

Secure Computing Magazine

Website / Facebook

- Het magazine is opgefrist, zoals u ziet. Nieuwe layout, nieuw lettertype en meer.
- Enkele vaste onderdelen zijn verwijderd of ingepast in de standaard tekstdelen. De verwijderde onderdelen zijn ingebed in de Secure Computing website.
- Er is getracht de leesbaarheid te vergroten door de artikelen korter te maken. De uitgebreide achtergrondartikelen zult u voortaan aantreffen op de website.
- De hyperlinks zijn terug waardoor u weer door kunt klikken naar het internet voor nog meer info betreffende het onderwerp..
- Het magazine is uitgebreid met informatie uit het buitenland, relevant of leerzaam voor Nederland.
- Nieuwe rubriek: Rechtspraak

Rubrieken:

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

INDEX

[Cerber ransomware](#)

[CJIB waarschuwt voor nepmails met verkeersboetes](#)

[D66 wil dat Nederland encryptiesoftware gaat verdedigen](#)

[Gmail komt met twee nieuwe beveiligingswaarschuwingen](#)

[Android-malware geen probleem voor virus scanners](#)

[Onderzoekers ontwikkelen firewall voor usb-apparaten](#)

[Malware steelt data van offline computer via geluid harde schijf](#)

[Overstap naar digitale portemonnee niet zonder risico](#)

[Sleutelsysteem miljoenen auto's Volkswagen Group gekraakt](#)

[Ransomware-as-a-service in opkomst](#)

[Android-malware Spveng verspreidt zich via mobiele advertenties](#)

[Wikileaks lekt onbedoeld een hoop malware](#)

[Twitter is niet verantwoordelijk voor terrorisme](#)

[Draadloos toetsenbord biedt open deur voor hackers](#)

[Canadese politie wil wachtwoorden via nieuwe wet opeisen](#)

[WhatsApp verwijderd berichten stiekem niet volledig](#)

[Is het strafbaar om je Netflix-wachtwoord te delen?](#)

[Snowden vermoedt politiek motief achter lekken NSA-malware](#)

[Meeste besmette e-mails bevatten zip-bijlage](#)

[130 organisaties wereldwijd besmet via 7z-bestanden](#)

[OM wil toegang tot versleutelde informatie kunnen krijgen](#)

[AG: kentekenfoto's Belastingdienst schenden privacy](#)

[Wat verzamelt de AIVD eigenlijk](#)

[Mensen negeren beveiligingsmelding op ongeschikte momenten](#)

[Slim stopcontact kan e-mailwachtwoord gebruiker lekken](#)

[Wat is encryptie?](#)

[VN: terroristen steeds vaker onzichtbaar op internet](#)

[Ziekenhuizen doelwit van nieuwe ransomware-campagne](#)

[Securitas wil inbraakinformatie via WhatsApp-buurtgroepen](#)

[Op Facebook in plaats van in een bende?](#)

[VS: Vrijheid van meningsuiting, sociale media en politiemensen](#)

[Ransomware vermomt zich als Windows Update](#)

[Firefox krijgt bescherming tegen MIME-aanvallen](#)

AKTUEEL

Minister wil fundamenteel ander forensisch onderzoek toestaan

Minister Van der Steur van Veiligheid en Justitie wil de komende jaren fundamenteel andere manieren van forensisch onderzoek toestaan op het gebied van digitaal bewijs, omdat "we anders simpelweg niet bij kunnen blijven." Dat liet de minister tijdens een algemeen overleg in juni weten.

Het verslag van dit algemeen overleg, dat forensisch onderzoek als onderwerp had en met de vaste commissie voor Veiligheid en Justitie plaatsvond, is nu openbaar gemaakt. Van der Steur stelt tijdens het overleg dat de komende jaren er een verandering in de aard van het forensisch onderzoek zal plaatsvinden. Het zal "heel veel" gaan om digitaal onderzoek naar digitaal bewijs en digitale sporen. Het kan dan bijvoorbeeld gaan om het gebruik van big data voor opsporingsdoeleinden.

"Dat debat moeten we zeker nog met de Kamer voeren. Ik sla dit debat overigens met enige zorg gade. Ten aanzien van het wetsvoorstel computercriminaliteit III, dat beoogt om op dit terrein in de toekomst een beetje bij te blijven, hoor ik in de Kamer een aantal heel kritische geluiden", laat de minister weten. Hij stelt dat als het Nationaal Forensisch Instituut (NFI) op de digitale snelweg dezelfde kwaliteit onderzoeken wil kunnen afleveren als bij traditionele sporen het geval is, er naar nieuwe bevoegdheden moet worden gekeken.

"We zullen moeten kijken naar nieuwe manieren om informatie te verwerken. We zullen dat debat echt aan moeten gaan. We zullen bereid moeten zijn om in de komende jaren fundamenteel andere manieren van forensisch onderzoek toe te staan op het gebied van digitaal bewijs, omdat we anders simpelweg niet bij kunnen blijven", merkt Van der Steur op. Wanneer het wetsvoorstel computercriminaliteit III in de Kamer zal worden behandeld is nog altijd onbekend.

Ga naar [de website](#) voor meer actuele onderwerpen !

Alerts

Via een e-mail die afkomstig lijkt van een koerier van PostNL proberen criminelen kwaadaardige software op uw computer te installeren.

Zogenaamd is het niet gelukt een pakket bij u af te leveren. In gebrekkig Nederlands staat er in het bericht dat u een boete moet betalen als u niet binnen dertig dagen het pakket alsnog in ontvangst neemt. De bedoeling van de mail is om u onrustig te maken en u op de link te laten klikken. Op dat moment loopt u de kans dat kwaadaardige software (malware) wordt geïnstalleerd. Het gaat hier om een variant van ransomware, waarbij uw bestanden kunnen worden versleuteld. U kunt pas weer uw documenten openen als u losgeld betaalt.

Het onderwerp van de mail luidt 'je hebt niet geleverde pakket'.

Open niet de 'factuur' die ene Melinda Intrum u stuurt via e-mail. Het gaat om een valse mail en als u de bijlage opent riskeert u een besmetting met kwaadaardige software.

Naar de inbox van de Fraudehelpdesk voor valse e-mails (valse-email@fraudehelpdesk.nl) zijn vandaag al vele honderden van deze valse e-mail gestuurd. Het bericht zou verstuurd zijn door incassobureau Intrum Justitia.

Krijgt u een sms-je over uw Apple-ID? Meteen weggooien. Ook als u geen Apple-ID heeft. Internetschurken proberen uw bankgegevens te bemachtigen door u te laten klikken op een linkje, waarmee u de speciale Apple-code opnieuw kunt instellen. Wie toch erop klikt, komt op een pagina die van Apple lijkt te zijn, maar dat niet is. Invullen van uw persoonlijke gegevens is helemaal uit den boze. Apple stuurt trouwens geen sms-jes.

Duizend dollar overmaken naar een bitcoinadres, anders sturen wij jouw zwarte boekhouding naar de rechtbank. Dat is de boodschap in een belabberd vertaalde email van een zekere Barbara Dost, die beweert dat zij

het computernetwerk in uw bedrijf al heeft platgelegd. De afzender moet een slechte dag gehad hebben, want de mail is niet alleen beïnvloed geformuleerd, maar ontbeert ook een rekeningnummer waarop de \$ 1.000 gestort zou moeten worden. Suggesteren dat uw malafide boekhouding interessant is voor Justitie slaat ook al nergens op. Kortom, een loos dreigement van een amateur in de cybercrime-wereld.

De email begint als volgt: Uwnetwerk is geheel aangetast heb je een kritieke kwetsbaarheid die geven u de volledige controle over uw netwerk en routename verbindingen.

Criminelen hebben een valse e-mail namens de Belastingdienst verstuurd die gericht is op ondernemers. Hierin vragen ze om het e-mailadres van de boekhouding van het bedrijf. Het onderwerp van de korte e-mail bestaat slechts uit het woord 'Informatie'.

Met de naam van het Centraal Justitieel Incassobureau (CJIB) is een nieuwe valse e-mail verschenen. Hierin wordt gedreigd dat uw rijbewijs is ingenomen.

Door te dreigen met vervelende gevolgen hopen de criminele afzenders van de mail dat u overgaat tot het betalen van een bepaald bedrag. Volgens de valse mail kunt u inname van uw rijbewijs voorkomen als u snel € 100,- overmaakt. Dit zou moeten via een PaySafeCard. Vervolgens staat er:

'Het innemen van uw rijbewijs betekent dat u uw rijbewijs met ingang van 03-08-2016 moet inleveren voor een periode van vier weken. Vanaf deze datum mag u geen motorrijtuig besturen van alle categorieën waarvoor het rijbewijs is afgegeven. Doet u dit wel, dan bent u strafbaar. (...) Ik adviseer u het rijbewijs aangekend te versturen.'



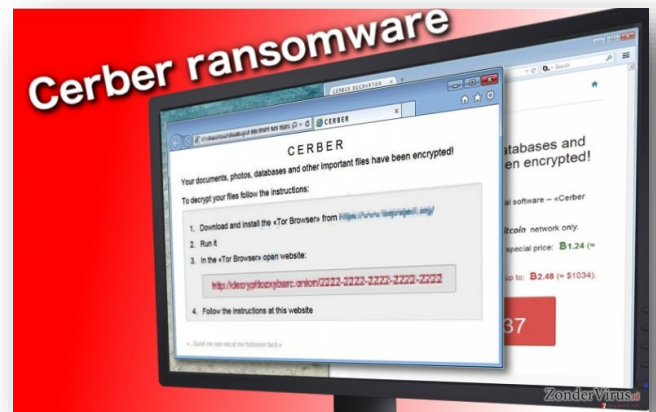
Cerber-ransomware niet meer te kraken via decryptietool

Slecht nieuws voor mensen en organisaties van wie de bestanden door de Cerber-ransomware zijn versleuteld, de versleutelde bestanden zijn namelijk niet meer kosteloos te ontsleutelen. Recentelijk kwam beveiligingsbedrijf Check Point met een gratis decryptietool om slachtoffers te helpen.

Het ging om een website waar slachtoffers een versleuteld bestand konden uploaden. Vervolgens gaf de website de decryptiesleutel terug om alle versleutelde bestanden op de computer te ontsleutelen. De ontwikkelaars van de Cerber-ransomware hebben als reactie de fout in het encryptieproces verholpen. Daardoor is het niet meer mogelijk om de bestanden via de website cerberdecrypt.com te ontsleutelen, aldus Check Point.

Het beveiligingsbedrijf stelt dat de afgelopen dagen toch nog honderden slachtoffers via de

website hun bestanden hebben teruggekregen. Bleeping Computer meldt dat de makers van de Cerber-ransomware op hun betaalpagina nu een [captcha-systeem](#) hebben toegevoegd. Mogelijk is dit gedaan om de geautomatiseerde dienst van Check Point tegen te gaan, maar zeker is dit niet.



CJIB waarschuwt voor nepmails met verkeersboetes

Het Centraal Justitieel Incassobureau ([CJIB](#)) waarschuwt internetgebruikers voor nepmails die op dit moment worden verstuurd en waarin wordt geëist dat de ontvanger 344 euro moet betalen voor het rijden door rood licht. In de e-mail wordt gesteld dat de ontvanger al meerdere keren per brief is verzocht om het openstaande bedrag te betalen, maar er nog niet is betaald.

Vervolgens wordt er gevraagd het openstaande bedrag binnen 3 dagen op een opgegeven rekeningnummer over te maken. Indien er niet wordt betaald dreigt de e-mail met het verhogen van het verschuldigde bedrag en verdere incassomaatregelen. "Het CJIB wil u waarschuwen voor vervalste verkeersboetes en nepmails. We blijven hier meldingen over ontvangen. Hebt u een mail ontvangen waarin staat dat u een boete moet betalen, dan is dit altijd een nepmail. Het CJIB mailt namelijk geen boetes of aanmaningen", aldus de overheidsinstantie.



D66 wil dat Nederland encryptiesoftware gaat verdedigen

Nederland moet in Europees verband encryptiesoftware verdedigen en erop aandringen dat bedrijven niet gedwongen worden om dergelijke software te verzwakken, zo vindt D66. De oproep is afkomstig van D66-Kamerlid Kees Verhoeven en gericht aan minister Van der Steur en minister Plasterk.

Verhoeven stelde Kamervragen naar aanleiding van het plan van de Franse overheid om met een wereldwijd initiatief versleutelde communicatie aan te pakken, aangezien terroristen hier gebruik van maken. Het D66-Kamerlid vraagt of de ministers zich in de analyse kunnen vinden dat terroristen niet afhankelijk zijn van berichtenapps als WhatsApp en Telegram en dat zij zeer gemakkelijk andere communicatiesoftware met sterke encryptie kunnen gebruiken.

Belang van encryptie

Ook wil het Kamerlid weten of de ministers nog steeds het belang van sterke encryptie onderschrijven voor de veiligheid op internet, ter ondersteuning van de bescherming van de persoonlijke levenssfeer van burgers, voor vertrouwelijke communicatie van overheid en bedrijven en voor de Nederlandse economie.

Plasterk en Van der Steur moeten verder duidelijk maken of ze het ermee eens zijn dat het afzwakken van encryptie geen duurzame oplossing biedt voor het opsporen van terroristen, maar dat het criminelen, buitenlandse inlichtingendiensten en staatshackers wel meer mogelijkheden biedt om persoonsgegevens en bedrijfsgeheimen te achterhalen en de vitale infrastructuur te hacken.

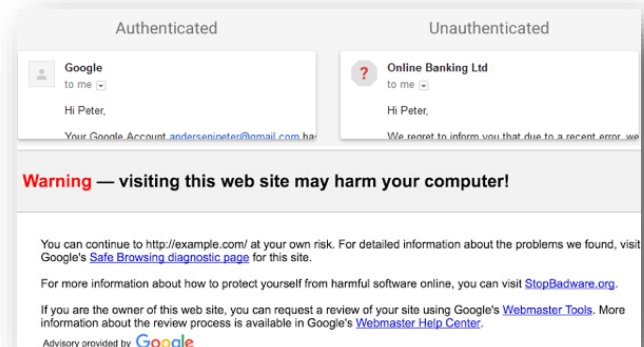
Aanvullend stelt Verhoeven dat het verzwakken van encryptie slecht is voor het vertrouwen in en gebruik van nieuwe technologische ontwikkelingen en hij wil weten wat de ministers hiervan vinden. Het Kamerlid wil verder weten of Plasterk en Van der Steur vinden dat er juist moet worden ingezet, ook in Europees verband, op het meer gebruiken van encryptie om de vrijheid en veiligheid van mensen en bedrijven te vergroten. Als laatste doet hij een oproep aan de ministers om zich voor encryptiesoftware in te zetten. "Bent u bereid in Europees verband erop aan te dringen dat bedrijven niet gedwon-



Gmail komt met twee nieuwe beveiligingswaarschuwingen

Gmail heeft twee nieuwe beveiligingswaarschuwingen laten zien die moeten voorkomen dat gebruikers het slachtoffer van phishing of andere vormen van fraude worden. In het geval de afzender van een bericht niet via het [Sender Policy Framework](#) (SPF) of [DKIM](#) (domain keys identified mail) kan worden bevestigd zal er een vraagteken in plaats van een profielfoto, logo of avatar van de afzender worden getoond.

Deze maatregel geldt voor de webversie en Gmail-app op Android. De tweede waarschuwing verschijnt alleen in de webversie en betreft e-mails die een gevaarlijke link bevatten. Het gaat dan om phishingsites of websites met malware of ongewenste software. Zodra een gebruiker op de link klikt verschijnt de waarschuwing. Hiervoor maakt Gmail gebruik van Google's eigen Safe Browsing-technologie die ook in browsers zoals Chrome, Safari en Firefox aanwezig is.



Android-malware geen probleem voor virus scanners

Malware op het Androidplatform is geen probleem voor virusscanners, zo blijkt uit een nieuwe test van het Duitse testlab AV-Test. Voor de test werden 26 mobiele security-apps vergeleken. Naast de detectie van kwaadaardige apps werden er ook naar systeembelasting en extra beveiligingsopties gekeken.

In totaal konden de apps een maximale score van 13 punten behalen. Met de detectie van malware waren maximaal 6 punten te verdienen. Voor dit onderdeel werden de 26 security-apps met bijna 3400 kwaadaardige apps getest die in de laatste vier weken zijn ontdekt. Daarnaast werden de oplossingen met bijna 3500 kwaadaardige apps in real-time getest. De apps scoren gemiddeld bij alle twee de tests boven de 99,5%. 19 apps halen de maximale 6 punten.

Hetzelfde aantal punten werd verdeeld voor de bruikbaarheid, zoals het batterijverbruik, systeembelasting, het genereren van veel dataverkeer en het onterecht alarm slaan bij schone applicaties van Google Play en andere officiële

marktplaatsen. Op dit onderdeel scoren 24 apps de maximale score van 6 punten. Alleen AVG en QuickHeal laten punten liggen.

Als laatste was er nog één punt te verdienen voor aanvullende beveiligingsmaatregelen, zoals anti-diefstal, encryptie en back-up. Een onderdeel waar alle 26 apps op scoren. Uiteindelijk komen 20 pakketten met een score van de maximale 13 punten als beste uit de bus. Van deze pakketten weten Antiy, Baidu, Bitdefender, Cheetah Mobile, PSafe, Qihoo 360, Sophos, Symantec, Tencent en Trend Micro 100% bij het vinden van malware te halen.



Onderzoekers ontwikkelen firewall voor usb-apparaten

Onderzoekers hebben een firewall voor usb-apparaten ontwikkeld om zo allerlei soorten usb-aanvallen te voorkomen. Door de complexe aard van usb is de echte functionaliteit voor gebruikers verborgen en besturingssystemen vertrouwen blindelings alle aangesloten usb-apparaten.

Dit heeft voor verschillende aanvallen gezorgd, bijvoorbeeld usb-sticks die de computer laten geloven dat ze een toetsenbord zijn en vervolgens allerlei commando's uitvoeren waardoor een aanvaller volledige controle krijgt. Als oplossing voor dit probleem bedachten onderzoekers van de Universiteit van Florida en Universiteit van Illinois "USBFILTER". Dit is een firewall die op pakket-niveau toegangscontrole over usb-apparaten geeft en kan voorkomen dat ongeautoriseerde apparaten verbinding met de computer maken.

Het filter is namelijk in staat om individuele usb-pakketten naar de verantwoordelijke processen te herleiden en ongeautoriseerde toegang te voorkomen. Niet alleen kan USBFILTER bepaalde usb-apparaten blokkeren, het kan ook de toegang tot een bepaalde applicatie beperken. Zo is het mogelijk om in te stellen dat alleen Skype de webcam mag benaderen. De impact van de firewall op de prestaties, bij bijvoorbeeld het kopiëren van bestanden, is volgens de onderzoekers verwaarloosbaar. De code van USBFILTER is via [GitHub](#) te downloaden.

Een firewall is een systeem dat de middelen van een netwerk of computer kan beschermen tegen misbruik van buitenaf. Het beschermde netwerk is vaak een intranet of intern netwerk en dit wordt beschermd tegen het internet. Het ongewenste verkeer bestaat bijvoorbeeld uit aanvallen van hackers en computerkrakers, inbraken en/of uitbraken van computervirussen en spyware.

Malware steelt data van offline computer via geluid harde schijf

Israëlische onderzoekers hebben malware ontwikkeld die het geluid van de harde schijf gebruikt om gegevens op computers die niet met internet verbonden zijn naar apparaten te versturen die wel internettoegang hebben. De onderzoekers noemen hun aanval "DiskFiltration".

Vanwege het risico op aanvallen is het een veel gegeven advies om computers met vertrouwelijke data niet op internet aan te sluiten. Een offline computer kan nog steeds worden geïnfecteerd, bijvoorbeeld via usb-sticks. Om vervolgens van een besmette offline computer data te stelen ontwikkelden onderzoekers verschillende methodes, zoals het gebruik van de speakers, zowel intern als extern, om via geluidssignalen de gegevens direct naar de aanvaller of een wel met internet verbonden besmette computer of smartphone terug te sturen.

Als oplossing kregen beheerders van offline computers het advies om de speakers van het systeem uit te schakelen of te verwijderen, om zo een 'audio-gap' te creëren. Onderzoekers van de Ben-Gurion Universiteit in Israël hebben echter verschillende manieren gevonden om zelfs van dit soort systemen gegevens te stelen. In juni kwamen ze met [Fansmitter](#), kwaadaardige code om via de ventilatoren van de computer gegevens door te sturen. Nu presenteren ze "DiskFiltration".

Deze malware gebruikt de leesarm van de harde schijf om lees- en schijfoperaties uit te voeren. Dit veroorzaakt een akoestisch signaal dat kan worden gebruikt om informatie naar een apparaat in de buurt te versturen. Het gaat

dan bijvoorbeeld om een besmette laptop, smartwatch of smartphone die over een microfoon beschikt en mogelijk met internet verbonden is. Op deze manier is het mogelijk om over een afstand van maximaal 2 meter 180 bits per minuut te versturen.

Volgens de onderzoekers is deze malware vooral interessant voor het aanvallen van systemen die niet met internet verbonden zijn of van computers die wel internettoegang hebben, maar waarvan de internetverbinding door ids- en ips-systemen wordt gemonitord. Om de aanvallen te voorkomen adviseren de onderzoekers om de harde schijven door stillere modellen of ssd's te vervangen, speciale kastjes te gebruiken of een zone in te stellen waarbij het bijvoorbeeld niet is toegestaan om in een ruimte met gevoelige systemen een smartphone mee te nemen.

Malware is elke software die gebruikt wordt om computersystemen te verstoren, gevoelige informatie te verzamelen of toegang te krijgen tot private computersystemen. Het woord is een samentrekking van het Engelse malicious software (kwaadaardige software, soms schadelijke software).



Overstap naar digitale portemonnee niet zonder risico

De overstap naar een digitale portemonnee, waarin zowel de identiteitsbewijzen, pasjes en zelfs het geld digitaal zijn, is niet zonder risico. Daarvoor waarschuwt Mark Rasch van zakelijke it-aanbieder Verizon Enterprise. Rasch vergelijkt de pasjes die veel mensen in hun portemonnee bewaren met een token.

Een rijbewijs is een door de overheid uitgegeven token dat aangeeft dat iemand in staat is een auto te besturen. Een pinpas is een token van een bank. Bonuskaarten zijn tokens die de relatie met een winkel of bedrijf weergeven. "Al deze tokens zijn binnenkort overbodig, als dat al niet het geval is", zegt Rasch. Toch verwacht hij niet dat fysieke pasjes zullen verdwijnen. Niet alleen is een fysiek pasje of een papieren notitie handiger te lezen dan een bestand op een smartphone, er zijn ook miljarden in de infrastructuur geïnvesteerd om met dergelijke fysieke tokens om te gaan.

De functionaliteit van deze tokens is echter al wel door bedrijven als Apple en Google in producten zoals Apple Pay en Android Pay gekopieerd. Foto's zijn tegenwoordig digitaal en ook bitcoin-betalingen worden op steeds meer plekken geaccepteerd. "Deze overstap van fysieke objecten naar een elektronische tegenhanger is niet zonder risico", gaat Rasch verder. Wie zijn fysieke portemonnee verliest heeft dit meestal snel door, maar de inhoud van een elektronische portemonnee kan worden gestolen zonder dat de eigenaar dit meteen doorheeft.

Volgens Rasch moet er bij de ontwikkeling van een tokensysteem, of het nu om een rijbewijs,

toegangskaat of financieel middel gaat, rekening worden gehouden hoe het kan worden gebruikt en misbruikt. "Ons vertrouwen in het token, in plaats van de persoon die het token aanbiedt, is misplaatst." Rasch stelt dat multifactorssystemen, al dan niet met een biometrisch onderdeel, hierbij kunnen helpen, maar hij waarschuwt ook dat er met de privacy- en anonimiteitsgevolgen van dergelijke systemen rekening moet worden gehouden.

"We moeten het recht en de mogelijkheid voor mensen behouden om dingen te doen zonder dat hun acties permanent worden vastgelegd", merkt hij op. Rasch besluit door te zeggen dat bij informatiebeveiliging niet alleen aan computers en netwerken moet worden gedacht, maar ook aan de manier hoe mensen met dergelijke systemen in zowel de fysieke als virtuele wereld omgaan.

Een token is over het algemeen een reeks cijfers of karakters die 'niet te verzinnen' is. Iemand die in het bezit is van het token kan het dus niet verzinnen hebben en bewijst daarmee het token te hebben.



Sleutelsysteem miljoenen auto's Volkswagen Group gekraakt

Onderzoekers zijn erin geslaagd om het sleutelsysteem van [de Volkswagen Group](#) te kraken waardoor het mogelijk is om op afstand miljoenen auto's te openen. Naast Volkswagens, Audi's en Skoda's zijn ook auto's van Alfa Romeo, Citroen, Fiat, Ford Mitsubishi, Nissan, Opel en Peugeot niet veilig.

Het gaat om twee verschillende aanvallen waarbij de onderzoekers met goedkope hardware het signaal van de sleutel opvangen en hiermee de sleutel klonen. De eerste aanval richt zich op auto's van de Volkswagen Group. In het netwerk van de auto wisten de onderzoekers een cryptografische sleutel te vinden die door miljoenen Volkswagens wordt gedeeld. Door vervolgens het signaal van de autosleutel op te vangen, dat voor elke autosleutel uniek is, is het samen met [cryptografische](#) sleutel mogelijk om de autosleutel te klonen. Hiermee kan vervolgens de auto worden opengemaakt.

Volkswagen gebruikt verschillende cryptografische sleutels voor verschillende jaren en modellen. De vier meestvoorkomende cryptografische sleutels worden echter door 100 miljoen Volkswagens gebruikt die in de afgelopen 20 jaar zijn verkocht, waaronder Audi en Skoda. Om de aanval uit te voeren moet een aanvaller wel binnen een straal van 90 meter van het voertuig zijn.

Tweede aanval

De tweede aanval richt zich op de HiTag2-encryptie die andere fabrikanten gebruiken en in miljoenen auto's aanwezig is. Ook bij deze aanval onderscheppen de onderzoekers de signalen van de sleutel. In totaal moet een aanvaller vier tot acht signalen van de sleutel

opvangen. Om dit te doen kan een aanvaller bijvoorbeeld het signaal van de autosleutel blokkeren, zodat de bestuurder een aantal keren op zijn sleutel drukt.

Met de onderschepte signalen kan de HiTag2-encryptie binnen een minuut worden gekraakt. Chipfabrikant NXP, dat de chips met de kwetsbare HiTag2-encryptie aan autofabrikanten verkoopt, zegt dat al jaren wordt aangeraden om een nieuwere encryptie te gebruiken. Volgens de onderzoekers heeft hun onderzoek op miljoenen auto's betrekking en kan het onopgeloste verzekeringsgevallen verklaren waarbij spullen uit vermeende gesloten auto's werden gestolen. Om autodieven niet te helpen zijn bepaalde onderzoeksgegevens, zoals encryptiesleutels, niet openbaar gemaakt. Daarnaast werd Volkswagen voor de publicatie van het onderzoek ingelicht.

[HiTag2 carjacking video](#)



Ransomware-as-a-service in opkomst

Door ransomware als dienst aan te bieden, kunnen ook minder technisch ingestelde criminelen veel slachtoffers maken. Om gebruik te mogen maken van software die door anderen is gemaakt, moeten ze wel een deel van de 'opbrengsten' afstaan.

Zo is de zogeheten 'ransomware-as-a-service' in opkomst. Eén van de ransomware-varianten die op een dergelijke manier te werk gaat, is het bekende Cerber. 'Gebruikers van Cerber krijgen een simpele gebruikersinterface voorgeschoteld, waar ze precies kunnen zien hoeveel infecties er dagelijks plaatsvinden en hoeveel losgeld er wordt betaald,' meldt de site.

Huren

Ransomware volgt daarmee onder meer in de voetsporen van DDoS-aanvallen, die via verborgen online marktplaatsen ook op bestelling leverbaar zijn. Net zoals hackers in te huren zijn, als je zelf niet over die know-how beschikt. Uiteraard in illegale circuits.

Infecties

Er zouden zodoende nu meer dan 150 verschillende Cerber-dreigingen in omloop zijn, die met name Windows-gebruikers op het oog hebben. In juli alleen al werden er 150.000 infecties opgemerkt. Opvallend genoeg blijven Oost-Europese landen buiten schot.



Ransomware is een chantagemethode op internet door middel van malware. Letterlijk vertaald betekent ransom: losgeld. Ransomware is een programma dat een computer (of gegevens die erop staan) blokkeert.

Android-malware Spveng verspreidt zich via

Antivirusfirma Kaspersky waarschuwt voor een nieuwe variant van de Android-malware Spveng, die zich dit keer in smartphones nestelt via Google's advertentienetwerk AdSense.

Android-toestellen kunnen simpelweg besmet worden zodra gebruikers een mobiele site laden die de advertenties van Google's netwerk draaien, en dat zijn er meer dan je wellicht denkt. Het virus komt automatisch binnen als .apk-bestand, installeert zichzelf en verdwijnt uit de lijst van geïnstalleerde apps, zodat 'ie onopgemerkt zijn gang kan gaan.

Doel van de trojan is uiteindelijk om gevoelige informatie te achterhalen, zoals creditcardgegevens. Android-gebruikers kunnen zich enerzijds beschermen met antivirus-app, want de Spveng-malware bestaat al een tijdje en zou dus opgepikt moeten worden door dergelijke beveiligingsapps.

Onbekende bronnen

Een andere manier om het virus te weren is door het 'installeren van apps uit onbekende bronnen' uit te zetten. Het is nu aan Google om de indringer uit het AdSense-netwerk te gooien. Websites kunnen er voor de zekerheid ook voor kiezen om in de tussentijd geen Google-advertenties meer aan te bieden.



Wikileaks lekt onbedoeld een hoop malware

In de haast om met nieuw gevoelig materiaal te komen, heeft [Wikileaks](#) meer dan 80 verschillend-varianten van malware gepubliceerd. Het gaat om gelekte e-mails die de klokkenluiderswebsite vrijgeeft van de AKP-partij van de Turkse president Erdogan. Veiligheidsexpert Vesselin Bontchev nam de berg gedumpte e-mails onder de loep, en stelde vast dat er heel wat geïnfecteerde berichten bij het lek zaten. Het overgrote deel van de malware was niet erg gevaarlijk: het bestond uit alledaagse spam en phishing e-mails. In het verleden heeft Wikileaks al eens bewust malware op de wereld losgelaten, maar dit lijkt niet nu het geval.

Volgens Wikileaks moeten de gelekte e-mails meer inzicht geven in de machtsstructuur binnen de AKP. Journalisten die de berichten hebben uitgepluisd, rapporteren echter dat het materiaal niet aan die verwachting voldoet. Het lek bestaat voornamelijk uit e-mails van mailinglijsten (denk bijvoorbeeld aan nieuwsbrieven) en inderdaad spam.

De klokkenluiderswebsite kan tegenwoordig op heel wat kritiek rekenen. Een maand geleden bleek bij een eerdere lek van Turkse informatie dat er een grote database was inbegrepen met uitgebreide informatie over bijna elke vrouw met stemrecht in Turkije, iets dat door verschillende experts als gevaarlijk en een grote inbreuk op de privacy werd bestempeld.



Twitter is niet verantwoordelijk voor terrorisme

IS gebruikt Twitter als een belangrijk medium voor propaganda en rekrutering. Naast andere sociale media als Telegram worden de berichten van 140 tekens ook vaak gebruikt om informatie over troepenbewegingen en andere westerse bezoekers door te sluisen. Als gevolg van dat netwerk werden vorig jaar nog twee Amerikaanse aannemers op gruwelijke wijze vermoord in Jordanië.

De weduwen van Lloyd Fields Jr. en James Damon Creach achtten Twitter verantwoordelijk voor de dood van de mannen en begonnen een rechtszaak tegen het medium. Ze gingen zelfs zo ver dat ze stelden dat Twitter de terroristische organisatie voorzag van materiële steun en middelen.

Zuiver geweten

Ze konden de rechter niet overtuigen, en die pleitte Twitter dan ook helemaal vrij. “Hoe gruwelijk de moorden ook zijn, Twitter kan niet worden beschouwd als uitgever of woordvoerder van de haatdragende boodschappen,” sprak de rechter. Het voorval valt volgens hem onder de zogenaamde ‘Communications Decency Act’, waarbij een online content provider niet verantwoordelijk is voor wat een derde partij online ziert.

Daarmee lijkt Twitter gezuiverd van elke betrokkenheid van terroristen op zijn platform. In theorie zou het zich dan ook afzijdig kunnen houden van de IS-boodschappen, al houdt het medium zich in realiteit actief bezig met het verwijderen van de berichten en hun afzenders. Cijfers van het Witte huis zouden bevestigen dat Twitter de IS-activiteit op zijn platform de voorbije twee jaar zo al met de helft kon doen dalen. Ze rusten dus zeker niet op hun lauweren.

Sinds Twitter besloot meer werk te maken van het verwijderen van tweets en twitteraars die extremisme en terrorisme propageren, zijn al 360 duizend accounts verwijderd. Het afgelopen halfjaar werden 235 duizend accounts opgeheven, gemiddeld 1300 per dag. Twitter heeft jarenlang volgehouden dat iedereen alles mocht twitteren maar onder druk van regeringen, opsporings- en inlichtingendiensten werd een koerswijziging ingezet.

Draadloos toetsenbord biedt open deur voor hackers

Onderzoekers van het beveiligingsbedrijf Bastille hebben verschillende kwetsbaarheden ontdekt bij veelgebruikte draadloze toetsenborden. Goedkopere toetsenborden van onder andere HP en Toshiba maken gebruik van hun eigen protocol om met de computer te verbinden. In tegenstelling tot bluetooth worden deze signalen veelal niet geëncrypteerd. Dit zorgt ervoor dat alles wat je typt, kan worden onderschept door hackers.

Volgens Bastille is het nog niet eens zo moeilijk om misbruik te maken van het lek. Al wat je nodig hebt, is een wifi-adaptor en –antenne van slechts enkele tientallen euro's. Met behulp van enkele regels Python-code kan een hacker hierna passief alles vastleggen wat je typt, zoals gebruikersnamen, wachtwoorden en kredietkaartinformatie.

De onderzoekers die aan de alarmbel trekken, staan versteld van het gemak waarmee hackers op deze manier gegevens kunnen verzamelen. "Ik denk dat veel consumenten verwachten dat een draadloos toetsenbord gebruiken veilig is. Ze zijn zich hoogstwaarschijnlijk niet bewust van het risico," vertelt Marc Newlin, één van de onderzoekers van Bastille.

Gelukkig zijn niet alle toetsenborden kwetsbaar voor het lek. Er is echter maar één ding dat je kan doen om zeker te zijn dat je geen slachtoffer wordt van de hack: gebruik een bedraad toetsenbord.



Canadese politie wil wachtwoorden via nieuwe wet opeisen

De Canadese politie wil dat er een nieuwe wet komt die mensen via een gerechtelijk bevel dwingt hun wachtwoorden of encryptiesleutels af te staan. Volgens de Canadian Association of Chiefs of Police maken criminelen steeds vaker gebruik van encryptie om hun activiteiten te verbergen.

Een nieuwe wet moet daarom de impact van versleutelde en met wachtwoorden beveiligde apparatuur aanpakken. Volgens vice-commissaris van de Canadese politie Joe Oliver is erop dit moment nog geen wetgeving die mensen dwingt om hun wachtwoord tijdens een politie-onderzoek af te staan, zo laat CTV News weten. "De slachtoffers in de digitale ruimte zijn echt. De mogelijkheden van de Canadese wetgeving en politie moeten de technologische ontwikkelingen kunnen bijbenen", vertelde Oliver tijdens een persconferentie. [OpenMedia](#), een organisatie die zich voor een open internet inzet, stelt dat het voorgestelde plan disproportioneel en ongrondwettig is.

WhatsApp verwijderd berichten stiekem niet volledig

Volgens iOS-onderzoeker Jonathan Zdziarski worden WhatsApp-berichten niet helemaal van je smartphone verwijderd, zelfs al heb je die opdracht gegeven aan de app. Zdziarski kwam daarachter toen hij verwijderde bestanden wilde herstellen. Het blijkt dat WhatsApp-conversaties vlot kunnen worden hersteld, iets wat niet zou mogen.

In de meeste gevallen werd de data door de app gemarkeerd als 'verwijderd', maar het werd niet door iets anders overschreven op de interne opslag. Dat maakt de baan vrij om relatief eenvoudig al die gegevens te herstellen in originele staat. Zdziarski wijt de fout aan een probleem in de SQLite-bibliotheek die de app codeert.

WhatsApp kreeg recent nog een pluim van verschillende privacy-advocaten door eerder dit jaar end-to-end encryptie te implementeren. Dit beschermt de data wanneer het in transit is, maar blijkbaar is er nog wel een probleem met alle berichten die lokaal op je smartphone staan.

Daarnaast mag je ook niet vergeten dat je de opdracht kan geven aan WhatsApp om berichten en foto's te back-uppen in iCloud of Google Drive. Indien je dat doet, heb je sowieso geen verhaal wanneer de politie beroep doet op je

online bestanden tijdens een onderzoek.

WhatsApp is daarin niet de enige, een heleboel andere messaging apps doen gelijkaardige cloud back-ups. Dat maakt hen allemaal niet 100% waterdicht op privacyvlak.

The Verge meldt dat deze ontdekking bijzonder relevant is voor de huidige gerechtelijke processen die WhatsApp heeft lopen op vlak van privacy. In Brazilië hebben lokale rechtbanken al met een black-out gedreigd van de berichtendienst indien het niet wil meewerken aan bepaalde dossiers. Voorlopig is het nog niet zover gekomen, maar met deze nieuwe ontdekking hebben onderzoekers alweer een extra middel om berichtgegevens te analyseren.



Is het strafbaar om je Netflix-wachtwoord te delen?

In de VS is het strafbaar je Netflix-wachtwoord te delen. Geldt dat ook bij ons?

Computervredebreuk is kort gezegd een computer binnendringen. In de Amerikaanse wet spreken ze ook van "exceeding authorization", om ook strafbaar te stellen dat je verder gaat dan je mocht in een computer waar je op zich mocht zijn. Wie als gewone gebruiker ergens mag inloggen en aan het beheerswachtwoord raadt, gaat zijn autorisatie te buiten en pleegt dan computervredebreuk.

In de die Amerikaanse zaak waren twee werknemers bij een concurrent gaan werken, en een derde werknemer had zijn wachtwoord uitgeleend zodat zij bij de klantendatabase konden. Dat wachtwoordgebruik werd gezien als een vorm van computervredebreuk. Die concurrent mocht niet in die computer zijn, ook niet met een login die technisch gewoon werkt.

Ik denk dat we in Nederland op dezelfde conclusie uit zouden komen. Als je ergens niet mag zijn in een computer, dan mag je dat ook niet met een geleend wachtwoord. (Dat noemen we een valse sleutel onder art. 138ab Strafrecht.)

Wel maakt het zoals altijd uit hoe je aan het wachtwoord kwam en wat je ermee doet. En dat maakt het gelijk zo lastig bij dingen als Netflix: dat zijn geen bedrijfsdatabanken waar ongeautoriseerde toegang eenvoudig aan af te meten is.

Met een Netflix-wachtwoord neem je gewoon de dienst af zoals die bedoeld is. Netflix controleert op het aantal gelijktijdige logins. Kennelijk dus geen probleem wie er het wachtwoord gebruikt, zolang het maar binnen het maximum blijft. Het lijkt me dan ook sterk dat dát een vorm van binnendringen is wanneer je anderen wachtwoord gebruikt.

Wel is het zo dat in de voorwaarden staat "de Account-eigenaar [mag] het wachtwoord of de gegevens van de Betalingsmethode die gekoppeld zijn aan het account (...) aan niemand bekendmaken." Maar de opstelling in de praktijk is belangrijker dan de exacte tekst van de voorwaarden. Zeker als ze dingen zeggen als "As long as they aren't selling them, members can use their passwords however they please."

Je loopt in Nederland misschien eerder tegen art. 326c Strafrecht aan: het afnemen van een betaaldienst zonder daarvoor te betalen. Maar ook dan: is het wel wettelijk gezien de aard van de dienst? De dienst wordt niet twee keer afgenomen waar één keer normaal is. Netflix regelt dat zelf. Dus wat is het probleem dat het strafrecht moet oplossen?



Snowden vermoedt politiek motief achter lekken NSA-malware

De groep die achter het lekken van vermeende NSA-malware zit heeft waarschijnlijk politieke motieven, zo stelt klokkenluider Edward Snowden op Twitter. Onlangs publiceerde een groep genaamd Shadow Brokers allerlei bestanden en informatie van de Equation Group.

Een groep cyberspionnen die banden met de NSA zou hebben. Experts vermoeden dat de bestanden en malware bij een hack van een server die NSA gebruikte zijn gestolen. Volgens Snowden is het niet ongekend dat dergelijke servers van de NSA worden gehackt. De klokkenluider stelt dat de NSA gebruikmaakt van de command & control-servers waar ook cybercriminelen gebruik van maken. Iets wat ook de rivalen van de Amerikaanse inlichtingendienst doen.

"De NSA kijkt vaak jaren ongezien mee op de command & control-servers en ORBs (proxy-hops) van staatshackers. Zo kunnen we hun operaties volgen", schrijft Snowden. De NSA zou op deze manier de hackingtools van andere partijen weten te stelen. Soms wordt de NSA echter zelf het doelwit van dergelijke aanvallen. De hackers van de NSA zouden dan ook instructies krijgen om hun hacktools na een

operatie niet op een server achter te laten, maar volgens Snowden zijn mensen soms lui. Het nieuws is dan ook niet dat een NSA-server door een rivaal is gehackt, maar dat een rivaal dit openbaar maakt, stelt Snowden.

"Waarom ze het hebben gedaan? Niemand weet het, maar ik vermoed een diplomatiek motief in plaats van inlichtingen." De klokkenluider wijst naar de escalatie rondom de hack van de Amerikaanse Democratische Partij. Hij ziet het lek dan ook als een waarschuwing dat iemand Amerikaanse verantwoordelijkheid voor elke aanval afkomstig van de gehackte malware-server kan aantonen. Iets wat weer gevolgen voor de relaties tussen de Verenigde Staten en diens bondgenoten kan hebben. Verder blijkt uit de nu gelekte data dat de aanvaller in juni 2013 zijn toegang tot de NSA-server verloor. De maand dat de onthullingen van Snowden openbaar werden.



Edward Snowden ✓
@Snowden



13) TL;DR: This leak looks like a somebody sending a message that an escalation in the attribution game could get messy fast.

4:49 AM - 16 Aug 2016

Meeste besmette e-mails bevatten zip-bijlage

De meeste kwaadaardige e-mails die in het tweede kwartaal van dit jaar internetgebruikers met malware probeerden te infecteren maakten hiervoor gebruik van [zip-bestanden](#). Dat blijkt uit kwartaalcijfers van het Russische anti-virusbedrijf Kaspersky Lab.

Van april tot en met juni ging het om miljoenen zip-bijlagen waarin malware zat verstopt, voornamelijk downloaders die ransomware op computers installeren. In de eerste weken van juni was er echter een daling van het aantal e-mails met besmette zip-bestanden. De oorzaak bleek te liggen in de inactiviteit van een botnet dat veel voor dergelijke spam wordt gebruikt. Eind juni werd het botnet weer operationeel wat te zien is in een stijging van het aantal besmette e-mailbijlagen. Naast de tijdelijke inactiviteit noemt Kaspersky het opvallend dat kwaadaardige zip-bijlagen niet in het weekend worden verstuurd.



130 organisaties wereldwijd besmet via 7z-bestanden

Een groep internetcriminelen heeft het afgelopen jaar via kwaadaardige e-mails 130 organisaties in meer dan 30 landen met malware weten te infecteren, om zo toegang tot intellectueel eigendom en zakelijke bankrekeningen te krijgen. Dat meldt het Russische anti-virusbedrijf Kaspersky Lab.

De groep verstuurde gerichte e-mails naar directeuren, managers en andere hooggeplaatste personen binnen industriële organisaties, ingenieursbureaus en productiebedrijven. De berichten leken van een bank in de Verenigde Arabische Emiraten afkomstig en hadden een 7z-bestand als bijlage. Dit 7z-bestand bevatte weer een exe-bestand. Als

gebruikers het bestand openden kon de malware toetsaanslagen, inloggegevens en accountgegevens stelen.

Op deze manier probeerden de aanvallers toegang tot zakelijke bankrekeningen en intellectueel eigendom te krijgen. Het intellectueel eigendom zou vervolgens aan geïnteresseerde partijen worden verkocht. Uit onderzoek blijkt dat de aanvallen al sinds maart 2015 plaatsvinden, waarbij er in juni van dit jaar een nieuwe aanvalsgolf werd waargenomen. De meeste getroffen organisaties bevinden zich in Spanje, gevolgd door Pakistan en de Verenigde Arabische Emiraten.

Een zipbestand of zipfile is een verliesvrij gecomprimeerd bestand waarin een of meer computerbestanden zijn ondergebracht.

OM wil toegang tot versleutelde informatie kunnen krijgen

Het Openbaar Ministerie wil de mogelijkheid hebben om versleutelde informatie na een bevel van de rechter toch te kunnen inzien. Dat zegt officier van justitie Martijn Egberts tegen de NOS. Volgens Egberts komt justitie bij het "overgrote deel" van de onderzoeken naar georganiseerde misdaad encryptie tegen. "Dan moet je denken aan liquidaties, afpersingen, drugszaken en kinderporno."

Encryptie maakt het volgens de officier moeilijker om op te sporen. "Wat wij het liefste zouden willen is dat er, na een rechtelijke toetsing, toch een mogelijkheid is om aan een

bedrijf te vragen om die informatie beschikbaar te stellen", zegt Egberts verder. De officier maakt de vergelijking met de mogelijkheid om telefoonverkeer af te tappen. Die is er niet met versleutelde communicatie. "Het is toch wel opmerkelijk dat er nu zo veel manieren zijn om te communiceren zonder dat de overheid toegang kan krijgen." Onlangs liet de Franse overheid weten dat het een wereldwijd initiatief tegen versleutelde communicatie wil.



AG: kentekenfoto's Belastingdienst schenden privacy

De kentekenfoto's die de Belastingdienst met behulp van [ANPR-technologie](#) op de Nederlandse snelwegen maakt zijn in strijd met het recht op bescherming van het privéleven zoals dat in het Europees verdrag voor de rechten van de mens (EVRM) is opgenomen, aldus de Advocaat-Generaal.

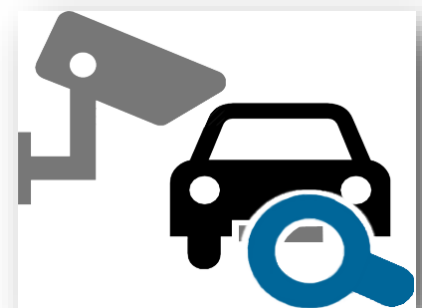
De Belastingdienst en politie maken elk jaar 3 miljard foto's van kentekens. De foto's worden gemaakt door kentekencamera's. De camera's maken [gebruik van automatische nummerplaattherkenning \(ANPR\)](#) en kunnen nummerplaten in seconden met een lijst van gestolen voertuigen en auto's van verdachte personen vergelijken. Ook de Belastingdienst maakt gebruik van de camera's, bijvoorbeeld om te controleren of leaserijders niet meer privékilometers rijden dan ze opgeven of om belastingontduikers op te pakken.

De betreffende camerabeelden geven echter een zeer gedetailleerd inzicht in het verplaatsingsgedrag van automobilisten. Advocaat Guido de Bont spande namens een client een procedure aan. Daarin stond de vraag centraal of deze wijze van gegevensverwerking wel voldoet aan de eisen die daaraan op grond van de Europese jurisprudentie worden

gesteld. Volgens De Bont is nergens in de wet opgenomen dat de Belastingdienst een dergelijke vergaande bevoegdheid heeft.

Hij krijgt bijval van in een advies van de Advocaat-Generaal: "Het komt mij derhalve voor dat de Belastingdienst te dezen handelt zonder dat daartoe in de Awb of de AWR een bevoegdheid is geregeld (i.e. niet op een wettelijke grondslag berust). Nu de inbreuk niet bij wet is voorzien, moet worden geconcludeerd dat het vastleggen van de ANPR-gegevens door de Belastingdienst op de openbare weg in strijd is met het door artikel 8 EVRM gewaarborgde recht op bescherming van het privéleven."

De Advocaat-Generaal heeft het cassatieberoep van De Bont dan ook gegrond verklaard. "Het gevolg is volgens de Advocaat-Generaal dat de met de ANPR-camera's verkregen gegevens niet mogen worden gebruikt bij het opleggen van de naheffingsaanslagen aan belanghebbende. Ook overweegt de Advocaat-Generaal dat de Hoge Raad de zaak zelf kan afdoen, hetgeen zal moeten resulteren in het vernietigen van de naheffingsaanslagen". Het gaat hier echter om een advies aan de Hoge Raad, die zich hier vervolgens over zal buigen.



Wat verzamelt de AIVD eigenlijk?

Gebrek aan mankracht is het probleem, niet een gebrek aan data

[De AIVD](#) beschikt op dit moment al over een breed assortiment van bevoegdheden waarmee ze onder andere je telefoongesprekken en e-mails kunnen onderscheppen, je gebruikersgegevens kunnen opvragen bij providers of je computer kunnen hacken. Niet voor niets zei hoogleraar en terrorisme-expert [Beatrice de Graaf](#), onlangs bij Nieuwsuur (dat de Nederlandse geheime diensten al over voldoende bevoegdheden ('maatregelen') beschikken om dreigingen in kaart te brengen).

Waar het vaak misgaat, is het gebrek aan interventievermogen. Oftewel een gebrek aan mankracht in de vorm van analisten, wijkagenten, maar ook leraren en jongerenwerkers. Zonder voldoende en kundige mensen heb je immers vrij weinig aan de verzamelde data. Het kabinet kan dus beter investeren in meer en betere mankracht, dan in een sleepnet om heel veel data van onschuldige burgers te verzamelen.

Inzageverzoek

Als je benieuwd bent wat de AIVD mogelijk nu al over je weet dan kan je een inzageverzoek indienen. Je hebt namelijk het recht op kennisneming van de persoonsgegevens die de AIVD over je heeft verzameld. Wat moet je hiervoor doen?

Vermeld in je verzoek duidelijk om welke informatie en over welke periode het gaat. Bijvoorbeeld dat het om alle gegevens gaat over jezelf en gegevens die herleidbaar zijn tot jezelf. Houd er wel rekening mee dat het moet gaan om onderwerpen die al langer dan 5 jaar gesloten zijn.

Vraag om een kopie van alle stukken waarin de verzochte gegevens staan.

Vermeld waar mogelijk de context waaronder

je bekend bent geworden bij en onder de AIVD. Bijvoorbeeld dat je hebt deelgenomen aan een bepaalde demonstratie of een periode lid was van een bepaalde organisatie.

Verwijs naar alle relevante wetten waarop je een beroep doet (dat is in ieder geval [de Wet op de inlichtingen- en veiligheidsdiensten 2002](#) maar kan onder omstandigheden ook nog andere wetgeving zijn).

Voeg een kopie van je legitimatiebewijs bij je verzoek. Wij raden aan om je BSN-nummer weg te strepen en de kopie van je legitimatiebewijs te markeren met dwars door de foto de volgende tekst: "inzageverzoek persoonsgegevens AIVD datum".



Stuur je verzoek per post naar het adres dat staat vermeld op de website van de AIVD.

De AIVD moet binnen drie maanden op een dergelijk verzoek reageren.

Houd er wel rekening mee dat de AIVD je verzoek op een groot aantal gronden kan afwijzen. Verzoeken die betrekking hebben op persoonsgegevens die van belang zijn voor lopend onderzoek, die zicht geven op geheime bronnen of betrekking hebben op andere personen, zullen bijvoorbeeld worden afgewezen. Toch is het de moeite waard om een verzoek in te dienen. Zo werden in 2014 toch

Mensen negeren beveiligingsmelding op ongeschikte momenten

Bijna 90% van de mensen negeert belangrijke beveiligingsmeldingen als ze op een ongeschikt moment verschijnen, zo blijkt uit onderzoek van onderzoekers van de Brigham Young University en ontwikkelaars van Google Chrome. Het gaat dan bijvoorbeeld om meldingen die verschijnen als mensen bezig zijn met het bekijken van video's, uploaden van bestanden of typen van een tekst.

"We ontdekten dat het brein niet goed met multitasking kan omgaan", zegt hoogleraar Anthony Vance die aan het onderzoek meewerkte. Hij stelt dat softwareontwikkelaars categorisch dit soort meldingen tonen zonder rekening ermee te houden wat de gebruiker op dat moment aan het doen is. "Ze storen ons continu en ons onderzoek laat zien dat er een hoge straf op staat om deze berichten op willekeurige momenten te tonen."

Zo negeerde 74% van de onderzoeksgroep beveiligingsmeldingen als ze bezig waren met het sluiten van een webpagina. 97% negeerde de meldingen als ze een video aan het kijken waren en 87% liet de waarschuwing aan zich voorbij gaan als ze bezig waren met het over-

brengen van informatie zoals een bevestigingscode. "Maar je kunt dit probleem eenvoudig verhelpen door het moment van de waarschuwingen beter te timen", aldus Jeff Jenkins die het onderzoek leidde.

Beveiligingsmeldingen krijgen de meeste aandacht als ze op moment verschijnen dat de gebruiker minder aan het doen is, bijvoorbeeld na het kijken van een video, het wachten op een website die aan het laden is of na het gebruik van een website. De onderzoekers erkennen dat dit vrij voor de hand liggend is, toch houden softwareontwikkelaars op dit moment zich helemaal niet bezig met het afstemmen van de beveiligingsmeldingen. Naar aanleiding van het onderzoek hebben de ontwikkelaars van [de Chrome Cleanup Tool](#), een programma om problemen in Google Chrome te verhelpen, besloten om in de toekomst de timing van de meldingen aan te passen.



De Chrome Cleanup Tool werkt voor alle browsers.

Computers kunnen worden geïnfecteerd met malware. Deze heeft vaak ook effect op browsers die u gebruikt. De Chrome Cleanup Tool verwijdert programma's die invloed kunnen hebben op Firefox, Edge, Internet Explorer en andere browsers.

De programma's die worden verwijderd door de Chrome Cleanup Tool, worden verwijderd omdat we weten dat deze programma's uw instellingen wijzigen zonder uw toestemming.

Slim stopcontact kan e-mailwachtwoord gebruiker lekken

Een slim stopcontact dat via een smartphone-app is te bedienen blijkt allerlei kwetsbaarheden te bevatten waardoor het op afstand kan worden aangevallen. Een aanvaller zou zo inloggegevens van het e-mailadres van de gebruiker kunnen achterhalen of het stopcontact kunnen bedienen.

In het ergste geval kan er zelfs kwaadaardige firmware worden geïnstalleerd. Het Roemeense anti-virusbedrijf Bitdefender ontdekte de problemen, maar wil de naam van fabrikant niet bekendmaken aangezien de kwetsbaarheden nog niet zijn opgelost. Het slimme stopcontact beschikt over een eigen wifi-netwerk dat via de smartphone-app is te bedienen. Zodra de app verbinding heeft met het stopcontact moet de gebruiker de inloggegevens van zijn eigen wifi-netwerk invoeren, zodat het stopcontact hierop wordt aangesloten.

Het eerste probleem waar de onderzoekers tegenaan liepen is dat het wifi-netwerk van het slimme stopcontact standaard een zwakke gebruikersnaam en wachtwoord gebruikt. Ook wordt gebruikers niet aangeraden het standaardwachtwoord van het stopcontact te veranderen. Verder blijkt dat de mobiele app om het stopcontact te bedienen gegevens zoals wifi-gebruikersnaam en -wachtwoord niet versleutelt. De gegevens die via de server van de fabrikant met de app en het apparaat worden uitgewisseld blijken ook niet te zijn versleuteld, maar alleen gecodeerd. Deze codering is weer te kraken.

Verder beschikt het slimme stopcontact over de mogelijkheid om gebruikers een e-mail te sturen als het een apparaat aan- of uitzet. Hiervoor moet de gebruiker wel de inloggegevens van zijn e-mailaccount invoeren.

Aanvallen

Door de slechte beveiliging kan een aanvaller die het [mac-adres](#) en het standaardwachtwoord weet op afstand toegang tot het stopcontact krijgen om vervolgens instellingen aan te passen of de inloggegevens van het ingestelde e-mailaccount te achterhalen. Verder blijkt dat via het instellen van een nieuw wachtwoord er command-injectie mogelijk is.

Op deze manier kan een aanvaller in het nieuwe wachtwoord allerlei opdrachten meegeven die het stopcontact vervolgens uitvoert. Zodoende is het mogelijk om het rootwachtwoord te overschrijven en de Telnet-dienst van het stopcontact te starten. Via Telnet kan de aanvaller ongeacht zijn locatie allerlei opdrachten uitvoeren en zelfs kwaadaardige firmware installeren. Hiermee kan bijvoorbeeld weer worden geprobeerd om andere apparaten in het netwerk aan te vallen.

"Tot nu toe waren de meeste Internet of Things-kwetsbaarheden alleen in de buurt van het huis aan te vallen waar ze werden gebruikt. Deze kwetsbaarheid geeft hackers de mogelijkheid om via het internet apparaten te besturen en de beperkingen van network address translation (NAT) te omzeilen. Dit is een ernstige kwetsbaarheid. We zouden een botnet van deze stopcontacten kunnen tegenkomen", zegt onderzoeker Alexandru Balan.

De fabrikant van het stopcontact heeft aangegeven in het derde kwartaal van dit jaar met een oplossing te komen.



Een MAC-adres is een vrijwel uniek identificatienummer dat aan een apparaat in een ethernetnetwerk is toegekend. In het OSI-model valt een MAC-adres in de datalinklaag (meer specifiek: de Media Access Control-sublaag). MAC staat voor "Media Access Control" en wordt ook wel hardware-adres of fysiek adres genoemd.

Wat is encryptie?

De procedure van het coderen en decoderen van gegevens wordt "encryptie" genoemd. Wanneer encryptie van gegevens heeft plaatsgevonden, is er [een algoritme](#) toegepast om de gegevens te coderen, zodat deze niet meer hun oorspronkelijk vorm hebben en niet kunnen worden gelezen. De gegevens kunnen alleen naar hun oorspronkelijke vorm worden gedecodeerd door een specifieke decryptie-sleutel toe te passen. Coderingstechnieken zijn een belangrijk onderdeel van gegevensbeveiliging. Hiermee wordt vertrouwelijke informatie beveiligd tegen bedreigingen zoals misbruik via malware en ongeoorloofde toegang door derden. Gegevensencryptie is een veelzijdige beveiligingsoplossing. Deze kan worden toegepast op informatie zoals een wachtwoord, of op grotere schaal op alle gegevens in een bestand of zelfs op alle gegevens in opslagmedia.

Bescherming van computergebruikers via encryptie

Je krijgt meestal te maken met gegevens-encryptie wanneer je persoonlijke gegevens moet invoeren in een webformulier. Sites van financiële instellingen, overheden, scholen en

winkels maken meestal gebruik van gegevens-encryptie om je tegen diefstal en fraude te beschermen. Controleer altijd of webformulieren veilig zijn en of je gegevens worden gecodeerd. Controleer het volgende:

De URL van de webpagina begint met "https": dit betekent dat je gegevens worden gecodeerd en worden overgedragen via een beveiligd protocol.

Een slotpictogram, meestal links- of rechtsonder in het browservenster. Wanneer je op het slotpictogram klikt, zie je de beveiligingsdetails voor de site.

Je verwacht dat vertrouwelijke gegevens die je invoert op de website van een externe partij worden gecodeerd en beveiligd. Zo ook moeten de gegevens op je thuiscomputer worden beschermd. Bestanden, wachtwoorden, e-mailberichten en back-ups van gegevens moeten worden gecodeerd, zodat deze zijn beveiligd tegen hackers en dieven. Er zijn veelzijdige beveiligingsoplossingen beschikbaar om vertrouwelijke gegevens te coderen en op te slaan.



VN: terroristen steeds vaker onzichtbaar op internet

Teruggekeerde strijders van IS en al-Qaida zijn steeds moeilijker te volgen voor inlichtingendiensten, omdat ze op internet met versleutelde berichten communiceren. Daarvoor waarschuwden deskundigen van de Verenigde Naties in een rapport.

Versleutelde berichten zijn teksten die door een computer zijn vervormd, waardoor ze voor buitenstaanders onleesbaar zijn. Alleen ontvangers met de juiste sleutel op hun computer kunnen de originele tekst lezen.

In het rapport schrijven de VN-experts dat de teruggekeerde strijders ook steeds meer gebruikmaken van het zogeheten [dark web](#). Dat is een verborgen deel van het internet dat niet rechtstreeks vindbaar is voor zoekmachines. Zelfs de meest hoogwaardige inlichtingendiensten lukt het hierdoor niet om grote hoeveelheden berichten te lezen, zeggen de experts.

De VN is bang dat de terroristen, nadat ze bijvoorbeeld in Syrië zijn geweest, in hun thuisland aanslagen beramen en dat de geheime diensten hier niets van afweten.

Het dark web is een onderdeel van het wereldwijde web dat niet rechtstreeks vindbaar is voor de zoekmachines. Het deel van het web dat gevonden kan worden door zoekrobots is maar een fractie van alle websites die zich op dat web bevinden. Naast die geïndexeerde websites zijn er ook websites die dit niet zijn, maar wel rechtstreeks toegankelijk zijn zolang men de url weet. Het kan hier gaan over gevoelige informatie of bijvoorbeeld overheidsdocumenten, waarvan men wil dat deze niet gemakkelijk terug te vinden zijn voor onbevoegden.

Ziekenhuizen doelwit van nieuwe ransomware campagne

Ziekenhuizen en andere zorgverleners zijn het voornaamste doelwit geworden van een nieuwe campagne van de Locky-ransomware, zo claimt het Amerikaanse [beveiligingsbedrijf FireEye](#). Via e-mails met als bijlage docm-bestanden werd de ransomware verspreid.

De [docm-bestanden](#) waren van [macro's](#) voorzien. Wanneer ingeschakeld werd door de macro's de Locky-ransomware op de computer gedownload. Deze ransomware versleutelt vervolgens allerlei bestanden voor losgeld. Volgens FireEye zijn zorgverleners het hardst door de nieuwste campagne getroffen, gevolgd door telecom- en transportbedrijven. Het gaat dan met name om organisaties die

zich in de Verenigde Staten, Japan en Zuid-Korea bevinden. Nederland komt niet terug in de statistieken van FireEye.

In mei van dit jaar liet minister Schippers van Volksgezondheid nog weten dat Nederlandse ziekenhuizen zelf verantwoordelijk zijn voor de aanpak van ransomware en niet de overheid. Op Kamervragen over de veiligheid van ziekenhuissystemen liet Schippers vorige maand nog weten dat het afgelopen jaar twee ziekenhuizen bij het Nationaal Cyber Security Center (NCSC) van de overheid een malwarebesmetting hadden gemeld.



Securitas wil inbraakinformatie via WhatsApp-buurtgroepen

Beveiliging Securitas wil data van WhatsApp-buurtgroepen gaan verzamelen om inbraakgolven te 'kunnen zien aankomen'.

Volgens de site Whatsapp Buurtpreventie Nederland zijn er minstens 4600 van dergelijke buurtgroepen; zo veel zijn er tenminste op die site aangemeld. En die genereren waardevolle data, stelt business developer Bert den Hartog van Securitas. Hij wil met die data 'op inbraakgolven anticiperen'.

Daarvoor moet eerst software ontwikkeld worden, die enerzijds alle berichten in die groepen centraal verzameld maar anderzijds ook rekening houdt met de privacy. Los daarvan is natuurlijk de vraag hoe betrouwbaar al die informatie is.



Op Facebook in plaats van in een bende?

Zou het? Zou internet écht de reden zijn dat de criminaliteit onder jongeren daalt? Criminoloog Frank Weerman, net aangesteld als hoogleraar jeugdcriminologie aan de Erasmus Universiteit, gaat het in ieder geval nader onderzoeken. Hij ziet dat internet de rol van de straat (deels) heeft overgenomen, dat Snapchat, YouTube en Instagram 'virtuele pleintjes' geworden zijn en dat bepaald gedrag uit het echte leven zich heeft verplaatst naar het virtuele leven. 'Ik zou graag willen weten of blootstelling aan crimineel gedrag op sociale media ook extra crimineel gedrag uitlokt',

aldus Weerman. Al eerder zei Weerman dat veel jongeren internet gebruiken om te laten zien dat ze veel durven en dat ze, door dat internet, veel status kunnen krijgen. En om die status is het natuurlijk te doen. 'Jezelf interessant voordoen op internet kan een vervanging zijn van crimineel gedrag: misschien komt het voor die jongeren op hetzelfde neer: het is een soort reputatiemanagement'.



VS: Vrijheid van meningsuiting, sociale media en politiemensen

Vrijheid van meningsuiting? Geldt voor iedereen. Maar niet (altijd) voor politiemensen. En zeker niet op sociale media.

Bij de politie in Tennessee speelden de afgelopen maanden meerdere zaken waarin loslippige agenten werden bestraft. Veel korpsen hebben strakke richtlijnen, soms een half A4-tje, soms wel vijftien, waarin precies wordt omschreven wat wel en wat niet kan. Maar kennelijk houdt niet iedere collega zich daar aan.

Zo kreeg een agent uit Nashville die een videoclip doorstuurde waarin het korps wordt bekritiseerd, als straf tien dagen geen salaris en werd een police officer die in een online ruzie terecht kwam, drie dagen niet betaald. Anderen werden geschorst dan wel ontslagen.

Regionale media schrijven dat zeker anno 2016, met veel 'raciale kwesties', polarisatie en terreurdreigingen, de 'free speech protection' die burgers hebben, voor agenten heel anders opgevat wordt.

Agenten moeten wennen aan het feit dat ze worden 'bekeken' door het publiek, niet alleen als ze in uniform op straat lopen maar zeker ook als ze online hun mening uiten, zegt

Eugene O'Donnell, oud-politieman bij de NYPD en nu professor aan John Jay College in New York. 'The landscape is littered with people who've lost their job over social media'.

Vaak is het een kwestie van naïviteit en emotie, stelt de in free speech gespecialiseerde jurist David Hudson. 'When your job is to handle people of various races' is het niet handig om in allerlei online discussie je persoonlijke mening te verkondigen.

Dat merkte ook police officer Virginia Awkward uit Memphis die een melding van huiselijk geweld kreeg en ter plaatse ontdekte dat de slachtoffers, een moeder en haar baby, in erbarmelijke omstandigheden gehuisvest waren. Awkward startte met een vriendin een GoFundMe-actie, haalde meer dan duizend dollar op voor moeder en dochter maar kreeg van haar werkgever twee berispingen en een dag schorsing omdat ze voor de actie geen toestemming had gevraagd. Tja.

Toch hebben agenten wel degelijk vrijheid van meningsuiting, stelt O'Donnell die vindt dat niet op elke slak zoveel zout moet worden gelegd.



Standaard meer privacy?

Internet en privacy, het zijn inmiddels tegenpolen van elkaar. Websites zijn continu bezig om jou en je gedrag in kaart te brengen. Hiervoor worden cookies en andere trucjes gebruikt. Met enige inspanning kun je je webbrowser voorzien van uitbreidingen om dit tegen te werken. Epic Privacy Browser is een kant-en-klare webbrowser waarbij je privacy centraal staat.

Chromium

Epic heeft drie belangrijke pijlers: privacy, snelheid en veiligheid. De browser is gebaseerd op Chromium. Deze versie van Google Chrome stelt ontwikkelaars in staat om de bouwstenen van Google Chrome te gebruiken voor onder andere een eigen webbrowser. Epic is te vinden op www.epicbrowser.com. Je kunt Epic gebruiken naast je bestaande browser. Epic toont rechtsboven in beeld een icoontje met een paraplu. Hier zie je welke onderdelen Epic voor je blokkeert, bijvoorbeeld reclames, tracking cookies, cookies van derden en andere 'spionnen'. Tijdens het internetten toont Epic steeds een discrete melding van geblokkeerde acties.

Eliminatie cookies

Epic elimineert cookies die websites aanbieden. Dit houdt in dat de cookies wel worden geaccepteerd, maar ook weer automatisch worden opgeschoond. Dit is eenvoudig te testen via www.html-kit.com/tools/cookiebuster. Klik op Set test cookie om een cookie te krijgen. De test-cookie verschijnt boven in beeld in een lijst. Dit soort cookies worden in de praktijk automatisch geïnjecteerd in je webbrowser op het moment dat je een website bezoekt. Sluit Epic, start de browser opnieuw en bezoek www.html-kit.com/tools/cookiebuster nog een keer. Je ziet dat je testcookie niet meer aanwezig is. Doe ditzelfde experiment met een 'normale webbrowser' en je ziet dat de cookies hier niet worden opgeruimd.

Reclame blokkeren

Het nadeel van het automatisch opschonen van cookies is dat je bij elk bezoek aan een website vaak opnieuw de melding moet wegstreken dat de website gebruikmaakt van cookies. Ook is het niet mogelijk om ingelogd te blijven. Als je bijvoorbeeld www.markp-laats.nl bezoekt met Epic en je aanmeldt, dien je dit bij je volgende bezoek opnieuw te doen. Epic heeft een uitgebreid filter voor internetreclames. Hierdoor verdwijnen de reclamebanners uit webpagina's. Je kunt de reclamefilters laten bijwerken via het paraplu-icoontje. Klik bij Adblock options op View om je filterlijst te bekijken en bij te werken.

Een cookie is een klein tekstbestandje dat een website op de harde schijf van je computer zet op het moment dat je de site bezoekt. De belangrijkste functie van cookies is om de ene gebruiker van de andere te onderscheiden.



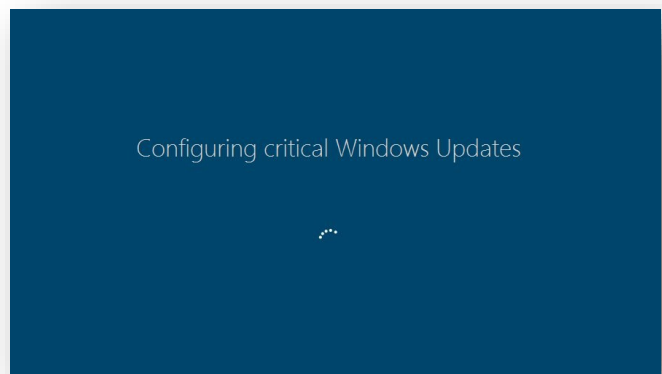
**Epic
Privacy
Browser**

Ransomware vermomt zich als Windows Update

Onderzoekers waarschuwen voor een nieuw ransomware-exemplaar dat slachtoffers laat geloven dat er updates voor Windows worden geïnstalleerd, maar in werkelijkheid in de achtergrond bezig is om allerlei bestanden te versleutelen. De ransomware wordt Fantom genoemd.

Hoe de ransomware zich precies verspreidt is onbekend, maar eenmaal actief start Fantom een bestand genaamd WindowsUpdate.exe. Dit bestand laat een vals Windows Update-scherm zien met de melding dat er updates voor het besturingssysteem worden geconfigureerd. In werkelijkheid is het een afleidingsmanoeuvre en worden bestanden op de computer versleuteld.

Hierna verschijnt op het bureaublad de boodschap "All files encrypted!!!" en krijgen slachtoffers het advies om een e-mail naar een bepaald e-mailadres voor verdere instructies te sturen, zo meldt Jakub Kroustek, onderzoeker van anti-virusbedrijf AVG. Bleeping Computer laat weten dat er nog geen manier is om versleutelde bestanden zonder te betalen te ontsleutelen. 9 van de 55 virusscanners op VirusTotal herkenden de ransomware.



Firefox krijgt bescherming tegen MIME-aanvallen

Mozilla gaat Firefox beschermen tegen aanvallen waarbij bestanden worden gebruikt die in werkelijkheid een ander soort bestand zijn dan ze claimen te zijn. Door de inhoud van een bestand te scannen kunnen browsers het bestandsformaat vaststellen, ongeacht welk contenttype de webserver meegeeft.

Als Firefox een script van een webserver opvraagt en de server vervolgens een script terugstuurt maar stelt dat het om een afbeelding gaat, kan Firefox toch het oorspronkelijke formaat detecteren en het script uitvoeren. Deze techniek wordt MIME-sniffing genoemd. MIME staat voor Multipurpose Internet Mail Extensions en is een standaard voor het definiëren van contenttypes.

Hoewel deze functionaliteit handig is maakt het ook een aanval genaamd "MIME confusion" mogelijk. Neem als voorbeeld een webapplicatie waar gebruikers afbeeldingen kunnen uploaden, maar er niet wordt gecontroleerd of de gebruiker ook daadwerkelijk een echte afbeelding heeft geupload. Zodoende kan een aanvaller een afbeelding met kwaadaardige scriptcode uploaden.

Zodra de browser het bestand tegenkomt zal die de code uitvoeren, waardoor het risico op bijvoorbeeld cross-site scripting en andere aanvallen bestaat. Vanaf Firefox 50 gaat Mozilla daarom stylesheets, afbeeldingen en scripts weigeren als hun MIME-type niet overeenkomt met de context waarin het bestand is geladen. Hiervoor moet de server wel een aparte header meesturen.



Cops in cyberspace

Scotland Yard heeft een nieuwe unit opgezet die met name op twitter en facebook moet gaan zoeken naar online misbruik, online haatzaaien en beledigingen en naar trollen en andere misbruikers. Deze 'Online Hate Crime Hub', jaarbudget 800 duizend pond en vijf fulltime krachten, moet de 'sluier van anonimiteit' weghalen van al die naarlingen die op internet niks anders doen dan beledigen, schelden en haatzaaien. 'By establishing this unit we are sending a strong message to those who use online forums to spread hate that their actions will not be tolerated', aldus een strijdvaardige politiewoordvoerder. 'The Met will make every effort to hold offenders to account and bring them to justice'.

Een vrouw (39, uit Katwijk) die uit wraak 'obscene' foto's en filmpjes van diverse politieagenten op facebook zette, is door de politierechter veroordeeld tot tachtig uur werkstraf. Ze was bekeurd toen haar hond buiten het losloopegebied liep en werd zo boos over die bekeuring dat ze de foto's bewerkte. Een agent kreeg een varkenssnuut, vergezeld van de tekst dat hij 'de wijkgig' was en 'geil word van de koning'. Een andere agent kreeg een piemel als neus. De vrouw bekende de feiten en moet verder 650 euro schadevergoeding betalen.

Het vragenuurtje op facebook van de politie Kaag en Braassem is een succes en wordt daarom voortgezet. In die sessies, die een uurtje duren, worden gemiddeld twintig tot vijftig vragen gesteld. Een politiewoordvoerder spreekt van een 'laagdrempelige manier' om burgers te woord te staan. 'We willen het elk kwartaal gaan doen'. Er zijn twee regels: niet schelden en vloeken en alleen vragen die betrekking hebben op politiewerk. De meeste vragen betreffen verkeerszaken, zo is gebleken. Onder de volgers wordt ook elke keer een 'blik achter de schermen' verlost.

De politie in België gaat voetgangers verbaliseren die op de openbare weg afgeleid worden door hun smartphone. De

actie is ingegeven door alle gedoe rond Pokémon Go, waarbij veel Pokémon-zoekers niet of nauwelijks op het verkeer of op overige weggebruikers letten. De bekeuring, 55 euro, vindt haar rechtsgrond in artikel 7.2 van de wegcode, een soort kapstokartikel waarin staat dat iedere weggebruiker 'zich correct moet gedragen op de openbare weg en anderen niet mag hinderen of in gevaar brengen'. Agenten moeten in hun proces-verbaal wel duidelijk omschrijven wat die hinder dan precies is.

Een 22-jarige man uit Maassluis aangehouden die wordt verdacht van het versturen van duizenden valse e-mails die van PostNL of incassobureau Intrum Justitia afkomstig leken. In de mails werd gevraagd om op een link te klikken, om bijvoorbeeld de track-and-tracecode van een zogenaamd besteld pakketje te volgen of een niet-bestaande schuld te voldoen.

De link in het bericht wees echter naar malware waardoor de man volledige controle over de computer kreeg, aldus de politie. De man kon hierdoor namens slachtoffers online aankopen doen of via internetbankieren geld overmaken. In sommige gevallen, waar een extra code nodig was voor het internetbankieren, benaderde hij de slachtoffers ook op andere manieren om zijn oplichtingspraktijken te kunnen laten slagen.

Een Nederlandse bank namens een aantal klanten hiervan aangifte. Hun uitgebreide interne onderzoek hielp het tactisch politieonderzoek snel in een bepaalde richting. De rechercheurs deden verder onderzoek, vergaarden bewijs en zo sloot het net zich rond de Maassluizenaar. Hij werd uiteindelijk in zijn ouderlijk huis aangehouden voor computervredesbreuk, oplichting en witwassen.

De zoveelste 'catch me if you can' zaak, dit keer in Surrey, Engeland. Daar zoekt de politie ene Harry Brackpool (24), op verdenking van een hele reeks strafbare feiten, waaronder enkele doodsb bedreigingen. Brackpool zag zijn opsporingsbericht en plaatste daarop direct een selfie, met zijn arm om een

(tuin)beeldje van een politieagent. Eerder toonde hij zichzelf al op het strand en poseerde hij bij een politieauto. 'Now the game begins', schreef Brackpool bij de selfie.

Het Team High Tech Crime van de politie heeft een server offline gehaald waarmee ransomware werd verspreid. De internetcriminelen wisten de computers van argeloze internetters te vergrendelen door het zogeheten [Wildfire-virus](#) los te laten. In Nederland en België werden zo bijna zesduizend slachtoffer gemaakt. 236 van hen betaalden in totaal 70 mille om hun computers weer te ontgrendelen. Alle slachtoffers krijgen bericht dat ze hun computers weer aan de praat kunnen krijgen via [Nomoreransom.org](#). Deze site is sinds een maandje in de lucht en al bijna driehonderd duizend keer bezocht.

Open bronnen zijn één ding maar op klokkenluidersite [Wikileaks](#) staan regelmatig privégegevens die eigenlijk nooit online hadden mogen komen, van onschuldige burgers, zoals zieke kinderen, slachtoffers van seksueel misbruik en mensen met mentale aandoeningen. Volgens persbureau AP neemt Wikileaks het niet zo nauw met de privacy – zo werden in 2015 niet alleen de medische gegevens van 'honderden' mensen gepubliceerd maar ook twee namen van minderjarige misbruikslachtoffers en de naam van de homoseksuele Saudiër. AP schrijft dat de database van Wikileaks ook steeds meer virussen en spam bevat. Wikileaks 'censureerde' eerder al gelekte documenten waarin onder meer social security numbers en creditcardnummers van Amerikaanse kiezers stonden.

Rechtspraak

De rechtbank in Den Bosch heeft een man (52, uit Gemert) tot een jaar celstraf veroordeeld voor vervaardiging en verspreiding van kinderporno. De verdachte moet daarnaast twee openstaande jaren celstraf uitzitten. Hij had kinderporno gemaakt van kleine jongetjes en zette die met naam en adres op internet. De man was in 2011 ook al veroordeeld in een kinderpornozaak. Volgens hem was er na zijn vrijlating in het dorp een hekzenjacht tegen hem ontkend en waren enkele slachtoffers van toen daarvan de aanjagers. Naar eigen zeggen dacht hij de dreigementen te kunnen stoppen door namen en adressen van die slachtoffers online te zetten. De politie vond geen enkele aanwijzing voor de dreigementen, de rechtbank sprak van 'een onvoorstelbare gedachtekrinkel'.

De rechtbank in Breda heeft een man (21, uit Werkendam) veroordeeld tot een (maximale) werkstraf van 200 uur en zes maanden voorwaardelijke jeugddetentie voor ontucht met een 7-jarig meisje en het in bezit hebben en vervaardigen van kinderporno. De man pleegde toen hij 18 was, ontucht met het dochtertje van kennissen. Het meisje mocht op zijn slaapkamer computerspelletjes spelen. Filmpjes van de ontucht verspreide de verdachte op internet. De man moet het meisje een schadevergoeding betalen en komt onder toezicht van de jeugdreclassering.

De politierechter in Zwolle heeft een vrouw (40, uit Zwolle) veroordeeld voor smaad. De vrouw kreeg een voorwaardelijke werkstraf van 25 uur, met een proeftijd van drie jaar, omdat ze een facebook-account had gemaakt op de naam van haar ex-partner. Op de pagina plaatste ze 'nare berichten' over de man. Ze noemde hem – drie jaar na het verbreken van de relatie – onder meer een leugenaar, een hoerenloper en een alcoholist. Naar eigen zeggen maakte de vrouw de account om de nieuwe vriendin van de man 'te laten weten hoe hij werkelijk is'. Volgens de officier

van justitie heeft 'elk verhaal twee kanten' maar was toch overduidelijk dat de vrouw fout was geweest. Hij eiste een voorwaardelijke werkstraf plus twee jaar proeftijd. De rechter gaf een jaar extra proeftijd.

Vanwege een vormfout heeft de rechtbank een man (61, uit Den Haag) ontslagen van rechtsvervolging voor het plegen van smaad. De man had in 2013 appjes van zijn schoonzoon op facebook gezet. Die app-berichtjes waren 'seksueel getint' en gericht aan de toen 13-jarige kleindochter van de verdachte. Het OM vond dat smaad maar omdat de klacht over de smaad destijds niet door de schoonzoon zelf was ingediend maar door zijn vrouw, de dochter van de verdachte dus, werd datzelfde OM niet-ontvankelijk verklaard. De verdachte vond dat overigens jammer. 'Ik had de zaak graag inhoudelijk willen uitvechten, om de maatschappij te beschermen tegen dit soort mensen'. Daarmee verklaarde hij ook waarom hij de appjes online had gezet. 'Ik wil voorkomen dat er meer slachtoffers worden gemaakt'. Het OM heeft overigens nog steeds niet besloten of de schoonzoon wordt vervolgd voor de berichtjes.

Gemeenteraadslid Christian Petermann (40, uit Heerlen) heeft van de rechter een geldboete van 500 euro gekregen (waarvan de helft voorwaardelijk) voor zijn 'kampbeultweet'. Daarin vergeleek hij officier van justitie Anja Janssen-De Boer, die betrokken was in het proces tegen politicus Jos van Rey, met SS-kampbewaakster Irma Grese. Petermann reageerde in zijn tweet op de straf die Janssen tegen Van Rey eiste. Hij vond die buitenproportioneel en schreef te hopen Janssen 'oftewel de Irma Grese van het OM nog vanavond verongelukt'. Volgens de rechtbank was die tweet 'onnodig kwetsend en beledigend' en tastte deze de waardigheid van de officier aan. De advocaat van Petermann sprak over vrijheid van meningsuiting maar de rechtbank noemde de tweet

'opzettelijk beledigend' en daarmee niet vallend onder die vrijheid van meningsuiting. Tegen Petermann was veertig uur taakstraf geëist maar de rechtbank vond een geldboete afdoende.

Een PSV-fan (21, uit Mierlo) die via sociale media had geprobeerd een vechtpartij te organiseren tussen fans van PSV en CSKA Moskou, is door de politierechter veroordeeld tot 120 uur werkstraf en drie maanden voorwaardelijk. De verdachte legde, naar eigen zeggen 'voor de grap', contact met CSKA-fans toen die club tegen PSV moest spelen, december 2015. In een groepsapp had hij met vrienden gesproken over het 'pakken' van Russische fans. Bij het stadion werden stickers gevonden waarop het telefoonnummer van de man stond, via die stickers konden Russische fans contact met hem zoeken. Het 06-nummer leidde onder meer naar facebookberichten waarin de verdachte over de geplande actie sprak. 'We delen stickers uit. Of ze willen vechten', schreef de man onder meer. En dat hij 'Moskou net aan de lijn' had. 'Ze willen elk aantal aandoen tot en met 200. Mochten we er meer dan 200 hebben konden ze nog wel aanvullen met pet en sjaals. Maar als we 30-30 zeggen kon dat ook. Waren voor alles in. Na de wedstrijd.' De man werd uiteindelijk op de avond van de wedstrijd door een arrestatieteam uit een café gehaald – hij had al een stadionverbod.

De rechtbank heeft een man (21, uit Breda) veroordeeld tot 240 uur werkstraf, vier maanden voorwaardelijk en verplichte therapie voor het verzamelen van kinderporno. De verdachte spaarde de beelden, afkomstig van een Russische website, zogenaamd 'voor de politie'. Naar eigen zeggen had hij de site via een vriend ontdekt en wilde hij de politie helpen. Maar de politie stond eerder bij hem op de stoep dan andersom.

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 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 afluisterapparatuur; voorbereidingshandelingen
- [Art. 139d, lid 2 Sr](#) Het ter beschikking stellen of voorhanden hebben van technische hulpmiddelen of toegangscoodes 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

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](#)
[Webinar Computercriminaliteit](#)
[Mousejack](#)
[Gegijzeld door Ransomware.](#)
[Wat nu?](#)
[Telefonische phishing](#)

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](#)

Veel meer handige tips vindt u op de [Secure Computing website](#).