



openHPI – Sicherheit im Internet Malware: Spektakuläre Beispiele

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

Malware – Einige Spektakuläre Beispiele

Wollen im Folgenden auf einige populäre Angriffe und Sicherheitsvorfälle im Internet eingehen, die durch Malware verursacht wurden:

- „Cookie Monster“
- Makroviren „I love you“
- Conficker
- Stuxnet
- Regin
- „Kampagnen“ Malvertising
- Ransom32

Cookie Monster ist weder richtiger Virus (repliziert sich nicht) noch Wurm (verbreitet sich nicht), wird deshalb als „Proto-Virus“ bezeichnet

- Erstes weltweit populäres Beispiel für Computer Malware
- Trieb sein Unwesen Ende der 1960er Jahre
- Zielte ursprünglich auf Nutzer des Computernetzwerks der Brown University ab
- Schickte Nachrichten, die andere Anwendungen blockierten und nach „Cookies“ fragten
 - beeinträchtigte damit stark die Leistungskraft des betroffenen Computers
- Erst nachdem Nutzer „Cookie“ eingetippt hatte, waren die blockierten Anwendungen weiter ausführbar und Nutzer konnte weiterarbeiten

ILOVEYOU-Schadsoftware, die ab dem 5. Mai 2000 aus Philippinen verbreitet wurde

- Wird als Email versendet mit dem Betreff „ILOVEYOU“ und dem Anhang „LOVE-LETTER-FOR-YOU.txt.vbs“
- Die .vbs (Visual Basic Script) Endung wurde in Windows Systemen nicht angezeigt und betroffene Nutzer öffneten die Malware als vermeintliche Textdatei
- Infiltrierte Malware versendete sich dann selbst an alle Kontakte aus dem Windows Adressbuch und überschrieb Bilddateien
 - Nutzer sahen Email als vertrauenswürdig an, da sie von einem bekannten Kontakt (aus dem Adressbuch) kam
- Schaden wird auf 5,5 – 8,7 Milliarden US\$ geschätzt
- Nach Schätzungen waren 10% aller Internetnutzer betroffen; in den ersten 10 Tagen wurden 50 Millionen Infektionen bekannt

Conficker wurde erstmals im November 2008 entdeckt

- Befiel Windows Systeme sowohl
 - über Schwachstellen in Windows als auch
 - über Attacken auf Administrator Passwörter
- Über Internetverbindungen zu anderen infizierten Computern wurden dann Erweiterungen nachgeladen
- Integrierte betroffene Systeme in ein Botnet
- Verschiedene Ausprägungen mit unterschiedlichen Angriffsarten
 - Befehle werden über das Netzwerk empfangen und ohne weitere Kontrolle ausgeführt
 - Installiert sich auf Wechselmedien und missbraucht „Autostart“ Funktion
 - Wörterbuch-Angriffe auf Admin-Passwort
 - Verwendet Datei-/ Druckerfreigaben zur Verbreitung

Stuxnet-Wurm wurde Ende 2007 in Umlauf gebracht, jedoch erst 2010 entdeckt

- Nutzt eine Vielzahl bis dahin unbekannter Schwachstellen in Windows Systemen und Netzwerken aus
- Sucht anschließend nach Kontrollsoftware der Firma Siemens:
 - Software zur Steuerung technischer Prozesse in Wasserwerken, Pipelines, Fabriken oder Atomkraftwerken
- Einmal über Wechselmedien (USB-Stick) ins Netzwerk eingeschleust, wird dann nur sporadischer Internetzugang benötigt für Rückmeldungen
- Veränderte unbemerkt Einstellungen der Steuerungssoftware
- Stuxnet führte im Ergebnis zu Zerstörungen in iranischen Atomkraftwerken und Verzögerung bei dessen Atomprogramm

Regin ist hochentwickelte Malware, die 2012 bekannt und hauptsächlich für Spionage-Zwecke eingesetzt worden war

- In den meisten Fällen befällt Regin Windows Systeme und enthält eine Vielzahl von Funktionalitäten:
 - Stehlen von Zugangsinformationen
 - Fernzugriff auf System (Steuerung von Maus und Tastatur)
 - Mitschneiden des Datenverkehrs
 - ...
- Infizierte auch Systeme von Mobilfunkbetreibern und konnte damit die Kommunikation beeinflussen und ausspionieren
- Die hohe Malware-Qualität und der komplexe Funktionsumfang deuten gerüchtemäßig hin auf Urheber mit staatlicher Unterstützung

Malvertising – Malicious Advertising (dt. bösartige Werbung)

- Angreifer registriert sich bei Werbenetzwerk und verteilt darüber bösartige Werbung
- Malware wird dann durch die bösartige Werbung nachgeladen, wenn dem Nutzer die entsprechende Werbung eingeblendet wird
- Im Oktober 2015 haben Cyberkriminelle in der sogenannten „Kampagnen“ Aktion Malware über bösartige Werbung verteilt
- Betroffene Internetseiten waren:
 - ebay.de
 - t-online.de
 - arcor.de
 - ...

Ransom32 wird seit Dezember 2015 auf einschlägigen Internetseiten als Ransomware-Dienst angeboten

- Malware wird einfach über die Internetseite erzeugt
- Ziel: Erpressung von Bitcoins (Kryptowährung) von Opfern
- 25% der „Einnahmen“ werden von den Entwicklern einbehalten

Die Entwickler setzen Techniken ein, die eine Ausführung auf unterschiedlichen Plattformen (z.B. Windows, Mac, Linux) ermöglicht

- Zusätzlich zur Verschlüsselung der Nutzerdaten enthält Ransom32 aber auch weitere Funktionen, z.B.
 - Sperren des Computers