Een hackingbusje en bigbrothersoftware: dit zijn de wapens die spionagebedrijf Intellexa aan dictators verkoop

Nikolas Vanhecke Roeland Termote

Jarenlang verkochten Europese bedrijven spionagesoftware aan dictaturen, leggen de Predator Files bloot. De bedrijven verenigden zich in de Intellexa-alliantie. Van massasurveillance tot telefoonhacking: het bondgenootschap had voor elk wat wils. Een overzicht.

Predator: maakt van een telefoon een spion

Dit is het bekendste en meest diepgaande product, gericht tegen telefoons. De Franse poot van de Intellexa-alliantie verkocht Predator onder verschillende namen, waaronder Arrow en Nova. Het gaat altijd om dezelfde spyware, die alle data op een smartphone kan opvissen: bezochte websites, mails, berichten (ook via geëncrypte chats) en zelfs paswoorden. Predator krijgt ook toegang tot de locatie en belgeschiedenis, kan screenshots nemen en de camera en microfoon activeren.

Twee weken geleden bracht Apple nog een update uit van zijn besturingssysteem iOS, na de ontdekking van een nieuwe kwetsbaarheid die Predator gebruikt om binnen te dringen op een telefoon.

Ons onderzoek rond de Predator Files werd gevoerd door vijftien media, gecoördineerd door European Investigative Collaborations (EIC), waar De Standaard deel van uitmaakt. Het is gebaseerd op honderden vertrouwelijke documenten die Mediapart en Der Spiegel verkregen en analyseerden met de hulp van het Security Lab van Amnesty International. ‘Sinds Intellexa weet dat hun Predator-spyware en aanvalscampagnes aan het licht komen, haasten ze zich om de servers voor besmettingen af te sluiten’, zegt Donncha O’Cearbhaill, die leiding geeft aan het Security Lab van Amnesty International. ‘Meer dan 70 procent van de Predator-servers is offline gehaald sinds half september.’ Rond die periode stuurden de leden van EIC lijsten met vragen om commentaar door naar de bedrijven en personen binnen Intellexa.

Alpha Max en het hackingbusje

Ons onderzoek toont hoe de leden van de Intellexa-alliantie in 2019 een ‘zero click’-methode ontwikkelden om de Predator-spyware te injecteren: de zogeheten ‘tactische’ of ‘veld’-besmetting. Die loopt via apparatuur die met radiogolven telefoons binnen een afstand van enkele honderden meters kan aanvallen. ‘SpearHead’ doet dat via WiFi-golven. ‘Alpha Max’ gebruikt gsm-netwerken en werkt via een antenne die de masten van mobiele operatoren imiteert. Wanneer een doelwit in de buurt is, wordt het ‘discreet losgemaakt van het netwerk’. Daarna worden ‘alle vormen van

communicatie opgenomen en bewaard en wordt het doelwit gelokaliseerd', staat in een brochure uit 2019.

Het topwapen van Intellexa is een busje met de naam AlphaSpear 360. Dat is uitgerust met SpearHead én Alpha Max. De prijs: negen miljoen euro voor het busje en de eerste honderd hacks. Intellexa biedt ook een drone aan, de SpearHead Airborne. Die werkt zonder het busje, maar kan alleen besmettingen via WiFi uitvoeren.

Cerebro, de bigbrothersoftware

Tien jaar lang was Cerebro de belangrijkste tool van Nexa, de Franse poot van de Intellexa-alliantie. Het werd verkocht als 'het eerste systeem ter wereld' dat in staat was om internetverkeer af te tappen 'op de schaal van een volledig land'. In 2007 heette het nog Eagle, toen het werd verkocht aan het regime van de Libische kolonel Kadhafi. Vijf jaar later werd het omgedoopt naar Cerebro. Daarmee deelt het de naam van een machine uit de X-Men-strips en -films waarmee een telepathische mutant alle andere mutanten ter wereld kan lokaliseren.

Concreet wordt het internetverkeer van een land of regio volledig opgezogen en dan opgeslagen in Cerebro. Zo maakt de software 'big data' doorzoekbaar. In het begin van Cerebro was een van de belangrijkste functies blootleggen wie met wie communiceert om zo netwerken van personen in kaart te brengen.

Operators kunnen ook zoeken op trefwoorden, doelen identificeren en vervolgens toegang krijgen tot al hun activiteiten, zowel in het verleden als in realtime: e-mails, websiteraadplegingen, activiteit op forums. Cerebro kan zelfs de gebruikersnamen en wachtwoorden vinden die door doelwitten zijn ingevoerd. Daarmee kunnen de Cerebro-gebruikers toegang krijgen tot hun verschillende accounts (Gmail, sociale netwerken, bank, enz.).

Zaakvoerders van Nexa verklaarden tijdens hun verhoren aan Franse speurders dat Cerebro geleidelijk aan zijn relevantie verloor doordat steeds meer online gegevens geëncrypt werden.

Lees ook