Sicherheitswarnung: Malware statt Reiseunterlagen

Gefälschte Buchungsbestätigungen locken in die Schadcode-Falle

(ddp direct) Die Ferienzeit rückt näher und viele Menschen nutzen das Internet, um sich eingehend über Reiseziele zu informieren oder gleich den ganzen Urlaub bequem im Internet zu buchen. So haben bereits im vergangenen Jahr mehr als 14 Millionen Deutsche eine Reise im Internet gebucht (Quelle VuMa 2011). Diesen Trend greifen Online-Kriminelle in einer aktuellen Kampagne auf. Die Täter versenden seit dieser Woche massenhaft Spam-Mails mit vermeintlichen Hotel-Buchungsbestätigungen. Statt der Reiseunterlagen befindet sich im Dateianhang ein gefährlicher Banking-Trojaner, der es auf das Online-Konto der ahnungslosen Empfänger abgesehen hat. Der Schädling wird bereits von G Data Sicherheitslösungen erkannt und abgewehrt.

Die Täter wissen, dass immer mehr Menschen ihren Urlaub online buchen und auf ihre Reise-, Flug- oder Hotelbestätigungen warten. Im vorliegenden Fall missbrauchen die Täter den Namen des beliebten Reiseportals Booking.com als vermeintlichen Absender. Nach dem Öffnen des Dateianhangs versucht sich ein gefährlicher Banking-Trojaner zu installieren, der es auf das Online-Konto der Opfer abgesehen hat, erklärt Ralf Benzmüller, Leiter der G Data SecurityLabs. Es ist nicht auszuschließen, dass in den kommenden Wochen weitere namhafte Reise-Anbieter für ähnliche Kampagnen missbraucht werden. Verbraucher, die ihren Urlaub online buchen, sollten genau prüfen, ob der Absender der Buchungsbestätigung mit dem Reiseanbieter übereinstimmt. Zudem sollten Empfänger bei gepackten Archiven verstärkt Vorsicht walten lassen und im Zweifelsfall den Anbieter kontaktieren. Der Einsatz einer leistungsfähigen Sicherheitslösung sollte ebenso obligatorisch sein, wie die unmittelbare Installation von Programm- oder Betriebssystem-Updates, um bestehende Sicherheitslücken zu schließen.

Schädling hat es auf das Bankkonto abgesehen
Der eingesetzte Schädling gehört nach Analysen der G Data SecurityLabs zur Banking-Trojaner-Familie Bebloh. Das Schadprogramm fällt immer wieder durch besonders ausgefeilte Angriffstaktiken auf, z.B. durch den sogenannten Retouren-Angriff. Hierbei wird durch eine Manipulation der angezeigten Online-Banking-Seite, dem Kunden ein fehlgeleiteter Zahlungseingang mit der Bitte um Rücküberweisung vorgegaukelt. Für den Kunden ist der Betrug nur schwer zu enttarnen, da der Betrag ebenfalls in der Kontoübersicht angezeigt wird. Dieser Angriff funktioniert unabhängig vom verwendeten TAN-Verfahren, da der Nutzer die Überweisung selbst ausführt und legitimiert.

Banking-Trojaner
Manipulationen durch Banking-Trojaner finden in spezifischen Dateien des Arbeitsspeichers statt. Herkömmliche Antivirenlösungen erkennen am ersten Tag jedoch nur 27 Prozent dieser Schädlinge. Mit G Data BankGuard hat der deutsche IT-Security-Hersteller eine neue Technologie entwickelt, die einen effektiven Schutz vor Banking-Trojanern bietet und die kritische Sicherheitslücke schließt.

G Data BankGuard ist mit allen am Markt befindlichen Antiviren-Lösungen kompatibel und ist bereits fester Bestandteil der G Data Security-Lösungen für Privatanwender ab der Produktgeneration 2012.

Weitere Informationen zur G Data BankGuard-Technologie: http://www.gdata.de/onlineshop/produkt/shop/2-privatanwender/1766-g-data-bankguard.html

Shortlink zu dieser Pressemitteilung:
http://shortpr.com/p7mdmx

Permanentlink zu dieser Pressemitteilung:
http://www.themenportal.de/wirtschaft/sicherheitswarnung-malware-statt-reiseunterlagen-60191

=== Gefälschte Buchungsbestätigungen locken in die Schadcode-Falle (Bild) ===

Die Ferienzeit rückt näher und viele Menschen nutzen das Internet, um sich eingehend über Reiseziele zu informieren oder gleich den ganzen Urlaub bequem im Internet zu buchen. So haben bereits im vergangenen Jahr mehr als 14 Millionen Deutsche eine Reise im Internet gebucht (Quelle VuMa 2011). Diesen Trend greifen Online-Kriminelle in einer aktuellen Kampagne auf. Die Täter versenden seit dieser Woche massenhaft Spam-Mails mit vermeintlichen Hotel-Buchungsbestätigungen. Statt der Reiseunterlagen befindet sich im Dateianhang ein gefährlicher Banking-Trojaner, der es auf das Online-Konto der ahnungslosen Empfänger abgesehen hat. Der Schädling wird bereits von G Data Sicherheitslösungen erkannt und abgewehrt.

Shortlink:
http://shortpr.com/1uyqm9

Permanentlink:
http://www.themenportal.de/bilder/gefaelschte-buchungsbestaetigungen-locken-in-die-schadcode-falle

=== Beispiel einer gefälschten Buchungsbestätigung mit Malware-Anhang (Bild) ===

Der eingesetzte Schädling gehört nach Analysen der G Data SecurityLabs zur Banking-Trojaner-Familie Bebloh. Das Schadprogramm fällt immer wieder durch besonders ausgefeilte Angriffstaktiken auf, z.B. durch den sogenannten Retouren-Angriff. Hierbei wird durch eine Manipulation der angezeigten Online-Banking-Seite, dem Kunden ein fehlgeleiteter Zahlungseingang mit der Bitte um Rücküberweisung vorgegaukelt. Für den Kunden ist der Betrug nur schwer zu enttarnen, da der Betrag ebenfalls in der Kontoübersicht angezeigt wird. Dieser Angriff funktioniert unabhängig vom verwendeten TAN-Verfahren, da der Nutzer die Überweisung selbst ausführt und legitimiert.

Shortlink:
http://shortpr.com/q009k7

Permanentlink:
http://www.themenportal.de/bilder/beispiel-einer-gefaelschten-buchungsbestaetigung-mit-malware-anhang

=== Ralf Benzmüller, IT-Sicherheitsexperte und Leiter der G Data SecurityLabs (Bild) ===

Die Täter wissen, dass immer mehr Menschen ihren Urlaub online buchen und auf ihre Reise-, Flug- oder Hotelbestätigungen warten. Im vorliegenden Fall missbrauchen die Täter den Namen des beliebten Reiseportals Booking.com als vermeintlichen Absender. Nach dem Öffnen des Dateianhangs versucht sich ein gefährlicher Banking-Trojaner zu installieren, der es auf das Online-Konto der Opfer abgesehen hat, erklärt Ralf Benzmüller, Leiter der G Data SecurityLabs. Es ist nicht auszuschließen, dass in den kommenden Wochen weitere namhafte Reise-Anbieter für ähnliche Kampagnen missbraucht werden. Verbraucher, die ihren Urlaub online buchen, sollten genau prüfen, ob der Absender der Buchungsbestätigung mit dem Reiseanbieter übereinstimmt. Zudem sollten Empfänger bei gepackten Archiven verstärkt Vorsicht walten lassen und im Zweifelsfall den Anbieter kontaktieren. Der Einsatz einer leistungsfähigen Sicherheitslösung sollte ebenso obligatorisch sein, wie die unmittelbare Installation von Programm- oder Betriebssystem-Updates, um bestehende Sicherheitslücken zu schließen.

Shortlink:
http://shortpr.com/unmrau

Permanentlink:
http://www.themenportal.de/bilder/ralf-benzmueller-it-sicherheitsexperte-und-leiter-der-g-data-securitylabs

Pressekontakt

G Data Software AG

Frau Kathrin Beckert
Königsallee b 178
44799 Bochum

presse@gdata.de

Firmenkontakt

G Data Software AG

Frau Kathrin Beckert
Königsallee b 178
44799 Bochum

gdata.de
presse@gdata.de

Die G Data Software AG, mit Unternehmenssitz in Bochum, ist ein innovatives und schnell expandierendes Softwarehaus mit Schwerpunkt auf IT-Sicherheitslösungen. Als Spezialist für Internetsicherheit und Pionier im Bereich Virenschutz entwickelte das 1985 in Bochum gegründete Unternehmen bereits vor mehr als 20 Jahren das erste Antiviren-Programm.G Data ist damit eines der ältesten Securitysoftware-Unternehmen der Welt.

Das Produktportfolio umfasst Sicherheitslösungen für Endkunden, den Mittelstand und für Großunternehmen. G Data Security-Lösungen sind in weltweit mehr als 90 Ländern erhältlich.

Weitere Informationen zum Unternehmen und zu G Data Security-Lösungen finden Sie unter www.gdata.de

Anlage: Bild