Link: <https://www.computerwoche.de/a/neues-mega-botnetz-aufgetaucht,1893592>

Noch kein probates Gegenmittel

Neues Mega-Botnetz aufgetaucht

Datum: 22.04.2009
Autor(en):Uli Ries

Über 1,9 Millionen infizierte PCs gehören zu einem kürzlich aufgetauchten Botnetz. Das Pikante: Einmal mehr sind auch PCs in großen Banken und vor allem Regierungsstellen betroffen. Die Schöpfer des extrem schwer zu entdeckenden Schädlings kommen offenbar aus der Ukraine.

Statistikfans: Die Botnetzbetreiber führen genau Buch, wie viele infizierte PCs unter ihrer Kontrolle stehen.
Foto: Finjan

Filtered bots: 1953448

Total bots: 1953448

Page : 1

▲	◆	◆
3884533	18.03.2009 07:52	303413
3884535	18.03.2009 07:52	303413

Wie die Antiviren-Jäger von **Finjan**¹ in ihrem **Blog**² schreiben, haben sie in den letzten Wochen zahlreiche Details über eines der momentan größten **Botnetze**³ zusammen getragen. Die Experten bekamen Zugriff auf den seit Februar 2009 aktiven Command-and-Control-Server des Netzes und konnten so die Zahl der weltweit infizierten PCs ermitteln: Über 1,9 Millionen Maschinen stehen unter der Kontrolle einer offenbar aus der Ukraine stammenden Gruppe von sechs Cyber-Kriminellen.

Laut Finjan stehen 45 Prozent aller infizierten Maschinen in den USA, immerhin vier Prozent des Botnetzes agiert von deutschen PCs aus. Betroffen sind nicht nur Rechner in Privathaushalten, sondern auch in zahlreichen Firmen. Insgesamt 77 Regierungsstellen weltweit kämpfen ebenfalls mit den Infektionen, allein 51 davon in den USA. Wie Ophir Shalitin, Marketingchef von Finjan, im Gespräch mit der Computerwoche erklärt, hat Finjan mehrere dutzend Firmen auf der Welt über die Infektion informiert. Außerdem wurden Strafverfolgungsbehörden mit hinzugezogen, hauptsächlich in den USA und Großbritannien.

Wie viele andere Botnetz-Schädlinge beherrscht auch die jüngst aufgetauchte, momentan noch namenlose Software zahlreiche Funktionen: Spamversand, anfertigen von Bildern des Bildschirminhalts des Opfers, auslesen E-Mail-Adressen, Kopieren von Dateien, mitschneiden von Tastatureingaben, kommunizieren per http mit anderen Rechnern, einschleusen von Code in andere Prozesse und so weiter. In ihrem Blog schreiben die Finjan-Mitarbeiter, dass die Kriminellen beinahe jede erdenkliche Funktion auf den kontrollierten PCs nutzen können.

Wie Shalitin weiter erklärt, gibt es daher keine eindeutig identifizierbaren Verhaltensmuster, da der Schädling in zig verschiedenen Varianten auftaucht. Dies liegt nicht zuletzt daran, dass er von verschiedenen, mit den ursprünglichen Programmierern verbundenen Netz-Gangstern verteilt wird. Letztere haben den Funktionsumfang jeweils angepasst. Diese zahlreichen Variationen machen es herkömmlicher **Antiviren-Software**⁴ laut Shalitin auch schwer bis unmöglich, den Schädling zu entdecken. Wie ein Test der Finjan-Experten belegt, schlugen bei einem Test Ende März lediglich vier von 39 Virenscannern an.

Verteilt wird die **Malware**⁵ über zahlreiche verschiedene Lücken in Browsern und Windows XP. Auffällig ist, dass laut Finjan offenbar nur Windows-XP-Maschinen betroffen sind und kein einziger Vista-PC. Allen Verteilungswegen gemeinsam ist, dass der Schädling über herkömmliche, mit böartigem Code infizierte Websites auf die PCs wandert.

Praktische Ratschläge, wie Unternehmen den Schädling aufspüren und im Schadensfall entfernen können, hatte Shalitin im Gespräch mit der Computerwoche nicht parat. Er verwies einzig darauf, per Netzwerküberwachungstool auf Datenpakete zu achten, die von bislang unbekanntem EXE-Files ins Internet wandern.

Links im Artikel:

¹ <http://www.finjan.com/content.aspx?id=175>

² <http://www.finjan.com/MCRCblog.aspx>

³ <http://de.wikipedia.org/wiki/Botnet>

⁴ https://www.computerwoche.de/knowledge_center/security/1885191/

⁵ <https://www.computerwoche.de/schwerpunkt/m/Malware.html>