



Veilig Digitaal Magazine

Jaargang 2

Januari / Februari 2018

[2018 wordt het jaar van hivenets, swarmbots en polymorfe malware](#)

[Wat kunnen we op securitygebied verwachten in 2018?](#)

[Heling van \(digitale\) gegevens strafbaar?](#)

[Politie mag computersysteem auto niet binnendringen](#)

[6% van de cybercrimezaken wordt opgelost](#)

[De sleepwet: wat is waar en wat niet?](#)

[“Niet gedacht dat politie met deze informatie zo onvoorzichtig te werk gaat”](#)

[Hoe cybercriminelen je op een foute link laten klikken](#)

[DearBytes waarschuwt voor grote roof cryptomunten](#)

[Bijna kwart doorgelaten e-mail onveilig](#)

[Deze vier dingen zijn strafbaar als je pikante foto's stuurt](#)

[Please Call Support For Windows Tech Support Scam](#)

[Mozilla heeft problemen met de nieuwe 'sleepwet'](#)

[Pas op met metadata in foto's](#)

[Malware omzeilt beveiliging: fileless malware](#)

[Europa stemt voor betere bescherming bij online aankopen](#)

[BIT helpt politie met bestrijding cybercrime](#)

[Grootste gevaar zit achter de computer](#)

[Hoe voorkomt u cyberaanvallen via Office-documenten?](#)

[Sterke stijging van het aantal impersonatieaanvallen](#)

[Interpol en FBI halen groot botnet uit de lucht](#)

[Politie spoort 97 money mules in Nederland op](#)

[Fingerprinting](#)

[Engeland: Politie waarschuwt voor 'grooming gangs'](#)

Rubrieken:

[Ga naar de Facebookpagina](#)

[Ga naar de website](#)

- [Cops in Cyberspace](#)
- [Rechtspraak](#)
- [Verschijningsvorm cybercrime](#)
- [Wetsartikel](#)
- [Video](#)
- [Handig](#)

2018 wordt het jaar van hivenets, swarmbots en polymorfe malware

De komende jaren zullen de aanvallen blijven toenemen, terwijl het overzicht en de grip op de huidige IT-infrastructuren afneemt. De groei van online apparaten waarmee verschillende persoonlijke en financiële informatie wordt opgevraagd en de inzet van IoT-apparaten, bieden cybercriminelen nieuwe kansen.

Cybercriminelen zijn als geen ander in staat om gebruik te maken van de laatste innovaties op het gebied van onder meer kunstmatige intelligentie om effectievere aanvallen te ontwikkelen. We verwachten dat deze trend in 2018 in een stroomversnelling komt en de aanzet geeft tot destructieve ontwikkelingen. De belangrijkste voorspellingen voor 2018 zijn:

1. De opkomst van zelflerende hivenets en swarmbots:

Na geavanceerde aanvallen zoals Hajime, Devil's Ivy en Reaper verwachten we dat cybercriminelen hun botnets zullen vervangen door intelligente clusters van geïnfecteerde apparaten, hivenets genoemd, om effectievere cyberaanvallen uit te voeren.

Hivenets maken gebruik van zelflerende functionaliteit om op ongekende schaal effectieve aanvallen op kwetsbare systemen uit te voeren. Ze zullen in staat zijn om met elkaar te communiceren en actie te ondernemen op basis van lokaal verzamelde informatie.

Ook de zombies die deel uitmaken van deze kwaadaardige netwerken zullen slimmer worden en instructies kunnen uitvoeren zonder input van de beheerder.

Hivenets zullen in staat zijn om exponentieel te groeien als zwermen, beter in staat zijn om gelijktijdig meerdere slachtoffers te treffen en het moeilijker maken om tegenmaatregelen te treffen. Hoewel cyberaanvallen momenteel nog geen gebruikmaken van zwermtechnologie, bevat hun code daar reeds de ingrediënten voor.

Cybercriminelen zouden code kunnen aanpassen om het zelflerende gehalte te verhogen. Ze zouden gebruik kunnen maken van zwermen van geïnfecteerde apparaten, ook wel swarmbots genoemd, om verschillende aanvalskanalen tegelijk te identificeren en benutten. Dit maakt het mogelijk om op enorme schaal razendsnelle aanvallen uit te voeren. Het hoge ontwikkelings-tempo zal een einde maken aan de voorspelbaarheid die nodig is om aanvallen af te slaan.



FortiGuard Labs registreerde begin dit jaar in één kwartaal maar liefst 2,9 miljard pogingen tot communicatie met botnets.

Dit geeft een idee van de omvang van de schade die hivenets en swarmbots zouden kunnen aanrichten.

2. Het gijzelen van zakelijke diensten is big business:

Hoewel de omvang van ransomware-bedreigingen het afgelopen jaar al met een factor 35 is gegroeid met de opkomst van ransomworms en andere nieuwe typen aanvallen, is het einde nog lang niet in zicht. Aanbieders van cloud-oplossingen en andere zakelijke diensten zullen naar alle waarschijnlijkheid de belangrijkste doelwitten van ransomware vormen.

Cybercriminelen proberen op deze manier nieuwe omzetstromen te genereren. De complexe, hyperverbonden netwerken die cloud providers hebben ontwikkeld kunnen uitgroeien tot een single point of failure voor honderden bedrijven, overheidsinstellingen, beheerders van vitale infrastructuur en zorginstellingen.

We voorspellen dat cybercriminelen kunstmatige intelligentie zullen combineren met aanvalsmethoden die zich op meerdere kanalen tegelijk richten om kwetsbaarheden in de omgeving van cloud providers op te sporen en misbruiken. Criminele organisaties zouden met dergelijke aanvallen bergen geld kunnen verdienen en de processen van honderden of duizenden bedrijven en tienduizenden of zelfs miljoenen klanten kunnen verstoren.

3. Geavanceerde malware die van gedaante verandert:

Het staat eraan te komen: malware die volledig door machines is ontwikkeld. Deze malware zal in staat zijn tot geautomatiseerde detectie van kwetsbaarheden en complexe gegevensanalyse.

Polymorfe malware is geen nieuw fenomeen, maar staat op het punt om een nieuwe gedaante aan te nemen.

Door kunstmatige intelligentie in te zetten voor de ontwikkeling van geavanceerde nieuwe code kan het detectiemechanisme sneller omzeilen. Door hun bestaande tools verder te ontwikkelen zullen cybercriminelen de best mogelijke exploit kunnen ontwikkelen op basis van de unieke kenmerken van elke kwetsbaarheid.



Malware is reeds in staat om gebruik te maken van leermodellen om de beveiliging te omzeilen en meer dan een miljoen virusvarianten per dag te creëren. Maar tot dusver is dit alles nog gebaseerd op één algoritme. Er is sprake van weinig raffinement, en cybercriminelen hebben weinig grip op de output.

FortiGuard Labs registreerde in 2017 in één kwartaal 62 miljoen malware-detecties. Daarvan waren 16,582 malware-varianten afkomstig van ruim 2.534 malware-families. Een op de vijf organisaties meldde dat het last had van malware op hun mobiele devices. De toegenomen automatisering van malware zal de situatie er het komende jaar alleen maar nijpender op maken.

4. Vitale infrastructuren in de schijnwerpers:

Aanbieders van vitale infrastructuren (zoals bijvoorbeeld nutsvoorzieningen of waterwerken) staan momenteel bovenaan de lijst van cyberdoelwitten.

Deze cyberaanvallen kunnen om strategische (cyberoorlog) dan wel economische motieven worden uitgevoerd. De meeste vitale infrastructuren en operationele technologie (OT)-netwerken zijn berucht om hun kwetsbaarheid.

De reden hiervoor is dat ze oorspronkelijk zijn ontwikkeld om van de buitenwereld afgescheiden te zijn. Tegenwoordig is er een geavanceerde netwerkbeveiliging nodig om deze infrastructuren veilig te houden. Gezien de verwoestende gevolgen die kunnen optreden als deze vitale infrastructuren worden gehackt of platgelegd, zijn aanbieders van vitale infrastructuren in een wapenwedloop beland waaraan overheden, criminelen en terroristen aan deelnemen.

De brutaliteit van hackers en de convergentie van operationele technologie (OT) en informatietechnologie (IT) zorgt ervoor dat de beveiliging van vitale infrastructuren in 2018 en daarna een topprioriteit wordt.

5. Cybercriminelen bieden nieuwe geautomatiseerde diensten aan op het dark web:

De ontwikkelingen binnen de wereld van cybercriminaliteit staan niet stil. Dat geldt ook voor het dark web. We verwachten dat er op deze zwarte markt nieuwe diensten zullen worden aangeboden. Crime-as-a-Service-aanbieders zullen nieuwe automatiseringstechnologie inzetten voor hun oplossingen.

We zien reeds dat diverse marktplaatsen op het dark web geavanceerde diensten aanbieden die gebruikmaken van machine learning. Een daarvan is FUD (fully undetected). Deze dienst stelt criminele programmeurs in staat om malware vóór verspreiding naar een analysediens te uploaden. Daarop ontvangen ze een rapport dat aangeeft of beveiligingsoplossingen van uiteenlopende leveranciers in staat waren om de malware te detecteren.

Om dit proces te versnellen zullen cybercriminelen intensiever gebruik gaan maken van machine learning voor het wijzigen van code op basis van wat er door het laboratorium is gedetecteerd.

Dit zal ertoe leiden dat malware en penetratietools moeilijker te detecteren worden. Sandboxtools die gebruikmaken van algoritmes voor machine learning stellen ons in staat om snel nieuwe bedreigingen te identificeren en op dynamische wijze tegenmaatregelen te treffen.

Er is echter geen reden waarom deze aanpak niet door cybercriminelen zou kunnen worden en ingezet voor het verkennen van netwerken, het vinden van doelwitten, het identificeren van zwakke schakels en het maken van blauwdrukken van omgevingen om virtuele penetratietests uit te voeren en vervolgens een aanval op te zetten en uit te voeren.



G DATA: Wat kunnen we op securitygebied verwachten in 2018?

Pseudo-ransomware

Ransomware-achtige malware zal het komende jaar ook op een andere manier worden ingezet, namelijk als dekmantel voor andere criminele activiteiten. We hebben hiervan al een eerste voorbeeld gezien, bij de hack van de Taiwanese Far East bank eerder dit jaar, waarbij zo'n 60 miljoen dollar is buitgemaakt. Achteraf bleek dat de criminelen gestart zijn met een ransomware-aanval. Terwijl de security- en IT-specialisten al hun aandacht nodig hadden voor het bestrijden en blokkeren van de ransomware, stuurden aanvallers spearphishingmails aan medewerkers van de bank. Die mails bevatten links naar malware waarmee vervolgens inloggegevens werden gestolen. Uiteindelijk slaagden ze er zo in om ongemerkt banktransacties uit te voeren, terwijl de aandacht was gericht op de ransomware. Ook dit soort inzet van pseudo-ransomware zullen we in 2018 helaas vaker gaan zien.

Tegelijkertijd blijft de 'echte' ransomware een reële dreiging, waarbij de focus van de criminelen steeds meer komt te liggen op bedrijven, in plaats van op particulieren. De invoering van de GDPR, volgend jaar mei, biedt criminelen nieuwe kansen. Het valt te verwachten dat ze hun ransomware zo zullen aanpassen dat deze niet alleen bestanden versleutelt, maar ook informatie wegsluist. Vervolgens moeten de getroffen

bedrijven niet alleen losgeld betalen om hun bestanden terug te krijgen, maar zullen ze mogelijk ook worden afgeperst om te voorkomen dat de gestolen informatie op straat komt en om boetes te vermijden. 'GDPR ransomware' dus, die vooral gericht zal zijn op grote organisaties.

Malware die rekenkracht steelt

Een andere opvallende trend die zich begint af te tekenen, is de inzet van malware voor cryptocurrency-mining. Daarbij is het doel van de criminelen niet om informatie te stelen of te versleutelen, maar proberen ze rekenkracht te stelen. Ook hiervan hebben we al een eerste voorbeeld gezien. Hoewel dit op het eerste gezicht misschien redelijk onschuldig lijkt, kan het wel degelijk voor problemen zorgen en schade aanrichten. Zware werklasten, vaak bedrijfskritische toepassingen, vertragen aanzienlijk en de mining-malware kan op een machine ook voor geheugenproblemen zorgen, met als gevolg systeemfouten en productiviteitsverlies.

Ook de talloze, vaak slecht beveiligde IoT-devices vormen een aantrekkelijk doelwit voor deze cryptocurrency-malware. Gezien de snel stijgende koers van Bitcoin, is deze vorm van cybercriminaliteit heel lucratief en dus aantrekkelijk.

Hoewel dit op het eerste gezicht misschien redelijk onschuldig lijkt, kan het wel degelijk voor problemen zorgen en schade aanrichten. Zware werklasten, vaak bedrijfskritische toepassingen, vertragen aanzienlijk en de mining-malware kan op een machine ook voor geheugenproblemen zorgen, met als gevolg systeemfouten en productiviteitsverlies. Ook de talloze, vaak slecht beveiligde IoT-devices vormen een aantrekkelijk doelwit voor deze cryptocurrency-malware. Gezien de snel stijgende koers van Bitcoin, is deze vorm van cybercriminaliteit heel lucratief en dus aantrekkelijk.

Een laatste trend die wij voorzien voor 2018 is de groeiende overlap tussen 'gewone' criminaliteit en cybercriminaliteit. Criminelen hebben intussen wel door dat er met cybercrime veel geld te verdienen valt tegen relatief geringe risico's. Dit zal de komende jaren tot uiting komen in nieuwe vormen van (cyber) criminaliteit. Denk bijvoorbeeld aan het stelen van voorgedrukte creditcards, die vervolgens misbruikt worden voor cybercrime.

Een ander mogelijke benadering is het hacken van logistieke informatiesystemen om zo ongemerkt de bestemming van waardevolle vrachtladingen te wijzigen. Of het hacken van containerregistratie-

systemen in de haven, waarbij bijvoorbeeld containers met drugs, wapens of andere waardevolle smokkelwaar 'verdwijnen' uit het registratiesysteem en zo makkelijker in handen van de criminelen komen.

Machine learning en deep learning
Natuurlijk zullen we in 2018 ook weer voor de nodige verrassingen komen te staan. Wie had in 2016 het lekken van de NSA-tools en -kwetsbaarheden voorzien, evenals de daarop volgende WannaCry-aanval? Feit is dat de criminelen steeds weer nieuwe methoden en technieken blijven ontwikkelen. Hun risico's zijn immers klein: als een bepaald stuk malware een fout bevat, kunnen ze die verhelpen en hun campagne voortzetten.

Voor de securitybedrijven en de doelwitten ligt dat anders. Zij kunnen zich geen fouten veroorloven. Gelukkig bieden innovatieve technieken op basis van machine learning en deep learning nieuwe mogelijkheden om verdachte activiteiten op een systeem of een netwerk tijdig te detecteren en vervolgens te blokkeren. Hoe het ook zij: 2018 zal weer een interessant jaar worden!

Heling van (digitale) gegevens strafbaar?

Er worden op internet feiten gepleegd waarbij gegevens worden verkregen via hacking of andere wijze, die interessant zijn voor derden om te kunnen gebruiken voor criminaliteit. Voorbeelden hiervan zijn persoonsgegevens uit databases die gekraakt zijn en daarna gebruikt kunnen worden om bijvoorbeeld goederen te kopen op het internet bij marktplaats e.d. Ook worden creditcardgegevens die via phishing worden verkregen, aangeboden op het internet en verkocht.

Hoewel in dit laatste geval het gebruik van deze gegevens om creditcards te maken al strafbaar is gesteld, is het voorhanden hebben, het overdragen en het kopen van deze gegevens zelf niet strafbaar.

Dit maakt het voor de opsporing lastig. Het wachten tot dat de gegevens daadwerkelijk worden gebruikt voor criminaliteit, betekent dat er niet opgetreden kan worden om misdrijven te voorkomen.

Dat is zeker niet vertrouwenwekkend naar de burger en in feite een slecht signaal omdat deze

vorm van heling in digitale zin wel zou mogen. Het verhandelen of verkopen van dergelijke gegevens heeft zich ontwikkeld tot een op zichzelf staande vorm van criminaliteit.

Dat heling van dit soort gegevens thans niet strafbaar is, houdt verband met het feit dat computergegevens op grond van de jurisprudentie slechts in bepaalde omstandigheden als een goed in de zin van de artikelen 310 en 416 van het Wetboek van Strafrecht (Sr) worden aangemerkt.

Dit is aan de orde als gegevens buiten de beschikkingsmacht van de rechthebbende zijn gebracht en in het economisch verkeer waarde vertegenwoordigen.

Hieruit vloeit voort dat het zonder toestemming van de rechthebbende kopiëren van diens gegevens en het vervolgens gebruiken of verhandelen van die gegevens als zodanig niet strafbaar is omdat de rechthebbende de beschikkingsmacht over die gegevens behoudt.

Minister: Politie mag computersysteem auto niet binnendringen

Het wetsvoorstel Computercriminaliteit III geeft de politie niet de bevoegdheid om het computersysteem van auto's binnen te dringen om die zo op afstand te kunnen stoppen. Dat heeft minister Grapperhaus van Justitie en Veiligheid op Kamervragen van D66-Kamerlid Verhoeven laten weten.

Aanleiding voor de Kamervragen was een opmerking van het hoofd van de Dienst Infrastructuur Gert Wibbelink in de Telegraaf. "We gaan steeds meer de digitale kant op. Straks kunnen we op afstand inbreken in de software van een rijdende wagen en de motor uitzetten", aldus Wibbelink.

Tijdens de behandeling van de wet Computercriminaliteit III stelde de toenmalige staatssecretaris Dijkhoff nog dat de bevoegdheid om in een geautomatiseerd werk onderzoek te doen er alleen is voor bepaalde onderzoekshandelingen, zoals het overnemen van gegevens. "In de wet staat niet dat je een auto mag

stoppen. Daar mag de bevoegdheid niet voor worden gebruikt", aldus Dijkhoff.

Verhoeven vroeg de minister dan ook om opheldering. "Zoals de toenmalige Staatssecretaris van Veiligheid en Justitie tijdens de behandeling in de Tweede Kamer heeft gemeld is het stoppen van een auto niet als onderzoekshandeling opgenomen. Volgens het wetsvoorstel is het dus niet toegestaan binnen te dringen in het computersysteem van een auto om deze te stoppen. Ik zal dit onder de aandacht brengen van de politie", zo luidt het antwoord van Grapperhaus. Het wetsvoorstel Computercriminaliteit III moet nog door de Eerste Kamer worden behandeld.



6% van de cybercrimezaken wordt opgelost

6% van alle cybercrimezaken wordt door de Nederlandse politie opgelost. In 8% van de zaken is duidelijk wie de verdachte is, al leidt dit niet altijd tot aanhoudingen.

Dit blijkt uit de reactie van minister Grapperhaus van Justitie en Veiligheid op vragen van de commissie Justitie en Veiligheid over de begroting voor volgend jaar,

meldt Security.nl. De minister spreekt over een oplossingspercentage van 6%. Dit percentage heeft betrekking op het aantal verdachten dat wordt doorgeleid aan het Openbaar Minister (OM) ten opzichte van het totaal aantal geregistreerde cybercrimedelicten. Het ophelderingspercentage ligt op 8%. Hierbij gaat het om het percentage zaken waarin de politie een verdachte op het oog heeft ten op zichten van het totaal aantal geregistreerde delicten.

6 miljoen euro voor aanpak cybercrime

De minister meldt dat de politie vol-

gend jaar veel zal investeren in de bestrijding van cybercrime. Hiervoor wordt in totaal 6 miljoen euro beschikbaar gesteld, dat wordt geïnvesteerd in onder meer het opzetten van een landelijk dekkend cybercrime intelligence netwerk en tools om effectiever informatie over cybercrime te kunnen verzamelen en opslaan.

Ook meldt de minister dat er in de begroting ruimte is voor het oprichten van gespecialiseerde rechtbankkamers voor cybercriminaliteit. Deze kamers richten zich specifiek op rechtspraak in cybercrime-gerelateerde rechtszaken, iets waar rechters eerder dit jaar om vroegen. De minister meldt dat hiervoor geen specifiek bedrag is gereserveerd en wordt gekeken op welke manier middelen uit het regeerakkoord besteed zullen worden.

De sleepwet: wat is waar en wat niet?

Er komt een referendum over de zogenoemde aftapwet, ook wel sleepwet genoemd. Dat heeft de Kiesraad woensdag bekendgemaakt. Het referendum zal zo goed als zeker samenvallen met de gemeenteraadsverkiezingen van 21 maart. Maar wat is die sleepwet nou?

Wat is de 'sleepwet' in het kort?

De 'sleepwet', of de Wet op de inlichtingen- en veiligheidsdiensten (Wiv), zoals de officiële naam luidt, maakt het mogelijk dat de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) grote hoeveelheden internetverkeer via de kabel mogen aftappen.

De AIVD leest straks dus al mijn appjes?

Nee, ten eerste moet er een bepaalde dreiging zijn voordat de inlichtingendiensten de glasvezelkabels van een verdachte en zijn omgeving mogen aftappen. Bovendien zijn appjes op Whatsapp sowieso niet te lezen vanwege de beveiliging, de zogenaamde encryptie, die het chatprogramma gebruikt.

Aftappen van glasvezelkabels? Daar vallen telefoongesprekken dus niet onder?

Juist wel. Telefoonverkeer, e-mails, sociale media, Whatsapp enzovoort verloopt uiteindelijk allemaal via glasvezelkabels.

De oude wet was toch voldoende?

In de oude wet (uit 2002), die dus op 1 mei 2018 wordt vervangen door de Wiv, is het voor de inlichtingendiensten alleen mogelijk om gericht communicatie via kabels af te tappen. Zo'n internet-tap is te beperkt om professionele hackers of terroristen te monitoren.

De inlichtingendiensten richten zich met de 'sleepwet' volledig op de laptops en computers van verdachte personen.

Natuurlijk zal het grootste gedeelte van het aftappen inderdaad bij laptops en computers gebeuren, maar vergeet niet dat steeds meer apparaten de komende jaren van wifi worden voorzien. Nu hebben we al horloges, ijskasten en zelfs auto's die verbonden zijn met een computer. Ook die apparaten kunnen allemaal getapt worden door de inlichtingendiensten.

De hele wet op inlichtingen- en veiligheidsdiensten (Wiv) is dubieus en moet eigenlijk van tafel. Nee, absoluut niet. De dreiging van terrorisme en hackers wordt iedere jaar groter en de veiligheidsdiensten moeten in staat zijn het land te beschermen tegen dit soort aanvallen. Daarvoor is deze nieuwe wet noodzakelijk. Dus niet de hele wet is omstreden, alleen bepaalde delen daarvan.

De AIVD luistert en leest straks dus de hele dag mee op zoek naar interessante informatie?

De AIVD heeft wel wat beters te doen. Pas als er een serieuze dreiging is kan de 'sleepwet' ingeschakeld worden. Het is dus niet zo dat alles afgeluisterd wordt. De inlichtingendiensten zijn niet eens in staat om zoveel informatie te werken.

De 'sleepwet' gaat pas in op 1 mei 2018 omdat het referendum van 21 maart de nieuwe wet nog kan tegenhouden.

Nee, het referendum van 21 maart is slechts raadgevend en kan de nieuwe wet dus niet tegenhouden. Bovendien heeft Sybrand Buma van het CDA al gezegd dat de uitslag van het referendum sowieso wordt genegeerd.

“Niet gedacht dat politie met deze informatie zo onvoorzichtig te werk gaat”

Studenten journalistiek die op verzoek van het tv-programma De Monitor (KRO-Ncrv) onderzoek deden naar berichten die de politie op sociale media plaatst, zeggen verbaasd te zijn in hoeveel van die berichten namen en adressen te achterhalen zijn.

De studenten analyseerden 258 accounts, vooral op twitter, en vonden 48 berichten waarbij de identiteit van verdachten te herleiden is. Daarnaast dertien berichten waarbij mensen herkenbaar in beeld zijn. ‘Ik had niet gedacht dat de politie met deze informatie zo onvoorzichtig te werk ging’, aldus studente Tamara. Ook student Max had soms geen enkele moeite om te achterhalen op welk adres iemand was aangehouden. ‘Ik kon zo herleiden waar die persoon woont’.

In beeld komen kentekens, huisnummers, gezichten en persoonlijke eigendommen. Opvallend vonden de studenten verder de toon in de berichten. Die is vaak niet neutraal. Het gaat om tweets over dron-

ken mannen met teksten als ‘waarom is dit nodig’, om onnodig gebruik van smileys, of over grappig bedoelde toevoegingen als ‘de ziekte van Heineken’.

Het programma, dat eerder liet zien dat in politieblogs slecht werd omgegaan met privacy en persoonsgegevens, verwijst wederom naar uitspraken van programmadirecteur Nieuwe Media en Digitale Dienstverlening Ron de Milde, die zegt dat een eindredacteur, protocollen of richtlijnen geen oplossingen zijn.

Terwijl die richtlijnen er wel degelijk zijn. Ze staan in (het door KRO-Ncrv gewobte) ‘Aan de slag met Twitter binnen de politieprofessie’ dat al in 2013 verscheen, maar kennelijk nog ‘niet altijd goed’ is bestudeerd.

Hoe cybercriminelen je op een foute link laten klikken

Nog al te vaak tuinen gebruikers in de phishing-trucs die cybercriminelen toepassen om data te stelen of malware te verspreiden. Onderzoekers aan de Amerikaanse universiteit Georgia Tech hebben een studie gemaakt van een van de meest succesvolle trucs van de afgelopen jaren:

Combosquatting.

Combosquatting is een formele term voor de misleidingstactiek waarbij cybercriminelen gebruik maken van een bekende naam om een malafide website-adres te creëren, waarbij ze aan de URL een extra woord toevoegen dat zo weinig mogelijk wantrouwen oproept. Uiteraard kunnen de online dieven geen gebruik maken van de URL van een officiële website, dus maken ze een kopie die daar zo veel mogelijk op lijkt. Denk bijvoorbeeld aan iets als www.mediamarkt.promotie.be, of www.ing.security.nl: webadressen die op het eerste zicht betrouwbaar lijken, maar dus niet officieel zijn. Een andere variant van de tactiek is typosquatting, waarbij men een officiële naam inzet met een spellingsfout.

Typosquatting wordt echter veel minder gebruikt dan combosquatting, zo wijst de studie uit. De onderzoekers namen 468 miljard DNS-verzoeken onder de loep over een periode van zes jaar. Van die verzoeken ging 2,7 miljoen naar phishingwebsites die combosquatting toepasten. Die aanval kwam met een factor honderd meer voor dan instanties waar men gebruik maakte van typosquatting. Het aantal websites dat gebruik maakte van combosquatting groeide gestaag tussen 2011 en

2016. “Dit is een tactiek die criminelen meer en meer gebruiken omdat ze zien dat het werkt,” stelt Manos Antonakakis, een van de auteurs van de studie. “De aanval is openlijk te zien, maar veel gebruikers zijn niet onderlegd genoeg om het verschil te merken met de officiële URL van een bekende website.”

Combosquatting is onder andere zo talrijk omdat cybercriminelen in principe een oneindig aantal variaties kunnen gebruiken op bekende namen. Bovendien zijn die domeinnamen vaak niet erg duur. Verder stelde het onderzoek ook vast dat dit type website duurzaam is. Phishing-websites worden vaak erg snel offline gehaald zodra men ze rapporteert bij de politie. In hun onderzoek vonden de wetenschappers dat 60 procent van de ontdekte combosquatting-websites zo’n drie jaar actief waren. De onderzoekers hopen met hun studie meer aandacht te vestigen op dit type van phishing, en de nood aan betere informatie voor gebruikers.



DearBytes waarschuwt voor grote roof cryptomunten

Cybercriminelen hebben de jacht ingezet op cryptomunten. Met behulp van phishingmails roven ze op grote schaal bitcoins of ethers. Zij zetten verfijnde phishingcampagnes op, die in zeer korte tijd veel geld opleveren. Dat stelt beveiligingsbedrijf DearBytes. Het dochterbedrijf van KPN stelt dat phishing steeds vaker wordt gebruikt om toegang te krijgen tot de digitale portemonnees ('wallets') waarin bijvoorbeeld bitcoins of ethers worden bewaard. Met de onderschepte inloggegevens roven ze de wallets van de slachtoffers leeg.

'Phishing naar cryptocurrency is een opkomend fenomeen', zegt Wesley Neelen, ethical hacker bij DearBytes. 'Zo zijn er iedere dag tientallen phishingcampagnes actief die zijn gericht op de gebruikers van de dienst MyEtherWallet waarmee je etherwallets kunt aanmaken.'

Neelen ontving onlangs een zeer professionele phishingmail gerelateerd aan MyEtherWallet waarin staat dat inloggen noodzakelijk is om de wallet te synchroniseren. Na het klikken krijgt de ontvanger een gekloonde MyEtherWallet-website voorgeschoteld die zeer lastig van echt is te onderscheiden. Door slim gebruik te maken van buitenlandse karakters in de domein toont de url-balk gewoon 'myetherwallet.com'. Bij de url is een zeer beperkte afwijking te zien, zoals in dit geval een kleine komma onder de laatste letter. Zelfs het groene slotje in de url-balk dat duidt op een veilige verbinding is aanwezig.

Onderzoek DearBytes

Onderzoek van Neelen leert dat criminelen op deze manier grote geldbedragen binnenslepen. Samen met een collega analyseerde hij eerder deze week een 'live logfile' van een webserver die wordt gebruikt voor het phishen naar My-

EtherWallet-inloggegevens. De analyse leverde een compleet overzicht op van gestolen wallets. Een van de slachtoffers raakte 42.50 ether kwijt, wat neerkomt op ongeveer 10.600 euro. De opbrengst bedroeg in de eerste twee uur nadat de phishingmail is verstuurd ongeveer 13.000 euro.

Te treffen maatregelen

De sterke opkomst van cryptomunten heeft tot een goudkoorts geleid. Niet alleen bij de bezitters van cryptocurrency, maar ook bij de criminelen die hun buit alleen maar in waarde zien stijgen. Bezitters van cryptomunten moeten daarom extra alert zijn op diefstal. In onderstaand kader geeft DearBytes een aantal tips.

Tips van DearBytes

Inhoud bekijken: Kijk kritisch naar de inhoud van e-mailberichten, een cryptocurrencywebsite zal niet vragen om bepaalde acties uit te voeren, zoals het inloggen op een website.

Instellingen browsers: Sommige browsers kun je ook zo instellen dat vreemde karakters in de url wel worden getoond, zodat snel is te zien of het webadres klopt. Het belangrijkste blijft echter het kritische beoordelen van e-mailberichten die je ontvangt.

Inspecteer het webverkeer: Organisaties scannen vaak hun e-mails centraal, maar webverkeer nog niet. Daarmee vertrouwen ze erop dat medewerkers phishingwebsites herkennen. Phishingcampagnes zijn echter zo vernuftig, dat zelfs de meest doorgewinterde securityexperts hierin trappen. Dus zet een proxy- en/of webscanning-tool in om gebruikers te helpen om kwaadaardige websites te weren.

Bijna kwart doorgelaten e-mail onveilig

De ingebouwde beveiligingssystemen van e-mailproviders zijn niet opgewassen tegen de groeiende dreiging van hackers en cybercriminelen. Bijna 25 procent van door e-mailproviders 'goedgekeurde' en doorgelaten e-mail is alsnog onveilig. Dat blijkt uit het kwartaalonderzoek 'Email Security Risk Assessment' door Mimecast naar de veiligheid van bekende e-mailoplossingen als Google G Suite en Microsoft 365.

Mimecast onderzocht binnenkomende e-mail van ruim 62.000 gebruikers over een periode van 428 dagen. Meer dan 45 miljoen door de interne securitysystemen doorgelaten e-mails werden onder de loep genomen. Hiervan werd 31 procent door Mimecast als 'onveilig' bestempeld. De test stuitte tot nu toe op meer dan 10,8 miljoen spammails, 8682 onveilige bestandstypen, 1778 bekende en 503 onbekende malware-bijlagen en 9667 valse e-mails.

Nico Deen, marketing directeur Noord-Europa bij Mimecast, geeft aan dat het gaat om emailscans die zij uitvoeren in opdracht van potentiële klanten. 'Het zijn prospects die toestemming geven om hun e-mail te scannen in een zogeheten 'e-mail risk security assessment'. Die e-mails gaan door speciale filters; gegevens worden volledig geanonimiseerd. Het gaat dus niet om e-mailverkeer dat wij voor onze klanten monitoren.'

Het rapport onderschrijft de noodzaak voor een gelaagde aanpak als het gaat om e-mailbeveiliging. 'De interne beveiligingssystemen van e-mailproviders zijn duidelijk niet

meer afdoende. Het gebruik van extra e-mailbeveiligingsoplossingen is noodzakelijk voor een goede beveiliging tegen bijvoorbeeld ransomware of aanvallen waarbij de hacker zich voordoeft als iemand anders', zegt Lisette Sens, directeur Europese partners bij Mimecast. Veel organisaties geloven dat hun e-mailprovider passende bescherming kan bieden tegen e-maildreigingen. Dat is volgens Sens echter een vals gevoel van veiligheid. Zij roept de gehele industrie op om te werken naar een hogere standaard van e-mailbeveiliging.

Mimecast is een Britse leverancier van cloudgebaseerde oplossingen om e-mail te beveiligen en te archiveren. Het bedrijf heeft zijn hoofdkantoor tegenwoordig in het Amerikaanse Boston.



Deze vier dingen zijn strafbaar als je pikante foto's stuurt

Jij bent 14 en die leuke jongen uit je klas is 15. Je hebt al een paar keer geflirt maar je weet nog steeds niet of hij je wel leuk vindt. Dus maak je op een dag een foto van jezelf in je mooiste string en die stuur je hem via Whatsapp. Je krijgt even later een foto van hem, zonder boxershirt. Dat is toch niet strafbaar?

Nou, eigenlijk wel. Alle seksueel getinte afbeeldingen waar minderjarigen op staan zijn volgens de wet kinderporno. En het maken, verspreiden of bezitten van kinderporno is strafbaar. Dus ja, het meisje uit dit voorbeeld en haar vriendje zijn allebei formeel strafbaar. Maar de wetgever is niet gek. Als het gaat om twee pubers die vrijwillig een beetje flirten wordt er niemand vervolgd. Maar waar ligt dan de grens tussen een onschuldig experiment en strafbare sexting? Politie en justitie maakten vorige week bekend waar ze op letten als het gaat om pikante beelden van minderjarigen.

1 – Dwang

Elke pikante foto of video die niet vrijwillig wordt gemaakt is strafbaar. Er zijn veel manieren om iemand te dwingen zo'n foto te maken tegen zijn of haar zin. Door geld te bieden bijvoorbeeld, of door te dreigen met pesten, met geweld, of dreigen een geheim te verklappen. Wat ook strafbaar is: stiekem filmen of fotograferen, bijvoorbeeld na het sporten. Dat gebeurt immers ook zonder toestemming van het slachtoffer.

2 – Leeftijdsverschil

Als een van beide partijen 23 jaar of ouder is en de ander minderjarig, is het uitwisselen van foto's strafbaar. En ook als het gaat om jongeren tussen 12 en 23 die meer dan vijf jaar van elkaar verschillen. Bovendien geldt de strafbaarheid al-

tijd als er een kind onder de 12 bij betrokken is. De wetgever gaat er van uit dat er in al die gevallen geen sprake kan zijn van gelijkwaardigheid van de partijen en dat er dus sprake is van dwang.

3 – Verspreiding

Als een meisje je een pikante foto stuurt wil je daar graag over opscheppen. Dus laat je die aan je vrienden zien. Die zijn enthousiast en vragen om hem door te sturen. Dat lijkt onschuldig maar het is strafbaar. Zij heeft immers geen toestemming gegeven om de foto aan anderen te laten zien en al helemaal niet om de foto te verspreiden. Want als een van die vrienden de foto online zet kan iedereen hem zien. Ook pedofielen, ook de ouders van het meisje, ook de baas van de supermarkt waar ze werkt. De gevolgen zijn niet te overzien. En dat wordt jou als verspreider van de foto aangerekend, ook al had je op zich geen kwade bedoelingen.

4 - Motief

Verspreiding is dus al strafbaar als je alleen maar een beetje wilde opscheppen tegenover je vrienden. Maar als je daar een gemene reden voor had is dat extra strafbaar. Bijvoorbeeld als je een foto verspreidt als wraak omdat ze het uitmaakt heeft. Of om te pesten, of om er geld aan te verdienen.

Al het gedrag zoals in deze vier punten beschreven is strafbaar. Maar niet alles is even ernstig. In het ergste geval word je aangeklaagd voor kinderporno en beland je in de gevangenis. Maar sexting kan ook leiden tot vervolging vanwege smaad, laster, belediging of schending van het portretrecht. Daarvoor kan de rechter ook een alternatieve straf geven, zoals een verplichte cursus bij HALT.

Please Call Support For Windows Tech Support Scam

De telefonische ondersteuning voor Windows Tech Support Scam is een melding die weergeeft dat het heeft vastgesteld dat u veel pop-ups krijgt of dat uw computer mogelijk trager werkt. Vervolgens wordt u gevraagd om een extern ondersteuningsnummer voor hulp te bellen. Omdat dit een oplichting is, moet u het vermelde telefoonnummer niet bellen.

Gelukkig kan deze melding afgesloten worden door Windows taakbeheer te openen en het browserproces te beëindigen. Het is echter belangrijk dat als u het browserproces beëindigt, u eerder gesloten sites niet opnieuw opent als de browser u vraagt wanneer u het opnieuw start. Aan de andere kant, als u deze soorten van technische ondersteuningszwendel voortdurend ziet, of deze pagina's zelf opent, dan is het mogelijk dat u bent geïnfecteerd met een adware of een ander ongewenst programma dat die deze melding weergeeft. Gebruik dan een programma als AdwCleaner om adware te verwijderen..

AdwCleaner is een gratis programma dat Adware, Toolbars, Potentially Unwanted Programs (PUP) en browser kapers op uw computer opzoekt en verwijdert. Door AdwCleaner te gebruiken, kunt u eenvoudig veel van dit soort programma's verwijderen voor een betere gebruikerservaring op uw computer en tijdens het surfen op internet.

Mozilla heeft problemen met de nieuwe 'sleepwet'

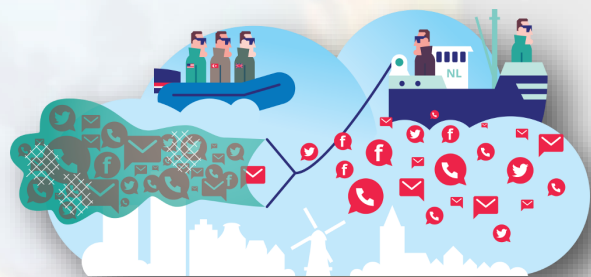
Mozilla-technici bespreken plannen om ondersteuning voor een door de overheid beheerde Nederlandse TLS / HTTPS-provider te verwijderen nadat de Nederlandse regering een nieuwe wet heeft goedgekeurd die lokale autoriteiten de bevoegdheid verleent om internetcommunicatie te onderscheppen met behulp van 'valse sleutels'. Als het plan wordt goedgekeurd, vertrouwt Firefox geen certificaten die zijn uitgegeven door de certificeringsinstantie (CA) van de Staat der Nederlanden.

Deze CA wordt beheerd door PKIOverheid / Logius, een afdeling van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties, hetzelfde ministerie dat toezicht houdt op de AIVD-inlichtingendienst. Nieuwe wetgeving geeft Nederlandse overheid de macht om internetverkeer te onderscheppen.

Wat de ingenieurs van Mozilla bang maakt, is de nieuwe Wet op de inlichtingen- veiligheidsdiensten (Wiv) Een nieuwe wet die dit jaar is goedgekeurd en die begin 2018 van kracht wordt. Deze nieuwe wet geeft Nederlandse autoriteiten de bevoegdheid om internetverkeer te onderscheppen en te analyseren. Hoewel andere landen vergelijkbare wetten hebben, is dit een bijzonderheid omdat autoriteiten autorisatie zullen hebben om geheime technische aanvallen uit te voeren om toegang te krijgen tot gecodeerd verkeer.

Dergelijke heimelijke technische mogelijkheden omvatten het gebruik van "valse sleutels", zoals vermeld in Artikel 45 1.b, een brede term die TLS-certificaten omvat.

Mozilla vreest dat de Nederlandse autoriteiten certificaten zullen afgeven via de door de lokale overheid beheerde CA, waarmee ze SSL-proxy's kunnen instellen voor het uitvoeren van Man-in-the-Middle (MitM) -aanvallen op alle gebruikers in een dragnet-achtige internetsurveillance-operatie.



Door de certificaten te wantrouwen, zal Firefox interceptiepogingen hinderen door SSL-certificaten voor die verbindingen weer te geven, waarbij de aandacht van de gebruikers wordt gevestigd op het feit dat er iets kan gebeuren. "Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties toestaan om een vertrouwde CA te blijven gebruiken in een land dat een belangrijk doorvoerpunt voor internet biedt, zou schadelijk zijn voor de veiligheid van alle Mozilla-gebruikers", zegt Chris van Pelt, de gebruiker die het probleem aan Mozilla drie meldde.

De kans is groot dat zowel Mozilla en eventueel alle andere grote browserleveranciers, de CA zullen wantrouwen.

Pas op met metadata in foto's

Tip 01: Metadata

Bij elke foto die je neemt met een digitaal toestel legt de camera niet alleen de afbeelding vast, maar voegt hij aan het bestand ook een heleboel randinformatie over die foto toe. Deze metadata, wat zoveel betekent als 'gegevens over gegevens', vormen als het ware de ingesloten informatiefiche van de foto. Metadata worden gegenereerd en opgeslagen bij digitale fototoestellen, maar ook bij geïntegreerde camera's, zoals die in je smartphone of tablet.

Tip 02: Exif-gegevens

Metadata zijn niet echt verborgen, maar je moet ze wel opvragen om ze te kunnen zien. Er zijn verschillende soorten metadata. Dat komt doordat deze gegevens niet gestandaardiseerd zijn. De meest bekende zijn de exif-tags, wat staat voor 'exchangeable image format'. Hierin staan de datum en tijd van de opname, het merk en het model van het toestel, een miniatuurafbeelding, de programmastand en een overzicht van alle instellingen (iso, diafragma, sluitertijd, brandpuntsafstand, flits, enzovoort).

Tip 03: Gps-locatie

Wanneer je toestel geolocalisatie ondersteunt, voegt het systeem in je camera of smartphone de coördinaten toe van de plaats waar je de foto hebt genomen. Dat is interessant wanneer je de foto later automatisch op een landkaart wilt weergeven. Deel je deze foto via het internet,

dan moet je wel weten dat de hele wereld hierdoor kan achterhalen in welk speeltuintje je kleuters vaak spelen en op welk adres je de prachtige interieurfoto's hebt genomen. Wil je al die privacygevoelige informatie niet delen, dan kun je de gegevens gelukkig verwijderen.

Tip 04: Verkenner

Wil je in Windows de exif-informatie uit een fotobestand bekijken en verwijderen, dan kun je dat eenvoudig doen via Windows Verkenner. Het nadeel van deze manier is dat je alleen de basisgegevens stript: je kunt niet alle exif-gegevens wissen. Open Windows Verkenner door op de combinatie Windows-toets+E te drukken en navigeer naar het fotobestand. Klik er met de rechtermuisknop op en kies Eigenschappen. Vervolgens open je het tabblad Details. Daar vind je de exif-informatie. Klik op Eigenschappen en persoonlijke gegevens verwijderen om de exif-data te wijzigen.

Mythes.

Het is overdreven te stellen dat je beter de metadata wist om de online fotobestanden veel kleiner te maken. De winst die je hierdoor boekt, is immers miniem.

Een tweede mythe is dat metadata verwijderen tegen de wet is. Uiteraard mag je de copyright-informatie niet weghalen van andermans foto's, maar zolang het gaat om je eigen afbeeldingen mag je ermee doen wat je wilt.

Malware omzeilt beveiliging: fileless malware

Antivirusprogramma's doorzoeken vooral bestanden op patronen van bekende malware-tools. Maar als er helemaal geen bestand op de harde schijf terechtkomt, zijn veel beveiligingsmaatregelen zinloos. Professionele spionnen, die zich richten op hooggeplaatste doelen in industrie en politiek, experimenteren al langer met zogeheten fileless malware. Nu is de cybermafia met een inhaalslag bezig.

Bij traditionele besmettingen van een computer, bijvoorbeeld met een exploit-kit, wordt de eigenlijke malware van internet gedownload en dan op de computer van het slachtoffer opgestart. Vervolgens gaat het kwaad zijn gang, bijvoorbeeld met bankfraude. Bij gerichte inbraken in bedrijfsnetwerken halen de aanvallers meestal eerst nog meer tools binnen om verder in het netwerk door te dringen. Beveiligingssoftware is daar inmiddels op ingesteld en zoekt gericht naar dit soort aanwijzingen voor een infectie.

Om ontdekking te voorkomen, laten cybercriminelen zo min mogelijk van dit soort sporen achter – insiders hebben het dan over Indicators of Compromise. Steeds vaker maken ze daarom helemaal geen bestanden meer aan. Kaspersky maakte bijvoorbeeld in februari melding van fileless attacks' bij meer dan 140 bedrijven in 40 landen. Daar zaten onder andere banken, overheidsinstanties en telecombedrijven bij.

Kaspersky vermoedt dat de daders te vinden zijn bij cybergangs die gespecialiseerd zijn in high-tech bankroof, zoals Carbanak en Gcman. Zulke fileless malware omzeilt niet alleen traditionele beveiligingsprocedures als het scannen van be-

standen door antivirussoftware. Ook moderne securityconcepten als de Software Restriction Policies en andere whitelisting-methodes doen er niks mee. De inbrekers gebruiken namelijk tools die al op het systeem aanwezig zijn voor de aanval en de daarop volgende data diefstal.

De onzichtbare aanwezigheid van malware staat of valt met ongemerkt binnendringen in het systeem. Office-bestanden met macro's vormen bijvoorbeeld een populaire invalspoort. In het ergste geval is een e-mail met een document zelfs speciaal afgestemd op de ontvanger, bijvoorbeeld in de vorm van een sollicitatie gericht aan de afdeling personeelszaken. De schadelijke code is daarbij versleuteld of in ieder geval onleesbaar gemaakt en wordt pas uitpakket bij het uitvoeren van de macro. Alternatieven daarvoor zijn JavaScript-bestanden (.js) en html-toepassingen (.hta) met JScript of VBScript. Echt zonder bestanden is dat allemaal nog niet. Uiteindelijk komt de malware toch in een bestand op de computer terecht. Je kunt het dus als zodanig herkennen en blokkeren of op zijn minst achteraf terugvinden in bijvoorbeeld de tmp-map van de getroffen gebruiker.

Bij besmetting met een exploit-kit (EK) werkt dat anders. Met de beruchte AnglerEK kun je al sinds 2014 malware zonder bestand binnendoelen op een doelcomputer en daar uitvoeren. Daarbij komt er niks meer in tmp-bestanden terecht. In plaats daarvan injecteert de exploit de schadelijke code in het werkgeheugen van een reeds actief proces en start het daar als nieuwe thread. Anglers concurrenten zoals de HanJuan-EK hebben deze techniek overgenomen.

Dat klinkt allemaal nog heel abstract, maar met een voorbeeld wordt het duidelijker. De fictieve gebruiker Lars kijkt als ontspanning na het werk graag naar kattenfilmpjes. Advertenties voor brokjes en krabpalen zijn voor hem dan ook niet meer dan normaal. Lars heeft geen idee dat een van de getoonde advertenties onderdeel uitmaakt van een malvertising-campagne waarmee de Angler-EK verspreid wordt. Lars hoeft niet eens op de advertentie zelf te klikken. In de code zit een onzichtbaar iframe dat zorgt voor een redirect naar de landing-page van de Angler-EK.

Dus terwijl Lars zich vergaapt aan Simon's Cat, controleert het JavaScript op de Angler-landing-page op de achtergrond zijn browser op beveiligingslekken. Is het raak, dan slaat de exploit toe. Om te beginnen controleert de binnengesmolde code of hij in een sandbox of een virtuele machine zit. Alleen als dat niet het geval is, laadt hij de eigenlijke payload van de internetserver van een oplichter. Die komt terecht in het werkgeheugen van de browser. Begint die met het typische 'MZ' van een PE-header, dan gaat het om traditionele malware. Het bestand wordt gewoon op de harde schijf gezet en uitgevoerd. Maar als de eerste twee bytes 0x9090 zijn, is er sprake van fileless malware.

Deze manier van besmetten heeft wel een probleem: zodra Lars zijn browser sluit, is alles weg. Zelfs als de inbrekers zich met OpenProcess en CreateRemoteThread in andere, continu draaiende processen als explorer.exe weten te nesten, is de nachtmerrie in ieder geval na een keer opnieuw opstarten voorbij. Dat kan precies de

bedoeling zijn als het om een doelwit gaat dat makkelijk opnieuw gehackt kan worden. Het voordeel is dan dat er geen sporen op het systeem achterblijven waaruit blijkt dat er ingebroken is of waarmee forensisch onderzoekers achteraf een duidelijk beeld kunnen krijgen van het gebeuren. De criminelen willen in geen geval bijzonder waardevolle hacktools op de harde schijf van hun slachtoffer laten rondslingeren. Dan zijn ze liever een deel van hun uitvalsbasis kwijt.



Europa stemt voor betere bescherming bij online aankopen

Het Europees Parlement heeft ingestemd met regels die consumenten beter moeten beschermen tegen fraude bij online aankopen. Deze regels bieden nationale autoriteiten meer mogelijkheden. Bij de stemming hebben 591 parlementsleden vóór gestemd en 80 tegen. Een aantal heeft geen stem uitgebracht.

Nationale autoriteiten krijgen hiermee meer mogelijkheden om schendingen van consumentenrecht bij online aankopen aan te pakken. Ook wordt het makkelijker om hun acties binnen de EU te coördineren en op elkaar af te stemmen.

Mazen dichten

De nieuwe regels zijn er onder meer op gericht om mazen in de wet te dichten en de verschillen tussen de EU-lidstaten te verkleinen.

Nationale autoriteiten moeten onder meer bij domeinbeheerders informatie kunnen opvragen om frauderende handelaren te kunnen identificeren.

Ook moeten ze voor een controle als mysteryshopper diensten en producten kunnen kopen.

Daarnaast moeten autoriteiten handelaren kunnen dwingen tot een oplossing voor gedupeerde consumenten.

Consumentenorganisaties

Verder zullen consumentenorganisaties meer worden betrokken bij het signaleren van misstanden. Mogelijk zijn deze organisaties hier sneller van op de hoogte dan de autoriteiten.

De Europese Commissie kan in actie komen als de fraude consumenten in ten minste twee derde van de lidstaten raakt of ten minste twee derde van de Europese bevolking treft.

BIT helpt politie met bestrijding cybercrime

Datacenterdienstverlener BIT zet zijn kennis van internettechnologie, de werking van e-maildiensten en het hosten van websites vrijwillig in binnen het project Greenfield Cyber.

Dit project is in het leven geroepen door de Nationale Politie om middels samenwerking met banken, internet-serviceproviders (isp's) en overheden cyberproblemen te beperken.

Het uitgangspunt van het project is door samenwerken met partners kennis te delen en coalities te smeden. Het doel van Greenfield Cyber is, volgens de politie, om de beweegredenen en manier van werken van de cybercrimineel te doorgronden, barrières en interventies te ontwikkelen en deze vervolgens om te zetten in acties om cybercrime aan te pakken. Allereerst wordt het fenomeen phishing aangepakt.

Volgens Wido Potters, managers sales & support bij BIT, vindt zijn bedrijf het een plicht om eenieder te voorzien van een veilig, open en vrij internet met waarborging van privacy. Daarnaast willen we ervoor zorgen dat het vertrouwen in internet niet verloren gaat. Als isp merken we dat door alle internetcriminaliteit het vertrouwen daalt en dat is slecht voor de digitale economie.'

Naast BIT zijn er nog andere samenwerkingspartners, te weten ING, Rabobank, De Volksbank, Bitonic, i3D.net, NSCR (Nederlands Studiecentrum Criminaliteit en Rechtshandhaving), het Openbaar Ministerie en het ministerie van Defensie



Grootste gevaar zit achter de computer

Het grootste gevaar online zit niet in de computer, maar achter de computer: de mens. Die opent links en bijlagen zonder op te letten, laat overall wachtwoorden achter en koopt apparaten met een krakkemikkige beveiliging. 'Picnic' heet dat als het weer eens misgaat: Problem In Chair, Not In Computer.

"Fouten in software zijn te repareren, fouten in de hersenen niet. Mensen leren niet. Wij zijn dinosaurussen, hopelijk doet de volgende generatie het beter", zegt Mikko Hyppönen. De Fin is topman van de belangrijke cyberbeveiligers F-Secure.

Internet of Things zorgt voor nieuwe revolutie Cyberbeveiligers als Hyppönen hebben een paar belangrijke jaren voor de boeg. Er is een nieuwe revolutie op komst: het internet der dingen. "In de afgelopen decennia zijn alle computers, laptops, smartphones en tablets online gegaan. Nu volgen alle andere apparaten." Wasmachines, broodroosters, koelkasten en sapcentrifuges, maar ook auto's en knuffels. Zulke apparaten zijn vaak slecht beveiligd. Hyppönen:

"Consumenten kijken naar de prijs, die vragen niet naar de firewall van een broodrooster."

Ingang tot het thuisnetwerk via de wasmachine Het grote gevaar zit niet in het hacken van het apparaat zelf. "Stel dat iemand je wasmachine hackt. Een hacker is echt niet geïnteresseerd in je kleren. Maar het is een ingang. Via je wasmachine kan hij in je thuisnetwerk kijken, en uiteindelijk kan hij bijvoorbeeld creditcardgegevens stelen."

Hacken van zelfrijdende auto's

Hetzelfde met slimme auto's. "Alles wat hackers doen, is logisch. Een hacker zal echt de remmen niet saboteren, zoals je in films ziet. Dan ga je dood en lever je ze geen geld op. Maar ze kunnen misschien wel je portier openmaken en je auto starten zonder sleutel. En misschien word je 's ochtends wakker, kijk je uit je raam en is je zelfrijdende auto zelf, op afstand bediend, naar een hacker in Litouwen gereden."

Onbeveiligde camera's: de rest kijkt mee

Wat Hyppönen bijvoorbeeld niet begrijpt, is dat sommige mensen een onbeveiligde camera zonder wachtwoord in huis hangen. "Ja, je kan je kinderkamer of je woonkamer zien. Maar de rest van het internet kijkt met je mee." Hackers kunnen zulke camera's bovendien 'rekruteren' voor hun cyberleger. Vorig jaar werd het internet in de Verenigde Staten grotendeels platgelegd door een gecoördineerde aanval met miljoenen gekaapte printers, babyfoons en bewakingscamera's. Onlangs kwam een nieuw netwerk aan het licht, wat betekent dat er misschien een nieuwe aanval op komst is.

Gijzelsoftware

Dit jaar waren er ook drie grote aanvallen met gijzelsoftware. Een daarvan trof onder meer een containerterminal in Rotterdam. „Daarna werd in bestuurskamers gesproken over cyberbeveiliging, maar dat is nu al voorbij. Blijkbaar hebben mensen een digitale ramp nodig om wakker te worden."

Hoe voorkomt u cyberaanvallen via Office-documenten?

Cybercriminelen voeren op grote schaal systeem-commando's uit via Office-documenten. Microsoft verhelpt het probleem niet. Beveiligingsbedrijf DearBytes heeft daarom drie maatregelen op een rij gezet waarmee de dreiging van dergelijke aanvallen kan worden gemitigeerd.

De aan Rusland gelinkte hackersgroep Fancy Bear, ook wel bekend als APT28, heeft de afgelopen weken Word-documenten de wereld in verspreid met namen als 'IsisAttackInNewYork.doc' en 'SabreGuard2017.docx'. Deze bestanden bieden in de praktijk echter geen nieuws over de terreuraanslag van eind oktober of over een oefening van het Amerikaanse leger in Oost-Europa. Op het moment dat gebruikers de documenten openen, worden zij geïnfecteerd met een stukje malware genaamd Seduploader. Hiermee scannen ze de computer van het slachtoffer om te kijken of het zin heeft om spyware te installeren.

Misbruik van lek in DDE

Fancy Bear maakt al vanaf eind oktober gebruik van een lek in de Microsoft Office-feature Dynamic Data Exchange (DDE). Dit onderdeel maakt het mogelijk om data van het ene Word-document in een ander Word-document te injecteren en biedt aanvallers daarmee een alternatief voor macro's. DDE is echter ook te misbruiken via Microsoft Outlook en Calendar-uitnodigingen, waardoor een aanvaller in de vorm van een e-mail zonder attachment vrij eenvoudig zijn code bij een slachtoffer krijgt. Erik Remmelzwaal, directeur bij DearBytes, zegt: "Cybercriminelen zijn snel boven op het lek gedoken, onder andere voor het verspreiden van de ransomware Locky. Organisaties hebben dus

maar kort de tijd om kritieke lekken te patchen en misbruik onmogelijk te maken."

Mitigerende maatregelen

Omdat Microsoft zelf geen actie heeft ondernomen, adviseert DearBytes daarom de volgende 3 maatregelen te treffen om te voorkomen dat organisaties slachtoffer worden van aanvallen via Office-

1. Schakel DDEAuto uit

Maak bijvoorbeeld gebruik van 'Disable DDEAuto'. Dit is een registryfile die wordt bijgehouden op GitHub en ervoor zorgt dat de 'update links'- en 'embedded files'-functionaliteiten worden uitgeschakeld.

2. Bekijk de oplossingen die Microsoft aanreikt

Microsoft legt op hun TechNet-website en op de supportwebsite uit hoe je OLE-objecten en macro's beter onder controle krijgt. Dit voorkomt echter niet dat .exe-bestanden direct worden gedownload en uitgevoerd.

3. Voorkom dat Office-onderdelen bepaalde andere executables aanroepen

Het gevolg van een DDE- maar ook van een macro-aanval is dat een aanvaller bijvoorbeeld Word of Outlook een ander programma laat starten. Nu is het niet vreemd dat Word een printerprogramma aanroept, maar dat het een systeemcommando wil uitvoeren, is voor de meeste gebruikers zeldzaam. Het researchteam van DearBytes meldt dat het gebruik van endpoint-protectionsoftware een effectieve methode kan zijn om te voorkomen dat Office-applicaties bepaalde andere executables starten. DearBytes heeft met behulp van McAfee Access Protection een blokkerende rule ontwikkeld die uitvoer van kwaadaardige code via DDE voorkomt. In deze 'blokkade' zijn bijvoorbeeld ongebruikelijke executables opgenomen zoals cmd.exe, powershell.exe, rundll32.exe en cscript.exe. De rule blijkt naast DDE-aanvallen ook effectief tegen macro-aanvallen.

Sterke stijging van het aantal impersonatieaanvallen

Cybercriminelen gebruiken steeds vaker impersonatietechnieken voor het omzeilen van e-mailbeveiligingssystemen. Bij een impersonatieaanval doet een cybercrimineel zich voor als iemand anders, vaak een persoon met een hoge functie binnen de organisatie. Via een authentiek ogende e-mail vraagt de aanvaller aan een nietsvermoedende medewerker om bijvoorbeeld een grote som geld over te maken.

Dat blijkt uit het Email Security Risk Assessment (ESRA)-rapport van Mimecast, specialist op het gebied van e-mailsecurity en -archivering. Veel bedrijven hebben hun e-mailbeveiliging ingericht op het voorkomen van malwarebesmettingen. Aanvallers zijn daardoor op zoek gegaan naar nieuwe manieren om slachtoffers te maken.

Forse stijging

Dit zien we terug in de cijfers. Het aantal malwareaanvallen via e-mail nam het afgelopen kwartaal wereldwijd met 'slechts' 15 procent toe. Het aantal impersonatieaanvallen groeide in diezelfde

periode echter met bijna 50 procent. Bovendien bleken e-mailbeveiligingssystemen bijna 7 keer zoveel impersonatieaanvallen te missen als malwareaanvallen.

Deze bevindingen liggen in het verlengde van een recente PhishMe-studie. Daaruit bleek dat ongeveer twee derde van de ondervraagde IT-managers te maken had met een veiligheidsincident dat voortkwam uit een misleidende e-mail.

Effectieve misleiding

"Impersonatieaanvallen zijn een gemakkelijke en effectieve manier om nietsvermoedende slachtoffers te misleiden. Hackers winnen vertrouwen met een combinatie van social engineering en technische middelen", zegt Ed Jennings, chiefofoperating officer bij Mimecast. "Dit laatste ESRA-rapport onthult dat veel e-mailbeveiligingsoplossingen zeer kwetsbaar zijn voor deze moeilijk te detecteren aanvallen. Cybercriminelen weten dat traditionele e-mailbeveiligingsdiensten hun mogelijkheden verbeteren om malware te stoppen, maar ineffectief blijven tegen impersonatie."

Interpol en FBI halen groot botnet uit de lucht

Bij een internationale politieactie is een groot botnet ontmanteld. Het netwerk van miljoenen gekaapte computers verspreidde onder meer ransomware en spyware. Een man uit Wit-Rusland is opgepakt.

Het netwerk, dat ontmanteld werd door de FBI en Interpol, heeft de naam Andromeda gekregen. De malware achter het botnet infecteerde computers, die daarvoor ook deel van Andromeda werden en voor verdere verspreiding zorgden.

De organisaties konden totnogtoe al twee miljoen unieke ip-adressen van slachtoffers identificeren, in 223 landen. Volgens Microsoft, dat meewerkte aan het onderzoek gaat het vooral om Aziatische landen. Al laat het bedrijf op een kaart zien dat de malware ook actief was in Europese landen, waaronder België. Microsoft analyseert dat het botnet verantwoordelijk voor verspreiding van verschillende soorten malware, waaronder de ransomware Petya.

Onderzoek

Andromeda wordt ook in verband gebracht met een ander netwerk, Avalanche. Dat probeerde gebruikersnamen en wachtwoorden voor internetbankieren in handen te krijgen. Bovendien wilden de

makers computers vergrendelen met gijzelsoftware. Avalanche werd vorig jaar uit de lucht gehaald na vier jaar onderzoek. Informatie uit die zaak werd gebruikt bij het oprollen van Andromeda.

Cybercrime

Het onderzoek werd uitgevoerd door justitie in de Verenigde Staten en Duitsland, in samenwerking met de Europese politiedienst Europol, de justitiële samenwerking Eurojust en Microsoft. "Dit is een mooi voorbeeld van een hoe bedrijven en internationale organisaties samenwerken om wereldwijd verspreide malware neer te halen. Hieruit kunnen we leren dat we door publiek-private samenwerking deze criminelen kunnen tegenhouden en zo het internet veiliger kunnen maken voor ons allemaal", zei Steven Wilson, het hoofd van Europols Cybercrime-afdeling.

Politie spoort 97 money mules in Nederland op

De Nederlandse politie heeft tijdens een internationale operatie 97 money mules opgespoord en 18 gearresteerd. De money mules lieten hun rekeningen gebruiken voor het witwassen van geld dat voornamelijk via cybercrime was verkregen, zo heeft de politie bekendgemaakt.

In totaal werden bij de internationale operatie met de naam "EMMA3" 766 money mules geïdentificeerd en in totaal 159 verdachten aangehouden. Ook werden 59 personen geïdentificeerd die money mules rekruteren. Aan de operatie deden opsporingsdiensten uit 26 landen mee, alsmede ruim 250 banken en private partijen, zo laat Europol weten.

De money mules zouden voor ruim 1700 transacties zijn gebruikt, waar een bedrag van bijna 31 miljoen euro is gemoeid. In Nederland gaat het om een bedrag van bijna 5 miljoen euro. Meer dan 90 procent van het

geld is afkomstig van cybercrime, zoals phishing, veilingfraude en ceo-fraude.

"In Nederland zien we dat ook jonge mensen vatbaar zijn om zich te laten verleiden/misbruiken door criminelen om crimineel geld wit te wassen. Deze doelgroep moet zich ervan bewust zijn dat de pakkans hoog is en de gevolgen voor de money mule ingrijpend", zegt Caroline Sander, teamleider van de ECTF van de Landelijke Eenheid. Money mules draaien namelijk op voor de schade, die vaak oploopt tot duizenden euro's, zo laat de politie weten. Ook worden money mules strafrechtelijk vervolgd. Verder kunnen ze acht jaar lang geen gebruikmaken van veel financiële diensten van banken. Ze kunnen dan bijvoorbeeld geen lening afsluiten of een nieuwe rekening openen.

Fingerprinting

Nu we in Europa en masse cookies zijn gaan blokkeren, zijn adverteerders meer overgestapt op fingerprinting. Hoe werkt dat precies en wat kun je er tegen doen als je niet wilt dat je op deze manier wordt gevolgd.

Door een trackingcookie te verwijderen, raakt je volger het spoor bijster. Cookies zijn daarom feitelijk een bijzonder transparante manier van privacyschending en daar was echt geen wetgeving tegen nodig. Browser-fingerprinting is daarentegen veel lastiger te bestrijden en je moet als gebruiker meer stappen zetten om je te verbergen in de massa.

Browser-fingerprinting is een paraplu-naam voor verschillende methodes die specifieke elementen detecteren die jouw browser uniek maken. Welke plug-ins, updates, schermresolutie, UA-string, onderliggende software en andere elementen je hebt, maken jouw browser uniek tussen miljoenen andere browsers.

Een simpel rekenvoorbeeld: stel dat 10.000 mensen dit artikel lezen. Die groep kun je aan de User Agent-string alleen al opsplitsen. Die informatie wordt gebruikt door webdiensten om te zien wat voor browser contact probeert te leggen en bevat daarom informatie als browser-engine, versienummer en het OS dat de browser draait. In het voorbeeld van de 10.000 Computerworld-lezers gebruikt de meerderheid Chrome, gevolgd door IE en Firefox. De grootste groep, Chrome-gebruikers, kun je verder onderverdelen in versies: van die 10.000 bezoekers heb je nieuwe versie Chrome 62 (176 gebruikers), Chrome 61 (3516 gebruikers), Chrome 60 (219) en 56 mensen draaien nog steeds versie 59.

Die subgroepen zijn verder op te splitsen aan de hand van besturingssystemen. Als je kijkt naar de grootste groep van die 10.000 bezoekers - de groep van 3516 lezers die Chrome 61 draait - zijn dat statistisch gezien 1639 gebruikers met Windows 7, 1029 hebben Windows 10, 103 lezers een Linux-distributie en 117 stuks een Mac.

Nou zullen deze cijfers niet helemaal stroken met de werkelijkheid, omdat Linux-gebruikers traditioneel diversere browsers gebruiken (Opera, Chromium, Firefox) dan mensen die Windows draaien en Mac-gebruikers vaker Safari - maar je snapt het basisidee. En dat gaat alleen nog maar om verfijning met de UA-string, een van verschillende elementen die worden gebruikt om browsers van elkaar te scheiden.

Een andere techniek is het gebruiken van HTML5-element canvas. Zelfs zonder de UA-string kunnen webserver achterhalen met welke client ze van doen hebben, door de manier waarop tekens worden gerenderd in HTML5. Die rendering verschilt in detail per specifieke configuratie, aan de hand van je OS, browser, grafische kaart of chipset.

Met een relatief kleine set aan tekens die worden gerenderd, ziet de webserver al zoveel verschillende variaties tussen bezoekers om ze van elkaar te kunnen scheiden. In een uitgebreid rapport van twee onderzoekers van de universiteit van Californië wordt dit in detail uiteengezet (PDF).

Deze methode is wat meer onder de aandacht gekomen, omdat Firefox vanaf versie 58 gebruikers een melding geeft als sites deze beeldinformatie willen hebben, waardoor gebruikers zich bewuster worden van deze feature. Dit is natuurlijk geen verkeerde ontwikkeling, maar het gebruik van canvas is dus slechts één factor van vele om unieke bezoekers te volgen.

Engeland: Politie waarschuwt voor 'grooming gangs'

Ook al worden er in Engeland en Wales maandelijks meer dan vierhonderd mannen opgepakt voor kindermisbruik en grooming, de arrestatie van zes jongeren in Stratford op één dag sloeg in als een bom.

De bende zou, met een lokale McDonald's als 'hoofdkantoor' zo'n dertig slachtoffers hebben gemaakt. Vier meisjes (13 en 15) hebben aangifte gedaan, de politie probeert de anderen over te halen dat ook te doen.

Volgens Detective Inspector Laura Hillier van de Metropolitan Police werden de meiden bij het fastfood-restaurant meegelokt en elders misbruikt. Hillier denkt dat de omvang van de zaak veel groter is als nu bekend maar ook dat het strak georganiseerde bendes zijn.

De jongste daders, meestal van dezelfde leeftijd als de slachtoffers, moesten contact leggen en de meisjes naar bepaalde locaties rijden waar oudere mannen meegingen in het misbruik.

Drank en drugs spelen een belangrijke rol, maar ook gewoon geld. Volgens Chief Constable Simon Bailey van de National Police Chief's Council zijn er in het hele land van zulke bendes actief. 'I think more children are being exploited because the volume of reports we are receiving just keeps on growing...

Profielfoto's meisjes misbruikt voor sekschantage op Twitter

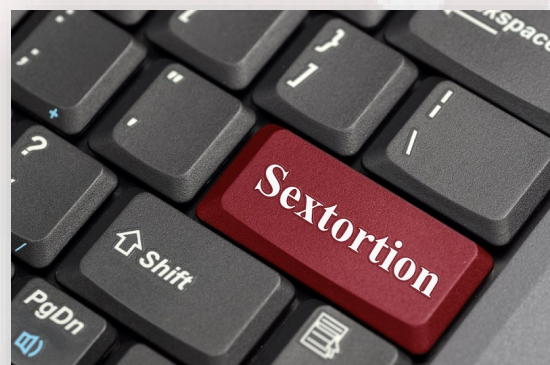
Van minstens vijf meisjes uit Brabant zijn profielfoto's misbruikt voor sekschantage op twitter. De foto's, gepikt van Instagram-accounts, werden ingezet om klanten te lokken voor seksdates en webcamshows.

Zo bood Sexy Bibi voor 100 euro een date van twee uur, op een adres waar een huis te koop staat. Naughty Kitty was goedkoper, 75 euro, haar adres gaf ze pas vrij na betaling. Onbekend is hoeveel meisjesfoto's in totaal zijn gebruikt door de oplichters. Volgens de politie zijn ook foto's van meisjes uit Zweden en de VS ingezet door deze oplichters. Mannen die op de tweets ingaan, worden gechanteerd. Ze moeten flink dokken, 'anders vertellen we je familie en werkgever dat je afspreekt met minderjarige hoertjes'.

Een van de meisjes is Elodie (17) die haar foto's terugvond met seksuele berichten eronder. 'Er stond dat ik zin had in een grote, zwarte pie-mel'. Foto's die ze op haar eigen instagram zette, stonden tien minuten later op twitter. Slechts met grote moeite wist ze het twitter-profiel verwijderd te krijgen. Dat lukte 'Melanie' niet. Ze stuurde haar id-bewijs al naar twitter maar het profiel is nog steeds online. Met wel drieduizend volgers.

Behalve aan twitter vragen de account te blokkeren, is aangifte doen natuurlijk een logische stap. Politiewoordvoerder Eric Passchier zegt dat zeker vijf meisjes al aangifte hebben gedaan. Van de gedupeerde mannen heeft nog niemand dat gedaan, vermoedelijk uit schaamte. De politie vraagt hen toch zich te melden.

Internetjurist Arnoud Engelfriet vreest echter dat de zaak 'waarschijnlijk niet veel prioriteit krijgt', zeker niet als de dader uit een land komt waarmee Nederland geen uitleveringsverdrag heeft. Bovendien blijft er ook dan altijd wel ergens een fotootje zwerven. 'Je blijft er altijd een beetje achteraan hollen' maar het internet is ook weer zo groot 'dat de kans klein is dat je het zelf tegenkomt'. Daar zit ook iets positiefs in, zegt hij. 'Je kunt je afvragen: als je het niet doorhebt, hoeveel last heb je er dan van?' Andere experts adviseren regelmatig jezelf te googelen.



Geavanceerde Beveiliging via U2F voor Google-accounts

Google lanceert nieuwe maatregelen om accounts extra te beschermen tegen indringers van buitenaf. Vanaf heden kun je jezelf aanmelden voor de Geavanceerde Beveiliging-instellingen, die werken via U2F.

Uiteraard is het al lang mogelijk om Google-accounts te beveiligen met authenticatie in twee stappen, waarbij een extra toegangscode per sms wordt verzonden. Maar wanneer een account is beschermd met de nieuwe, geavanceerde beveiligingslaag van Google, komt daar nog een derde optie bij.

Het programma maakt namelijk gebruik van de Universal 2nd Factor, oftewel U2F. Dat betekent dat er tijdens de inlogprocedure een fysieke sleutel op een apparaat aangesloten moet zijn, in de vorm van een U2F-usb-stick of bluetooth-dongle.

Investering

Google raadt de Yubico FIDO U2F Security Key aan voor pc's en de Feitian MultiPass FIDO-beveiligingssleutel voor smartphones. Die kosten enkele tientjes per stuk. Waarschijnlijk hebben de meeste reguliere gebruikers dat er niet voor over. Voor hen is deze beveiligingscheck voldoende.

Het blijft overigens niet bij deze maatregel. Eenmaal aangemeld bij dit beveiligingsprogramma, kunnen apps en programma's van derden geen toegang meer krijgen tot je Google-account. Ook kun je Google-diensten alleen nog maar gebruiken via de Chrome-browser.



E-mail spoofing

E-mail spoofing is een term die gebruikt wordt om frauduleuze e-mailactiviteiten te beschrijven. Deze activiteiten houden in dat specifieke eigenschappen van het e-mailbericht, zoals From (Van), Return-Path (Afzender) en Reply-To (Antwoorden naar) worden gewijzigd. Hierdoor lijkt het alsof de e-mail afkomstig is van een andere bron. E-mail spoofing is een veelgebruikte techniek voor het versturen van spam.

Spoofing-van e-mailadressen is vrij gemakkelijk. Alles wat iemand nodig heeft om een e-mailadres te spoofen is een SMTP (Simple Mail Transfer Protocol) server (een server die e-mail kan versturen) en de juiste e-mailsoftware. De meeste website hosting diensten zullen zelfs een SMTP-server in hun hosting pakket. Het is ook mogelijk om e-mail van uw eigen computer te verzenden als u een SMTP-server erin laadt, maar de meeste ISP's blokkeren poort 25 (die vereist is om e-mail te versturen).

Veel van de beschikbare gratis SMTP-servers laten u toe om een ander 'vanaf'-adres te tonen dan het daadwerkelijk geregistreerde domein waaruit de e-mail wordt verzonden. Echter, aan de ontvanger van het bericht, zullen ze zien dat het daadwerkelijk afkomstig is van het adres dat u heeft gespecificeerd.

Hoe kan ik mezelf beschermen tegen spoofing?

- Gebruik uw spamfilters. Bijna elke gratis (en betaalde) e-mailservice heeft spamfilters en junkboxen. Als er iets naar je junk mail gaat, moet je het niet gewoon deblokkeren. Onderzoek de email, ook al lijkt het dat het komt van iemand die je kent. Zorg ervoor dat het echt van die persoon is gekomen en dat het voor u bestemd is.
- Klik nooit op een onverwachte link of download een onbekende bijlage. Bijna alle grote bedrijven (zoals banken) hebben een beleid dat vereist dat als ze u nodig hebben om op een link naar hun site te klikken, ze een of andere identificatie bevatten, zoals uw naam of laatste vier cijfers van een rekeningnummer. Let hier vooral op. Te veel mensen zien een generieke e-mail die gewoon zegt: "Uw account is in gevaar gebracht, klik hier om te valideren." Geen legitieme bank of instelling zal dat ooit verzenden. Zij zouden zeggen: "Beste heer/mevrouw XXXX, wij geloven dat uw account is gecompromitteerd, bel ons op XXX-XXX-XXXX."
- Leer om e-mailberichtenkoppen te lezen en domeinnamen en IP-adressen te controleren. Bijna alle e-mailprogramma's laten u met uw muis over een e-mailadres schuiven. Wat je in de pop-up (meestal linksonder in het scherm) ziet, moet identiek zijn aan waar je overheen schuift. Als het iets anders is, dan is het waarschijnlijk spam of phishing voor informatie.

Protectie tegen e-mailphishing (DMARC, DKIM en SPF)

Phishing protectie

Fishing wordt door aanvallers toegepast om e-mails te vervalsen en betrouwbaar te laten lijken, terwijl ze dat in werkelijkheid niet zijn. De standaarden SPF, DKIM en DMARC worden gebruikt om de integriteit (echtsheidskenmerken, e-mailauthenticatie) van e-mail te borgen, zodat ontvangers kunnen controleren of e-mails ook daadwerkelijk afkomstig zijn van de veronderstelde afzender. Dit betekent dat phishingmails van aanvallers beter kunnen worden herkend, en dat de kans op misbruik afneemt.

SPF, DKIM en DMARC werken op domeinnaamniveau, en maken gebruik van DNS als mechanisme om bepaalde informatie te delen met het gehele internet. Ondanks het feit dat het gebruik van DNSSEC niet noodzakelijk is voor deze standaarden, wordt het gebruik ervan sterk aangeraden. Doordat DNSSEC de authenticiteit en integriteit van DNS antwoordberichten borgt, kan deze worden gebruikt als onderliggende beveiligingslaag voor andere beveiligingsstandaarden zoals SPF, DKIM en DMARC.

Wat is DKIM?

DKIM staat voor Domain Keys Identified Mail. Met DKIM kunnen e-mailberichten worden gewaarmerkt. De ontvanger van een e-mail kan op die manier controleren of een e-mailbericht écht van de afzender afkomstig is en of het bericht onderweg ongewijzigd is gebleven. DKIM houdt zelf geen spam tegen, maar markeert legitieme e-mail als geldig met behulp van een DKIM handtekening. De ontvangende mailserver kan vervolgens op basis van de public key in het DNS-record valideren of de DKIM handtekening klopt. Een spamfilter kan vervolgens op basis van een foutieve of ontbrekende DKIM handtekening e-mail beschou-

wen als SPAM. Het gebruik van DKIM helpt dus wel om spam te bestrijden.

Wat is SPF?

Het protocol Sender Policy Framework (afgekort SPF) heeft als doel spam te verminderen. SPF controleert of een verzendende mailserver die e-mail namens een domein wil versturen, ook daadwerkelijk gerechtigd is om dit te mogen doen. SPF voegt een extra informatieveld toe aan het DNS-record van een domein. In dit record wordt op basis van IP-adressen en/of hostnames vermeld welke mailservers namens dit domein e-mail mogen verzenden (een whitelist). Staat een mailserver niet in dit record en verzendt deze toch e-mail met het betreffende domein als afzender, dan wordt de e-mail beschouwd als SPAM.

Wat is DMARC?

DMARC staat voor Domain-based Message Authentication, Reporting and Conformance. Met behulp van deze standaard kan een e-mailprovider kenbaar maken hoe andere (ontvangende) mailservers om dienen te gaan met de resultaten van de SPF- en/of DKIM-controles van ontvangen e-mails. Dit gebeurt door het publiceren van een DMARC beleid in het DNS-record van een domein. In versimpelde vorm stelt dit beleid bijvoorbeeld: "als de DKIM-handtekening niet klopt of ontbreekt, of als de verzendende mailserver niet voorkomt in de lijst met geautoriseerde mailserver, behandel deze e-mail dan als SPAM".

Dit betekent wel dat een beheerder van een domein dient te borgen dat DKIM en SPF goed blijven functioneren, omdat fouten ook kunnen resulteren in het beschouwen van legitieme e-mailberichten als SPAM.

Cops in cyberspace

De politie heeft in de eerste tien maanden van 2017 al 160 malafide webshops offline gehaald, tegen 35 in heel 2016. Volgens projectleider Gijs van der Linden van het Landelijk Meldpunt Internetoplichting (LMIO) zijn er vooral in de laatste paar maanden van het jaar erg veel van die malafide webshops actief: sinterklaas- en kerstinkopen! Dat valt enerzijds op, anderzijds wordt de fraude ook harder aangepakt: al na drie aangiften worden betaaldiensten ingelicht die de rekeningen kunnen blokkeren. Veelvoorkomend zijn Chinese internetoplichters die domeinnamen opkopen die niet meer actief zijn. Op de site van een lokale bakker kan dus 'zomaar' elektronica worden verkocht. Oppassen, adviseert Van der Linden. 'We hebben voorbij zien komen dat een domeinnaam van een forum over kanker ineens kleding verkocht'.

Omdat de Greater Manchester Police weigert de gegevens van haar zoon te verwijderen, heeft een moeder het korps aangeklaagd. Het joch stuurde in 2015, 14 jaar jong, een pielfoto via Snapchat naar een vriendinnetje. De schoolleiding merkte dat en vertelde het zijn moeder. De politie legde de jongen uit dat het om kinderporno ging en maakte daar keurig melding van in de politiesystemen. De zaak werd geseponeerd maar alle gegevens staan nog steeds in het systeem. Volgens zijn moeder kan hem dat later schaden, bijvoorbeeld als hij gaat solliciteren. 'For all of his adult life it hangs over him', vertelde ze de BBC. Ze vindt het gek dat kinderen 'gecriminaliseerd' worden voor iets waarvoor ze niet eens zouden worden aangepakt als ze 18 zijn. Haar advocaat stelt dat de jon-

gen 'recht heeft op een privéleven', de politie verwijst naar wetten en beleidsregels. Het is de eerste rechtszaak op dit gebied in Engeland.

In de VS is een geheim agent (35) veroordeeld omdat hij rond de 1600 bitcoins gestolen had uit een wallet van de Amerikaanse overheid. Opvallend is dat de man al zes jaar celstraf uitzit voor een andere bitcoinroof. Hij was in 2013 betrokken bij het oprollen van het illegale Silk Road en wist toen voor tonnen aan bitcoins te stelen van de verdachte eigenaren. Tijdens verlof wist hij de nieuwe diefstal te plegen. De bitcoins waren door de overheid in beslag genomen bij een bitcoinbeurs. De verdachte agent wist de wallet echter te kraken en de bitcoins, omgerekend zo'n 10 miljoen euro, op z'n eigen rekening te zetten. Hij moet, na het uitzitten van de eerste straf, de nieuwe straf van twee jaar uitzitten.

De FBI heeft veel moeite met het ontsleutelen van de telefoon van Devin Kelley, de man die vorige week in/bij een kerk in Texas 26 mensen neerschoot. Volgens FBI-topman Christopher Combs is zelfs onbekend hoeveel tijd nodig om het apparaat te kraken. 'Dat kan morgen zijn, volgende week of over een maand'. Kelley zelf kan in ieder geval niet meer om toestemming gevraagd worden. Combs wil verder niet zeggen welk toestel Kelley gebruikte. 'Ik wil niet tegen iedere schurk zeggen welke telefoon hij moet kopen'. De FBI meldde eerder dat er nog zo'n 7500 mobiele apparaten op ontsluiting wachten. Een daarvan is de telefoon van de extremist die in 2015 in Garland het vuur opende op een

cartoon-tentoonstelling. Deze man zou meer dan honderd appjes hebben gestuurd naar 'een terrorist in het buitenland' maar 'we weten nog steeds niet wat hij toen zei'. Justitie-minister Jeff Sessions klaagde daarom al over de gebrekkige medewerking van techbedrijven.

Onlangs in Italië circa vijftig zogeheten Cumps opgepakt. Cumps zijn jonge maffiosi, vaak zoons of neven van de oude maffia-garde. Ze verdienen bakken met geld, gebruiken zware wapens en voelen zich onaantastbaar. Dat blijkt vooral op sociale media – precies daar werd het bewijs tegen hen gevonden. Politie en OM vonden daar vrij simpel honderden foto's en filmpjes waarin ze met dure spullen pronkten, grootse feesten hielden en trots lieten zien wat ze allemaal aan rijkdom verzameld hadden – opsporing was nog nooit zo gemakkelijk! De NOS spreekt van een trend: 'terwijl hun vaders en ooms vooral de luwte opzochten om een low profile te bewaren, SnapInstaFaceAppen de jonkies zich in het blikveld van de politie en worden ze makkelijk gegrepen'. Ook de politie zelf speelt een rol. Volgens inspecteur Michele Spina uit Napels hebben de jonge camorristi geen rolmodellen meer. 'De oude garde hebben we opgepakt en ze kunnen van niemand meer leren hoe je een clan leidt'. Alleen uit tv-series of films maar ja, 'daar leren ze niet wat een crimineel leven inhoudt'.

Rechtspraak

De rechtbank Midden-Nederland heeft twee mannen (24, uit Utrecht en Amsterdam) veroordeeld tot respectievelijk zes en vierenhalf jaar celstraf voor grootschalige drugshandel via het dark web en het witwassen van bitcoins. De mannen verkochten een half jaar lang drugs, vooral speed en xtc, aan klanten in onder meer Frankrijk, Engeland, Spanje en Japan. De verdiende bitcoins werden bij een zogeheten bitcoin mixing service ‘gemengd’ met legale bitcoins. De hoofdverdachte zou in totaal 20 duizend bitcoins hebben gehad, toen 5 mln euro waard (nu bijna 115 mln maar dat terzijde – rené). Twee andere (vrouwelijke) verdachten in de zaak kregen elk drie maanden voorwaardelijk en 180 uur taakstraf, een vijfde verdachte kreeg een boete van 30 mille voor witwassen en wapenbezit, een zesde werd vrijgesproken.

Een ict-student is in hoger beroep door het Gerechtshof Amsterdam veroordeeld tot een gevangenisstraf van 30 maanden, waarvan 15 voorwaardelijk. De verdachte heeft zich ruim twee jaar lang schuldig gemaakt aan computercriminaliteit. Hij heeft zijn informaticakennis gebruikt om websites te hacken door gebruik te maken van daarvoor bestemde softwareprogramma’s. De verdachte maakte daarbij gebruik

van inloggegevens van zijn buurvrouw. Deze gegevens waren door haar aan hem gegeven, omdat de verdachte de buurvrouw had verteld dat zijn internet het niet goed deed en hij internet nodig had voor school. Door deze gegevens op deze wijze te misbruiken heeft de verdachte niet alleen misbruik gemaakt van het door de buurvrouw in hem gestelde vertrouwen, maar heeft hij haar ook betrokken in het strafrechtelijk onderzoek

Een rechtbank in Uppsala, Zweden heeft een man (41) veroordeeld tot tien jaar celstraf voor het online misbruiken van minderjarige meisjes. De verdachte is onder meer schuldig bevonden aan verkrachting en grooming. Volgens de Zweedse wet is verkrachting niet beperkt tot fysiek contact tussen dader en slachtoffer. De grooming gebeurde op een inmiddels klassieke manier: hij zocht online contact met meisjes in de VS, Canada en Schotland, dwong ze tot seksuele handelingen voor de webcam en gaf via Skype instructies wat ze moesten doen. Daarna dreigde hij de beelden online te zetten als ze niet nóg een filmpje wilden maken.

De politie wist 27 slachtoffers te identificeren, waarvan 18 jonger dan vijftien. De verdachte was in 2009 al eens veroordeeld voor soortgelijke feiten maar ‘ging in

deze zaak veel verder’, schrijft Aftenbladet.

Een man (34, uit Hengelo) is veroordeeld tot vijf jaar celstraf en tbs met dwangverpleging voor het plegen van ontucht met twee jonge meisjes en het produceren, bezitten en verspreiden van kinderporno. Verdachte Kris K. misbruikte een 4-jarig nichtje en het 5-jarig dochttertje van een goede vriend. Als ‘Naomi’ beheerde hij het chatkanaal Prinses Jade Chat op het dark web. Toen hij een foto van een naakt meisje op een klimrek in Hengelo stuurde naar een onderveragent in Nieuw-Zeeland, startte de politie een onderzoek. Bij huiszoeking vond de politie zeven geschakelde computers waarop 2,5 miljoen foto’s en 10 duizend video’s waren opgeslagen, maar ook luiers en kinderkleding. Allemaal versleuteld – de verdachte had een ict-bedrijfje. Rechercheurs wisten die bestanden alleen te openen met hulp van de verdachte die overigens al eerder behandeld was voor zijn pedofiele afwijking en die zelfs tijdens die behandeling nog meisjes misbruikte. De straf is conform de eis van het OM.

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 lid 1	350b lid 2
• 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 vervolghandelingen		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 af luisterapparatuur; 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 valselyk 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

(ga voor meer video naar de videowall op de website www.veiligdigitaal.com)

INDEX

Tek Tok Late Night:

1. [Privacy](#)
2. [Internetvrijheid](#)
3. [Digitale veiligheid](#)
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 telefoon](#)
- [Documentaire: Veiligheid en privacy](#)
- [Herken een nep-hotspot](#)
- [Gebruik wachtzinnen](#)
- [Drive-by-downloads voorkomen](#)
- [Hoe herken je een phishing mail](#)
- [Beveiligd internetbankieren](#)
- [Privacy—ik heb toch niets te verbergen](#)
- [Mousejack](#)

Help wanted:

- [Grooming](#)
- [Sexting](#)
- [Webcammisbruik](#)
- [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](#)