Voor De Correspondent volgt technologiespecialist Chris van 't Hof de ethische hacker 0xDUDE. Hoe maakte hij het internet veiliger?

Dimitri Tokmetzis
Correspondent Veiligheidsindustrie

Portret

06.01.2017 • *Leestijd 7 - 9 minuten*

Victor Gevers, alias 0xDUDE, nam afgelopen jaar een sabbatical om lekken op het internet op te sporen en te melden. Zijn oogst in een jaar tijd: 690 serieuze lekken bij 590 organisaties in 71 landen. Een terugblik op een jaar lang ethisch hacken.

Deze hacker nam een jaar vrij om het internet veiliger te maken. Dit is zijn oogst

Gastcorrespondent
Helpende hackers

Illustraties: Rob van Barneveld (voor De Correspondent)

Je zou kunnen zeggen dat 0xDUDE een helpende hacker is, maar feitelijk hackt hij niet: hij speurt online naar databases die openstaan, oordeelt of daar gevoelige gegevens in staan en probeert via de eigenaar van de site de database weer dicht te laten zetten.

In 2016 vond hij in totaal 690 serieuze lekken bij 590 organisaties in 71 landen. Die heeft hij allemaal gemeld, waarna het grootste deel werd opgelost.

Makkelijk was het jaar voor 0xDUDE allerminst. Hij werd niet betaald voor zijn werk en het aantal uur dat hij in het project besloot te stoppen, is ontzagwekkend.
Illustratief voor zijn vastberadenheid, is het feit dat we elkaar voor

onze maandelijkse update zelfs een keer ontmoetten in een ziekenhuis, omdat zijn vrouw zou worden geopereerd. Gevers bleef zoveel mogelijk bij haar, maar hield zijn laptop op schoot om door te kunnen werken. Hij wilde niet afwijken van zijn oorspronkelijke voornemen: alle 366 dagen 15 uur per dag besteden aan het opsporen en oplossen van lekken.

Lekken melden

Het aantal door oxDUDE gevonden lekken moet in perspectief worden geplaatst, want het ene lek is het andere niet. Soms is er sprake van een vergeten database die openstaat en die na een kort mailtje weer wordt dichtgezet, terwijl het in andere gevallen structurele lekken betreft die betrekking hebben op veel meer websites.

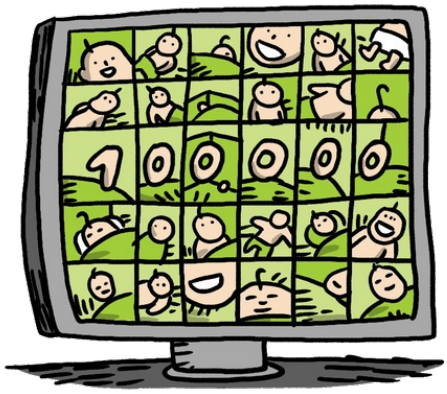
Het ene lek is bij een klein bedrijfje aan de andere kant van de wereld en het andere bij een overheidsorganisatie of multinational die grote hoeveelheden persoonlijke gegevens verwerkt.

Het waarschijnlijk grootste lek dat door oxDUDE werd gevonden, betrof een Chinees telecombedrijf. Hij vond daar een open register met een overzicht van alle abonnees. oxDUDE: ‘Er stonden ontzettend veel abonnees in met hun naam, nummer en adres, terwijl je er zo toegang tot kon krijgen met volledige admin rechten, wat betekent dat ik of iemand anders de data ook aan had kunnen passen.’

Een ander omvangrijk lek had betrekking op een bedrijf dat de gegevens beheert van het grootste deel van de Amerikaanse bloedbanken. oxDUDE schat dat zij 40 procent van alle donoren in

de VS verwerken.

Al hun gegevens stonden open en bloot online. Totdat hij er melding van maakte. Nog een opmerkelijke vondst waren honderdduizenden babycams die onbeveiligd online stonden, waardoor de beelden voor iedereen toegankelijk waren.



Wat doe je als je een lek vindt?
Melden. Maar bij wie? Dat blijkt elke keer weer lastig te bepalen. Soms heeft een website een duidelijke eigenaar waarvan contactgegevens zijn te achterhalen, maar meestal is dat niet het geval.

En wat te doen als een enorme hoeveelheid via internet te benaderen apparaten verkeerd zijn ingesteld door hun gebruikers, zodat ze data lekken of kunnen worden ingezet voor grootschalige DDoS aanvallen? Dan neemt 0xDUDE contact op met de fabrikant of verkoper van het apparaat, om via hen alle meldingen door te sturen naar een hostingprovider die veel van deze apparaten in zijn netwerk heeft. Of hij geeft het probleem door aan een landelijk CERT (Computer Emergency Response Team).

De reacties

Bulkmeldingen telt 0xDUDE als één afgehandeld lek. Zo bezien is 690 een indrukwekkende oogst. In 334 gevallen kreeg 0xDUDE na zijn melding ook een reactie met een bevestiging van het lek, vaak voorzien van een bedankje en het goede nieuws dat het lek inmiddels was gedicht.

Een terugkoppeling van 48 procent is in mijn ervaring met helpende

hackers behoorlijk hoog. Bovendien was dat de stand op 3 januari, toen de 34 meldingen die hij in de laatste dagen van het jaar deed wellicht nog bij de verantwoordelijken terecht moesten komen.

Het is dus waarschijnlijk dat de teller nog oploopt. Ook voor het aantal opgeloste lekken, dat nu al opvallend hoog is: 539 van de 690 gevonden lekken zijn gedicht, een percentage van 78 procent.

Hoe verklaart 0xDUDE het grote aantal organisaties dat het lek wel dicht, maar een reactie achterwege laat? Hadden hun oplossingen niets met zijn meldingen te maken? Dat is onwaarschijnlijk. Vaak ziet 0xDUDE in zijn scans dat het lek al aardig oud is en na zijn melding plotseling wordt gedicht.

De verklaring is dat organisaties beducht zijn voor aansprakelijkheid.
Als zij toegeven data te hebben gelekt, zou iemand daar aangifte van kunnen doen. Sinds 1 januari 2016 kan het lekken van data namelijk worden beboet door de Autoriteit Persoonsgegevens.

Ook kunnen organisaties bang zijn om het vertrouwen van klanten of zakenpartners te verliezen. Daarom zijn er veel hackers die lekken niet melden maar ze direct delen op hackersfora. Of ze richten zich op betaald werk. Zo niet 0xDUDE.

Campagne voeren

Naast het melden van lekken, trad 0xDUDE afgelopen jaar ook regelmatig naar buiten met zijn verhaal. Waar de ooit zo verlegen Gevers eerder achter de schermen werkte, ging hij in 2016 op tournee.

Hij bezocht hackerspaces, congressen, bedrijven en veel overheidsorganisaties - niet alleen in Nederland, maar ook in Hongarije, de VS en Senegal. Hij ging langs bij verschillende landelijke CERTs van overheden en SOCs (Security Operations Centers) van grote IT-bedrijven. Overal was zijn boodschap: deze bronnen met gevoelige gegevens staan open, doe ze dicht.

Een keer, tijdens een meeting van het Global Forum on Cyber Expertise in Boedapest, zag ik hoe 0xDUDE tijdens het ontbijt in het hotel al druk op zijn laptop zat te werken, terwijl de andere congresgasten nog slaperig in hun kopjes staarden.

Tijdens zijn presentatie die middag, begreep ik waarom. 'Kijk, dit is de kassa van ons hotel,' zei hij, waarop sommige bezoekers wellicht werden herinnerd aan wat ze de avond daarvoor hadden gedronken en gedaan. Gelukkig kon hij ook melden dat het lek inmiddels was gedicht.

Daarna toonde hij wat pagina's met getallen en Hongaarse teksten: 'Is er iemand die weet wat dit kan zijn?' Na wat rumoer werd er vanuit de zaal geroepen: 'Dat zijn de recepten voor medicijnen van een groot bedrijf naast het hotel…' Waarop een vertegenwoordiger van een CERT vroeg: 'Hoe heb je ze gehackt? Gebruik je brute forcing?' 0xDUDE: 'Nee, de database stond gewoon open, maar ik heb ze vanmorgen gewaarschuwd en inmiddels is deze gedicht.'

Tijdens de pauze stonden CERTs van verschillende landen in de rij om met hem te praten. 'Dat is belangrijk,' vertelt hij me later. 'Nu kan ik veel van mijn meldingen voortaan bij hen kwijt.'

Tijdens meer besloten bijeenkomsten kan hij verder gaan. Dan laat hij bijvoorbeeld zien welke sites zijn gehackt door activisten,

jihadisten of cybercriminelen, of hoeveel er op het Dark Web wordt geboden voor onze persoonlijke gegevens.

Wat ook goed werkt is het tonen van een lijst met wachtwoorden, die vermoedelijk van mensen in de zaal zijn. Uiteraard zonder gebruikersnamen of site erbij, want anders brengt hij hen in gevaar. Voor degenen die hun wachtwoord herkennen is de boodschap duidelijk: hun online identiteit is niet veilig. Zo'n lijst laat tevens zien hoe simpel wachtwoorden vaak zijn, zoals het bekende 12345, maar ook p@ssword of Ajax 01.

Tegenslagen

Naast zichzelf, heeft Gevers ook een vrouw en drie kinderen te onderhouden. Zij zien zijn reddingsacties met lede ogen aan. Niet in de minste plaats omdat hij niet betaald wordt voor zijn werk.

Het ging op zich goed tot oktober, maar toen was zijn geld op. Een sponsoractie via de door hem en zijn collega Vincent Toms opgezette stichting Global Defense of the Internet (GDI) had wel wat zakgeld opgeleverd, maar niet genoeg om zijn gezin te onderhouden.

En naast vijftien uur per dag lekken vinden en melden, blijft er niet veel tijd over voor een betaalde klus.

Bovendien had Gevers de ambitie om vanuit GDI een online platform te bouwen waar hij en Toms al hun kennis en kunde zouden kunnen delen, Open Source Intelligence (OSINT) in hackersjargon. Daarvoor moesten ze de boer op.

Dieptepunt was 13 november. Om financiering binnen te halen, had Gevers het OSINT platform net bij het SIDN fonds gepitcht. Hij kwam bij de laatste acht en moest het resultaat afwachten. Toen hij die avond naar huis reisde, kreeg hij een telefoontje van een Amerikaans bedrijf. Voor de komende vijf jaar wilden zij voorzien in

een ruim inkomen voor Gevers en zijn gezin, met een totaal van 500.000 dollar. Ze stelden echter ook een onoverkomelijke voorwaarde: stoppen met het melden van zijn lekken.

Dit was niet de eerste keer dat Gevers een dergelijk voorstel kreeg, maar door gebrek aan geld werd hij nu nog harder met de gevolgen van zijn eigen principes geconfronteerd. U kunt zich de reacties in huize Gevers wellicht voorstellen.

Om lucht te geven aan zijn frustratie citeert @0xDUDE het aanbod de volgende dag op Twitter: "If you stop your plans to create a free threat intelligence platform w correlated OSINT events you & @GDI_FDN be handsomely compensated." Maar niet dus.

Hulptroepen

Immaterieel was er wel veel bijval. SURFnet, de organisatie die de IT verzorgt voor het Nederlands hoger onderwijs, had GDI in januari al de SURF Award uitgereikt en daarmee 2500 euro geschonken. Bovendien zouden Gevers en Toms hun OSINT platform op de servers van SURFnet mogen hosten.

In september wonnen ze ook de Digital Impact Award, wat breed werd uitgemeten in NRC Handelsblad. En er waren veel hackers die Gevers bijstonden, door mee te helpen met het melden en afhandelen van lekken.

Verder trad Gevers op 30 november samen met de hackers van Zerocopter op in een aflevering van Zembla: Hacken voor dummies. Daarin lieten ze samen met de journalisten zien waar er beveiligingscamera's en opslagschijven onbeveiligd online

staan, zodat de beelden en de data daarvan in principe voor iedereen toegankelijk is. Het dichten van de lekken handelde Gevers af.

Ook betrokken de WICS (Women in Cybersecurity) hem bij hun onthullingen over kwetsbaarheden in ziekenhuizen, die resulteerden in een kritisch stuk in Trouw en Kamervragen aan de Minister van Justitie.

Al met al heeft Gevers in 2016 in totaal meer dan 5.000 uur besteedt aan het vinden en melden van datalekken - een gemiddelde van 15 uur per dag. Hiermee heeft hij zijn voornemen op zich volbracht. Wel hield hij steeds minder tijd over om het OSINT platform op te zetten, omdat hij in oktober door geldgebrek weer aan het werk moest.

Toen ik hem daarover sprak, rond half november, was zijn antwoord strijdlustig: ‘De 366 wedstrijd is verloren, maar de oorlog niet. Volgend jaar kom ik terug en dan neem ik mijn vrienden mee.’

Met dat voornemen in het achterhoofd ontvangt hij in de laatste dagen van het jaar goed nieuws: op 22 december honoreert het SIDN Fonds zijn voorstel, wat betekent dat GDI 75.000 euro krijgt om het OSINT platform te bouwen. En ook andere geldschieters lijken eindelijk over de brug te komen.

Hoeveel internetgebruikers 0xDUDE in 2016 heeft beschermd, met zijn voorlichtingscampagne en 539 gedichte lekken, is onmogelijk in te schatten. Hetzelfde geldt voor het effect van de meer dan 4.512 meldingen die hij in de zestien voorafgaande jaren heeft gedaan. Zonder twijfel gaat het om de persoonlijke gegevens van vele miljoenen mensen; doodgewone internetgebruikers die waarschijnlijk nog nooit van Gevers hebben gehoord.

Meer lezen?

Je las de pdf-versie van dit verhaal. Voor het volledige artikel met links, infocards, eventuele videos en ledenbijdragen, ga naar:
https://decorrespondent.nl/5964/deze-hacker-nam-een-jaar-vrij-om-het-internet-veiliger-te-maken-dit-is-zijn-oogst/1445174246208-333961bf

De Correspondent is een dagelijks, advertentievrij medium met als belangrijkste doelstelling om de wereld van meer context te voorzien. Door het nieuws in een breder perspectief of in een ander licht te plaatsen, willen wij het begrip 'actualiteit' herdefiniëren: niet om je aandacht te trekken, maar om je inzicht te bieden in hoe de wereld werkt.

decorrespondent.nl

Alle verhalen lezen? Dat kan voor €6 per maand op: decorrespondent.nl