



W H I T E P A P E R

Botnetze –
Geschäfte mit Zombies



Die vorliegende Analyse erklärt, was genau unter Zombie-Netzen oder auch Botnetzen zu verstehen ist, wie sie aufgebaut sind und wie sich mit ihnen Geld verdienen lässt. Zudem beschäftigt sich der Bericht mit aktuellen Tendenzen in der Botnetz-Entwicklung.

Botnetze gibt es schon seit etwa 10 Jahren und ungefähr genau so lange warnen Experten bereits vor der Gefahr, die von ihnen ausgeht. Trotzdem wird das Problem weiterhin unterschätzt und vielen Anwendern ist nicht klar, worin die tatsächliche Bedrohung durch Zombie-Netze besteht. Es sei denn, ihnen wurde bereits die Internetverbindung gekappt, Geld von der Kreditkarte abgebucht oder das E-Mail-Postfach beziehungsweise der IM-Account gestohlen.

Was ist ein Botnetz?

Ein Botnetz ist ein Netzwerk aus Computern, die mit einem Schadprogramm des Typs Backdoor infiziert sind. Dieses ermöglicht es Cyberkriminellen, die befallenen Rechner fernzusteuern. Das gelingt ihnen wahlweise bei einzelnen Computern, einem größeren Teil der betroffenen PCs oder auch mit dem gesamten Netz.

Speziell zum Aufbau von Botnetzen entwickelte Schadprogramme des Typs Backdoor nennt man Bots. Botnetze verfügen über gewaltige Rechenressourcen und sind eine gefährliche Waffe im Cyberspace sowie ein effektives Mittel zum illegalen Gelderwerb. Die zu einem Botnetz gehörenden Computer können von den Cyberkriminellen von jedem beliebigen Standort aus gesteuert werden. Stadt, Land und sogar Kontinent spielen dabei keine Rolle. Zudem wahrt das Internet die Anonymität der Botnetz-Betreiber.

Die mit Bots infizierten Computer können direkt oder indirekt gesteuert werden. Im ersten Fall kontaktiert der Kriminelle einen infizierten Computer und steuert diesen mittels Befehlen, die im Bot-Programm integriert sind. Bei der indirekten Steuerung meldet sich der Bot selbst beim Steuerungszentrum oder anderen Computern im Netz und führt von ihnen empfangene Befehle aus.

Der Besitzer eines infizierten Computers ahnt in der Regel nicht, dass sein Rechner von Ganoven zweckentfremdet wird. Aus diesem Grund werden von Bots befallene und heimlich von Cyberkriminellen kontrollierte PCs auch als Zombie-Computer bezeichnet. Ein Verbund aus Rechnern nennt sich deshalb Zombie-Netz. Bei den meisten Zombies handelt es sich um PCs von Heimanwendern.

Einsatzszenarien für Botnetze

Botnetze lassen sich zu vielerlei kriminellen Aktivitäten wie Spam-Versand nutzen und könnten sogar einen Cyberkrieg zwischen verschiedenen Staaten auslösen.

► **Spam-Versand:** Hierbei handelt es sich um die am weitesten verbreitete und dabei eine sehr einfache Art, Botnetze zu kriminellen Zwecken zu nutzen. Nach Einschätzungen von Experten gelangen derzeit über 80 Prozent aller Spam-Mails über Zombie-Computer in Umlauf. Dabei stammt der Werbemüll nicht zwangsläufig von den Botnetz-Betreibern, da sie ihre Rechner-Infrastruktur gegen einen gewissen Betrag an Spammer vermieten.

Spammer wissen, wie wertvoll Botnetze sind. Nach Einschätzungen von Kaspersky Lab verdient ein durchschnittlicher Spammer zwischen 50.000 und 100.000 US-Dollar im Jahr. Aus vielen tausenden von Computern bestehende Botnetze ermöglichen es ihnen, innerhalb kürzester Zeit Millionen von Reklame-Mails zu versenden. Die Methode bietet Spammern aber noch einen weiteren Vorteil. Denn üblicherweise landen Adressen, von denen aus aktiv Spam verschickt wird, auf den Blacklists der E-Mail-Server und werden daher blockiert oder automatisch als Spam gekennzeichnet. Indem sie ihren Werbemüll von vielen hunderttausend Zombie-Computern verschicken, können sie dieses Problem teilweise umgehen.

Botnetze sind für Spammer auch deshalb so attraktiv, weil sie darüber auf infizierten Computern gespeicherte E-Mail-Adressen stehlen können. Diese werden entweder weiterverkauft oder von den Betreibern selbst zum Spam-Versand verwendet. Dabei fallen ihnen bei einem ständig wachsenden Botnetz immer mehr E-Mail-Adressen in die Hände.

► **Cyber-Erpressung:** Sehr häufig werden Botnetze zu erpresserischen Zwecken genutzt. Dabei führen nicht selten einige hunderttausend infizierte Rechner so genannte DDoS-Attacken durch (Distributed Denial of Service), indem sie den anzugreifenden Server mit einer Unmenge von falschen Anfragen überhäufen. Irgendwann kann sie der Server nicht mehr bearbeiten und ist auf Grund von Überlastung für Anwender nicht mehr erreichbar. In der Regel fordern die Kriminellen Geld, damit sie die Angriffe einstellen.

Heute sind viele Firmen auf das Internet angewiesen. Sind die Unternehmens-Server nicht erreichbar, kommen die Geschäfte völlig zum Erliegen, was wiederum zu finanziellen Verlusten führt. Um mit ihren Servern so schnell wie möglich weiterarbeiten zu können, erfüllen Unternehmen lieber die Forderungen der Erpresser, als sich an die Polizei zu wenden. Genau darauf spekulieren die Cyberkriminellen, weshalb DDoS-Attacken ständig zunehmen.

DDoS-Attacken werden aber auch zu politischen Zwecken eingesetzt und zielen dabei meist auf Server staatlicher Institutionen oder Regierungsorganisationen ab. Diese Art von Angriffen ist auch deshalb besonders gefährlich, da sie von anderen Ländern zur Provokation genutzt werden können. Deren Cyberangriff kann über die Server eines anderen Landes laufen und unter Umständen vom Territorium eines dritten Landes aus gesteuert werden.

- ▶ **Anonymer Internetzugang:** Cyberkriminelle können über Zombie-Computer anonyme Verbindungen zu Internetservern herstellen und Verbrechen begehen, zum Beispiel Websites hacken oder gestohlenen Geld transferieren.
- ▶ **Verkauf und Vermietung von Botnetzen:** Auch durch den Verkauf oder die Vermietung von Botnetzen lässt sich illegales Geld verdienen. Der Aufbau von Botnetzen, die zum Verkauf bestimmt sind, ist ein eigener Geschäftszweig im Cyberkriminellen-Business.
- ▶ **Phishing:** Adressen von Phishing-Sites landen unter Umständen recht schnell auf verschiedenen Blacklists. Indem die Cyberkriminellen die infizierten Computer eines Botnetzes als Proxy-Server verwenden, können sie die tatsächliche Adresse ihrer Phishing-Site schnell ändern und verschleiern.
- ▶ **Diebstahl vertraulicher Daten:** Der Diebstahl vertraulicher Daten ist und bleibt für Cyberkriminelle überaus attraktiv. Mit Hilfe von Botnetzen kann die Chance außerdem um ein tausendfaches höher liegen, an Passwörter für E-Mail-Clients, Chat-Programme, FTP-Ressourcen und Websites heranzukommen sowie andere wichtige Anwenderdaten zu stehlen. Der Bot, mit dem die Computer innerhalb des Zombie-Netztes infiziert sind, kann andere Schadprogramme wie Trojaner herunterladen und damit weiteren Schaden anrichten. Dabei fallen den Kriminellen alle auf den Zombie-Rechnern gespeicherten Passwörter in die Hände. Die Zugangsdaten werden anschließend verkauft oder zur massenhaften Infizierung von Websites verwendet, um den Bot weiter zu verbreiten und das Zombie-Netz zu vergrößern. Das geschieht zum Beispiel mittels der Passwörter für alle gefundenen FTP-Accounts.

Befehle für Bots

Bots können die unterschiedlichsten Befehle ausführen, beschränken sich in der Regel aber auf unten stehende Kommandos. Deren Bezeichnungen können zwar je nach Bot abweichen, ihre Funktion bleibt jedoch dieselbe.

- ▶ **Update:** Download und Start einer ausführbaren Datei von einem Server. Hierbei handelt es sich um einen Basisbefehl, welcher den Bot auf Anweisung des Zombie-Netz-Betreibers auf eine neuere Version aktualisiert. Dieser Befehl ermöglicht es zudem, Computer mit anderen Schadprogrammen wie Viren

oder Würmer zu infizieren sowie andere Bots zu installieren. Mit der Update-Anweisung können auf allen zum Botnetz gehörenden Computern gleichzeitig trojanische Programme installiert werden, die nach gespeicherten Passwörtern suchen und diese an einen Web-Server schicken.

- ▶ **Flood:** Dieser Befehl sendet eine große Anzahl falscher Anfragen an einen bestimmten Server im Internet, um diesen außer Kraft zu setzen oder die Kanäle eines bestimmten Netzwerksegments zu überlasten. Eine derartige Anfragenflut kann ernsthafte Serverstörungen zur Folge haben und dazu führen, dass der Server für normale Anwender nicht mehr erreichbar ist. Flood-Angriffe unter Verwendung von Botnetzen nennt man DDoS-Attacken. Es gibt viele Möglichkeiten, falsche Netzanfragen zu erstellen, auf die an dieser Stelle nicht näher eingegangen wird.
- ▶ **Spam:** Mit dieser Anweisung laden infizierte Rechner eine Spam-Mail herunter und verteilen sie an ausgewählte Adressen. Jedem Bot wird eine bestimmte Anzahl von Adressen zugeteilt.
- ▶ **Proxy:** Verwenden der Zombie-Computer als Proxy-Server. Meist wird diese Funktion nicht über einen separaten Befehl ausgeführt, sondern gehört zum Funktionsumfang des Bots. Mit der Proxy-Anweisung lässt sich jeder zum Botnetz gehörende Computer als Proxy-Server deklarieren und verschleiern so die tatsächliche Adresse, über die das Botnetz gesteuert wird.
- ▶ **Sonstige:** Andere Befehle werden wesentlich seltener verwendet und kommen nur in vereinzelt Botnetzen zum Einsatz. Mit Hilfe dieser Anweisungen können Bots unter anderem folgende Aktionen ausführen: Übermittlung von Screenshots, überwachen der Tastatureingaben, protokollieren der Netzaktivität des Anwenders als Vorbereitung zum Datendiebstahl, versenden bestimmter Dateien vom infizierten Computer, anfordern von Software-Versionsnummern, empfangen detaillierter Informationen zum Anwendersystem und dessen Umgebung, übertragen einer Liste der zum Botnetz gehörenden Computer und andere.

Botnetz-Typen

Botnetze werden entweder nach ihrer Netzwerk-Topologie oder ihren Steuerprotokollen klassifiziert.

Klassifizierung von Botnetzen nach ihrer Architektur

Gegenwärtig sind lediglich zwei verschiedene Botnetz-Architekturen bekannt.

① Botnetze mit Steuerungszentrum. In einem so organisierten Botnetz sind alle Zombie-Computer mit einem Steuerungszentrum oder auch C&C (Command&Control Centre) verbunden. Das C&C registriert neu hinzugekommene Bots in seiner Datenbank, überwacht ihren Zustand und schickt ihnen die von den Botnetz-Betreibern ausgewählten Befehle. Entsprechend sind im Steuerungszentrum alle an das Netz angeschlossenen Zombie-Computer sichtbar. Zur Steuerung eines zentralisierten Zombie-Netzes muss dessen Betreiber auf die Kommandozentrale zugreifen können.

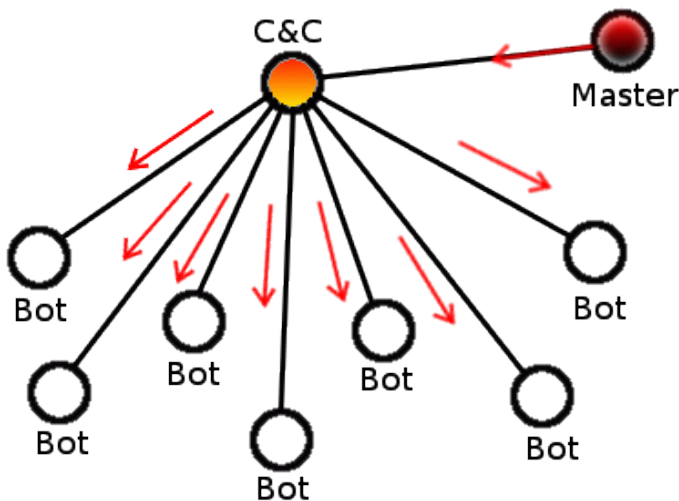


Abb. 1: Zentralisierte Topologie (C&C)

Botnetze mit zentralisierter Steuerung sind der am weitesten verbreitete Typ von Zombie-Netzen. Derartige Botnetze sind einfach zu entwickeln, lassen sich einfach verwalten und sie reagieren schnell auf Befehle. Allerdings ist es auch vergleichsweise einfach, solche Botnetze außer Kraft zu setzen, denn zu diesem Zweck muss lediglich das C&C deaktiviert werden.

② Dezentralisierte oder P2P-Botnetze (von engl. „Peer-to-Peer“). Zu dezentralisierten Netzen zusammengeschlossene Bots verbinden sich nicht mit einem Steuerungszentrum, sondern jeweils mit einigen anderen infizierten Computern aus dem Zombie-Verbund. Jeder Bot verfügt über eine Adressliste einiger Nachbar-Rechner und leitet eingehende Befehle an diese weiter. Um ein dezentralisiertes Botnetz zu steuern, muss der Cyberkriminelle lediglich Zugriff auf einen der zum Zombie-Netz gehörenden Computer haben.

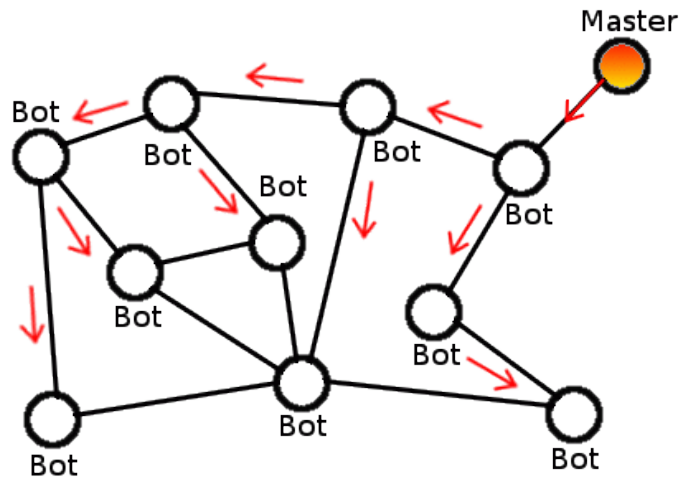


Abb. 2: Dezentralisierte Topologie (P2P)

Der Aufbau eines dezentralisierten Botnetzes ist in der Praxis recht aufwändig. Jeder neu infizierte Computer muss über eine Liste derjenigen Bots verfügen, mit denen er sich innerhalb des Zombie-Netzes verbinden soll. Sehr viel einfacher ist es, dem Bot die Liste seiner Nachbarn zunächst über einen zentralisierten Server mitzuteilen und ihn erst dann in das P2P-Netz zu integrieren. Auch P2P-Netze bedienen sich dieser Topologie, nutzen jedoch zeitweise ein C&C. Da dezentralisierte Botnetze nicht über ein Steuerungszentrum verfügen, ist es auch weitaus schwieriger, sie zu neutralisieren.

Klassifizierung von Botnetzen nach dem verwendeten Netzwerkprotokoll

Damit die Befehle des Botnetz-Betreibers alle infizierten Rechner erreichen, muss eine Verbindung zwischen den Zombie-Computern und dem Steuer-PC bestehen. Sämtlicher über Netzwerke laufender Datenverkehr läuft nach Protokollen ab, welche die Kommunikation zwischen den einzelnen Teilnehmern regeln. Daher werden Botnetze auch nach den von ihnen verwendeten Netzwerk-Protokollen klassifiziert und unterteilen sich wie folgt.

① **IRC-orientiert:** Einer der ältesten Botnetz-Typen, bei dem die Steuerung der Bots auf dem IRC (Internet Relay Chat) basiert. In so einem Netz verbindet sich jeder infizierte Computer mit einem IRC-Server, dessen Adresse fest im Bot verankert ist. Danach empfängt der PC über einen bestimmten IRC-Kanal die Befehle des Botnetz-Betreibers.

② **IM-orientiert:** Ein weniger verbreiteter Botnetz-Typ. Er unterscheidet sich von der IRC-orientierten Variante nur darin, dass der Datentransfer über Instant-Messaging-Dienste (IM) wie AOL, MSN, ICQ und andere abläuft. Derartige Botnetze sind nicht sehr populär, weil jeder infizierte Rechner einen eigenen IM-Account benötigt. Zudem müssen die Bots eine Netzverbindung aufbauen und dann ständig online bleiben. Da es bei den meisten IM-Diensten nicht möglich ist, sich mit dem gleichen Account von unterschiedlichen Computern aus einzuloggen, muss jeder Bot über eigene Zugangsdaten verfügen. Zudem versuchen die IM-Anbieter zu verhindern, dass sich Accounts automatisch erstellen lassen. Daher

sind die Betreiber von IM-orientierten Botnetzen stark eingeschränkt, was die Anzahl der Accounts und Bots betrifft, die gleichzeitig online sein können. Natürlich können sich die infizierten PCs auch ein und dasselbe Konto und damit die Online-Zeit teilen. Doch auch diese Variante ist äußerst umständlich, da ein solches Netz nur sehr langsam auf Befehle reagiert.

- ③ **Web-orientiert:** Ein vergleichsweise neuer und sich schnell entwickelnder Botnetz-Typ, der über das Internet gesteuert wird. Der Bot verbindet sich mit einem bestimmten Webserver, nimmt von diesem Befehle entgegen und übermittelt ihm im Gegenzug Daten. Botnetze dieser Art sind aus mehreren Gründen populär: Sie lassen sich problemlos einrichten, können auf eine Vielzahl von Webservern zurückgreifen lassen sich über ein Web-Interface bequem steuern.
- ④ **Andere:** Neben den oben aufgeführten Botnetz-Typen gibt es weitere, die über ein eigenes Protokoll kommunizieren und nur auf dem TCP/IP-Stack basieren. Solche Botnetze verwenden nur die allgemeinen Protokolle TCP, ICMP und UDP.

Entwicklung der Botnetze

Die Geschichte der Botnetze beginnt in den Jahren 1998 und 1999, als mit den heute wohlbekanntesten Schädlingen NetBus und BackOrifice2000 die ersten trojanischen Programme des Typs Backdoor auf den Plan traten. Beide Programme verfügten erstmals über zahlreiche Funktionen zum Steuern infizierter Computer. Cyberkriminelle hatten dadurch erstmals die Möglichkeit, mit den Dateien eines entfernten Computers zu arbeiten, dort neue Programme auszuführen, Screenshots zu erstellen, die Lade des CD-Laufwerks zu öffnen oder zu schließen und vieles mehr.

Trojaner des Typs Backdoor liefen ohne Zustimmung oder Wissen des Anwenders auf dessen Computer. Zur Steuerung eines infizierten Rechners mussten die Hacker zunächst eine Netzwerk-Verbindung herstellen. Die ersten Backdoors liefen in lokalen Netzwerken auf Basis des TCP/IP-Protokolls und demonstrierten im Grunde die verschiedenen Einsatzmöglichkeiten der Windows-API zum fernsteuern von Computern.

Bereits um das Jahr 2000 ließen sich mehrere Computer gleichzeitig über dort installierte Clients steuern. Im Gegensatz zu modernen Backdoors übernahmen die Programme NetBus und BackOrifice2000 allerdings die Rolle eines Netzservers. Sie öffneten einen bestimmten Port und warteten anschließend darauf, dass ihr „Schöpfer“ sich einwählt. Aktuelle Backdoors, die zum Aufbau von Botnetzen dienen, stellen die Verbindung selbst her.

Der nächste Entwicklungsschritt basierte auf der Idee, dass mit einem Backdoor-Programm infizierte Com-

puter die Netzwerk-Verbindung selbst herstellen und danach ständig online sichtbar sein sollten. Das setzte natürlich voraus, dass die Rechner eingeschaltet und funktionstüchtig sind. Vermutlich ging dieser Entwicklungsschritt von einem Hacker aus, denn die Bots der neuen Generation verwendeten mit IRC (Internet Relay Chat) einen traditionell von Hackern genutzten Verbindungskanal. Da im IRC bereits Bot-Programme mit offenem Quellcode eingesetzt wurden, vereinfachte das die Malware-Entwicklung immens. Allerdings waren die IRC-Bots nicht für die Remotesteuerung eines Systems vorgesehen und verfügten über andere Funktionen. Sie beantworteten beispielsweise Anwenderanfragen und lieferten verschiedene Informationen zur Wetterlage oder dem letzten Login eines Chat-Besuchers.

Nachdem sie einen Computer infiziert hatten, nahmen die neuen Bots unter dem Deckmantel eines Besuchers mit den IRC-Servern Verbindung auf und warteten auf Nachricht des Botnetz-Betreibers. Dieser konnte jederzeit die Liste der Bots einsehen, allen infizierten Computern gleichzeitig Befehle erteilen oder eine private Mitteilung an nur einen einzigen Rechner schicken. Damit wurde erstmals ein Botnetz realisiert, das über eine Steuerzentrale verfügt, die später auch C&C (Command & Control Centre) genannt wurde.

Die einfache Syntax des IRC-Protokolls erleichterte es den Hackern, Bots zu entwickeln. Um die Dienste eines IRC-Servers zu nutzen, benötigt man kein spezielles Client-Programm, sondern kann universelle Netzclients wie etwa Netcat oder Telnet dafür verwenden.

Die Existenz von IRC-Botnetzen sprach sich schnell in Hackerkreisen herum. Das rief schon bald die ersten „Botnetz-Piraten“ auf den Plan. Diese verfügten teilweise über die gleichen Netzwerk-Kenntnisse wie die Betreiber von Botnetzen, versuchten aber, ihr Geld ein bisschen leichter zu verdienen.

Die Botnetz-Piraten kidnapten IRC-Kanäle, in denen sich auffällig viele Besucher tummelten. Anschließend ließen sie ihre Bots auf andere und passwortgeschützte IRC-Kanäle los und erlangten schließlich die vollständige Kontrolle über ein „fremdes“ Netz infizierter Rechner.

Die Verlagerung der Steuerungszentren ins Internet markiert die nächste Etappe in der Botnet-Entwicklung. Zunächst entwickelten die Hacker Fernsteuerungstechniken für Server, die auf bekannten Skript-Engines wie etwa Perl und PHP oder in seltenen Fällen auch ASP oder JSP liefen. Später stellten sie eine Verbindung zwischen einem Web-Server und Rechnern her, die im lokalen Netzwerk eingebunden waren. Damit konnten die Hacker so konfigurierte Computer von jedem beliebigen Standort aus steuern. Eine Anleitung, wie man in das lokale Netzwerk integrierte Computer fernsteuern und dabei Schutzfunktionen wie Proxy oder NAT umgehen konnte, wurde im Internet veröf-

fentlicht und stieß in einschlägigen Kreisen auf große Resonanz. Die Remotesteuerung basierte darauf, eine HTTP-Verbindung mit der Steuerzentrale aufzubauen und dabei die lokale Konfiguration des Computers zu verwenden.

Gab der Anwender in der Systemkonfiguration Adresse, Port, Login und Passwort für den Proxy-Server ein, wurde über die Datei Wininet.dll automatisch der Webzugriff per HTTP-Protokoll aktiviert. Aus Sicht der Programmierer war das eine einfache und bequeme Lösung.

Die mehr oder weniger legalen Fernsteuerungs-Techniken legten den Grundstein für den Aufbau weborientierter Botnetze. Kurz darauf tauchte ein simples Skript zur Steuerung eines kleinen Computernetzwerks auf, was Cyberkriminelle zu ihren Zwecken nutzten.

Weborientierte Botnetze erwiesen sich als äußerst komfortabel und erfreuen sich im Cyberkriminellen-Milieu bis heute großer Beliebtheit. Die meisten Computer lassen sich über jedes internetfähige Gerät steuern. Darunter fallen auch zu WAP und GPRS kompatible Mobiltelefone, deren Benutzeroberfläche jedes Kind bedienen kann. Der stetig fortschreitende Ausbau der Internet-Infrastruktur und die immer ausgefeilteren Web-Technologien trieben die Verbreitung von Web-Botnetzen zusätzlich voran.

Es gab auch Versuche, über IM-Kanäle gesteuerte Botnetze zu entwickeln. Sie waren allerdings kaum verbreitet, weil sich Hacker dazu für jeden Rechner eine IM-Nummer besorgen mussten und Schutzsysteme eine automatische Account-Registrierung verhindern. Damit war die Evolution der Botnetze aber noch nicht abgeschlossen. Nachdem sie mit verschiedenen Protokoll-Varianten experimentiert hatten, fokussierten sich die Botnetz-Entwickler auf die Architektur ihrer Netze. Es hatte sich gezeigt, dass klassische Botnetze, die aus vielen Rechnern und einer Steuerzentrale bestehen, überaus verwundbar sind. Sie sind von einem kritischen Knoten abhängig, nämlich dem Steuerungszentrum. Wird dieses ausgeschaltet, so ist im Prinzip das gesamte Netz verloren. Zwar werden auch hin und wieder Zombie-Netze eingesetzt, deren Computer mit verschiedenen Bots infiziert sind und von mehreren Steuerungszentren kontrolliert werden. Derartige Netze sind allerdings wesentlich schwieriger zu verwalten, da zwei bis drei Steuerungszentren gleichzeitig überwacht werden müssen.

Aus Sicht von IT-Sicherheitsexperten können sich Botnetze mit P2P-Architektur, die also ohne Kommandozentrale auskommen, als äußerst effektiv und gefährlich erweisen. Um ein solches Netz zu steuern, müssen deren Betreiber nur einem einzigen Rechner einen Befehl erteilen. Prinzipiell kann sich jeder infizierte Computer mit jedem anderen Computer innerhalb des Zombie-Netzes verbinden. Während Hacker mit diesen Botnet-

zen schon recht lange experimentieren, erschien der erste P2P-Verbund erst im vergangenen Jahr. Auf diese Art der Zombie-Netze richten IT-Sicherheitsexperten nun hauptsächlich ihre Aufmerksamkeit.

P2P-Botnetze: „Sturm-Botnetz“

Im Jahr 2007 wurden IT-Sicherheitsexperten von einem P2P-Botnetz auf Trab gehalten, das Hacker mit Hilfe eines Schädlings namens StormWorm errichteten. Nach der massiven Verbreitung dieses Sturmwurms zu urteilen, verfügten dessen Autoren offensichtlich über eine ganze „Fabrik“ zur Entwicklung neuer Versionen. Seit Januar 2007 treffen bei Kaspersky Lab täglich drei bis fünf neue Varianten des Sturmwurms ein, der als Email-Worm.Win32.Zhelatin klassifiziert wird.

Nach Ansicht von Fachleuten handelt es sich bei dem Sturmwurm um ein neuartiges Schadprogramm zum Aufbau von Zombie-Netzen. Die folgenden Merkmale belegen, dass dieser Bot von Profis entwickelt und verbreitet wird, die außerdem die Architektur sowie den Schutz ihres Zombie-Netzes genau durchdacht haben:

- ▶ Der Code des Bots mutiert ähnlich wie bei einem polymorphen Virus, ist jedoch nicht Bestandteil des Programms, sondern liegt auf einem speziellen Webserver. Dieser Mechanismus wird als „Server-Polymorphismus“ (server-side-polymorphism) bezeichnet.
- ▶ Die Mutationen treten mit einer hohen Frequenz auf und geschehen teilweise im Stundenrhythmus. Das geschieht jedoch serverseitig und macht damit die Updates der Antiviren-Datenbanken für viele Anwender nutzlos.
- ▶ Das Sturm-Botnetz schützt sich vor allzu neugierigen Blicken. Viele Antiviren-Hersteller laden in regelmäßigen Abständen neue Exemplare des Wurms von den Servern herunter, über die das Schadprogramm verbreitet wird. Geschieht das von einer Adresse aus auffallend häufig, erhalten die Bots den Befehl, diese per DDoS-Attacke anzugreifen.
- ▶ Das Bot-Programm verhält sich im System möglichst unauffällig. Aggressiv agierende Programme werden relativ schnell von Anwendern und Administratoren entdeckt. Daher sind Schädlinge, die ihre Aktivität zu verbergen wissen und sich dabei keiner wesentlichen Computerressourcen bedienen, besser vor Entdeckung geschützt.
- ▶ Der Sturmwurm kommuniziert nicht mit einem zentralen Server, sondern verbindet sich lediglich mit einigen „benachbarten“ Computern, die ebenfalls infiziert sind. Daher ist es praktisch unmöglich, sämtliche zum P2P-Netz gehörende Zombies zu identifizieren. Zu demselben Zweck können auch Aufklärungsgruppen gebildet werden. Jedes ihrer Mitglieder kennt dabei nur einige andere Teilnehmer, so dass bei Enttarnung eines einzelnen Agenten nicht die gesamte Gruppe auffliegt.

► Die Autoren des Wurms greifen ständig zu neuen Verbreitungsmethoden. Anfangs wurde das Schadprogramm meist in Form einer PDF-Datei an Spam-Mitteilungen angehängt. Nachfolgender Werbemüll enthielt Links auf infizierte Files. Die Malware-Autoren versuchten außerdem, automatisch Blogbeiträge zu versenden, die Links auf infizierte Websites enthalten. Alle aufgeführten Verbreitungsmethoden wurden immer auch von raffinierten Social-Engineering-Techniken begleitet.

Das Sturm-Botnetz brachte eine Menge Probleme mit sich. Neben massenhaften Versand von Spam steht es im Verdacht, an verschiedenen groß angelegten DDoS-Attacken beteiligt gewesen zu sein. Nach Ansicht einiger Experten fällt darunter auch die Cyberattacke auf Estland im Jahr 2007. Die Einsatzszenarien eines solchen Zombie-Netzes lassen bei Providern und Internet-Hosts schlimme Befürchtungen aufkommen. Diese werden insbesondere dadurch verstärkt, dass der tatsächliche Umfang des Sturm-Botnetzes völlig unbekannt ist. Während sich andere auf einer Kommandozentrale basierende Zombie-Netze ohne weiteres sichtbar machen lassen, hat kein IT-Sicherheitsexperte jemals alle an das Sturmnetz angeschlossenen Rechner zu Gesicht bekommen. Unterschiedlichen Schätzungen zufolge umfasst das Sturmwurm-Botnetz zwischen 50.000 und 10 Millionen Zombie-Computer.

Gegen Ende des Jahres 2007 schien das Sturm-Botnetz zu schrumpfen, obwohl Kaspersky Lab nach wie vor täglich mehrere neue Versionen des Bots erhielt. Einige Fachleute meinen, dass das Zombie-Netz häppchenweise verkauft wurde. Andere vermuten, dass es sich als unrentabel erwiesen hat und der erzielte Gewinn die Kosten für Entwicklung und Unterhalt nicht deckte.

P2P-Botnetze: Mayday

Ein anderes nach Ansicht von Kaspersky Lab interessantes Botnetz ist „Mayday“, weil es sich bezüglich seiner technischen Umsetzung von seinen Vorgängern unterscheidet. Als Namensgeber fungiert die Domain, mit der eines der Malware-Exemplare kommunizierte. Kaspersky Lab führt Mayday in seiner Datenbank unter Backdoor.Win32.Mayday.

Mayday bedient sich ebenso wie der Sturmwurm der P2P-Architektur. Nachdem Mayday einen Rechner infiziert hat, meldet er sich bei einem im Programmcode festgelegten Webserver, schreibt sich in dessen Datenbank und erhält daraufhin eine Liste aller anderen Zombie-PCs. Beim Sturm-Botnetzes wurde nur ein Teil dieser Liste übermittelt. Anschließend stellt Mayday eine Verbindung zu anderen Bots innerhalb des Zombie-Netzes her.

Während der Aufbauphase des Botnetzes registrierte Kaspersky Lab in Großbritannien, den USA, den Nie-

derlanden und Deutschland sechs verschiedene Server, mit denen die Bots in Kontakt traten. Anfang März war nur noch einer dieser Server in Betrieb, der ungefähr 3.000 Bots steuerte. An dieser Stelle sei daran erinnert, dass das Sturm-Botnetz vorsichtigen Schätzungen zufolge mehrere zehntausend infizierte Rechner umfasst. Neben der Größe bleibt das Mayday-Botnetz auch in anderen wichtigen Bereichen hinter seinem älteren Bruder zurück: Das Mayday-Botnetz verwendet zum einen ein primitives und unverschlüsseltes Kommunikationsprotokoll. Zum anderen enthält der Code des Schadprogramms keine Funktionen, die eine Analyse durch Antiviren-Software erschweren. Das wichtigste Kriterium: Im Gegensatz zum Sturmwurm erscheinen weitaus weniger neue Varianten des Mayday-Bots. Das Programm Backdoor.Win32.Mayday wurde bereits Ende November 2007 erstmals von Kaspersky Lab erfasst und innerhalb der nächsten vier Monate kamen nur gut 20 verschiedene Programmvarianten hinzu.

Aus technischer Sicht sind zwei ungewöhnliche Mayday-Techniken erwähnenswert.

Die P2P-Kommunikation läuft in diesem Zombie-Netz über ICMP-Mitteilungen (Internet Control Message Protocol) mit einer Payload von 32 Byte. Die meisten Nutzer kennen ICMP im Zusammenhang mit dem Kommandozeilentool Ping. Das Protokoll bedient sich dessen Funktionen, um die Erreichbarkeit eines Netzhosts zu überprüfen, kann allerdings noch weitaus mehr. In Netzwerken dient das Internet Control Message Protocol zum Austausch von Informations- und Fehlermeldungen über das Internet-Protokoll (IP).

Die folgende Abbildung zeigt die Oberfläche eines Paketsniffer-Programms, das die Übertragung von ICMP-Paketen durch den Mayday-Bot aufgezeichnet hat. Bis dato war Kaspersky Lab kein Bot bekannt, welches das ICMP zum Datentransfer nutzt.

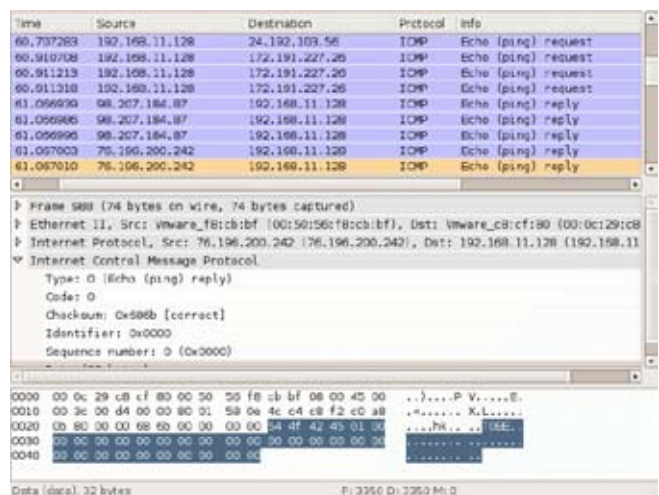


Abb. 3: Vom Mayday-Bot versendete ICMP-Pakete

Mit Hilfe des ICMP identifiziert Mayday infizierte Rechner und prüft, ob sie im Netzwerk erreichbar sind. Weil der Bot auf Windows XP SP2 zugeschnitten ist, ändert er nach Programmstart die Firewall-Regeln so, dass ICMP-Pakete zugelassen werden.

Die zweite und wichtigere technische Auffälligkeit des Mayday-Botnetzes hat mit dem Aufbau seines Steuerungszentrums zu tun.

Das Botnetz greift für sein web-orientiertes Steuerungszentrum auf das CGI zurück (Common Gateway Interface). Damit wird der Datenaustausch zwischen einem Webserver und anderer Software dynamisch gesteuert. Mit CGI-Anwendungen lassen sich Webseiten deshalb interaktiv gestalten. Ein CGI-Skript geht ebenso vor, benötigt für die Darstellung allerdings einen Interpreter. In der Regel verwenden Cyberkriminelle solche Skript-Engines, um Kommandozentralen für web-orientierte Botnetze zu entwickeln.

Mit Hilfe der zuständigen Behörden gelangte Kaspersky Lab in den Besitz eines Programms, das im Kommandozentrum des Mayday-Botnetzes eingesetzt wird. Die Server-Software von Mayday besteht aus einer 1,2 MByte großen ausführbaren ELF-Datei, die ohne Module und damit auch ohne Skript-Engine auskommt. ELF-Files sind das Linux-Gegenstück zu den EXE-Dateien der Windows-Welt. Auf den ersten Blick scheint es nichts besonderes zu sein, dass die Autoren von Mayday eine CGI-Anwendung anstatt eines CGI-Skripts entwickelt haben. Trotzdem wirft diese Entscheidung eine Reihe von Fragen auf.

Eine CGI-Anwendung zu entwickeln ist in mancher Hinsicht komplizierter als die Programmierung eines CGI-Skripts, da sie besondere Anforderungen an stabilen und zuverlässigen Code stellt. Derzeit basieren 99 Prozent aller Web-Entwicklungen auf Skript-Engines. Monolithische ausführbare CGI-Programme werden nur dann entwickelt, wenn es dringend erforderlich ist, alles bis ins kleinste Detail zu optimieren. Meistens setzen nur große Firmen diese Methode bei Anwendungen ein, die auch unter enormer Belastung einwandfrei funktionieren müssen. CGI-Programme werden beispielsweise in den Websystemen von eBay, Paypal und Yahoo verwendet.

Zu welchem Zweck wurde also für das Mayday-Botnetz eine ausführbare CGI-Datei ohne Module entwickelt? Die Entwickler wollten es möglicherweise Dritten erschweren, die Steuerzentrale zu verändern oder weiterzuverkaufen. Eine Strukturanalyse der Server-Software zeigt, dass der Code akkurat und das Klassensystem universell umgesetzt wurden. Das lässt den Schluss zu, dass hinter dieser hochkomplexen Entwicklung ein gut organisiertes Spezialistenteam steckt. Zudem mussten die Cyberkriminellen ihr Mayday-Botnetz vermutlich für Windows- und für Linux-Rechner gleichzeitig entwickeln.

Im Frühjahr 2008 registrierte Kaspersky Lab nicht eine einzige neue Version des Mayday-Bots. Vielleicht haben sich die Autoren dieses Schadprogramms nur eine Auszeit genommen und das Mayday-Botnetz tritt in nächster Zukunft erneut in Erscheinung.

Geschäfte mit Botnetzen

Botnetze sind und bleiben ein Problem, nicht zuletzt weil ihre Entwicklung immer weiter vorangetrieben wird. Mittlerweile hat sich dafür ein kompletter illegaler Markt gebildet. Cyberkriminelle, die Botnetze zu ihren Zwecken einsetzen wollen, benötigen heute weder spezielle Kenntnisse noch größeres Eigenkapital. Für Interessenten gibt es Komplettangebote zu moderaten Preisen. Darin enthalten sind Software, komplette eingerichtete Netze und anonyme Hosting-Services.

Ein Blick auf die „dunklen“ Seiten des Internets zeigt, wie die Botnetz-Industrie funktioniert und wie sie die Betreiber von Zombie-Netzen betreut.

Die erste Voraussetzung für den Aufbau eines Botnetzes ist der Bot selbst. Dabei handelt es sich um ein Programm, das ohne Wissen des Anwenders auf dessen Computer verschiedene Aktionen ausführt. Die für den Aufbau eines Botnetzes notwendige Software gibt es im Internet. Man muss die entsprechenden Angebote lediglich finden und sich dann an die Inserenten wenden.

Product # 1

Do not trust anonymity of cheap services? Built up your own! Bot + adminpanel kit will help you in this. Features:

- opens socks4/socks5/http/https proxy on the computer
- non-standard ports

installs deeply into the system

- bypass most firewalls
- not detected by most antivirus

Admin Panel: (also see picture)

Sign-based sessions

- display speed of proxy-server
- autodisable bots with no external IP
- mapping of the country (geo2ip base 28 mb)

text reports:

- total number of bots
- strict design of admin panel

Periodic updates, friendly (and most importantly - permanent) Support.
 Cost - 400 WMZ.
 Demo version for review upon request.

Abb. 4: Angebot zum Verkauf eines Bots und Steuerungspanels (Übersetzung aus dem Russischen)

Die Preise für Bots liegen zwischen fünf und 1.000 US-Dollar, je nachdem wie verbreitet der Schädling ist, ob Antiviren-Programme ihn erkennen und welche Befehle er unterstützt.

Für den Aufbau eines simplen web-orientierten Zombie-Netzes braucht es zunächst Hosting-Speicherplatz für die Steuerzentrale. Jeder Interessent kann Webpace

inklusive Support mieten und erhält damit die Möglichkeit, den Server anonym zu nutzen. Üblicherweise garantiert der Hostler, dass selbst die Behörden nicht auf die Journaldateien zugreifen können. Im Internet kursieren zahlreiche Angebote wie das Folgende.



Abb. 5: Offerte für Hosting-Services zum Aufbau eines Botnetzes

Ist das C&C eingerichtet, fehlen nur noch die infizierten Computer. Interessenten können sich aber gleich mit einem fertig eingerichteten Netz samt fremden Bots eindecken. Da der Diebstahl von Botnetzen im Cyberkriminellen-Milieu keine Seltenheit ist, tauschen Käufer normalerweise sowohl das Schadprogramm als auch die Steuerzentrale aus und erhalten so die vollständige Kontrolle über das Zombie-Netz. Dabei weisen Cyberkriminelle den Bot im gekauften Netz an, einen neuen Bot mit der geänderten Adresse des C&C zu starten und sich anschließend selbst zu löschen. Eine solche „Revision“ eines Botnetzes ist auch in punkto Sicherheit und Anonymität durchaus sinnvoll. Die früheren Versionen des C&C und des Bots könnten bereits vor ihrem Verkauf ins Visier von IT-Sicherheitsexperten geraten sein.

Leider erfordert der Aufbau eines eigenen Botnetzes auch keine allzu großen Anstrengungen, denn die dafür notwendigen Mittel sind ebenso im Internet erhältlich. Die bekanntesten dieser Programmpakete heißen Mpack, Icepack und WebAttacker. Durch Ausnutzen von Sicherheitslücken in der Browsersoftware oder entsprechenden Plugins können diese so genannten ExploitPacks Computersysteme beim Besuch verseuchter Websites infizieren.

Durch die Sicherheitslücke lädt der Browser eine ausführbare Datei auf den Computer des Anwenders und startet sie. Bei dieser Datei handelt es sich um das Bot-Programm, das den neuen Zombie-Computer nun an das Botnetz anschließt und dem Cyberkriminellen die Kontrolle überlässt.

Selbst Jugendliche können sich im Internet problemlos solche Hacker-Tools besorgen und versuchen, an deren Weiterverkauf zu verdienen.



Abb. 6: Ein 16jähriger verkauft MPack

Das ExploitPack wurde ursprünglich von russischen Hackern entwickelt, fand aber bald Interessenten in anderen Ländern. Die entsprechenden Schadprogramme tauchten zum Beispiel in China auf, wo sie nun aktiv eingesetzt werden. Das belegt den kommerziellen Erfolg des ExploitPack auf dem Schwarzmarkt.



Abb. 7: Russische Originalversion und lokalisierte chinesische Version von IcePack

Je einfacher sich ein derartiges System bedienen lässt, desto erfolgreicher und populärer ist es im Cyberkriminellen-Milieu. Um die Beliebtheit und die Nachfrage dieser Machwerke zu steigern, entwickeln ihre Programmierer simple Installations- und Konfigurations-Mechanismen bis hin zu Systemen für das C&C.

Zur Installation eines Kommandozeentrums müssen in der Regel lediglich Dateien auf den Webserver kopiert und das Skript install.php im Browser aufgerufen werden. Die Setup-Prozedur wird durch das Web-Interface des Installationsprogramms noch weiter vereinfacht: Die Cyberkriminellen müssen nur die Felder im Web-Formular korrekt ausfüllen, um das Kommandozentrum richtig zu konfigurieren und einsatzbereit zu machen.

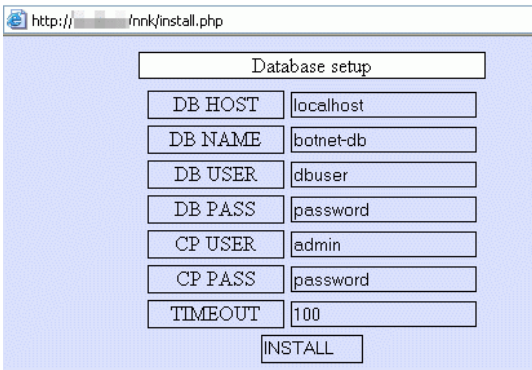


Abb. 8: Web-Installation für ein C&C

Den Cyberkriminellen ist durchaus bewusst, dass ein Bot-Programm früher oder später von Antiviren-Produkten erkannt wird. Solche Rechner sind dann nicht nur für die Kriminellen verloren. Auch das Infektions-Tempo für neue Computer verlangsamt sich merklich. Die Cyberkriminellen versuchen daher, ihre Botnetze mit verschiedenen Methoden zu schützen. Besonders effektiv sind dabei Modifikationen, die ausführbaren Code verschlüsseln, verpacken oder verstecken. Auf dem Cyber-Schwarzmarkt gibt es die dafür passenden Tools.



Abb. 9: Ein Angebot für ein Tool, das Programme vor AV-Produkten versteckt

Alles, was man für den erfolgreichen Einsatz und die Entwicklung von Botnetzen braucht, ist also im Internet zu haben. Bisher gibt es keine Möglichkeit, die Botnetz-Industrie aufzuhalten.

Fazit

Gegenwärtig gehören Botnetze zu den wichtigsten illegalen Einnahmequellen im Internet und sind in den Händen von Kriminellen eine gefährliche Waffe. Man kann daher kaum davon ausgehen, dass letztere freiwillig auf ein derart effektives Instrument verzichten werden. IT-Sicherheitsexperten erwarten, dass sich die Botnetz-Technologie künftig noch weiterentwickeln wird.

Botnetze sind besonders deswegen so gefährlich, da sie sich immer einfacher steuern lassen und selbst Laien schon bald damit umgehen können. Statt spezieller Kenntnisse braucht es nur noch die entsprechenden finanziellen Mittel. Zudem sind die Preise auf dem gut organisierten Botnetz-Markt überaus moderat.

Nicht nur Cyberkriminelle könnten an dem Aufbau internationaler Botnetze interessiert sein, sondern auch Staaten, die Zombie-Netze als politisches Druckmittel und Waffe gegen andere Staaten einzusetzen bereit sind. Da sich infizierte Computer unabhängig von ihrem geografischen Standort anonym steuern lassen, kann man mit ihrer Hilfe einen Cyberkrieg provozieren. Dazu muss lediglich ein Angriff auf die Server eines Landes von Computern des anderen Landes aus organisiert werden.

In Bot-Netzwerken, die etliche tausend, mehrere hunderttausend oder zum Teil Millionen von infizierten Computern umfassen, liegt ein äußerst gefährliches Potential, das bisher glücklicherweise noch nicht voll ausgeschöpft wird. Dabei stützt sich diese geballte Cyber-Macht mehrheitlich auf infizierte Privat-Computer, die von den Kriminellen zu ihren Zwecken ausgenutzt werden.

Stellt man sich nun zehn Freunde und Bekannte vor, die einen Computer besitzen, so hat sehr wahrscheinlich einer von ihnen einen Zombie-Rechner zu Hause stehen. Und wer weiß, vielleicht sind ausgerechnet Sie es?

Vitaly Kamluk
Senior Virus Analyst, Kaspersky Lab

Kaspersky Lab

Kaspersky Lab reagiert im weltweiten Vergleich von Antivirus-Herstellern meist am schnellsten auf IT-Sicherheitsbedrohungen wie Viren, Spyware, Crime-ware, Hacker, Phishing-Attacken und Spam.

Die Produkte des global agierenden Unternehmens mit Hauptsitz in Moskau haben sich sowohl bei Endkunden als auch bei KMUs, Großunternehmen und im mobilen Umfeld durch ihre erstklassigen Erkennungsraten und minimalen Reaktionszeiten einen Namen gemacht.

Neben den Stand-Alone-Lösungen des Security-Experten ist Kaspersky-Technologie Bestandteil vieler Produkte und Dienstleistungen führender IT-Sicherheitsunternehmen.

Kontakt

Kaspersky Labs GmbH
Steinheilstr. 13
85053 Ingolstadt

Telefon: +49 (0)841 981 89 0
Telefax: +49 (0)841 981 89 100

info@kaspersky.de
www.kaspersky.de