de Correspondent

Voor De Correspondent volgt technologiespecialist Chris van 't Hof de ethische hacker 0xDUDE. Waarom wil die het internet veiliger maken?

Dimitri Tokmetzis
Correspondent Veiligheidsindustrie

Portret

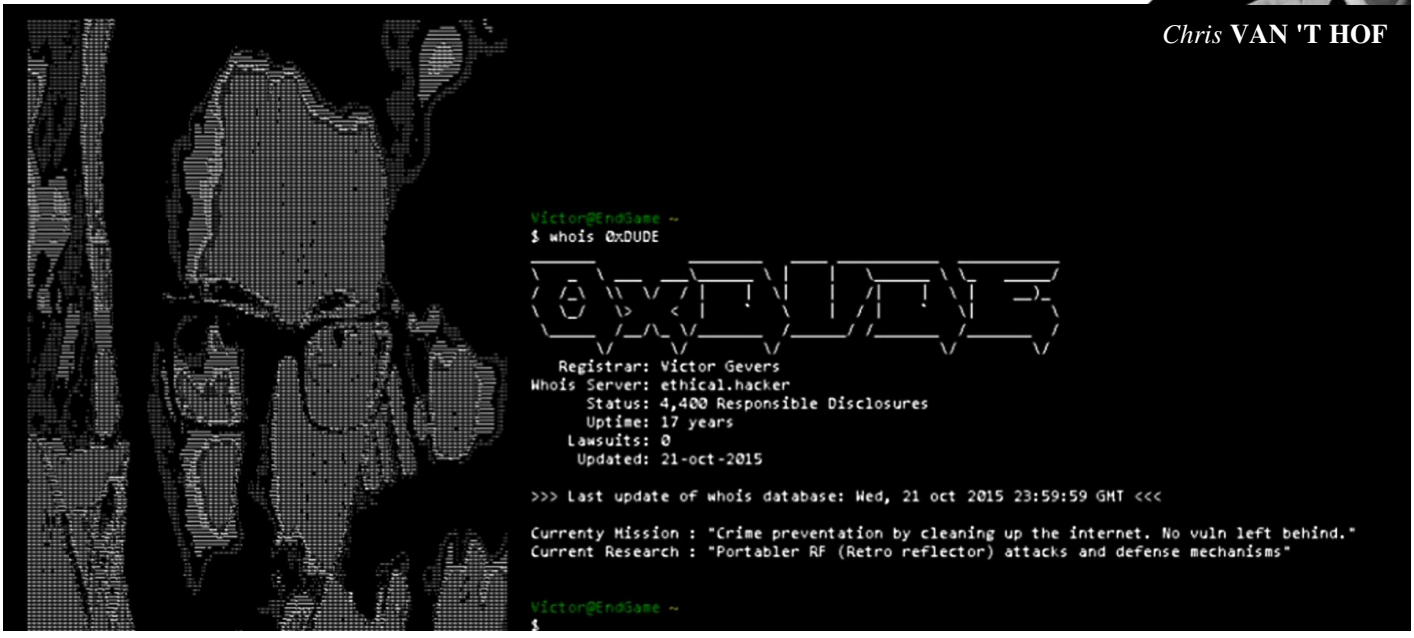
12.04.2016 • *Leestijd 6 - 7 minuten*

Maak kennis met 0xDUDE. Dit hele jaar speurt hij vijftien uur per dag het internet af om kwetsbaarheden in websites te vinden. Wat drijft deze ethische hacker? Begin van een portretreeks.

Deze hacker heeft waarschijnlijk ook jouw gegevens gered

Gastcorrespondent
Helpende hackers

Chris **VAN 'T HOF**



Een man met een zwarte baard zit half in het duister naar drie beeldschermen te kijken. Het is 1 januari 2016 en opeens gaan de zwaailichten aan: de hacksabbatical van 0xDUDE is begonnen.

0xDUDE speurt dit jaar - 366 dagen, vijftien uur per dag - het internet af naar kwetsbaarheden. Niet om mensen te hacken, juist om te voorkomen dat ze gehackt worden. Hij meldt zijn vondsten vervolgens discreet bij de eigenaren van de systemen.

De afgelopen vier jaar deed ik onderzoek naar helpende hackers als 0xDUDE. In die periode zag ik hoe tweeëntwintig jonge mannen en twee dames vanuit de marge van de samenleving in de schijnwerpers van de media terechtkwamen.

Telkens legde een jong, verlegen en welbespraakt iemand uit hoe dat kon: een *revenge of the nerds*. Voorheen verguisd door bedrijven, bedreigd door advocaten en onbegrepen door de rest van de samenleving, werden ze nu gevraagd door topbedrijven, omarmd door de overheid en fel verdedigd in de Tweede Kamer.

Ik besloot er een boek over te schrijven: Helpende Hackers (2015). Dat sloot ik af met een portret van 0xDUDE, die ik aankondigde als: '*The biggest Dude of 'm all* .' Hij had in zestien jaar tijd bijna 4.000 meldingen gedaan. Gewoon, naast zijn werk als ambtenaar.

Doordat hij die kwetsbaarheden enkel bij de websitebeheerders meldde, is geen van die onthullingen naar buiten gekomen. Ik heb me daarom voorgenomen zijn verhaal naar buiten te brengen. Om te laten zien hoe onveilig internet vandaag de dag is en wat bedrijven, overheden en andere eigenaren van informatiesystemen daaraan moeten doen. Maar ook om te laten zien hoe één man het verschil kan maken.

0xDUDE

Onze eerste ontmoeting was op Twitter. @0xDUDE tweet regelmatig over veiligheidsproblemen. Op 14 oktober 2013 stuurde hij een privébericht:

'*Hey Chris. Als ik http://www.tektok.nl/templates/system/css/system.css... moet geloven draait de site nog op Joomla 1.5? Heb niet verder gekeken maar wellicht handig 2 upgrade? :-)*'

Scannen naar verouderde versies is een bekende manier voor hackers om kwetsbaarheden te vinden. Als software fouten bevat die misbruikt kunnen worden, worden die gefixt en

vrijgegeven als een volgende versie. Maar voor die fix zijn ze vaak al bekend bij hackers, die ze melden of inderdaad misbruiken.

0xDUDE vertelde dat hij al 3.600 meldingen had gedaan

Onze tweede ontmoeting was op een cybersecuritycongres in Den Haag. Met mijn productieteam had ik de dag ervoor een studio ingericht om interviews te doen met de sprekers en bezoekers van het congres. Die avond stuurde hij me een privébericht met een foto van de zaal. Hij bleek verantwoordelijk voor de beveiliging van de conferentie.

Op de conferentie zelf kon ik hem de volgende dag nergens vinden. Pas toen we onze camera's, belichting en praattafel opruimden, zag ik een man met zwarte baard en zwart T-shirt zitten: 0xDUDE. Hij vertelde dat hij al 3.600 meldingen van kwetsbaarheden had gedaan.

'Wat? Dat kan niet!' riep ik uit. 'Hoelang heb je daar dan over gedaan?'
'Zestien jaar, nooit uitgekomen. Ook nooit een rechtszaak gehad,' zei hij rustig.

Wat 0xDUDE doet

Ik besloot hem uitgebreid te spreken en te volgen voor mijn boek. De eerste keer dat ik hem weer zag, was op de slotconferentie van de Alert Onlinecampagne, op 6 november 2014. Terwijl gewichtige mannen voorbijkwamen met jassen, tassen en kaartjes, stelde 0xDUDE zich voor het eerst voor: Victor Gevers.

Waarom dan 0xDUDE? De '0' bleek een eerbetoon aan een personage uit de cultfilm Hackers. Zero Cool is daarin een mysterieuze elfjarige die allerlei systemen platlegt. Gevers maakte daar '0x' van, omdat computers x'en gebruiken om aan te geven dat een getal in een bepaald getallenstelsel valt. En 'DUDE' omdat hij 'zomaar een gast is die liever op de achtergrond opereert.' Victor heeft namelijk een sociale fobie: hij leeft teruggetrokken en heeft moeite met onbekende mensen.

Gevers vertelde in de lunchroom waar we neerstreken dat hij het Tinbergencollege heeft gedaan, richting economie, met daarna wat losse cursussen in IT-beveiliging en -management. Maar eigenlijk was hij, zoals zoveel hackers, autodidact: 'Gewoon netjes de opleiding afmaken, maar intussen wel je eigen plan trekken.' Na wat werkervaring kwam hij terecht bij de overheid, ver weg van de IT-afdeling, maar wel dicht bij de directie en het management.

Gaandeweg gaf hij steeds meer vrij over zijn technische kennis en belandde hij alsnog in de beveiliging. 'Een soort dekmantel, want als je zegt dat je ethisch hacker bent, schrikt dat af.' Uiteindelijk werd hij Security Architect, naast zijn meldactiviteiten als 0xDUDE. In de afgelopen vijf jaar heeft hij daar in totaal 9.000 uur aan besteed. Vaak maakte hij dagen van

wel twintig uur.

Hoe 0xDUDE dat doet

Gevers maakt vooral gebruik van wat hij 'open source intelligence' noemt. Oftewel: zoekmachines, databases met scanresultaten en lijsten met kwetsbaarheden die iedereen online kan raadplegen. Die informatie vergelijkt hij met wat hij online ziet. Vindt hij een kwetsbaarheid, dan maakt hij een kort rapport, eventueel met screenshots en een beschrijving hoe de beveiliging weer op orde komt. Dat rapport stuurt hij naar het algemene info@adres, de communicatieafdeling van de organisatie, of een medewerker die hij vindt op LinkedIn.

Hij hackt dus niet echt, maar laat wel zien dat het kan en hoe dat voorkomen kan worden. Vaak blijkt dat genoeg. Het lek wordt gedicht, hij krijgt een kort bedankje en gaat door met de volgende.

Wie gaan het slordigst met onze data om? Gevers ziet vooral dat wetenschappers wel heel erg makkelijk data met elkaar delen, ook als dat gevoelige persoonsgegevens zijn. Verder nemen personeelsfunctionarissen en directeuren het niet zo nauw met gegevens over collega's. Dat ziet hij aan het gebruik van een zogenoemde Network-attached storage, een NAS. Dat is een opslagmedium dat op het netwerk is aangesloten. Zo'n NAS staat soms gewoon open en is dan eigenlijk een soort online usb-stick.

Wie gaan het slordigst met onze data om? Gevers zag in die tijd vooral wetenschappers die heel erg makkelijk data met elkaar delen

Af en toe zocht hij daarom op internet naar bestanden op dit soort apparaten met trefwoorden als: 'patiënt,' 'klant,' 'dossier,' 'belangrijk,' 'onderzoek,' 'vertrouwelijk,' 'confidentieel,' 'paspoort,' of 'geheim.'

Als hij dan zo'n open NAS vond, keek hij niet in de bestanden, maar maakte hij een screenshot van de mappenstructuur. Daarna zocht hij via LinkedIn of de bedrijfswebsite de betrokken persoon.

Zo heeft hij in 2014 en 2015 heel veel mensen gewaarschuwd en hun openstaande NAS'en dicht laten zetten. Deze individuele meldingen tellen overigens niet mee in zijn totale aantal, want dat zou te makkelijk zijn.

Wat 0xDUDE gaat doen

Ik heb Gevers weleens gevraagd waarom hij niet voor zichzelf begint: lekker hacken, mensen wakker schudden en er nog goed voor betaald krijgen ook. Maar zo werkt het volgens hem niet. Als je hackt in opdracht van de eigenaar van een systeem, mag je meestal maar met beperkte middelen, in een beperkte tijd, een beperkt deel van het systeem testen. Echte

hackers houden zich niet aan die beperkingen, dus hoe realistisch is zo'n test dan? Daarom blijft het 'vrijwilligerswerk' minstens zo belangrijk, ook al zitten organisaties daar niet altijd op te wachten. Tenminste, dat was toen, in 2014 en 2015.

Het tij voor ethisch hacken lijkt de afgelopen jaren te keren. In de Tweede Kamer wordt steeds vaker opgeroepen meer begrip voor helpende hackers te tonen. Het Nationaal Cyber Security Centrum publiceerde een 'Leidraad responsible disclosure.' Ook bemiddelt het steeds vaker tussen betrokken partijen. Uit een aantal rechtszaken volgde verder dat je mag hacken als dat het maatschappelijk belang dient en je zorgvuldig te werk gaat. Steeds meer organisaties openen ook een meldpunt waar helpende hackers terecht kunnen met hun bevindingen. En steeds meer hackers komen onbevreesd uit voor wat zij doen.

Ook Gevers is er nu klaar voor om meer op de voorgrond te treden en begint voorzichtig hier en daar presentaties te geven over zijn ervaringen. *Het Financieele Dagblad* maakte een uitgebreid portret van hem en meerdere media volgden.

Toch bleef het wringen, de combinatie werk en melden. 0xDUDE zag in de avonduren zijn database met gevonden kwetsbaarheden alsmaar groeien en wilde die het liefst allemaal afhandelen. Hij bedacht daarom de volgende oplossing: ik neem een jaar sabbatical om me er volledig op te focussen. Verschillende mensen haakten aan om Gevers te ondersteunen in zijn missie. En zo begon 0xDUDE op 1 januari 2016 aan zijn hacksabbatical.

Lees in mijn volgende verhaal hoe hij in de eerste maand al 170 kwetsbaarheden vond, meldde en afhandelde.

Lees ook: