Dauerbrenner Malware: diese aktuellen Brandherde müssen im Auge behalten werden

SophosLabs analysiert in einem ausführlichen Report Malware-Aktivitäten aus dem Jahr 2016 und zieht Schlüsse für die weitere Entwicklung

Wiesbaden, 14. Februar 2017 – SophosLabs hat die Malware-Aktivitäten der letzten Monate analysiert und auf dieser Grundlage einen ausführlichen Report über die Entwicklung der Gefahren durch Malware erstellt. Demnach ändert sich die Bedrohungslage zwar beinahe täglich, Hauptziele der Hacker werden jedoch wie im Vorjahr Windows-Geräte sein. Auch andere Plattformen gelangen zunehmend ins Visier der Cyberkriminellen. SophosLabs identifiziert vier Trends, die 2016 Fahrt aufgenommen haben und voraussichtlich in den nächsten Monaten massiver auftreten:

1. Linux-Malware, die Sicherheitslücken bei IoT-Geräten ausnutzt
2. Allgegenwärtige Android-Malware – unvermindert häufig
3. MacOS Malware, die potenziell unerwünschte Anwendungen (PUA) verbreitet
4. Microsoft Word Intruder Malware, die über Office-Anwendungen hinaus geht

Linux und Internet of Things
Linux wird immer häufiger für Angriffe auf IoT-Geräte – von der Webcam bis hin zu vernetzten Haushaltsgeräten – genutzt. Standardpasswörter, veraltete Linux-Versionen und fehlende Verschlüsselung laden zukünftig Angreifer dazu ein, sich diesen Geräten zu widmen.

Android-Malware
Über 20 Prozent der 2016 analysierten Malware-Angriffe auf Android-Geräte gingen nach dem gleichen Muster vor und wurden durch Werbung und Registrierungsprozesse aktiviert. Diese Malwareart – am häufigsten in Form von Andr/PornClk vorkommend – lädt Android Application Packages (APKs) herunter, platziert Shortcuts auf den Bildschirm und ist so in der Lage an Informationen wie Geräte-ID, Telefonnummer oder andere sensible Daten zu gelangen.

MacOS Malware
Malware für MacOS-Geräte ist hauptsächlich dazu konzipiert, Passwörter durch Platzierung eines speziellen Codes zu stehlen, wie zum Beispiel OSX/KeRanger--A. Zwar werden auch in Zukunft weniger Angriffe auf Mac- als auf Windows-Geräte erfolgen, doch die Zeiten, als sich MacOS-Nutzer sicher fühlen konnten, sind lange vorbei.

Windows-Malware
In der Vergangenheit zielten Windows-basierte Malware-Kits auf Office- bzw. Word-Anwendungen, doch zukünftig erweitert sich deren Wirkungskreis durch Exploits, die nicht auf MS Office basieren. So wurde beispielsweise im Sommer 2016 erstmal ein Exploit entdeckt, der Schwachstellen im Adobe Flash Player ausnutzte.

Fazit
Diese vier Beispiele zeigen, dass der Cyber-Kriminalismus immer professioneller wird und vor allem gezielter vorgeht. Unternehmen müssen, neben einem schlagkräftigen Next-Gen-IT-Sicherheitskonzept, vor allem dafür sorgen, dass Endanwender bedacht und verantwortlich handeln, um nicht Opfer von beispielsweise Social Engineering-Angriffen zu werden.

Der vollständige Report „Looking ahead: SophosLabs 2017 Malware Forecast“ steht in englischer Sprache unter
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophoslabs-2017-malware-forecast-report.pdf?la=en
als Download zur Verfügung.

Über Sophos

Mehr als 100 Millionen Anwender in 150 Ländern verlassen sich auf Sophos‘ Complete-Security-Lösungen als den besten Schutz vor komplexen IT-Bedrohungen und Datenverlust. Sophos bietet dafür preisgekrönte Verschlüsselungs-, Endpoint-Security-, Web-, Email-, Mobile- und Network Security-Lösungen an, die einfach zu verwalten, zu installieren und einzusetzen sind. Das Angebot wird von einem weltweiten Netzwerk eigener Analysezentren, den SophosLabs, unterstützt.
Sophos hat seinen Hauptsitz in Boston, USA, und Oxford, Großbritannien. In Deutschland hat das Unternehmen seinen Hauptsitz in Wiesbaden und ist in Österreich und der Schweiz je an einem Standort vertreten. Weitere Informationen unter www.sophos.de.

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
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