Malware

2.1.1 Den Begriff Malware verstehen

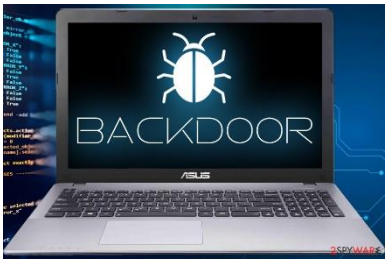
Malware (kurz für "Malicious Software") ist ein Überbegriff für verschiedene Arten von schädlicher Software, die entwickelt wurde, um Computersysteme, Netzwerke oder Geräte zu schädigen, zu stören oder unautorisierten Zugriff zu ermöglichen.

Wie Malware auf Geräten verborgen werden kann:

1. **Trojaner:** Ein Trojaner tarnt sich als nützliche Software, um Benutzer dazu zu bringen, ihn herunterzuladen und zu installieren. Ein Beispiel ist ein Spiel oder ein Programm, das in Wirklichkeit schädliche Funktionen ausführt.
   - **Beispiel:** Ein Benutzer lädt ein kostenloses Spiel herunter, das als harmlos erscheint, aber in Wirklichkeit Daten stiehlt.

2. **Rootkit:** Dies ist eine Art von Malware, die darauf abzielt, sich in das Betriebssystem einzunisten und unentdeckt zu bleiben. Sie ermöglicht Angreifern den Zugriff auf das System und die Kontrolle darüber.
   - **Beispiel:** Ein Rootkit könnte verwendet werden, um eine Hintertür (Backdoor) zu installieren, durch die der Angreifer Zugriff auf persönliche Daten erhält.

3. **Backdoor:** Eine Backdoor ist eine Art von Malware, die es einem Angreifer ermöglicht, sich unbemerkt in ein System einzuschleichen. Sie kann absichtlich in Software integriert werden oder durch einen Trojaner installiert werden.
   - **Beispiel:** Ein Entwickler könnte unwissentlich eine Backdoor in ein Programm einfügen, die dann von Hackern ausgenutzt wird.

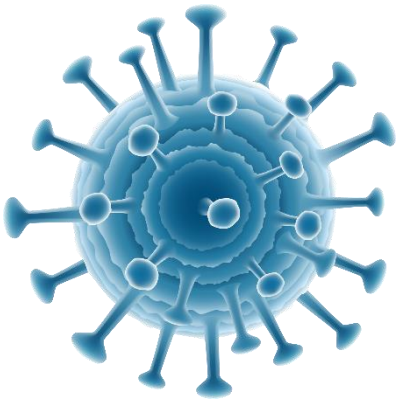


4. **Drive-by Download:** Hierbei handelt es sich um eine Methode, bei der Malware automatisch heruntergeladen wird, wenn ein Benutzer eine kompromittierte Website besucht, ohne dass eine Interaktion erforderlich ist.
   - **Beispiel:** Der Benutzer klickt auf einen Link, der eine infizierte Website öffnet, und die Malware wird sofort heruntergeladen.

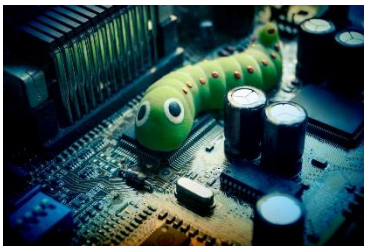
5. **Cross-Site Scripting (XSS):** Diese Technik erlaubt es Angreifern, schädlichen Code in eine vertrauenswürdige Website einzufügen. Wenn ein Benutzer die Website besucht, wird der schädliche Code ausgeführt.
   - **Beispiel:** Ein Angreifer könnte ein Kommentarfeld auf einer Website verwenden, um JavaScript einzuschleusen, das Cookies des Benutzers stiehlt.

2.1.2 Arten von sich selbst verbreitender Malware

1. **Virus:** Ein Virus ist ein Programm, das sich an andere Programme oder Dateien anheftet und sich verbreitet, wenn diese Programme ausgeführt oder Dateien geöffnet werden. Viren können Schäden anrichten, indem sie Dateien löschen oder verändern. Das Virus wird meist unbeabsichtigt von Benutzern verbreitet.
   - **Beispiel:** Ein Benutzer öffnet ein infiziertes Dokument, das einen Virus enthält, der sich dann auf andere Dateien auf dem Computer ausbreitet.



2. **Wurm:** Ein Wurm ist eine Art von Malware, die sich selbstständig über Netzwerke verbreitet. Im Gegensatz zu Viren benötigen Würmer keine Wirtsdatei, um sich zu replizieren.
   - **Beispiel:** Ein Wurm kann sich über E-Mail-Anhänge verbreiten. Wenn ein Benutzer einen infizierten Anhang öffnet, wird der Wurm aktiviert und beginnt, sich an andere Kontakte in seinem Adressbuch zu senden.



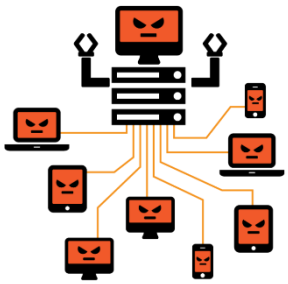
2.1.3 Arten von Malware für Datendiebstahl, Betrug oder Erpressung

1. **Adware:** Adware zeigt Werbung an, oft ohne die Zustimmung des Benutzers. Einige Adware-Programme sammeln auch Daten über das Surfverhalten der Benutzer, um gezielte Werbung zu schalten.
   - **Beispiel:** Ein Benutzer installiert eine kostenlose Software, die Werbung in seinem Webbrowser anzeigt und dabei Informationen über seine Online-Aktivitäten sammelt.

2. **Ransomware:** Ransomware verschlüsselt Dateien auf dem Computer des Opfers und fordert Lösegeld, um die Dateien wieder freizugeben. Diese Art von Malware kann äußerst schädlich sein.
   - **Beispiel:** Ein Benutzer erhält eine Meldung, dass seine Dateien verschlüsselt wurden und ein Lösegeld in Bitcoin gezahlt werden muss, um sie wieder zu entschlüsseln.

3. **Spyware:** Spyware sammelt heimlich Informationen über die Aktivitäten eines Benutzers, oft ohne dessen Wissen. Dazu gehören Passwörter, Kreditkarteninformationen und Surfgewohnheiten.
   - **Beispiel:** Eine Anwendung, die heimlich Tastatureingaben aufzeichnet, um Zugang zu Bankdaten zu erhalten.

4. **Botnet:** Ein Botnet besteht aus einer Gruppe von infizierten Computern, die von einem Angreifer kontrolliert werden. Diese Computer (Bots) können für verschiedene böswillige Aktivitäten genutzt werden, wie z. B. Distributed Denial-of-Service (DDoS) Angriffe.
   - **Beispiel:** Ein Angreifer nutzt ein Botnet, um eine Website durch eine Flut von Anfragen lahmzulegen.



5. **Keylogger:** Keylogger sind Programme, die die Tastatureingaben eines Benutzers aufzeichnen. Sie werden häufig verwendet, um Passwörter und persönliche Informationen zu stehlen.
   - **Beispiel:** Ein Benutzer tippt sein Passwort ein, während ein Keylogger im Hintergrund läuft und die Eingaben aufzeichnet.

6. **Dialer:** Dialer sind Programme, die den Internetzugang eines Benutzers ohne dessen Zustimmung ändern. Sie können hohe Telefongebühren verursachen, indem sie zu kostenpflichtigen Nummern verbinden.
   - **Beispiel:** Ein Benutzer installiert ein kostenloses Programm, das im Hintergrund einen Dialer aktiviert, der teure Anrufe zu einer kostenpflichtigen Nummer tätigt.