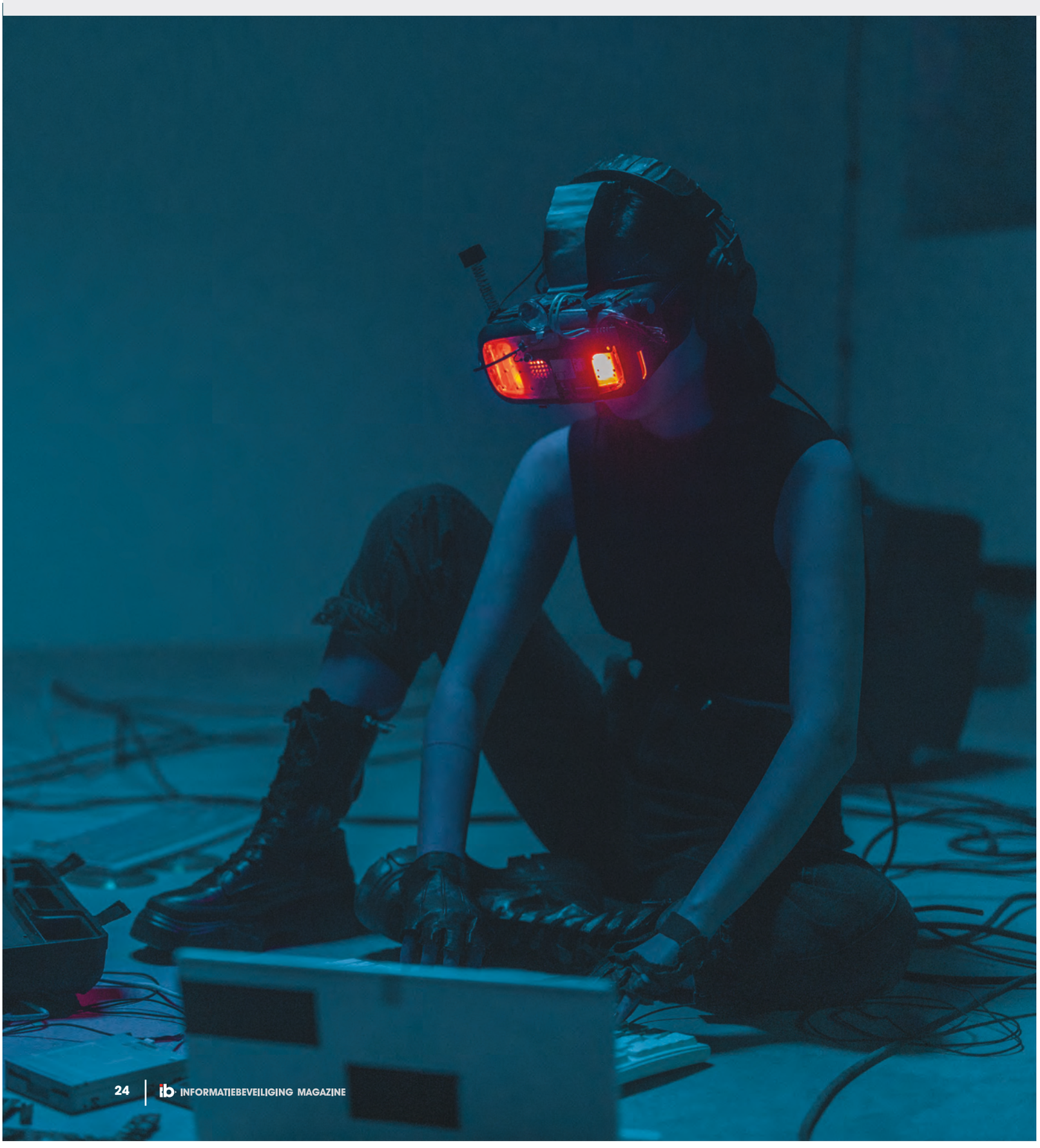
Auteur: Stefan Tezgel is sinds 2015 cybersecurity-adviseur bij CGI. Sinds 2011 is Stefan actief in de informatiebeveiliging met een achtergrond in de ICT en in digitaal onderzoek. Door de jaren heen heeft hij heel breed ervaring opgedaan aan zowel de functionele als technische kant van de informatiebeveiliging. Hij is te bereiken onder stefan.tezgel@cgi.com.



De ontwikkelingen van een vrijwillig cyberleger

Daar stond ik dan op de 'ONE', met natte handen die een papiertje met mijn laatste krabbels vasthielden. Mocht de techniek falen dan had ik altijd nog mijn verhaal bij de hand. 973 vakgenoten keken mij vanuit het donker aan, een 'make-it-or-break-it' moment. 'Cyberwarfare', een belangrijk en zeer actueel onderwerp. 'Go hard or go home.' Een zachte 'hit-it' en de zelfgemaakte compilatie van beeldmateriaal begon te spelen. Ik ga het nu echt doen! 'Spot on' en ik begon aan het verhaal…

Het is eind februari als de eerste berichten over het begin van de oorlog tussen Rusland en Oekraïne mijn telefoon bereiken. Ik lees de berichten met verbazing en tegelijkertijd voel ik mijn maag omdraaien. Het zal toch niet… maar het nieuws laat me vanaf dat moment niet meer los. Ik bedenk hoe het zal zijn voor al die arme mensen. Wat een hel om in te belanden. Ik kan me niet inbeelden hoe het voor de mensen daar moet zijn, want ik heb altijd in een vrij land en in een veilige situatie gezeten.

Dan, een paar dagen later. Het ministerie van Digitale Transformatie van Oekraïne roept een vrijwillig cyberleger bijeen (1). Oekraïne is al langer bezig met het idee om een cyberleger in te zetten, maar roept nu de wereld op om mee te denken en mee te doen. Ik ben geïntrigeerd, een eerste cyberoorlog en eentje die opvallend open en zichtbaar plaatsvindt! Hoe zou zich dat gaan ontwikkelen? Wie sluit zich daarbij aan? En ook wat zijn ieders motieven? Ik besluit me dan ook aan te melden via het kanaal op Telegram (2) alleen dan wel in de observatiestand.

Ik ben ervan overtuigd dat wij als security professionals op het scherpst van de snede moeten snappen wat er in de wereld van digitale veiligheid gebeurt. Het leert ons de tactieken, technieken en procedures die ingezet worden om systemen te compromitteren. Op die manier krijgen we meer inzicht in de 'modus operandi' en kunnen we daar ook de passende maatregelen op inzetten en onszelf beter beschermen.

De eerste dertig dagen

Tegen mijn verwachtingen in was er in de eerste dagen niet echt veel tractie. Het startte met een oproep van het ministerie van Digitale Transformatie en die was vrij duidelijk: *'voer cyberaanvallen en DDoS-aanvallen uit', 'zorg dat men weet wat er gebeurt in Oekraïne', 'val media aan en rapporteer propaganda en desinformatie'*. Een breed geformuleerde opdracht dus. De eerste gesprekken en kleine discussies vinden plaats in de Telegram groep. Ik besluit een aantal mensen via privé chat te benaderen met vragen over waarom ze meedoen, wat ze hopen te bereiken en hoe ze zelf denken te kunnen bijdragen. Het valt me op dat ik meteen in gesprek raak met mensen die allerlei beroepen uitoefenen: leraren, kantoormedewerkers, cybersecurity-specialisten en zelfs een lasser. Eén ding is duidelijk: de informatieoorlog is begonnen en er zijn op dag één al 160.000 mensen (3) die daaraan willen bijdragen.

In de eerste dagen worden enkele doelwitten genoemd, instructies gaan over en weer en ook persoonlijke informatie van vooraanstaande tv-sterren en -presentatoren wordt gedeeld. De effectiviteit van DDoS-aanvallen varieert van takedowns van 5 tot 45 minuten. De eerste 'defacements' (4)(5) vinden plaats en er wordt een dashboard geïntroduceerd waarop duidelijk wordt welke systemen er onbereikbaar worden gemaakt en ook gehouden. Ook wordt er buitgemaakte informatie gedeeld: persoonlijke informatie en duizenden actieve creditcards van Russische burgers. Deze informatie wordt vervolgens gebruikt om mensen geautomati-

seerd te laten bellen door bots en foto's van het slagveld worden via sociale media verspreid. Daar wordt zelfs een video over gemaakt (6).

In de resterende dagen van de eerste oorlogsweek vinden de eerste optimalisaties plaats. URL's worden IP-adressen met specifieke poortnummers en bepaalde targets worden nader onderzocht op (nog) meer relevante doelen. Korte tijd daarna verschuiven de doelwitten die in het Telegram kanaal gedeeld worden van financiële systemen naar systemen die betrokken zijn bij de oorlogvoering op de grond, waaronder GLONASS (het Russische satelliet navigatie systeem), transport (Belarus Railway Network) en later ook telecom (MTS, Beeline). Zoals via de oproep: *'stop de navigatie en de supply chain van Rusland'* (7)(8).

In de tweede week blijven systemen die betrokken zijn bij de oorlogvoering op de grond het primaire doelwit. Secundair worden de eerder al gemarkeerde doelwitten, waaronder media, overheid en de financiële sector. Vanaf 11 maart wordt ook de civiele infrastructuur betrokken in de targets: bezorgdiensten, nieuwssites, apotheken en bioscopen worden in datzelfde weekend massaal aangevallen (9).

De derde week worden nieuwe verdedigingstechnieken waargenomen aan de kant van Rusland. Bepaald netwerkverkeer lijkt niet meer aan te komen in Rusland. Vanaf dat moment gaan de aanvalstechnieken op de schop, iedereen krijgt het advies een VPN te gaan gebruiken, voorzien van de instructie hoe dat op een succesvolle wijze in te zetten. De dagen erna volgt optimalisatie na optimalisatie, met de constante boodschap om vooral de voornoemde doelwitten te blijven aanvallen.

De laatste week van deze eerste maand wordt er ingezet op de pakketdiensten, dat blijkt tal van leveringen te vertragen en het blijkt een groot effect te hebben (10)(11). Dit wordt ook het doelwit voor de resterende dagen van de eerste maand. Ook wordt deze week voor het eerst opgeroepen om een specifieke tool te gaan gebruiken (12), DB1000N ofwel 'Death by a 1000 Needles'. Een tool die op Oekraïense bodem is ontwikkeld. Deze tool is open source en te vinden op Github (een open-source samenwerkingsplatform) (13) en kan worden gezien als een heus 'cyberwapen' met meer dan 59 unieke 'contributors'.

De dagen die volgden

In de dagen die volgen gaan de aanvallen verder, de impact wordt groter en de eerste grote gevallen van computervredebreuk worden bekend. Er blijken op grote schaal cyberaanvallen uitgevoerd te zijn onder de regen van DDoS-aanvallen. De televisiemedia wordt gehackt, EGAIS (gebruikt voor alcohol tracking) wordt zodanig geraakt dat brouwerijen en fabrieken moeten sluiten en Rutube (de Russische equivalent van YouTube) wordt compleet overgenomen.

In het laatste geval werd de systeembeheerder vanwege abnormaal systeemgedrag naar de serverruimte gelokt. Eenmaal aangekomen in de serverruimte werden zijn inloggegevens onbruikbaar gemaakt en werd het systeem van toegangspassen overgenomen. Hierdoor kon hij niet alleen de serverruimte niet meer verlaten, hij moest ook moedeloos toekijken hoe er petabytes aan data onherstelbaar werden vernietigd (14)(15).

Wat je de afgelopen maanden ziet gebeuren als je de berichten in het Telegram kanaal analyseert, zijn verdere optimalisaties die in stappen worden doorgevoerd. Daar waar het begon met een tool (DB1000N) worden er nu meerdere tools aangeraden (MHDDOS, Distress en uaShield). Er zijn nu uitgebreide instructies over het gebruik van een VPN en er is een officiële chatbot waarbij mensen zich kunnen aanmelden om deel te nemen aan een vrijwillig botnet. Een belangrijke, naar mijn mening zorgwekkende ontwikkeling is dat er geen doelwitten meer 'omgeroepen' worden, maar dat er nu wordt gewerkt met een 'target list' die gesloten is voor de vrijwillige deelnemers.

Nu de tijd verstrijkt komen er meer en meer datalekken aan het licht. Onder de regen van alle DDoS- aanvallen blijken er diepgaandere cyberoperaties te hebben plaatsgevonden. De gekozen doelwitten waren niet zomaar gekozen en de DDoS-aanvallen bleken niet alleen tot doel te hebben systemen onbereikbaar te houden. Roseltorg (een belangrijk Russisch procurement platform), Right Line (belangrijke cloudopslag), Gazprom (belangrijke Russische gasleverancier) en Wagner (een particulier militair bedrijf) zijn allemaal gehackt en hebben kostbare informatie verloren aan het Oekraïense cyberleger. De werkwijze van deze hacks verschillen enorm (van gestolen accounts tot maandenlang wachten op het juiste moment) en elk van deze acties zijn het waard om nader te bestuderen. Datzelfde geldt voor het open source zijn van de ingezette tooling en het gekozen communicatieplatform (Telegram).

Ik ben ervan overtuigd dat er maar weinig mensen notie hadden genomen van het feit dat zij volledig zichtbaar voor de buitenwereld hun activiteiten uitvoerden. Ik heb tientallen mensen gesproken die zich voordeden als zijnde een lid van bekende hacking groepen, die vervolgens ook tools deelden waarvan ze zelf niet begrepen wat die tools exact deden. Zij deelden deze informatie en tools ook open en bloot vanaf hun eigen persoonlijke mailadres zonder zich bewust te zijn wat voor spoor van vernieling zij achterlieten en hoe hun naam en hun informatie terug te leiden was naar hun eigen persoon.

De vier belangrijkste lessen

De belangrijkste lessen wil ik hier ook graag delen. Dat zijn er vier:

1. Het vrijwillige cyberleger werd een snelgroeiende community die gecentraliseerd was opgezet en in de eerste weken een groei naar volwassenheid doormaakte. Mensen werden meer betrokken ook onderling, men wilde elkaar technieken en werkwijzen bijbrengen en men reageerde actief op aankondigingen in het kanaal.
2. Vanaf de eerste dagen was er sprake van een daadkrachtig optreden van het vrijwillige cyberleger. In zeer korte tijd is de effectiviteit toegenomen en ontstond er duidelijkheid in hoe mensen konden bijdragen.
3. Als er een verdeling wordt gemaakt tussen de 'goede' en 'slechte' partij, lijken legaliteit en ethische principes te verdwijnen. Niet-militaire doelwitten werden ook aangevallen, privésystemen werden binnengedrongen en de bijkomende schade door de uitgevoerde acties leken deelnemers aan het vrijwillige cyberleger minder te interesseren.
4. Het ad hoc oproepen om aan te sluiten bij het cyberleger creëerde een enorme valse start. Het doel was duidelijk, maar de manier waarop die doelen bereikt moesten worden niet, met als gevolg een enorme chaos. Er kwam een separaat chatkanaal (17) waarin deelnemers ook weer subkanalen deelden. Men verspreidde diverse uitvoerbare bestanden, potentiële malware, verschillende handleidingen, malafide websites, spyware en andere narigheid.

En hoewel deze inzichten waardevol zijn, hoop ik vooral dat er liever gisteren nog dan vandaag een einde komt aan de oorlog in Oekraïne. Ondanks intensieve grip op de media in Rusland zijn er inmiddels serieuze tegengeluiden van publieke figuren (18)(19) te lezen op sociale media (20) en ook te horen van politieke leiders uit het oosten (21) en verzetsgroepen (22). Dit biedt hoop voor de toekomst en de betrokken families. Будь мужнім.

Referenties

(1) https://t.me/mintsyfra/2609
(2) https://t.me/s/itarmyofukraine2022
(3) https://tgstat.com/channel/@itarmyofukraine2022/stat/subscribers
(4) https://t.me/itarmyofukraine2022/175
(5) https://www.bleepingcomputer.com/news/security/ukraine-says-its-it-army-has-taken-down-key-russian-sites/
(6) https://www.youtube.com/watch?v=1sfpTldvpPE
(7) https://www.reuters.com/world/europe/ukraines-it-army-targets-belarus-railway-network-russian-gps-2022-03-03/
(8) https://t.me/itarmyofukraine2022/120
(9) https://t.me/itarmyofukraine2022/197
(10) https://t.me/itarmyofukraine2022/235
(11) https://t.me/itarmyofukraine2022/236
(12) https://t.me/itarmyofukraine2022/229
(13) https://github.com/arriven/db1000n
(14) Rutube https://www.nbcnews.com/tech/tech-news/rutube-down-russia-hack-attack-ukraine-rcna28299
(15) Rutube https://www.youtube.com/watch?v=pggg8sEDhjA
(16) https://itarmy.com.ua/instruction/
(17) https://t.me/+H6PnjkydZX0xNDky
(18) https://nos.nl/artikel/2445109-russische-popster-veroordeelt-oorlog-in-oekraine-maakt-van-ons-een-paria
(19) https://www.pzc.nl/buitenlands-voetbal/ex-captain-russisch-voetbalelftal-keert-zich-tegen-poetin-misschien-beland-ik-in-de-cel-of-word-ik-vermoord~abe076b1
(20) https://www.volkskrant.nl/nieuws-achtergrond/kritiek-op-oorlog-zwelt-aan-op-ruslands-grootste-sociale-medium-poetin-is-een-pathologische-leugenaar~bc2a848d/
(21) https://www.bnnvara.nl/joop/artikelen/china-en-india-laten-rusland-vallen-poetin-verder-in-het-nauw
(22) https://nos.nl/artikel/2423515-partizanen-in-belarus-leggen-spoor-plat-om-russisch-leger-te-dwarsbomen