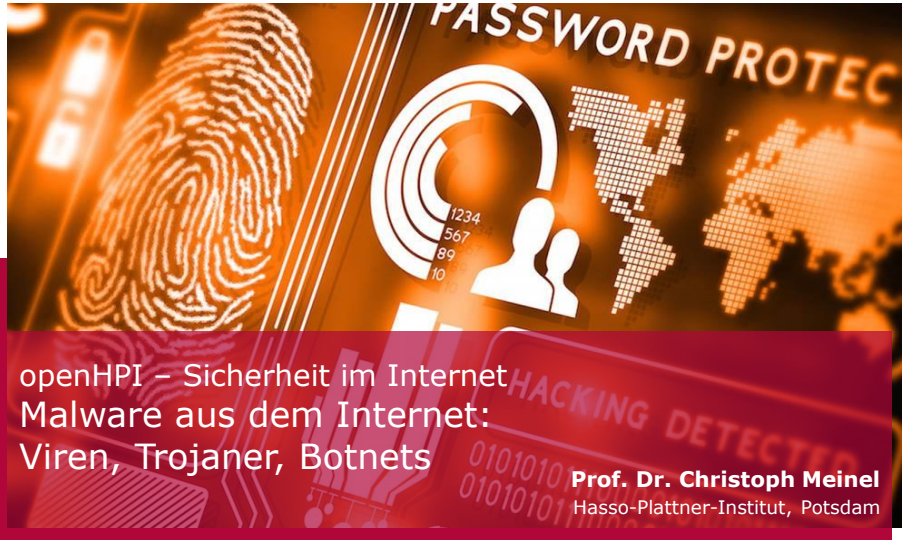




openHPI – Sicherheit im Internet
Malware aus dem Internet:
Viren, Trojaner, Botnets

Prof. Dr. Christoph Meinel
Hasso-Plattner-Institut, Potsdam

Malware - Schadsoftware

Malware - Malicious Software – Bezeichnung für Schadsoftware, also für bösartige Software, die von Hackern meist über das Internet auf das Gerät eines ahnungslosen Nutzers geschmuggelt wird, um dort im Sinne der Cyberangreifer aktiv zu werden

Bekannte Beispiele von Malware sind z.B.

- Viren
- Würmer
- Trojaner
- Botnets
- Rootkits
- Adware
- Spyware
- ...

Als **Viren** werden schädliche Miniprogramme bezeichnet, die sich selbständig in bestehende Programme („Wirtsprogramm“) integrieren

- Verfälscht bzw. verändert Wirtsprogramm
- Integration erfolgt teilweise sogar, ohne dass sich die Größenangabe oder das letzte Änderungsdatum des Wirtsprogramms verändert
- Vervielfältigt sich lokal mithilfe des Wirtsprogramms
 - Reproduktion wirkt sich insbesondere auf die Leistung des infizierten Systems aus
- Kann Arbeitsfähigkeit des Systems (Computer, Laptop, Smartphone, ...) beeinflussen

Würmer sind Schadprogramme, die sich nach Ausführung selbständig über das Netzwerk oder Wechselmedien (z.B. USB-Sticks) verbreiten

- Kann sich nach Weiterverbreitung selbst starten
 - Nutzer muss Ausführung nicht ausdrücklich zustimmen
 - Oftmals schnellere Ausbreitung als Viren
- Funktioniert eigenständig, braucht kein Wirtsprogramm
- Schadcode (Payload) hat nach Ausführung oft verheerende Auswirkungen auf das befallene System:
 - Beeinträchtigung der Leistung,
 - Nachinstallation anderer Malware,
 - Öffnung von Hintertüren (Backdoors),
 - infizierter Rechner wird zu Bot in einem Botnet gemacht,
 - ...

Malware: Trojaner bzw. Trojanisches Pferd

Als **Trojaner** werden Computerprogramme mit versteckter Schadfunktion bezeichnet, die sich als nützliche Anwendungen tarnen

- Bei Ausführung der vermeintlich gutartigen Anwendung wird automatisch die schädliche Funktion ausgeführt
 - teilweise parallel zu erwarteter Funktionalität, um unbemerkt zu bleiben
- Trojaner können sich auch als Dokumente oder Dateien tarnen
 - Schadfunktion wird beim Öffnen des Dokuments / der Datei ausgeführt
 - **Beispiel:** Vorgespiegeltes Login-Formular, um Nutzernamen-Passwort-Kombination abzugreifen

Malware: Keylogger

Ein **Keylogger** ist ein Miniprogramm, das sämtliche Tastatureingaben des Benutzers aufzeichnet

- Leistungsfähigere Varianten erfassen zusätzlich den Inhalt des Bildschirms
- Aufnahme der Tastatureingaben wird z.B. gestartet, wenn auf dem Bildschirm ein Eingabefeld für Passwörter erscheint
- Die aufgezeichneten Nutzereingaben werden dann in einer für den Angreifer zugänglichen Datei abgelegt oder an den Angreifer gesendet
- Angreifer verwendet Informationen z.B.
 - zum Identitätsdiebstahl,
 - für Banküberweisungen,
 - ...

Ein **Botnet** ist ein Zusammenschluss zahlreicher verschiedener Computer – **Bots** –, der typischerweise ohne Wissen der Computerbesitzer erstellt wird

- Zentraler „Command and Control Server“ – **C&C Server** – in den Händen eines Angreifers verwaltet, koordiniert und steuert die (zahlreichen) Bots aus der Ferne
- C&C Server übernimmt Kontrolle über die Bots und schickt Handlungsanweisungen an die Bots, die diese dann selbstständig ausführen, z.B. Start eines DoS-Angriffs ...
- Botnets mit vielen ferngesteuerten Bots können mit sehr hoher Rechenkraft eine Vielzahl gefährlicher Angriffe ausführen ... → eigenständiger Clip zu Botnets

Ein **Rootkit** ist eine Schadsoftware, die dem Angreifer einen kontinuierlichen Zugriff auf ein einmal gekapertes System ermöglicht

- Werden meist bei einem Einbruch auf dem System installiert
- Versucht seine eigene Existenz auf dem System zu verbergen
 - offene Verbindung oder bestimmte Dateien werden maskiert
 - weitere Schadprogramme werden vor Nutzer/ Antivirus versteckt

Eine **Backdoor** ermöglicht es einem Angreifer, unberechtigt auf einem fremden Computer Zugriff zu erlangen

- Für Cyberkriminelle ist es sehr attraktiv, über versteckte Zugänge zu einem System zu verfügen

Malware: Adware

Als **Adware** werden Programme bezeichnet, die zusätzlich zur eigentlichen Funktionalität Werbung einblenden

- Adware kann sich auch in den Web-Browser einnisten, wodurch auf jeder Internetseite Werbung eingeblendet werden kann
- Auch Schadsoftware, die Werbung verwendet, wird als Adware bezeichnet, z.B.
 - Browser-Plugins, die JavaScript mit Werbung auf jeder Seite einbetten

Malware: Spyware

Als **Spyware** wird Software bezeichnet, die ohne Zustimmung des Besitzers eigene, sensible Daten an Dritte versendet, z.B.

- Hersteller der Software, Anbieter von Webdiensten, staatliche Behörden, ausländische Geheimdienste, ...
- Spyware wird auch als Spionagesoftware, Schnüffelsoftware, Spähprogramm, ... bezeichnet
- Datenübermittlung erfolgt im Verborgenen
- Wird oft eingesetzt, um personalisierte Werbung anzuzeigen und das Surfverhalten zu verfolgen
- Aber auch genutzt für die Informationsbeschaffung von persönlichen Daten, z.B.
 - Passwörtern,
 - Kreditkartendaten,
 - ...

Malware: Scareware

Scareware versucht durch das Vortäuschen von Fehlermeldungen, Virusinfektionen oder anderen Problemen Nutzer zu verunsichern

- Oftmals werden besonders aktuelle oder prominente Viren- und Fehlermeldungen verwendet, um die Bedrohung möglichst dramatisch erscheinen zu lassen
- Dann werden Strafzahlungen oder kostenpflichtige Reparaturen gefordert
- In Deutschland sehr bekannt:
 - Aufzählung von Rechtsverstößen des Nutzers im Namen der Polizei
 - Aufforderung einer Strafzahlung
 - ...



Malware: Rogueware/ Rogue-Antivirus

Rogueware ist ein eigenständiges Programm, das eine vertrauenswürdige Herkunft vortäuscht, um an sensible Informationen oder an Geld zu gelangen

- Vortäuschung der Säuberung des Computers, während dabei dann Schadprogramme eingeschleust oder Daten gestohlen werden

Rogue-Antivirus ist eine spezielle Art von Rogueware, die sich als Antivirusprogramm tarnt

- „Scannt“ Computer und „findet“ verschiedene Schadsoftware
- Es wird kein wirklicher Scan durchgeführt, aber es werden „Infektionen“ gemeldet (auch auf fehlerfreiem System)
- Nutzer wird anschließend aufgefordert, eine kostenpflichtige Reparatur durchzuführen

Als **Ransomware** wird ein Schadprogramm bezeichnet, das dem Nutzer den Zugriff auf seine Daten verwehrt und Geld zur Freischaltung erpresst

- Verschlüsseln persönliche Daten so, dass das Opfer seine eigenen Daten nicht mehr einsehen und nutzen kann
- Dann wird dem Opfer eine kostenpflichtige Entschlüsselung der Daten angeboten
- BSI rät von Zahlung ab, da oft weitere Aufforderungen folgen oder Daten trotz Zahlung nicht entschlüsselt werden
- Infektion erfolgt über Email-Anhänge, Trojaner, ...

Schutzmaßnahme:

- Regelmäßige Sicherung aller wichtigen Daten und Unterbindung des initial notwendigen Zugriffs auf den Computer

Heutige Schadsoftware (Malware) lässt sich zumeist **nicht mehr eindeutig** einer der genannten Typen zuordnen

- Meist werden innerhalb einer Malware verschiedene Schadfunktionen eingesetzt. Teilweise können auch zusätzliche Bestandteile nachgeladen werden
- **Beispiel:** Bekannte **Carberp** Malware enthält verschiedene Funktionen von einem
 - Trojaner
 - Keylogger
 - Rootkit
 - Backdoor
 - ...