Nicolas Mönch
inf8969
Informatik-Seminar SS2012: IT-Sicherheit
Dozent: Dr. Gerd Beuster

BOTNETS

Inhaltsverzeichnis

Zusammenfassung

Botnets sind eine der beliebtesten und mächtigsten Werkzeuge, die Cyberkriminellen zur Verfügung stehen. Sie bestehen aus in der Regel tausenden Rechnern, welche der Besitzer eines solchen Botnets unter seine Kontrolle gebracht hat und welche er unter Umständen sogar zeitlich koordiniert für seine in der Regel illegalen Ziele einsetzen kann. Solche Netze werden kontinuierlich weitereinwickelt, sodass neuerdings erste Varianten für Apple's MAC OS X und Smartphones auf Android-Basis entdeckt wurden. Diese Seminarausarbeitung befasst sich mit der Arbeitsweise von Bots, verschiedenen Botnet-Topologien, insbesondere ihrer Kommunikations-mechanismen, sowie deren Anwendungsgebieten und gängigen Erkennungs- und Abwehrmaßnahmen.

1. Definitionen und Grundlagen

1.1 Was sind Bots?

Bots sind im Allgemeinen Programme, die weitestgehend selbstständig sich wiederholende Aufgaben und Befehle ausführen. In diesem Zusammenhang jedoch versteht man unter einem Bot ein schädliches Programm, welches ohne Kenntnisnahme des Betroffenen im Hintergrund des PCs ausgeführt wird und durch das Netzwerk übermittelte Befehle abarbeitet. Bots dienen somit der Fernsteuerung fremder System für eigene Zwecke.[1, Kapitel 2][2]

1.2 Was sind Botnets?

Unter Botnets versteht man den Zusammenschluss mehrerer Bots zu einem Netz, welches unter der Kontrolle eines sogenannten Bot-Herders steht. Der Bot-Herder kann hierbei über Server mit seinen Bots kommunizieren und ihnen neue Aufgaben übermitteln. Die Verwendungsmöglichkeiten von Botnets sind vielseitig und vorrangig nur durch die Ideenvielfalt der Botnet-Betreiber beschränkt. Gängige Verwendungen sind unter anderem der Versand von Spam, DDoS-Attacken, sowie Klickbetrug(vgl. Kap 3).[1, Kapitel 2][3][9]

1.3 Lebenszyklus eines Bots

Bevor man die Funktionsweise eines Botnets verstehen kann, muss man sich darüber im Klaren sein, wie ein Anwender sich mit einem Bot infizieren und so zum Teil eines Botnets, üblicherweise auch als Zombie bezeichnet, werden kann und wie er sich grundsätzlich nach der Injektion verhält (vgl. [1 Kap. 2][5][7]).

1. Injektion

   Es gibt viele Möglichkeiten, einen PC zu infizieren. Generell kann man diese unterteilen in durch den Benutzer aktiv begünstigte und passive Injektionen. Bei der aktiven Variante wird der Nutzer dazu verleitet, bösartige Software herunterzuladen und auszuführen, etwa durch Email-Anhänge oder durch eine nach außen seriös wirkende Software, die den Bot enthält. Gängig sind zum Beispiel Meldungen, bei denen der Benutzer dazu aufgefordert wird, weitere Plugins zu installieren, um eine Webseite richtig darstellen zu können. Eine weitere Möglichkeit besteht darin, den Benutzer auf infizierte Webseiten zu locken, etwa durch Spammails oder Spamnachrichten aus Instant Messengern, auf denen dann automatisch im Hintergrund Malware heruntergeladen und ausgeführt wird (Stichwort: Drive-By-

Downloads). Nachteil dieser aktiven Varianten ist, dass der Erfolg vom Nichtwissen und Leichtsinn des Anwenders abhängig ist. Passive Varianten hingegen arbeiten ohne Benutzereinwirkung. Dabei wird versucht, Systeme durch Betriebssystem- oder Softwaresicherheitslücken zu infiltrieren. Eine wichtige Rolle dabei spielt der in den meisten Bots vorhandene Scanning-Mechanismus, der Systeme auf offene Ports testet. Gehört dabei ein Port zu einer Anwendung mit bekannten Sicherheitslücken, so wird das System über diese Schwachstelle angegriffen und infiziert. Ein weiterer Angriffspunkt sind Hintertüren, die möglicherweise von anderen Trojanern hinterlassen wurden. Andere Botnetfamilien hingegen versuchen, Zugriff zu Systemen über die Windows-Freigaben mit Hilfe von Password Guessing und Brute-Force Attacks zu erlangen.

2. Registrierung des Bots beim Kontrollserver

   Nach erfolgreicher Injektion versucht der Bot sich zunächst mit seinem Kontrollserver (Command&Control-Server, C&C, vgl Kapitel 2.1) zu verbinden und signalisiert somit seine Existenz.

3. Nachladen von Modulen

   Möglicherweise, aber nicht Zwangsläufig, folgt daraufhin das Nachladen von Modulen, welche zum Beispiel Updates für den Bot, Informationen über weitere C&C-Server oder aber auch Software zur Bekämpfung des Antivirenprogramms enthalten können.

4. Sicherung des Systems

   Um seine Existenz auf dem System zu sichern, versucht der Bot, das Antivirenprogramm mittels seiner Software zu entfernen, sich vor ihm zu verstecken oder es soweit zu verändern, dass es nur noch ineffektiv arbeitet. Bei letzterer Variante wirkt das Antivirenprogramm für den Benutzer noch aktiv, jedoch ist es so beeinflusst, dass es keine Aktivitäten des Bots erkennen und berichten wird.

5. Befehle empfangen und ausführen

   Nachdem das System nun Teil des Botnets geworden ist, verbindet es sich regelmäßig zum C&C-Server, um dort Befehle zu empfangen, gegebenenfalls weitere Module nachzuladen und im Anschluss der Ausführung der Befehle die Ergebnisse zu übermitteln. In diesem Stadium verbleibt der Bot, bis er schließlich - ob freiwillig oder nicht - vom System entfernt wird. Bei der freiwilligen Entfernung versuchen Bots häufig, ihre Spuren zu verwischen, indem sie sämtliche durch sie erzeugte Dateien und von ihnen verursachte Logeinträge

entfernen.

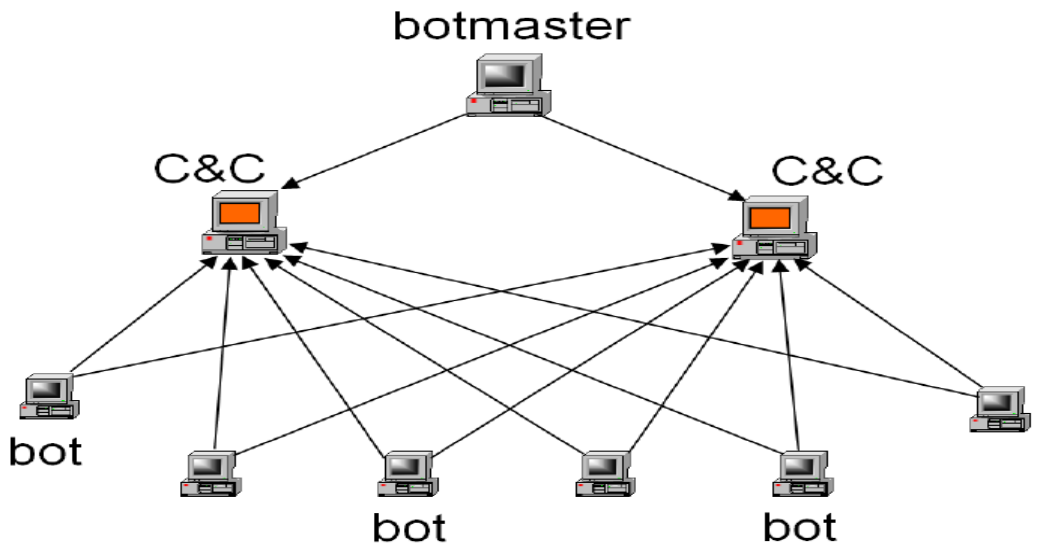
Zusammengefasst sind Bots also durch Schadsoftware ferngesteuerte Rechner, in denen ihn gefährdende Sicherheits- und Kontrolldienste ineffektiv gemacht wurden. Sie verfügen über Mechanismen, um sich mit einem Kontrollserver zu verbinden und so koordiniert und vielseitig agieren zu können. Der folgende Abschnitt erläutert die Funktionsweise von Botnets anhand deren Struktur und Kommunikationsarten.

2. Funktionsweise von Botnets

2.1 Strukturen

Die wichtigste Komponente eines Botnets ist die bereits erwähnte Kontrolleinheit, über die der Bot-Herder mit seinen Bots kommunizieren kann. Über sie werden Befehle vermittelt und gegebenenfalls Ergebnisse entgegengenommen. Die Form dieser Kontrolleinheit kann variieren und hängt stark von der Topologie, sowie des genutzten Protokolls des Botnets ab, welche im Folgenden erläutert werden.

1. Zentralisierte Topologie



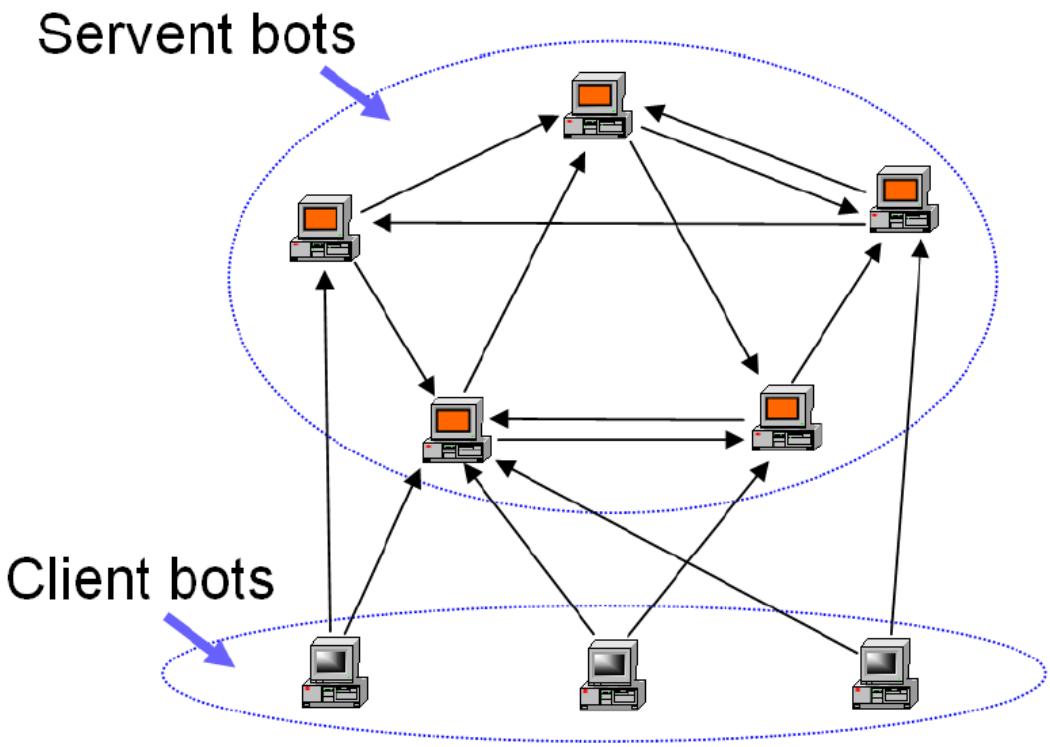
Quelle: http://static.usenix.org/event/hotbots07/tech/full_papers/wang/wang_html/figure1.png

Botnets mit zentralisierter Topologie verfügen über Command&Control-Center (C&C), welche in der Obhut des Bot-Herders liegen, und zu denen sich alle Bots des Botnets verbinden. Das C&C registriert dabei neue Bots, überwacht sie und vermittelt Befehle an sie. Somit ist es dem Bot-Herder möglich, mit allen Bots gleichzeitig und mit geringer Verzögerung zu kommunizieren. Der Nachteil dieser Variante besteht darin, dass die C&Cs einen zentralen Angriffspunkt gegen das Botnet darstellen: Geraten sie aus der Kontrolle des Bot-Herders, so gibt es keine Möglichkeit der Kontaktaufnahme zum Botnet, welches somit außer Kraft gesetzt ist.

Desweiteren können Botnets mit zentralisierter Topologie nach ihrem Kommunikationsprotokoll unterschieden werden (vgl. [1, Kapitel 3][9][10][12]):

- IRC-basierte Botnets verwenden das Internet Relay Chat zur Kommunikation zwischen Bots und dem C&C. Dabei verfügen die Bots über in sich fest verankerte Adressen des IRC- Servers. IRC-Server haben den Vorteil, dass sie sehr schnell und einfach zu erstellen sind, und über sie bidirektional kommuniziert werden kann. Der Nachrichtenaustausch findet über private Nachrichten oder innerhalb der Channel unter Umständen mithilfe der Willkommensnachrichten statt.
- IM-basierte Botnets kommunizieren über Dienste wie z.B. ICQ, Windows-Live-Messenger. Da jedoch jeder Bot sein eigenes Benutzerprofil bei einem dieser Dienste besitzen muss und sich diese nicht automatisiert erstellen lassen, hat sich dieser Ansatz nicht durchsetzen können und wird in der Praxis kaum angetroffen [1].
- Web-basierte Botnets erfreuen sich hingegen großer Popularität. Bots verbinden sich mit einem Webserver, von welchem sie Befehle erhalten und Daten abliefern können. Solche Webserver lassen sich leicht einrichten und bequem per Webinterface steuern.
- Vereinzelt gibt es Botnet-Typen, welche ausschließlich die allgemeinen Protokolle TCP, ICMP und UDP verwenden.

2. **Dezentralisierte Topologie**



Quelle: http://static.usenix.org/event/hotbots07/tech/full_papers/wang/wang_html/figure2.png

Botnets mit dezentralisierter bzw. Peer-to-Peer(P2P) Topologie verfügen nicht über ein zentrales C&C. Ein Bot, der zu einem Botnet mit dieser Topologie gehört, verfügt über eine Liste benachbarter Bots, mit denen er kommunizieren kann. Sobald der Bot Befehle empfängt, leitet er diese an seine benachbarten Bots weiter. Auf diese Weise propagieren sich die Befehle durch das Netzwerk. Dem Bot-Herder hingegen genügt es, Kontrolle über einen einzigen Bot zu erlangen. Der Aufbau eines solchen Botnets gestaltet sich schwierig, da jeder Bot eine individuelle Liste benachbarter Bots erhalten muss. Daher wird für diesen Zweck häufig ein C&C eingesetzt. Sobald diese Liste jedoch übermittelt wurde, findet keine weitere Verbindungsaufnahme zum C&C statt. Nachteile dieser Architektur sind der erhöhte Zeitaufwand für das Vermitteln von Befehlen, sowie die erschwerte Kontrolle und Übersicht über das Netzwerk. Ein Außerkraftsetzen eines solchen Netzwerkes gestaltet sich hingegen deutlich schwerer als bei zentralisierten Netzwerken.[1, Kapitel 3][7][9][10][12]

2.2 Methoden zur Sicherung der Kommunikation

Botnets mit zentralisierter Topologie sind darauf angewiesen, dass Bots jederzeit das C&C auffinden können. Tritt dieser Fall nicht ein, so kann der Bot keine neuen Befehle entgegennehmen und scheidet somit aus dem Botnet aus. Als Gegenmaßnahme nutzen Botnets DNS-Technologien, welche die Wahrscheinlichkeit des Eintretens eines solchen Falls verringern sollen (vgl. [1, Kapitel 3][7][10]):

1. Domain Name

Durch Einsatz dieser Technik werden im Bot hart kodierte Adressen durch einen Domain Name ersetzt. Somit ist es ohne Auswirkungen auf die Bots möglich, die IP-Adresse des C&C zu ändern.

2. Multihoming

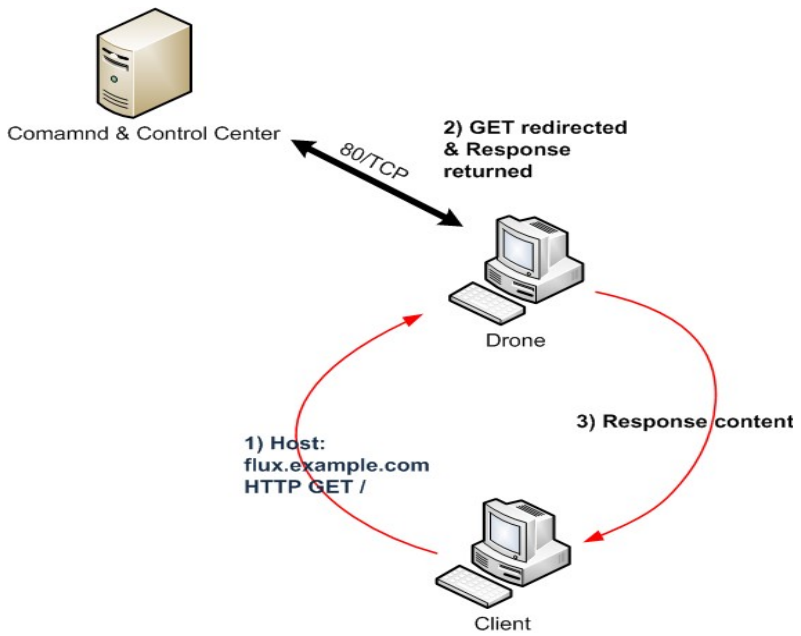
Durch Multihoming kann ein DNS-Record auf mehrere IP-Adressen und somit mehrere C&Cs verweisen, sodass bei Ausfall einzelner C&Cs trotzdem eine Verbindung hergestellt werden kann.

3. Dynamic DNS

Mit Dynamic DNS ist es möglich, DNS-Konfigurationen in Echtzeit zu verändern. Botnets benutzen Dynamic DNS um heruntergefahrene C&Cs durch neue zu ersetzen.

4. Fast Flux

Fast Flux ist eine DNS-Technik zum Tarnen von C&Cs. Ziel ist es, einen DNS-Eintrag auf möglichst viele IP-Adressen verweisen zu lassen. Bei den IP-Adressen handelt es sich um Bots, welche als Proxy-Server für das C&C dienen und im Hintergrund Anfragen an das C&C weiterleiten. Fast Flux bedient sich dabei der Lastverteilung per DNS (Round-Robin-DNS). Diese Technik sorgt dafür, dass die aus den DNS-Anfragen resultierende Liste von IP-Adressen permutiert wird und somit mit hoher Frequenz verschiedene IP-Adressen ermittelt werden. Zusätzlich erhalten die DNS-Einträge nur eine geringe Lebenszeit (geringer TTL-Wert im Minutenbereich).



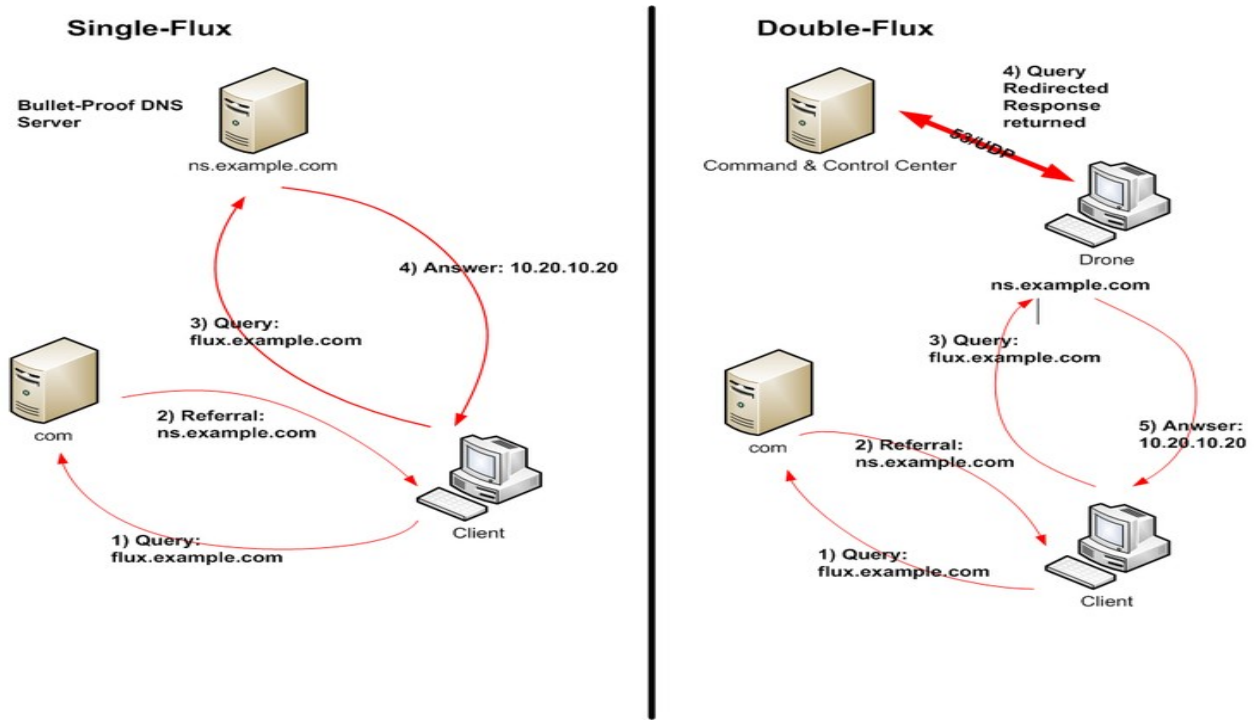
Quelle: http://de.wikipedia.org/w/index.php?title=Datei:Fast-Flux.png&filetimestamp=20100510171920

Single-Flux-Netzwerke:

Bei Single-Flux-Netzwerken handelt es sich um eine einfache Sorte von Fast Flux. Hierbei tragen sich regelmäßig Bots im DNS A-Record der Domäne ein.

Double-Flux-Netzwerke:

Bei Double-Flux-Netzwerken wir zusätzlich zum Single-Flux-Verfahren auch der Nameserver stündlich ausgetauscht. Bots tragen sich hierzu in den DNS NS-Record für die DNS Zone ein. Diese Nameserver kommunizieren ebenfalls im Hintergrund mit dem C&C.



Quelle: http://www.honeynet.org/node/135

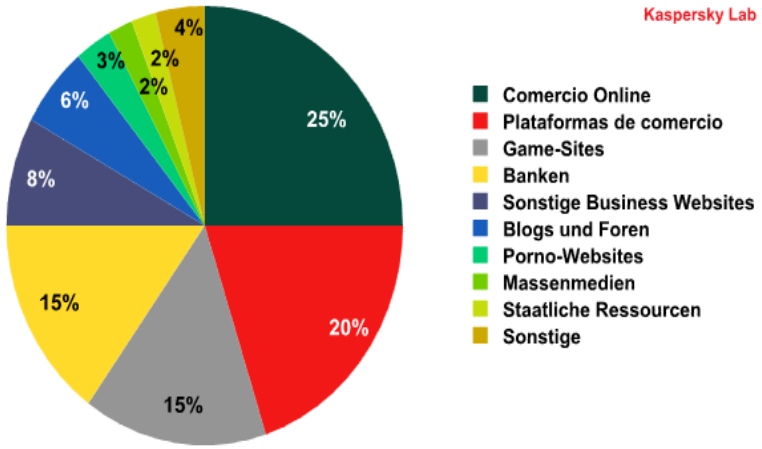
3. Anwendungsgebiete

Botnets sind vielseitig einsetzbar. Die gängigsten Anwendungsgebiete werden im Folgenden beleuchtet. Dabei entstehen Angriffe meist nicht aus dem Interesse des Botnet-Betreiber selbst, viel mehr ist in den vergangenen Jahren durch Vermietung von Botnets für zweifelhafte Verwendungszwecke eine Untergrundwirtschaft entstanden.

3.1 Distributed Denial of Service (DDoS)

Da Botnets üblicherweise aus einer großen Anzahl an Bots bestehen und diese zeitlich koordiniert agieren können, sind sie sehr gut dafür geeignet, DDoS-Attacken auszuführen. Ziel ist es, möglichst viele Anfragen gleichzeitig an eine Website zu stellen, sodass dessen Server unter der Last des entstandenen Datenverkehrs zusammenbricht und die Seite für den normalen Besucher nicht mehr erreichbar ist. Ziele dieser Angriffe sind in der Regel Webseiten, die über das Internet Serviceleistungen bereitstellen, wie zum Beispiel Online-Shops oder Glücksspiel- und Wettanbieter. Durch die Zeiten, in denen die Websites nicht online ist, entstehen bei den Opfern Einnahmeeinbußen und nicht zuletzt Imageschäden. Nicht zuletzt dadurch ist es in der Praxis auch rentabel, DDoS-Attacken anzudrohen und so Geld zu erpressen.

Opfer von DDoS-Attacken nach Branche.



Quelle: http://www.viruslist.com/de/analysis?pubid=200883774

3.2 Versand von Spamnachrichten

Der weitestverbreitete Verwendungszweck von Botnets liegt darin, Spamnachrichten zu versenden. Laut MessageLabs Intelligence: 2010 Annual Security Report von Symantec[17] stammten ca. 88% aller versandten Spamnachrichten aus Botnets. Durch den Einsatz einer großer Anzahl von Bots muss jeder einzelne von ihnen keine große Anzahl an Mails versenden und so sinkt die Wahrscheinlichkeit, dass die IP-Adressen der Bots auf den Blacklists der E-Mail-Server landen und somit als Spam identifiziert werden. Spam wird in den meisten Fällen zu Werbezwecken verwendet, desweiteren aber auch zum Versand von Schadsoftware in E-Mail-Anhängen, sowie zum Verbreiten von in den E-Mails enthaltenen Links, welche auf Phishing-Webseiten führen, auf denen versucht wird, dem Opfer sensible Informationen zum Beispiel durch die Aufforderung der Eingabe der Kreditkartendaten auf gefälschten Bankseiten zu entlocken. Ein weiterer Vorteil für Spammer, welche mit Botnets agieren, liegt darin, dass die Bots gleichzeitig dafür genutzt werden können, ihre Rechner nach gespeicherten E-Mail-Adressen zu durchsuchen. Diese wiederum können zum Spam-Versand genutzt oder verkauft werden.

3.3 Klickbetrug

Eine weitere Geldeinnahmequelle für Botnet-Betreiber besteht im Klickbetrug. Hierbei werden Konten bei Werbefirmen angelegt, welche für Werbung nach Besuchern der Website oder Anzahl der Klicke auf die Werbebanner zahlen. Diese Aufgabe wird dann von den Bots übernommen.

3.4 Datendiebstahl & Ransomware

Ebenfalls möglich ist es, über die Bots die auf den Rechnern gespeicherten Zugangsdaten für E-Mail-Konten, Chat-Programme, FTP-Server und Webseiten und weitere Daten zu stehlen. Diese können dann verkauft oder selbst verwertet werden. Auch ein Einsatz als Ransomware ist denkbar, bei dem private Daten des Benutzers verschlüsselt oder der Zugriff auf jene verhindert wird. Im Folgenden erfolgt eine Freigabe bzw. Entschlüsselung der Daten lediglich gegen Zahlung eines Lösegelds.

3.5 aktuelle Situation

Die derzeit größten Botnets dienen nahezu ausschließlich zum Versand von Spam. Ihre größten Vertreter sind das Cutwail- sowie das Grum-Botnet. Zusammen verfügen sie über ca. 3,5 Millionen infiltrierte Rechner[6]. Für besonderes Aufsehen sorgten Anfang des Jahres allerdings andere Botnets. Zum einen geht es dabei um das Flashback-Botnet, welches sich im Gegensatz zu herkömmlichen Botnets nicht auf Windows-, sondern auf Mac-OS-X-Maschinen verbreitete. Zeitweilig sollen rund 550000 Rechner infiziert worden sein[14]. Die Verbreitung erfolgte u.a. durch eine Java-Sicherheitslücke. Desweiteren wurde ebenfalls Anfang dieses Jahres ein Botnet entdeckt, welches aus Smartphones auf Android-Basis besteht. Dieses Botnet kontrolliert rund 140000 Geräte in China und wird zum Versand von Premium-SMS genutzt. Verbreitet hat es sich durch einen alternativen App-Store[15].[1, Kapitel 2][5][6][7][9]

4. Methoden zur Erkennung und Größenabschätzung von Botnets

Dieses Kapitel beschreibt beispielhaft einige Techniken, die zur Botnet-Erkennung und Größeneinschätzung eingesetzt werden. Unterscheiden lassen sich diese in passive und aktive Techniken. Passive Techniken beziehen ihre Daten aus dem einfachen Beobachten und Mitschreiben der Aktivitäten, welche innerhalb eines Netzwerk stattfinden. Dadurch sind sie leicht nachvollziehbar und ohne aktives Eingreifen ist es dem Bot-Herder nicht möglich, herauszufinden, ob diese Techniken in einem bestimmten Netz gegen ihn eingesetzt werden. Nachteilig hingegen ist, dass diese Techniken nur beschränkt Daten für die Analyse ermitteln können. Im Gegensatz zu passiven beziehen aktive Methoden ihre Daten, indem sie sich Zugang zum Netzwerk verschaffen und dort mit den Teilnehmern interagieren. So können weitaus detailliertere Informationen gesammelt werden, jedoch besteht ebenfalls die Gefahr, die Ergebnisse durch das eigene Eingreifen

zu verfälschen. Aktive Techniken können möglicherweise vom Bot-Herder als solche erkannt werden, sodass dieser Gegenmaßnahmen wie die Veränderung der Botnet-Struktur oder Angriffe wie DDoS-Attacken gegen das Netzwerk einleiten kann.

4.1 Passiv: Intrusion Detection System (IDS)

IDS sind Systeme zur Erkennung von Angriffen aus dem Netz. Unterschieden werden sie in netzwerkbasierte und hostbasierte IDS. Identifiziert ein IDS eine Aktivität als einen Angriff, veranlasst diese Gegenmaßnahmen, zum Beispiel werden gesendete Pakete zurückgewiesen oder zur Analyse weitergeleitet, oder es werden offene Verbindungen geschlossen. Durch die Analyse ermittelte Informationen über diese Angriffe können für Blacklists und/oder für die Verbesserung der Firewall genutzt werden. Der Nachteil dieser Technik besteht darin, dass es für große Netzwerke sehr aufwendig ist, den kompletten Datenverkehr zu untersuchen. Filtert man den Datenverkehr jedoch vorher, so verliert das System an Effektivität, da die Wahrscheinlichkeit, bösartige Pakete zu übersehen, steigt. Außerdem erkennt diese Technik nur verseuchte Pakete anhand von Mustern bekannter Signaturen. Verteilt man diese Signaturen auf mehrere Pakete, werden wiederum andere Techniken zu deren Erkennung benötigt. Ebenfalls problematisch ist, dass IDSs vor dem Problem stehen, bei moderaten Einstellungen zur Gefahrenerkennung nicht alle Attacken zu erkennen, bei erhöhten Einstellungen jedoch häufig regulären Datenverkehr als Attacken zu werten.[2][7]

4.2 Passiv: Honeypots

Ein Honeypot ist ein gezielt schwach geschützter Bereich innerhalb eines Netzwerks, in dem Netzwerkdienste und Verhalten von Anwendern simuliert werden. Honeypots sollen somit Angreifer anlocken und von dem realen und besser geschützten Netzwerk ablenken. Innerhalb des Honeypots werden alle Zugriffe protokolliert, wodurch Informationen über Angriffsmuster und Verhalten nach der Injektion gesammelt werden können. Honeypots bieten Dienste, welche vom Anwender oder dessen Kommunikationspartnern nicht genutzt werden. Wird jedoch ein solcher Dienst in Anspruch genommen, so kann man dies als Angriffsversuch werten, da Angreifer nicht zwischen Honeypots und den realen Servern und Programmen unterscheiden können. Alle hierbei entstehenden Aktivitäten werden vom Honeypot protokolliert.[2][5][7]

4.3 Aktiv: Sinkholing

Unter Sinkholing versteht man eine aktive Größenabschätzungsmethode, durch die Bots eines Botnets beim Versuch der Kontaktaufnahme zum C&C durch Änderung des Domain Name auf einen eigenen Server geleitet werden. Auf dem eigenen Server können Analyse-Frameworks eingesetzt werden, welche dann die Größe und Aktivität eines Botnets abschätzen und gesendete Pakete der Bots untersuchen können. Möglich ist auch eine gleichzeitige Weiterleitung der Bots zum C&C, sodass der Bot-Herder nichts von dem Sinkhole mitbekommt. Durch diese Weiterleitung bleiben die Bots zwar aktiv, trotzdem können sie genutzt werden, um Informationen über das Botnet zu sammeln und im Folgenden koordiniert mehrere C&Cs eines Botnets abzuschalten.[2]

5. Abwehrmaßnahmen gegen Botnets

Im folgenden Abschnitt werden verschiedene Gegenmaßnahmen zur Abwehr bzw. Schwächung von Botnets erläutert.

5.1 Blacklisting

Diese Maßnahme hat keine direkte Auswirkung auf das Botnet an sich, jedoch kann durch Blacklisting die von Botnets ausgehende Gefahr verringert werden, indem IP-Adressen von infizierten Rechnern und auf sie verweisende URLs blockiert werden. Blacklists haben den Vorteil, dass sie von unterschiedlichen Programmen gemeinsam verwendet werden, wie zum Beispiel von Antivirenprogrammen und Browsern.

5.2 Direkte Außerbetriebnahme von C&Cs

Diese Gegenmaßnahme bezieht sich auf zentralisierte Botnets mit der Absicht, C&Cs außer Betrieb zu nehmen. Durch das reine Ausschalten solcher Kontrollstrukturen bleiben die Teilnehmer des Botnets weiterhin infiziert, sodass hier ein weiterer Eingriff durch geeignete Antivirenprogramme und ähnliche Werkzeuge von Nöten ist, worauf aber in diesem Abschnitt nicht weiter eingegangen werden soll. Konnte durch Erkennungs- und Größenabschätzungsmethoden wie in Kapitel 4 erläutert, durch beispielsweise Dekompilation oder andere Analysetechniken der Standort eines C&Cs herausgefunden werden, so wird versucht, mittels Kooperation der für den Server verantwortlichen Service-Provider das C&C außer Betrieb zu nehmen. Da C&Cs jedoch meist fragwürdige Provider auswählen, welche die Anonymität ihrer Kunden auch in solchen Fällen garantieren, ist die Variante nicht häufig erfolgreich. Zusätzliches Hindernis können ebenfalls die

Gesetze der Länder, in denen der Provider ansässig ist, sein. [2]

5.3 Walled Garden

Die Idee hinter einem „Walled Garden“ besteht darin, als infiziert erkannte Systeme unter Quarantäne zu setzen. Abgesehen von Anfragen für Seiten, welche zur Bekämpfung von Malware dienen und auf einer speziellen Whitelist stehen, werden alle Verbindungsaufbauversuche durch den Internet Service Provider blockiert und der Benutzer auf eine Informationsseite weitergeleitet, welche ihn über den Befall und weitere Gegenmaßnahmen in Kenntnis setzt.[2]

5.4 Gegenmaßnahmen für P2P-Botnets

In P2P-Botnets besitzt jeder Bot eine begrenzte Liste benachbarter Bots. Verbindet sich ein neuer Bot mit dem Botnet, so wird dieser Peer innerhalb des Netzes bekannt gemacht. Gegenmaßnahmen versuchen dies auszunutzen. Beispielsweise wird versucht, lokalisierten Bots eine Vielzahl invaliden Peers bekannt zu machen und somit deren Listen mit falschen Einträgen zu füllen, welche wiederum unter den Bots weiter verteilt werden.[2]

6. Literaturverzeichnis

[1]Schiller, Craig; Binkley, Jim: Botnets: The Killer Web App. 1. Auflage, Syngress, 2007, ISBN-13: 978-1597491358

[2]Plohmann, Daniel; Gerhards-Padilla; Leder, Felix: Botnets: Detection, Measurement, Disinfection & Defence. ENISA, Mai 2011, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/botnets/botnets-measurement-detection-disinfection-and-defence

[3]Dunham, Ken; Melnick, Jim: Malicious Bots: An Inside Look Into the Cyber-Criminal Underground of the Internet. Auerbach Pubn, 2008, ISBN-13: 978-1420069037

[4]Wang, Qian; Chen, Zesheng; Chen, Chao; Pissinou, Niki: On the Robustness of the Botnet Topology Formed by Worm Infection. Department of Electrical & Computer Engineering, Florida International University, Department of Engineering, Indiana University - Purdue University Fort Wayne, Indiana, 2010, http://www2.fiu.edu/~qwang003/publications/globecom2010.pdf

[5]Cisco: Botnets: The New Threat Landscape White Paper, 2007, http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns171/ns441/networking_solutions_whitepaper0900aecd8072a537.pdf

[6]McAfee: McAfee Threats Report, First Quarter 2012, 2012, http://www.mcafee.com/de/resources/reports/rp-quarterly-threat-q1-2012.pdf

[7]Krogoth: Botnet construction, control and concealment. 2008, www.shadowserver.org/wiki/uploads/Infomation/thesis_botnet_krogoth_2008_final.pdf

[8]Shadowserver: www.shadowserver.org

[9]Kaspersky: Botnetze – Geschäfte mit Zombies, Whitepaper, 2008, http://www.ectacom.com/images/stories/vendors/kaspersky/wp/wp_de_botnetze_geschaefte_mit_zombies_v1_0_0408.pdf

[10]Damballa: Botnet Communication Topologies, Whitepaper, 2009, https://www.damballa.com/downloads/r_pubs/WP%20Botnet%20Communications%20Primer%20%282009-06-04%29.pdf

[11]Trend Micro: The Botnet Chronicles, Whitepaper, 2010, http://countermeasures.trendmicro.eu/wp-content/uploads/2012/02/the_botnet_chronicles_-_a_journey_to_infamy__nov_2010_.pdf

[12]Bu, Zheng; Bueno, Pedro; Kashyap, Rahul: Das neue Zeitalter der Botnets, McAfee Whitepaper, 2010, http://www.mcafee.com/de/resources/white-papers/wp-new-era-of-botnets.pdf

[13]Strayer, W. Timothy; Lapsely, David; Walsh, Robert; Livadas, Carl: Botnet Detection Based on Network Behavior, 2008, http://www.ir.bbn.com/documents/articles/BotnetDetectChapter.pdf

[14]heise.de: AV-Firma vermutet größere Verbreitung des Mac-Trojaners "Flashback", 2012, http://www.heise.de/security/meldung/AV-Firma-vermutet-groessere-Verbreitung-des-Mac-Trojaners-Flashback-1516895.html

[15]heise.de: Smartphone-Botnetz erwirtschaftet angeblich Millionen mit Premium-SMS, 2012, http://www.heise.de/security/meldung/Smartphone-Botnetz-erwirtschaftet-angeblich-Millionen-mit-Premium-SMS-1433332.html

[16]honeynet.org: www.honeynet.org

[17]Symantec: MessageLabs Intelligence: 2010 Annual Security Report, 2010, www.inteco.es/file/27gHxrzWsYyeyRTFYq8MuQ