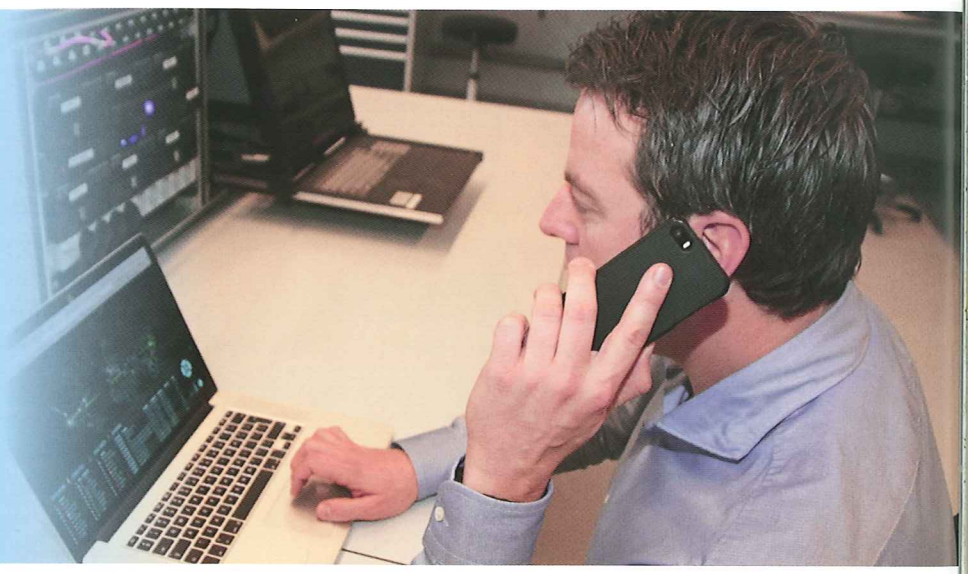
Foto: Loes van der Meer

Robin Stellaard is operationeel expert intelligence bij het Team High Tech Crime van de Nederlandse politie. Wat waren zijn meest opvallende telefoontjes?

5 telefoontjes aan Robin Stellaard



1 Door politiecollega's uit Duitsland word ik gevraagd om met spoed een server veilig te stellen die gehost wordt in Nederland en malware verspreidt.

Op basis van het Verdrag van Boedapest van de Raad van Europa ('Cybercrime Convention') zijn wij als Team High Tech Crime (THTC) het Nederlandse aanspreekpunt voor alle landen die dit verdrag hebben ondertekend. Cybercrime laat zich niet stoppen door landgrenzen, de data zijn vaak vluchtig en de aanpak vraagt om specialistische kennis en expertise. Daarom is op ons team een '24/7 contact point' ingericht om onder andere verzoeken vanuit het buitenland snel opvolging te geven, in afwachting van het formele rechtshulpverzoek. Dit doen we door het zelf uit te voeren of door te zorgen dat het verzoek op de goede plek terecht komt.
Ik bespreek met een digitaal rechercheur het Duitse verzoek. We proberen het verzoek zo helder en duidelijk mogelijk te krijgen alvorens ik het 24/7 verzoek voorleg aan onze cyberofficier Martijn Egberts. Met Egberts bespreek ik het verzoek en we stemmen af bij welke politie-eenheid dit verzoek belegd zou kunnen worden. In dit geval werd dit de eenheid Rotterdam en daarom zet de officier het verzoek door naar het IRC in Rotterdam.

2 Een telecombedrijfje belt mij met de melding dat een van zijn servers gehackt is en vraagt of wij interesse hebben in de door hem aangetroffen data op deze server.

Na onderzoek van de data bleek het te gaan om een server die door cybercriminelen gebruikt werd voor de verspreiding van *ransomware*. Dit type malware versleutelt (encrypt) bestanden op een geïnfecteerde computer en vraagt de gebruiker vervolgens om een geldbedrag om deze bestanden te ontsleutelen (decrypten). Wij hadden het geluk dat op deze server ook 1500 digitale 'sleutels' stonden om de bestanden te ontsleutelen. Het is voor de politie alleen erg lastig om deze digitale sleutels te distribueren onder de slachtoffers van deze specifieke ransomware, bijvoorbeeld via de website

van de politie. Wij hebben niet de illusie dat een slachtoffer uit Kazachstan de website van de Nederlandse politie zal vinden, laat staan vertrouwen. Daarom hebben wij de sleutels gedeeld met een internationaal antivirusbedrijf. Zij hadden binnen zeer korte tijd een website in de lucht vanwaar slachtoffers hun digitale sleutel konden afhalen. In de tussentijd werd door ons team de zaak verder voorbereid voor een strafrechtelijk onderzoek naar de hack op de server en de verspreiding van ransomware. Twee Nederlandse verdachten zijn inmiddels opgepakt, mede op basis van informatie die het antivirus bedrijf teruggaf. We hebben veel lof gekregen van slachtoffers die door onze actie hun bestanden konden ontsleutelen en zo hun foto's – soms van overleden dierbaren – weer terug hebben. Tot slot had het antivirusbedrijf goede PR. Win-winsituatie dus.

3 Door de 24/7 waakdienst van het Nationaal Cyber Security Center (NCSC), word ik gebeld dat zij benaderd zijn door een kabelexploitant en dat dit bedrijf aangifte wil doen van een zeer grote DDoS-aanval op hun servers.

Vanuit de politie werk ik veel samen met het NCSC. Het NCSC signaleert dag en nacht nieuwe 'digitale' dreigingen en kwetsbaarheden en voorziet zijn netwerk van contacten van opvolgbare informatie. Ik neem direct contact op met de kabelexploitant en bespreek de zaak kort en inhoudelijk om te zien of deze zaak past bij de inzetcriteria van Team High Tech Crime. Na overleg met een teamleider van THTC en officier Martijn Egberts is besloten dat wij de zaak gaan oppakken en in dit geval de aangifte zelf opnemen. Deze aanval werd direct opgeëist door cybercriminelen in een filmpje op Youtube. Direct neem ik ook contact op met een digitaal rechercheur om zo snel mogelijk informatie uit open bronnen zoals openbare Twitteraccounts, nieuwswebsites en Youtube veilig te stellen voor onderzoek voordat deze is verdwenen. Door deze snelle aanpak kregen wij in een vroeg stadium zicht op een groep verdachten die inmiddels zijn aangehouden.

4 Een politiecollega van Eenheid Noord-Holland vraagt of wij kennis hebben van bepaalde malware.

Ik zet deze vraag door naar één van de digitale rechercheurs van ons team die hem verder informeert. Doordat de politie-eenheden zelfstandig cybercrime-zaken moeten gaan uitvoeren, wordt het Team High Crime steeds vaker benaderd door politiecollega's van de lokale eenheden. Dit heeft er vooral mee te maken dat wij inmiddels veel ervaring hebben met de aanpak van cybercrime en wij onze kennis en kunde graag uitdragen. Wij leveren geen capaciteit maar vervullen meer een adviserende rol.

5 Op ons Twitterkanaal word ik door een securityspecialist benaderd over een hackonderzoek dat hij met ons wil delen.

Uit zijn onderzoekgegevens blijkt dat een bedrijf besmet is geweest met een Remote Access Tool (RAT) waarmee op afstand digitaal op de computer kon worden meegekeken door de cybercriminelen. Gezien de mogelijke schade en betrokken bedrijven die slachtoffer waren hebben we direct een opsporingsteam samengesteld. Wij hebben getracht de schade zo klein mogelijk te houden door te zorgen dat de verdachten geen gebruik meer konden maken van hun server door deze offline te halen. Vervolgens zijn wij bedrijven gaan informeren dat zij slachtoffer zijn geworden, zodat zij intern de schade konden beperken. Pas in een later stadium zijn wij onderzoek gaan doen naar verdachten.

Bij de aanpak van cybercrime levert 'tegenhouden' vaak meer op dan strafrechtelijke vervolging van verdachten. Schadebeperking door dreigingsanalyses over een type malware naar een branche sturen, bijvoorbeeld banksector, helpt bedrijven om hun security policies en mechanisms te verhogen om zo schades te beperken. Naast de eerder genoemde voorbeelden van slachtoffernotificatie kan ook het verstoren van het cybercriminele bedrijfsproces zeer effectief zijn. ■

OPENBAAR MINISTERIE

OPPORTUUN

01

Relatiemagazine van het Openbaar Ministerie - jaargang 22 - februari 2016

Cocaïnesmokkel in de haven

En andere 'zaken met effect'

De verijdelde liquidatie

Theo Hofstee wil rode vlaggetjes bij tikkende tijdbommen