Hoe Europese bedrijven spyware leverden aan dictators

Roeland Termote en Nikolas Vanhecke

Vanuit Europa wordt spionageapparatuur over de hele wereld verkocht, ook aan dictators met wie volgens de Europese regels geen handel mag worden gedreven. Dat blijkt uit Predator Files, een onderzoek van De Standaard en zijn partners. ‘Als deze deal uitlekt, zijn we dood.’

Ayman Nour liep in de val door een berichtje op Whatsapp. Op 22 juni 2021 las de Egyptische oppositiepoliticus een bericht met een link naar een nieuwsartikel: ‘Turkije roept Egyptische oppositiezenders op om te stoppen met de kritiek op Egypte.’ Het bericht, onderdeel van een reeks, leek afkomstig van een Egyptische afzender die Nour nooit had ontmoet, maar ongevraagde berichten vond de politicus niet vreemd. Hij werd een beroemdheid in zijn land nadat hij het als eerste presidentskandidaat ooit had durven op te nemen tegen wijlen dictator Hosni Moebarak en prompt in de gevangenis was beland. Na de Arabische Lente en de staatsgreep door huidig Egyptisch leider Abdul Fatah al-Sisi in 2013 vluchtte Nour naar Turkije. Daar runde hij El Sharq TV, een satellietkanaal dat het regime van Al-Sisi op de korrel neemt.

Dat maakte de kop van het nieuwsartikel uiterst relevant voor Nour. Maar de identiteit van de verzender bleek vals. De reeks links was fake. Zodra Nour een van de berichten aanklikte, zette hij de deur open voor spionagesoftware. Vanaf dat moment konden zijn vijanden alles volgen wat door zijn telefoon passeerde.

‘Ik ging er altijd al van uit dat mijn telefoons werden afgeluisterd’, zegt de dissident. Zekerheid had hij niet, tot hij eind 2021 besloot om zijn toestel te laten testen door het Citizen Lab van de Universiteit van Toronto. Dat instituut, gespecialiseerd in cyberspionage, bevestigde Nours vermoedens. Zijn telefoon was besmet met twee spionageprogramma’s. Een van de twee heette Pegasus. Dat programma werd berucht toen de ngo Forbidden Stories en een consortium van journalisten in 2021 lange lijsten lekten van – vaak wereldberoemde – doelwitten en slachtoffers. Het andere programma heette Predator, ‘roofdier’.

Predator is software die diep infiltreert in de telefoons van zijn doelwitten. Veiligheidsdiensten maken er gebruik van om de communicatie van drugsbaronnen, maffiabazen en terroristen te volgen. Om te voorkomen dat dat soort software in verkeerde handen terechtkomt, heeft de EU de verkoop ervan strikt gereglementeerd. Predator werd ontwikkeld in Europa. Ook de financiers en verkopers werkten vanuit de EU. Toch werden ook mensen als Ayman Nour, die niets te maken hebben met criminaliteit, een prooi van Predator. Hoe kan dat?

De Standaard en zijn internationale partners werpen een licht op de duistere wereld van de handel in spionagesoftware. Op basis van vertrouwelijke data die onze partners Mediapart en Der Spiegel

verkregen en deelden met het onderzoekscollectief European Investigative Collaborations (EIC), publiceren we de Predator Files. Dat onderzoek neemt u de volgende dagen mee in de interne keuken van een van de meest ambitieuze spionageprojecten ter wereld: de Intellexa-alliantie.

De Egyptische oppositiepoliticus Ayman Nour werd het slachtoffer van Predator. — © Rhonald Blommestijn

Predator Files toont hoe dit bondgenootschap – opgebouwd rond het Franse bedrijf Nexa en zijn Israëlisch-Europese partners – tot ver buiten Europa zakendeed met dubieuze regimes.

In Frankrijk was Nexa een prestigieuze leverancier van surveillancesoftware voor de inlichtingendienst DGSE en verschillende Franse ministeries. Maar volgens onze informatie waren ook autoritaire staten in Afrika, het Midden-Oosten en Azië klant bij de groep rond Nexa. Ons onderzoek laat zien hoe deze dreiging voor de democratie zich, ondanks strikte Europese regels, verspreidde vanuit het hart van de EU.

Codenaam Toblerone

Negen maanden voor de besmetting van Nours telefoon, in september 2020, maakten werknemers van de Nexa-groep zich op voor een presentatie van hun hackingsoftware bij een Egyptische veiligheidsdienst. In een Whatsappgroep overlegden ze hoe ze hun toekomstige klant, die zelf de telefoons zou meebrengen, helemaal konden overdonderen. ‘We moeten onze demonstratie geven met de telefoons die zij uit de doos halen’, zei een van de werknemers. ‘Als we moeten voorbereiden, verknalt dat het wow-effect.’ Het succes van een aanval met Predator hangt af van het besturingssysteem op de telefoon. Als dat helemaal up-to-date is, bestaat de kans dat de poging mislukt. Ze wilden vermijden dat ze tijdens de demonstratie zouden moeten prutsen met de toestellen.

De zorgen waren onterecht, blijkt uit onze documenten. Op de laatste dag van 2020 stuurde Stéphane Saliès, medeoprichter van Nexa, zijn collega’s een Whatsappbericht met drie champagnefles-emoji’s: het contract met Egypte was getekend. ‘Great!!! Happy New Year’, reageerde zijn Israëlische zakenpartner Tal Dilian. Het was dan nog even wachten op een kopie van het contract, waarschuwde Saliès, ‘want je weet maar nooit met de farao’s’. Maar de Egyptenaren hapten toe en sloten een contract af met Ames, een zusterbedrijf van Nexa in Dubai, voor 9,5 miljoen euro.

Het was niet de eerste keer dat de mannen achter Nexa zakendeden met het regime van de Egyptische dictator Al-Sisi. In 2014 leverden ze een pakket ter waarde van 13 miljoen euro met de naam Cerebro dat in staat is om het telefoon- en internetverkeer van een volledig land te traceren. Ook toen verliep de transactie via de Emiraten.

De verkoop van Cerebro aan Egypte kreeg binnen de groep de codenaam Toblerone. Het lijkt een verwijzing naar de vorm van de piramides. Dossiers de naam van snoepgoed geven was een running joke. De samenwerking met Saudi-Arabië heette Kinder, Oostenrijk werd Pretzel en

Pakistan Pim's.

Het Franse gerecht lachte niet mee. Eind 2017 begon het een onderzoek wegens de verkoop van Cerebro aan het regime van Al-Sisi. De verdenking: 'medeplichtigheid aan marteling'.

Saliès wist dus dat hij zich opnieuw op glad ijs begaf toen hij in 2021 Predator verkocht aan de Egyptenaren. In een telefoongesprek dat werd afgeluisterd door de Franse speurders, waarschuwde hij een collega dat de deal nooit in de media mocht komen. Als dat zou gebeuren, 'zijn we dood', zei Saliès.

Tijdens datzelfde gesprek gaf hij toe dat hij zich ervan bewust was dat zijn klanten 'zo ongeveer alles' konden doen met hun software om telefoons te hacken. 'Kijk naar wat er in Saudi-Arabië is gebeurd, daar hebben ze het toch verprutst, met Bezos en Khashoggi', zei Saliès. Dat was een verwijzing naar de Pegasus-spionagesoftware die werd aangetroffen op de telefoons van de Saudische journalist Jamal Khashoggi, die een column had in The Washington Post, en Jeff Bezos, die behalve techgigant Amazon die krant bezit. Khashoggi werd in Istanbul om het leven gebracht door een Saudisch moordcommando, concludeerde de Amerikaanse inlichtingendienst CIA. De moord zette de schijnwerpers op het gebruik van spyware tegen dissidenten.

'Het kan veel pijn doen', waarschuwde Saliès. Hij had het niet over slachtoffers als Jamal Khashoggi of Ayman Nour, maar wel over de risico's voor zichzelf en zijn bedrijven. 'Eén of twee fouten en je krijgt de boemerang recht in je gezicht.'

Big brother op bestelling

Saliès wist waarover hij sprak. De 59-jarige fysicus, die studeerde in Parijs en Silicon Valley, draaide al jaren mee in de sector van spionagetechnologie. Hij was onder meer manager bij Amesys, de voorloper van Nexa. Dat bedrijf waagde zich in 2007 aan een samenwerking met het regime van de Libische dictator Moammar Kadhafi. Aan kolonel Kadhafi verkochten ze Eagle, de oorspronkelijke versie van Cerebro. Volgens het Franse onderzoeksmedium Reflets waren ook Frankrijk, Guinee, Marokko en Gabon klant bij Amesys.

In 2011 lekte de verkoop aan Kadhafi uit. De ngo's Ligue des Droits Humains (LDH) en Fédération Internationale des Droits Humains (FIDH) dienden in Frankrijk een klacht in tegen het bedrijf. Volgens hen hadden Kadhafi's beulen de surveillancetools ingezet tegen hun bevolking. Het Tribunaal voor Oorlogsmisdaden en Misdaden tegen de Mensheid in Parijs onderzocht Amesys wegens het verlenen van steun aan marteling. Het bedrijf sloot de deuren, maar Saliès kocht de rechten op de technologie. Hij doopte die om tot Cerebro en richtte, samen met verscheidene Amesys-toppers, het bedrijf Nexa op.

Ze breidden hun arsenaal uit. Boven op technologie om internetverkeer te scannen, maakte Nexa apparatuur die satelliettelefoons kan afluisteren en andere vormen van gesproken communicatie kan onderscheppen. En ze ontwikkelden 'Imsi-catchers', 'valse gsm-masten' die elke mobiele telefoon kunnen afluisteren binnen een afstand van een paar honderd meter. Al die systemen

konden op hun beurt verbinding maken met Cerebro, dat de onderschepte informatie combineerde en analyseerde, leert een brochure van Nexa. Zo ontstond een digitale controletoren om ongemerkt de communicatie tussen de burgers van een heel land te overzien.

Geïnteresseerde kopers waren er genoeg. Bij de klanten van Nexa waren volgens interne documenten verscheidene Europese democratieën: Frankrijk, Zwitserland, Oostenrijk en Duitsland. Maar de belofte van big brother op bestelling sloeg ook aan bij regimes met een problematische reputatie inzake democratie of mensenrechten. Europese exportrestricties zijn in principe een grote hinderpaal voor de uitvoer van gevoelige spionagetechnologie naar dat soort landen.

Maar de Fransen hadden een sluiproute ter beschikking, dankzij Nexa's zusterbedrijf Ames. Die firma – die formeel losstond van Nexa, maar zowel dezelfde aandeelhouders als hetzelfde personeel deelde – was gevestigd in Dubai. De bedoeling, volgens Saliès zelf, was de nabijheid voor alle klanten te verzekeren, maar een intern document geeft andere redenen: de vestiging in Dubai elimineerde het 'obstakel' van de Europese regelgeving. In vergelijking met Nexa had Ames in de Verenigde Arabische Emiraten minder last van lange controles en afgewezen uitvoervergunningen bij leveringen aan gevoelige landen.

Het leverde Saliès en zijn kompanen miljoenen op. De troebele moraal van de sector, de juridische tegenslagen en het risico op publieke affronten: Saliès nam het er allemaal bij. In notities die afkomstig lijken van een teambuilding-sessie, omschreef hij zijn drijfveer: rijk worden om 'op een grote boot te zeilen'.

Toen hij later door de politie werd verhoord, verklaarde hij dat hij 25.000 euro per maand verdiende, en met een Porsche Macan en een Mercedes GT reed. Samen zijn die 170.000 euro waard. Ook had hij een huis van 4 miljoen euro in de buurt van Parijs en een villa in Dubai van 1,5 miljoen.

Maar technologische vooruitgang haalde zijn bedrijf in. Cerebro, het topproduct, werd geleidelijk onbruikbaar. De traceersoftware werkte enkel wanneer de onderschepte data niet versleuteld waren. Naarmate het wereldwijde internetverkeer steeds meer geëncrypteerd raakte, verloor de software zijn nut.

De alliantie

Om in de business te blijven, moesten Saliès en co. vernieuwen. Daarvoor kregen ze de hulp van een Israëlische ICT-ondernemer met een lange staat van dienst. Tal Dilian (62) werkte meer dan twintig jaar voor het Israëlische leger. Eerst als paracommando, nadien als baas van de mythische eenheid 81, die gesofisticeerde cyberwapens vervaardigt voor Israëlische soldaten en spionnen. Nadat Dilian de eenheid in 2003 had moeten verlaten na beschuldigingen van verduistering, besloot hij zijn knowhow commercieel in te zetten. In 2014 verdiende Dilian ruim 20 miljoen dollar aan de verkoop van een bedrijf dat software produceerde die de locatie van elke telefoon in

enkele seconden kan achterhalen.

Met een deel van zijn geld kocht hij zich in bij een Europese firma die de eerste versie van Predator zou ontwikkelen. Maar hoe krachtig die spyware ook was, hij had één manco: het doelwit moest nog altijd op een link klikken om besmet te raken – zoals de Egyptenaar Nour deed. Bij de grote rivaal Pegasus, in handen van de Israëlische concurrent NSO, was dat niet nodig. Die was al uitgerust met de heilige graal van de spionagesector: 'zero click'-technologie, die geen actie vereist van het doelwit. Dat is wat dictators het liefste willen.

Door producten uit Dilians arsenaal te combineren met Nexa's eigen gamma aan spyware, slaagden ook zij er uiteindelijk in die technologie aan te bieden. Dankzij Nexa's adresboekje lag een nieuwe markt voor het grijpen. In februari 2019 stuurden Nexa en Dilians spionagegroep een perscommuniqué uit: voortaan maakten ze samen deel uit van de 'Intellexa-alliantie'.

Een intern document toont hoe de alliantie een 'hacking van' ontwierp: een busje waarin de meest geavanceerde technologie van Dilian en Nexa gebundeld zat. Vanuit dat busje is het mogelijk in te breken in alle smartphones die zich in een brede straal rond het voertuig bevinden, zonder dat de eigenaars hun toestel zelfs maar uit hun zak moeten halen.

Eind 2019 toonde Dilian aan het Amerikaanse magazine Forbes hoe dat in zijn werk ging. De guitig kijkende man met grijs haar en stoppelbaard leidde een videoploeg naar een braakliggend terrein op Cyprus, zijn thuishaven op dat moment. Het eiland is een aantrekkelijke plek voor cyberondernemers die pakweg het Midden-Oosten willen bedienen terwijl ze toch kunnen schermen met het label 'voldoet aan de standaarden van de EU'.

De Israëliër toonde de reporters de binnenkant van een zwarte bestelwagen, volgeladen met elektronische apparatuur die volgens Dilian 9 miljoen dollar waard was. Vanuit zijn mobiele controlecentrum, vertelde hij de journalisten geestdriftig, had hij toegang tot 'Whatsappberichten, Facebookchats, tekstberichten, telefoongesprekken en contacten' van 'elke smartphone in een straal van 500 meter'.

Om de technologie te demonstreren, stuurde hij twee medewerkers uit op een wandeling. Zij deden zich voor als doelwitten. 'We zullen hen opsporen, [hun telefoon] onderscheppen en besmetten', aldus Dilian in het filmpje. Hij zoomde in op een van zijn medewerkers die zich enkele honderden meters verder bevond, met een Huawei-telefoon in de hand. Op Dilians monitor sprong een licht van groen op rood. Met behulp van de wifi-onderscheppers kreeg hij ongemerkt toegang tot het toestel. De foto's, berichten en privédata van de Huawei-gebruiker verschenen op de schermen in zijn bestelwagen. Dilian glunderde.

De Cypriotische overheid kon de mediastunt niet smaken. Ze liet de bestelwagen in beslag nemen. Het onderzoek eindigde twee jaar later met een boete van een miljoen dollar. Voor Dilian was het geen aderlating. Aan Forbes vertelde hij dat hij droomde van verkoopcijfers tot 500 miljoen euro.

De 'goeie jongens'

De Israëlische cyberondernemer verliet Cyprus en richtte nieuwe bedrijven op in Ierland en Griekenland. Daar haalde hij zich in 2022 nog veel meer ongewenste aandacht op de hals.

In de zomer van dat jaar kreeg de Griekse regering van premier Kyriakos Mitsotakis het benauwd. Nikos Androulakis, de leider van de sociaaldemocratische oppositiepartij Pasok, bleek het doelwit te zijn geweest van een hackingpoging met de Predator-spyware. De onthulling volgde op het nieuws dat een Griekse journalist, die schreef over corruptie in de elite, daadwerkelijk gehackt werd. Nog later bracht de Griekse krant Documento een lijst naar buiten van hooggeplaatste personen die gesurveilleerd werden door de inlichtingendiensten of een doelwit waren van Predator. Op het lijstje stonden ook rivalen van de centrumrechtse Mitsotakis binnen zijn eigen partij.

De Griekse premier Kyriakos Mitsotakis en Nikos Androulakis (rechts), leider van de sociaaldemocratische oppositiepartij Pasok. — © Rhonald Blommestijn

De premier had, meteen na zijn verkiezingsoverwinning in 2019, de inlichtingendiensten onder controle van zijn kabinet geplaatst. De kabinetsmedewerker belast met die operatie? De neef van premier Mitsotakis. Toen ook nog eens bleek dat de inlichtingendiensten bij zowel de gehackte journalist als de oppositieleider een telefoontap hadden geplaatst, moesten de chef van de inlichtingendienst en de neef van Mitsotakis opstappen. Het afluisteren van een oppositieleider ‘was verkeerd’, gaf Mitsotakis toe. ‘Ik wist er niet van en ik zou het natuurlijk nooit hebben toegestaan.’ De premier spartelde door de crisis. In juni werd hij verkozen voor een tweede ambtstermijn.

De verschillende onderzoeken naar de zaak lopen nog. In december 2022 vielen speurders de Griekse kantoren van Dilians bedrijf binnen. Ook al zijn er talloze aanwijzingen van de inzet van de Predator-spyware, officieel blijven de Griekse autoriteiten ontkennen dat ze die ooit hebben aangekocht.

Tegenover de Forbes-journalisten beweerde Dilian dat hij selectief omspringt met zijn klanten. ‘We werken alleen met de goeie jongens. Maar soms gedragen de goeie jongens zich niet goed.’ Daar kan hij niets aan doen, vindt hij. ‘Wij zijn niet de politiemannen of rechters van deze wereld.’

Maar wie zijn in de wereld van Dilian de ‘goeie jongens’? De Grieken? De geheim agenten van de Egyptische dictator Al-Sisi? Of zelfs de milities van de Libische veldmaarschalk Khalifa Haftar?

Zelf afgeluisterd

Op 21 mei 2021 belde Stéphane Saliès, samen met Dilian een steunpilaar van de Intellexa-alliantie, zijn Duitse bedrijfsadvocaat. Hij had een dringend probleem. ‘We hebben een aanvraag uit een superslecht land’, zei Saliès. Hij wilde van zijn advocaat weten of hightech spionageapparatuur leveren aan het leger van de Libische Haftar ‘compleet verboden was’ en of er misschien toch iets te regelen viel.

Haftar zwaait de plak in het oosten van het door burgeroorlog verscheurde land. De internationale

gemeenschap erkent zijn bewind niet, mensenrechtenverenigingen beschuldigen zijn bewind van oorlogsmisdaden. Sinds 2011 geldt er ook een wapenembargo tegen Libië, goedgekeurd door de VN-Veiligheidsraad. Het antwoord op Saliès' vraag moest dus duidelijk zijn. 'Je weet dat we geen zaken doen met landen waartegen een wapenembargo van kracht is', zei zijn advocaat. Toch wilde Saliès doorzetten met de levering. Waarom enkele miljoenen laten liggen?

In een rapport van 41 pagina's hadden de Fransen de mannen van Haftar warm proberen te maken voor hun topproduct: de AlphaSpear 360, de bestelwagen waarmee Dilian pronkte tegen de Forbes-reporters. Haftar leek de bestelwagen niet nodig te hebben en koos voor een bescheidener winkelmandje: hij had 3,3 miljoen veil voor geavanceerde afluistersystemen voor mobiele telefoons en satelliettelefoons. Eind 2020 ondertekende het Haftar-regime de verkoopovereenkomst.

Om de bestelde goederen tot bij de klant te krijgen, was een exportvergunning nodig. Maar welk land zou groen licht geven voor de levering van spionageapparatuur aan een warlord die onder een VN-wapenembargo valt?

Stéphane Saliès (links) en Tal Dilian. — © DS collage

Saliès en zijn advocaat bedachten een plan. De oplossing lag opnieuw bij Nexa's zusterbedrijf Ames in Dubai. Door apparatuur voor Haftar langs het Verenigd Koninkrijk en Dubai naar Libië te verschepen, hoopte Saliès te vermijden exportlicenties aan te moeten vragen in landen die daar moeilijk over zouden doen.

Wat Saliès niet wist, was dat hij intussen zelf werd afgeluisterd – door het Franse gerecht. Drie weken na het dringende telefoontje met zijn advocaat vielen speurders bij hem binnen en werd hij gearresteerd. Tijdens zijn verhoor verklaarde hij dat de apparatuur voor Haftar 'in een hangar' in Dubai stond te wachten op de juiste exportlicenties.

Naar eigen zeggen zou hij nooit leveren zonder exportvergunning. De Franse gendarmes hechtten er weinig geloof aan. 'De verkoop gebeurde onder een embargo, door langs verschillende landen te passeren, om zo te ontsnappen aan de beperkingen', staat in hun verslag.

'Vrede zij met u'

Voor Nexa lijken de laatste onderzoeken het schandaal te veel. De zaakvoerders herdoopten het bedrijf tot RB42. Maar er is nog meer veranderd. 'Na meer dan tien jaar in de bestrijding van misdaad in Frankrijk en de rest van de wereld,' aldus het bedrijf, 'zal het zich louter toeleggen op cyberdefensie.' Afgelopen met de aanvallende hackingtechnologieën, dus.

Maar is de breuk met het verleden werkelijk wat ze lijkt? Onderzoek in de Emiraten wijst op tekenen van leven bij Ames, het zusterbedrijf dat gebruikt werd als tussenschakel voor gevoelige deals. De firma vernieuwde er onlangs haar exportlicentie.

De Israëlische betrokkenen worden in Europa of Israël op geen enkele manier juridisch aangepakt. Dat is anders in de Verenigde Staten. Het Amerikaanse ministerie van Handel plaatste

verschillende bedrijven waarin Dilian betrokken was op een zwarte lijst wegens hun negatieve impact op internationale mensenrechten.

Hoeveel indruk het maakt op Dilian, is onduidelijk. In de gespecialiseerde pers over de inlichtingenindustrie verscheen in januari 2023 een stuk dat suggereert dat hij op het punt staat een nieuw superbedrijf op te richten in Tel Aviv.

We willen hem confronteren met onze bevindingen. Daarvoor trekken EIC-reporters naar een dorpje in de Zwitserse Alpen ten zuiden van het meer van Genève, waar Dilian en zijn vrouw een chalet bezitten. Aanbellen levert niets op, maar op tegeltjes naast de voordeur hebben 'Tal' en zijn vrouw een bijbelvers achtergelaten voor elke bezoeker: 'Vrede zij met u. Vrede zij met uw huis en al wat je hebt.'

De boodschap zal de Predator-slachtoffers cynisch in de oren klinken. Nog geen twee weken geleden raakte bekend dat de Egyptische politicus Ahmed Eltantawy doelwit werd van de spyware, vlak nadat hij had aangekondigd kandidaat te zijn in de presidentsverkiezingen van volgend jaar. Hij kreeg kwaadaardige links doorgestuurd, via Whatsapp.

Reactie

EIC heeft de managers van de Intellexa-bedrijven gecontacteerd met een uitgebreide reeks vragen om commentaar. Tal Dilian reageerde in het geheel niet.

De zaakvoerders achter het Franse Nexa lieten via hun advocaat weten dat ze 'het ethische dilemma dat onze activiteiten met zich meebrengen nooit hebben onderschat'. 'We waren ons ervan bewust dat sommige landen waaraan we verkochten inzake de rechtsstaat verre van perfect waren. Maar we waren ons er ook van bewust dat onze aanpak deel uitmaakte van de impuls van de internationale gemeenschap om deze landen richting democratie te sturen.'

Ze zeggen dat ze de regels altijd hebben gerespecteerd en dat ze Predator-contracten hebben opgezegd vooraleer die operationeel waren. Dat was wel pas na de huiszoekingen van 2021. 'Die wezen ons op de risico's rond dit soort deals. We beseften dat onze vergunningen ons niet voldoende beschermden en geen garantie boden tegen inbreuken op de mensenrechten.'

Ames, het zusterbedrijf in Dubai waarlangs wapenleveringen liepen, is volgens zijn eigenaars nog amper actief. Ze verwachten het de komende maanden helemaal te sluiten.