techpulse.be

Bekeerde hacker voorspelt cyberwereldoorlog - TechPulse

web design and development by www.octagram.ro

11-14 minuten

Michael ‘MafiaBoy’ Calce is een bijzondere figuur. In 2000, op vijftienjarige leeftijd, legde hij Yahoo, eBay, Amazon, Dell en CNN een uur lang plat. De aanvallen kwamen er nadat enkele hackers hem vertelden dat het onmogelijk was om websites van zulke grote en machtige bedrijven neer te halen. Woorden die de jonge MafiaBoy niet graag hoorde: “vroeger draaide het voor een hacker immers niet om geld, maar om prestige en erkenning,” herinnert Calce zich.

Paniek

“Iedereen, hacker of niet, heeft ooit in zijn leven wel eens het gevoel ‘fuck, wat heb ik gedaan?’ Voor mij kwam dat moment er in 2002, toen president Bill Clinton op televisie verkondigde dat een speciale taskforce werd opgericht om mij te vinden. Slik.” Calce had naar eigen zeggen geen idee dat zijn acties zo’n grote gevolgen zouden hebben. Naast een paniekaanval bij de getroffen bedrijven hield de gebeurtenis het volledige internet nog een tijdlang in zijn greep. Ook wij (ZDNet) hielden het voorval in 2000 nauwlettend in de gaten.

De acties van Calce kostten de Amerikaanse economie ongeveer anderhalf miljard dollar; een massa geld voor wat toen

nog steeds een opkomende industrie was. De dotcomcrisis zat er bovendien aan te komen, wat de zenuwachtigheid van de Amerikaanse president geen goed deed.

Canadese strafmaat

Uiteindelijk zou het nog vier maanden duren vooraleer de Canadese politie de jonge hacker wist op te sporen. In de zoektocht naar erkenning en beruchtheid was hij beginnen opscheppen over zijn daden in de chatroom van een Californische universiteit. De rechtszaak zou ruim een jaar aanslepen en al die tijd werd in de media gewag gemaakt van een zware straf, om een voorbeeld te stellen. Die kwam er niet: “het werden acht maanden in een open opvangcentrum, een boete van 250 dollar en vijf jaar internetverbod. God zegene Canada,” lacht Calce, en de zaal met hem.

Ik bevind mij op de HP Innovation Summit in Londen en Calce heeft de zaal op zijn hand. De hele middag door luistert iedereen beleefd, en bij momenten geboeid, naar de vele sprekers.

Wanneer Calce het podium op komt, wordt evenwel duidelijk naar wiens presentatie iedereen echt uitkeek. MafiaBoy heeft nog geen minuut nodig om met enkele mopjes en een straf verhaal de journalisten en HP-medewerkers te boeien.

“Mijn drijfveer in alles wat ik doe, is niet het oplossen van een puzzel,” zegt Calce. “Het boeit mij daarentegen mateloos om verschillende manieren te bedenken om één puzzel op te lossen.” Toen zijn vader in 1990 thuiskwam met een computer om zijn bescheiden zaak te moderniseren, mocht Calce het uitvogelen. “Maar het zou oneerbiedig zijn om te zeggen dat hij de kat bij de melk heeft gezet.”

Gratis internet

Calce’s fascinatie voor het internet begon in 1993, hij was dan 9 jaar. Hij kwam in het bezit van een cd die de gebruiker een maand lang gratis internettoegang bezorgde. Al snel kreeg hij ruzie met een oudere internaut die het internet geen plaats vond voor jonge nieuwsgierigen. “Hij sneed mijn toegang tot het internet af, in een vingerknip. Ik was kwaad, maar ook gefascineerd.” De vonk sloeg over en al snel kwam hij erachter welk programma hem het onrecht had aangedaan.

“Uiteraard begon ik dat programma zelf te gebruiken op zeer regelmatige basis,” zegt Calce. Met het juiste gereedschap op zijn computer slaagde hij erin om als negenjarige tientallen volwassenen te beduvelen met ‘social engineering’: hij stuurde e-mails naar mensen met internettoegang en vertelde hen dat ze hun inloggegevens moesten doorsturen omdat het systeem werd geüpdatet. Een truc die vandaag nog steeds in omloop is.

Natuurlijk was ik dol op de macht die ik bezat.

“Ik kon gratis op internet, zo veel en zo vaak ik wou,” vertelt

Calce, duidelijk nog steeds trots op de prestaties van zijn jonge jaren. “Niet dat ik er veel te zoeken had, maar ik was in het bezit van zoveel macht dat ik er niet weg kon blijven. En die truc waarbij je iemand van het internet afsneed? Die gebruikte ik vaak,” zegt hij, opnieuw met een grijns op het gezicht. De zaal lacht mee, want de man heeft berouw getoond, hij was toen nog jong en het was allemaal toch onschuldig, niet?

Piraterij

De onschuldige kwajongensstreken escaleerden snel tot meer. Op elfjarige leeftijd zoekt hij nieuwe manieren om games te kunnen downloaden. Toen gebeurde dat met behulp van bots die elke downloader een bepaalde bandbreedte toewijzen. Op het forum van de downloadsite komt hij in contact met hackers die manieren kennen om sneller te downloaden. Hij leert zichzelf programmeren om die bots te kunnen omzeilen en om indruk te maken op het forum.

Calce blijft nieuwe trucs toevoegen aan zijn arsenaal en in 1997, hij is dan dertien jaar, wordt hij gerekruteerd door een van de meest beruchte hackersgroepen van dat moment: het Russische TNT. Zowat de helft van alle malware uit die periode is afkomstig van een lid van deze notoire club. Calce laat zich meer en meer in met kleine hackersoorlogjes die moeten uitwijzen wie de beste is. In 1997 worden al bescheiden sommen verdient met malware, maar de meesten is het nog steeds te doen om de erkenning van medehackers.

De bedenkers

Altijd op zoek naar meer erkenning, meer puzzels, meer oplossingen en steeds grotere uitdagingen staat Calce mee aan

de wieg van DDoS-aanvallen. Samen met zijn vrienden-hackers maken ze hun aanvallen grootser en gerichter. Het culmineert in 2000 in Project Rivolta, een gecoördineerde aanval op enkele van de belangrijkste websites van hun tijd. Een aanval die leidde tot de totstandkoming van verschillende wetten die de exploten van Calce moesten definiëren buiten de aanvaardbare grenzen van de wet. Hoeveel wetten zijn er al geschreven ter uwer ere?

Na zijn digitale huisarrest ging Calce niet opnieuw aan de slag als hacker. “In mijn dagen als hacker hield ik mezelf voor dat ik bezig was met een goede zaak: ik zorgde voor de bewustmaking rond internetveiligheid,” zegt Calce. “Ik deed het ook nooit voor het geld, puur om mezelf berucht te maken. Het was bovendien moeilijk om berouw te voelen voor mij daden terwijl ik ze uitvoerde; je hebt namelijk niet het idee dat wat je doet illegaal is, of dat je er een economie zoveel geld mee kan kosten. Het enige dat mij bezighield, was dat andere hackers zeiden dat het onmogelijk was en dat ik, een vijftienjarige, ze wel even op hun plaats zou zetten.”

Calce noemt zichzelf een goed persoon, met dank aan een goede opvoeding: “Ik deed het nooit om mensen geld af te luizen, ik wilde gewoon kunnen opscheppen. En natuurlijk was ik dol op de macht die ik bezat.”

Reputatieschade

Maar de tijden veranderen. Vroeger werd een hacker door onzuivere figuren aangeworven op basis van reputatie. Een hacker nam ook niet zomaar elke klus aan, uit schrik dat het zorgvuldig opgebouwde imago besmeurd werd. “Vandaag is het evenwel de hoogste bieder die iets gedaan krijgt. En dat mag je heel letterlijk nemen: een hacker zal zijn malware verkopen aan de hoogste bieder, wie dat ook moge zijn,” legt Calce uit.

Linux: de snelste weg naar het hackerschap. Beeld: zoljo | iStock

Het draait meer dan ooit om geld: hacken is een industrie op zichzelf geworden. “Het is nooit zo makkelijk geweest voor vijftienjarigen om te beginnen hacken. Je downloadt Kali Linux, installeert enkele plug-ins en je bent vertrokken. Ransomware koop je aan als een suite en je krijgt er een helpdesk bij. Je hebt slechts een halfuur voorbereiding nodig om je te mengen in verkiezingen – ik ga geen voorbeelden noemen.”

Bovendien speelt normvervaging eveneens een grote rol volgens Calce: “de huidige generatie vijftienjarigen weet niet meer waar de grens ligt. Grofgebektheid wordt op het internet als normaal gezien, en presidenten doen er vaak zelfs nog een schepje bovenop. En het wordt steeds makkelijker om economische schade aan te richten als je malware vrij goedkoop kan

aanschaffen."

We lezen en zien zoveel spionageverhalen dat we vergeten dat vele van die verzinsels geënt zijn op praktijkvoorbeelden.

Ethish hacken

Calce verkoopt zijn diensten vandaag aan 'de goeien'. Hij voert met zijn bedrijf penetratietests uit die onderzoeken hoe sterk de beveiliging van een bedrijf of organisatie is, en daarnaast werkt hij samen met HP om betere beveiligingsmethodes te bedenken. Waar ziet hij vandaag de grootste tekortkomingen? "Werknemers zijn nog steeds de zwakste schakel. Bedrijven kunnen zo goed beveiligd zijn als ze willen, het is nog altijd een eitje om via een nietsvermoedend personeelslid binnen te geraken."

"Een tijdje geleden deed ik een penetratietest voor een groot bedrijf. Ik dacht mezelf nog eens uit te dagen en de conventionele methodes, social engineering en phishing, links te laten liggen. Ik onderzocht de routines van enkele werknemers en kwam uit bij een man, niet oud, niet jong, iemand die even goed met een computer kan werken als de volgende in de rij."

"Hij werkte elke dag op de trein op weg naar zijn werk. Hij volgde braaf de voorschriften van zijn IT-departement: bescherm de 'line of sight', de kijkhoek, zet bluetooth uit enzovoort. Hij gebruikte wel het internet van de trein, omdat dat nodig was voor zijn werk. Ik kraakte de router van de trein, legde hem plat en presenteerde mijn computer als nieuwe treinnetwerk, enkel en alleen door het een gelijkende naam te geven. De man logde in en van zodra hij aankwam op zijn kantoor en zijn computer verbinding maakte met het bedrijfsnetwerk, had ik het hele bedrijf in handen."

Riolering

Het klinkt als een Ian Fleming-verhaal, maar het gebeurt echt. We lezen en zien zoveel spionageverhalen dat we vergeten dat vele van die verzinsels geënt zijn op praktijkvoorbeelden. Bovendien helpt het niet dat onderwijzing in de gevaren van het internet nog steeds geen prioriteit is in onze bedrijfswereld. Wij Belgen moeten nochtans beter weten: een tijd geleden stonden we nog bovenaan in de lijst van meest gedupeerde landen.

“Bedrijven zijn te veel gericht op de voor- en achterdeur. Ze denken dat als ze die beveiligen, ze veilig zijn. Hackers denken echter meer als inbrekers: als de deur van de kluis te zwaar beveiligd is, dan gaan ze wel via de riolering. Ze vinden altijd wel een zwakke plek,” zegt Calce.

Voorlopig is er nog niets ontploft, maar wat als dat wel gebeurt?

Naar de wuppe

Calce had het eerder al over verkiezingen die beïnvloed werden. Het kost ieder weldenkend mens exact twee seconden om door te hebben waar hij op alludeert: Donald Trump. Met de nakende verkiezingen in Frankrijk en Duitsland kan dat wel eens een gevaarlijk precedent worden: “als je iets doet zonder resultaat, kan het even duren vooraleer iemand anders het opnieuw probeert, maar als iets succesvol is, is het logisch dat anderen zullen volgen,” zegt Calce.

Hij is er dan ook van overtuigd dat deze situatie vroeg of laat zal escaleren: “achter de schermen woedt al langer een hevige strijd, met een grote impact op verschillende landen. De volgende grote oorlog wordt sowieso een cyberoorlog waarbij de grote infrastructuur een doelwit zal zijn: kerncentrales, ziekenhuizen, internetproviders,… Voorlopig is er nog niets ontploft, maar wat als dat wel gebeurt?” vraagt Calce zich af.

“Je hebt immers maar één getalenteerde hacker nodig om de vlam in de pan te doen slaan. De V.S. hebben goede hackers, China ook, maar in Roemenië vind je eveneens genoeg individuen die een oorlog kunnen starten. Maar de echte heersers van het internet vind je nog steeds in Rusland: de hackersgemeenschap daar is nog steeds de beste ter wereld. Met de stijgende spanningen met de V.S. en Syrië kan morgen de hel losreken.”