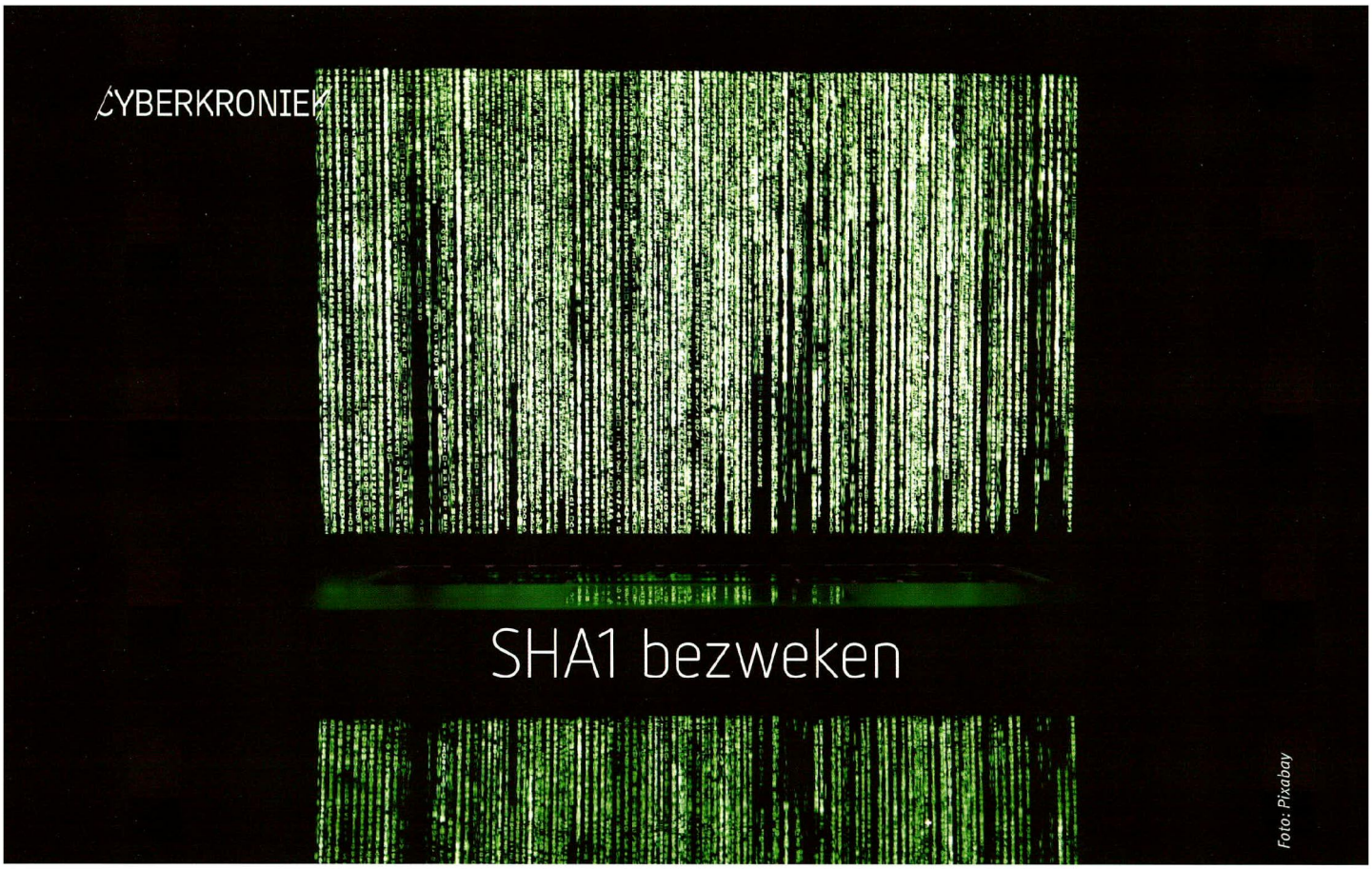
Publicatie : Automatie/PMA
Datum : 31 jul 2017
cm2 : 1.170
Pagina : 36
Advertentiewaarde : € 4.970,00
Regio : Nederland
Frequentie : 8x per jaar
Oplage : 11.000



SHA1 bezweken

Foto: Pixabay

Het zat er al enige tijd aan te komen, maar het "SHA1" hash-algoritme is gekraakt. Een hash is een digitale samenvatting van een document of een andere groep bits. Als het document wijzigt, zal de hash ook wijzigen. Zo is eenvoudig aan te tonen of een document nog origineel is. ▷ Rob Hulsebos

Maar als een document zodanig te wijzigen is dat er tóch de origineel berekende hash uit komt, dan vervalt de betrouwbaarheid van het algoritme, en kunnen we het niet meer gebruiken om de authenticiteit van documenten aan te tonen. Overigens worden hashes niet alleen gebruikt voor documenten, maar ook voor beveiligde internetcommunicatie (https), creditcardtransacties, software-archieven, digitale handtekeningen, backupsystemen, e-mailafzender-verificatie et cetera. Ook die zijn niet meer te vertrouwen op de uniekheid van hun hash. Uiteraard is de hash in aantallen bits altijd korter dan de data zelf. Dus er kan een tweede dataset zijn die exact dezelfde hash oplevert. Dit heet dan een "collision". Als een hash bijvoorbeeld 1024 bits groot is, is de kans dat twee documenten dezelfde hash hebben 1 op 2^1024 (ruwweg 10^-310). Dus in de praktijk is de kans op een collision heel, heel, heel erg klein. Maar als het nu mogelijk is om de inhoud van een bestand op voorhand zó vast te stellen dat de hash gelijk wordt aan de hash van een ander bestand, dan is het algoritme bezweken. Valse documenten, transacties, websites, en nog veel zijn nu naar willekeur aan te maken.

Tot nu toe was alleen maar theoretisch aangetoond dat zo'n falsificatie mogelijk was. Maar eind februari heeft onderzoeker Marc Stevens van het CWI (Centrum voor Wiskunde en Informatica, Amsterdam) aangetoond dat een collision-aanval mogelijk is. Hij is hier zeven jaar mee bezig geweest. Stevens heeft hulp gekregen van Google, die de rekenkracht beschikbaar stelde. Met één

Wat is een hash

Een hash wordt berekend via een wiskundig algoritme over alle betrokken data, bijvoorbeeld de inhoud van een document. Een hash is een hele efficiënte manier van "samenvatten". Het lijkt een beetje op de "negenproef" zoals die gebruikt wordt op bankrekeningnummers, of een "checksum" uit netwerkprotocollen. De bedoeling is dat elke wijziging, hoe klein ook, in een document - of bankrekeningnummer, of netwerkbericht - leidt tot een andere waarde voor de hash. Dan is duidelijk dat er iets gewijzigd is.

Publicatie : Automatie/PMA
Datum : 31 jul 2017
cm2 : 1.170
Pagina : 36
Advertentiewaarde : € 4.970,00
Regio : Nederland
Frequentie : 8x per jaar
Oplage : 11.000

Website

De website “shattered.io” geeft meer diepgaande uitleg over het gedane onderzoek. Daar zijn ook pdf’s te vinden met dezelfde hash en er kunnen bestanden getest worden op de mogelijkheid dat ze gebruikt worden in een collision-aanval.

CPU zou voor de collision-aanval 6.500 jaar rekentijd nodig zijn geweest, met Google’s rekenkracht kon het al in acht dagen. Door verdere wiskundige optimalisaties zal deze tijd de komende jaren nog verder naar beneden gaan, net zoals de tijd die nodig is voor het kraken van het WEP-wachtwoordalgoritme uit wifi in de loop der jaren versneld is van enkele dagen naar fracties van een seconde. Dit brengt de techniek dan in het bereik van criminelen.

Gelukkig is er wel een opvolger van SHA-1, namelijk: SHA-2, en inmiddels ook SHA-3. Veel IT-bedrijven, zoals ook Google, hebben jaren geleden al aangekondigd te gaan stoppen met het ondersteunen van SHA-1 in hun producten. De Google- en Firefoxbrowsers geven sinds begin dit jaar een foutmelding op elke website die nog op SHA-1 vertrouwt. Oudere types smart-tv’s van Philips

Opvolgers

SHA1’s hash is maar 160 bits groot, en dat is tegenwoordig te weinig. Opvolgers SHA2 en SHA3 bevatten 256 en 512 bits hashes.

zijn ook gestopt met SHA-1, maar deze tv’s waren niet meer aan te passen voor moderne algoritmes. Veel functies van die tv’s werken nu niet meer; als doekje voor het bloeden gaf Philips de eigenaren een Amazon Fire tv-stick. Banken gebruiken SHA-1 ook al niet meer.

Sinds 2011 wordt bedrijven al aangeraden om te stoppen met het gebruik van SHA-1. Dat hebben echter heel velen nog niet gedaan. Dat geeft niet direct een onveilige situatie, maar lang wachten is niet verstandig. Het nog oudere “MD5” hashing algoritme, dat vroeger werd gebruikt als handtekening voor Windows softwareupdates, werd door hackers destijds snel misbruikt om malware, voorzien van valse digitale handtekeningen, op een pc geïnstalleerd te krijgen.

Wannacry ransomware en zijn opvolger

Afgelopen mei was de “Wannacry” ransomware uitgebreid in het nieuws, enerzijds vanwege het grote aantal geïnfecteerde PC’s wereldwijd, en anderzijds de relatie met recent gelekte NSA-malware, dit alles gekoppeld aan een knullige implementatie. ▷ Rob Hulsebos

Opvallend aan Wannacry was de wereldwijde verspreiding. Zo raakten de systemen van de Duitse spoorwegen, diverse ziekenhuizen in het Verenigd Koninkrijk, en de Moskouse metro besmet, evenals Renault, Telefonica, een luchtvaartmaatschappij, FedEx, Hitachi en PetroBras (op en.wikipedia.org/wiki/WannaCry_ransomware_attack is een grotere lijst te vinden), en dit zijn nog maar de organisaties die besmetting durfden toe te geven. In Nederland waren de parkeergara- ▸

Publicatie : Automatie/PMA
Datum : 31 jul 2017
cm2 : 1.170
Pagina : 36
Advertentiewaarde : € 4.970,00
Regio : Nederland
Frequentie : 8x per jaar
Oplage : 11.000

ges van QPark getroffen, waardoor de betaalautomaten niet meer functioneerden. Het duurde meer dan een dag voordat alle systemen weer operationeel waren. Volgens het Nationaal Cybersecurity Centrum (NCSC) is in Nederland geen vitale infrastructuur getroffen, noch overheidsinstellingen.

De auteurs van WannaCry hebben de malware niet al te goed geïmplementeerd, waardoor de opbrengsten (in Bitcoins) vrij laag bleven. Dit is te volgen omdat de Bitcoin-administratie publiek is, (behalve over wie toegang heeft tot het geld). Ook hebben de auteurs fouten gemaakt in hun eigen administratie, waardoor slachtoffers die wel het losgeld betalen geen zekerheid hebben of ze de decodeersleutel krijgen. Tenslotte zat er een logische fout in de code, waardoor een beveiligingsonderzoeker met een eenvoudige maatregel de malware wereldwijd kon neutraliseren. Daarvoor was wel noodzakelijk dat de geïnfecteerde systemen toegang tot internet hadden. Was die er niet, dan bleef de malware actief en werd begonnen met het encrypten van bestanden. Opvallend is juist de noodzaak tot het hebben van internettoegang, normaliter horen we vaak het advies om juist zoveel mogelijk losgekoppeld te zijn van internet.

Uiteraard is ook interessant te weten of bescherming tegen WannaCry mogelijk is. In principe wel: Microsoft had een patch voor het lek in Windows al in maart uitgerold. Dus diegenen die hun systemen up-to-date hadden, liepen geen risico. En Microsoft hielp ook diegenen die nog Windows/XP gebruiken: alhoewel de ondersteuning voor XP al jaren geleden geëindigd is, bracht het bedrijf toch nog een speciale patch uit. Zo'n 98% van de slachtoffers draaide Windows 7. Windows 10 is niet kwetsbaar voor Wannacry. Sterker nog, Microsoft claimt dat Windows 10 met de recente "Creators Update" elke ransomware binnen zeer korte tijd kan stoppen, waardoor men hooguit maar een paar bestanden kwijt zou raken. Uiteraard is dit een gevaarlijke claim van Microsoft, hackers zullen extra hun best gaan doen om er toch door te komen.

Het Eindhovense SecurityMatters, wiens "SilentDefense" product malware kan detecteren aan de hand van afwijkende patronen van netwerkverkeer, bracht naar buiten dat hun product zonder enige configuratie of update Wannacry kon detecteren. Dat is altijd sneller dan het beste antiviruspakket, en maakt het ook mogelijk om toekomstige malware te detecteren.

Al met al heeft Wannacry ca. 4 miljoen systemen wereldwijd besmet. Dankzij de toevallige snelle neutralisering en de programmeerfouten is de schade van Wannacy relatief beperkt gebleven. Maar het wachten was op nieuwe ransomware die deze fouten niet maakt, en dan kunnen de gevolgen wel eens groter zijn. Dat is eind juni dan ook gebeurd: een nieuwe uitbraak van ransomware genaamd "Pnyetya" (of "Petya" of "GoldenEye" genoemd) infecteerde wereldwijd bedrijven. Daarbij maakte de ransomware gebruik van dezelfde zwakheden in Windows als Wannacry. Dat wil zeggen dat de geïnfecteerde bedrijven sinds maart dus niets hebben gedaan om de bekende zwakheden in Windows dicht te zetten. Wereldwijd waren nog minstens 38 miljoen Windows systemen te vinden die nog kwetsbaar waren, aldus antivirusleverancier Avast.

Volgens Ronald Prins van beveiligingsbedrijf FoxIT is de nieuwe malware gekoppeld aan gebruikers van het Oekraïense boekhoudpakket "MEDoc", dat aldaar ook verplicht is voor het doen van belastingaangifte. Via de servers van dit bedrijf kon de malware een bedrijf binnenkomen, of zich daarna verder te verspreiden. Volgens Prins is het niet eens de bedoeling van de hackers om geld te verdienen, maar vooral om zoveel mogelijk schade aan te richten. Alle infecties buiten Oekraïne lijken te herleiden te zijn tot gebruikers van MEDoc. Maar dat wil natuurlijk niet zeggen dat Pnyetya niet 'uit kan breken', net zoals in 2010 ook bij Stuxnet gebeurd is. In Nederland waren o.a. containerbedrijf Maersk, MSD (facrmacie), TNT (pakketbezorger) en Raab Kärcher (bouwmaterialen) getroffen. De politie had uit voorzorg delen van haar IT-systemen losgekoppeld.