Using Malware Analysis to Evaluate Botnet Resilience

Rossow, C.

2013

document version
Publisher's PDF, also known as Version of record

Samenvatting

Titel: Een evaluatie van de robuustheid van botnets door middel van malware analyse

Botnets, netwerken van op afstand bedienbare met malware-geïnfecteerde PC systemen, vormen een bedreiging voor miljoenen gebruikers door het versturen van spam, het stelen van gevoelige gegevens of het onbereikbaar maken van essentile services. De onderzoeksgemeenschap is zich bewust van de mogelijkheden van botnets in het algemeen, echter is er geen voldoende inzicht in de veerkracht van deze kwaadaardige netwerken. Zo is het onduidelijk hoe botmasters ervoor zorgen dat botnets gedurende vele jaren operationeel blijven, hoe lang botnets operationeel zijn en hoeveel geïnfecteerde PCs deel uitmaken van deze netwerken.

In dit proefschrift willen wij de manier van onderzoek naar de veerkracht van botnets verbeteren. Als eerste hebben we onderzocht hoe experimenten met botnets kunnen worden uitgevoerd op een wetenschappelijk verantwoorde manier. In hoofdstuk 3 bespreken wij richtlijnen die ons in staat stellen botnets te analyseren in een veilige, realistische omgeving en op een transparante wetenschappelijk correcte manier. Door middel van een literatuurstudie, bestaande uit 36 wetenschappelijke publicaties waarin malware experimenten worden beschreven, onderbouwen wij het belang van dergelijke richtlijnen. Uit dit onderzoek concluderen wij dat het merendeel van de bestudeerde publicaties profijt zouden hebben gehad bij het volgen van de voorgestelde richtlijnen. Vervolgens hebben we gebruik gemaakt van deze richtlijnen om Sandnet, een dynamische malware analyse systeem dat wordt besproken in hoofdstuk 4, te ontwikkelen. We lanceerden Sandnet in februari 2010 als een ondersteunende tool bij het uitvoeren van analyses naar botnets.

Een compleet onderzoek naar de veerkracht van botnets dient twee kanten van het botnet probleem te belichten. De veerkracht van botnets wordt namelijk mede bepaald door de infrastructuur waarvan de aanvallers gebruik maken of waarmee huidige kwaadaardige netwerken worden uitgebreid. In dit proefschrift laten wij zien dat botnets zelden zelf verspreiden, maar gebruik maken van een malware installatie infrastructuur om nieuwe PC systemen te infecteren. Dus om een compleet beeld te schetsen, moeten we ook de veerkracht van malware installatie infrastructuren analyseren. In dit proefschrift wordt het onderzoek

naar de veerkracht van botnets daarom in twee delen behandeld.

In het eerste deel, behandeld in hoofdstuk 5, bespreken we de werking van 23 malware downloaders. Deze malware downloaders installeren voortdurend massaal malafide programma's op al geïnfecteerde PC systemen. Om deze malware installatie infrastructuren te beschermen combineren aanvallers zowel technische als organisatorische maatregelen. Technische maatregelen zijn het coderen en verborgen houden van C&C-kanalen, maar vaak scheiden aanvallers ook de C&C-infrastructuur van de malware installatie infrastructuren. Naast technische maatregelen zorgen malware downloaders ervoor dat hun C&C hosting providers en C&C domein registrars systematisch veranderen. Het toepassen van deze technieken door malware downloaders is een van de redenen dat botnets zo succesvol blijven. Wij stellen twee nieuwe technieken voor die gebruik maken van de publieke aard van de malware installatie infrastructuren om automatisch malware samples te verzamelen voor verdere analyse.

In hoofdstuk 6 laten we zien dat botnet architecturen zeer veerkrachtig kunnen zijn. In het bijzonder behandelen wij de huidige trend in de ontwikkeling van peer-to-peer (P2P) botnets, die speciaal zijn ontworpen om zeer veerkrachtig te zijn. We vergelijken het herstelvermogen van zes bestaande P2P botnets met historische P2P botnets als deze doelbewust worden verstoord. Om de veerkracht van deze P2P botnets te testen hebben wij prototypes ontwikkeld die de botnets verstoren. Deze prototypes hebben geholpen om sinkholing operaties voor te bereiden tegen succesvolle P2P botnets zoals Zeus en ZeroAccess. Uit onderzoek, met gebruik van deze prototypes, blijkt dat deze trend van zeer veerkrachtige P2P botnets leidt tot kwaadaardige netwerken die niet meer gemakkelijk kunnen worden verstoord. Botmasters gebruiken bijvoorbeeld reputatie regelingen of implementeren P2P protocollen met zelfherstellende peerlists wat sinkholing pogingen beperkt. Daarnaast vallen P2P botnets terug op secundaire C&C backup kanalen bij het falen van hun P2P C&C component. Uit ons onderzoek blijkt dat met slechts kleine aanpassingen van de P2P-protocollen dergelijke netwerken zeer veerkrachtig worden. Als gevolg hiervan verwachten wij een opkomst van P2P botnets in de nabije toekomst.

Wij hebben met name technieken onderzocht die botmasters gebruiken om succesvol hun botnets operationeel te houden voor vele jaren. Onze waarnemingen impliceren dat botnet ontmantel strategien veel verder moeten gaan dan het buitenwerking stellen van enkele C&C servers of C&C domeinen. Zulke initiatieven leiden alleen tot tijdelijke verstoring van een botnet en botmasters zullen gebruik maken van hun resterende infrastructuur om de botnets weer operationeel te maken. Deze veerkracht van botnets wordt mede bepaald door relatief eenvoudig organisatorische maatregelingen van de botmasters. Bijvoorbeeld, als C&C eindpunten worden gehost op meerdere plaatsen, dan moeten meerdere partijen in verschillende tijdzones en wetgevingen samenwerken om de botnet te ontmantelen. Onze analyses geven inzicht in de algehele veerkracht van botnets. Dergelijke analyses zijn bijvoorbeeld nuttig bij toekomstige pogingen om botnets te ontmantelen. Onze discussie maakt mensen bewust van de veerkracht van botnets en stimuleert het onderzoek naar alternatieve methoden om deze kwaadaardige netwerken te ontmantelen.