Pressemitteilung

Trend Micro Malware Report für August 2008: „Bitte aktualisieren Sie Ihre Malware!“

Malware tarnt sich als Sicherheitslösung; ZLOB leitet Suchmaschinen-Traffic um

Unterschleissheim – 11. September 2008 – Trend Micro (TSE: 4704) informiert über die Entwicklung der aktuellen Bedrohungslandschaft im August 2008: Immer häufiger tarnen sich Trojaner als Sicherheitslösungen bzw. Updates für Betriebssysteme, um arglose Anwender zur Installation zu bewegen. Darüber hinaus entdeckte Trend Micro im August neue Varianten der ZLOB-Familie. Das Gefährliche: Der Trojaner manipuliert lokale Einstellungen, so dass Internet-Anfragen nach Belieben auf gefährliche Seiten umgeleitet werden können. Zu den weiteren Ereignissen des vergangenen Monats gehören der Facebook-Wurm und Malware auf der International Space Station (ISS).

Die Mehrheit der Computernutzer weiss: Betriebssystem, Sicherheitslösungen und andere Applikationen müssen immer über die neuesten Updates verfügen – und genau dieses Sicherheitsbewusstsein versucht die Malware-Szene jetzt verstärkt auszunutzen. Im August entdeckte Trend Micro eine steigende Anzahl von Trojanern, die sich als Sicherheitssoftware tarnen. Die Infektionskette beginnt üblicherweise mit einer Spam-E-Mail, die zum Beispiel einen Link zu einem angeblichen Prominenten-Video enthält. Wird dieser Link geöffnet, beginnen der automatische Download und die Installation eines Trojaners. Im Folgenden erhält der Anwender wiederholte „Infektionsalarme“ und „Update-Aufforderungen“, während im Hintergrund zusätzliche Malware installiert wird. Ein Vertreter dieser Kategorie, von Trend Micro als TROJ_FAKEAV.CX erkannt, fordert den Anwender sogar zum Erwerb einer Lizenz für die angebliche Demoversion des falschen Sicherheitsprogramms auf. Dieser Social-Engineering-Trick lässt sich natürlich auch auf Betriebssysteme und andere Applikationen ausweiten: So entdeckte Trend Micro im vergangenen Monat verschiedene Spam-Mails mit Links zu „kritischen Updates“ für Windows XP und Vista sowie für eine amerikanischen Banking-Software.

Falsch verbunden: ZLOB manipuliert DNS-Auflösung

Vor mehr als einem Jahr entdeckten Trend Micro Experten ein Netzwerk aus mehr als 900 irregulären DNS (Domain Name System) Servern, die mit der ZLOB Trojaner-Familie in Verbindung standen. DNS-Server haben die wichtige Aufgabe, Domain-Namen in IP-Adressen zu übersetzen und somit sicherzustellen, dass Anwender mit der gewünschten Internet-Seite verbunden werden. Im August sind jetzt ZLOB-Varianten aufgetaucht, mit denen Angreifer die lokalen Einstellungen auf Computern manipulieren können, um Internet-Anfragen über das ZLOB-DNS-Netzwerk zu leiten.

Davon sind aktuell besonders vier der grössten Suchmaschinen betroffen: Suchanfragen werden ohne Wissen des Anwenders auf andere Internet-Seiten umgeleitet. Dort findet sich zwar eine vertraute Liste der Suchergebnisse, aber nach Erkenntnissen von Trend Micro ist die überwiegende Mehrzahl der ergänzenden „Sponsored Links“ gefälscht. Für die Suchmaschinen bedeutet dieser „Click Fraud“ immense finanzielle Verluste und Anwender können nicht mehr sicher sein, auf vertrauenswürdige Webseiten zu gelangen.

Mit immer neuen Social-Engineering-Tricks gelingt es den Kriminellen hinter ZLOB, die Verbreitungszahlen auf einem konstant hohen Niveau zu halten. Allein für das zweite Halbjahr 2007 geht Microsoft von rund 14.000.000 Infektionen aus. Auf Seiten der Suchmaschinenbetreiber ist das Problem bekannt, aber gegen lokale Manipulationen kann nicht vorgegangen werden. Anwender können sich hingegen durch „in-the-cloud“-Technologien wie das Trend Micro Smart Protection Network (SPN) schützen: Durch Korrelation umfangreicher Informationen und einer Reputationsanalyse erkennt SPN die gefälschte Webseiten und verhindert die Täuschung des Anwenders.

Wurm spezialisiert sich auf Facebook

Mit WORM_KOOBFACE.E und KOOBFACE.D hat die Malware-Szene im August die populäre Social-Networking-Site „Facebook“ ins Fadenkreuz genommen: Beide Würmer machen sich die Interaktivität des Web 2.0-Angebots zu nutze und suchen auf infizierten Systemen gezielt nach bestimmten Zeichenfolgen in Cookies, die von Facebook verwendet

werden. Sobald so eine Zeichenfolge gefunden wurde, kann der Wurm auf das Facebook-Anwenderprofil zugreifen. So lassen sich zum Beispiel dem öffentlichen Profil Links zu Kopien des Wurms hinzufügen, die dann wiederum von arglosen Nutzern angeklickt werden. Kunden von Trend Micro sind über das Smart Protection Network vor dem versehentlichen Aufruf dieser gefährlichen Links geschützt.

Erste Malware im All...oder doch nicht?

Als angeblich erste Malware im All bzw. auf der International Space Station (ISS) wurde WORM_AUTORUN.BPN im August grosse Medienaufmerksamkeit zuteil. Laut der NASA handelte es sich nicht wirklich um ein Debut: Die amerikanische Raumfahrtbehörde wurde nach eigenen Angaben schon früher mit orbitaler Malware konfrontiert, allerdings nur selten und auf nicht-kritischen Systemen. Trotzdem sollte der Vorfall als Warnung dienen: Wenn Malware sogar in die unendlichen Weiten des Weltraums vordringen kann, ist auf der Erde höchste Vorsicht geboten.

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 aufrecht erhalten und können persönliche Informationen und Daten vor Malware, Spam, Datenlecks und den neuesten Web Threats geschützt werden.

Unter www.trendmicro.com/go/trendwatch 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. 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.

Pressekontakt:

Communication Partners AG
Fabienne Strobel
Haldenstrasse 5
CH-6340 Baar
Telefon: 041 768 11 77
Fax: 041 768 11 79
E-Mail: fstrobel@cpartners.com

Herausgegeben im Auftrag von:

Trend Micro Deutschland GmbH
Hana Göllnitz
Lise-Meitner-Strasse 4
D-85716 Unterschleissheim
Telefon: 0049 89 37479 863
Fax: 0049 89 37479 799
E-Mail: hana_goellnitz@trendmicro.de