Der monatliche Security Awareness Newsletter für Jedermann

Stoppen Sie Malware

Überblick

Sie haben wahrscheinlich schon von Begriffen wie Virus, Trojaner, Ransomware oder Rootkit gehört, wenn von Cybersicherheit die Rede ist. Dies sind verschiedene Arten von bösartigen Programmen, genannt Malware, mit denen Cyberkriminelle Computer und Geräte infizieren. Einmal installiert, können diese tun was sie wollen. Erfahren Sie, was Malware ist, welche Gefahren sie birgt und vor allem, was Sie tun können, um sich davor zu schützen.

Was ist Malware?

Einfach ausgedrückt: Malware ist Software, also ein Computerprogramm, mit dem bösartige Aktionen ausgeführt werden. Dieser Begriff ist eine Kombination aus den Wörtern bösartig (englisch: “malicious”) und Software. Cyberkriminelle installieren Malware auf Ihren Computern oder Geräten, um die Kontrolle über diese zu erlangen. Einmal installiert, kann Malware Kriminellen ermöglichen, Ihre Online-Aktivitäten auszuspionieren, Ihre Passwörter oder Dateien zu stehlen oder Ihr System zu benutzen um andere anzugreifen. Malware kann sogar die Kontrolle über Ihre eigenen Dateien übernehmen und verlangt, dass Sie ein Lösegeld zahlen um sie zurückzubekommen. Viele Menschen glauben, dass Malware nur für Windows-Computer ein Problem darstellt. Leider kann Malware jedes Gerät infizieren, von Mac Computern und Smartphones, bis hin zu Digitalrekordern und Sicherheitskameras. Je mehr Computer und Geräte Cyberkriminelle infizieren, desto mehr Geld können sie verdienen. Deshalb ist jeder ein Ziel, auch Sie.

Schützen Sie sich selbst – Stoppen Sie Malware

Sie denken vielleicht, dass Sie nichts weiter tun müssen, als ein Sicherheitsprogramm wie Antivirensoftware zu installieren, und Sie sind sicher vor einer Infektion. Leider kann Antiviren-Software nicht alle Malware stoppen. Cyberkriminelle entwickeln ständig neue und ausgefeiltere Malware, die sich der Erkennung entziehen kann. Im Gegenzug aktualisieren Antiviren-Anbieter ihre Produkte ständig mit neuen Funktionen zur Erkennung von Malware. In vielerlei Hinsicht ist es ein Wettrüsten geworden, und die Bösen sind meist einen Schritt voraus. Da Sie sich nicht allein auf Antiviren-Software verlassen können, sollten Sie hier weitere Schritte unternehmen, um sich zu schützen:

Cyberkriminelle infizieren häufig Computer oder Geräte, indem sie Schwachstellen in Ihrer Software ausnutzen. Je aktueller Ihre Software ist, desto weniger Schwachstellen haben Ihre Systeme und desto schwieriger ist es für Cyberkriminelle, sie zu infizieren. Stellen Sie sicher, dass Ihre Betriebssysteme, Anwendungen, Browser inkl. der Browser-Plugins und Geräte immer auf dem neuesten Stand sind. Der einfachste Weg dies sicherzustellen, ist die automatische Aktualisierung zu aktivieren, wann immer dies möglich ist.

Cyberkriminelle infizieren Computer oder mobile Geräte, indem sie gefälschte Computerprogramme oder mobile Anwendungen erstellen, diese ins Internet stellen und Sie dann zum Herunterladen und Installieren verleiten. Installieren Sie nur Programme oder Anwendungen, die Sie von vertrauenswürdigen Online-Shops heruntergeladen haben. Halten Sie sich auch fern von mobilen Anwendungen, die brandneu sind, nur wenige positive Bewertungen haben, selten aktualisiert werden oder von einer kleinen Anzahl Nutzer heruntergeladen wurden. Sie arbeiten mit einem Computerprogramm oder einer mobilen Anwendung nicht mehr? Löschen Sie sie.

Cyberkriminelle überlisten ihre Ziele oft, um Malware für sie zu installieren. Beispielsweise können sie Ihnen eine E-Mail schicken, die legitim aussieht und einen Anhang oder einen Link enthält. Vielleicht kommt die E-Mail von Ihrer Bank oder einem Freund. Wenn Sie jedoch die angehängte Datei öffnen oder auf den Link klicken, aktivieren Sie bösartigen Code, der Malware auf Ihrem System installiert. Wenn eine Nachricht ein starkes Gefühl der Dringlichkeit erzeugt oder zu gut ist um wahr zu sein, könnte es ein Angriff sein. Seien Sie misstrauisch, der gesunde Menschenverstand ist oft Ihre beste Verteidigung.

Sichern Sie Ihr System und Ihre Dateien regelmäßig auf Cloud-basierte Dienste oder speichern Sie Ihre Backups offline, z. B. auf getrennten externen Laufwerken. Dies schützt Ihre Backups, falls Malware versucht sie zu verschlüsseln oder zu löschen. Backups sind kritisch, sie sind oft die einzige Möglichkeit, sich von einer Malware-Infektion zu erholen.

Der beste Weg, um sich gegen Malware zu schützen, ist alle Ihre Software und Geräte auf dem neuesten Stand zu halten, vertrauenswürdige Antivirensoftware zu installieren und immer aufmerksam zu sein, wenn jemand versucht Sie dazu zu verleiten Ihr eigenes System zu infizieren. Wenn alles andere fehlschlägt, sind regelmäßige Backups oft die einzige Möglichkeit zur Wiederherstellung.

Deutsche Ausgabe

Diese OUCH! Ausgabe wurde von Marek Kreul und René Wiedewilt aus dem Englischen übersetzt. Beide arbeiten für das CERT eines DAX-Konzerns und haben sich auf IT-Forensik spezialisiert. Sie haben langjährige Erfahrung im Bereich IT-Sicherheit und sind mehrfach GIAC zertifiziert.

Gast-Autor

Lenny Zeltser *bekämpft Malware, indem er bei Minerva Labs Endpoint Security-Produkte entwickelt und am SANS-Institut unterrichtet. Lenny ist auf Twitter als @lennyzeltser aktiv und schreibt einen Sicherheitsblog auf zeltser.com.*

Weiterführende Informationen

Ransomware:	https://www.sans.org/u/EdI
Backups:	https://www.sans.org/u/EdN
Stopp den Phishzug:	https://www.sans.org/u/EdS