- **Sollte dieser Newsletter bei Ihnen nicht einwandfrei angezeigt werden, beachten Sie bitte die beigefügte Version als PDF.**

SPAM-Welle nach den Anschlägen in Frankreich

Art der Bedrohung

SPAM-Mails (Hoax) und Massennachrichten in den sozialen Medien mit dem Betreff „On Est Tous Paris“, „We are all Paris“ oder „Wir sind Paris“. Die Meldung warnt vor dem Erhalt einer E-Mail oder Nachricht mit dem obigen Betreff, welche einen Trojaner enthält.

Modus Operandi

Internationalen und nationalen Informationsquellen zufolge, verbreitet sich seit Sonntag die Warnmeldung vor dem „On Est Tous Paris“-Trojaner wie ein Lauffeuer. In der Mitteilung selbst wird vor dem Erhalt einer E-Mail und Mitteilungen in den sozialen Medien gewarnt, in welcher sich ein Bild mit der Hand eines Babys befindet. Auf dem Namensband ist dabei die Aufschrift „On Est Tous Paris“, „We are all Paris“ oder „Wir sind Paris“ vermerkt.

Derzeit gibt es keine gesicherten Hinweise darauf, dass diese Nachricht tatsächlich existiert, zumal es weder das „Cyber Service Crime French Ministry od Defense“ gibt, noch der in der Mail angeführte „Broadcast“ durch den Sender „Europe 1“ stattgefunden haben soll.

Trotzdem ist besondere Vorsicht geboten!

Nach dem Terror-Anschlag auf „Charlie Hebdo“ wurde genau diese beschriebene Nachricht für die Verbreitung eines Trojaners und damit verbundenen Hacker-Angriffen benutzt. Da der damals benutze Trojaner zu diesem Zeitpunkt sehr neu war, wurde er auch kaum von Antivirensoftware erkannt und waren zahlreiche Computersysteme davon betroffen. Ein ähnliches oder Wiederholungs-Szenario kann somit nicht ausgeschlossen werden.

Empfohlene Vorgangsweisen:

- Verbreiten Sie bitte derartige Nachrichten und Informationen nicht ungeprüft weiter, suchen Sie im Internet nach Updates zu den jeweiligen Sachverhalten.
- Beteiligen Sie sich bitte nicht „unbewußt“ an der Verbreitung von SPAM-Mails, vermeiden Sie ungewollte Panikmache und Verunsicherung anderer.
- Öffnen Sie keinesfalls Ihnen unbekannte Dateianhänge, insbesondere wenn es sich um die beschriebenen oder ähnlichen Mitteilungen handelt .
- Wenn Sie sich unsicher sind, öffnen Sie derartige Dateien in einer gesicherten Umgebung

(Sandbox, virtuelle Systeme mit Option auf Rücksetzung) oder bedienen Sie sich unterstützenden Seiten im Internet (z.B. Virustotal.com).

- Halten Sie Ihre System-Software sowie Viren- und Malwareschutz aktuell, machen Sie regelmäßig Updates.
- Legen Sie sich für die Ihnen wichtigen Daten regelmäßig Daten-BackUps an, verwahren Sie das Sicherungsmedium getrennt vom System.
- Beachten Sie die Sicherheitshinweise und Tipps, für einen Sicheren Umgang mit dem Internet und Schutz vor IT-Kriminalität der Kriminalprävention: http://www.bmi.gv.at.

Die englische Version der vermutlichen Falschmeldung:

- **"You might receive an email called " We All Paris "that has been widely disseminated since this WEEKEND. In this message a baby photo with a bracelet saying "we are all PARIS " prompts you to click on the photo ! DO NOT CLICK this message. It contains malware (viruses) that can take away from your phone or computer control and retrieve all your data and passwords [Source:. Cyber Service Crime French Ministry of Defense]. So, send this message to your contacts. It is urgent and it's going very fast, and it has been circulating since Sunday. The confirmation of this information was broadcast on Europe 1 this morning (sic).**

Ein für die Verbreitung des „Charlie Hebdo" – Trojaners verwendetes Bild:

Weitere Quellen:

- Artikel der Huffingtompost Frankreich in französischer Sprache betreffend der Fake-Mail: http://www.huffingtonpost.fr/2015/11/16/mail-on-est-tous-paris-fake-fausse-alerte_n_8573180.html
- Artikel von HowToRemove.Guide betreffend der Fake-Mail-Warnung in englischer Sprache: http://howtoremove.guide/on-est-tous-paris-virus-hoax-surges-in-france/
- Artikel von Mimikama.at über den „Charlie Hebdo“-Trojaner: http://www.mimikama.at/allgemein/achtung-charlie-hebdo-trojaner-unterwegs/

HERAUSGEBER: Bundesministerium für Inneres
Bundeskriminalamt
A-1090 Wien, Josef Holaubek Platz 1
Tel.: +43 1 24836 986500

FEEDBACK

NEWSLETTER AN-/ABMELDUNG