

Kampf gegen die „Zombie-Armee“

Mehr als 350 internationale Experten der Polizei und aus der Wirtschaft erörterten Strategien gegen Bedrohungen durch BotNets aus dem Internet.

Die fünfte *BotNet Task Force* (BTF) Konferenz fand Mitte Jänner 2007 in der Microsoft-Zentrale in Redmond im Bundesstaat Washington statt. Drei Tage erörterten Experten die neuesten Entwicklungen und mögliche Präventiv- und Ermittlungsmethoden.

Österreich war durch Experten des Bundeskriminalamts vertreten.

Der Begriff „BotNet“ ist abgeleitet von den Wörtern „Robot“ und „Network“. Bot-

Nets sind auch bekannt unter dem Namen „Zombie-Armee“. Es handelt sich um eine große Anzahl von Internet-Computern, die ohne Wissen der Besitzer manipuliert wurden, um „ferngesteuert“ bestimmte negative und in der Regel strafbare Aktivitäten durchzuführen. Sie dienen ihrem „Herrn“, um dessen kriminelle Aktivitäten relativ anonym durchführen zu können. Dazu zählt der Weiterversand von Viren und Spam-Mails oder der Diebstahl von Kreditkarten- oder Bankinformationen. Manche solcher Netzwerke setzen sich aus Millionen von manipulierten Computern zusammen und können auch für „distributed Denial of Service“ Attacks gebraucht werden. Durch solche Attacks werden Dienste im Internet oder die gesamte Internetverbindung blockiert, danach folgen oft Erpressungsversuche: Um von solchen Attacks in Zukunft verschont zu werden, müsste ein gewisser Betrag überwiesen werden.

Es wird geschätzt, dass täglich ca. 170.000 ungeschützte Computer neu befallen werden. Einzelne aufgedeckte



BotNet-Konferenz in Redmond: Bernhard Otupal (Interpol), Steve Santorelli (Microsoft), Erhart Friessnik und Manfred Meikl (Bundeskriminalamt).

BotNets enthielten bis zu 1,5 Millionen ferngesteuerter Maschinen. 30.000 sind bereits genug, um eine Webseite im Internet unzugänglich zu machen. Der finanzielle Schaden, der durch diese Netzwerke verursacht wird, ist unerschätzbar. Experten bezeichnen diese Technologie als die größte Gefahr für das Internet – noch vor Viren und Spam-Mails.



Schadprogramme haben immer häufiger ausgeklügelte Mechanismen, um sich vor Antivirensoftware zu tarnen.

Die Ermittlungen sind extrem schwierig, zumal die Täter über ausgereifte Verschleiertechniken verfügen. Nur eine enge internationale Zusammenarbeit zwischen Polizei, Privatwirtschaft und Universitäten kann langfristig zur Aufklärung dieser Straftaten führen. Bei der Konferenz in den USA wurde eine noch engere Zusammenarbeit aller Beteiligten vereinbart, um gemeinsam Strategien und Gegenmaßnahmen einzuleiten und auszubauen.

Interpol ist in den Kampf gegen diese Technologien seit langer Zeit eng eingebunden und entwickelt für die Polizei detaillierte technische Beschreibungen und Ermittlungsrichtlinien. Interpol-Schulungen in diesem Bereich werden unter enger Einbeziehung der Wirtschaft und der Wissenschaft entwickelt und werden noch heuer Polizeiexperten aus aller Welt angeboten.

Die nächste Konferenz der *BotNet Task Force*, die auch einer Bestandsaufnahme des Erfolgs in diesem Kampf dienen wird, wird im Spätherbst im Generalsekretariat der Interpol in Lyon abgehalten.

Da es sich in aller Regel bei den infizierten Computern um ungeschützte Geräte von Privatanwendern handelt, die sich der Gefahr nicht bewusst sind, die von ihren Computern ausgeht, ist Aufklärung der wichtigste Faktor im Kampf gegen diese relativ neue Kriminalitätsform. Antivirenprogramme und Firewalls, die regelmäßig aktualisiert werden müssen, bieten gegen beinahe alle Botnet-Formen einen guten Schutz.

Bernhard Otupal