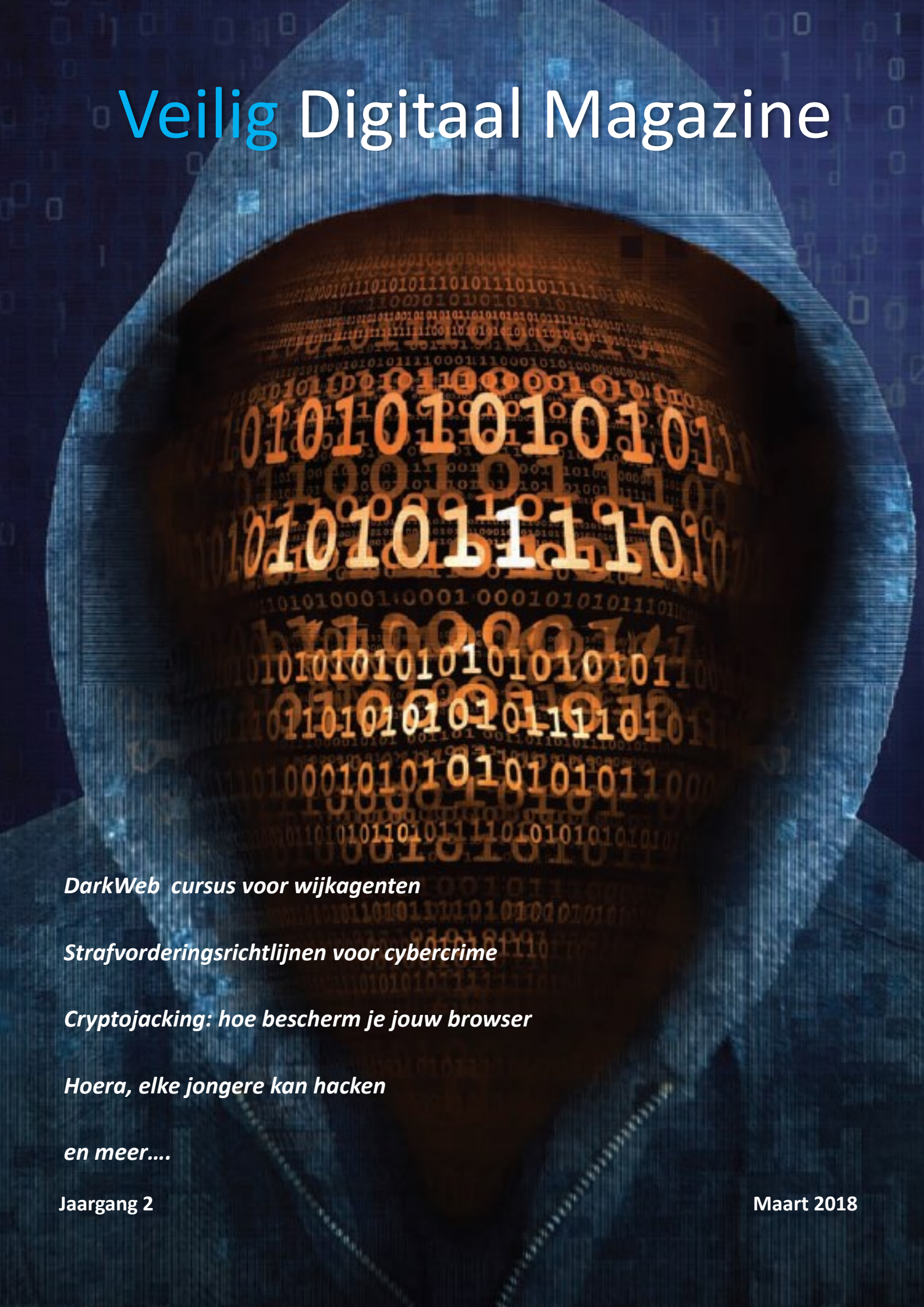
Veilig Digitaal Magazine



DarkWeb cursus voor wijkagenten

Strafvorderingsrichtlijnen voor cybercrime

Cryptojacking: hoe bescherm je jouw browser

Hoera, elke jongere kan hacken

en meer….

Jaargang 2

Maart 2018

INDEX

Veilig Digitaal Magazine is een uit-gave van veiligdigitaal.com

Rubrieken:

Ga naar de Facebookpagina

Ga naar de website

- Cops in Cyberspace
- Rechtspraak
- Verschijningsvorm cybercrime
- Wetsartikel
- Video
- Handig

Van opsporen naar oplossen: dit zijn de hiaten in de cybercrime-strafrechtketen

De politie en het Openbaar Ministerie hebben hun cybercrimedoelstellingen niet behaald. Volgens de minister van Justitie en Veiligheid komt dit door een gebrek aan expertise binnen de regionale politieteams. Met de komst van de regionale cybercrimeteams moet een eind worden gemaakt aan het gebrek aan kennis en expertise en de opsporing van cybercrime verbeteren. Het uitbouwen van deze teams is een stap in de goede richting. Echter, een reconstructie van een hackerzaak toont de hiaten in de cybercrime strafrechtketen.

In 2016 kreeg de Rotterdamse “superhacker” Jair M. een straf opgelegd van 497 dagen, waarvan 360 dagen voorwaardelijk. M. veroorzaakte grote opschudding door in 2013 een vwo-examen Frans online te zetten, dat later gestolen bleek te zijn bij de Ibn Ghaldoun school in Rotterdam. Ook had hij naaktfoto’s van een meisje online gezet.

Volgens het Hof had M. onder meer malware verspreid waarmee hij ongemerkt de besturing van computers van anderen kon overnemen. Hierdoor kon hij gegevens die op die computers stonden downloaden, veranderen of wissen. Ook zorgde door hem verspreide malware ervoor dat bij het opstarten van een besmette computer de webcam automatisch aanging en beelden naar hem verzond. Op deze manier heeft M. honderden mensen bespied en een enorme hoeveelheid computerdata binnengehaald.

Toename cybercriminaliteit, maar onvoldoende kennis en expertise bij politie

De zaak M. is bijzonder omdat hackers niet vaak daadwerkelijk gepakt en veroordeeld worden voor gepleegde daden. Dit jaar maakte het ministerie van Veiligheid en Justitie bekend dat de eigen gestelde doelstelling van het aantal uitgevoerde reguliere cybercrime onderzoeken niet gehaald is. Als reden werd aangegeven dat het de regionale politie-eenheden (basisteams en districtsrecherches) aan kennis en expertise op het gebied van cybercrime ontbreekt.

Om de kennis en expertise van de regionale eenheden te verbeteren moeten daarom aan het einde van dit jaar in alle eenheden cybercrime teams actief zijn. Deze teams gaan helpen met het opbouwen en uitleren van kennis en expertise. Zij gaan de basisteams en districtsrecherche ook ondersteunen zodat zij zelf deze cybercrime onderzoeken kunnen uitvoeren.

Alleen kennis en kunde uitbouwen van de politie is niet genoeg

Het uitbouwen van de kennis en expertise binnen de politie is een mooie doelstelling, maar voor een effectieve aanpak dient niet alleen de politie, maar de gehele strafrechtketen een inhaalslag te maken. Het oppakken van een cybercrime zaak vergt nu eenmaal andere kennis en kunde. De huidige hiaten in deze keten zorgen ervoor dat cybercriminelen makkelijk door het net vallen. Om de keten te verbeteren is het daarom nodig de verschillende schakels beter onder de loep te nemen.

Hiaten in de strafrechtketen: een reconstructie
De zaak van “superhacker” Jair M is een succesverhaal. Echter, daartegenover staan de niet behaalde doelstellingen en diverse kritische uitlatingen in de media door topbestuurders van de politie, OM en Rechtspraak. Waar zitten nou precies de pijnpunten? De beschreven casus leent zich uitstekend om de hiaten in de strafrechtketen te illustreren:

Opnemen van een aangifte
De zaak van M. kwam aan het rollen toen een meisje intieme foto’s van zichzelf op social media zag die zij daar zelf niet heeft geplaatst. Ze meldde zich bij de politie met het vermoeden dat haar foto’s zijn gestolen. Op dat moment is de modus operandi van de dader nog onduidelijk, in tegenstelling tot klassieke misdrijven is bewijs bij cybercrime delicten niet direct zichtbaar.

Het is de taak van de politie om de aangifte op de juiste manier op te nemen waarin duidelijk sprake is van een strafbaar feit en de juiste vragen te stellen zodat er voldoende aanknopingspunten zijn om het onderzoek te starten. Als in de aangifte onvoldoende aanknopingspunten naar voren komt, dan bestaat de kans dat de zaak opzij geschoven wordt voordat er een onderzoek gestart wordt. Kennis over cybercrime en de juridische basis daarvan zijn daarom essentieel voor de frontoffice medewerkers.

Slachtofferhulp
Echter, kennis is niet alleen essentieel voor een goede aangifte. Minstens zo belangrijk is dat deze politiemedewerkers de slachtoffers ter woord kunnen staan. Het is niet ondenkbaar dat slachtoffers zelf niet begrijpen wat er aan de hand is.

De politie zou in staat moeten zijn om de gevolgen van het cybercrime delict te overzien zodat zij burgers kunnen adviseren en op te vangen.

Snelle doorstroming
Voordat de zaak doorgezet wordt naar de recherche wordt de zaak beoordeeld op opsporingsindicatie. Bij onvoldoende opsporingsindicatie wordt de zaak geseponeerd, wat het belang van een gedegen aangifte nogmaals onderstreept.

Als er genoeg aanknopingspunten zijn dan wordt de zaak geprioriteerd en doorgezet naar de recherche. Voordat het onderzoek dus daadwerkelijk begint kan daar al een tijd overheen zijn gegaan, afhankelijk van hoeveel prioriteit aan een zaak wordt gegeven.

In de meeste gevallen worden telefoons, laptops e.d. pas veiliggesteld voor onderzoek als het onderzoek geopend is. Hier bestaat het gevaar dat data verloren gaat als er teveel tijd tussen de aangifte en de start van het onderzoek zit.

Gebrek aan kennis bij de OM en de rechtspraak

In de zaak van M. kon de politie alles direct terugleiden naar zijn computer. Hij had geen maatregelen getroffen om zijn identiteit te verhullen. Dit was een meevaller voor de opsporingsdiensten, zij konden hierdoor relatief eenvoudig zijn identiteit achterhalen zonder uitzonderlijke middelen en kennis. V
olgens Gerrit van der Burg, voorzitter van het college van procureurs-generaal van het Openbaar Ministerie, is het gebrek van kennis binnen het OM en de ingewikkelde encryptie waarmee opsporingsdiensten te kampen hebben één van de grootste problemen om effectief de cybercriminaliteit aan te pakken.

De technologische ontwikkelingen volgen elkaar in een rap tempo op en dat is moeilijk bij te houden, aldus Van der Burg.

Bij de behandeling van de Rotterdamse hackzaak was een forensisch deskundige aanwezig om tekst en uitleg te geven over de werkwijze van de Jair M. Onlangs spraken Christiaan Baardman en Leendert Verheij, raadsheer en president bij het gerechtshof Den Haag zich uit over het gebrek aan kennis van cybercriminaliteit binnen de rechtspraak. Zij pleiten voor een speciale cybercrimekamer zoals die ook bestaat voor belastingzaken.
Cybercriminaliteit verandert continue, aldus Baardman. “Waar een moord een moord blijft, is cybercriminaliteit doorlopend technisch aan het innoveren.” Rechters moeten zich daarom permanent bij laten scholen.

Dit legt een institutioneel knelpunt bloot bij de politie, het OM en de rechtspraak. De aard van klassieke misdrijven zoals vermogensdelicten en geweldsdelicten blijven onveranderd. Daarom bestaat de noodzaak om intensief ontwikkelingen bij te houden en vaardigheden bij te spijkeren niet.
Om cybercrime daders effectief op te sporen, te vervolgen en te veroordelen bestaat deze noodzaak wel en daarbij hoort een omgeving die dat faciliteert en daarvoor de ruimte biedt.

Ketenbrede inspanning
De reconstructie van de zaak Jair M toont aan dat het versterken van de politie als cybercrime fighter niet voldoende is omdat het opsporen van cybercrimedaders slechts de eerste stap is om de dader te stoppen.

Hoewel het goed is dat Justitie en Veiligheid extra inspanning wil leveren om deze bijzondere vorm van criminaliteit aan te pakken, dient de gehele strafrechtketen kennis en kunde op het gebied van cybercrime te vergroten om cybercriminelen effectief te kunnen vervolgen.

Alleen zo kunnen cybercriminelen niet alleen gepakt, maar ook daadwerkelijk aangepakt worden!

Hoe cybercriminelen verdienen aan ransomware

Ransomware verspreiden is een lucratieve business. Maar hoe verdienen cybercriminelen er precies aan? Wij (PCMweb) spraken experts Christiaan Beek van McAfee en John Fokker van het Team High Tech Crime over de verschillende verdienmodellen.

Zowel Fokker als Beek zien dat de opkomst van de bitcoin voor een echte opleving heeft gezorgd in de verspreiding van ransomware. Beek: “Als je kijkt naar de oorsprong van ransomware, dan begon dat in de jaren 80 vooral met concepten. In de jaren 90 evolueerde dat naar iets andere modellen, maar pas toen de bitcoin opkwam kwam ineens dat besef: ‘nu kan ik mijn geld écht anoniem ontvangen’. Dat was echt een keerpunt voor ransomware, en daarmee ransomware-as-a-service.”

De bitcoin is behalve vanwege de anonimiteit ook om andere redenen populair. Het gebruiksgemak van de munt helpt ook mee, denkt Fokker. “Vroeger was cybercrime nog ingewikkeld. Als je bijvoorbeeld in gestolen creditcardinformatie ging handelen moest je zelf kaarten laten drukken, dat was een hoop gedoe en lang niet iedereen kon dat. Met de bitcoin gaat alles geautomatiseerd en hoef je in feite alleen maar een adres in te vullen in het programma dat je koopt, je krijgt automatisch betaald.”

Ook is het veel makkelijker om malware te kopen met bitcoins, want een transactie is zo simpel als het invullen van een bitcoinadres. Dat was vroeger wel anders, toen je je criminele activiteiten nog moest financieren met witgewassen geld – ook niet iets dat voor iedereen was weggelegd. Wie vroeger malware online wilde kopen, moest dat doen met alternatieve betaalwijzen zoals Ukash (een betaalmethode die bekend werd door het Ukash-politievirus, een vroege vorm van ‘scareware’), of met dubieuze overschrijvingen via Western Union.

Anoniem of niet?

Wel denken zowel Beek en Fokker beide dat de bitcoin binnenkort uit de gratie raakt bij malwareverkopers en -verspreiders. Beek: “De bitcoin is behoorlijk anoniem, maar niet honderd procent. Met genoeg moeite kun je wel achterhalen waar een bitcoingebruiker vandaan komt.” Volgens Beek ligt dat echter vooral in de gebrekkige internationale samenwerking, want bitcoingegevens uit een ander land achterhalen is nog lastig.

Beide experts vermoeden dat er in de toekomst andere manieren opkomen om zowel te betalen voor malwarepakketten, als voor het losgeld bij ransomware. Dat kunnen andere cryptovaluta’s zijn of weer andere betaalmethodes, maar er gaat in ieder geval íéts veranderen. Beek: “De opsporingsdiensten investeren steeds meer in bestrijding. Uiteindelijk wordt het niet aantrekkelijk bitcoins te blijven gebruiken.”

Verdienmodellen

Mede door het gemak van de bitcoin is het ook makkelijker om verschillende verdienmodellen toe te passen voor ransomware. Daarbij zien zowel Fokker als Beek van McAfee twee verschillende modellen. Bij één daarvan koop je rechtstreeks een pakket met ransomware en deel je de winst met de maker. Beek: “In de ransomware zit code om de binnengehaalde inkomsten meteen te verdelen tussen twee bitcoinadressen. De verspreider krijgt dan 70 procent, de maker de overige 30. Dat is zeker voor de maker aantrekkelijk, want die heeft vrijwel geen omkijken meer naar de campagne én hij loopt bijna geen risico.”

Het huidige populairdere model blijkt echter vooral het huren van een command-and-control-server te zijn. Daarbij kun je als koper een pakket afsluiten waarbij je voor een bepaalde periode een server huurt om de ransomwareverspreiding te doen. Hoe langer je die server huurt, hoe meer je betaalt. In zulke gevallen ligt het risico voor een groot deel ook juist bij de server-aanbieder, maar volgens Beek is het steeds makkelijker die anoniem te houden. “Als je het goed doet wordt je niet zomaar gepakt. De makers van malware zijn vaak slim genoeg zich goed verborgen te houden.”

Affiliate-programma's

Er is nog een ander populair model, maar dat is vooral weggelegd voor serieuzere criminelen, dat volgens Fokker ook meer op georganiseerde misdaad lijkt met grote bendes. Het zijn de zogenoemde affiliate-programma’s. Je moet je daar als crimineel op ‘inkopen’, door een vast bedrag per maand te betalen. Daarmee worden de c&c-servers betaald, maar wordt er ook gezorgd voor genoeg beveiliging en anonimiteit voor zowel de makers als de verspreiders.

Bij zo’n affiliate-model is je reputatie erg belangrijk. Ironisch genoeg kijken de makers naar hoe betrouwbaar de kopers zijn. Fokker: “Je moet vaak je skills kunnen aantonen als koper, zodat iedereen zeker weet dat de pakkans kleiner wordt omdat er dan geen fouten worden gemaakt.” Die vraag naar reputatie lijkt gek, maar dat is wel één van de belangrijkste redenen waarom ransomware ook werkt. Wanneer een bende bereid is bestanden inderdaad te ontcijferen nadat iemand betaalt, zijn in de toekomst méér slachtoffers bereid geld neer te leggen voor die ransomware.

Kat in de zak

Als je te maken hebt met criminelen neem je altijd risico’s. Het kopen van malware of ransomware gaat daarom nooit gegarandeerd goed, zoals Beek ook ontdekte toen hij een nieuwe vorm van ransomware-as-a-service ontdekte. “We kochten het voor onderzoek, maar toen we niks kregen en contact opnamen met de verkopers kregen we niets meer te horen.” Reputaties op darkweb-marktplaatsen zijn daarom belangrijk, maar zelfs dan weet je nooit zeker of je een fatsoenlijk product koopt – en geloof maar niet dat je dan bij iemand kunt aankloppen voor hulp.

Deze 3 cybercrimeontwikkelingen zijn zorgwekkend

Steeds meer (overheids)organisaties zijn zich bewust van de risico's van cybercrime zoals ransomware en DDoS-aanvallen. Cybercriminelen ontwikkelen daarom continu nieuwe aanvalsmethoden. Dit zijn de meest opvallende trends volgens Erik Remmelzwaal, directeur bij DearBytes.

1 Traditionele identificatie werkt niet meer.
Een inlog met gebruikersnaam en wachtwoord is vandaag de dag niet meer genoeg om gevoelige gegevens af te schermen. Zeker niet voor politici en CEO's. Zo heeft John Podesta, de campagneleider van Hillary Clinton, laten zien wat de gevolgen zijn. De Russische hackersgroep Fancy Bear ontfutselde hem zijn Gmail-inloggegevens. Hierdoor kwam een grote hoeveelheid vertrouwelijke e-mailberichten op straat te liggen.

Tweefactorauthenticatie wordt veelal als een oplossing gezien bij dit soort situaties. De gebruiker voert tijdens het inloggen iets in wat hij weet (zoals een wachtwoord) en iets wat hij heeft (zoals een sms-code). Deze methode biedt echter in vele gevallen schijnveiligheid. De veiligheid is namelijk erg afhankelijk van de betrouwbaarheid van het tweede identificatiemiddel.

Zo kondigde Google het afgelopen jaar aan dat high value targets, zoals bekendheden en CEO's, voorzien worden van een hardwaretoken als authenticatiemiddel. "Dat doen zij niet zomaar", concludeert Remmelzwaal. "Blijkbaar bieden softwarematige varianten zoals sms of Google Authenticator onvoldoende zekerheid om hun identiteiten vast te stellen."
Remmelzwaal voorziet een trend dat hardwaretokens voor veel toepassingen weer de standaard worden bij tweefactorauthenticatie. "Een embedded chip op een USB-token of een SIM-kaart zijn moeilijker te manipuleren. Het niet kunnen overleggen van deze identificatiemethode zou in de toekomst zomaar direct gevolgen kunnen hebben voor compliance. Bijvoorbeeld bij de bescherming van speciale persoonsgegevens."

2 Van losgeld naar destructie
De tijd dat cybercriminelen het uitsluitend hadden voorzien op het stelen van inloggegevens en persoonlijke informatie lijkt voorbij. "We zien nu de eerste gevallen van wat we inmiddels Destruction of Service ofwel DeOS noemen", zegt Remmelzwaal.

“Bij een DeOS-aanval gaat het de criminelen niet zozeer om het stelen van persoonlijke gegevens, maar vooral om het volledig onbruikbaar maken van data of zelfs complete applicaties.”
“Bij ransomware zien we dat de gebruiker na betaling van enkele bitcoins soms weer toegang krijgt tot zijn versleutelde gegevens. In het geval van Destruction of Service zijn de criminelen er doelbewust op uit om deze data voorgoed te vernietigen. Daarnaast willen ze vaak de software uitschakelen.”

De Petya-uitbraak in juni 2017 was een goed voorbeeld van een DeOS-aanval. In eerste instantie leek het te gaan om een ransomwareaanval, maar al snel werd duidelijk dat vernietiging het primaire doel was. Het was de aanvallers te doen om verstoring van bijvoorbeeld de energievoorziening, het betalingsverkeer en de luchtvaart. “Door Petya weten we nu eindelijk hoe een cyberwar eruitziet”, aldus Remmelzwaal.

3. Infiltreren criminelen in opensourceprojecten?
We hebben de afgelopen jaren een enorme groei gezien in het gebruik van opensourcesoftware. Een toename in het aantal cyberaanvallen op bekende opensourceproducten is dan bijna onvermijdelijk. Maar we lopen volgens Remmelzwaal ook een heel ander en veel minder bekend risico. “Het risico bestaat dat cybercriminelen als programmeur of tester infiltreren in een opensourceproject. Daar moeten we alert op zijn.”
Bovendien moeten we bekijken of het nog wel voldoende is dat alle deelnemers aan een opensourceproject de broncode van de software controleren op fouten. Remmelzwaal: “Zij moeten namelijk niet alleen kijken naar technische fouten en bugs, maar ook achterhalen of bepaalde programmatuur kan worden misbruikt voor criminele doeleinden. Het is bijvoorbeeld niet ondenkbaar dat cybercriminelen een functie voor het versturen van gegevens gebruiken om juist een virus toe te voegen aan diezelfde data.”

“Gelukkig zien we dat mensen zich meer en meer bewust worden van de maatregelen die zij moeten nemen om online veilig te zijn”, zegt Remmelzwaal. “Helaas zien cybercriminelen deze ontwikkeling ook. Zij zoeken daarom continu naar nieuwe mogelijkheden om aanvallen uit te voeren. Vandaar dat je aan de ene kant natuurlijk moet blijven proberen misbruik te voorkomen. Van de andere kant moet je er altijd van uitgaan dat je gehackt wordt of al bent, waardoor monitoring belangrijk blijft. Ofwel mijn tip voor 2018: assume compromise.”

Cryptojacking:
hoe bescherm je je browser tegen ongewenst mijnen?

Vorig jaar september was het een verhaal: The Pirate Bay had in het geniep een script geïnstalleerd om bezoekers de cryptovaluta Monero te laten genereren terwijl ze op zoek waren naar de nieuwste torrents. Op die manier kon de site iets van inkomsten genereren. Advertenties worden massaal geblokkeerd, dus dit was een alternatieve manier om iets te verdienen.

De trend in de laatste paar maanden heeft laten zien dat steeds meer websites en zelfs Android apps deze methode wel zien zitten. Het heeft inmiddels ook al een naam: cryptojacking. Tijd om je er tegen te wapenen dus.

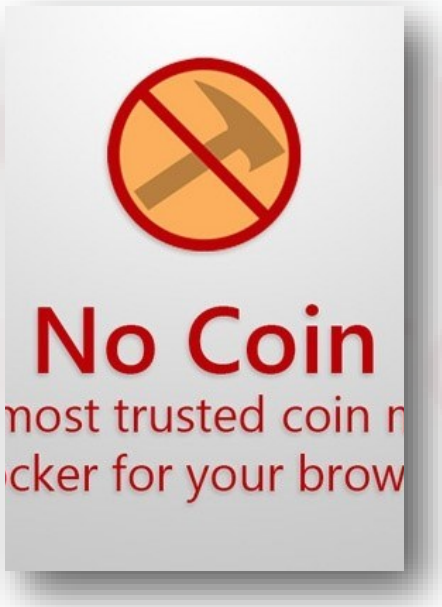
Wat kan ik doen?
Als je al gebruik maakt van een adblocker kun je die zo instellen dat de sites waar de mijn-scripts op staan geblokkeerd worden. Voor Adblock Plus (en vermoedelijk ook voor andere adblockers) kun je een eigen filter instellen voor deze term:
||coin-hive.com/lib/coinhive.min.js

Als je Chrome als browser gebruikt kun je de Coin-Hive Blocker extensie downloaden en dan is het ook geregeld. Opera doet het nog beter: die hebben in hun aanstaande versie bij de security-lijstjes in de voorkeuren ook 'NoCoin' staan en door die aan te zetten ben je ook automatisch beveiligd. Sowieso een goede browser, trouwens.

Let wel: dit zijn allemaal varianten op dezelfde methode, namelijk het blokkeren van het pad richting Coinhive. Als iemand een andere variant maakt die ergens anders heen gaat moet dat gat ook weer gedicht worden.

Bad Android
Voor Android apps is het iets lastiger, want die doen het nóg stiekemer. De apps in kwestie openen een onzichtbaar browservenster in de achtergrond om te gaan mijnen. Daar ben je echt afhankelijk van mensen die doorzien wat er gebeurt en een snelle reactie van Google om dit soort apps te verwijderen.

Oppassen met wat je downloadt dus. Het enige 'voordeel' is dat het resultaat van een app of site die dit doet zich vrij snel vertaalt in fysieke issues aan je computer of telefoon: staat je laptop uit het niets op het punt om op te stijgen? Is je telefoon ineens wel heel snel leeg? Dan zou je wel eens goed met een cryptohacking site of app te doen kunnen hebben. Hou het in de gaten en bescherm jezelf, want als je dan toch belachelijk veel stroom wilt verspillen aan het mijnen van cryptogeld, doe het dan in elk geval voor jezelf.



Hoera, elke jongere kan hacken

De toekomst is ICT-gedreven, door jong en oud. We zijn qua nuttige skills dus voorbij computer- en internetgebruik en zetten volgende stappen: mediawijsheid, digiveiligheid en hacken.

Jongeren die software ontwikkelen zijn in wezen ook hackers; zij stoeien met softwarecode. Zij maken nieuwe apps, zij zorgen voor innovatie. Maar er is ook een schaduwkant. Er is namelijk een subtiele overgang van hacker naar cracker, van beveiliging aan de tand voelen naar beveiliging misbruiken, van wit naar zwart.

Interpol waarschuwt de wereld voor een trend die wij bij Kaspersky Lab ook zien: het wordt steeds gemakkelijker en jongeren lopen voorop. Computers, smartphones en apps, maar ook hackmiddelen worden steeds gebruiksvriendelijker. Elke beginneling kan zó een gevorderde worden. Bovendien is het cool.

Hacken is cool

Mediawijze, tech-savvy jongeren zien dat de wereld draait om ICT en dat zij met hacken daarin groot kunnen worden. Bijvoorbeeld door met overtuigende nepmails wachtwoorden van leraren buit te maken. Wie is er op school cooler dan degene die elke onvoldoende kan veranderen in een voldoende?

Cracken is uncool

“Voor jongeren is het een statussymbool geworden om op computers in te breken”, constateert Interpol-topman Christophe Durand. De belangrijke nuance is dat het bij cybercriminelen gaat om gewin, maar bij jongeren om de kick en de status. Zij en mensen in hun omgeving lopen echter het risico van de subtiele overgang; van hacker naar cracker. Digitaal kattenkwaad kan zó uit de hand lopen.

Vele ouders zullen het al wel weten: verbieden is niet de oplossing. Bovendien bestaan er al vele verboden: wetten en regels die computerinbreken strafbaar stellen. Politie, Justitie en Interpol pakken dit streng aan. Tegelijkertijd moeten wij als leraren, ouders, vrienden, ICT-beveiligingsdirecteuren, kortom: leden van de maatschappij, ook optreden. Door te sturen op moraal en ethiek.

Oudercoaching

Nieuwsgierige jongeren hebben waarschijnlijk geen hulp nodig voor de ontwikkeling van hun tech-skills. Wel kunnen ze richting gebruiken voor goed en fout, voor white hat hacking versus black hat hacking en de grijstinten daartussen. Want digitaal kattenkwaad of fouten uit het verleden kunnen je flink opbreken in de toekomst. Ook nadat je je skills hebt ingezet voor goed. Hoera, elke jongere kan hacken … help!

Klanten kleine banken makkelijker slachtoffer phishing-aanvallen

Hoe lang worden we met zijn allen al gewaarschuwd voor phishing-aanvallen? We internetbankieren inmiddels al 20 (!) jaar maar de situatie waarin eigenlijk iedereen online zijn zaken doet is pas iets van de laatste vijf jaar. Dan spreekt het vanzelf dat het aantal phishing-aanvallen vanzelf toeneemt, want er is geen sappigere prijs dan iemands bankgegevens.

Alle campagnes van de overheid en banken ten spijt blijven de criminelen het online proberen en stijgt het aantal phishing-aanvallen nog steeds elk jaar. Daar komt nog eens bij dat mensen net zo goed opletten bij phishing-mails dan ze doen bij die campagnes, want de valse mails worden ook nog eens nauwelijks herkend.

Ook recent was het weer raak: klanten van internetbank Knab lieten zich foppen door een valse website die hun inloggegevens doorsluisde, waarna criminelen hun rekening plunderden, zo blijkt uit onderzoek van Trouw. Inmiddels is het geld terug overgemaakt naar de mensen, maar het was wel even schrikken voor de online bank.

Het opvallende was dat de klanten gewoon 'knab' gegoogeld hadden en dat er toen een Google advertentie naar boven kwam met de tekst 'inloggen Knab'. Die verwees weer door naar een nagemaakte inlogpagina van de bank (mét groen HTTPS slotje) en zo werden de klanten misleid. Het clevere was dat de criminelen de klanten na een aantal pogingen (toen zij al in de rekening zaten) alsnog lieten inloggen en daarna vanwege een 'onregelmatigheid' verificatiestappen lieten doorlopen, die eigenlijk de verificatie was voor het overmaken van duizenden euro's naar een andere bankrekening.
Dit houdt nooit op

Voor Knab was dit een verrassing, maar dat zou het niet mogen zijn. Elke partij die veel geld beheert voor klanten zal slachtoffer van phishing worden, ook al zijn ze relatief klein. Sterker nog: de kans dat je met phishing wordt geconfronteerd als klant is bij een kleine partij misschien nog wel groter, want de cybercriminelen weten dat de bescherming tegen dit soort fraude bij een kleiner bedrijf nooit kan tippen aan wat een ABN of Rabobank kan doen.

Daarnaast speelt ook mee dat we als consument steeds makkelijker gaan geloven dat ons niks kan gebeuren. Dan helpt het ook niet dat bijvoorbeeld een https-verbinding met een groen slotje zo makkelijk te krijgen is voor elke webpagina dat je daar ook niks meer aan kunt afzien.

Geen omwegen
Het enige dat echt werkt is dat je nooit maar dan ook nooit via andere wegen naar je bank gaat dan direct. Gebruik de app die je bank verstrekt of ga direct naar de webpagina van je bank. En dan niet direct in de zin van drie letters in je zoekbalk gooien en op het bovenste resultaat klikken. Google is inmiddels zo ver heen dat als je op ABN zoekt het bovenste resultaat een advertentie is en dat dan pas de url die je intypte er staat. Blijven opletten dus,

Activiteit op zwarte markt voorspelt cyberaanval

Cybercrime is tegenwoordig een zakelijke wereld, compleet met ecosystemen, vertrouwen, eerlijke handel en marktwerking. De TU Eindhoven (TUe) heeft empirisch bewijs gevonden van de directe correlatie tussen marktactiviteit op de cybercrimemarkt en het risico op daadwerkelijke cyberaanvallen.

Universitair docent Luca Allodi heeft uitgebreid onderzoek gedaan naar de economische aspecten van cybercrime. Hiervoor is hij geïnfiltreerd in een grote zwarte cybermarkt, die volgens de TUe één van de belangrijkste Russische cybercrimemarkten uit de ondergrondse wereld is. Het door Allodi uitgevoerde onderzoek omvat zeven jaar aan gegevensverzameling en uitgebreide analyse hiervan.

Vraag, aanbod en inzet

Deze jarenlange analyse van de economische en organisatorische principes heeft inzichten opgeleverd over handel in en gebruik van exploits. Informatie over kwetsbaarheden plus aanvalscode om die uit te buiten, worden namelijk niet zomaar verhandeld. Vraag en aanbod spelen een rol op ondergrondse markten, met daarbij ook een relatie naar de inzet van exploits.

Zo blijkt er dus een onderbouwde link te leggen tussen de marktactiviteit rond bepaalde exploits en beoogd gebruik daarvan. Dit komt dus neer op de uitvoering van cyberaanvallen. Het monitoren van exploitprijzen en de verhandeling geeft dus indicatoren voor aankomende aanvallen.

Pro-actieve tegenmaatregelen

Er bestaat een kwantitatieve relaties tussen de ‘populariteit’ van een exploit op de cybercrimemarkt met het daadwerkelijke gebruik van de betreffende exploit, legt de TUe uit in een persbericht. “De analyse heeft onderzoekers voor het eerst in staat gesteld het veranderende risico op cyberaanvallen te voorspellen, gebaseerd op waargenomen (of potentiële) marktactiviteit op een cybercrime markt”, aldus de Technische Universiteit.

Bovendien kan deze verbetering voor risico-inschatting praktisch neerkomen op concrete, defensieve tegenmaatregelen. “Dit kan softwareontwikkelaars, beleidsmakers en eindgebruikers helpen om efficiënter middelen toe te wijzen aan het beheer van 'cyberrisico', door bijvoorbeeld de relatie te kwantificeren tussen kwetsbaarheidskenmerken en de kans op cyberaanvallen.

Marktwerking en eerlijke handel

Verder levert het onderzoek van Allodi ook inzichten op over de economie van cybercriminaliteit. De onderzoeker heeft bijvoorbeeld ontdekt dat de ondergrondse prijzen voor exploits vergelijkbaar zijn met de beloningen bij bovengrondse premieprogramma's voor het verantwoord melden van kwetsbaarheden.

De zogeheten bug bounty programma's van ICT-leveranciers en ook ICT-gebruikende organisaties blijken dus te concurreren met de zwarte markt. "Dit kan als gevolg hebben dat de cybercrime markten programmeertalent wegtrekken van de legitieme markt", merkt de TUe op.

Opvallend is ook dat er sprake is van eer en eerlijkheid in het criminele circuit. Eerlijke handel staat daar hoog in het vaandel. Dit uit zich onder meer in het werken met officiële koopovereenkomsten tussen koper en verkoper. Hierbij kunnen kopers van exploits vaak proefversies gebruiken om de aangeboden waar te testen.

Eigen berechting van oplichters

Daarnaast worden oplichters binnen de cybercrimewereld berecht via een openbare rechtszaak met rechters, getuigen en bewijsmateriaal. "Allemaal kenmerken die een solide basis bieden voor handel en technologische innovatie", concludeert de TU Eindhoven.

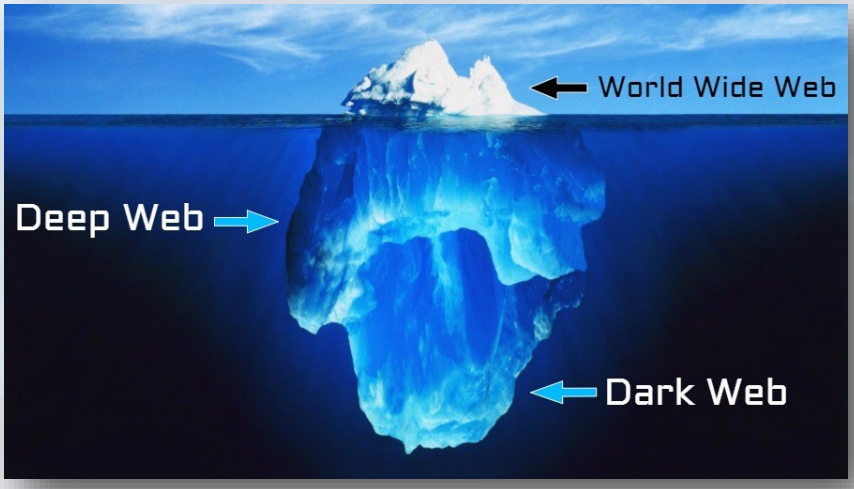
Dark-webopleiding voor wijkagenten in de maak

Het Cyber Science Center van de NHL werkt aan een dark-webopleiding die geschikt moet zijn voor alle politiemensen.

Volgens lector Wouter Stol is dat absolute noodzaak. ‘Agenten moeten ook hun digitale vaardigheden op peil gaan houden. Wie in opleiding is tot wijkagent, wordt amper onderwezen over online criminaliteit’. En dat het dark web ‘exclusief terrein is van gespecialiseerde digitale recher-cheurs’, is volgens hem onzin.

‘Als een wijkagent niet weet hoe het dark web werkt, wordt hij uitgela-chen. Feitelijk is het dark web gewoon onderdeel van zijn wijk’. De oplei-ding moet ook geschikt zijn voor agenten in andere landen – waar het dark web bij de politie net zo onbekend is. De NHL werkt in het project ‘Police Detectives on the TOR network’ samen met onder meer Zweden waar ze de technische kant van de opleiding ontwikkelen.

Volgens criminoloog Bram Emmen, betrokken bij het project, is het dark web ‘uiterst saai, voor wie niet weet waar hij moet beginnen’, maar is lang niet alles er illegaal. Politiechef Max Daniel zegt in het artikel dat hij de training niet wil inpassen in de huidige IBT. ‘Wat moet daar dan plaats voor maken? Schieten?’



Bron: CSC

“Wie kinderporno zoekt, moet op YouTube zijn”

Kinderrechtenorganisatie Child Focus spreekt van ‘grijzezonekinderporno’, die gewoon op YouTube staat.

Die videosite is door pedoseksuelen ‘gekaapt’ en in gebruik ‘als uitstalraam’. De filmpjes zelf zijn uiteraard niet strafbaar, maar wie contact opneemt met de beheerders van zulke accounts, kan het verboden materiaal in handen krijgen, bevestigt Yasmin van Damme van Child Focus.

‘Je vraagt je af waarom de filmpjes 8 tot 10 miljoen views hebben, tot je naar de comments scrolt. Daar lees je werkelijk het vunzigste dat je kunt bedenken’.

De Engelse krant The Times ging undercover op zoek en vond onder meer een Braziliaanse account waarop onschuldige kinderfilmpjes stonden. Maar in een mailtje beloofde de beheerder maar liefst 315 gigabyte aan kinderporno.

Andere accounts bleken door te linken naar versleutelde chatdiensten als Telegram. Van Damme zegt dat Youtube veel te weinig doet om dit tegen te gaan. Als ze namens Child Focus, zelf ‘trusted flagger’, een filmpje aanmerkt als illegaal, gebeurt er vaak niks. ‘Er is een totaal gebrek aan transparantie’.

Pedofielen delen massaal (Nederlandse) kinderfoto's op openbare Russische site

Via een openbare Russische website Image Search zouden pedofielen wereldwijd 'miljoenen' foto's uitwisselen die afkomstig zijn van facebook, instagram en andere sociale media.

De onderzoeksredactie van RTL Nieuws zegt dat in deze 'schimmige ruilhandel' van kinderfoto's ook Nederlandse kinderen betrokken zijn. Onderzoeker Sijmen Ruwhof schrijft op zijn eigen site dat de Russische site maar liefst drie miljoen foto's bevat.
Het overgrote deel daarvan zijn onschuldige vakantiefoto's maar die worden op de site wel voorzien van seksueel getinte titels als 'Cute 15yo dutch girl, nice boobs' of 'super hot Dutch boy'.

Commentaren op de foto's zijn vaak expliciet; gebruikers wisselen e-mailadressen uit en worden aangespoord méér materiaal te sturen. Ruwhof noemt het opvallend dat zulke sites in alle openheid blijven bestaan. 'Het is zó toegankelijk dat ik daar heel erg van schrik'. Naar zijn schatting zijn er enkele honderden foto's van Nederlandse kinderen te vinden.
Een moeder van een daarvan zei tegen RTL dat de foto's van haar facebookpagina gepikt zijn. 'Het is verschrikkelijk dat onschuldige foto's op deze manier worden misbruikt'.

Volgens de Nederlandse politie is er tegen de site nog niks gedaan vanwege capaciteitsgebrek. Landelijk coördinator Kinderporno en Kindersekstoerisme Ben van Mierlo zei tegen RTL Nieuws dat het bij zulke sites altijd de vraag is wat onderzoek oplevert. 'Kunnen we die energie dan niet beter stoppen in zaken waarvan we op voorhand vermoeden dat daar actueel misbruik speelt'.

Directeur Arda Gerkens van het meldpunt Kinderporno zegt iets vergelijkbaars. 'Ze doen geen strafbare dingen onder de Nederlandse wetgeving, ook al vinden wij dit erg onwenselijk en onsmakelijk'. In het verleden, ontdekte RTL verder, zijn individuele gebruikers van de site wel vervolgd en veroordeeld.

Bitcoin te transparant voor criminelen

Waar de investeerder dus wel brood ziet in bitcoin, stappen criminelen over op andere cryptomunten, meldt persbureau Bloomberg. De reden: opsporingsdiensten worden steeds beter in het volgen van transacties met bitcoin. Het gevolg daarvan is dat criminelen overstappen op andere cryptomunten waarschuwde Europol in oktober van vorig jaar.

Dat geldt bijvoorbeeld voor monero, die volgens data van Coin Market Cap in twee maanden tijd van zo'n 90 dollar steeg naar de huidige koers van 390 dollar. Dat is een relatief grotere stijging dan die van bitcoin in dezelfde periode.

Monero anoniemer dan bitcoin
Dat criminelen deze munt kiezen in plaats van de bitcoin heeft te maken met de manier hoe beide cryptomunten zijn ontworpen. Omdat iedere transactie met een bitcoin wordt opgeslagen op de blockchain, kunnen opsporingsdiensten die data gebruiken als bewijsmateriaal.

De monero is juist ontworpen om de gebruikers zo veel mogelijk privacy te geven. Het adres van de ontvanger wordt versleuteld opgeslagen op de blockchain en de monero creëert meerderde valse adressen om de verzender af te schermen. Ook wordt het overgemaakte bedrag versluierd.

Monero is een digitaal betaalsysteem op basis van blockchain technologie en tevens een cryptocurrency. De cryptomunt (XMR) onderscheidt zich van andere cryptovaluta's door 100% financiele privacy te bieden en transacties onherleidbaar op te nemen in de blockchain.

Monero is een innovatieve blockchain technologie welke het mogelijk maakt voor gebruikers om betalingen verrichten zonder dat informatie over de verzender, ontvanger of de transactie zelf verhuld wordt. Daarmee kunnen eigenaren van de XMR cryptovaluta hun eigen bank zijn en zodoende hun financiele privacy waarborgen.

De digitale valuta XMR is velig, prive en ontraceerbaar. Net als Bitcoin en bijna alle andere altcoins, maakt XMR gebruik van blockchain om een decentraal betaalsysteem te faciliteren. Normaal gesproken bieden cryptocurrencies echter slechts een bepaalde mate van privacy, omdat in een blockchain informatie over transacties publiek beschikbaar is.

Dat betekent dat iedereen die dat wilt in een blockchain kan zoeken naar een bepaalde transactie, de waarde van de transactie kan achter halen en op basis van het wallet adres kan traceren wie de verzender was en wie de ontvanger.

Met Monero wordt deze informatie echter prive gemaakt. Wie de XRP blockchain bekijkt, kan zodoende nooit achterhalen wat de afkomst, bestemming en inhoud van een transactie was.

Daarvoor maakt Monero gebruik van een speciale techniek genaamd “Ring Signatures”, welke de publieke encryptiesleutels van gebruikers door elkaar haalt. Doordat meerdere publieke sleutels (Public Keys) van diverse gebruikers door meerdere “ringen” gaan in de blockchain, zijn transacties niet meer te traceren c.q. herleiden.

Het Monero platform wordt momenteel voornamelijk gebruikt als decentraal betaalsysteem, maar kan ook worden gebruikt om andere vormen van informatie uit te wisselen op een veilige en onherleidbare manier.
De onderliggende technologie en cryptografie kan bijvoorbeeld worden ingezet om vertrouwelijke data geheim te houden, bijvoorbeeld om Internet-of-Things apparaten en de tussenliggende communicatie te beveiligen.

Monero is in 2014 gelanceerd en heeft sindsdien een belangrijke positie ingenomen in de cryptocurrency markt.

De schaalbaarheid van de cryptomunt en de manier waarop het decentrale betaalsysteem de privacy van de gebruikers waarborgt, geeft de valuta een aanzienlijke waarde.

De anonimiteit van Monero maakt XMR ook populair op het Darknet: mensen kunnen elkaar daar betalen voor mogelijk illegale goederen of diensten, zonder dat de transacties getraceerd kunnen worden.

Wpa3 gaat draadloze netwerken beter beveiligen

De Wi-Fi Alliance, de organisatie achter de wifi-standaard, heeft bekendgemaakt dat de beveiliging van draadloze netwerken verbeterd wordt. De huidige beveiliging wpa2 wordt opgevolgd door wpa3 dat ook zonder wachtwoord bij open netwerken encryptie biedt.

De Wi-Fi Alliance heeft op elektronicabeurs CES bekendgemaakt dat de wpa2-beveiliging wordt opgevolgd door wpa3. De Wi-Fi Alliance heeft vier verbeteringen ten opzichte van het huidige wpa2 bekendgemaakt.

Altijd versleuteling
Een van de manieren waarop wpa3 veiliger is ten opzichte van het huidige wpa2 is dat ook gebruikers van een open netwerk een versleutelde verbinding met ieder een unieke sleutel krijgen. Hierdoor kan verkeer uit de lucht niet langer afgeluisterd worden. Uiteraard is je verkeer eventueel nog wel inzichtelijk voor de beheerder van het netwerk of andere gebruikers, dus zorg ervoor dat gevoelig verkeer altijd extra beveiligd is via bijvoorbeeld een versleuteld protocol of vpn-dienst. Dat is niet de enige verbetering. Zo zou Wpa3 zou ook veilig moeten zijn als gebruikers korte niet complexe wachtwoorden gebruiken. Daarnaast moet wpa3 eenvoudiger te gebruiken zijn op apparaten zonder scherm. Tot slot wordt 192bit-encryptie toegevoegd voor gebruikers met heel hoge eisen zoals de overheid en defensie.

Wpa3 moet in 2018 in producten verschijnen. De introductie van wpa3 betekent overigens niet dat wpa2 niet meer ondersteund wordt. De Wi-Fi Alliance zegt dat het wpa2 ook in de toekomst blijft verbeteren.

Geen overbodige luxe, denk bijvoorbeeld aan de KRACK-kwetsbaarheid die vorig jaar ontdekt werd.

Wat beweegt een computercrimineel?

Het verschil tussen een computercrimineel en een straatrover is duidelijk. Marleen Weulen Kranenbarg promoveerde erop aan de VU.

Zijn drijfveren om te hacken waren „intellectuele nieuwsgierigheid en het najagen van kennis en avontuur", zei Kevin Mitnick in 2011 tegen The Huffington Post. „Het ging mij nooit om geld stelen of kwaadaardige software schrijven."

Mitnick is een van de beroemdste ex-computercriminelen. Toen de FBI in 1992 huiszoeking bij hem deed, stond een doos donuts klaar. 'FBI-donuts' stond erop. Mitnick had de telefoons van de dienst gehackt en een alarmsysteem gemaakt voor als ze in de buurt waren. Uiteindelijk zat hij vijf jaar in de cel.

Nieuwsgierigheid, Mitnicks reden om te hacken, is vaak de belangrijkste motivatie voor computercriminaliteit. Dat blijkt uit onderzoek van criminoloog Marleen Weulen Kranenbarg (27). Ze promoveert deze week aan de Vrije Universiteit in Amsterdam op de verschillen tussen traditionele boeven en computercriminelen.

Het klinkt als een excuus in de rechtszaal: hacken uit nieuwsgierigheid, niet om het geld. Weulen Kranenbarg: „In de rechtszaal heb je een goede reden om je zo te verantwoorden, maar jaren na je misdaad in mijn geanonimiseerde enquête is dat minder. Computercriminelen noemden – in tegenstelling tot 'normale' criminelen – minder vaak financiële redenen voor hun gedrag. Als belangrijkste motivatie voor hacken en verspreiden van malware, kwaadaardige software, zeiden ze dat ze nieuwsgierig waren en iets wilden leren. Hacken gebeurt ook vaak om een boodschap over te brengen. Aanvallen die een site platleggen worden bijvoorbeeld gedaan om te pesten."

Volgens justitie kraakte een Leeuwarder meer dan honderd persoonlijke socialemedia-accounts. Hij deed zich voor als websitebouwer en onderschepte zo wachtwoorden. Is hij een typische computercrimineel?
„Werken in de IT-sector kan de kans op computercriminaliteit verhogen. Werk hebben verlaagt de kans op computercriminaliteit niet. Bij gewone criminaliteit is dat juist wel zo."

Zijn er meer verschillen?
„De computercrimineel is gemiddeld enkele jaren jonger, is net wat vaker Nederlands van afkomst en doet vaker een opleiding dan de traditionele boef. Een opleiding volgen kan zelfs de kans op computercriminaliteit verhogen. Deze criminelen nemen vaker een voorbeeld aan een ouder iemand, terwijl traditionele boeven meer opkijken tegen leeftijdgenoten. Het is een herkenbaar beeld: vrienden die elkaar op straat de criminaliteit in trekken."

Moet de criminologie zich opnieuw uitvinden door de groeiende groep computercriminelen?
„Traditionele voorspellers voor criminaliteit – geen werk, foute leeftijdgenoten – zijn niet of nauwelijks van toepassing op cybercriminelen. Daarom moeten verklaringen en interventies die gestoeld zijn op traditionele criminaliteit worden geüpdatet."

Slimme analyse van Alphabet-dochter bestrijdt cybercrime

Google's moederbedrijf Alphabet krijgt een nieuwe dochter Chronicle, dat bedrijven gaat helpen bij het detecteren en bestrijden van cyberaanvallen. Het bedrijf bestaat uit twee delen, schrijft CEO Stephen Gillett van Chronicle in een blog. Het ene is een nieuw intelligent analyseplatform dat beveiligingsdata gebruikt voor cybersecurity, en het andere deel is malware-analysedienst VirusTotal dat Google in 2012 aankocht.
Volgens Gillett hebben bedrijven moeite om de grote hoeveelheden data die ze op het gebied van beveiliging vergaren goed in te zetten. Potentiële aanwijzingen van activiteiten die wijzen op hackaanvallen worden daardoor nu over het hoofd gezien en weggegooid, schrijft hij. “Het aantal cyberdreigingen groeit harder dan beveiligingsteams en budgetten aankunnen, en er is een enorm tekort aan talent. De enorme toename van data van de tientallen securityproducten die een gemiddeld groot bedrijf gebruikt, maakt het – paradoxaal – moeilijker en niet makkelijker om dreigingen te vinden en te onderzoeken.”

Machine learning

Het nieuwe dataplatform maakt gebruik van dezelfde infrastructuur waar ook andere initiatieven van Alphabet op draaien. Daardoor kan Chronicle klanten veel rekenkracht en opslag bieden, zegt Gillett. Ook machine learning technieken die eveneens door andere Alphabet-dochters worden gebruikt, worden door Chronicle aangeboden aan klanten.
Het bedrijf kan, zo schrijft Gillett, een zoekopdracht en analyse binnen enkele minuten uitvoeren in plaats van de gebruikelijke uren of dagen. En omdat de data goedkoop en makkelijk opgeslagen kan worden, valt ook historische data nog te gebruiken voor de analyse en herkenning van patronen.

X-project

Het cybersecuritybedrijf komt voort uit Alphabets onderzoeksdochter X, dat experimentele projecten uitvoert. Sommige daarvan lijken vergezocht; de zogeheten Moonshots. Bij X is in februari 2016 de basis gelegd voor Chronicle. Er zijn inmiddels verschillende beveilingingsexperts betrokken bij dit nieuwe Alphabet-bedrijf. Dit zijn onder meer: Mike Wiacek en Shapor Naghibzadeh uit het beveiligingsteam van Google en Bernardo Quintero, de oprichter van VirusTotal. VirusTotal is een gratis online service die malware analyseert of deze al bekend is bij antivirusmakers of websitescanners.

Cybercrime via facturen: oude wijn in nieuwe zakken

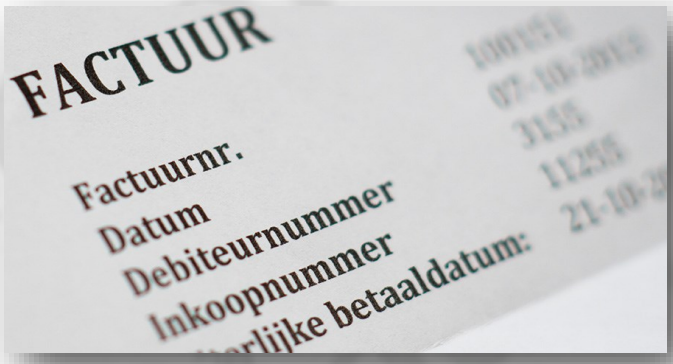
Voortdurend verzinnen criminelen nieuwe manieren om te knoeien met facturen en zo geld te verdienen over de rug van organisaties. De aloude truc van het aanpassen van alleen rekeningnummers op papier, is tegenwoordig online overgenomen door cybercriminelen.

Inmiddels is deze vorm van factuurfraude nog maar een paar keer voorgekomen in Europa, maar genoeg om zorgwekkend te zijn. Criminelen komen vaak binnen via geïnfecteerde facturen en zoeken zo naar de database van de klantgegevens. Vervolgens passen ze het sjabloon aan dat wordt gebruikt om de facturen mee te sturen. Soms kan hier georganiseerde misdaad achter schuilgaan, omdat geavanceerde vaardigheden nodig zijn om dit voor elkaar te krijgen.

Verschillende varianten van factuurfraude:
Het manipuleren van papieren facturen.
Criminelen bemachtigen een factuur (tool) van een organisatie en veranderen het rekeningnummer in dat van de oplichter. Dat kan uiteenlopen van het zichtbaar aanpassen van de gegevens met een stempel of sticker tot totaal gephotoshopte facturen.
Het versturen van spookfacturen.
Een spookfactuur is een rekening voor een opdracht die nooit is uitgevoerd. Dit zijn op een factuur lijkende aanbiedingen.
Het manipuleren van boekhoudsoftware.
Cybercriminelen installeren schadelijke software, malware (tool), op een bedrijfscomputer waarmee ze de rekeningnummers in de boekhoudsoftware kunnen aanpassen. Na de koppeling met internetbankieren wordt dan ongemerkt geld overgemaakt naar de crimineel.
Brief met 'gewijzigd rekeningnummer'.
Oplichters sturen een brief naar klanten van een organisatie namens een andere organisatie. In de brief melden ze dat het rekeningnummer is gewijzigd naar een nieuw (vals) rekeningnummer.

Cybercriminelen worden steeds geraffineerder en professioneler als het gaat om het oplichten van organisaties. Het is vooral belangrijk om medewerkers te wijzen op de gevaren van cybercrime (tool). Dat geldt vooral voor medewerkers op afdelingen waar betaalopdrachten worden verwerkt.

Door duidelijke procedures voor facturatie te stellen en controlestappen in te bouwen kan het risico op factuurfraude worden beperkt. Bovendien is het goed om medewerkers bewust te maken van verdachte omstandigheden zoals schadelijke links en bijlages in e-mails of dwingende telefoontjes die een urgente betaling afdwingen.



Mensen overschatten zich online

Mensen zijn online niet zo goed als ze denken. We overschatten hoeveel we weten van digitale veiligheid. We denken dat we er veel verstand van hebben, maar dat klopt vaak niet, zegt beveiliger Symantec. Zo maken mensen geregeld de fout om één wachtwoord voor meerdere accounts te gebruiken. Als bij één site een inbraak is, kunnen hackers proberen of de gestolen wachtwoorden ook ergens anders werken. We laten onze virtuele achterdeur openstaan, aldus Symantec.

Volgens Symantec werden vorig jaar 3,4 miljoen Nederlanders slachtoffer van cybercrime, dus ongeveer een op de vijf mensen. Ze raakten in totaal 1,3 miljard euro kwijt. Het gemiddelde slachtoffer is enthousiast over technologie en gebruikt graag meerdere apparaten. Zo hebben slachtoffers bovengemiddeld vaak een smartwatch of een slim huishoudelijk apparaat. Tegelijk hebben ze een „blinde vlek" voor veiligheid.

In heel Europa kregen 98,2 miljoen mensen te maken met digitale misdaad. De schade daarvan bedroeg 23,3 miljard euro. Dat is ongeveer de omvang van de economie van IJsland.

Phishing

De meest voorkomende vorm van cybercrime in Nederland is phishing. Daarbij worden mensen door oplichters aangespoord om ergens hun gebruikersnaam en wachtwoord in te vullen, zodat de cybercriminelen daarmee hun slag kunnen slaan. Symantec sprak met meer dan 20.000 mensen in twintig landen, onder wie ruim duizend Nederlanders. Uit het onderzoek blijkt uit dat veel mensen vertrouwen hebben in de digitale veiligheid van banken en providers, en in zichzelf. Het vertrouwen in de overheid en in sociale media daalde juist.

Bron: Symantec

400.000 Nederlandse cryptogokkers

Ongeveer 400 duizend Nederlanders hebben geïnvesteerd in cryptomunten. Dit blijkt althans uit een representatief onderzoek van Peil.nl onder drieduizend Nederlanders. Het onderzoek is uitgevoerd in opdracht van Dag van de Crypto, dat volgende week een congres over het onderwerp organiseert. Uit een peiling van een paar maanden geleden door een ander onderzoeksbureau kwam nog een veel lager aantal naar voren: 130 duizend.

De forse koersstijgingen van cryptomunten in november en december 2017 zouden veel nieuwe beleggers over de streep hebben getrokken. Als gevolg van de koersdalingen van de afgelopen weken staan velen van hen dan wel weer op verlies. De doorsnee-cryptobezitter is een hogeropgeleide man tussen de 25 en 45 jaar, wiens portefeuille een gemiddelde waarde heeft van 7.300 euro. Dat zou betekenen dat cryptogeld nu bijna 1 procent van het totale spaartegoed (340 miljard euro) van alle Nederlanders tezamen bedraagt. Maar liefst 22 procent van de Nederlanders vindt cryptomunten oplichterij. Bij de bezitters van cryptomunten ligt dat uiteraard een stuk lager: 1 procent.

Al eerder werd duidelijk dat marktpartijen en toezichthouders in Nederland weinig zien in een verbod op de handel in cryptomunten. Wel vinden ze dat er heldere regels moeten komen om misbruik tegen te gaan. Dat bleek tijdens een hoorzitting over het onderwerp in de Tweede Kamer. Als het om regelgeving gaat wordt met name gekeken naar De Nederlandsche Bank en de Autoriteit Financiële Markten (AFM). Het probleem is echter dat cryptomunten geen erkende betaalmiddelen zijn en dus niet onder het toezicht van die organisaties vallen. Wel waarschuwden beide toezichthouders maar weer eens voor de grote risico's van beleggen in cryptomunten.

Verdwenen in het digitale niets

Het klonk allemaal zo mooi wat hippe startup Confido geïnteresseerde beleggers voorhield: een op blockchain gebaseerde app voor betalingen en voor het tracken-en-tracen van bestellingen. Om geld op te halen, maakte Confido gebruik van het even populaire als riskante investeringsmodel van de ICO (Initial Coin Offering).

Hierbij lanceren bedrijven hun eigen nieuwe cryptomunt waarop beleggers kunnen intekenen. In dit geval haalde Confido hiermee 374.000 dollar aan ethers op, een bestaande cryptomunt. Alles zag er goed uit, totdat alle digitale sporen van Confido op zondag ineens verdwenen. Website, Twitter-account: alles weg. Oprichter 'Joost van Doorn' (onduidelijk of deze man echt bestaat) publiceerde nog wel een korte verklaring waarin hij namens het bedrijf excuses maakt en verwijst naar vage juridische problemen. ‘Het was nooit onze bedoeling om investeerders schade toe te brengen; we zagen dit niet aankomen’, zo schrijft hij. Maar volgens het bedrijf dat Confido met zijn ICO begeleidde zijn het gewoon verdomd goede oplichters, schrijft Motherboard. Onlangs nog waarschuwden de Autoriteit Financiële Markten en De Nederlandsche Bank nog voor ICO’s omdat hier geen enkele controle op is.

Het succes van Operatie Bakovia

Een Roemeense bende infecteerde tienduizenden computers met een virus dat bestanden gijzelt. Dankzij de Nederlandse politie werden onlangs vijf verdachten gearresteerd. Een reconstructie van Operatie Bakovia.

De deur van een appartement in een anoniem Roemeens flatgebouw zwaait open. Direct stormen agenten met getrokken wapens naar binnen. In de woning vinden zij servers, laptops en honderden simkaarten. Twee verdachten worden aangehouden. Vanuit deze plek stuurden zij volgens de autoriteiten op grote schaal computervirussen de wereld in.
Het is halverwege december. Een dag na de inval, op vrijdag de vijftiende, worden nog eens twee verdachten opgepakt op het vliegveld van Boekarest. Ze waren op het moment niet in de flat aanwezig en staan op het punt het land te verlaten. Later wordt nog een verdachte gearresteerd.
De aanhoudingen zijn voor de Nederlandse politie, die beelden van de arrestaties online zet, het resultaat van een lang onderzoek met de naam 'Operatie Bakovia'. Gert Ras, hoofd van Team High Tech Crime van de politie, spreekt over een 'opvallend succes'. "Ik ken geen andere casus waar verdachten van zo'n grote ransomwarecampagne zijn aangehouden. Hoewel onderzoek nog moet uitwijzen hoeveel ze precies hebben verdiend, gaan we ervan uit dat ze tienduizenden computers hebben geïnfecteerd."

Nederlandse gedupeerden

De Nederlandse politie maakt in 2015 voor het eerst kennis met het werk van de verdachten. Er komen tweehonderd aangiftes van slachtoffers binnen. Maar het werkelijk aantal geïnfecteerde computers in Nederland ligt veel hoger, zegt de politie. Het is een bekend gegeven dat een klein deel van de mensen die te maken krijgen met internetcriminaliteit aangifte doet. Volgens het CBS meldde zich in 2016 maar acht procent.

De slachtoffers hebben een e-mail gekregen die afkomstig lijkt van KPN en die gaat over een rekening die betaald moet worden. Klikt een slachtoffer op de link, dan wordt niet de rekening gedownload, maar een virus met de naam CTB-locker. Dat begint direct bestanden op de computer te versleutelen.
Het slachtoffer krijgt een scherm te zien waarin losgeld wordt geëist variërend van zo'n 400 tot 800 dollar. Als een slachtoffer niet binnen 96 uur geld overmaakt via virtueel betaalmiddel Bitcoin, dan maakt het virus alle bestanden permanent ontoegankelijk, staat er.

De mail is volgens Christiaan Beek, security-onderzoeker bij het Amerikaanse bedrijf McAfee, in opvallend goede spelling en bewoordingen opgesteld. Ook de naam onder de mail klopt: de man is volgens zijn Linkedinpagina op dat moment verantwoordelijk voor de klantenservice bij KPN. Voor Beek reden genoeg te concluderen dat het om een goed voorbereide phishingcampagne gaat.

Darkweb
Het team van Beek heeft al eerder kennis gemaakt met de ransomware die de bende gebruikt. De makers ervan - dat zijn niet de Roemeense verdachten zelf - zijn in juni 2014 begonnen met adverteren op het zogenoemde darkweb. Dat deel van internet is alleen met een speciale anonieme server te bereiken. Het is bekend dat er op levendige marktplaatsen op het darkweb van alles te koop is, waaronder computervirussen.

Voor 1500 dollar heb je er de eerste versie van CTB-locker. Andere varianten kosten het dubbele. Kopers kunnen ook kiezen voor de optie om de ransomware via een soort leasesysteem te gebruiken. Dertig procent van de opbrengsten moet de koper dan afstaan aan de maker van het virus. Het is een systeem dat ook wel cybercrime-as-a-service wordt genoemd: oftewel internetcriminelen maken gebruik van elkaars expertise en diensten. CTB-locker geniet gretig aftrek op het darkweb. Volgens McAfee groeit het virus in 2016 zelfs uit tot de grootste ransomware-familie van dat jaar.

Operatie Bakovia

Voor de politie begint dan het ingewikkelde deel van Operatie Bakovia. Er ligt een phishingmail, er zijn een hoop Nederlandse slachtoffers, nu moet de bron van de besmetting nog gevonden worden. In het onderzoek dat volgt, stuit Team High Tech Crime, de internetspecialisten van de politie, op informatie dat een Nederlandse server betrokken is bij het verspreiden van CTB-locker. Het gaat om tips vanuit meerdere bronnen, zegt Gert Ras. Meer details wil hij op dit moment niet geven.

De server in Nederland is één van de computers in een groot wereldwijd netwerk dat de criminelen gebruiken om hun aanvallen uit te voeren. Je kunt zo'n server vrij eenvoudig huren, zonder dat de verhuurder ervan weet waarvoor het gebruikt wordt. Nu de politie weet dat de Roemenen gebruikmaken van een server in Nederland, kan er getapt worden. De politie kan dan meekijken met al het verkeer dat erin en eruit gaat. Daaruit blijkt dat de server van de Roemenen wordt gebruikt om de phishingcampagnes uit te voeren.

Reden genoeg om ook naar de inhoud van de server te willen kijken. Daarvoor maakt de politie een kopie van de hele inhoud. Dat gebeurt zonder dat de criminelen het door hebben. De server is tijdens het kopiëren even uit de lucht, maar dat gebeurt wel vaker, dus het wekt geen argwaan. Het blijkt een cruciale stap in het onderzoek.

De specialisten van de politie treffen er een schat aan informatie aan. Zoals verschillende varianten van CTB-locker en een ander virus met de naam Cerber. Naar dat laatste virus blijkt de US Secret Service onderzoek te doen. Nu zijn ook de Amerikanen betrokken bij de zaak.

Op de server staat ook een berg aan e-mails en correspondentie. Niet alleen internetgebruikers in Nederland, België en Italië blijken het doelwit te zijn van de criminelen. De campagnes met geïnfecteerde e-mails gericht op Ierland en Noorwegen staan op het punt te beginnen. De criminelen hebben al een lijst met miljoenen e-mailadressen van burgers klaar staan.

Virus ontleden

Het is voor de politie nu een kwestie van zoeken naar aanknopingspunten die iets over de eigenaar van de server zeggen. Dat is vooral letten op foutjes van de criminelen. Zo wordt het virus stukje bij stukje ontleed in de hoop dat ze ergens per ongeluk een spoor hebben achtergelaten.

Wat de politie vaak ook helpt is het feit dat de criminelen de server hebben moeten huren. Niet dat ze daarbij keurig hun naam en adres achterlaten, maar voor de politie kan zo'n handeling wel informatie opleveren. Een IP-adres bijvoorbeeld.
De politie besluit ook de hulp van securitybedrijf McAfee in te schakelen. Ras: "Wij doen zelf ook een uitgebreide analyse, maar zo'n virus binnenstebuiten keren, dat is hun vak. Eigenlijk vragen we dus aan het bedrijf: missen wij iets?"

Het team van Christiaan Beek krijgt, net als veel andere bedrijven in de branche, met regelmaat dergelijke vragen van justitie. Dat gaat via een officieel rechtelijk verzoek. Dat de politie nu bij McAfee uitkomt, is geen toeval. Het bedrijf weet al veel over CTB-locker, dat virus dat ze al in 2014 voor het eerst tegenkwamen.

Het, zoals Ras het noemt, 'woud aan spoortjes' verzameld door McAfee en de politie, brengt succes. De identiteit van de verdachten wordt achterhaald. En dat leidt naar Roemenië. Op dat punt draagt de Nederlandse politie het dossier over aan de Roemeense collega's. Aan de autoriteiten daar de taak om de zaak verder af te handelen. Dat gebeurt, de flat in Roemenië wordt binnengevallen.

Signaal naar criminelen

Operatie Bakovia is typerend voor het werk van het Team High Tech Crime van de politie, zegt Ras. Eigenlijk heeft elk onderzoek naar digitale criminaliteit een internationale component. Dat betekent veel overleg met buitenlandse collega's - veelal gefaciliteerd door de Europese politieorganisatie Europol - en regelmatig een oefening in geduld. Niet in elk land gaat vervolging even snel.

Dat Operatie Bakovia succesvol eindigt, ziet Ras als een visitekaartje voor zijn afdeling. "Ik geloof echt dat er een signaal uitgaat naar criminelen. De Roemeense groep had heel bewust een campagne op Nederland gericht. Maar nu weten ze: dat kan dus tot gevolg hebben dat je het Team High Tech Crime achter je aan krijgt."

Ook volgens Beek is de aanhouding van verdachten allerminst vanzelfsprekend. In veel onderzoeken lukt het uiteindelijk niet om te achterhalen wie er achter het toetsenbord zit. Er zijn nou eenmaal veel manieren om anoniem te blijven online. Bovendien gebruiken criminelen nog weleens afleidingsmanoeuvres.

Beek: "Ze laten bijvoorbeeld sporen achter in de code waardoor het lijkt alsof ze uit Nederland komen. Daarmee proberen criminelen onderzoekers op het verkeerde been te zetten."

Overigens betekent het oprollen van de Roemeense bende nog niet dat hun slachtoffers uit de problemen zijn. Nog altijd zijn de sleutels die toegang geven tot de bestanden niet gevonden. Ook is het nog niet gelukt de bestanden op een andere manier te ontsleutelen. CTB-locker blijkt bijzonder degelijke ransomware te zijn.

Doe-het-zelf opsporing met Sherlock-app

Met alle nieuws over politie-apps en ‘do it yourself policing’ komt ook de Sherlock-app weer in beeld.

Deze app, in ontwikkeling bij TNO én de politie, moet burgerparticipatie opnieuw vormgeven. ‘Binnen de politie dringt het besef door dat een échte revolutie nodig is als het gaat om burgerparticipatie’, zegt Arnout de Vries van TNO.

De Sherlock-app biedt gebruikers een eigen opsporingsdossier waarin ze locatie, (zichtbare) sporen, gestolen goederen, getuigenverklaringen etcetera kunnen vastleggen. Als het dossier compleet is, kan een opsporingsbericht worden gedeeld en kan het geheel naar de politie worden gestuurd. Politie en gebruiker wisselen vervolgens updates uit via de app.

Volgens De Vries is de politie nog vaak traditioneel bezig en hebben burgers behalve ogen en oren , ook hersenen met kennis en denkkracht en handen en benen om iets te doen. De politie kan de schaarse opsporingscapaciteit dan effectiever inzetten en meer zaken oplossen, hoopt hij. ‘Wat is er handiger dan dat ik na een inbraak zelf bij mijn buren langsga voor een verklaring?’ Van de risico’s is De Vries zich bewust, maar die zijn er ook zonder de app al. ‘Burgers starten nu ook al eigen onderzoeken via facebook’.

Bij de politie zelf is vooral een cultuurverandering nodig. ‘De opsporingstak van de politie vertrouwt niet zomaar burgerspeurneuzen die zelf hun zaak willen oplossen. Het kost tijd om een meer open houding te realiseren richting goedwillende burgers, en politieprocessen te veranderen’.

Oppassen voor nep-wallet & nep-cryptomunt SpriteCoin

Fortinet FortiGuard Labs heeft een nieuwe ransomware-variant ontdekt, die voor de betaling van losgeld alleen de in 2014 geïntroduceerde open source cryptovaluta Monero accepteert. Dit laat een breuk zien met de op brede schaal gebruikte Bitcoin op het gebied van ransomware. De makers van deze malware zijn goed op de hoogte van de laatste trends en gebeurtenissen en lijken te willen profiteren van de hype rond cryptovaluta's.

Ransomware

Deze nieuwe vorm van ransomware vraagt echter niet alleen om een betaling met Monero, het geeft zich ook uit als cryptovaluta-gerelateerde password store. De malware doet zich voor als 'SpriteCoin wallet' en vraagt de gebruiker om een wachtwoord aan te maken. In plaats van de blockchain te downloaden, versleutelt de ransomware de bestanden van het slachtoffer. Vervolgens vraagt deze losgeld in de vorm van Monero in ruil voor het vrijgeven van de data.

Het voor de ransomware gebruikte uitvoerbare bestand (dat in het veld in de vorm van spritecoind[.]exe is aangetroffen) is verpakt in een Ultimate Packer for eXecutables (UPX)-compressiebestand als simpele techniek om beveiligingsmechanismen te omzeilen. De ransomware tovert de gebruikelijke melding "Uw bestanden zijn versleuteld" op het scherm en vraagt het slachtoffer om 0,3 Monero. Dit komt op het moment van schrijven overeen met 84,50 euro.

Analyse

Uit de analyse van Fortinet blijkt dat het malwarefragment een ingebouwde SQLite engine bevat. Fortinet vermoedt daarom dat de ransomware gebruikmaakt van SQLite voor de opslag van de aanmeldingsgegevens die het verzamelt.

De ransomware probeert eerst om aanmeldingsgegevens voor Chrome te bemachtigen. Als die niet worden aangetroffen, zoekt deze toegang tot de database met aanmeldingsgegevens van Firefox. De ransomware zoekt vervolgens naar specifieke bestanden om te versleutelen. Versleutelde bestanden krijgen de extensie .encrypted.

Malware
De ransomware maakt de ellende nog groter door tijdens de ontsleutelingsfase een andere malware-variant te installeren die in staat is om digitale certificaten te verzamelen, afbeeldingen uit te lezen (scan van creditcards etc) en webcams te activeren. Hoe de malware precies te werk gaat lees je hier in het blog van Fortinet.

Ze raden organisaties aan om niet alleen de laatste malware signatures te downloaden, maar zich ook op ransomware-aanvallen voor te bereiden door een solide back-up- en herstelplan te ontwikkelen. Het is belangrijk om niet louter gebruik te maken van back-ups in schaduwvolumes, omdat sommige ransomware-varianten die verwijderen.

Makers van malware weten dat de meeste gebruikers geen regelmatige back-ups van hun systeem maken. Maar voor het geval iemand toch een back-up opslaat in een schaduwvolume of vergelijkbare back-up maakt, bouwen zij code in de ransomware in om die onklaar te maken. Een simpele offline back-up van belangrijke bestanden kan dus een hoop tijdverlies en frustratie voorkomen. Best practices vragen om waakzaamheid met het maken van reservekopieën en het regelmatig maken van back-ups.

Eerste strafvorderingsrichtlijn cybercrime in werking

De eerste strafvorderingsrichtlijn cybercrime is per 1 februari van kracht geworden Deze richtlijn biedt de officier van justitie handvatten voor het bepalen van een straf(eis) in (eenvoudige) cyber-zaken.

De richtlijn is bedoeld voor de verschillende vormen van cybercrime zoals computervredebreuk, Ddos-aanval en in het bezit hebben/plaatsen van ransomware. Aan de hand van de criteria in de richtlijn kan de officier van justitie in strafzaken een straf eisen, een transactie aanbieden of een OM-strafbeschikking opleggen.

Veiligheidsrisico's
Aanleiding voor deze richtlijn is dat met de nieuwe technologie voorwerpen aangesloten zijn op het internet en gegevens worden uitgewisseld. Dit brengt veiligheidsriscico's met zich mee voor burgers, bedrijven en overheid.

Dankzij de technologische mogelijkheden kunnen cybercriminelen in korte tijd in principe vanaf elke plek in de wereld grote aantallen slachtoffers maken. Burgers en bedrijven kunnen slachtoffer worden van ransonware, kwaadaardige 'gijzelingssoftware'.

Door Ddos-aanvallen worden websites met zwak beveiligde apparaten zoals webcams en digitale videorecorders platgelegd. Het aantal gevallen van cybercrime waarbij computers niet alleen als middel worden ingezet maar ook doelwit zijn, neemt toe.

Categorieën
De richtlijn is onderverdeeld in vier categorieën.

- Bij de eerste categorie cybercrime in de relatiesfeer gaat het om zaken waar bijvoorbeeld een ex-partner/ex-werknemer inbreekt in een account of (bedrijfs)server.

- Bij cybercrime met als oogmerk diefstal van vermogen onder andere om diefstal internetbankieren, het gebruik van crypto/ malware of het hacken van een server ten behoeve van phishen.

- Bij cybercrime met als oogmerk het overnemen van gegevens bijvoorbeeld om bedrijfsspionage of tentamenfraude.

- Onder de vierde categorie cybercrime met een ideologisch (niet zijnde terroristisch) oogmerk vallen zaken als DdoS-aanvallen met beperkte impact. Deze is afhankelijk van de financiële schade en in hoeverre diensten zijn getroffen. Daarnaast defacing, het wijzigen, beschadigen of vervangen van webpagina's door hackers.

Cybercrime, alleen en eenmalig gepleegd.

Cybercrime in relatiesfeer (ex-partners, ex-werknemers, etc.)	**first offender**	**1x recidive***
Inbreken in een (social media of mail) account of (bedrijfs)server (art. 138ab Sr)	TS 20–80 uur	TS 30–120 uur en een voorwaardelijke gevangenisstraf
Wijzigen wachtwoorden/ ontoegankelijke maken van gegevens (art. 350a Sr)	TS 20–100 uur	TS 30–150 uur en een voorwaardelijke gevangenisstraf
Verwijderen / ontoegankelijk maken van gegevens/ toevoegen van gegevens (art. 350a Sr / 138ab Sr)	TS 20–120 uur	TS 30–180 uur en een voorwaardelijke gevangenisstraf
DDoS aanval met beperkte impact** (art. 138b Sr)	TS 60 uur	TS 90 uur
Het versturen van een smadelijk/lasterlijk bericht vanuit het account van je (ex-)partner (smaad en computervredebreuk)	TS 120 uur	TS 180 uur en een voorwaardelijke gevangenisstraf
Cybercrime met oogmerk diefstal vermogen (diefstal internetbankieren, art. 139d Sr, crypto/ransomware)	**first offender**	**1x recidive***
Diefstal internetbankieren (art. 311 Sr / 138ab Sr) – tot € 10.000,-	TS tot 120 uur/ GS 1 week tot 2 mnd	GS 10 weken tot 4 mnd
– van € 10.000,– t/m € 100.000,–	TS vanaf 120 uur/ GS 2 tot 5 mnd	GS 4 mnd tot 6 mnd
– meer dan € 100.000,-	GS vanaf 5 mnd	GS vanaf 7 mnd
Voorhanden hebben van malware / wachtwoorden / inloggegevens (art. 139d lid 2 sub a en b Sr)	GS 2 weken	GS 3 wkn
Gebruik van crypto- en ransomware (art. 326/284 Sr)	GS 3 maanden	GS 4 mnd
Hacken van een server ten behoeve van b.v. phishen (art. 138ab Sr)	GS 1 maand	GS 6 wkn
Cybercrime met oogmerk overnemen gegevens ((bedrijfs)spionage, tentamenfraude, etc)	**first offender**	**1x recidive***
Inbreken in account met het oogmerk gegevens over te nemen (art. 138ab Sr)	GS 2 maanden	GS 3 maanden
Het voorhanden hebben van malware (art. 139d lid 2 sub a en b SR)	GS 1 maand	GS 6 wkn
Cybercrime met ideologisch (niet zijnde terroristisch) oogmerk (DDos, art. 350a Sr, defacing)	**first offender**	**1x recidive***
Defacen website (art. 350a Sr)	TS 60 uur	TS 90 uur en een voorwaardelijke gevangenisstraf
DDoS aanval met beperkte impact** (art. 138b Sr)	TS 60 uur	TS 90 uur
Bijzonderheden Uitgangspunt is dat de dader de schade vergoedt.		

Strafverzwarende/verminderende factoren o.a .:
- gebruik malware
- schade / herstel
- aard van gegevens
- *kwetsbaar slachtoffer*
- verbeurdverklaring computers/gegevensdragers
- *meermalen recidive* (maatwerk)

Cybercrime, meermalen gepleegd, veelal in georganiseerd verband en in combinatie met andere strafbare feiten

Cybercrime met oogmerk diefstal vermogen (diefstal internetbankieren, art. 139d Sr, crypto/ransomware)	**first offender**	**1x recidive**
Medeplegen van diefstal met valse sleutel en computervredebreuk, bestaande uit het inloggen op een bankrekening en het vervolgens overmaken van geld naar rekening van derde(n), met inloggegevens waartoe dader niet gerechtigd was. Meestal zijn de inloggegevens (deels) verkregen dmv phishing en/of malware (art. 138ab/139d/311/326/420bis Sr)	GS 3 jaar	GS 4 jaar
Grootschalige ransomware-campagne	GS 3 jaar	GS 4 jaar
Bijzonderheden Uitgangspunt is dat de dader de schade vergoedt.		
Strafverzwarende/verminderende factoren o.a.:		
– Mate van inbreuk op de privacy van het slachtoffer – Aantal slachtoffers – Mate van georganiseerdheid – Hoogte schade – *meermalen recidive* (maatwerk)		

Legenda

Malware = Samentrekking van malicious software. Malware is de term die tegenwoordig als generieke aanduiding wordt gebruikt voor onder andere virussen, wormen en Trojaanse paarden.

Ransomware = Type malware dat systemen en/of informatie daarop blokkeert en alleen tegen betaling van losgeld toegankelijk maakt.

Cryptoware = Type ransomware dat bestanden op een computer of in een netwerk versleutelt. De sleutel wordt alleen tegen betaling vrijgegeven.

Phishing = Verzamelnaam voor digitale activiteiten die tot doel hebben persoonlijke informatie aan mensen te ontfutselen. Deze persoonlijke informatie kan worden misbruikt voor bijvoorbeeld creditcardfraude, maar ook voor identiteitsdiefstal. Spearphishing is een variant die zich richt op één persoon of een zeer beperkte groep personen in bijvoorbeeld een organisatie, die specifiek worden uitgekozen op basis van hun toegangspositie om een zo groot mogelijk effect te sorteren zonder al te veel op te vallen.

Defacing = Bij defacing worden websites door hackers gewijzigd, beschadigd of vervangen.

DDoS = (Distributed) Denial of Service is de benaming voor een type aanval waarbij een bepaalde dienst (bijvoorbeeld een website) onbereikbaar wordt voor de gebruikelijke afnemers van de dienst. Een DoS op een website wordt vaak uitgevoerd door de website te bestoken met veel netwerkverkeer, waardoor deze onbereikbaar wordt.

Afkortingen

TS = Taakstraf

GS = gevangenisstraf

Politie, sociale media en geheimhoudingsplicht

Het blijft wringen, al die agenten op sociale media.

De wens om transparant te zijn, verbinding te maken met burgers en gewoon te laten zien wat politiewerk nu is, botst keer op keer met regels over privacy en geheimhouding.
In vlogs zijn mensen soms geblurd maar nog steeds herkenbaar, straten en huisnummers zijn herkenbaar en er wordt gewoon binnenshuis gefilmd.
De Monitor legde deze recentelijk de vinger weer eens op de zere plekken: hoewel politieagenten een geheimhoudingsplicht hebben, wordt veel persoonlijke info niettemin gewoon geopenbaard.

Advocaat Aldo Verbruggen vindt het delen van privé-informatie ‘ronduit verbijsterend’.
Verbruggen, oud-ovj, vraagt zich af waarom er zoveel foto’s en filmpjes gedeeld worden, waar de informatie ook gewoon in een tekstberichtje kan.
‘Concentreer je op jezelf, breng jezelf in beeld en niet degenen op wie je je acties richt’. En als dat toch gebeurt, dan ‘gewoon onherkenbaar’.

Voorzitter Jeroen Soeteman van de Nederlandse Vereniging Van Strafrechtadvocaten (NVSA) wijst er verder op dat het veelvuldig delen van informatie over verdachten door de politie via sociale media zelfs kan leiden tot strafvermindering. ‘Ze worden dan aan de digitaal schandpaal genageld, voordat er een rechterlijke uitspraak is geweest en dat is al een straf op zich. De rechter kan hier rekening mee houden’.

Volgens Soeteman is elke burger onschuldig totdat de rechter hem heeft veroordeeld. Maar wanneer de politie privacygevoelige informatie van een verdachte naar buiten brengt op sociale media, ‘kan de rest van de maatschappij al denken dat de burger schuldig is. En dat mag niet’. Immers, mensen kunnen verhaal gaan halen bij de verdachte en ‘dat is geen goede ontwikkeling’.

Het OM zegt dat er ‘scherper’ gelet zal gaan worden op beelden waarbij de privacy van verdachten in het geding is.

Bitcoinhype veroorzaakt goudkoorts onder cybercriminelen

Cybercriminelen storten zich massaal op cryptomunten. Zij hebben diverse technieken en tools ontwikkeld om mensen op te lichten die handelen in de populaire cryptovaluta. Digital Shadows onderzocht de meest gebruikte technieken. In het onderzoeksrapport worden voorbeelden genoemd als cryptojacking, de overname van accounts, mining-fraude en valse introducties van nieuwe cryptomunten (initial coin offerings; ICO's).

Rick Holland, Vice President Strategy bij Digital Shadows: "De ontwikkelingen in de cryptowereld volgen zich in hoog tempo op. Momenteel zijn er 1.442 verschillende cryptovaluta's in omloop en er worden wekelijks nieuwe alternatieve digitale valuta's ('altcoins') uitgebracht. Criminelen zien kansen in de ongereguleerde wereld van cryptomunten. Nietsvermoedende mensen willen namelijk profiteren van cryptovaluta's, maar vormen een eenvoudige prooi. Wie cryptovaluta's aanschaft en verhandelt, moet dus waakzaam blijven tijdens elke stap in de transactiecyclus."

Het onderzoeksrapport 'The New Gold Rush' biedt een beschrijving van de meest gebruikte tactieken voor het minen en stelen van crypotovaluta's:

- Botnets: botnets – computerlegers – worden al langer gebruikt voor het minen van bitcoins, maar waren erg complex. Botnets maken nu een comeback, omdat recentere cryptovaluta's zoals Monero makkelijker te minen zijn. Je huurt al een botnet voor 40 dollar.
- Crypto Jacker: deze nieuwe mining-tool combineert de malware Coinhive, Authedmine en Crypto-Loot binnen een WordPress plug-in en voegt daar SEO-functionaliteiten aan toe. De software is verkrijgbaar voor slechts 29 dollar. Gebruikers kunnen hiermee populaire websites klonen en inzetten voor spamcampagnes.
- Aanvallen bij cryptobeurzen: wanneer mensen cryptovaluta willen omzetten in echt geld, gaan ze naar de cryptobeurs. Criminelen zien hier hun kans schoon om wallets te hacken en de buitgemaakte inloggegevens te verkopen. De accountgegevens worden gestolen met technieken als phishing en credential stuffing. Digital Shadows vond op criminele fora al meer dan 100 gebruikersaccounts die pas sinds januari 2018 werden aangeboden.
- ICO's en valse cryptobeurzen: valse cryptobeurzen zijn populair. Criminelen creëren volledig verzonnen cryptomunten en voeren daarmee scams uit. Ze maken een scamsite aan en verleiden zullen nietsvermoedende mensen om te investeren in deze neppe cryptovaluta.
- Pump and dump: pump and dump-criminelen drijven kunstmatig de koers op van kleine, minder bekende cryptovaluta's om te profiteren van de stijging. Ze halen hun winst vlak voordat de koers instort. In januari 2018 observeerde Digital Shadows meer dan 20 van dit soort activiteiten.

Computers besmet om wachtwoorden onlinebankieren

Hackers proberen met besmette computers de gebruikersnamen en wachtwoorden van klanten van grote banken in handen te krijgen. Daarvoor waarschuwt beveiliger ESET.

Het schadelijke programma Trickbot zorgt ervoor dat een bezochte website stiekem wordt aangepast. Een gebruiker vult nietsvermoedend bijvoorbeeld creditcardgegevens in en die informatie belandt zo in handen van de aanvallers.
Meerdere banken zijn doelwit

De aanvallers hebben in elk geval ING en de GarantiBank in het vizier, en het is niet uit te sluiten dat ABN AMRO, de Rabobank, de Triodos Bank, de Volksbank (SNS Bank, ASN Bank en RegioBank), Knab, Credit Europe Bank, Amsterdam Trade Bank, KasBank en DHB Bank ook doelwit zijn. Net als vergelijkbare schadelijke programma's zou Trickbot ook grote Duitse banken, ICS (het moederbedrijf van Visa en MasterCard) en webwinkels Amazon, Otto en Coolblue onder vuur kunnen nemen, evenals Booking.com en Blockchain.info, dat wordt gebruikt voor de handel in bitcoins.

Trickbot wordt aangestuurd vanaf zogeheten command & control-servers die voornamelijk in Rusland zijn. Dat wil niet zeggen dat de daders zich in Rusland bevinden, zij kunnen over de hele wereld zijn.

De schadelijke software houdt geen verband met de recente DDoS-aanvallen op grote banken als ING, ABN AMRO en de Rabobank, en de Belastingdienst. Die sites werden bestookt met verkeer en bezweken onder de druk. Ze werden onbereikbaar, waardoor niemand kon inloggen. Het is nog niet bekend wie achter die aanvallen zitten en wat hun motieven zijn.

Cops in cyberspace

In Nantes, Frankrijk hebben 'ten minste zeven' agenten 'op persoonlijke titel' aangifte gedaan van 'minachting' en belediging, na een tweet van de acteur-regisseur Mathieu Kassovitz. In die tweet reageerde Kassovitz op een grootschalige drugscontrole in een psychiatrisch ziekenhuis. In totaal 24 agenten vonden bij die actie niet meer dan 7 gram hash. 'Stelletje klootzakken', reageerde Kassovitz op de vondst. '24 agenten voor 7 gram, jullie zijn een bastaardbende'. De agenten pikten dat niet. Ook de politievakbond UNSA was boos en wil nu actie tegen de regisseur. Politie-prefect Eric Morvan sprak zijn steun uit voor de agenten. 'Een comment is gratis, natuurlijk, maar dit is een onnodige belediging'.

———————————————

Het Nederlandse Watch-team, een digitaal speurteam van kinderhulporganisatie Terre des Hommes, heeft in 2017 in totaal 53 'loverboy-dossiers' aan de politie overgedragen. Medewerkers van Watch kregen in 2017 140 tips en speurden vooral online in open bronnen naar sporen van pooiers, slachtoffers en klanten. Eens in de twee weken is er overleg met de politie. Dat is vooral eenrichtingsverkeer, zegt Watch-projectleider Gideon van Aartsen. 'Soms horen we van de politie dat ze niet met een zaak door konden. Dan pakken wij het weer op'. Onduidelijk is dus hoeveel zaken door justitie in behandeling zijn genomen, of hoeveel verdachten zijn vervolgd. Wel duidelijk is dat veel pooierboys vanuit Brabant werken: een op vijf. Mogelijk is dat te verklaren door de nabijheid van Duitsland en België, waar veel illegale prostitutie plaatsvindt.

'Per ongeluk' en 'toen we iets aan het testen waren', heeft de politie van Sydney een arrestatieplan live uitgezonden op Periscope. Agenten bespraken de aanhouding van een man die raketonderdelen en -technologie zou willen verkopen om zo geld op te halen voor Noord-Korea. Wat ze kennelijk niet wisten, is dat hun gesprek – onder meer over het tijdstip van de aanhouding – live werd uitgezonden op Periscope en werd gelinkt op twitter. Schieten op de verdachte was niet nodig, en veel collega's waren er ook al niet nodig, zeiden de agenten onder meer. 'Het gaat maar om een paar mensen en een forensische bestelwagen'. De tweet werd sneller ontdekt dan de live stream. Die werd door ongeveer veertig mensen bekeken.

———————————————-

De politie Brabant heeft twee gesloten bitcoinminers teruggevonden. Er is een verdachte aangehouden op verdenking van heling. De computers werden begin januari gestolen uit een schuur in Eindhoven. Twee van de drie werden getraceerd in Vlijmen, naar de derde wordt nog gezocht. Volgens de politie toont het onderzoek hoe 'de klassieke als de hedendaagse innovatie opsporingsmethoden elkaar aanvullen'.

———————————————-

Tja. Wéér een nieuw app die politie en burgers met elkaar in contact moet brengen. Dit keer komt het initiatief uit Twente waar de app 'Mijnbuur' wordt getest. Enkele wijkagenten uit Twente werkten mee aan de app die volgens ontwikkelaar Ancel Gerla een vervanging moet zijn van Whatsapp. 'Daar ontstaan vaak lange discussies en dat leidt tot ergernis', stelt Gerla. 'Door de stroom aan berichten gaat een telefoon namelijk constant af, terwijl veel meldingen niet voor alle lezers relevant zijn'. Mijnbuur werkt met categorieën (nieuwtjes, helpen, overlast en onraad) en afzenders kunnen kiezen wie het bericht moet ontvangen. Bij overlast of onraad kan de wijkagent aan het gesprek worden toegevoegd maar ook medewerkers van de gemeente. Gerla noemt de app niet snel genoeg om 112 te vervangen maar 'het is wel goed om de buurt te waarschuwen na een inbraak, zodat de wijkagent vervolgens tips kan geven om erger te voorkomen'. Mogelijk wordt ook de afdeling webcare aangesloten.

———————————————

Toen de politie Doetinchem op facebook melding maakte van een aanhouding, reageerden veel mensen boos. Agenten werden uitgescholden, maar onduidelijk is precies met welke woorden. Een aantal personen heeft inmiddels van de politie een 'ontbieding verhoor' thuis gekregen, een brief waarin ze uitgenodigd worden om op het bureau gehoord te worden. 'Wij begrijpen dat het werk dat wij doen niet altijd alleen maar lovende reacties oproept', aldus de brief. Het is ook niet erg als mensen kritisch zijn, maar 'wordt die mening echter beledigend en plaats je die op social media, dan vinden wij dat wel een probleem'. Beledigingen op facebook zijn net zo strafbaar als op straat, benadrukt de politie. En dus worden die mensen op het bureau verwacht.

Rechtspraak

De politierechter in Den Bosch heeft een man (48, uit Haren) veroordeeld tot tachtig uur taakstraf voor opruiïng, discriminatie, groepsbelediging en aanzetten tot haat en geweld. De verdachte plaatste tussen oktober en december 2015 tal van discriminerende teksten op facebook. Hollanders moesten zich 'bewapenen tegen dat moslimtuig', schreef de man. 'Uitroeien dat islamtuig, die moslimsmeerlappen'. Na aangifte door het meldpunt internetdiscriminatie, november 2015, werd de man uiteindelijk mei 2016 door de politie verhoord. Naar eigen zeggen stond de man toen nog steeds achter die teksten. Opvallend is dat facebook de teksten pas anderhalf jaar na publicatie verwijderde.

————————————————

De rechtbank in Assen heeft een docent (40, uit Assen) veroordeeldtot dertig maanden celstraf (waarvan tien voorwaardelijk). De man, docent op groene school Terra, pleegde ontucht met een 13-jarige leerlinge. Hij mag verder niet meer in de woonplaats van het meisje komen én vijf jaar lang niet voor de klas staan. In de zaak legde de docent via Whatsapp contact met het meisje. In die gesprekken werkte de verdachte, tevens mentor van het meisje, 'maandenlang toe naar het ontmaagden van zijn leerlinge'. Hij stuurde naaktfilmpjes van zichzelf, vroeg het meisje soortgelijke filmpjes te maken en te sturen. In de bosjes bij school betastte hij haar. Op de computer van de docent stonden zo'n negenhonderd kinderpornofoto's.

————————————————-

Voor grootschalige internetoplichting zijn vier mannen (tussen 24 en 31, uit Den Haag, Bussum en Enschede) veroordeeld tot celstraffen van 48 tot 146 weken. De mannen hadden webshops nagemaakt van bekende merken als Mediamarkt, BCC en Prenatal, waarna ze op Marktplaats advertenties plaatsten en klanten naar de namaakwebshops leidden. Enkele honderden mensen werden slachtoffer. Het OM vond dat de mannen in georganiseerd verband actief waren, de rechtbank zag dat anders: de mannen waren onafhankelijk van elkaar met hetzelfde strafbare feit bezig.

==========

De rechtbank heeft Romano P. (22, uit Rotterdam) veroordeeld tot vier jaar celstraf voor het afpersen van twee slachtoffers. De verdachte deed op een datingsite alsof hij een jong meisje was, naar eigen zeggen om de mannen 'een lesje te leren' die seks met minderjarigen zochten. De slachtoffers kregen echter geen date maar werden verrast door de verdachte. Ze werden bedreigd en afgeperst: ze moesten flink betalen om foto's en filmpjes zogenaamd offline te houden. De verdachte, in het verleden ook al eens veroordeeld voor afpersing, moet in totaal 28 mille terugbetalen. Het OM had vijf jaar gevangenisstraf geëist.

————————————————-

Een man (67, uit Alkmaar) die vorig jaar jonge meisjes uit Middenmeer, is veroordeeld tot twaalf maanden celstraf (de helft voorwaardelijk) en reclasseringstoezicht. De man heet Henry maar noemde zich op facebook André. Met dat alias viel hij tientallen meisjes lastig. Hij stuurde ze onder meer piemelfoto's en vroeg de meisjes om naaktfoto's. Hij liep tegen de lamp toen een vader uit Middenmeer ontdekte dat zijn dochter via Whatsapp met de man aan het chatten was. Politieonderzoek leidde vervolgens, met enige vertraging, tot aanhouding en vervolging. Toen de man september 2017 na een maand voorarrest werd vrijgelaten, ging hij direct weer aan de slag. De man moet verder drie jaar lang zijn computers laten onderzoeken op kinderporno.

Verschijningsvorm cybercrime	138ab *lid 1*	138ab *lid 2*	138ab *lid 3*	138b	139c *lid 1*	139d	139e	161 *sexies*	161 *septies*	350a *lid 1*	350a *lid 2*	350a *lid 3*	350b *lid1*	350b *lid2*
• Malware														
Malware maken en/of verspreiden	X					X		X	X	X	X	X	X	X
Malware (Trojaanse paarden) gebruiken	X	X			X			X	X	X	X	X	X	
• Computerinbraak														
Computerinbraak (hacking)	X		X								X			
Computerinbraak vervolg-handelingen		X	X		X	X	X	X	X	X	X	X		
Portscan						X								
Spoofing/cache poisoning	X	X		X	X	X	X	X		X	X			
Sniffing					X	X	X			X				
Draadloze netwerken hacken/ misbruiken	X	X	X	X	X		X	X		X	X			
Password guessing	X			X		X								
• Website aanvallen														
Veroorzaken open relay									X				X	
Wederrechtelijk open relay gebruiken	X							X		X				
Defacing/vernielen website	X							X	X	X			X	
Defacing/doorleiden internet-verkeer	X							X	X	X				
Cross-site scripting	X	X			X	X	X	X		X			X	
SQL-injecties	X	X						X		X				
• Botnets														
Botnet bouwen en beheren	X	X	X		X					X		X		
• Denial of Service														
DDoS-aanval				X				X		X			X	
• Social Engineering														
Phishing		X			X		X							
Vishing/Smishing		X			X									
• E-mail gerelateerd														
Wederrechtelijk open mail relay gebruiken	X							X	X	X				
Spamming (met DoS tot gevolg)				X				X	X				X	

Wetsartikel

Art. 138ab, lid 1 Sr Hacken: opzettelijk en wederrechtelijk binnendringen van een geautomatiseerd werk

Art. 138ab, lid 2 Sr Hacken: overnemen, aftappen of opnemen van gegevens uit een geautomatiseerd werk na binnendringen daarvan

Art. 138ab, lid 3 Sr Hacken door tussenkomst van een openbaar telecommunicatienetwerk

Art. 138b Sr Het belemmeren van toegang tot of gebruik van een geautomatiseerd werk

Art. 139c Sr Het aftappen of opnemen van gegevens (afluisteren)

Art. 139d, lid 1 Sr Plaatsen van opname-, aftap- of afluisterapparatuur; voorbereidingshandelingen

Art. 139d, lid 2 Sr Het ter beschikking stellen of voorhanden hebben van technische hulpmiddelen of toegangscodes bedoeld om het binnendringen van een geautomatiseerd werk, belemmeren van toegang of aftappen te plegen

Art. 139d, lid 3 Sr Zoals in art. 139d, lid 2 Sr, maar met oogmerk gericht op art. 138ab, lid 2 en 3 Sr

Art. 139e Sr Het bezit en verspreiden van gegevens of een voorwerp waarop gegevens staan die door wederrechtelijk aftappen of opnemen zijn verkregen

Art. 161sexies Sr Opzettelijk vernielen etc. van een geautomatiseerd werk of werk voor telecommunicatie; voorbereidingshandelingen

Art. 161septies Sr Vernieling etc. van een geautomatiseerd werk of werk voor telecommunicatie door schuld

Art. 231b Sr Identiteitsfraude

Art. 232 Sr Opzettelijk valselijk opmaken, vervalsen, gebruiken, etc. van betaalpas, waardekaart e.d.

Art. 240b Sr Kinderpornografie

Art. 248e Sr Grooming

Art. 273, lid 2 Sr Bekendmaking bedrijfsgeheimen; heling computergegevens ondernemingen

Art. 273d Sr Schending telecommunicatiegeheim

Art. 317, lid 2 Sr Afpersing door de bedreiging dat gegevens opgeslagen door een geautomatiseerd werk onbruikbaar, ontoegankelijk of gewist worden

Art. 326c Sr Het misbruiken van een publieke telecommunicatiedienst met het oogmerk daarvoor niet volledig te betalen

Art. 350a, lid 1 Sr Opzettelijke vernieling van gegevens die door middel van een geautomatiseerd werk of door telecommunicatie zijn opgeslagen, worden verwerkt of overgedragen

Art. 350a, lid 2 Sr Het feit gepleegd in lid 1 met tussenkomst van een openbaar telecommunicatienetwerk

Art. 350a, lid 3 Sr Opzettelijk gegevens ter beschikking stellen of verspreiden die zijn bestemd om schade aan te richten in een geautomatiseerd werk

Art. 350b, lid 1 Sr Vernieling door schuld van gegevens die door middel van een geautomatiseerd werk of door telecommunicatie zijn opgeslagen, worden verwerkt of overgedragen

Art. 350b, lid 2 Sr Door schuld gegevens ter beschikking stellen of verspreiden die zijn bestemd om schade aan te richten in een geautomatiseerd werk

Video

Tek Tok Late Night:

1. Privacy
2. Internetvrijheid
3. Digitale veilig heid
4. High Tech Crime
5. Data in onderwijs
6. Cybersurveillance
7. Techtrends in onderwijs
8. Veilig internetten
9. MKB cyber secure
10. Cyberellende bij Tek Tok
11. Standaarden en keurmerken
12. Operation Hijg Tech Crime
13. Kraak van de Maand

You Tube:

- Doe jij het veilig online
- Malware
- WiFi ontvangst verbeteren
- Internetfraude via de tele-foon
- Documentaire: Veiligheid en privacy
- Herken een nep-hotspot
- Gebruik wachtzinnen
- Drive-by-downloads voorko-men
- Hoe herken je een phishing mail
- Beveiligd internetbankieren
- Privacy—ik heb toch niets te verbergen
- Mousejack

Help wanted:

- Grooming
- Sexting
- Webcammis-bruik
- Bedreigd/ gechanteerd
- Kinderporno
- Nepprofiel

Handig

Phishing- / valse e-mails melden:

ABN AMRO Bank: valse-email@nl.abnamro.com

ING Bank: valse-email@ing.nl

Rabobank: valse-email@rabobank.nl

SNS Bank: valse-email@sns.nl

ICS- / ABN AMRO creditcards: valse-email@icscards.nl

Tips voor veilig handelen op Marktplaats

Internetoplichting: controleer vooraf de (bank)gegevens van de verkoper via

www.mijnpolitie.nl/miocheck

Komt de verkoper voor op de website Opgelet op internet ?

Malware ID website met info omtrent verwijderen van infecties

PCrisk verwijderingsrichtlijnen voor spyware en virussen

Cookie Verwijderen kennisdatabase voor het verwijderen van adware, hijackers, ransomware, toolbars en pop-ups

Computer woordenboek

Secure Computing Naslag