.”

Podle agentury Reuters podepsaly mexické vládní agentury se společností NSO Group v letech 2011 až 2018, především za vlády pravicového prezidenta Enriqueho Peña Nieta, smlouvy v hodnotě až 160 milionů dolarů. Díky těmto investicím se operátoři Pegasu mohli zaměřit mimo jiné na

vyšetřovatele, kteří se zabývali násilným zmizením 43 studentů ve státě Guerrero mexickými bezpečnostními silami v roce 2014. Terčem útoku se stali také manželka, děti a kardiolog levicového politika Andrése Manuela Lópeze Obradora, který mezitím vystřídal Peñu Nieta.

V Bahrajnu laboratoř Citizen Lab ověřila, že pět z devíti nedávno hacknutých čísel je uvedeno na seznamu projektu Pegasus. Ačkoli Bahrajn a Izrael formálně normalizovaly vztahy teprve v loňském roce, bilaterální spřízněnost předcházela oficiálnímu vyznání lásky a bahrajnská vláda pravděpodobně v roce 2017 přidala do svého represivního arzenálu špionážní software Pegasus.

Jistě není těžké pochopit, proč by se "nejvýkonnější špionážní software, jaký byl kdy vyvinut", mohl hodit v místě, které je známé potlačováním, zadržováním, mučením a zabíjením protestujících – nemluvě o odebírání občanství bahrajnským občanům, kteří se příliš angažují v oblasti lidských práv, aktivismu, žurnalistiky a dalších ohrožujících aktivit.

Spojené arabské emiráty (SAE), které v loňském roce oslavily normalizaci vztahů s Izraelem, již dlouho spolupracují s izraelskou špionážní technologií, o čemž svědčí i masový civilní sledovací systém Falcon Eye, který v Abú Zabí instalovala společnost vlastněná Izraelem.

Článek Middle East Eye z roku 2015 citoval zdroj blízký společnosti Falcon Eye ohledně jejích funkcí: "Každý člověk je sledován od okamžiku, kdy opustí práh svého domu, až do okamžiku, kdy se k němu vrátí. Jejich pracovní, sociální a behaviorální vzorce jsou zaznamenávány, analyzovány a archivovány".

Jako by to nestačilo, telefon autora článku skončil – kde jinde? – na seznamu projektu Pegasus.

V roce 2016 analytici zdokumentovali pokus o hackerský útok programu Pegasus na vyznamenaného emirátského obhájce lidských práv Ahmeda Mansoora, který je v současné době vězněn za tak ohavné zločiny, jako je urážka "postavení a prestiže SAE". Co by ostatně mohlo být kritizováno v prestižní zemi, kde byly občanské svobody zlikvidovány a nahrazeny nákupními centry a umělými ostrovy – a kde osoby podezřelé z opozice vůči tomuto uspořádání mají nárok na vězení, mučení a zmizení?

Tolik k "politice lidských práv" společnosti NSO, která je uvedena na internetových stránkách firmy a která údajně zahrnuje "smluvní závazky, které vyžadují, aby zákazníci společnosti NSO omezili používání produktů společnosti na prevenci a vyšetřování závažných trestných činů, včetně terorismu, a aby zajistili, že produkty nebudou používány k porušování lidských práv".

Izraelské ministerstvo obrany musí údajně jako dodatečnou záruku schvalovat všechny prodeje špionážního softwaru NSO klientům po celém světě.

Vzhledem k tomu, že izraelská definice protiterorismu zahrnuje například bombardování palestinských civilistů, není samozřejmě těžké pochopit, že lidská práva mohou jít stranou.

Jedinečné postavení Izraele jako státu apartheidu a násilné okupační mocnosti mu totiž dává značnou výhodu ve vývozu tradičních zbraní, ale i produktů kybernetické bezpečnosti a dalších represivních zkušeností, které jsou testovány na skutečných Palestincích.

Už v roce 2016 měl Izrael nejvíce sledovacích společností v přepočtu na obyvatele na celé planetě. A jak ukazuje případ společností NSO a Pegasus, soukromý sledovací průmysl může stoupat do stále větších výšin díky velkému množství bývalých izraelských vojenských kyberšpiónů, kteří se chtějí zapojit do akce v lukrativním a do značné míry neregulovaném oboru.

V roce 2019 mimochodem společnost WhatsApp vlastněná Facebookem podala žalobu na NSO kvůli

obvinění z hackerství – právní boj, který stále pokračuje a k němuž se mezitím připojil Microsoft a další technologičtí giganti. Nehledě na to, že několik z nich bylo samo zapleteno do cenzury palestinských novinářů a aktivistů – nebo že Microsoft kdysi investoval do izraelské firmy na rozpoznávání obličejů, která tajně sledovala Palestince na Západním břehu Jordánu.

Pro podobně solidní etiku není třeba hledat nic jiného než článek Associated Press ze 4. srpna, který upřesňuje, že penzijní fond státních zaměstnanců státu Oregon byl "jedním z největších investorů, ne-li největším" investorem do soukromé kapitálové společnosti s většinovým podílem v NSO Group.

Ve své nové zprávě o Bahrajnu Citizen Lab uvádí, že "pod záminkou řešení COVID-19 bahrajnská vláda zavedla další omezení svobody projevu". Je tedy nepochybně méně než potěšující, že Naftali Bennett – ultrapravicový bývalý izraelský ministr obrany, který v roce 2020 navrhl zapojení NSO do boje proti koronaviru – je nyní izraelským premiérem.

Vzhledem k tomu, že izraelská mise, jejímž cílem je normalizovat likvidaci práv Palestinců, pokračuje současně s normalizací masové špionáže a faktickou kriminalizací svobody myšlení, nesmíme ztrácet ze zřetele, že nic z toho ve skutečnosti normální není.

Autor: Belan Fernandez

Překlad: zvedavec