+++ Trend Micro Kommentar +++

„Yes, we scare“: Den Browser abzusichern ist das beste Mittel gegen Schadsoftware aus der Cloud

Von Raimund Genes, CTO bei Trend Micro

Hallbergmoos – 18. März 2010 – Die Vernetzung und Spezialisierung in der kriminellen Untergrundwirtschaft nimmt immer bedrohlichere Ausmasse an. So wurde das „Servicespektrum“ des „YES Exploit System“, einer Art Malware as a Service-Lösung für Cyberkriminelle, jüngst um die „Dienstleistung“ voll automatisierter Tests von Schadsoftware gegen die Lösungen von insgesamt 26 IT-Sicherheitsherstellern erweitert. Zusammen mit dem bereits existierenden Prüfdienst, welche Webadressen von den Sicherheitslösungen als bösartig aussortiert werden, ist die Dienstleistung für eine Abonnementgebühr von nur 70 US-Dollar im Monat zu haben.

Ist einmal sicher gestellt, dass die getestete Schadsoftware unerkannt bleibt, lässt sie sich auf Wunsch über das YES-System verbreiten. Die Kriminellen brauchen nur anzuklicken, in welchen Ländern ihre bösartige Software aktiv werden soll, in welchen Browsern und auf welchen Betriebssystemen. Die Auswahl ist gross, denn die Bande hinter dem YES-System behauptet, dass sie in der neuesten Version „alle Windows-Versionen 9x bis 7, sowohl 32 als auch 64 BIT, und sämtliche Browser, die ein angreifbares Plugin haben, gehackt“ habe. Dabei wird zunächst Schadcode in ansonsten saubere Webseiten eingefügt. Sobald Anwender solche infizierten Seiten besuchen, werden sie vom YES-System auf einen Server der Kriminellen umgeleitet, von dem aus dann bösartige Dateien auf ihre infizierten Rechner abgesetzt werden.

Das System ist eindeutig auf die Unterstützung von miteinander in Verbindung stehenden Anbieterinfrastrukturen der Schattenwirtschaft ausgerichtet. Es stellt eine vollständige Plattform für die Lieferung von Schadsoftware zugunsten von kriminellen Geschäften dar, möglicherweise, um eine neue ZeuS-Kampagne – ZeuS ist ein Botnetz, das die befallenen Systeme zu Zombie-Rechnern macht, die von den Cyberkriminellen kontrolliert und ausspioniert werden – anzustossen oder um irgendeine Scareware – das heisst Software, die den Anwendern über fiktive Warnmeldungen Furcht einflösst und sie zu falschem Verhalten wie dem Anklicken eines bösartigen Links verleitet – zu verteilen. YES ist häufig in einen vollständigen Service für ZeuS-Angebote eingebunden.

Den Browser absichern

Trend Micro rät daher, die eingesetzten Sicherheitslösungen stets aktuell zu halten und alle verfügbaren Aktualisierungen für die verwendeten Browser zu installieren. Darüber hinaus bietet Trend Micro Anwendern, die nicht zu seinem Kundenstamm zählen, kostenlose Werkzeuge an, die das Ausnutzen von Browser-Lücken durch noch nicht bekannte Schadsoftware verhindern helfen. Dazu zählen etwa Browser Guard oder Web Protection Add On für den Internet Explorer von Microsoft. Browser Guard entdeckt und blockiert Techniken, wie sie das YES-System anwendet, um Anwendersysteme zu infizieren. Das Web Protection Add On verhindert den Zugriff auf bösartige Webseiten oder solche mit zweifelhaftem Ruf. Beide Schutztechniken sind selbstverständlich Teil der kommerziellen Trend Micro-Lösungen wie Trend Micro Internet Security für Endanwender.

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