Gegenwart und Zukunft des Spam

Ich werde zunächst kurz auf aktuelle Entwicklungen im Bereich EMail-Spam eingehen und dann zu den bereits absehbaren Entwicklungen übergehen. Zum derzeitigen Zeitpunkt muß man leider sagen, das der Kampf der Anti-Spam und IT-Security Firmen bei weitem nicht geschlagen ist und wir mit Spam auch in Zukunft rechnen müssen.

von Dr. Alexander Seewald

Spam wird zur Zeit nicht mehr durch eigene Rechner der Spammer wie früher, sondern durch gekapterte Rechner unschuldiger Internet-Benutzer - so wie Sie und ich - gesendet. Diese umfunktionierten Rechner nennt man Bots, was sich von Softbots (Software Robots) ableitet. Man kann mehr oder weniger unschuldig zu so etwas kommen, zum Beispiel, wenn man sein Betriebssystem nicht regelmäßig updated und ein Wurm (= Software, die sich von selbst verbreitet - im Gegensatz zum Virus, der zunächst auf den Benutzer angewiesen ist) eine bekannte Schwachstelle ausnützt. Oder man klickt auf eine scheinbar harmlose Mail, oder man surft im Internet an einer entsprechend präparierten Seite vorbei, oder, oder ... die Möglichkeiten, sich so etwas einzufangen, sind inzwischen endlos. Abhilfe schafft nur ein regelmäßig - am besten automatisch - upgedatetes Betriebssystem und eine aktuelle, ebenfalls regelmäßig upgedatete Sicherheitssuite.

Um ein Gefühl dafür zu geben, wie groß dieses Problem ist: das FBI, welches im Juni die Kampagne OPERATION BOT ROAST gestartet hat, schätzt mindestens eine Million potentielle Opfer (d.h. gekapterte Rechner) weltweit. Hierbei wurden allerdings nur die langfristig aktiven Botnetze gezählt, was das Problem deutlich unterschätzt.

Bots sind in riesigen Netzwerken zusammengefaßt und arbeiten gemeinsam. Ein Kommando an das Botnetz wird damit parallel von bis zu 100.000 Rechnern ausgeführt. Damit können zum Senden von Spam die gemeinsame Internet-Bandbreite aller dieser Rechner verwendet werden. Zwei Drittel aller Botnetze sind weniger als einen Tag aktiv - sie werden aufgebaut, getestet, verwendet, und dann wieder abgebaut, um Spuren zu verwischen. Tausende solcher Botnetze werden jeden Tag auf- und abgebaut. Ein typischer verletzlicher Rechner wird deshalb zu verschiedenen Zeitpunkten unterschiedliche Aufgaben innerhalb verschiedener Botnetze wahrnehmen - sogar Mehrfachinfektionen sind möglich, womit ein gewiefter Botnetz-Betreiber das Botnetz eines Konkurrenten übernehmen kann.

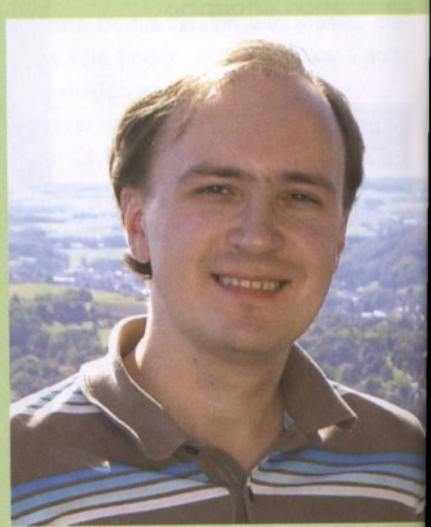
Die hierbei verwendete Bot-Software kommt in verschiedenen Varianten (Agobot, SDBot, GT-Bots, Kaiten...) und hat vielseitige Features, wie Nachladen von neuen Versionen, Verstecken vor dem Betriebssystem und Virenscannern über rootkits, Wurm-Funktionalität zur autonomen Vermehrung, Backdoor-Funktionalität um Zugriff auf den gekaperten Rechner von außen zu ermöglichen und Spyware zum Ausspionieren von Passwörtern und Kreditkartennummern. Die meisten Bots verhalten sich passiv und warten auf Befehle vom „Botherder" (Bot-Hirte). Die häufigste Verwendung ist noch immer die zum Versenden von Spam, aber es gibt auch andere, wie wir später sehen werden.

> „ ...die Möglichkeiten, sich etwas einzufangen, sind inzwischen endlos... „

Beim Versenden von Spams haben die Spammer inzwischen diversifiziert und sich damit neue illegale Einkommensquellen erschlossen. Es gibt derzeit verschiedenste Gruppen von Spam. Die einfachste ist diejenige, welche ein Produkt verkaufen will (Viagra ist da wohl das häufigste). Das ist also eine Marketing-Aktion, die direkt oder indirekt über die Anbieter solcher Produkte bezahlt wird, und ist als solche - mit mehr oder weniger Aufwand - grundsätzlich zum Auftraggeber zurückverfolgbar.

Deshalb gibt es jetzt auch andere Arten von Spam ohne expliziten Auftraggeber, mit denen sich die Spammer unabhängig finanzieren können. Ein wachsender Anteil sind Spams, die einem eine „günstige" Aktie ans Herz legen und so die Aktienkurse beeinflussen wollen (sog. pump-and-dump Spams). Hierbei spekuliert der Spammer entweder auf einen leichten Anstieg kurz nach der Aussendung - oder auf einen Abstieg der Aktie, sobald die gutgläubigen Opfer sehen, daß damit kein Gewinn zu machen ist. Hier ein etwas plumpes aktuelles Beispiel. Man sieht aber, das aktuelle Themen relativ kurzfristig aufgegriffen werden (zB junger Eisbär Knut), und es werden sehr billige Aktien (sog. penny-stocks) verwendet. Diese spezifische Aktie hat seit Mitte 2007 massiv an Wert verloren und ist dadurch wahrscheinlich erst für die Spammer interessant geworden.

zum Autor:



Dr. Alexander K. Seewald ist seit mehreren Jahren in der Spam-Forschung tätig und hat u.a. Spamfiltersysteme für das Österreichische Forschungsinstitut für Artificial Intelligence entwickelt. Seit 2000 in der Forschung, war er sowohl an Forschungsinstituten im Bereich Grundlagen- und angewandter Forschung (Maschinelles Lernen und Data Mining), als auch in der Privatwirtschaft (Bankensektor und IT-Security) tätig. Seit Juni 2007 ist er unabhängiger Forscher und teilt seine Arbeitszeit zwischen seinen vielseitigen Forschungsinteressen und rein kommerziellen Projekten auf. In Kürze startet das von netIdee.at geförderte Forschungsprojekt „Frühwarnsystem für Botnetze", welches er in Kooperation mit Prof. Gansterer, Universität Wien durchführen wird.

Ich moechte Sie begruessen, ich heisse Doktor DIEDRICH.

Hiermit moechte ich Sie ueber den Erfolg einer Netzverkaufsgesellschaft informieren. Verschiedene Waren werden ueber Internet verkauft und die Verkaufsvolumen steigen vom Jahr zu Jahr das ist schon nicht merkwuerdig.

Ueber das Internet sind die Waren billiger, es ist bequemer sie zu bestellen, fast jedes Netz-Geschaeft bittet Lieferung und Rabatte an. Eines der besten Beispiele vom Internet-Geschaeft ist die Firma Tier-spezi AG (ISIN: CH0027339107,WKN: A0LB1T).

Dieses Unternehmen verkauft Waren fuer unsere Lieblinge . Dieses Unternehmen hat eigenes Geschaeftenetz und eigene Produktionslinien, am besten laeuft das Geschaeft ueber das Internet .

Die Kapitalisierung und der Verkaufswuchs der Firma ist unbeschreiblich, nur in zweijaehriger Taetigkeit ist es dem Unternehmen gelungen, auf den offenen Markt aufzutreten und eigene Aktien den Privatunternehmern anzubieten. Im Zusammenhang mit der Geschichte des Eisbaeren Knut hat sich die Denkensweise der Menschen veraendert, man nimmt obdachlose Huende und Katzen. Die Verkaufsvolumen der Tierspesi AG sind unwahrscheinlich gestiegen. Deswegen braucht die Firma neue Investitionen fuer die Produktionserweiterung.

Pruefen Sie die Marktdaten des Tier-spezi AG (Zeichen: TS1,ISIN: CH0027339107,WKN: A0LB1T)

Das ist eine wunderbare Chance fuer das weitere Wachstum der Gesellschaft!

Phinshing

Aber dort ist noch nicht Schluß. Der wohl komplexeste aktuelle Trick ist Phishing. Hierbei wird eine legitim aussehende Spam-Mail geschickt, die einen dazu einlädt, seine Telebanking-Zugangsdaten (PIN & TANs) zu „überprüfen" - meist aus Sicherheitsgründen. Man wird über einen Link in der Mail auf eine gefälschte Seite gelockt, die täuschend echt aussieht, und schon hat der Spammer die Zugangsdaten. Das allein reicht noch nicht, denn Banktransfers können ja gut verfolgt werden. Also gibt es eine zweite Gruppe von Spam-Mails, die lukrative Nebenjobs anbieten. Man soll täglich ein paar Stunden am Internet sitzen und Geld von A nach B überweisen, und kriegt dafür ein paar Prozent Provision. Das Geld wird so über die naiven Mittelsmänner gewaschen - das verzögert die Verfolgung ein paar Stunden - und in der Zwischenzeit irgendwo auf der Welt in bar abgehoben. Die Mittelsmänner werden erwischt und hart bestraft - der Großteil des Geldes ist dann aber natürlich schon weg. Ein bombensicheres Geschäft für den Spammer, ein großes Ärgernis für Opfer und Mittelsmänner, und eine große weltweite Herausforderung für den Bankensektor.

Unabhängig davon werden Spams auch der Form nach tendenziell schwieriger zu filtern. Ein etwa ein Jahr altes Konzept, welches laufend weiter entwickelt wird, sind Image-Spams: der Spam-Inhalt ist nur im Bild, der Text dazu ist aus irgendeiner zufällig gewählten Quelle, die einer legitimen Mail möglichst ähnlich ist.

Die erste klassische Epoche wird repräsentiert durch die schon erwähnte grosse Anthologie Manyoshu („Sammlung der Myriaden Blätter"), die vermutlich durch den Sammeleifer des Dichters um so eine möglichst grosse Reichhaltigkeit an Klängen zu erzielen. Die Regeln des Tanka wurden schon 700 Jahre vor unserer Zeitrechnung durch Sosano-Ono-Mikoto, einen Dichter des heroischen Zeitalters,

Die einzelnen Persönlichkeiten treten in dieser lyrischen Kunst nicht stark hervor, im Gegensatz zur chinesischen. Japan ist das Land der Gelegenheitsdichter. Wir besitzen Gedichte von Kaisern und Kaiserinnen,

so habe ich, obwohl ein Freund konzentrierten Ausdrucks, erst in zweiter Linie auf Knappheit der Form gehalten und vor allem der Klarheit und Durchsichtigkeit mich befleissigt. Hätte ich überall die Knappheit

Dieser Text ist aus einem Buch von Projekt Gutenberg.net, „Japanischer Frühling - Nachdichtungen Japanischer Lyrik" (Hans Bethge), verstümmelt und rearrangiert aus dem Geleitwort. Warum ist das ein Problem? Praktisch alle erfolgreichen kommerziellen und Open Source Spamfilter verlassen sich zum Großteil auf lernende Naive-Bayes Filter. Diese verstehen allerdings nur den Text einer EMail. Zum Glück digitalisiert das Projekt Gutenberg.net aus Copyrightgründen hauptsächlich Texte, die älter als 70 Jahre sind und dadurch ist dieser Text von einem typischen EMail-Text noch relativ leicht zu unterscheiden. Allerdings werden die Spammer eines Tages Sammlungen von genügend vielen legitimen deutschsprachigen Mails haben, sodaß man über kurz oder lang die eingebetteten Bilder ebenfalls analysieren muß. Das ist zwar technisch möglich, aber viel aufwendiger als die Analyse des Textes, und würde den Aufwand für das Aussortierung von Spams schlagartig erhöhen.

Bank Austria Creditanstalt

Member of UniCredit Group

Neue Schutzmassnahmen der Bank Austria Creditanstalt!
Für alle Bank Austria Creditanstalt Kunden

Sehr geehrte Nutzer der Bank Austria Creditanstalt Online-Bankings,
wir freuen uns Ihnen neue Informationen über die Sicherheit im Internet erteilen zu dürfen. Bitte lesen sie es aufmerksam!

Weltweit gilt das Online-Banking durch nummeriertes TAN Verfahren als eines der sichersten Legitimations-Verfahren für Online-Bankgeschafte. Dennoch gab es in letzter Zeit immer wieder Versuche, auf betrugerische Art und Weise das Geld von Bank Austria Creditanstalt Kunden ins Ausland zu überweisen.

Leider ist uns momentan das Verfahren, dass die Betrüger benutzen, nicht bekannt.

Um unsere Kunden von Betrüger zu schützen, hat unser Sicherheitsteam für neue Schutzmassnahmen entschieden. Beachten sie bitte, dass die Einsetzung dieser Schutzmassnahmen erforderlich für alle Bank Austria Creditanstalt Kunden ist!

Um diese Massnahmen einführen zu können, müssen sie 20 TANs aus ihrer aktuellen Tan-Liste eingeben.

Folgen sie bitte diesen Link, um Ihr Konto bei der Bank Austria Creditanstalt zu authentifizieren —
https://www.ba-ca.com/security/html/bankid.html

Achtung! Wir bitten unsere Kunden um Verständnis fur diese Überprufung. Alle Bank Austria Creditanstalt Konten die nicht innerhalb eines Tages authentifiziert werden, werden gesperrt!

Bots

Bots werden aber nicht nur zum Versenden von Spams verwendet. Man kann damit auch unliebsame Konkurrenz ausschalten, indem man ihr Netzwerk lahmlegt (über sog. Distributed-Denial-of-Service Attacken); Information über den Benutzer des Rechners sammeln (Passworte, Kreditkartennummern, Name, eBay-Zugangsdaten, ...); sich über bekannte Schwachstellen weiterverbreiten und somit das Botnetz vergrößern; Google AdSense und andere Online-Werbungssysteme über die Simulation von Klicks durch das Botnetz manipulieren (Adware); Passwörter brute-force knacken - selbst ein durchschnittliches Botnetz hat schon die Rechenkapazität eines Supercomputers - und das Abhören des lokalen Netzwerks, wo noch immer viele Passwörter ohne Verschlüsselung gesendet werden. Und das sind nur die bekannten Verwendungen von Botnets! Auch für diese Aktivitäten gibt es einen lukrativen Schwarzmarkt, der den Spammern eine weitere illegale Einkommensquelle beschert.

Weitere wichtige Werkzeuge im Kampf gegen Botnetze sind Honeypots. Das sind Rechner, die scheinbar Schwachstellen aufweisen und somit von anderen Bots oder Wurm-Software angegriffen werden, tatsächlich aber diese böse Software (Malware, zB Bot-Software, Wurm-Software, Viren) nur sammeln. Automatische Analysewerkzeuge (sog. Sandboxes, zB Norman Sandbox) lassen die Malware in einer virtuellen Umgebung ablaufen und analysieren damit automatisch deren Verhalten.

Distributed-Denial-of-Service (DDoS) Attacken waren bis vor kurzem am populärsten, zB das bezahlte Ausschalten der Webseite eines Konkurrenten oder von mißliebigen Anti-Spam und Anti-Virusfirmen. Die Anti-Spam Firma BlueFrog ist durch solche Attacken in den Konkurs getrieben worden. Früher ist man davon ausgegangen, das die Hälfte der Botnetze für solche Attacken verwendet wird. Derzeit ist der Trend zu DDoS allerdings rückläufig. Man führt das darauf zurück, das solche Attacken durch die große Anzahl versendeter Pakete die Auffindung des Botnetzes ermöglichen und damit eine Rückverfolgung zum Botherder erleichtern. Kurz gesagt, das Risiko für die Spammer ist derzeit zu hoch, was voraussichtlich den Preis für solche Attacken in die Höhe treiben wird. Wir werden also in Zukunft weniger, dafür wesentlich schwieriger zu bekämpfende und umfangreichere Attacken zu erwarten haben. Spezifisch angepaßte Bots, die nicht upgedated werden können und zeitgesteuert bereits lange vorher platziert werden - und dann auf einmal losschlagen - können in freier Wildbahn bereits beobachtet werden.

Aktuell hat sich auch die Kommunikation zwischen Bots über Internet Relay Chat (IRC) als zu unsicher für die Spammer herausgestellt, da das IRC-Protokoll zu leicht überwacht, rückverfolgt und gesperrt werden kann. Derzeit gibt es vermehrt Bots, die via HTTP oder sogar peer-to-peer (so wie Skype und eDonkey; zum Beispiel StormWorm & Nugache) kommunizieren, was wesentlich schwieriger zu überwachen und sperren ist. Honeypots werden erkannt und vermieden oder absichtlich mit falscher Malware beliefert. Auch Sandboxes werden zunehmend ausgehebelt - einerseits durch subtile Checks, mit denen ein Bot überprüfen kann, ob er in einer virtuellen Umgebung abläuft; andererseits durch zeitverzögerte Aktivierung, die eine automatische Analyse aus Zeitgründen nicht mehr sinnvoll ermöglicht.

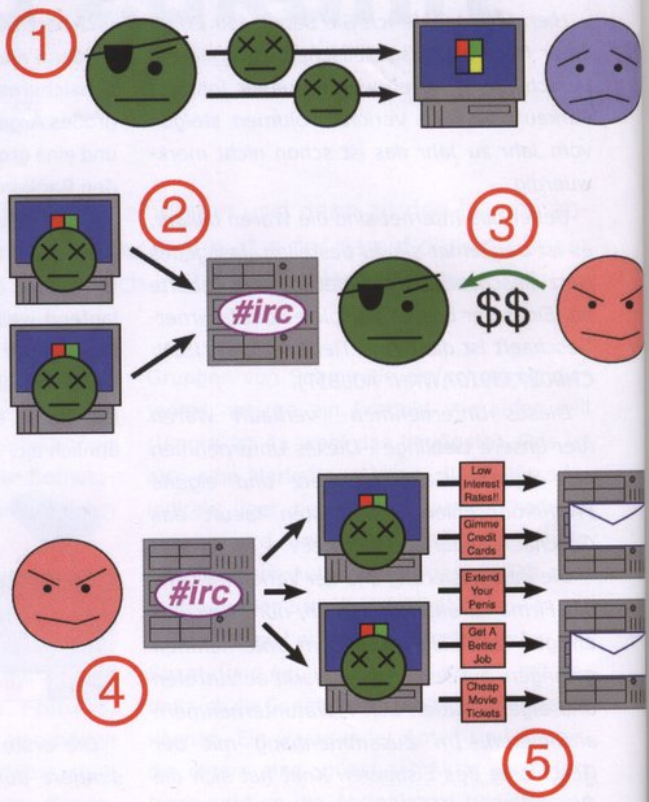
Die Bekämpfung von Spam ist aus Zeitgründen derzeit rein reaktiv: Spams und Malware werden gesammelt und dann erst spezifische Abwehrmaßnahmen entwickelt. Der größte Anteil der Malware wird nicht mehr von Menschen im Detail analysiert - man begnügt sich mit einer Signatur, um diese robust zu erkennen und beschäftigt sich mit deren Verhalten nur in Ausnahmefällen. Dadurch werden die neuen Funktionen von Bot-Software erst in der freien Wildbahn erkennbar. Obwohl es seitens der Spammer automatische Methoden zur Generierung von vielen Varianten von Bot-Software gibt - teilweise stündlich oder sogar minütlich neue Varianten - hält die automatische Analyse in vielen Bereichen damit nicht Schritt. Hier sind die Spammer leider einen wesentlichen Schritt voraus.

Die derzeitige Herausforderung ist es deshalb, von der reaktiven Vorgehensweise zur proaktiven überzugehen, und damit die Spammer einzuholen. Dies beinhaltet eine massive Verbesserung der automatischen Analyse von Botnetz-Aktivität und Malware-Analyse, und erfordert die Zusammenarbeit zwischen IT-Sicherheitsfirmen, Behörden, Internet Service Providern, den DNS Registries und den Betreibern der Netzwerk-Infrastruktur, um die Ergebnisse auch zeitlich kurzfristig einsetzen zu können, bevor die Spammer ihre Spuren verwischen können. Auf diesem Gebiet geschieht zur Zeit sehr viel - es bleibt aber noch genug zu tun, bevor man sich entspannen kann und das Spam-Problem für gelöst ansieht.

Was Sie persönlich gegen Botnetze machen können: Sorgen Sie für einen sicheren Rechner und installieren Sie immer die aktuellen Sicherheitsupdates. Installieren Sie eine Personal Firewall und ein aktuelles Virenschutz-Programm sowie einen guten Spamfilter. Und wenn Sie trotzdem etwas Verdächtiges an Ihrem Rechner bemerken, wenden Sie sich an einen Spezialisten. Damit arbeiten Sie mit daran, das Spam mittelfristig keine Zukunft mehr hat.

Weiterführende Hinweise und aktuelle Statistiken über Botnetze gibt es auf *http://www.shadowserver.org* und *http://www.spamhaus.org*. Auch im Rahmen des „Frühwarnsystem für Botnetze" Projektes wird es in Kürze eine Webseite geben, die unter *http://botnetz-tracker.seewald.at* zur Verfügung stehen wird.

Wie ein Botnet arbeitet



1. Ein botherder schickt Viren oder Wuermer aus, welche Rechner unschuldiger Computerbenutzer infizieren und dort seine Bot-Software installieren.
2. Der Bot auf dem infizierten PC loggt sich in einen bestimmten IRC oder Webserver (sog. Command-and-control (C&C) Server)
3. Ein Spammer kauft sich Zugriff auf das Botnetz vom Botherder.
4. Der Spammer sendet Instruktionen via C&C Server zu den infizierten PCs...
5. ...welche die Spam-Mails zu Mailservern verschicken.