PRESSEINFORMATION

FKIE-Wissenschaftler präsentiert neuen Ansatz zur Detektion von Malware-Daten in Bilddateien

Im Dschungel der Cyberbedrohungen kommen immer wieder neue Methoden ans Licht, derer sich Angreifer bedienen. Gut getarnte Angriffsmuster und stetig an Fortschritt wachsende Varianten ermöglichen Cyberkriminellen Zugang zu fremden Netzwerken. Auch in Bilddateien, zum Beispiel in dem weit verbreiteten JPEG-Format, kann sich Malware verbergen, auf diese Weise bestehende Schutzsysteme umgehen, Computer und Netzwerke infizieren oder unbemerkt vertrauliche Daten ausschleusen. Jonathan Chapman, Wissenschaftler am Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE, hat sich diesem Problem angenommen und eine Methode entwickelt, die Anomalien in Bilddateien aufspürt und diese anhand ihrer ungewöhnlichen Struktur herausfiltert und erkennt. Ihre Funktion hat er anhand eines Datensatzes von über 500.000 Bilddateien erfolgreich überprüft. Im Rahmen des »USENIX Security Symposiums«, das vom 15. bis 17. August 2018 in Baltimore stattfindet, stellt der FKIE-Wissenschaftler seine Ergebnisse erstmals vor.

Der Ansatz, den der IT-Experte aus der Abteilung »Cyber Analysis and Defense« entwickelt hat, erkennt durch die Einbettung von Malware-Daten bedingte strukturelle Anomalien in Bilddateien. Dies kann dazu genutzt werden, um in einem solchen Fall einen Alarm auszulösen und die Übertragung zu unterbrechen. Besonders ist an dem Ansatz, dass er nicht eine bestimmte Form von Malware erkennt, sondern signifikante Strukturanomalien in Bilddateien ausreichen, um eine verdeckt kommunizierende Malware zu detektieren.

SAD THUG, kurz für »Structural Anomaly Detection for Transmissions of High-value Information Using Graphics« – unter diesem Titel stellt Jonathan Chapman den Ansatz in Baltimore vor –, erkennt, wie die Strukturen von Bilddateien aussehen müssen, um diese als gut oder bösartig zu klassifizieren. Im Gegensatz zu einem bereits existierenden Ansatz wurde zur Erkennung von strukturellen Anomalien bei JPEG-Dateien auch Maschinelles Lernen eingesetzt und so anhand großer Datensätze erlernt, wie die Struktur nicht-infizierter Bilddateien auszusehen hat.

Redaktion
Silke Wiesemann | silke.wiesemann@fkie.fraunhofer.de | Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE, Fraunhoferstraße 20, 53343 Wachtberg-Werthhoven | www.fkie.fraunhofer.de | Telefon +49 228 9435-103

Mehr als 500.000 Bilddateien hat der FKIE-Wissenschaftler als Grundlage für »SAD THUG« verwendet. Die Ergebnisse sind beeindruckend: Bei JPEG-Dateien (511.024) lag die Rate bei der Erkennung von Malware bei 99,24 Prozent und weist zugleich eine äußerst niedrige Falsch-Positiv-Rate von 0,52 Prozent auf. Bei PNG-Dateien lag das Ergebnis aufgrund des deutlich kleineren Datensatzes von nur 60.083 Bilddateien und des damit verbundenen geringeren Lerneffekts der Software bei einer Falsch-Positiv-Rate von 1,1 Prozent. Allerdings wurden auch hier 99,32 Prozent der Malware-Bilder korrekt erkannt.

Somit bietet »SAD THUG« Computernutzern und vor allem IT-Administratoren weltweit eine sehr effektive Lösung für das Problem in Bilddateien eingebetteter Schadsoftware. Denn nicht nur in Dateien, die E-Mails anhängen, kann sich eine solche Malware verbergen, sondern auch in den tagtäglich millionenfach in den Sozialen Netzwerken wie Facebook und Twitter verwendeten Bilddateien. Über sie hielt beispielsweise die Ransomware »CryLocker« den Kontakt zu ihren Autoren. Diese Form von Malware verschlüsselt wichtige Dateien der infizierten Nutzersysteme mit einem geheimen Code, den die Autoren nur nach Zahlung eines Lösegelds (»ransom«) bereitstellen. Aktuellen Schätzungen zufolge entstand der Weltwirtschaft hierdurch 2017 ein Schaden in Höhe von mehr als 4,3 Milliarden Euro. Chapman: »Der neue Ansatz erkennt nicht nur eine bestimmte Methode zum Verstecken von Schadsoftware-Informationen, sondern buchstäblich jede Methode, die die Struktur einer Containerdatei verändert. Viele der Angriffe, die in den vergangenen Monaten bekannt geworden sind, nutzen Werkzeuge, die mit ›SAD THUG‹ hätten erkannt und unter Umständen frühzeitig abgewehrt werden können. Das gilt nicht zuletzt auch für die dem russischen Geheimdienst zugerechnete *Hammertoss*-Malware.«

Ansprechpartner
Jonathan Chapman, Abteilung »Cyber Analysis and Defense« | Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE | Wachtberg | www.fkie.fraunhofer.de | jonathan.pascal.chapman@fkie.fraunhofer.de | Telefon: + 49 228 50212-573

Das **Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE** ist in seinem Kern auf die Unterstützung staatlicher Institutionen im Bereich der Äußeren und Inneren Sicherheit ausgerichtet. Herausragende Bedeutung hat die strategische Kooperation mit dem Verteidigungsministerium, dem Bundesamt für Sicherheit in der Informationstechnik und der Bundespolizei. Im Bereich der Wirtschaft fokussiert FKIE auf Sicherheit an Flughäfen und im Luftverkehr, bei Maritimen Systemen und in der IT-Branche. Mit seinen etwa 430 Mitarbeitern an den Standorten Bonn und Wachtberg ist das FKIE ein führendes Institut für anwendungsorientierte Forschung und praxisnahe Innovation in der Informations- und Kommunikationstechnologie sowie im Bereich der menschengerechten Gestaltung von Technik.