AK Sicherheit, 04.02.2009, Protokoll
Thema der Sitzung: Botnetze

13:00 Registrierung
13:15 Beginn der Sitzung

Die übliche Vorstellungsrunde aller Teilnehmer entfiel aus Zeitgründen wegen der etwa 40 Anwesenden (bei 50 Anmeldungen) und der hohen Anzahl (5) der Referate.

Herr Dr. Brand berichtete, dass das Thema der letzten Sitzung, die tiefenpsychologische Studie zur Wirkungsanalyse von CISOs, beim Treffen der AK-Leiter am 22.01.09 ein bemerkenswertes Echo fand. Er führte das darauf zurück, dass "weiche" Themen in der Diskussion immer gerne angenommen werden. Das heutige "harte" Thema erfahre aber auch ein großes Interesse, wie die Zahl der Anwesenden zeige und die Tatsache, dass auch drei Vertreter der Presse, die Herren Laufen (für SWR), Reintjes (für DLF) und Spierling (für CZ), anwesend seien.

Anschließend wurden verschiedene Aspekte der Botnetze in Referaten vorgestellt und in Diskussionen vertieft. Es folgt eine kurze Zusammenfassung, dabei wird der Zusammenhang zwischen Bots und Spamversendern als bekannt vorausgesetzt. Alle Beiträge befinden sich im Dokumentenweb des Arbeitskreises (siehe http://www.eco.de/arbeitskreise/1675.htm).

Bots im Kontext von Spam
Christian J. Dietrich, Leiter Forschungsbereich Email-Sicherheit und Botnetze, Institut für Internet-Sicherheit if(is)

Herr Dietrich stellte zunächst Auswirkungen der Trennung des ISP McColo am 11.11.08 vom Internet vor, und zwar anhand der stark nachlassenden Anfragen an die Blacklist des iX-Spamfilters "NiX Spam". Dass auch der Ham-Anteil am 11.11. stark sank, bedeute, dass er zuvor oft falsch klassifiziert wurde, eine typische Schwäche von Blacklisten-Verfahren. Zur Verbesserung schlägt er die IP-Reputation vor. Allerdings seien ¾ der gerouteten IPv4-Adressen noch nicht in Erscheinung getreten und deshalb für ein Reputationsmaß nicht zugänglich. Aus der Zählung von mailsendenden IP-Adressen über mehrere Monate hinweg schloss er, dass es statistisch 12 Jahre dauert, bis alle gerouteten Adressen mindestens einmal gesichtet wurden. Sodann stellte Herr Dietrich einen Spam-Generator vor, der auch den klassischen Spamfilter SpamAssassin unterläuft.

Tracking Botnets
Thorsten Holz, Projektleiter Deutsches Honeynet-Projekt, Universität Mannheim, Laboratory for Dependable Distributed Systems

Herr Holz war leider krankheitsbedingt verhindert, sein Beitrag befindet sich aber ebenfalls im Dokumentenweb des Arbeitskreises.

Projekte des LKA Niedersachsen zur Bekämpfung von Botnetzen
Jens Kolpack, Sachgebiet 31.2 "Anlassunabhängige Recherche in Datennetzen", LKA Niedersachsen

Herr Kolpack berichtete, dass das genannte Sachgebiet eine Art Internet-Streife darstelle und 2006 eingerichtet worden sei. Ähnliche Dienststellen gebe es bei anderen LKA, beim BKA und beim Zoll. Es gehe um Gefahrenabwehr (z.B. zum Schutz politischer Großereignisse oder allgemein gegen Botnetze), und um Strafverfolgung (bei Kinderpornografie, Extremismus usw.). Beim Thema Botnetze habe man sich mit

Spam- und Bot-Analyse befasst. Wenn eine deutsche IP-Adresse als Zombie erkannt wurde, habe man den Provider informiert. Dabei hätten insbesondere große Provider wenig Kooperation gezeigt. Bei der Bot-Analyse habe man Trojaner ausgelöst, um durch ihre Beobachtung gehackte Server zu ermitteln.

Abuse-Management bei NetCologne - Identifizieren und Stoppen von Zombies
Dietmar Braun, Technischer Leiter Anti Spam Task Force des eco / Gunther Nitzsche, System Engineer, NetCologne GmbH

NetCologne hat ein Honeypotsystem zur Erkennung und zum Blocken trojanisierter PCs aus NetCologne-eigenen IP-Adressräumen erfolgreich im Einsatz. Herr Nitzsche beschrieb die Wirkungsweise des Systems, das aus der Software nepenthes mit eigenen Erweiterungen besteht. Nach Identifikation eines Angriffes werde der User schließlich über ein selbst entwickeltes Abuse Management Tool gesperrt. Dieses Tool wurde von Herrn Braun vorgestellt. Der User werde nach Sperrung auf ein "enforced portal" geleitet, das ihn informiert und ihm (nur) Zugriff auf ein Sicherheitspaket gewährt, damit er sein System desinfizieren kann. Das Portal ermöglicht dem User dann auch das selbständige Freischalten (mit Eskalation im Wiederholungsfall). Mit diesem wohlwollenden Ansatz hat NetCologne gute Erfahrungen gemacht. Auf Basis der eigenen Ergebnisse wirbt NetCologne für eine Intensivierung der Kooperation zwischen den ISPs, z.B. durch Aufbau eines "trusted ISP-Honeynets".

Rechtliche Aspekte beim Kampf gegen Botnetze
RA Frank Ackermann, Senior Legal Counsel, eco

Herr Ackermann erläuterte Maßnahmen gegen Botnetz-Betreiber und -Spammer auf der Basis von Straf- und Wettbewerbsrecht. Den Datenschutz beim Aufspüren eines Zombies im Kundennetz sieht er auch vor dem Hintergrund des Fernmeldegeheimnisses (§ 88 TKG) als nicht (notwendig) verletzt an, da das TKG auch Maßnahmen zum Schutz der technischen Systeme vorsehe. Dabei vertrat er eine weitere Rechtsauffassung zum möglichen Kontrolleingriff als einige anwesende ISP-Vertreter, was einige Diskussionen auslöste.

Die aktuelle Lage im Sicherheitsbereich: Zombies und mehr
Dr. Kurt Brand, Geschäftsführer, Pallas GmbH

Herr Dr. Brand geht in seinem Vortrag auf die Spam-Entwicklung der letzten zwei Jahre ein, die durch Abschalten von McColo um ein Jahr "zurückgeworfen" worden sei. Die täglich sendenden Bots seien von 10 Millionen auf 5 abgesackt, inzwischen aber wieder auf 7 Millionen gestiegen. Die Spam-Ausbrüche seien nach McColo weniger massiv aber zahlreicher geworden. Er wies auf die Wichtigkeit von Real-Time-Reputation hin, um nur kurzzeitig sendende Spamquellen und neue Virenausbrüche abzuwehren. Künftig werde eine entsprechend schnelle Erkennung von Malpages im Web nötig, die die nächste Herausforderung bei der Gefahrenabwehr darstellten. Erste Produkte dazu seien am Markt.

Verschiedenes, Themen und Termine

Der Arbeitskreis wird künftig an drei festen Terminen pro Jahr tagen, und zwar jeweils am ersten Mittwoch der Monate 02 / 05 / 10. In der nächsten Sitzung am 06.05.09 in Köln steht die "Sicherheit in der Gesundheitstelematik" im Fokus. Für den 07.10.09 wird noch ein Themenpate gesucht, der ein interessantes Thema auch durch Einwerbung von Expertenreferaten gestaltet. Vorgeschlagene Themen sind im Protokoll der letzten Sitzung zusammengestellt.

17:50 Ende der Sitzung
gezeichnet: Dr. Kurt Brand (Arbeitskreisleiter), 24.02.2009