Scareware statt Malware: vom blühenden Geschäft mit „Fake Alerts“

Angst ist ein Brandbeschleuniger für Kriminelle. Kein Wunder also, dass „Scareware“ boomt. SophosLabs enthüllt in seinem jüngsten Report, dass die Angreifer fertige Bausätze verwenden, es mit ihren „Panikanzeigen“ auch auf deutsche Webseiten und mobile Geräte abgesehen haben. Dabei werden Werbenetzwerke zu Tathelfern.

Online-Werbenetzwerke gibt es nicht ohne ihren Parasiten: bösartige Web-Banner. Besonders „Pop-under“-Werbung, die die Pop-up-Blockierungsfunktionen der Browser umgeht, ist ein Problem, denn einige dieser „Pop-unders“ vermitteln ihren Nutzern sehr glaubhaft, dass etwas mit ihren Geräten nicht stimmt. Diese „Fake-Alerts“ nutzen häufig Werbenetzwerke für die Verbreitung von potentiell unerwünschten Anwendungen. Und da sie keinen offensichtlich bösartigen Code enthalten, lösen die meisten keine Anti-Malware-Erkennung aus. Sie sind eine Art „Scareware“-Version böswilliger Werbung - Scarevertising.

Hier die wichtigsten Erkenntnisse aus dem Report:

Warnmeldungsbetrug in deutscher, japanischer und französischer Sprache

Betrügereien, die Webseiten benutzen, die so gestaltet sind, dass sie den Warnmeldungen mobiler Betriebssysteme ähneln, gibt es nicht erst seit gestern. Aber während sich diese Betrügereien in der Vergangenheit weitgehend auf englischsprachige Ziele konzentriert haben, fanden die SophosLabs vermehrt Versionen von „Browser-Lock“-Angriffen, die auf japanisch-, deutsch- und französischsprachige Benutzer abzielen. Einige verwenden dasselbe Windows 10er-Thema, das in den aktuellsten englischen Sprachkits entdeckt wurde, während andere Beispiele älterer Betrugskampagnen des technischen Supports verwenden, die aus mehreren Kits zusammengeschraubt wurden. Sie alle verwenden bösartige Cursor-Skripte.

Ziele der Fake Alerts: Mobile Browser, Android und iOS

Die überwiegende Mehrheit der gefälschten Warnmeldungen, die in Netzwerken mit Malware gefunden wurden, zielte auf mobile Browser ab. Android und iOS sind zu einem beliebten Ziel für Malvertising geworden, da sie zu einem immer größeren Anteil für den Internetverkehr verantwortlich sind – und die Betrüger folgten diesem Trend konsequent. Die meisten gefälschten iOS-Benachrichtigungen verknüpften sich zum Beispiel mit App Store-Angeboten für eine Gruppe von Anwendungen, die sich als Virtual Private Networking- und Site-Blocker-Tools ausgaben.

Auf Desktop-Nutzer wartet kriminelles Telefonmarketing

Während die Zahl der gefälschten Handy-Warnungen zunimmt, sind Betrügereien mit dem Desktop-Support nach wie vor ein altbewährtes Modell, um an das Geld von weniger erfahrenen Computer- und Gerätebenutzer zu kommen. Was als Kaltakquise-Telefonmarketing-Betrug begann, hat sich in den letzten Jahren allmählich zu einem „Pull“-Modell entwickelt, bei dem Web-Inhalte genutzt werden, um die Opfer aktiv zum Callcenter zu bringen. Dort soll ihnen üblicherweise legitime oder betrügerische Malware-Schutzsoftware oder eine andere Dienstleistung verkauft werden, die oft eine dauerhafte Hintertür für spätere Aktivitäten beinhalten. „Pop-up“-Kampagnen sind wahrscheinlich die wirtschaftlichsten und effektivsten Mittel für diese Art von Betrügereien. Da sie das Opfer zum Anruf auffordern, filtern die gefälschten Pop-up-Warnungen standardmäßig weniger skeptische Ziele aus, und sie kosten in der Regel nur Centbeträge pro zugestelltes Ziel.

Fertige Malvertising-Bausätze mit Warnton
Die Malvertising-Seiten sind in der Regel als verpackte Kits (Bündel von vorgefertigten HTML-, JavaScript- und PHP-Dateien, die auf einem Webserver entpackt werden können) erhältlich, die in Foren gekauft oder einfach unverhohlen von anderen Betrügern geklaut werden und nur geringe technische Fähigkeiten erfordern. Alle Kits enthalten Sounddateien und versuchen, diese abzuspielen: zu hören ist bei erfolgreicher Aktivierung zumeist ein Systemton und eine Warnung per Computerstimme vor Systemproblemen.

Missbrauch von App-Stores: Mobilgeräte bleiben anfällig für Malvertising
Zumindest auf dem Desktop gibt es mehrere Möglichkeiten, eine Begegnung mit einer gefälschten Warnseite von vornherein zu verhindern. Pop-Up-Blocker im Browser bieten einen gewissen Schutz vor Pop-Under-Werbung. Reputationsbasierte Blockierungen und Malware-Schutz können ebenfalls viele dieser Websites blockieren (Sophos z.B. blockiert alle Browser-Locker-Websites, die hier als „FakeAlert-B“ identifiziert wurden und verhindert, dass sie geöffnet werden).

Das Problem auf der mobilen Seite bleibt jedoch eine mangelnde Aufmerksamkeit der Nutzer. Während Apple und Google es Betrügern erschwert haben, Browser-Funktionen für ihre Zwecke zu nutzen, ist der „Popup“-Schutz nach wie vor schwach und der Missbrauch von App-Stores weiterhin ein Problem. Da der Schutz vor Malvertising auf Desktops zunimmt, werden sich mehr Betrüger auf die Schwächen mobiler Geräte konzentrieren.

Der ausführliche Report findet sich unter https://news.sophos.com/en-us/2020/09/09/faking-it-the-thriving-business-of-fake-alert-web-scams/ , eine Liste der Hashes und Domänen für die von den SophosLabs beobachteten Landing Pages gibt es unter https://github.com/sophoslabs.

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de