Bescherm je bedrijf tegen bedreigen van buitenaf

DE GEVAREN VAN EEN BOTNET

WOUTER HOEFFNAGEL

Een botnet is een groep aan elkaar gekoppelde geïnfecteerde computers, ook wel zombies genoemd. Een dergelijk netwerk wordt beheerd door een beheerder, ook bekend als 'bot herder'. Deze kan het botnet besturen en inzetten voor vaak criminele praktijken. Voorbeelden hiervan zijn het versturen van spam, het opzetten van een DDoS-aanval (Distributed Denial of Service) of het verspreiden van malware. Maar wat zijn eigenlijk de gevaren van een botnet en hoe kan een bedrijf zichzelf hier tegen beschermen?

Een van de gevaren van een botnet is de manier waarop het netwerk zich gedraagt. De malware beschikt vaak over verschillende manieren om een computer te kunnen infecteren, waardoor een botnet in korte tijd zeer groot kan worden. Een botnet van tien- tot honderdduizenden machines is dan ook geen uitzondering. "Een botnet is te vergelijken met een Zwitsers zakmes. De malware maakt vaak gebruik van meerdere technieken waardoor zij makkelijk PC's kunnen bereiken. Het botnet wordt hierdoor groot en kan uiteindelijk uit duizenden tot in sommige gevallen zelfs miljoenen computers bestaan. De computer zijn op dat moment gegijzeld en kunnen door de bot herder, de beheerder van het botnet, worden gedirigeerd. Door hun grootte zijn botnets moeilijk aan te pakken", aldus Eddy Willems, Virus Specialist bij Kaspersky. "Een ander gevaar van botnets is het feit dat zij zich zeer goed kunnen verbergen op de computer. De malware wordt dan ook vaak pas na lange tijd of zelfs helemaal niet door de gebruiker ontdekt", zegt Willems.

Veel gevaren

Daarnaast zijn botnets veelzijdig, er zijn veel manieren waarop een botnet schade kan toebrengen. Rik Ferguson, Senior Security Advisor bij Trend Micro: "Botnets brengen veel gevaren met zich mee. Een met een bot geïnfecteerde machine kan worden ingezet voor allerlei criminele activiteiten. Zo kan de machine worden ingezet voor om andere PC's aan te vallen met behulp van DDoS, kan spam worden verzonden, malafide of illegale websites worden gehost, persoonlijke informatie worden gestolen en toetsaanslagen worden opgeslagen. Ook is het mogelijk dat een bot instructies krijgt om extra malafide software te downloaden. Daarnaast kunnen online sessies worden onderschept en aangepast, zoals online bankieren. Geïnfecteerde machines worden vaak verhuurd aan andere criminelen zodat zij spam of malware kunnen distribueren."

Maar wat kan een bedrijf eigenlijk doen om zichzelf hier tegen te beschermen? Verschillende resellers leveren beveiligingspakketten die computers beschermen tegen een botnet-infectie, en eventuele malware kunnen verwijderen. Daarnaast is het echter ook van belang om de software op computers waaronder het besturingssysteem, anti-virussoftware en firewalls up-to-date te houden. "Veel botnets gebruiken fouten in het operating system (OS). Deze fouten worden meestal snel verholpen met behulp van patches, maar niet iedere systeembeheerder installeert deze even snel. Het is echter van belang het OS up-to-date te houden. Daarnaast is het ook belangrijk de anti-virussoftware te updaten, waardoor deze berekend is op de nieuwste virussen. Ten slot kan ook op firewallniveau maatregelen worden genomen, zoals het dichthouden van alle poorten die niet gebruikt worden", aldus Willems.

Patches en updates

Ook Ferguson is van mening dat een goed beveiligd systeem begint met het up-to-date houden van software. "Een bedrijf kan een aantal dingen doen om zichzelf te beschermen tegen botnet-infecties. Een aantal zijn van groot belang, maar ook gratis uit te voeren zoals het installeren van de nieuwste patches en updates. Het merendeel van de malware maakt gebruik van bekende, en vaak met een patch

verholpen, zwaktes in een systeem. Door zowel het besturingssysteem als de overige software altijd up-to-date te houden worden de mogelijkheden om het systeem binnen te dringen geminimaliseerd. Deze methode werkt uiteraard niet tegen de allernieuwste malware, of tegen malware die wordt geïnstalleerd met behulp van social engineering."

Deze laatste groep, nieuwe malware die fouten in software gebruiken die nog niet door patches zijn aangepast of malware die geïnstalleerd wordt door gebruik te maken van social engineering, wordt hierdoor dus niet tegen gehouden. Vandaar dat verschillende resellers softwarepakketen leveren die malware opsporen en proberen te verwijderen. Dit is echter niet eenvoudig aangezien de makers van malware rekening houden met deze opsporingstechnieken. "Het is belangrijk een effectieve anti-malware-oplossing draaiende te hebben. Moderne malware is echter speciaal geschreven om niet gedetecteerd te worden door anti-virus technieken die naar patronen kijken. Criminelen testen hun malware vaak tegen de anti-virussoftware van alle fabrikanten, en brengen deze pas uit nadat zij zeker weten dat deze niet gedetecteerd wordt. Vervolgens blijven zij hun malware updaten om detectie en verwijdering te voorkomen", aldus Ferguson.

Smart Protection Network

Trend Micro is één van de bedrijven die een product levert dat computers moet beschermen tegen botnet-infecties. Ferguson: "Trend Micro's Smart Protection Network maakt gebruik van kennis van verschillende bronnen en een holistische kijk op de dreiging. Daarom kan de software bescherming bieden tegen bekende, maar vooral ook onbekende malware. De software concentreert zich niet op malafide bestanden, aangezien tijdens het schrijven van malware rekening wordt gehouden met deze vorm van detectie. Daarom wordt de kennis over malafide bestanden gecombineerd met kennis over e-mailbronnen (bijvoorbeeld het IP-adres van een mailserver die spam verstuurd) en kennis over weblocaties (bijvoorbeeld een webserver die een kwaadwillige website host)." Trend Micro heeft hierbij geen OEM-technologie nodig van andere resellers, waardoor alles binnenhuis ontwikkeld kan worden.

Het is van belang dat deze kennis real-time beschikbaar is bij iedere eindgebruiker. "Daarom zijn wij overstapt op een op cloud-gebaseerde dynamische database waarbij iedere beschermde pc continu up-to-date is, zonder dat hiervoor bijvoorbeeld lijsten met malafide URLs hoeven worden verstrekt. Hierdoor wordt een beschermde laag gecreëerd en worden malafide bestanden, e-mails en webpagina's geblokkeerd voordat de klant slachtoffer kan worden. Deze methode werkt ook tegen al geïnfecteerde computers, doordat met behulp van bijvoorbeeld het IP-adres van een webserver het verkeer van de bot naar zijn 'thuispunt' kan worden gedetecteerd, zodat deze kan worden geblokkeerd en de beheerder kan worden gewaarschuwd. Zo wordt voorkomen dat informatie wordt verzonden of nieuwe malafide componenten kunnen worden gedownload."

Kaspersky

Een ander voorbeeld is Kaspersky, dat onder andere Kaspersky Internet Security 2010 levert. Willems: "Wij bieden een aantal producten aan die hier bescherming tegen bieden. Een voorbeeld is Kaspersky Internet Security 2010. Deze bevat meerdere beschermingstechnieken speciaal tegen botnets. Zo is de software voorzien van de anti-botnettechnologie, waarbij een aanval wordt afgeslagen door de computer ongeveer een uur compleet af te schermen van de buitenwereld. Hierdoor kan de aanvaller geen toegang krijgen tot het systeem. Daarnaast maken wij gebruik van een groene zone op de PC. Het surfen naar geïnfecteerde websites blijkt nog steeds een belangrijke oorzaak voor het ongewild deelnemen aan een botnet. Daarom hebben wij een soort virtuele zandbak om de browser heen gebouwd. Deze browser wordt vervolgens altijd in een veilige modus opgestart. De gebruiker kan nog steeds vrij surfen over het internet, echter wordt na het afsluiten van de browser alle mogelijke botnet-infecties automatisch verwijderd. Deze techniek vraagt niet veel van de PC, waardoor tijdens het surfen geen hinder wordt ondervonden. Alleen het opstarten van de browser duurt een fractie van een seconde langer."

Een botnet is dus een gevaar voor bedrijven. Niet alleen hebben zij veel methodes om computers van een bedrijf te infecteren en toe te voegen aan het netwerk, ook zijn zij zeer lastig te detecteren. Daarnaast kan een botnet in worden gezet voor een breed scala van doeleinden. Het aanschaffen van oplossingen die computers beschermd tegen een botnet-infectie is dus van groot belang, wat de markt voor IT-resellers interessant maakt. ●