SOPHOS

Sophos-Honeypot:

Wie man 5 Millionen Spam-E-Mails verschickt – ohne es zu merken

Botnetze geraten immer wieder in die Schlagzeilen. Das ist kein Wunder, denn diese auch als „Zombies“ betitelte Malware ist die Gelddruckmaschine Nummer eins der modernen Cybercrime-Welt. Die Idee dahinter ist einfach: die Malware auf den infizierten Rechnern verbindet sich regelmäßig mit ihrem Heimatserver. Sie tut das, indem sie harmlos scheinende Web Requests via HTTP versendet und sich wie ein ganz normaler Browser benimmt. Aber anstatt die Daten für eine Internetseite abzurufen, lädt der Bot, der Malware Roboter, neue Instruktionen für seine kriminellen Machenschaften und führt diese mit Hilfe des Rechners und des verbundenen Netzwerks aus.

Zu diesen Schandtaten gehören unter anderem:

- Erfassen der genutzten Eingabetasten, um Nutzernamen und Passwörter zu stehlen.
- Durchforsten der gespeicherten Dateien nach solchen, die zu Geld gemacht werden können.
- Animieren des Nutzers, bestimmte Werbung zu klicken, um Pay-per-Click-Umsätze zu generieren.
- Einstellen von „Empfehlungen“ für den Freundeskreis des Nutzers in Social-Media-Netzwerken.
- Download von noch mehr Malware, wie z.B. Ransomware, die Daten verschlüsselt und ein Lösegeld fordert.
- Nutzung des Rechners als Proxy, um diesen dann an andere Kriminelle zu vermieten oder Spuren zu verwischen.
- Attackieren anderer Webseiten, wobei es so scheint, dass der übernommene Rechner der Bösewicht ist.

Die mit Abstand am weitesten verbreitete Straftat in Verbindung mit Bots ist das Versenden von Spam-Nachrichten. Die Spammer aktivieren dazu nicht einfach nur einen Bot, vielmehr bauen sie ein ganzes Netz auf, das mehrere 10.000 und mehr Rechner kontrollieren kann. Diese Strategie bietet den Kriminellen einige entscheidende Vorteile:

Widerstandsfähigkeit. Aufgrund der Vernetzung gibt es keinen entscheidenden Schwachpunkt im System. Selbst wenn die Hälfte der betroffenen Rechner gereinigt werden, kann die andere Hälfte ihr Unwesen fortsetzen.

Preis-Leistungsverhältnis. Die Kriminellen zahlen für die enorme Bandbreite keinen Cent, zur Kasse gebeten werden vielmehr die betroffenen Nutzer. Bei ihnen liegt auch das Risiko, vom ISP geblockt zu werden, da sie die einzig Sichtbaren in der Spam-Kette sind.

Performance. 10.000 Rechner, die 10.000 Spam-Emails verschicken, machen dies bedeutend schneller als ein Server, der 100 Millionen Nachrichten versenden muss.
Aber wieviel Spam kann ein Botnetz denn nun tatsächlich versenden? SophosLabs ging dieser Frage nach und konfigurierte speziell hierfür einen „Honeypot“. Diese Fliegenfalle für

verschiedene IT-Sicherheitstests nimmt in diesem speziellen Fall Spamming-Befehle von den Besitzern des Botnetzes an, generiert Spam und versendet ihn. Natürlich wurde im Rahmen des Versuchsaufbaus garantiert, dass die ins System eingespeisten Nachrichten mit Hilfe eines speziell eingerichteten Sackgassen-Servers, der nicht vom Internet abgetrennt war, kein Eigenleben entwickeln und tatsächlich eine Spamwelle erzeugen konnte. Die Spamwelle wurde also so konstruiert, dass sie zwar loslegen, dann aber schnell wieder geblockt und statistisch erfasst werden konnte, ohne wirklichen Schaden anzurichten.

Im Rahmen des Versuchsaufbaus muss berücksichtigt werden, dass die Zahlen eines echten Botnetzes etwas niedriger ausfallen, da nicht alle eingebundenen Server fehlerfrei arbeiten. Die Ergebnisse geben dennoch einen sehr guten Eindruck, in welchem Umfang Kriminelle schon von einem einzigen kompromittierten Rechner in ihrem Botnetz profitieren. Innerhalb einer Woche wurden bei unserem Versuch von einem einzelnen Rechner, der mit nur einer Malware infiziert war, folgende „Erfolge“ registriert:

- 5,5 Millionen E-Mail-Adressen gespammt
- 30 GB ausgehende E-Mails versandt
- 750.286 individuelle Spam-Nachrichten versandt
- 26% beinhalteten eine weitere Malware, davon 11 verschiedene Typen
- 74% enthielten einen Link zu einer pharmazeutischen Webseite
- 3771 verschiedene URL-Kurzversionen wurden verwendet

Da viele Nutzer über ein unbegrenztes Datenvolumen verfügen, oder ihre ISPs lediglich die Downloads messen, sind 30 GB keine besonders hohe Summe. Dieser Wert basiert zudem auf einem durchschnittlichen Datendurchsatz von 400 KB pro Sekunde. Das ist weniger als die Hälfte der Upload-Bandbreite einer regulären ADSL-Verbindung. Es steht also in den meisten Fällen noch jede Menge Bandbreite zur Verfügung, so dass die Spamaktion von diesen Nutzern höchstwahrscheinlich nicht einmal bemerkt oder zumindest nicht weiter untersucht wird, da der aufs Gesamtsystem gar nicht vorhanden oder nur sehr minimal ist.

Wenn man nun die Zahlen eines einzelnen, infizierten Rechners auf ein 10.000-Computer-Botnetz anwendet, kommt eine gigantische Zahl heraus: 50 Milliarden Spam-E-Mails pro Woche könnten versendet werden. Dieses Ergebnis macht noch einmal deutlich wie wichtig es ist, Vorkehrungsmaßnahmen zu treffen. Wer nicht Teil der Lösung ist, ist Teil des Problems. Effektive Spamfilter, eine Firewall und Antiviren-Programme, die kurzen Prozess mit Zombie-Malware machen, sollten genauso selbstverständlich sein, wie das sofortige Säubern eines Rechners, wenn eine Infizierung festgestellt wurde. Für diese Aufgaben stehen zahlreiche kostenlose Programme zur Verfügung, beispielsweise die Sophos UTM Home Edition.

Über Sophos

Mehr als 100 Millionen Anwender in 150 Ländern verlassen sich auf Sophos‘ Complete-Security-Lösungen als den besten Schutz vor komplexen IT-Bedrohungen und Datenverlust. Sophos bietet dafür preisgekrönte Verschlüsselungs-, Endpoint-Security-, Web-, Email-, Mobile- und Network Security-Lösungen an, die einfach zu verwalten, zu installieren und einzusetzen sind. Das Angebot wird von einem weltweiten Netzwerk eigener Analysezentren, den SophosLabs, unterstützt.
Sophos hat seinen Hauptsitz in Boston, USA, und Oxford, Großbritannien. In Deutschland hat das Unternehmen seinen Hauptsitz in Wiesbaden und ist in Österreich und der Schweiz je an einem Standort vertreten. Weitere Informationen unter www.sophos.de.

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Christiane Capps, +49-174-3335550
Ulrike Masztalerz, +49-30-55248198
sophos@tc-communications.de