Harvester weckt Schläfer-Malware

TU Darmstadt und Fraunhofer SIT haben ein Analysetool entwickelt, das schlafenden Android-Schadcode blitzschnell enttarnt

(Mynewsdesk) Hacker und Cyberkriminelle nutzen immer häufiger ?Schläfer?-Software, um Schadcode für mobile Geräte in Apps zu verstecken. Diese ?schlafende? Malware tut zunächst einmal nichts. Erst nach einem bestimmten Zeitraum oder festgelegten Aktionen wird sie aktiv, was die Erkennung enorm erschwert. Sicherheitsforscher der TU Darmstadt und des Fraunhofer-Instituts für Sichere Informationstechnologie SIT haben deshalb das Analysewerkzeug Harvester entwickelt, das Sicherheitsanalysten dabei hilft, ?Schläfer?-Schadcode in Android-Apps in Minutenschnelle zu enttarnen.

Millionen von Android-Geräten sind bereits mit mobilem ?Schläfer?-Schadcode, auch timing bombs genannt, infiziert ? auf den ersten Blick scheinen sie normale Software zu sein. Ihr schädliches Potenzial entfalten sie erst nach einer längeren Inkubationszeit. Für den Smartphone-Besitzer ist es dann schwierig festzustellen, was die eigentliche Ursache dieses zeitverzögerten Angriffs ist. Ein aktuelles Beispiel ist der Banking-Trojaner BadAccents, ein zweistufiger Schadcode, der beim Herunterladen einer vermeintlichen Raubkopie des Films ?The Interview? aufs Smartphone kommt. Aktiv werden einzelne Komponenten in BadAccents erst unter bestimmten Umständen, etwa wenn das Smartphone per SMS bestimmte Befehle empfängt.

Auch für Sicherheitsanalysten, etwa von Antiviren-Herstellern, ist schlafender Schadcode, der erst unter speziellen Ereignissen ausgelöst wird, ein Problem. Sie müssen jeden Tag mehrere Tausend neue Apps darauf prüfen, ob sie potenziell schädlich sind oder nicht. Daher bleiben für die Analyse jeder App nur wenige Minuten Zeit. Um eine Schläfer-App zu enttarnen, müsste ein Analyst eine solche Untersuchung tagelang ausführen und sämtliche Ereigniskombinationen simulieren, denn im Vorhinein weiß man nicht, was den Schadcode aktiviert. Um Schläfer-Apps schneller finden zu können, haben IT-Sicherheitsexperten der Technischen Universität Darmstadt und des Fraunhofer SIT das Analysetool Harvester entwickelt. Das Analysewerkzeug nutzt eine einzigartige Kombination von Softwareanalyse-Techniken und Codeumwandlung und spart Sicherheitsanalysten damit viel Zeit.

Harvester untersucht nicht den gesamten Code der Original-App, sondern analysiert verdächtige Programmstellen. Die Software nutzt hierfür ein spezielles Verfahren der statischen Analyse, ?backwards slicing? oder ?program slicing?. Mithilfe des Tools können Analysten einfach den Teil des Codes herausschneiden, den sie näher untersuchen möchten ? alles andere wird kurzerhand weggelassen. Dadurch wird etwaiger Schadcode direkt ausgeführt und programmierte Wartezeiten sowie Ereignisfilter entfallen. Ist Schadcode gefunden worden, kann Harvester außerdem vollautomatisch wichtige Informationen (Ziel-Telefonnummern, Inhalte von SMSen, Entschlüsselungs-Schlüssel, URLs, etc.) aus dem schädlichen Android-Codes extrahieren, mit denen der Analyst auf Art und Quelle der Malware schließen kann. Für die Teilanalyse einer Codestelle benötigt Harvester rund eine Minute ? das haben die Experten von TU Darmstadt und Fraunhofer SIT an mehr als 13.500 gängigen Malware-Beispielen getestet.

Das Testwerkzeug funktioniert sogar, wenn der Code der schädlichen App stark verschleiert ist oder andere Anti-Analyse-Techniken genutzt wurden. Eine Basisvariante steht als Open Source-Tool für wissenschaftliche Zwecke zur Verfügung, eine Nutzung durch Privatanwender ist nicht vorgesehen. Für die kommerzielle Nutzung können Unternehmen eine Version mit erweiterter Funktionalität lizenzieren. Harvester ist Teil eines Analyseframeworks, das derzeit in Darmstadt entwickelt wird. Mit dem Framework lässt sich Android-Code extrem schnell und einfach untersuchen.

Mehr Informationen:
Die Basisvariante für wissenschaftliche Zwecke ist über die Projektgruppe von Prof. Dr. Eric Bodden zugänglich. Weitere Informationen und Ansprechpartner zu Harvester finden sich im Internet unter www.sit.fraunhofer.de/harvester oder im Blog der Forschungsgruppe unter http://sseblog.ec-spride.de/2015/01/korea-threat-compain-2014/

Shortlink zu dieser Pressemitteilung:
http://shortpr.com/mh9ufz

Permanentlink zu dieser Pressemitteilung:
http://www.themenportal.de/it-hightech/harvester-weckt-schlaefer-malware-77599

=== Harvester-Illustration (Bild) ===

Mit Harvester lassen sich Schläfer-Apps in kürzester Zeit enttarnen. Das Analysewerkzeug entdeckt tickende Zeitbomben im Code.

Shortlink:
http://shortpr.com/4z9lh9

Permanentlink:
http://www.themenportal.de/bilder/harvester-illustration

Pressekontakt

Fraunhofer-Institut für Sichere Informationstechnologie

Herr Oliver Küch
Rheinstraße 75
64295 Darmstadt

presse@sit.fraunhofer.de

Firmenkontakt

Fraunhofer-Institut für Sichere Informationstechnologie

Herr Oliver Küch
Rheinstraße 75
64295 Darmstadt

sit.fraunhofer.de
presse@sit.fraunhofer.de

Die Informationstechnologie hat bereits weite Teile unseres Alltags durchdrungen: Ob Auto, Telefon oder Heizung ohne IT-Einsatz sind die meisten Geräte und Anlagen heute nicht mehr denkbar. Insbesondere Unternehmen nutzen ---IT-Systeme zur effektiven Gestaltung ihrer Arbeitsprozesse. Das Fraunhofer-Institut für Sichere Informationstechnologie beschäftigt sich mit dem Schutz dieser Systeme vor Ausfällen, Angriffen und Manipu-lationen.

Das Fraunhofer-Institut SIT ist Teil des größten Cybersicherheitsforschungszentrums Deutschlands in Darmstadt und zählt auch weltweit auf vielen Gebieten zu den führenden Forschungseinrichtungen zur Cybersicherheit weltweit.

Anlage: Bild