

FBI warnt vor Storm-Wurm und Botnetzen

Behörde fordert "Internet-Intelligenz" von Usern - Social-Engineering-Angriff mit ungewöhnlichem Thema

Das [FBI](#) hat in dieser Woche vor E-Mails gewarnt, die mit Malware-Links das Zombie-PC-Netz des Wurms "Storm" zu vergrößern suchen. Eine angebliche FBI-Überwachung auf der Social-Networking-Seite Facebook war das Thema, mit dem Nutzer auf verseuchte Webseiten gelockt werden sollten. "Das war ein typischer Social-Engineering-Angriff mit einem ungewöhnlichen Thema", urteilt Rainer Link, Senior Security Specialist Anti-Malware bei [Trend Micro](#), im Gespräch mit presstext. Diese Themenwahl zielt auf großes Interesse unter Usern und somit viele Opfer ab. Nicht geplant war wohl der Nebeneffekt, dass das FBI publikumswirksam Internet-Intelligenz von Nutzern fordert und über Botnetze aufklärt. E-Mail-Titel wie "FBI bypasses Facebook to nail you" ("Das FBI umgeht Facebook, um Sie festzunageln") waren es, die bei der aktuellen Storm-Kampagne das Interesse der Nutzer zu wecken suchten.

Infektion

Wer auf der verlinkten Webseite mehr über die Spionage der Behörde auf Facebook erfahren wollte, wurde mit Storm infiziert und dadurch Teil des Wurm-Botnetzes. Reagiert hat darauf auch das FBI, das angesichts des Themas vor Storm und Botnetzen allgemein gewarnt hat. Das dürfte aber kaum Ziel der E-Mail-Kampagne gewesen sein. "Wenn das FBI warnt, ist das öffentliche Interesse in den USA deutlich höher", erklärt Link. Somit könnten mehr User über Würmer und Botnetze aufgeklärt werden als bei üblichen Storm-Wellen. "Wir fordern Bürger auf, Internet-intelligent zu werden, um dadurch Verbreitung von Botnetzen zu bremsen", so FBI Special Agent Richard Kolko anlässlich der aktuellen Storm-Welle. Als Beispiele für kriminelle Aktivitäten, für die Computer ahnungsloser Nutzer in Botnetzen missbraucht werden könnten, führt die Behörde Identitätsdiebstahl, Denial-of-Service-Angriffe, Phishing, Klick-Betrug und die Massenverteilung von Spam und Spyware an. Weiters hat das FBI auf ihr [Internet Crime Complaint Center](#) aufmerksam gemacht und User zu verantwortungsvollem Verhalten im Umgang mit E-Mails ermahnt.

Forderungen

Nicht auf Spam zu reagieren und keine Links oder Attachments in unbekanntem Mails zu öffnen, sind die Kernforderungen des FBI. Dass E-Mails mit böartigen Dateianhängen nach wie vor eine Bedrohung sind, betont auch Link. "Wir waren etwas überrascht, wie viele Kampagnen mit Attachments es in letzter Zeit gegeben hat", so der Malware-Experte zu presstext. Vor kurzem beobachtet wurden beispielsweise Trojaner in Form angeblicher Rechnungen von UPS und PayPal. Letztere wurden Ende Juli auch in einer lokalisierten deutschen Version verschickt. Es sei denkbar, dass Cyberkriminelle mit der Nutzung der vermeintlich veralteten Verbreitungsmethode eine höhere Malware-Reichweite erzielen wollen, so Link. "Es gibt schließlich unterschiedliche Arten von Usern", erklärt der Malware-Experte. Wer bei URLs vorsichtig sei, sei das leider nicht unbedingt auch bei Anhängen. (pte)