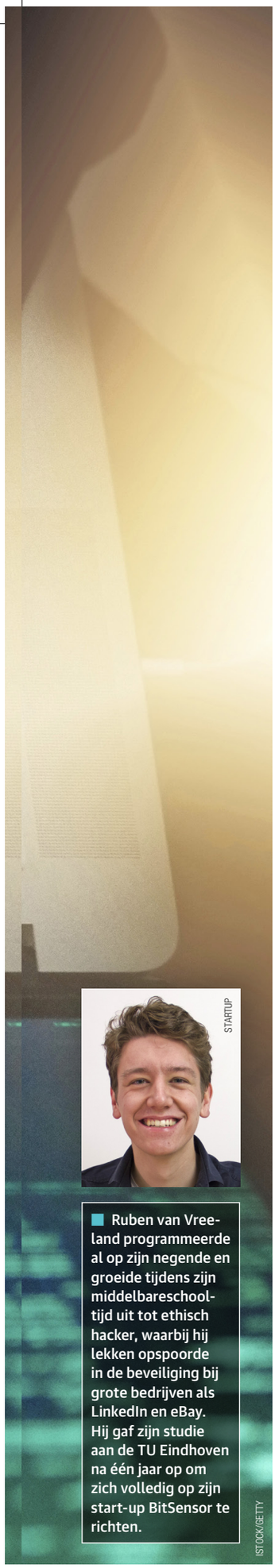
NederTech

Technische hoogstandjes van eigen bodem zijn er genoeg. In NederTech elke maand een mooi voorbeeld. Deze keer: cybersecurity traceert hackers in 50 millisecondes.

Tekst: Hidde Tangerman

NEDERLANDSE SOFTWARE SIGNALEERT DIGITALE AANVALLEN RAZENDSNEL

Hack de hacker



STARTUP

Ruben van Vreeland programmeerde al op zijn negende en groeide tijdens zijn middelbareschooltijd uit tot ethisch hacker, waarbij hij lekken opspoorde in de beveiliging bij grote bedrijven als LinkedIn en eBay. Hij gaf zijn studie aan de TU Eindhoven na één jaar op om zich volledig op zijn start-up BitSensor te richten.

ISTOCK/GETTY

Ruben van Vreeland was er vroeg bij: op zijn negende leerde hij al programmeren en op de middelbare school hackte hij doodleuk de applicaties waar zijn schoolprogramma's op draaiden. Als tiener wist hij binnen te dringen bij de grootste webplatforms van Silicon Valley, zoals Indiegogo, eBay en LinkedIn. Dat alles als ethische hacker met de beste bedoelingen - de kick van een geslaagde hack was weliswaar leuk, maar Van Vreeland wilde vooral bedrijven helpen door zwakke plekken in hun beveiligingssoftware op te sporen.

Die opwindende jaren waren voor Van Vreeland de voedingsbodem voor het inzicht dat er dringend behoefte was aan nieuwe beveiligingssoftware: "Als de beste securityteams ter wereld niet eens merken dat ze worden aangevallen, hebben ze iets anders nodig dan hun bestaande beveiliging."

Samen met Alex Dings, zijn toenmalige studiegenoot aan de Technische Universiteit Eindhoven, richtte hij BitSensor op. De twee oud-studenten hebben hun studie stopgezet om zich te focussen op hun bedrijf. Ze hebben inmiddels software ontwikkeld die hacks binnen 50 milliseconden kan signaleren. In de praktijk betekent dat: op het moment dat ze worden uitgevoerd. En dat terwijl het gemiddeld negen maanden duurt voordat een bedrijf door heeft dat het is gehackt. 'Binnen 50 milliseconden'; dat is nogal een claim - en een doorbraak. Dings en Van Vreeland benaderen cybersecurity dan ook anders dan anderen.

Unieke aanpak

De huidige beveiligingssoftware is vaak een schil die als een soort vangnet om een applicatie heen zit. Dat vangnet kijkt naar de input, oftewel het dataverkeer dat vanuit gebruikers naar de applicatie toe gaat. Zodra daar verdachte commando's of coderegels tussen zitten, slaat de software alarm en blokkeert hij die gebruikers. Helaas is dat meestal niet genoeg om hackers buiten de deur te houden. Dings: "Input die niet voorkomt in de dataset van dat beveiligingsprogramma, maar die wel slecht is voor de applicatie, passeert het vangnet gewoon. Hackers verzinnen aan de lopende band dat soort nieuwe *signatures*; dat is de sport."

De mannen van BitSensor installeren hun beveiligingssoftware in de applicatie zelf, bijvoorbeeld in een webshop of een app voor online-bankieren. Hun aanpak is uniek omdat ze niet focussen op het inkomende dataverkeer, maar juist de output in de gaten houden: de commando's die de applicatie teruggeeft als reactie op de input.

BITSENSOR

Mede-oprichter Alex Dings legt uit hoe BitSensor hackersprofielen aanmaakt op basis van gegevens als cookies, programmeertaal en tijdzone. Op het moment dat een hacker zijn aanval lanceert, heeft BitSensor hem meteen in de gaten.

Een hacker begint bijna altijd met het opvragen van de loginpagina van een website of app, wat vaak website/login of website/admin is. Bij een van die twee commando's geeft de applicatie een zogenoemde 404 error terug met de mededeling dat die pagina niet bestaat. "Doorgaans werd zo'n error als onbelangrijk gezien," zegt Dings, "maar wij vinden hem juist heel belangrijk, want zo'n melding is vaak stap één van het aanvalsplan van een hacker. Dus hoe meer errors de applicatie teruggeeft, hoe groter de kans dat er een hacker bezig is. Met deze kennis kun je die bezoeker met kwade bedoelingen snel opsporen en meteen isoleren van de gewone websitebezoekers."

Al meteen bij de eerste error maakt de BitSensor-software een profiel van de hacker aan, waarin onder meer zijn IP-adres, inlognaam, browser- en taalinstellingen en de tijdzone waarin hij of zij opereert worden meegenomen.

Zo kan de software de hacker meteen identificeren zodra hij de echte aanval inzet. Dit alles gebeurt binnen die 50 milliseconden. Vervolgens kan BitSensor de aanval blokkeren of de hacker naar een *sandbox* leiden. Dat is een kopie van de website, maar dan zonder data. De software observeert in die sandbox hoe de hacker de aanval opbouwt, slaat de aanvalstechnieken op en wordt daardoor steeds beter.

Blufpoker

Op deze manier volgt BitSensor elke aanvalspoging van a tot z. De software weet precies waar de hacker is geweest en - mocht de hacker onverhoopt door de blokkade heen breken - welke data hij heeft buitgemaakt. Die kennis is een troef als de hacker na de aanval probeert losgeld op te strijken voor de gestolen data. "Hackers bluffen vaak dat ze data gaan vrijgeven die ze helemaal niet hebben", vertelt Dings. "Bij ons kan dat niet meer."

BitSensor heeft momenteel vooral banken, verzekeraars en overheden als klant. In een gemiddelde week zien de Eindhovense ondernemers per klant ongeveer 20.000 digitale aanvallen voorbijkomen, afkomstig van zo'n twintig menselijke hackers en talloze bots.

De data die Dings en Van Vreeland over hackers verzamelen en opslaan, kunnen interessant zijn voor politie en justitie, want die hebben nog veel moeite met attributie: het herleiden van de hack tot de hacker. BitSensor helpt hier graag bij. "Wij vinden het belangrijk dat justitie niet-ethische hackers opspoort", zegt Van Vreeland. "De data die daarvoor nodig zijn, kunnen we op een presenteerblaadje aanreiken." ■