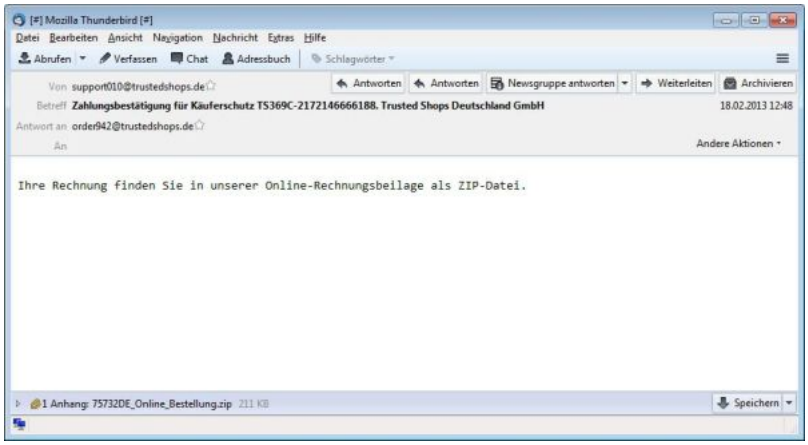
# Malware-Angriffe per E-Mail gegen Nutzer von Online-Shops

19.02.2013, 18:08 | IT, New Media & Software

Pressemitteilung von: *eleven GmbH*




Beispiel E-Mail Trusted Shops. (Quelle: Eleven Research)

Malware-Kampagne nutzt weitverbreitetes Trusted-Shops-Gütesiegel als Köder

Berlin 19. Februar 2013 – Das Research-Team von Eleven, führender deutscher E-Mail-Sicherheitsdienstleister, warnt vor einer massiven Welle virenverseuchter E-Mails, die derzeit im deutschsprachigen Raum unterwegs ist. Die Kampagne zielt auf Nutzer von Online-Shops ab und hat Betreffzeilen wie: „Zahlungsbestätigung für Käuferschutz TS369C-2172146666188. Trusted Shops Deutschland GmbH“ oder „Käuferschutz TS689C-5047642656087 zur Bestellung bei Smartbuyglasses.de“. Weitere Online-Shops, deren Namen von den Urhebern genutzt werden, sind unter anderem Veromoda.com, Frick-wein.de oder Apodiscounter.de.

Die Masche der Betrüger: In den E-Mails wird behauptet, der Empfänger hätte einen Käuferschutz beim Online-Shop-Zertifizierer Trusted Shops abgeschlossen, dessen Bestätigung bzw. Rechnung sich im Anhang der E-Mail befände. Statt der Bestätigung enthält der Anhang, der sich als komprimierte Zip-Datei tarnt, eine ausführbare Datei, die beispielweise den Namen Online_Bestellung.exe oder ähnliches trägt. Öffnet der Nutzer diese, wird der Trojaner 3.ETZ, der vor allem Windows-Systeme befällt, auf den Rechner des Nutzers geladen. Versandt wird die Welle fast ausschließlich von deutschen IP-Adressen. Der Trusted-Shops-Käuferschutz wird für Online-Shops angeboten, die das Trusted-Shops-Gütesiegel tragen und sichert den Kunden im Fall der Nichtlieferung oder nach Rückgabe der Ware gegen den Verlust seiner Kaufpreiszahlung ab.

Eleven rät Nutzern, solche E-Mails sofort zu löschen und in keinem Fall den Dateianhang anzuklicken. Besondere Vorsicht gilt generell bei vermeintlich harmlos wirkenden Dateianhängen: Oftmals tarnen die Online-Betrüger die Anhänge als Word- (.doc) oder PDF-Dokumente (.pdf), obwohl es sich tatsächlich um eine ausführbare Date (.exe) handelt. Wenn Nutzer sich nicht sicher sind, ob eine E-Mail, die beispielsweise eine angebliche Rechnung oder ähnliches enthält, echt ist, sollte der Anhang in keinem Fall geöffnet werden. Stattdessen sollte die Website des Anbieters, die oft einen Kundenbereich anbieten, in dem auch Rechnungen abrufbar sind, aufgesucht oder der Anbieter direkt kontaktiert werden.

**Portrait**

Eleven - E-Mail-Sicherheit Made in Germany
Eleven ist führender E-Mail-Sicherheitsanbieter aus Deutschland und bietet mit der Technologie eXpurgate einen weltweit einzigartigen Spam-Filter und E-Mail-Kategorisierungsdienst, der zuverlässig vor Spam- und Phishing-E-Mails schützt, potenziell gefährliche E-Mails erkennt und darüber hinaus zwischen individuellen Nachrichten und jeglicher Art von Massen-E-Mails unterscheidet. Zusätzlich bietet eXpurgate umfangreiche Virenschutzoptionen und eine leistungsfähige E-Mail-Firewall.

Mehr als 45.000 Unternehmen jeder Größe nutzen die Lösungen von Eleven. Täglich werden über 1 Milliarde E-Mails von Eleven geprüft und kategorisiert. Zu den Kunden gehören neben Internet Service Providern und Telekommunikationsdienstleistern wie T-Online, O2, 1&1 und freenet zahlreiche namhafte Unternehmen und öffentliche Einrichtungen, darunter Air Berlin, BMW, der Bundesverband deutscher Banken, DATEV, die Freie Universität Berlin, die Landesbank Berlin, RTL, SAP, ThyssenKrupp oder die Tobit Software AG. Mehr Informationen unter http://www.eleven.de.

News-ID: 699414 • Views: 655 (Stand: 01.08.2026)

Link zur Pressemitteilung:
https://www.openpr.de/news/699414/Malware-Angriffe-per-E-Mail-gegen-Nutzer-von-Online-Shops.html