

Pressesprecher: Achim Fischer
Telefon 06 21 / 1 81-1013
fischer@verwaltung.uni-mannheim.de
www.uni-mannheim.de

Mannheim, 3. März 2010

Presseinformation

Weltweit größter Schlag gegen Spam-Netzwerk

- **Mannheimer Forscher an Zerstörung eines kriminellen Computernetzwerks beteiligt**

Vier Universitäten, das Unternehmen Microsoft und ein US-Gericht haben den bislang größten Schlag gegen kriminelle Spam-Versender erzielt. Eine maßgebliche Rolle spielten dabei Forscher der Universität Mannheim. Gemeinsam mit den Universitäten Washington, Bonn und der TU Wien legten die Mannheimer Informatiker das so genannte „Waledac-Botnetz“ lahm, das täglich bis zu 1,5 Milliarden Spam („Müll“)-Mails verschickt hat.

- Hunderttausende Computer waren meist ohne das Wissen ihrer Besitzer Teil des „Waledac-Botnetzes“. Botnetze vernetzen Computerprogramme, die weitgehend selbständig sich wiederholende Aufgaben abarbeiten. Die Internetnutzer hatten sich über E-Mailanhänge oder präparierte Webseiten Programme eingefangen, mit deren Hilfe Hacker die Computer nutzen konnten, um etwa Spam-Mails zu versenden. Indem einerseits Forscher der Universitäten Bonn, Mannheim und TU Wien die Kommunikation der infizierten Computer lahmlegten, das Unternehmen Microsoft eine Klage gegen Betreiber von kriminellen Internet-Adressen erhoben hatte und infolge dieser Klage 273 Domains gesperrt wurden, ist es gelungen, das „Waledac-Botnetz“ auszuschalten. „Die Aktion hat gezeigt, dass eine Zusammenarbeit zwischen Unternehmen, Forschern und Gerichten funktioniert und im Kampf gegen Internet-Kriminalität zum Erfolg führen kann“, erklärt ein an der Aktion beteiligter Forscher von der Universität Mannheim.

Dabei stellte das „Waledac-Botnetz“ eine besondere Herausforderung dar: Anders als in einfachen Netzwerken, in denen die infizierten Computer direkt mit dem zentralen Server der Kriminellen kommunizieren, waren in diesem Botnetz Computer als „Vermittler“ zwischengeschaltet, die von insgesamt acht verschiedenen Servern betrieben wurden und die Kommunikation mit den infizierten Rechnern steuerten. Die Computerwissenschaftler haben an der „Vermittlerstelle“ eingegriffen, sich selbst quasi als „Vermittler“ installiert und so die Kommunikation der Botnetz-Betreiber mit den infizierten Computern unterbrochen. Darüber hinaus ist es gelungen, die vom Netzwerk genutzten Server abzuschalten.

Gleichzeitig wurden auf Gerichtsbeschluss knapp 300 Internet-Domains abgeschaltet. In monatelangen Ermittlungen hatte das Unternehmen Microsoft,

dessen E-Maildienst Hotmail betroffen war, 273 Internet-Adressen ausfindig gemacht, über die das Botnetz gesteuert wurde. Gegen die Betreiber dieser Internet-Adressen hatte Microsoft dann Anfang vergangener Woche vor einem Bundesgericht im US-Staat Virginia Klage eingereicht und Rückendeckung erhalten: Das Gericht verpflichtete das Unternehmen, das die Adressen verwaltet, diese stillzulegen. Damit sind die betroffenen Internet-Seiten nicht länger erreichbar, das Botnetz nicht mehr funktionsfähig.

Infiziert sind Computer weltweit. Mit der Zerstörung des Botnetzes wurde die Schadsoftware auf den infizierten Computern nicht entfernt. Dazu muss vom Benutzer entweder manuell ein Entfernungswerkzeug ausgeführt oder ein aktueller Virenschanner betrieben werden, der die schädlichen Programme eliminiert. Als Schutz vor Schadsoftware hilft generell Wachsamkeit beim Surfen sowie das regelmäßige Einspielen von Sicherheits-Updates auf dem eigenen PC.

Kontakt:

Prof. Dr. Felix Freiling
Lehrstuhl für Praktische Informatik I
Tel.: 0621 / 181-2545
E-Mail: walowdac[at]informatik.uni-mannheim.de