de Correspondent

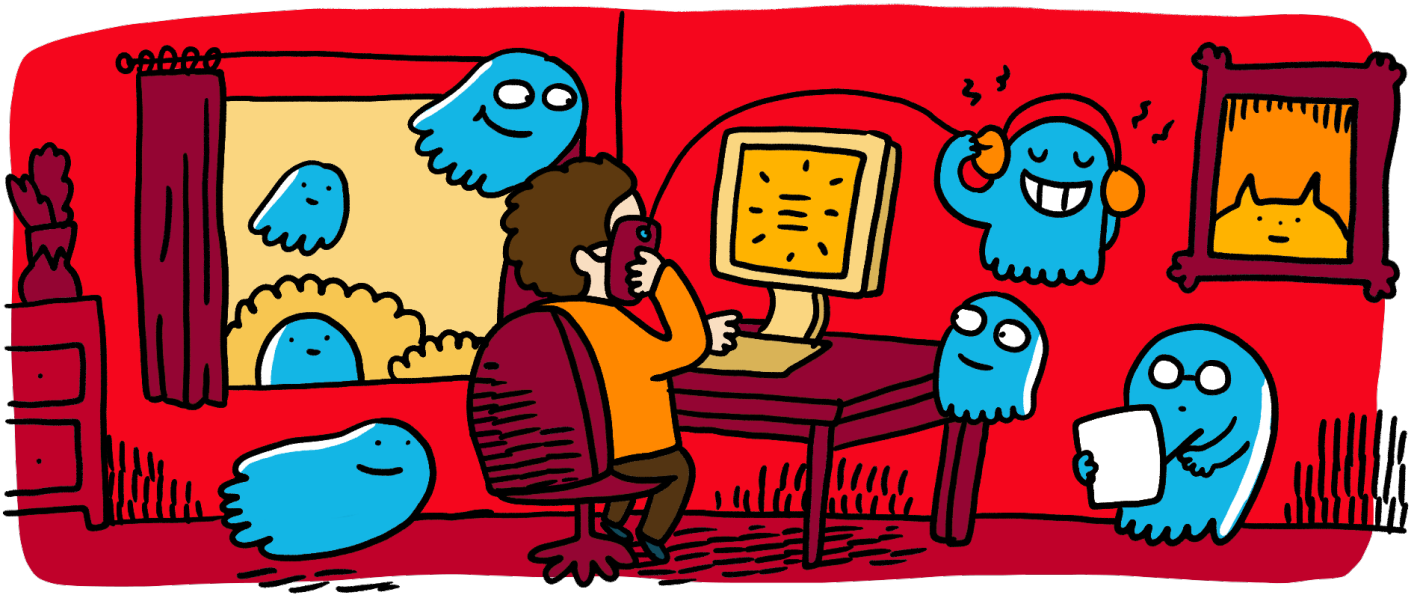
28.12.2016 • Leestijd 9 - 12 minuten

Steeds vaker worden computers besmet door kwaadaardige advertenties. Hoe kan dit en waarom is het zo moeilijk om een oplossing te vinden?

Deze boodschap wordt u aangeboden door een crimineel

Correspondent Veiligheidsindustrie

Dimitri **TOKMETZIS**



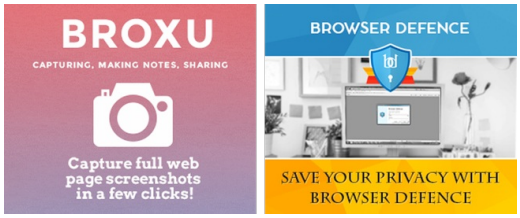
Illustratie's: Rob van Barneveld (voor De Correspondent)

Als de krantenjongen 's ochtends zijn ronde maakt door de buurt, heeft hij niet door dat hij achtervolgd wordt door een dief. Die kijkt waar de jongen stopt en beoordeelt, eerst nog van een afstandje, of het huis van de abonnee interessant genoeg is om in te breken. Als dat het geval is, snelt de dief dichterbij en gluurt door de brievenbus. De krantenjongen lijkt blind voor hem te zijn. De dief kijkt of er een zwak slot op de deur zit en of er geen alarmsysteem hangt. Op het moment dat de krantenjongen de krant door de brievenbus duwt, glipt hij stilletjes en ongezien naar binnen.

Eenmaal in het huis, waart hij rond als een spook. Hij neust door de lades en kastjes van de bewoners en maakt een kopie van wat hij vindt. Die kopietjes stuurt hij, via de internetverbinding, naar zijn baas die zich in een ander land schuilhoudt. Als de nietsvermoedende bewoners hun bankzaken regelen, kijkt de dief over hun schouder mee. De hele dag noteert hij wat de bewoners doen. Soms neemt hij hun gesprekken op geluidsband of video op. Geregeld krijgt

hij de opdracht van zijn baas om collega's op pad te sturen, die in andere huizen inbreken.

Deze beschrijving is een vertaling naar het echte leven van een onderbelichte vorm van digitale criminaliteit: malvertising. Twee weken geleden publiceerde het internetbeveiligingsbedrijf ESET een onderzoek naar een online inbraakgolf waarin precies zo te werk is gegaan. Als je de afgelopen maanden een van deze advertenties op een website bent tegengekomen, heb je misschien zo'n dief in huis gehaald.



De onderzoekers van ESET noemen deze inbraakgolf Stegano, naar steganografie, de kunst en wetenschap van het verbergen van informatie in afbeeldingen. Stegano laat zien hoe professioneel malvertising is geworden, hoe kwetsbaar het online advertentie-ecosysteem is voor kwaadwillenden en hoezeer wij allemaal met dat ecosysteem verknoopt zijn geraakt.

Voor een dief is dat ecosysteem van adverteerders het paradijs. Want verplaats je even in de schoenen van een online crimineel. Het is potentieel lucratief iemands computer te besmetten. Je kunt wachtwoorden achterhalen, en belangrijker nog, ook financiële transacties onderscheppen en geld stelen.

Hoe besmet je iemands computer? Je kunt altijd rekenen op

de slordigheid en goedgelovigheid van mensen. Wachtwoorden die makkelijk te raden zijn. Of ze openen bestanden of links die ze beter dicht kunnen laten. Je kan ook de technologie proberen te kraken door bijvoorbeeld misbruik te maken van fouten in software. Beide kosten veel tijd. Je kunt als hacker specialisten inhuren die jouw malware voor je verspreiden, maar dat kost weer geld.

Steeds meer criminelen beginnen te beseffen dat de voordeur handiger is. En dat die wordt opengehouden door de advertentie-industrie.

Hoe criminelen malvertising inzetten

De laatste jaren heeft die industrie een enorme infrastructuur opgebouwd om alle mensen die op internet zitten tot in iedere hoek en op ieder apparaat te kunnen volgen. Ze hebben deals met websites om spionageapparatuur - die ze zelf schattig cookies noemen - op je computer te mogen plaatsen. Zelfs als je een redelijk privacyvriendelijk platform als De Correspondent leest, kijkt er een aantal bedrijven mee, zoals Google, Vimeo, Soundcloud en New Relic. Bij een site als Nu.nl of Telegraaf.nl zijn dat er zo vijftig.

Die infrastructuur is fenomenaal complex geworden en het bespioneren van internetgebruikers is vrijwel geheel geautomatiseerd. Op het moment dat jij bijvoorbeeld een website laadt, gaat er een bericht van die site naar een online veiling met daarbij wat informatie over jou en waar de advertentie moet komen. Honderden bedrijven kunnen direct op jou bieden. De winnaar mag zijn advertentie,

meestal een plaatje, meeladen met de webpagina. Dit gebeurt in de tijdspanne van een hartslag. Real time bidding heet deze vorm van adverteren.

Een paar jaar geleden ging een aantal criminelen gewoon meebieden. Stegano laat zien hoezeer deze criminelen hun kunst hebben verfijnd.

Stap 1. De criminelen achter Stegano hebben de veiling gewonnen.

Stap 2. Je browser krijgt de opdracht om de advertenties, in dit geval de plaatjes van hierboven, op te halen op een webserver van de criminelen.

Stap 3. De server stuurt eerst een heel klein beetje code, die bekijkt wat voor besturingssysteem je gebruikt, waar je je ongeveer bevindt, de resolutie van je scherm en nog een paar kleine dingen.

Stap 4. Met deze antwoorden bepaalt de server van de criminelen of hij je een schoon of besmet plaatje geeft. Als je een Apple hebt, krijg je bijvoorbeeld het schone plaatje, omdat de code alleen Windowscomputers kan besmetten. Of andersom.

Stap 5. Het besmette plaatje wijkt een klein beetje af van het schone plaatje. In het plaatje dat de

transparantie regelt, zit wat code verstopt die je browser wel uitleest, maar die je met het blote oog niet kan zien. Je hoeft dus niet op het plaatje te l automatisch geladen.

Stap 6. De kwaadaardige code gaat op verkenning uit. Hij kijkt welke browser je gebruikt en of er een antivirusprogramma is geïnstalleerd. En de code onderzoekt of hij niet bekeken wordt. Antivirusonderzoekers gebruiken speciale software om malware te vinden en te onderzoeken. Als de kwaadaardige code zo'n antivirusprogramma vindt, doet hij niets meer.

Stap 7. Als alle tekenen gunstig zijn, wordt weer contact gelegd met een computer van de criminelen. Dit gebeurt over een versleutelde verbinding via een keten van verschillende links, zodat de kwaadaardige computer moeilijk te vinden is. Op die computer staat nog meer malware waarmee de criminelen een achterdeur kunnen inbouwen in het besmette toestel.

Stap 8. Voordat die achterdeur wordt geforceerd, gaat er weer een verkenner aan de slag om er zeker van te zijn dat er geen nieuwsgierige onderzoekers meekijken. Pas als daar zekerheid over is, wordt weer andere malware geïnstalleerd.

Stap 9. De criminelen kunnen oogsten. Ze kunnen internetverkeer onderscheppen, financiële informatie stelen, screenshots maken, alle toetsaanslagen registreren en nog veel meer.

De voorzichtigheid en paranoia van de criminelen - het gebruik van de verkenners - zorgden ervoor dat de bende maandenlang ongezien zijn gang kon gaan. Heel af en toe vielen zijn activiteiten op, zoals in juni van dit jaar. Een ander securitybedrijf, Proofpoint, schreef toen over een bende die deze vorm van besmetting gebruikte. Ze bereikten meer dan een miljoen mensen per dag en wisten telkens duizenden computers te besmetten. Proofpoint noemde deze groep AdGholas. Volgens een ander bedrijf, Malwarebytes, hebben we hier te maken met dezelfde bende als Stegano, maar hebben ze hun werkterrein veranderd. De bende hield zich na ontdekking even stil.

Waar ESET zwijgt over de identiteit van de geïnfecteerde advertentienetwerken, noemt Malwarebytes wel namen. De bende misbruikte het netwerk van Admedia, Yahoo! en MSN (van Microsoft). Dit zijn niet bepaald kleintjes in de advertentiewereld en ze werken vaak met grote, belangrijke websites.

Hoe worden criminelen toegelaten tot deze grote netwerken?

Hoe kan het dat een crimineel toegang kan krijgen tot de netwerken van deze gereputeerde bedrijven? Volgens Jérôme Segura, onderzoeker bij Malwarebytes en iemand die geldt

als dé expert op het gebied van malvertising, kan deze bende zijn gang gaan omdat het advertentiesysteem zo complex is geworden. ‘Stel je voor dat je naar *The New York Times* surft. Op dat moment wordt er dus een veiling in gang gezet door het advertentienetwerk waar *The New York Times* mee werkt. Als niemand op de advertentie biedt, wordt de vraag op een ander netwerk uitgezet. En als daar niemand biedt, wordt de vraag naar weer een ander netwerk uitgezet. Hoe verder je van het oorspronkelijke advertentienetwerk komt, hoe onbetrouwbaarder de adverteerders worden.’

Grote advertentiebedrijven als Google, Yahoo! en Microsoft doen volgens Segura goed onderzoek naar de achtergrond van de adverteerders voordat die toegang krijgen op hun netwerken. Maar bij andere netwerken is dat soms niet het geval, bijvoorbeeld bij netwerken die adverteren op pornosites en sites met illegale downloads. ‘Een kwaadwillende kan zich bij zo’n netwerk aansluiten en proberen op te bieden naar die gereputeerde grote sites,’ aldus Segura. Sommige criminelen misleiden het advertentienetwerk door zich voor te doen als respectabel bedrijf. Ze richten een nepfirma op en slijten aanvankelijk gewone advertenties waar niets mis mee is. Maar op bepaalde tijden, bijvoorbeeld ’s nachts of in het weekend, verspreiden ze advertenties met malware.

Segura vertelt ook over een nieuwe vorm van misleiding die hij onlangs in Engeland tegenkwam. Criminelen hacken een site van een kleine ondernemer, bijvoorbeeld van een

elektricien (www.electrician.co.uk). Zonder dat de eigenaar het doorheeft, voegen ze een domeinnaam toe aan de internetsite (www.ads.electrician.co.uk). Vervolgens gaan ze namens deze elektricien advertenties verspreiden. Voor het advertentienetwerk komen die van een legitiem adres. Domeinschaduwen wordt dit genoemd.

Hoe groot is het probleem?

Cijfers over de omvang van malvertising zijn moeilijk te vinden. Op smoezelige sites is de kans dat je binnen een paar minuten een kwaadaardige advertentie krijgt geserveerd vrij groot, zegt Segura. Voor kwalitatief goede websites is het moeilijker een schatting te geven. En de omvang van malvertising is nogal relatief, zegt Segura. ‘Als ik met een adverteerder spreek, dan gaat het bijvoorbeeld over 100.000 besmettingen. Voor hem is 100.000 een laag getal: adverteerders rekenen vaak in honderden miljoenen impressies. Maar vanuit het perspectief van de beveiligingswereld is 100.000 echt een enorm succesvolle besmetting.’

Ook Yonathan Klijnsma, onderzoeker bij RiskIQ, durft zich niet aan een schatting te wagen. De besmettingen gaan volgens hem in golven. Toen een bende werd opgerold die een belangrijk deel van de malware leverde aan malvertisers, was het ineens een stuk rustiger, maar volgens Klijnsma is het simpelweg wachten totdat er nieuwe malware beschikbaar is en malvertisers weer toeslaan.

Doen advertentiebedrijven er genoeg tegen?

Doen advertentiebedrijven en -netwerken hier wel genoeg tegen? En wat kunnen ze dan doen? De eerste stap, zegt Segura, is dat advertentiebedrijven er transparant over zijn. En dat viel lange tijd nogal tegen.

Maar grote uitbraken halen steeds vaker het nieuws. Afgelopen voorjaar leverden 288 Nederlandse websites, zoals Nu.nl, Marktplaats.nl en RTL.nl, ineens malware aan bezoekers. Het probleem bleek te zitten bij advertentiebedrijf Improve Digital, dat onder andere in Amsterdam is gevestigd en veel grote Nederlandse sites als klant heeft. Improve Digital wil niet over het voorval praten.

Het is dit soort zwijgen dat het snel inspelen op dreigingen zo moeilijk maakt, zegt Segura. ‘Als advertentiebedrijven onderling gegevens uitwisselen, maar ook met de beveiligingsbedrijven, kunnen we veel sneller dit soort malware vinden en bestrijden.’ Uiteraard heeft ook Segura hier een commercieel belang in.

De Nederlandse toezichthouder Autoriteit Consument en Markt (ACM) probeert al een paar

advertentiebedrijven ertoe te bewegen actie te ondernemen. Maar de toezichthouder wil ervoor waken d[e] beklaagdenbankje te zetten. ‘Zij zij[n] slachtoffer van,’ zegt een woordvoerder.

De ACM juichte wel toe dat vorig jaar brancheverenigingIAB Nederland het plan smeedde een soort helpdesk op te richten, gerund door Deloitte en Fox-IT. Dat meldpunt zou advertenties moeten screenen en uitbraken van besmettingen de kop in moeten drukken. Het probleem is alleen dat zo’n platform niet rendabel is. Daarnaast is het Nederlandse advertentienetwerk zo vervlochten met andere netwerken, dat alleen een Nederlands initiatief niet voldoende is. Dat gaat ‘m dus niet worden.

In Amerika is men inmiddels een klein stapje verder. Daar is intussen overleg geweest tussen de directeuren van een aantal grote advertentiebedrijven en -netwerken en een aantal opsporingsdiensten. Daar is een werkgroep nu bezig om standaarden te ontwikkelen over hoe advertenties gescand moeten worden. Zo moet er een betere controle komen als advertenties van buiten een vertrouwd netwerk komen. Als advertenties veel verwijzingen bevatten naar vreemde domeinen, moet er ook extra aandacht zijn. Daarnaast is het vooral belangrijk dat advertentienetwerken goed bijhouden in hoeverre de beheerders van de netwerken toezicht houden op wie zich bij het netwerk aansluit. Het is een begin.

Kan ik er zelf iets tegen doen?

Ondertussen is het vooral zaak om zelf alert te zijn. Een belangrijke misvatting, zegt Segura, is dat mensen denken dat als ze maar nergens op klikken er niets aan de hand is. Maar dat is niet zo.

De besmetting vindt plaats op het moment dat een plaatje geladen wordt. Dat is tegen te houden, bijvoorbeeld met een adblocker. Volgens Segura is er echter een effectievere manier om malware buiten de deur te houden: zorgen dat de software op je computer altijd up-to-date is.

De criminelen gebruiken bekende zwakheden in software om computers te besmetten. Wie up-to-date is, loopt simpelweg minder kans op besmetting. En zorg ervoor dat er een virusscanner op je computer zit. Stegano infecteerde computers niet als er een scanner werd waargenomen. Hoe minder kans je de malvertisers geeft, hoe veiliger je bent.

Meer lezen over online beveiliging?

aangeboden-door-een-crimineel/1458966466848-b867dfea

De Correspondent is een dagelijks, advertentievrij medium met als belangrijkste doelstelling om de wereld van meer context te voorzien. Door het nieuws in een breder perspectief of in een ander licht te plaatsen, willen wij het begrip 'actualiteit' herdefiniëren: niet om je aandacht te trekken, maar om je inzicht te bieden in hoe de wereld werkt.

Alle verhalen lezen? Dat kan voor €6 per maand op: decorrespondent.nl

decorrespondent.nl