idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Press release

Ruhr-Universität Bochum
Dr. Julia Weiler
07/03/2019
http://idw-online.de/en/news718593

Research results
Information technology, Politics
transregional, national

Code von chinesischer Überwachsungsapp analysiert

Wie eine chinesische Überwachungsapp funktioniert, die Einreisende beim Grenzübertritt aus Kirgistan nach China auf ihrem Handy installieren lassen müssen, haben IT-Sicherheitsforscher der Ruhr-Universität Bochum (RUB) gemeinsam mit einem Rechercheverbund von NDR und Süddeutscher Zeitung (SZ) analysiert. Die Wissenschaftler fanden heraus, dass die App das Handy nach etwa 73.000 bestimmten Dateien durchforstet. Außerdem erstellt sie für den Grenzbeamten einen Bericht, der unter anderem die letzten Telefonaktivitäten, Kontakte, SMS-Nachrichten und genutzten Social-Media-Accounts enthält.

Ihre Ergebnisse veröffentlichten die Wissenschaftler online unter https://dwuid.com/content/analyzing-mobilehunter. Die Medien berichteten am 2. Juli 2019 über die Rechercheergebnisse.

Ein Leser der SZ hatte die Zeitung auf das Verfahren aufmerksam gemacht, bei dem Einreisende ihr entsperrtes Handy an einen Grenzbeamten zur Installation der App übergeben müssen. Daraufhin nahmen die Medienhäuser die Recherche auf und zogen die Expertise von Prof. Dr. Thorsten Holz hinzu. Der Leiter des Lehrstuhls für Systemsicherheit am Horst-Görtz-Institut für IT-Sicherheit der RUB, einer der Sprecher des Exzellenzclusters Casa – kurz für Cyber-Sicherheit im Zeitalter großskaliger Angreifer –, ist Experte für die Analyse von Softwareapplikationen.

Gemeinsam mit seinem Doktoranden Moritz Contag untersuchte er sowohl die eigentliche App als auch speziell zwei Unterprogramme der App, die nur als Maschinencode aus Nullen und Einsen vorlagen. Dieser Code kann direkt vom Prozessor ausgeführt werden, ist aber für Menschen nicht verständlich.

Bericht über Social-Media-Accounts und Telefonaktivitäten

Die analysierte Android-App erstellt einen Bericht, der Informationen enthält wie die im Telefon gespeicherten Kontakte, gesendete SMS-Nachrichten und eine Liste der letzten Anrufaktivitäten inklusive der Funkstelle, mit der das Handy verbunden war. Mithilfe des ersten Unterprogramms werden Informationen darüber gesammelt, welche chinesischen Social-Media-Apps auf dem Handy installiert sind und welche Accounts damit verbunden sind.

Das zweite Unterprogramm durchforstet das Handy nach bestimmten Dateien. Dazu enthält sie eine Liste von 73.315 sogenannten Prüfsummen. Diese werden üblicherweise genutzt, um die Integrität von Dateien sicherzustellen; sie sind eine Art digitaler Fingerabdruck. Lädt man zum Beispiel eine Datei aus dem Internet herunter, wird häufig auch eine dazu passende Prüfsumme angegeben. Nach erfolgtem Download kann der Computer oder das mobile Endgerät die Prüfsumme der heruntergeladenen Datei berechnen und sie mit der erwarteten Prüfsumme vergleichen. Wird die Datei beim Download beschädigt, so stimmen die berechnete und die erwartete Prüfsumme nicht überein. Sind die beiden Werte gleich, ist sichergestellt, dass die Datei unverändert ist.

Auf der Suche nach bestimmten Videos

Jede Datei, also jedes Video, jede Text- oder Audiodatei, hat in der Prüfsumme somit ihren eigenen digitalen Fingerabdruck. Die App berechnet die Prüfsummen für alle auf dem Handy verfügbaren Dateien und gleicht sie mit einer hinterlegten Liste ab. „Aus den Prüfsummen kann man allerdings nicht direkt auf den Inhalt der Datei schließen“, erklärt Thorsten Holz. In dem Unterprogramm der App fanden die Bochumer Forscher neben den Prüfsummen für jede Datei noch eine zweite Information, nämlich die Dateigröße.

Anhand dieser Parameter hat das Team der RUB mehr als 1.300 Dateien identifizieren und dem Rechercheteam von SZ und NDR zur Verfügung stellen können. Zusammen mit anderen Quellen konnten insgesamt mehr als 2.000 Dateien rekonstruiert werden, die das Rechercheteam dann gemeinsam mit Kollegen des Guardian und der New York Times im Detail untersuchte. Darunter waren Videos und Audiodateien mit islamistischer Propaganda, aber beispielsweise auch ein Dokument zum Dalai Lama oder ein Rocksong einer japanischen Band.

„Bei der App handelt es sich um ein Überwachungsinstrument, mit dem man das Handy an der Grenze sehr schnell und effizient nach bestimmten Informationen durchsuchen kann“, folgert Thorsten Holz.

contact for scientific information:

Prof. Dr. Thorsten Holz
Lehrstuhl für Systemsicherheit
Horst-Görtz-Institut für IT-Sicherheit
Ruhr-Universität Bochum
Tel.: 0234 32 25199
E-Mail: thorsten.holz@rub.de

URL for press release: https://www.casa.rub.de/en/ Exzellenzcluster Casa

URL for press release: https://hgi.rub.de/home/ Horst-Görtz-Institut für IT-Sicherheit

Diese chinesische App wird Einreisenden beim Grenzübertritt aus Kirgistan auf dem Handy installiert.
© Mareen Meyer (Dieses Foto darf nur für eine Berichterstattung mit Bezug zur Ruhr-Universität Bochum im Kontext dieser Presseinformation verwendet werden.)

Prof. Dr. Thorsten Holz (rechts) und Moritz Contag vom Lehrstuhl für Systemsicherheit
© Mareen Meyer (Dieses Foto darf nur für eine Berichterstattung mit Bezug zur Ruhr-Universität Bochum im Kontext dieser Presseinformation verwendet werden.)