Hamburger Abendblatt vom 23.01.2012

Stormarner jagen Internet-Bande mit FBI

Jan Drömer und Dirk Kollberg haben Machenschaften russischer Computer-Betrüger aufgedeckt. Jetzt arbeiten sie mit US-Ermittlern zusammen

DOROTHEA BENEDIKT

Die beiden IT-Experten Jan Drömer, 32 (l.), und Dirk Kollberg, 38, sitzen oft stundenlang vor ihren Laptops und gehen auf Verbrecherjagd im Netz Foto: Dorothea Benedikt

AMMERSBEK :: Schadenfreude ist bekanntlich die schönste Freude. Dies dürfte auch der Grund sein, warum lustige Videos bei Tausenden von Internet-Usern so beliebt sind. Doch den Schaden haben am Ende die Betrachter selbst. Denn Cyber-Kriminelle machen sich diese Vorliebe zu Nutze und verseuchen die Computer der Internet-Surfer mit Viren. Später sollen sie dann für die vermeintliche Beseitigung der Schäden Geld überweisen.

Zwei IT-Profis aus Ammersbek und Hamburg sind einer Gruppe von Internet-Betrügern dabei auf die Schliche kommen und haben ihre perfiden Machenschaften aufgedeckt. Insbesondere für die amerikanischen Ermittlungsbehörden sind die Ergebnisse von Jan Drömer und Dirk Kollberg von großem Interesse. Das Federal Bureau of Investigation, besser bekannt als das FBI, arbeitet mit den beiden deutschen Internet-Experten zusammen.

„Erstmals sind wir 2008 auf den Koobface-Virus aufmerksam geworden", sagt der Ammersbeker Jan Drömer, der in Hamburg als IT-Manager arbeitet und in seiner Freizeit im Netz auf Verbrecherjagd geht. So entdeckte der 32-Jährige mit seinem Freund Dirk Kollberg auch die Masche einer russischen Internet-Gang. Die Betrüger verbreiteten über soziale Netzwerke wie Facebook oder Twitter den Koobface-Virus. Sie erstellten ein gefälschtes Benutzerprofil und versendeten darüber lustige Kurzfilme. Kollberg: „Doch wer sich ein Video ansehen wollte, wurde aufgefordert, die aktuelle Version des Flash Player runter zu laden."

Die fünf Jungs aus Stankt Petersburg sind quasi die Marketing-Experten, sie akquirieren die Kunden
Dirk Kollberg, IT-Profi

Die Masche der Cyber-Kriminellen: Das Programm sah dem des bekannten Software-Herstellers Adobe zum Verwechseln ähnlich. Und so fielen Tausende von Internet-Nutzern auf den Trick rein und luden sich die Schadsoftware auf ihren PC.

„Ich wurde sofort skeptisch, als ich das Programm sah", erinnert sich Drömer. Deswegen machten sich die beiden IT-Experten sofort ans Werk. Sie installierten die Software auf einem separaten Computer, den sie für solche Zwecke zuhause stehen haben, und beobachteten, wo sich das Koobface-Virus einnistet und was es mit dem Rechner macht. „Wir konnten beobachten, dass das Programm versuchte, Daten an einen Server zu schicken", sagt Kollberg. Diesen Server guckten sie sich dann genauer an. „Darauf kann jeder im Internet zugreifen", sagt Drömer. Denn Internet-Firmen vermieten Datenvolumen auf ihren Hochleistungsrechnern. Auch Kriminelle mieten sich Speicherplätze auf den legalen Servern, auf denen Protokolle geführt werden. „Betrüger geben gefälschte Firmenadressen bei den Betreibern an und achten darauf, dass in den Aufzeichnungen keine Verbindungen zu den eigenen Computern auftauchen", sagt Drömer.

Doch wie im richtigen Leben machen auch Cyber-Kriminelle Fehler. [illegible]

einen Link in dem Protokoll, der sich als Archiv der Cyber-Gangster entpuppte. „Volltreffer", sagt Kollberg. In diesem Archiv waren quasi die Baupläne für das Koobface-Virus und für weitere Schadprogramme zum Ausspionieren von Computern. Für den 38-Jährigen, der in Ahrensburg aufgewachsen ist, waren diese Daten von großer Bedeutung. Denn Kollberg arbeitet für das britische Anti-Viren- und IT-Sicherheitsunternehmen Sophos. Wie in der Medizin konnte er jetzt Gegenmittel entwickeln.

Aber nicht nur die Viren-Programme weckten das Interesse der beiden IT-Profis. In dem Archiv befand sich auch eine Software, die die Mitglieder der Betrüger-Bande täglich per SMS darüber informierte, wie viel Geld sie mit ihrer Masche eingenommen haben. „Pro Jahr waren es etwa zwei Millionen US-Dollar", sagt der Ammersbeker.

Fünf Handy-Nummern tauchten in der Datei auf. Von nun an war es für Drömer und Kollberg ein leichtes Spiel die Cyber-Kriminellen ausfindig zu machen. Beide schlugen sie quasi mit ihren eigenen Waffen und spionierten sie aus. „Es fing damit an, dass wir eine Mobil-

Ein Internet-Betrüger aus St. Petersburg prahlt im Netz mit seinem Porsche

Nummer in einer Verkaufsanzeige für ein Auto entdeckt haben. In der Annonce standen auch Name und Adresse des Verkäufers", sagt Kollberg. Mit den persönlichen Daten des Betrügers aus St. Petersburg machten sich beide im Netz auf die Suche und wurden prompt fündig. In sozialen Netzwerken und Chats prahlte der Gangster mit seinem ergaunerten Reichtum. Auf zahlreichen Bildern, die er in seinem echten Profil hochgeladen hatte, sah man den Russen mit teuren Sportwagen und in Luxushotels. Damit nicht genug, er veröffentlichte auch Bilder von seinen Komplizen, die ausgelassen Partys feierten oder zusammen in ihrem Büro in St. Petersburg vor dem Rechner saßen. Auch die vier anderen Handy-Nummern ließen sich dann schnell zuordnen.

Etwa sechs Monate spionierten Drömer und Kollberg die Cyber-Gang aus, bis sie die Identität der Russen kannten. „Parallel haben wir die Betreiber von Facebook und die Agenten des FBI über unsere Ergebnisse informiert", sagt der 32-Jährige. Facebook interessierte sich vorrangig für die Programmierung der gefälschten Internet-Videos. „Die Betreiber können dann spezielle Programme entwickeln, die diese Schadsoftware erkennen und die Zugänge ermitteln, von denen diese gestreut werden", sagt Kollberg. Die US-Ermittler interessierte indes die Struktur der Internet-Bande.

„Die fünf Jungs aus St. Petersburg sind quasi die Marketing-Experten, sie akquirieren die Kunden. Ist ein Computer infiziert, greifen dann andere Betrüger darauf zurück und installieren wie bei den Koobface-Opfern eine Erpressersoftware darauf. Der Benutzer bekommt die Meldung, dass er einen Virus auf seinem PC hat. Dann erscheint auch gleich das Gegenmittel dafür, eine Software für 80 Dollar, die aus dem Netz geladen werden muss und die völlig wirkungslos ist", erklärt Kollberg: „Für dieses Programm sind andere Kriminelle verantwortlich, die überall auf der Welt Bankkonten haben und auf den Geldtransfer spezialisiert sind. Von diesen Einnahmen bekommt dann die St. Petersburger Internet-Gang über Mittelsmännern einen Teil ab. Es ist quasi das organisierte Verbrechen im Netz." Auch solch einer Erpresser-Firma sind Kollberg und Drömer in den vergangenen Jahren auf die Schliche gekommen und haben dies dem FBI gemeldet. 2010 wurde die Internetbande mit Sitz in Kiew in der Ukraine von einem US-Gericht dazu verurteilt, den amerikanischen Geschädigten 163,2 Millionen Doller zu erstatten.

Ob auch die St. Petersburger vor einem Richter landen, ist noch unklar. „Der FBI-Agent, mit dem wir zusammenarbeiten, sagte uns, dass sie noch ermitteln", sagt Drömer. Die beiden deutschen IT-Profis haben es indes auf die nächsten Cyber-Gangster abgesehen und gehen in der Ammersbeker Wohnung weltweit auf die Jagd.

Cyber-Betrüger ergaunern 61,5 Millionen Euro von deutschen Internet-Nutzern

Das Internet wird zunehmend zum Tatort. Das aktuelle Lagebild „Cybercrime 2010" des Bundeskriminalamtes bestätigt dies. 2010 ist die Zahl der in Deutschland erfassten Cybercrime-Fälle im Vergleich zum Vorjahr um 19 Prozent auf 60 000 Straftaten gestiegen.

Cybercrime umfasst dabei alle Verbrechen, die mit moderner Informations- und Kommunikationstechnik begangen werden. **27 000 Anzeigen**, fast die Hälfte der registrierten Taten, betreffen Betrügereien wie das Ausspähen von Onlinebanking-Daten.

61,5 Millionen Euro ergaunerten die Internet-Kriminellen laut BKA im Vorjahr. 2009 waren es 37 Millionen Euro. IT-Experten gehen jedoch von einem großen Dunkelfeld aus. Viele User, die beispielsweise 30 Euro für ein wirkungsloses Anti-Viren-Programm ausgegeben haben, würden selten Anzeige erstatten.

Internet-Experten mahnen, dass dies die Masche der Cyber-Täter sei und fordern Opfer dazu auf, Straftaten der Polizei zu melden. Denn nur wenn es Geschädigte gibt, gibt es für die Ermittler auch Täter. (dob)