+++ News Alert Trend Micro +++

Windows Shortcut-Schwachstelle öffnet nun auch Zeus/ZBOT-Varianten und Sality Tür und Tor

Hallbergmoos – 29. Juli 2010 – Wie von Trend Micro bereits in der vergangenen Woche berichtet, haben die Exploits der Windows Shortcut-Schwachstelle kontinuierlich zugenommen. Das Expertenteam von Trend Micro hat nun herausgefunden, dass neuerdings auch ZBOT-Varianten über bösartige Anhänge in Spam-Nachrichten auf diesem Wege verbreitet werden. Diese bösartigen Mails geben vor, von Microsoft selbst zu stammen und eine Installationsanleitung für ein angebliches Sicherheits-Update zu enthalten, wobei sogar ein vermeintliches Kennwort für die vorgeblich geschützte ZIP-Datei mitgeliefert wird. Im Betreff führen diese das irreführende Versprechen, ein „Microsoft Windows Security Advisory" zu beinhalten. Das an diese Nachrichten angehängte Archiv enthält jedoch eine bösartige .LNK-Datei, die Trend Micro als LNK_STUXNET.SM identifiziert hat. Darüber hinaus wurde eine bösartige .DLL-Datei entdeckt, die als TROJ_ZBOT.BXW ihr Unwesen treibt.

Wird der Exploit-Code im Shortcut angestossen, so führt er die Malware-Komponente aus, die dann ihrerseits den Hauptschädling TROJ_ZBOT.BXW herunterlädt und ausführt. Dabei handelt es sich um eine ZBOT 2.0-Variante, die Trend Micro schon zu Beginn dieses Jahres entdeckt hatte. Bereits bekannte SALITY-Dateiinfektoren wie beispielsweise PE_SALITY.LNK-O werden jedoch nun auch für diese Schwachstelle eingesetzt.

Zur Erinnerung: Bisher wurde noch kein Patch für diese immer gefährlicher werdende Schwachstelle zur Verfügung gestellt, sondern lediglich ein sogenanntes „Fix-Tool" für das Deaktivieren von .LNK und .PIF! veröffentlicht.

Alle Nutzer von Trend Micro-Produkten sind automatisch vor derlei Bedrohungen geschützt, da diese bereits vor einer möglichen Ausführung blockiert werden. Weitere Informationen zu den Gefahren dieser Windows-Schwachstelle sind im deutschsprachigen Trend Micro-Blog unter http://blog.trendmicro.de/zeuszbot-and-sality-nutzen-die-shortcut-schwachstelle/ erhältlich.

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