Hackingaanval op de EU heeft Vietnamese vingerafdrukken

Roeland Termote en Nikolas Vanhecke in samenwerking met EIC

Europees parlementsvoorzitter Roberta Metsola, hoge EU-ambtenaren en Amerikaanse politici: allemaal belandden ze in het sleepnet van een hackingoperatie. Onderzoek naar de herkomst van de aanval wijst naar Vietnam, maar de oorsprong van de spyware is Europees.

'Hoe ernstig neemt de wereld Peking nog, nu meer landen zich verzetten tegen China?' Op 1 juni zocht een zekere @Joseph_Gordon16 op X (het voormalige Twitter) de aandacht van Roberta Metsola, de voorzitter van het Europees Parlement.

De X-post van 'Joseph Gordon' aan Metsola bevatte, naast een prikkelende vraag over de mondiale invloed van het Chinese regime, ook een link. Die leek sterk op het webadres van de Hongkongse krant South China Morning Post, maar leidde in werkelijkheid naar een website die bezoekers kan besmetten met spyware. Predator, de hackingsoftware achter de website, heeft aan één klik genoeg om alle data op te zuigen op het toestel van zijn prooi.

Metsola was niet het enige doelwit van de hackers. Diezelfde dag kreeg ook de Europese Commissie de link toegestuurd. In de maanden voordien probeerde 'Joseph Gordon' al om de Belgische directeur-generaal voor Klimaatactie bij de Commissie, Kurt Vandenberghe, in de val te lokken. Net als zijn Bulgaarse collega belast met Maritieme Zaken, Charlina Vitcheva.

Ook een reeks agentschappen verbonden aan de Commissie kregen een bericht van Gordon. Zoals het Oostendse European Marine Observation and Data Network (EMODnet), dat mariene data vergaart. Of het European Research Executive Agency, geleid door de Belg Marc Tachelet.

Ongewone tactiek

In totaal probeerde het malafide X-account zeker vijftig personen of organisaties naar een Predator-site te lokken, steeds volgens dezelfde modus operandi. Dat blijkt uit onderzoek van Amnesty International en de Predator Files, een project van het journalistieke collectief EIC, waar De Standaard deel van uitmaakt. Dankzij vertrouwelijke documenten die Mediapart en Der Spiegel in handen kregen en deelden met EIC, konden we de interne keuken blootleggen van Europese spyware-leveranciers met een wereldwijd klantenbestand.

Het bericht aan Roberta Metsola, met de malafide link — © Amnesty

Ook de Threat Analysis Group van IT-gigant Google onderzocht de berichten die het Joseph Gordon-profiel de wereld instuurde. Zij bevestigden dat de meegezonden url's toebehoren aan het spyware-systeem Predator. Behalve EU-ambtenaren werden ook vier Amerikaanse

volksvertegenwoordigers, de Taiwanese president Tsai Ing-Wen, CNN-reporters en de Duitse ambassadeur in Washington blootgesteld aan malafide berichten.

Opvallend is dat veel van die berichten in de publieke X-tijdslijn belandden van mensen en instellingen met honderdduizenden volgers. Dat is een ongewone tactiek, want zowel onnauwkeurig als makkelijk detecteerbaar.

Wie is 'Joseph Gordon'?

Maar wie is 'Joseph Gordon'? Op zijn pagina op de socialenetwerksite, die intussen niet meer bestaat, ziet de verzender van de berichten eruit als een jonge Aziaat. Als profielfoto gebruikt hij een spiegelselfie. De achtergrondfoto is die van de skyline van Singapore. Dat is ook de locatie die hij opgeeft.

Informatie uit het Predator Files-onderzoek wijst erop dat achter het account 'Joseph Gordon' de hand van het Vietnamese ministerie van Publieke Veiligheid schuilde.

Documenten die De Standaard kon inzien tonen dat Ames, het zusterbedrijf van de Franse spionagegigant Nexa die de Predator-spyware als zijn topproduct verkocht, werkte aan de verkoop van een hackingsysteem voor 'MOPS'. Die afkorting wordt gebruikt voor het Vietnamese ministerie van Publieke Veiligheid, dat optreedt als de sterke arm van het repressieve regime in Hanoi. In de 'finale versie' van een verkoopsovereenkomst voor Vietnam, uit februari 2021, staat dat die deal moet verlopen via een bedrijf in Hongkong.

Exportpapieren verkregen door EIC en Amnesty International geven aan dat hetzelfde Hongkongse bedrijf in november 2021 per vliegtuig computerhardware bezorgde aan een staatsbedrijf in Vietnam, dat goederen importeert voor het Ministerie van Publieke Veiligheid. Tussen de goederen zit onder meer een 'mobiele smartphonemonitoring-module'. De producent van de goederen krijgt op de exportpapieren de code 'AS', die de bewindvoerders achter Predator-verkoper Ames ook intern gebruiken om hun bedrijf mee aan te duiden.

De documenten bevatten nog meer veelzeggende aanwijzingen. Het Vietnamese spyware-contract kreeg de naam 'Anglerfish': 'diepzeehengelvis'. Dat lijkt geen toeval. De Europese doelwitten van de hackers waren in de weer met mariene dossiers die ook voor de Vietnamese regering van het grootste belang waren.

Visexport

Tussen de EU en Vietnam heerst al een paar jaar een conflict over illegale visserij. De Commissie vindt dat het land te weinig doet om die praktijk te bestrijden, die de maritieme ecosystemen in de Stille Oceaan bedreigt. Daarom deelde Europa in 2017 een 'gele kaart' uit aan Vietnam. Dat is een opstapje naar een 'rode kaart', die de visexport uit het land zou stilleggen. Daarmee had Hanoi een sterk motief om te achterhalen wat zich afspeelt in de Europese machtscentra die beslissen over het visserijbeleid.

Amnesty-onderzoekers besluiten dat de 'Joseph Gordon'-hackingcampagne waarschijnlijk uitgevoerd werd door 'agenten van de Vietnamese autoriteiten'. Onafhankelijk onderzoek van het gerenommeerde Citizen Lab van de Universiteit van Toronto en de Threat Analysis Group van internetgigant Google ondersteunt die conclusie. 'Wij geloven dat deze Predator-aanvalsinfrastuctuur gelinkt is aan een overheidsactor in Vietnam', verklaarde Google aan EIC.

De regering van Vietnam antwoordde niet op onze vragen over de kwestie, net zo min als Intellexa, het bedrijf dat de Predator-spyware ontwikkelde in Europa. De Franse bewindslui achter Nexa en Ames, die Predator verkochten als partner van Intellexa, verklaarden tegenover EIC dat ze zich altijd aan de regels rond de uitvoer van spyware hebben gehouden.

Bovendien zeggen ze dat ze afstand gedaan hebben van al hun Predator-contracten vanaf het 'derde kwartaal van 2021', voor ze dus operationeel werden. Die zouden ze overgedragen hebben aan hun voormalige partners bij Intellexa. Op die manier nemen de Fransen ook afstand van de aanvallen op de EU-bewindslui.

De misstanden met Predator die nu aan het oppervlak komen, lijken wel voor paniek te zorgen. 'Sinds midden-september werd meer dan 70 procent van de Predator-servers die we traceerden offline gehaald', zegt Donncha O' Cearbhaill, de directeur van het Security Lab van Amnesty.

De Europese Commissie zegt dat ze weet heeft van de berichten over Predator-aanvallen tegen volgers van Europese organisaties. 'We onderzoeken elk incident', zegt een woordvoerder. 'Op dit moment heeft de Commissie geen aanwijzingen van een succesvolle besmetting en is er geen impact waar te nemen.'

Berlijnse dissident aangevallen

De hackers wierpen hun sleepnet nog breder. Naast leden van de Europese elite bleken Amerikaanse politici en journalisten interessant voor de hackers, om onduidelijke redenen. Wel helder is waarom ook een Vietnamees met een winkeltje voor bewakingsapparatuur in Berlijn interessant kon zijn voor Joseph Gordon.

Khoa Le Trung is een staatsvijand van het autoritaire regime in Hanoi. Vanuit een Aziatische markthal in de Duitse hoofdstad runt de Vietnamese dissident een internetportaal voor landgenoten die op zoek zijn naar kritische feiten over hun regering. Le's website vergaart miljoenen clicks en onthult misstanden, zoals de poging tot kidnapping van een Vietnamese ex-politicus in Berlijn. In Vietnam is zijn portaal geblokkeerd, maar de macht van Hanoi reikt veel verder.

Ook in Berlijn ontvangt de dissident geregeld doodsbedreigingen. 'Vooral van Vietnamezen in Duitsland', zegt hij tegen Amnesty. 'Ze dreigen mijn hoofd af te snijden als ik zo verder doe. Telkens wanneer ik ergens heen ga, moet ik nadenken of dat zinvol is. Ik moet het ook altijd doorgeven aan de politie.'

Zijn bedreigers komen soms tot in zijn winkeltje, waar hij ook zijn piepkleine opnamestudio

geïnstalleerd heeft. Vandaag wordt zijn zaak beschermd door een kogelvrije deur.

Maar spyware-links kan zo'n gepantserde deur niet stoppen. Waakzaamheid wel. Op 9 februari kreeg Le van 'Joseph Gordon' een link die op een nieuwsbericht leek. Hij klikte er niet op, want hij volgt al jaren strikte regels. 'Ik zeg ook tegen al mijn medewerkers dat ze nooit op verdachte links mogen klikken', zegt Le. 'Voor de communicatie met mijn bronnen en aanhangers gebruik ik code. Als de Vietnamese staat de inhoud van mijn gsm zou kunnen lezen, zou dat levensbedreigend zijn voor mijn medewerkers en mijn contacten.'

Net als de EU-ambtenaren zegt ook Le deze dans ontsprongen te zijn. De aanval was klungelig, vindt Citizen Lab-onderzoeker John Scott-Railton, die talloze gelijkaardige gevallen onderzocht. Maar de pogingen waren ook schokkend publiek. 'Iemand zal hiervoor ontslagen worden. Een Predator-klant is momenteel duidelijk aan het ondervinden dat Twitter uitbuiten een vreselijk idee is. Maar het feit dat dit gebeurt, toont dat Predator nog steeds naar roekeloze actoren gaat.'

Lees ook