



Gefälschte LinkedIn E-Mails locken in die Schadcode-Falle

G Data deckt neue eCrime-Masche auf und verzeichnet einen Anstieg von Mails mit Links zu Schadcode-Webseiten

(ddp direct) Spam-Mails sind bei Cyber-Kriminellen sehr beliebt und werden von den Tätern nicht nur für Phishing-Attacken genutzt, sondern auch zur Initiierung von Schadcode-Angriffen. Die G Data SecurityLabs beobachten eine steigende Anzahl dieser Angriffsmethode. Dabei werden die Mail-Empfänger auf eine präparierte Webseite gelockt um den Rechner mit einem Schadprogramm zu infizieren. Im aktuellen Fall setzen die Täter auf den Versand von angeblichen Kontaktanfragen des sozialen Netzwerks LinkedIn. Die verschickten Mails enthalten Links zu Webseiten, auf denen Exploit-Kits hinterlegt sind. Besucht ein Mail-Empfänger eine dieser Seiten, wird der Rechner auf Schwachstellen in der installierten Software hin überprüft, z.B. nicht installierte Patches. Ist die Suche erfolgreich, wird beliebiger Schadcode nachgeladen, um z.B. Zugangsdaten zu Online-Bankkunden oder Mail-Postfächer zu stehlen. G Data Kunden sind vor den gefährlichen Webseiten geschützt. Dennoch rät der deutsche IT-Security-Hersteller dazu, den Rechner mit Hilfe von bereitgestellten Updates für das Betriebssystem und die installierten Programme stets auf dem aktuellsten Stand zu halten.

Exploit-Kits als profitables eCrime-Geschäft

Der Einsatz von Exploit-Kits ist bei Cyber-Kriminellen beliebt um Schwachstellen in PCs zu ermitteln und sie anschließend für gezielte Schadcode-Angriffe auszunutzen. Dabei lassen sich Exploit-Kits auch von nicht so erfahrenen Online-Tätern leicht einsetzen. In speziellen Untergrund Märkten wird daher eine Fülle von Exploit-Kits und ganze Angriffs-Pakete angeboten, die alle nötigen Dienstleistungen enthalten, die für einen Angriff nötig sind.

Sicherheitstipps für Internetnutzer

* Der Einsatz einer aktuellen und umfassenden Sicherheitslösung mit einem Virens Scanner, Firewall, Web- und Echtzeitschutz gehört zur Grundausstattung eines PCs. Diese sollte auch ein Spam-Filter zur Abwehr ungewollter Spam-Mails umfassen.

* Das installierte Betriebssystem und die eingesetzte Software sollten durch regelmäßige Updates immer auf den neuesten Stand gehalten werden um Sicherheitslücken durch veraltete Programme zu schließen.

* Spam-Mails sollten am besten umgehend und ungelesen gelöscht werden. Darin enthaltene Links und Datei-Anhänge sollten nicht angeklickt werden, die könnten geradewegs in die Schadcode-Falle führen.

Shortlink zu dieser Pressemitteilung:

<http://shortpr.com/d73mjnb>

Permanenterlink zu dieser Pressemitteilung:

<http://www.themenportal.de/wirtschaft/gefaelschte-linkedin-e-mails-locken-in-die-schadcode-falle-34317>

=== Gefälschte LinkedIn-Kontaktanfrage (Bild) ===

Spam-Mails sind bei Cyber-Kriminellen sehr beliebt und werden von den Tätern nicht nur für Phishing-Attacken genutzt, sondern auch zur Initiierung von Schadcode-Angriffen. Die G Data SecurityLabs beobachten eine steigende Anzahl dieser Angriffsmethode. Dabei werden die Mail-Empfänger auf eine präparierte Webseite gelockt um den Rechner mit einem Schadprogramm zu infizieren. Im aktuellen Fall setzen die Täter auf den Versand von angeblichen Kontaktanfragen des sozialen Netzwerks LinkedIn. Die verschickten Mails enthalten Links zu Webseiten, auf denen Exploit-Kits hinterlegt sind. Besucht ein Mail-Empfänger eine dieser Seiten, wird der Rechner auf Schwachstellen in der installierten Software hin überprüft, z.B. nicht installierte Patches. Ist die Suche erfolgreich, wird beliebiger Schadcode nachgeladen, um z.B. Zugangsdaten zu Online-Bankkunden oder Mail-Postfächer zu stehlen. G Data Kunden sind vor den gefährlichen Webseiten geschützt. Dennoch rät der deutsche IT-Security-Hersteller dazu, den Rechner mit Hilfe von bereitgestellten Updates für das Betriebssystem und die installierten Programme stets auf dem aktuellsten Stand zu halten.

Shortlink:

<http://shortpr.com/13gkqv>

Permanenterlink:

<http://www.themenportal.de/bilder/gefaelschte-linkedin-kontaktanfrage>

=== G Data deckt neue eCrime-Masche auf und verzeichnet einen Anstieg von Mails mit Links zu Schadcode-Webseiten (Dokument) ===

Spam-Mails sind bei Cyber-Kriminellen sehr beliebt und werden von den Tätern nicht nur für Phishing-Attacken genutzt, sondern auch zur Initiierung von Schadcode-Angriffen. Die G Data SecurityLabs beobachten eine steigende Anzahl dieser Angriffsmethode. Dabei werden die Mail-Empfänger auf eine präparierte Webseite gelockt um den Rechner mit einem Schadprogramm zu infizieren. Im aktuellen Fall setzen die Täter auf den Versand von angeblichen Kontaktanfragen des sozialen Netzwerks LinkedIn. Die verschickten Mails enthalten Links zu Webseiten, auf denen Exploit-Kits hinterlegt sind. Besucht ein Mail-Empfänger eine dieser Seiten, wird der Rechner auf Schwachstellen in der installierten Software hin überprüft, z.B. nicht installierte Patches. Ist die Suche erfolgreich, wird beliebiger Schadcode nachgeladen, um z.B. Zugangsdaten zu Online-Bankkunden oder Mail-Postfächer zu stehlen. G Data Kunden sind vor den gefährlichen Webseiten geschützt. Dennoch rät der deutsche IT-Security-Hersteller dazu, den Rechner mit Hilfe von bereitgestellten Updates für das Betriebssystem und die installierten Programme stets auf dem aktuellsten Stand zu halten.

Shortlink:

<http://shortpr.com/0c52rc>

Permanenterlink:

<http://www.themenportal.de/dokumente/g-data-deckt-neue-ecrime-masche-auf-und-verzeichnet-einen-anstieg-von-mails-mit-links-zu-schadcode-webseiten>

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

