BEGRIFFSDEFINITIONEN

MALWARE

Der Begriff „Malware“ – ein Zusammenschluss der Wörter „Malicious“ (schädlich) und „Software“ – wird heute verwendet, um schädliche Programme jeder Art auf Computern oder mobilen Geräten zu beschreiben. Diese Programme werden ohne Zustimmung des Benutzers installiert und können eine Reihe unangenehmer Folgen haben. So können sie beispielsweise die Systemleistung reduzieren, innerhalb Ihres Systems nach persönlichen Daten suchen, Informationen löschen oder sogar den Betrieb computergesteuerter Hardware beeinträchtigen. Hacker entwickeln immer raffiniertere Methoden, um in Systeme einzudringen, und sorgen so für eine wahre Flut auf dem Malware-Markt. Sehen wir uns einmal einige der häufigsten Malware-Arten an.

Computerviren:
Computerviren haben ihren Namen durch die Fähigkeit erhalten, mehrere Dateien auf einem Computer zu „infizieren“. Sie verbreiten sich auf andere Geräte, wenn diese infizierten Dateien per E-Mail versendet oder über einen Wechseldatenträger, wie z. B. einen USB-Stick oder (damals noch) eine Diskette, übertragen werden. Laut National Institute of Standards and Technology (NIST) wurde der erste Computervirus namens „Brain“ 1986 entwickelt. Zwei Brüder waren es leid, dass Kunden die Software aus ihrem Geschäft illegal kopierten, und entwickelten so den Virus, der den Boot-Sektor der Disketten von Softwaredieben infizieren sollte. So wurde der Virus beim Kopieren der Disketten weitergegeben.

Würmer:
Im Gegensatz zu Viren sind Würmer nicht auf menschliche Hilfe angewiesen, um sich zu verbreiten: Sie infizieren ein Gerät und nutzen dann Computernetzwerke, um sich auf andere Computer zu verbreiten – ohne Zutun der Benutzer. Indem sie Schwachstellen in den entsprechenden Netzwerken, wie z. B. Sicherheitslücken in E-Mail-Programmen, ausnutzen, können Würmer Tausende Kopien von sich versenden, um so neue Systeme zu infizieren und den Prozess erneut durchzuführen. Während viele Würmer früher lediglich Systemressourcen verbrauchten und so die Leistung reduzierten, enthalten die meisten neuen Würmer sogenannte „Payloads“, die dazu dienen, Dateien zu stehlen oder zu löschen.

Adware:
Eines der am weitesten verbreiteten Online-Ärgernisse ist Adware. Diese Programme zeigen automatisch Werbeanzeigen auf dem Host-Computer an. Bekannte Arten von Adware sind beispielsweise Pop-up-Werbeanzeigen auf Webseiten oder in vermeintlich kostenlosen Anwendungen integrierte Werbung. Zwar ist viele Adware verhältnismäßig harmlos, jedoch gibt es Varianten, die Tracking-Tools nutzen, um Ihren Standort oder Ihren Browserverlauf zu ermitteln und gezielte Werbeanzeigen auf Ihrem Bildschirm anzuzeigen. BetaNews berichtet sogar von einer neuen Form von Adware, die Ihre Antiviren-Software deaktivieren kann. Da Adware mit Kenntnis und Zustimmung des Benutzers installiert wird, kann sie nicht als „Malware“ bezeichnet werden. Deshalb wird sie häufig als „potenziell unerwünschte Programme“ bezeichnet.

Spyware:
Spyware (kurz für „Spionagesoftware“) tut genau das, was ihr Name vermuten lässt: Sie spioniert Ihren Computer aus. Sie erfasst Daten, wie z. B. Ihre Tastenanschläge, Surfgewohnheiten und sogar Anmeldedaten, die dann an Dritte gesendet werden – für gewöhnlich Cyberkriminelle. Sie kann auch bestimmte Sicherheitseinstellungen auf Ihrem Computer ändern oder Ihre Netzwerkverbindungen beeinträchtigen. Laut TechEye bieten neue Arten von Spyware Unternehmen sogar die Möglichkeit, das Verhalten ihrer Benutzer über verschiedene Geräte hinweg nachzuverfolgen – und das ohne ihre Zustimmung.

Ransomware:
Ransomware infiziert Ihren Computer, verschlüsselt vertrauliche Daten, wie z. B. persönliche Dokumente und Fotos, und verlangt ein Lösegeld für ihre Entschlüsselung. Wenn Sie die Zahlung verweigern, werden die Daten gelöscht. Manche Ransomware-Varianten blockieren auch gleich den gesamten Zugriff auf den Computer. In den Lösegeldforderungen wird möglicherweise behauptet, es handele sich um legitime Strafverfolgungsbehörden, die Sie bei illegalen Aktivitäten erwischt haben. Im Juni 2015 erhielt das Internet Crime Complaint Center des FBI Beschwerden von Benutzern, die durch eine gewöhnliche Ransomware namens CryptoWall insgesamt einen Schaden von 18 Millionen US-Dollar erlitten hatten.

Bots:
Bei Bots handelt es sich um Programme, die automatisch bestimmte Aktionen durchführen sollen. Sie dienen vielen legitimen Zwecken, können jedoch auch als eine Art von Malware zweckentfremdet werden. Einmal auf einem Computer angelangt, können Bots das Gerät dazu bringen, bestimmte Befehle auszuführen – ohne Wissen oder gar Zustimmung des Benutzers. Hacker können auch versuchen, mehrere Computer mit dem gleichen Bot zu infizieren, um so ein sogenanntes „Botnet" (kurz für „Roboternetzwerk") zu schaffen, das für die Remote-Steuerung der infizierten Computer genutzt werden kann. Mithilfe eines Botnet stehlen Cyberkriminelle vertrauliche Daten, spionieren die Aktivitäten ihrer Opfer aus, verbreiten automatisch Spam oder führen verheerende DDoS-Angriffe auf Computernetzwerke durch.

Rootkits:
Rootkits ermöglichen den Remote-Zugriff auf einen Computer zur Fernsteuerung durch Dritte. Diese Programme sind äußerst nützlich für IT-Experten, die Netzwerkprobleme an entfernten Standorten beheben müssen. Sie können jedoch auch schnell zur Gefahr werden: Sind sie einmal installiert, ermöglichen es Rootkits den Angreifern, die vollständige Kontrolle über das Gerät zu übernehmen, um Daten zu stehlen oder andere Malware zu installieren. Rootkits arbeiten unbemerkt und verschleiern ihre Existenz. Die Erkennung dieser Art schädlichen Codes erfordert die manuelle Überwachung auf ungewöhnliches Verhalten sowie die regelmäßige Installation neuer Patches für Betriebssystem und andere Software, um potenzielle Infektionsvektoren zu beseitigen.

Trojanische Pferde:
Diese Programme werden im Allgemeinen nur als „Trojaner" bezeichnet und tarnen sich als legitime Datei oder Software. Einmal heruntergeladen und installiert, nehmen Trojaner Änderungen am Computer vor und führen ohne Wissen oder Zustimmung des Opfers schädliche Aktivitäten durch.

Bugs:
Sogenannte „Bugs", also kleine Fehler im Softwarecode, stellen keine Art von Malware dar, sondern einfach Fehler der Programmierer. Auch sie können sich jedoch schädlich auf Ihren Computer auswirken, beispielsweise in Form von Abstürzen oder einer Verringerung der Systemleistung. Sicherheitsfehler jedoch bieten Angreifern Möglichkeiten, die Verteidigung zu umgehen und das Gerät zu infizieren. Durch Sicherheitskontrollen versuchen Entwickler, solche Fehler zu beseitigen. Es ist jedoch zwingend erforderlich, die entsprechenden Software-Patches auch zu installieren.

Quelle: https://www.kaspersky.de/resource-center/threats/computer-viruses-and-malware-facts-and-faqs