Malware

Dieser Artikel führt Sie in die Welt der Schadprogramme ein. Sie erfahren, wie Malware grundlegend funktioniert und lernen die gängigsten Infektionswege und schädlichen Verhaltensweisen kennen. Dabei wird Ihnen jeweils vor Augen geführt, wie unsere «5 Schritte für Ihre digitale Sicherheit» Sie effektiv schützen.

Wichtigste Merkpunkte:

- Malware sind Computerprogramme, mit unerwünschten und oft schädlichen Funktionen.
- Die Ausprägungen von Malware sind vielseitig und bedürfen unterschiedlicher Präventionsmassnahmen.
- In den letzten Jahren haben die Risiken durch Malware weiter zugenommen.
- Die Risiken durch Malware lassen sich mit unseren «5 Schritte für Ihre digitale Sicherheit (https://www.ebas.ch/5-schritte-fuer-ihre-digitale-sicherheit/) » effektiv reduzieren.

Malware – ein unerwünschtes Computerprogramm

Das Wort Malware ist ein Überbegriff für Computerprogramme, die meistens bewusst erstellt werden, um den Benutzern zu Schaden.

Ähnlich wie bei herkömmlicher Software hat sich auch die Erschaffung und Verbreitung von Malware weiterentwickelt. Ersteres geschieht vermehrt auf einem professionellen Niveau und trägt zu einer grösseren Volatilität der Malware-Entwicklung bei. Zudem wird Malware immer gezielter verbreitet. Privatpersonen sowie KMU werden systematisch angegriffen.

Infektion

Wie alle Computerprogramme ist auch Malware nichts anderes als eine Reihe von Anweisungen, welche durch den Computer ausgeführt werden.

Um ihre schädigende Wirkung zu erreichen, muss Malware demnach durch das System ausgeführt werden. Dies geschieht entweder auf Anweisung des Benutzers oder eines bereits laufenden Programms.

Ersteres geschieht bekanntlich, indem den Benutzern entweder ein möglicher Nutzen oder abwendbarer Schaden vorgegaukelt wird. Malware, welche über diesen Weg ausgeführt wird, ist unter dem Überbegriff Trojanisches Pferd oder kurz Trojaner bekannt. Sie tarnt sich als nützliches Programm und wird in der Regel durch das Opfer selbst gestartet. Einmal ausgeführt, entfaltet es seine schädigende Wirkung.

Dabei muss es sich nicht zwingend um klassisch ausführbare Programmdateien handeln. Auch Office-Dokumente und PDF-Dateien können sogenannte Makros enthalten, welche durch die jeweiligen Programme ausgeführt werden.

Derartige Täuschungsversuche lassen sich oft durch unseren «Schritt 5 – Aufpassen und wachsam sein (https://www.ebas.ch/5-aufpassen-und-wachsam-sein/) » entlarven und verhindern.

Wenn Malware durch ein laufendes Programm, ohne Zutun einer Person, ausgeführt wird, geschieht dies über das

Copyright – Alle Rechte vorbehalten. Hochschule Luzern – Informatik

Ausnutzen einer sogenannte Sicherheitslücke. Dabei handelt es sich um Fehler in der Programmlogik, welche Auswirkungen auf die Sicherheit haben können.

Sicherheitslücken in Browsern (https://www.ebas.ch/browser/) erlauben es beispielsweise sogenannte Drive-By-Downloads (https://www.ebas.ch/drive-by-download/) zu realisieren. Auch Sicherheitslücken im Betriebssystem werden gerne ausgenutzt, um beispielsweise Schadsoftware über externe Datenträger wie USB-Sticks oder das Netzwerk einzuschleusen. Malware, welche sich selbstständig über derartige Fehler verbreitet, wird als Wurm bezeichnet.

Sicherheitslücken werden regelmässig durch Softwarehersteller geschlossen, indem Updates zur Verfügung gestellt werden. Deswegen gilt als wichtigste Massnahme zur Vorbeugung von Malwareinfektionen «Schritt 3 – Vorbeugen mit Software-Updates (https://www.ebas.ch/3-vorbeugen-mit-software-updates/) ».

Einmal ausgeführt gilt es für die meisten Malware Varianten mittels unterschiedlicher Methoden sicherzustellen, dass ihr Schadcode immer wieder gestartet wird. Ein Virus schreibt zu diesem Zweck den eigenen Schadcode in andere Programme. So genannte Rootkits nisten sich hierzu direkt im Code des Betriebssystems ein.

Schädliche Wirkung

Das Risiko einer Malwareinfektion lässt sich nicht vollständig vermeiden. Deswegen ist es ratsam auch Massnahmen für den Fall einer erfolgreichen Infektion vorzusehen.

Nachfolgend werden gängige Schadensszenarien vorgestellt und es wird erläutert, wie diese durch unsere «5 Schritte für Ihre digitale Sicherheit (https://www.ebas.ch/5-schritte-fuer-ihre-digitale-sicherheit/) » reduziert werden können.

Verlangsamung des Systems

Die missbräuchliche Nutzung von System- und Netzwerkressourcen kann die Arbeit mit einem infizierten Gerät stark verlangsamen oder gar verunmöglichen. Einen grossen Einfluss auf die Leistung eines Systems hat Malware, welche beispielsweise für das Schürfen von Kryptowährungen (Crypto Miner), Knacken von Passwörtern oder dem Durchführen von Angriffen auf weitere Systeme (z.B. Distributed Denial-of-Service) erstellt wurde.

Diese Art der Malware entfaltet Ihren Nutzen mit der Infektion einer möglichst grossen Anzahl an Systemen, welche in ein so genanntes Botnetz zusammengefasst werden.

Solche Malware ist darauf ausgelegt, längerfristig auf einem System ihr Unwesen zu treiben und sollte früher oder später durch ein Antivirenprogramm entdeckt werden. Damit dies jedoch richtig funktioniert, muss es regelmässig aktualisiert und wiederholend ein vollständiger Scan des ganzen Systems durchgeführt werden. Weitere Informationen dazu unter «Schritt 2 – Überwachen mit Virenschutz und Firewall (https://www.ebas.ch/2-ueberwachen-mit-virenschutz-und-firewall/) ».

Anzeigen von Werbung

Die unter dem Begriff Adware bekannten Programme machen sich durch das Einblenden von Werbeanzeigen bei ihren Opfern unbeliebt.

Wird ein System mit unerwartet viel Werbung geplagt, ist dies ein Indikator für weitere Malware Infektionen und sollte als Anlass zu einer Systemsäuberung genommen werden.

Beschränkt sich die Werbung auf Webseiten und wird lediglich innerhalb ihres Browsers angezeigt, könnte es sich lohnen, unsere Tipps für mehr Datenschutz und Privatsphäre (https://www.ebas.ch/privatsphaere-und-datenschutz-im-inter-

Copyright – Alle Rechte vorbehalten. Hochschule Luzern – Informatik

net/) im Internet oder der Verwendung von Werbeblockern (https://www.ebas.ch/ad-blocker-und-anti-tracking-tools/) zu befolgen.

Sammeln von Informationen
Malware mit Spyware Eigenschaften zeichnet sich dadurch aus, dass sie gezielt Informationen über ihre Opfer sammeln und weiterleiten. Dies kann beispielsweise die Analyse des Surfverhaltens, das Abhorchen von Tastaturanschlägen (Keylogger) oder das Stehlen von sensiblen Daten beinhalten.

Um die Risiken durch Spyware zu verringern, empfiehlt es sich, die eigenen digitalen Aktivitäten zu segmentieren und ein datensparsames Verhalten an den Tag zu legen. Durch die Befolgung von «Schritt 4 – Schützen der Online-Zugänge (https://www.ebas.ch/4-schuetzen-der-online-zugaenge/) » reduzieren Sie effektiv das Schadensausmass bei einem erfolgreichen Spionageangriff. So führt beispielsweise beim Einsatz von Zwei-Faktor-Authentifizierung ein ausspioniertes Passwort nicht sofort zur Kompromittierung Ihres E-Banking Accounts.

Verschlüsselung oder Zerstörung von Daten
Die Verschlüsselung von Daten wird hauptsächlich als Druckmittel bei Erpressungsversuchen mit so genannter Ransomware eingesetzt.

In einem solchen Fall hilft nach der Systembereinigung meist nur die Wiederherstellung der Daten aus einem bereits erstellten Backup. «Schritt 1 – Sichern der Daten (https://www.ebas.ch/1-sichern-der-daten/) » fungiert hierbei als Grundpfeiler für eine erfolgreiche Datenwiederherstellung.

Kombinierte Angriffe
Das mögliche Verhalten von Malware beschränkt sich nicht nur auf die beschriebenen Szenarien. So werden oft mehrere der beschriebenen Verhaltensweisen kombiniert oder neuartige Vorgehensweisen entwickelt.

Ersteres wird durch den Einsatz sogenannter Downloader erreicht, welche automatisch oder auf Befehl weitere Malware auf das Zielsystem nachladen.

Ein prominentes Beispiel für kombinierte Angriffe sind Erpressungen, bei welchen in einem ersten Schritt ein Zielsystem ausgespäht und im zweiten Schritt die Daten verschlüsselt werden. Dies erlaubt es den Erpressern mehr Druck auf ihre Opfer auszuüben, indem ihnen beispielsweise angedroht wird, die erbeuteten Daten zu veröffentlichen oder der Konkurrenz zukommen zu lassen.

Identifizierung und Säuberung

Mit der Befolgung unserer «5 Schritte für Ihre digitale Sicherheit (https://www.ebas.ch/5-schritte-fuer-ihre-digitale-sicherheit/) » reduzieren sie effektiv die Eintretenswahrscheinlichkeit einer Malwareinfektion und der damit verbundenen Schadenszenarien.

Gänzlich lässt sich das Risiko jedoch nicht ausschliessen. Lesen Sie unseren Artikel «Malwareinfektion (https://www.ebas.ch/malwareinfektion/) » um zu erfahren, wie Sie eine Infektion erkennen und beheben können.

Als Malware, Schadprogramm oder Schadsoftware werden Computerprogramme bezeichnet, die entwickelt wurden, um, aus Sicht des Opfers, unerwünschte und gegebenenfalls schädliche Funktionen auszuführen. Der Begriff setzt sich aus den beiden Wörtern malicious «bösartig» und Software zusammen.

Copyright – Alle Rechte vorbehalten. Hochschule Luzern – Informatik