Gefälschte Service-Mails locken Online-Banking-Kunden in die Falle

G Data deckt neue Masche zur Verbreitung von ZeuS auf

(ddp direct)Die Experten der G Data SecurityLabs warnen vor einer aktuellen Betrugsmasche, die Online-Banking-Kunden ins Visier nimmt: Internet-Nutzer erhalten Spam-Mails mit dem Hinweis, dass ein Bezahlvorgang nicht funktioniert haben soll. Um diesen zu wiederholen, sollen die Empfänger auf den eingefügten Link klicken, welcher direkt auf eine mit ZeuS-Schadcode verseuchte Internetseite führt. Unbemerkt vom Anwender installiert sich der Schädling bei unzureichend geschützten Rechnern automatisch per Drive-by-Download. Die Schadfunktion des Computerschädlings hat es auf Online-Banking-Geschäfte abgesehen. G Data rät Empfängern derartiger Spam-Mails diese direkt zu löschen und auf keinen Fall die eingebundenen Links anzuklicken. Im Zuge des Weihnachtsgeschäfts rechnet G Data mit einem vermehrten Aufkommen von Spam-Mails, die Anwender in die Schadcode-Falle locken sollen.

Bei den bisher entdeckten Spam-Mails geben die Absender sich als Bankberater aus, die ihre Kunden über eine angeblich nicht durchgeführte Transaktion informieren. Die enthaltene Transaktions-ID ist zufällig gewählt und bezieht sich daher nicht auf einen realen Bezahlvorgang. Beim diesem Spam-Versand missbrauchen die Täter die Namen diverser internationaler Banken. Deutsche Empfänger können die gefälschten Bank-Mails leicht enttarnen, da die bisher aufgetretenen Exemplare alle in Englisch verfasst wurden.

Die in den Mails eingebunden Links verweisen auf verschiedene Webseiten, auf der der Anwender zunächst aufgefordert wird, ein Update für seinen Adobe Flash Player herunterzuladen. Dieses Software-Update ist gefälscht und enthält ZeuS-Schadcode. Die Internetseite an sich ist allerdings auch mit einem verschleierten JavaScript verseucht. Das vom JavaScript gestartete Programm startet über eine alte und bereits bekannte Java-Schwachstelle einen Angriff auf den PC und versucht so, ZeuS-Malware einzuschleusen. G Data-Kunden sind auch von der aktuellen Version von ZeuS geschützt. Die G Data Sicherheitslösungen erkennen und blocken den Schädling.

G Data Sicherheitstipps

- Anwender sollten alle Mails ungelesen löschen, die von Dienstleistern stammen, die sie nicht nutzen oder dessen Mails sie nicht abonniert haben. Angehängte Dateien sollten auf keinen Fall geöffnet und eingebundene URLs nicht angeklickt werden. Diese könnten ansonsten eine Schadcode-Infektion zur Folge haben
- Bankdaten oder andere persönliche Informationen sollten Nutzer niemals per Mail oder auf dubiosen Webseiten angeben.
- Um sich auf einer Webseite einzuloggen, sollte nicht der Link in der E-Mail angeklickt werden. Anwender sollten die URL manuell eintippen oder die Favoriten-Funktion des Browsers nutzen.
- Auf dem Computer sollte eine umfassende und leistungsstarke Sicherheitslösung installiert sein, um sich gegen Online-Bedrohungen abzusichern.

Mehr Information zu dieser Spam-Masche im G Data SecurityBlog: http://blog.gdatasoftware.com/blog/article/various-money-related-spams-serve-as-versatile-attack-vector-to-spread-zeus.html

Mehr Informationen über kriminelle Maschen bei Mails sind im G Data Whitepaper Gefährliche E-Mails erhältlich: http://www.gdata.de/virenforschung/info/whitepaper.html

Shortlink zu dieser Pressemitteilung:
http://shortpr.com/7cpf3l

Permanentlink zu dieser Pressemitteilung:
http://www.themenportal.de/internet/gefaelschte-service-mails-locken-online-banking-kunden-in-die-falle-36479

=== Online-Gangster machen Jagd auf Bankkunden (Bild) ===

Bei den bisher entdeckten Spam-Mails geben die Absender sich als Bankberater aus, die ihre Kunden über eine angeblich nicht durchgeführte Transaktion informieren. Die enthaltene Transaktions-ID ist zufällig gewählt und bezieht sich daher nicht auf einen realen Bezahlvorgang. Beim diesem Spam-Versand missbrauchen die Täter die Namen diverser internationaler Banken. Deutsche Empfänger können die gefälschten Bank-Mails leicht enttarnen, da die bisher aufgetretenen Exemplare alle in Englisch verfasst wurden.

Shortlink:
http://shortpr.com/wu73u8

Permanentlink:
http://www.themenportal.de/bilder/online-gangster-machen-jagd-auf-bankkunden

=== Spam-Mail lockt in die Zeus-Falle (Bild) ===

Die in den Mails eingebunden Links verweisen auf verschiedene Webseiten, auf der der Anwender zunächst aufgefordert wird, ein Update für seinen Adobe Flash Player herunterzuladen. Dieses Software-Update ist gefälscht und enthält ZeuS-Schadcode. Die Internetseite an sich ist allerdings auch mit einem verschleierten JavaScript verseucht. Das vom JavaScript gestartete Programm startet über eine alte und bereits bekannte Java-Schwachstelle einen Angriff auf den PC und versucht so, ZeuS-Malware einzuschleusen.

Shortlink:
http://shortpr.com/z6h8ke

Permanentlink:
http://www.themenportal.de/bilder/spam-mail-lockt-in-die-zeus-falle

=== G Data Software AG (Bild) ===

G Data Software AG

Shortlink:
http://shortpr.com/fllr8t

Permanentlink:
http://www.themenportal.de/bilder/g-data-software-ag-85861

=== Im aktuellen Report "Gefährliche E-Mails" erklären die G Data Sicherheitsexperten die gängigsten Maschen der Spammer. (Dokument) ===

Das Kommunikationsmedium E-Mail ist in der heutigen Zeit aus dem Berufsalltag und auch aus dem Privatbereich nicht mehr wegzudenken. Der Versand von E-Mails ist extrem kostengünstig und schnell und das bei einer weltweiten Reichweite.

Anwender benutzen zum Arbeiten mit E-Mails installierte Programme auf ihrem Rechner (E-Mail Clients) oder rufen die E-Mails per Browser ab. Eine derart beliebte Funktion lockt natürlich auch Betrüger an, die technische Unzulänglichkeiten ausnutzen.

Die Abwicklung des Versands und Empfangs von Mails wird dabei im Hintergrund vorgenommen und der Anwender bekommt davon im Idealfall nichts mit. Das Protokoll zum Versand nennt sich SMTP, Simple Mail Transfer Protocol. Empfangen werden E-Mails über POP3 (Post Office Protocol,Version 3) oder IMAP (Internet Message Access Protocol).

Der Aufbau von elektronischer Post ist, ähnlich wie bei einer Postkarte, aufgeteilt. Auf der einen Seite, im Informationsteil (Header), werden Absenderdaten, Empfängerdaten, Datum, Betreff etc.untergebracht. Der zweite Bestandteil ist der Textteil (Body), der den eigentlichen Inhalt transportiert.

Da beim Versand einer Mail im SMTP keine Authentifizierung des Klartextes stattfindet, kann an dieser Stelle geschummelt werden: Es ist zum Beispiel möglich, die Absenderadresse im Header zu ändern und so dem Empfänger eine falsche Identität vorzugaukeln. Auch Inhalte können ohne großen Aufwand manipuliert werden.

Bei all den schon erwähnten positiven Eigenschaften von E-Mails gibt es allerdings auch die andere Seite der Medaille: Das E-Mail Postfach quillt schon wieder über, der Großteil der empfangenen Mails ist unerwünschte Post mit zwielichtigen Werbeversprechen, Traumjobangeboten, Flirteinladungen und ähnliches. Was die Computeranwender dieser Welt täglich nervt ist ïÂ•Â?Spam1.

Diese unaufgefordert und massenhaft empfangenen Mails sind nicht nur wegen ihrer hohen Anzahl störend, sondern können auch gefährlich sein.

Betrügerische und gefährliche E-Mails kommen in vielen verschiedenen Varianten. Als unerwünschte Werbemail, Phishing, Malware mit Dateianhang oder einem Link auf präparierte Webseiten. Bevor im folgenden Kapitel die einzelnen Vorgehensweisen und Maschen der E-Mail-Betrüger genau beschrieben werden, wollen wir noch einige Hintergründe beleuchten.

Shortlink:
http://shortpr.com/v6l9p2

Permanentlink:
http://www.themenportal.
de/dokumente/im-aktuellen-report-gefaehrliche-e-mails-erklaeren-die-g-data-sicherheitsexperten-die-gaengigsten-maschen-der-spammer

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. Seit mehr als fünf Jahren hat zudem kein anderer europäischer Hersteller von Security-Software häufiger nationale und internationale Testsiege und Auszeichnungen errungen als G Data.

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