NYA
ARGUS

HUNDRAFJORTONDE ÅRGÅNGEN Nr 11 10.10.2021

KOMMENTARER: TRYGVE SÖDERLING

Med spionen i fickan

Officiellt ska hackningsprogrammet Pegasus förebygga brott.
I verkligheten används det för att begå brott, inklusive mord.

I juli i år meddelade Amnesty International att man hade kommit över en lista på 50 000 telefonnummer som potentiellt kan ha hackats av regimer som skaffat sig det israeliska spionprogrammet Pegasus. Minst 600 av numren tillhörde politiker i olika länder, bland dem Frankrikes president Emmanuel Macron och 15 ministrar i hans regering. I deras fall antogs Marocko vara intressenten.

Verklig fara innebär Pegasus i alla fall för de journalister, mänskorättsaktivister och regimkritiker som också finns med i denna telefonkatalog för repression – guld värd för de auktoritära regimer som prenumererar på progammet genom det israeliska bolaget Niv, Shalev & Omri (NSO). Trots programmets namn, som anknyter till skaldekonstens bevingade pegas, handlar det om en trojansk häst.

Världskänt blev spionprogrammet i samband med styckmordet på journalisten Jamal Khashoggi på Saudiarabiens konsulat i Istanbul 2018. Före mordet hade flera i hans närmaste krets fått sina telefoner hackade av den saudiska regimen, som är en av många belåtna NSO-kunder.

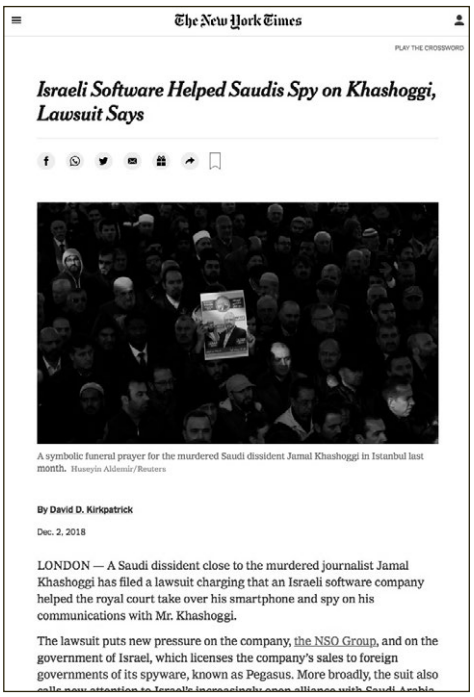
Exempel på att Pegasus använts mot regimkritiker hade då redan sipprat fram i offentligheten under ett par års tid, framför allt från Mexiko. 2016 kom *The New York Times* över interna NSO-dokument som bland annat innehöll företagets prislista: för spionage på tio iPhones debiterade bolaget initialt 1 150 000 dollar, plus 17 % av detta för varje följande år.

Pegasus är så avancerat – skryter företaget – att offret inte ens behöver klicka på någon länk eller svara på samtal eller mejl för att programmet ska installera sig och låta en tredje part ta över telefonen. Pegasus ger sig själv administratörstatus, med större rättigheter än telefonens ägare: spionen kan slå på mikrofonen och kameran, läsa gps-positioner och alla meddelanden, hämta data ur alla appar. Att använda krypterade tjänster som Signal eller Telegram är meningslöst, eftersom Pegasus-spionen ”ser” telefonen innan krypteringen.

Den mexikanska regeringen, före regimskiftet 2018, hör till de tidigast avslöjade kunderna hos NSO. Mellan 2011 och 2017 ska den ha betalat 80 miljoner dollar för tjänsten, som bland annat använts för att sabotera och förhindra utredningen av en massaker 2014 där 43 studenter ”försvann” efter en protest i Mexico City. Många mexikanska journalister och aktivister har hackats, till och med hälsoaktivister som arbetat för att minska konsumtionen av läskedrycker har trakasserats och utsatts för Pegasus-attacker. När den mexikanska staten, nu under ny regim, åtalade tidigare ”säkerhets”-chefen Tomás Zerón de Lucio för bortrövande, tortyr, för-

störande av bevismaterial och försnillande av 85 miljoner dollar, flydde han logiskt nog till Israel, som vägrar att utlämna honom.

NSO själva hävdar att deras digitala vapen enbart säljs till schyssta regimer och enbart för att förebygga brottslighet och terrorism. Listan på hittills kända kunder talar ett annat språk. Förutom Saudiarabien och tidigare Mexiko finns där bland andra Förenade Arabemiraten, Algeriet, Rwanda, Indien, Botswana, Azerbajdzjan, Bahrain, Kazakstan och Ungern. Med sådana kunder blir försäljaren medbrottsling.



The New York Times

PLAY THE CROSSWORD

Israeli Software Helped Saudis Spy on Khashoggi, Lawsuit Says

A symbolic funeral prayer for the murdered Saudi dissident Jamal Khashoggi in Istanbul last month. Huseyin Aldemir/Reuters

By David D. Kirkpatrick

Dec. 2, 2018

LONDON — A Saudi dissident close to the murdered journalist Jamal Khashoggi has filed a lawsuit charging that an Israeli software company helped the royal court take over his smartphone and spy on his communications with Mr. Khashoggi.

The lawsuit puts new pressure on the company, the NSO Group, and on the government of Israel, which licenses the company's sales to foreign governments of its spyware, known as Pegasus. More broadly, the suit also

Åtal: Saudiarabien spionerade på Khashoggi med israelisk programvara. The New York Times *2.12 2018.*

Efter avslöjandet i juli i år sa Europakommissionens ordförande Ursula von der Leyen att om Ungern använt Pegasus är det ”helt oacceptabelt och mot alla slags regler vi har i EU”.

Trots att kriminella missbruk av Pegasus nu har dokumenterats gång på gång under minst fem års tid, och troligen utövats i tio, är det som om de indignerade reaktionerna i media och från politiker varje gång skulle försvinna i ett svart hål, för att sedan yrvaket upprepas vid nästa avslöjande.

Snarare än att drabbas av sanktioner och kontroll har uppmärksamheten gett utvecklaren NSO gratis reklam bland tyrannerna. Liksom med de enorma skatteparadis-avslöjandena – nu senast ”Pandorapappren” – är de som drar nytta av kriminella kryphål alltför mäktiga, eller har alltför mäktiga beskyddare, för att ropen på lagstiftning och straff ska resultera i annat än tomma löften och varm luft.

Stormakter som Kina och USA har sina egna spionprogram (vi minns förstås Edward Snowdens avslöjande av amerikanska NSA 2013), men med sin överrock USA:s goda minne har israeliska NSO obekymrat kunnat fortsätta sälja Pegasus till skurkstater och diktaturer.

Det är lätt att föreställa sig hur högljudda protesterna skulle vara i väst om Kina lika öppet skulle marknadsföra cyberintrång till samma typ av avnämare.

På statlig nivå händer ingenting, men Facebook-ägda Whatsapp åtalade NSO 2019 för dataintrången i deras krypterade tjänst. Också Reportrar utan gränser (Reporters sans frontières) förbereder åtal mot NSO. ”Pegasus är ett motbjudande verktyg, som tagits fram av digitala legosoldater för att användas av pressfrihetens fiender för att förtrycka journalister”, skriver Erik Halkjær, ordförande för RSF Sverige, i ett pressmeddelande. Och i en kommentar i *Dagens Nyheter* den 21.7 i år konstaterar Erik de la Reguera att avlyssning på entreprenad

> … innebär ökad risk för övergrepp, men också för en ny sorts rovkapitalism: korrumperade regeringar som säljer data och affärshemligheter till högstbjudande, och organiserad brottslighet som får tillträde till människors privata sfär. Behovet av globala regleringar är uppenbart.

Om det är möjligt att väcka frågan om reglering av destruktiva algoritmer i Facebook – som nyligen visselblåsaren Frances Haugen gjort inför kongressen i USA – borde det också vara möjligt att stoppa spridning av cybervapnet Pegasus till förtrycksregimer, om viljan att skydda dissidenter och aktivister finns. Det borde gå att ställa de ansvariga inför rätta och dra ur sladden på NSO.

10.10.2021

Källor bl.a. *The New York Times* 25.8 och 2.9 2016; 4.1, 11.2, 19.6, 10 och 11.7 2017; 20.2, 27.9, 8.10 och 2.12 2018; 21.3, 29.10 och 6.11 2019; 22.1 2020; 15, 17, 18 och 20.7, 28.8 och 13.9 2021; *Dagens Nyheter* 20.7 och 14.12 2020; 26.5, 10 och 19–22.7 2021; *Helsingin Sanomat* 20.6 2017, 3.12 2018 , 23.3, 14.5, 29.10 och 5.11 2019; 22.1, 3.2 och 14.7 2020; 22.1, 18–22.7, 29.7 och 7.10 2021.