

F-Secure Threat Report 2014: Erstes Halbjahr durch Ransomware geprägt, auch Android-Geräte stehen im Visier der Erpresser

Die erste Hälfte des Jahres 2014 zeigte sich wahrhaftig erpresserisch – es konnte ein Anstieg der Online-Attacken auf User verzeichnet werden, bei denen es nur darum ging, die Daten der User zu sperren und gegen ein Lösegeld zu erpressen. Auch mobile Endgeräte sind davon betroffen. Laut dem jüngsten Threat Report H1 2014 von F-Secure Labs ist die Datensicherheit von privaten, beruflichen und behördlichen Nutzern anhand der zunehmenden Anzahl von Angriffen mit Schadsoftware wichtiger denn je. Ransomware verlangt die Zahlung einer Summe X im Austausch fürs Entsperrnen von Dateien des Users.

Weiterhin ein Anstieg mobiler Malware – insbesondere bei Android

295 neue Familien und Varianten von mobiler Malware wurden im 2. Quartal 2014 entdeckt, davon eine auf iOS gerichtete Malware. Im Vorquartal waren es noch 277 neue Bedrohungen, wovon 275 auf Android-Geräte abzielten. Zu den Top 3 der Android-Bedrohungen gehören ganz klar Trojaner, die entweder SMS-Nachrichten an Premium-Nummern versenden oder Daten abgreifen und an entfernte Server schicken. Die im Juni veröffentlichte Malware Slocker, die sich als legitime App ausgibt, war die bislang erste bekannte Ransomware, die auf einer mobilen Plattform erschien.

Conficker hält sich wacker, dank veralteter Software

Mit einem Anteil von 31 Prozent macht der sechs Jahre alte Downadup/Conficker Wurm am meisten von sich reden. Er dominiert ganz klar die Top Ten. Der Wurm hat Millionen von Rechnern in mehr als 200

Ländern infiziert – Brasilien belegt dabei Platz 1. Dass der Wurm nach wie vor noch beständig ist, ruht insbesondere auf veralteter bzw. nicht gepatchter Software auf Rechnern, hauptsächlich mit dem Betriebssystem Windows XP. Bezeichnend, wie wichtig es ist, die Software auf dem Rechner aktuell zu halten und alte Sicherheitslöcher zu schließen.

Neue (weitere) Mac Malware aufgetaucht

25 neue Bedrohungen für den Mac haben die finnischen Sicherheitsexperten in der ersten Jahreshälfte entdecken können. Einige davon wurden eingesetzt, um Organisationen anzugreifen. Die Anzahl der Bedrohungen ist zwar im Vergleich zur zweiten Jahreshälfte 2013 um knapp 40 Prozent gestiegen – zwischen Juli und Dezember des Vorjahres waren es 18 Bedrohungen. Verglichen mit der ersten Jahreshälfte 2013 mit 33 Bedrohungen ist die Anzahl um knapp 25 Prozent gesunken.

Im [Webinar am vergangenen Freitag](#) diskutierten Mikko Hypponen, Chief Research Officer, und Sean Sullivan, Security Advisor, beide vom F-Secure Labs, über die Entwicklungen des vergangenen Halbjahres. Unter anderem ging es auch um Havex – ein Trojaner, der überwiegend industrielle Kontrollanlagen zum Ziel hat und den die F-Secure Forscher im Juni entdeckten.

„Anfang dieses Jahres sind Details aufgetaucht, die ein faszinierendes Bild ergeben. Aus Malware mit krimineller Absicht entwickelte sich nun Malware zu Spionagezwecken“, sagt Sullivan. „Die bösen Jungs da draußen sind mittlerweile nicht nur an Kreditkartendaten interessiert. Alles ist nun von Interesse und es gibt wahrscheinlich eine sehr breite Käuferschicht für kritische Unternehmensdaten.“

Im Threat Report finden sich darüber hinaus weitere Informationen, wie etwa:

- Verschiedene Strafverfolgungsbehörden haben das GameOver ZeuS (GOZ) Botnet erfolgreich zerschlagen – doch was ist jetzt als nächstes zu erwarten?
- Die aktuelle Bedrohungslage – der am meisten bemerkenswerte Trend im ersten Halbjahr ist das anhaltende Wachstum von Ransomware. Doch damit nicht Schluss, was noch?
- PC Malware: Die Top Ten der aktuellen Threats – Newcomer sind Wormlink, BrowserExploit und Expiro, sowie die Top Ten der betroffenen Regionen.
- Mobile Malware: Android weiter Angriffsziel Nummer eins.
- Mac Malware: Malware wird immer anspruchsvoller in Bezug auf ihre Fähigkeiten und ihre Verbreitungsmethoden.

Lesen Sie den vollständigen [Threat Report H1 2014](#).

F-Secure – Switch on freedom

F-Secure ist ein Online-Sicherheits- und Datenschutz-Unternehmen aus Finnland. Wir bieten Millionen von Menschen rund um den Globus die Macht, unsichtbar zu surfen, Inhalte zu speichern und zu teilen, sicher vor Online-Bedrohungen. Wir sind hier, um für die digitale Freiheit zu kämpfen. Schließen Sie sich der Bewegung an und schalten Sie um auf Freiheit.