

+++ *News Alert Trend Micro* +++

Trend Micro analysiert den Betrug mit gestohlenen Klicks

Hallbergmoos – 10. August 2010 – Das Geschäft mit gestohlenen Klicks blüht. Trend Micro hat in den vergangenen Monaten die Machenschaften von Online-Banden analysiert, die Suchergebnisse oder Anzeigen manipulieren, um die Klicks der arglosen Anwender umzuleiten und anschliessend weiterverkaufen. Dieses Betrugsmodell ist ein Massengeschäft, bei dem auch die Betreiber kleiner Botnetze von zirka 150'000 gekaperten Rechnern jedes Jahr Millionengewinne erzielen können – und das obwohl der Preis pro gestohlenem Klick im Durchschnitt bei nur einem oder zwei Eurocents liegt.

Zum Einsatz kommt dabei eine bestimmte Art Schadsoftware, so genannte Browser Hijacker, die insbesondere für den Missbrauch von Suchergebnissen genutzt werden. Zwar ist die Funktionsweise der von den Anwendern benutzten Suchmaschinen dadurch nicht beeinträchtigt. Sobald jedoch die User ein Suchergebnis oder einen Werbelink anklicken, werden sie auf eine fremde Webseite umgeleitet, damit ihre Klicks von den Online-Betrügern zu Geld gemacht werden können. Die gekaperten Klicks werden dabei an sogenannte Traffic Broker verkauft, die als Zwischenhändler fungieren und gleichzeitig die innovativen Werkzeuge überlisten, mit denen sich etablierte Suchmaschinenbetreiber oder Online-Marketiers gegen Betrügereien zu wappnen versuchen. Einen solchen kriminellen Zwischenhändler hat Trend Micro in der Nähe von St. Petersburg in Russland ausgemacht, der auch Briefkastenfirmen in Grossbritannien und auf den Seychellen besitzt und bereits seit 2005, vielleicht sogar seit 2003 „im Geschäft“ ist.

Da der Betrug in der Regel von den Anwendern bald bemerkt wird – schliesslich sehen sie ja, dass sie weitergeleitet werden und nicht zu den gewünschten Internetseiten gelangen – müssen die Cyberkriminellen jeden Tag sehr viele Systeme neu infizieren. Darüber hinaus aber versuchen sie mit neuen Tricks, die Lebensdauer ihrer Schadsoftware auf den infizierten Rechnern, die in dem von Trend Micro analysierten Fall bei sechs bis zwölf Tagen liegt, zu verlängern. Einer dieser Tricks ist die Verwendung von DNS-Komponenten in der Schadsoftware, welche die DNS-Einstellungen in den Browsern ändern. Diese Komponenten können auch nach dem erfolgreichen Entfernen des Botnetzes weiter auf dem Rechner bleiben und damit die Neuinfektion ermöglichen.

Weitere Informationen zu Struktur und Funktionsweise dieses Betrugsmodells sind im deutschen Trend Micro-Blog unter <http://blog.trendmicro.de/wie-wird-man-millionar-%E2%80%93-kriminellen-banden-der-betrugische-traffic-broker-und-gestohlene-klicks/> erhältlich. Anwender von Trend Micro-Lösungen sind vor der beschriebenen Attacke über das Trend Micro Smart Protection Network geschützt. Denn die darin enthaltenen Webreputationsdienste sorgen dafür, dass die Weiterleitung von gefälschten Suchergebnissen unterbunden wird.

Über Trend Micro

Trend Micro, einer der international führenden Anbieter für Internet-Content-Security, richtet seinen Fokus auf den sicheren Austausch digitaler Daten für Unternehmen und Endanwender. Als Vorreiter seiner Branche baut Trend Micro seine Kompetenz auf dem Gebiet der integrierten Threat Management Technologien kontinuierlich aus. Mit diesen kann die Betriebskontinuität aufrechterhalten und können persönliche Informationen und Daten vor Malware, Spam, Datenlecks und den neuesten Web Threats geschützt werden. Unter <http://blog.trendmicro.de> informieren sich Anwender zu aktuellen Bedrohungen. Die flexiblen Lösungen von Trend Micro sind in verschiedenen Formfaktoren verfügbar und werden durch ein globales Netzwerk von Sicherheits-Experten rund um die Uhr unterstützt. Zahlreiche Trend Micro-Lösungen nutzen das Trend Micro Smart Protection Network, eine wegweisende Cloud-Client-Infrastruktur, die für den Echtzeit-Schutz vor aktuellen und neuen Bedrohungen innovative, Cloud-basierende Reputationstechnologien und Feedback-Schleifen mit der Expertise der TrendLabs-Forscher kombiniert. Trend Micro ist ein transnationales Unternehmen mit Hauptsitz in Tokio und bietet seine Sicherheitslösungen über Vertriebspartner weltweit an. Weitere Informationen zu Trend Micro finden Sie im Internet unter www.trendmicro-europe.com.

Ansprechpartner für die Presse:

Trend Micro Deutschland GmbH
Hana Göllnitz
Zeppelinstrasse 1
D-85399 Hallbergmoos
Telefon: 0049 811 88990 863
E-Mail: hana_goellnitz@trendmicro.de

Communication Partners AG
Patrick Bergmann
Haldenstrasse 5
CH-6340 Baar
Telefon: 041 768 11 77
E-Mail: pbergmann@cpartners.com