Kassandra – A Firefox Security Demonstration Add-On

IT Security / Betreuer: Dr. Emmanuel Benoist
Experte: Armin Blum

Anhand einer Erweiterung, eines sogenannten Add-Ons, konnten wir diverse Schwachstellen im Design des Firefox Browser aufdecken. Wir waren in der Lage, bestehende Sitzungen (Ebay, Gmail…) zu übernehmen, die Tastaturschläge des Benutzers aufzuzeichnen, Passwortfelder zur Laufzeit zu manipulieren und private Dateien auf dem Laufwerk auszuspähen. Verschiedene Viren- und Internetscanner waren nicht in der Lage, Kassandra zu entdecken. Ein weiteres Highlight ist das Verstecken und Auslesen von geheimen Nachrichten in Bildern auf Google+.

Firefox und seine Erweiterungen

Der Web-Browser nimmt in unserer vernetzten Gesellschaft einen immer grösseren Stellenwert ein, und dieser Trend wird sich mit den fortschreitenden technischen Möglichkeiten noch einmal vergrössern.
Die **Version 1.0** von Firefox wurde Ende 2004 veröffentlicht, und seitdem konnte der quelloffene Browser seinen Marktanteil auf gut 25 Prozent ausbauen, dies nicht zuletzt wegen seinen Erweiterungen, den sogenannten **Add-Ons**, deren Sicherheit wir uns in dieser Bachelor-Thesis gewidmet haben.

Der Fuchs im Schafspelz

Ein Benutzer, so unerfahren er auch sein mag, würde sich kein Add-On installieren, wenn er auf den ersten Blick sehen würde, dass es seine Passwörter und Login-Daten stehlen würde. Deshalb haben wir ein sogenanntes Overlay programmiert, das dem Benutzer die aktuellen Angebote der Detailhandelskette **Denner** anzeigt. Auf Knopfdruck erscheint dann unser richtiges Add-On namens **Kassandra** (Seherin und Tochter des Trojanischen Königs Priamos, die die Trojaner vor der List der Griechen warnte). Wir haben unsere Arbeit so benannt, weil wir uns wie die Griechen einer List bedienen, um den Benutzer dazu zu bewegen, unsere Erweiterungen zu installieren.

Ein Add-On, viele Möglichkeiten

Nachdem sich ein Benutzer Kassandra installiert hat (über Social-Engineering oder über einen anderen Kanal) stehen uns folgende Möglichkeiten offen, um persönliche und private Daten des User auszuspionieren sowie ihn auf falsche Seiten zu leiten:

- *Keylogging* – Aufzeichnen der Tastaturschläge inklusive Screenshot der besuchten Seite
- *Redirection* – Fernsteuern auf fremde Seiten
- *Session Hijacking* – Übernahme einer laufenden Sitzung (Ebay, Ricardo, GMail…)
- *Server Socket* – Verbindung per Telnet auf den Rechner des Benutzers (Lesen / Schreiben von Dateien auf der Festplatte, Verändern der Lesezeichen, Durchsuchen des Verlaufes…)
- *DOM Manipulation* – Ersetzen von Formularen und auslesen von gespeicherten Passwörtern
- *Spoofing* – Weiterleitung auf einen anderen Server und Täuschung des Benutzers, damit er sich bei einer fremden Seite anmeldet (GMail / Yahoo Mail)
- *Kryptographie* – Verschlüsselte Dateien zur Laufzeit in ein Objekt mit lauffähigem Code umwandeln zur Täuschung von Malware-Scannern

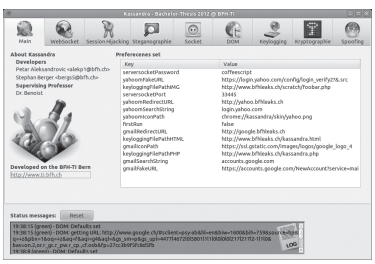
Das letzte Feature von Kassandra könnte z. B. von Regimegegnern in unterdrückten Ländern verwendet werden:

- *Steganographie* – Das Verstecken von geheimen Nachrichten in Bildern auf Google+

Unter dem Radar

Verschiedene Tests mit Viren- und Internetscannern von namhaften Anbietern verliefen positiv in dem Sinne, dass Kassandra **unentdeckt** geblieben ist, und zwar bei allen oben vorgestellten Funktionen. Dies zeigt deutlich, dass im Hinblick auf die Sicherheit von Browsern noch eine Menge Potential vorhanden ist, um den Benutzern die grösstmögliche Sicherheit gewährleisten zu können.

Denner Promotions – Das Overlay für Kassandra



Der Hauptbereich von Kassandra

Petar Aleksandrovic
petar.aleksandrovic@gmail.com

Stephan Berger