Kapitel 8: Schadsoftware

8: Malicious Software (Malware)

Malware (http://www.itwissen.info/definition/lexikon/Malware-malware.html)

Mal (*malicious* (eng.) oder *malus* (lat.)) + (Soft) **ware**

[. . .] Malware ist bösartige Schadsoftware, die die IT-Sicherheit und die Funktionsfähigkeit von Computern und Systemen beeinträchtigt. [. . .] Bei Malware handelt es sich immer um Aktivitäten, die vom Benutzer nicht erwünscht sind und durch Robots (Bot) übertragen und verbreitet werden.

- Virus, Wurm, Trojanisches Pferd, Backdoor
- Spyware, Adware, Scareware, Ransomware, Rogueware
- Malware musst nicht immer bösartig sein (Welchia Worm)
- Malware zählt immer zu **vorsätzlichen Handlungen**

IT-Sicherheit – Deutschland

Von Malware befallene Computer

Infizierung

- Rot ca. 30%
- Grün ca. 20%
- Blau ca. 15%

Quelle: `https://www.netzsieger.de/ratgeber/malware-statistiken`

IT-Sicherheit – Deutschland

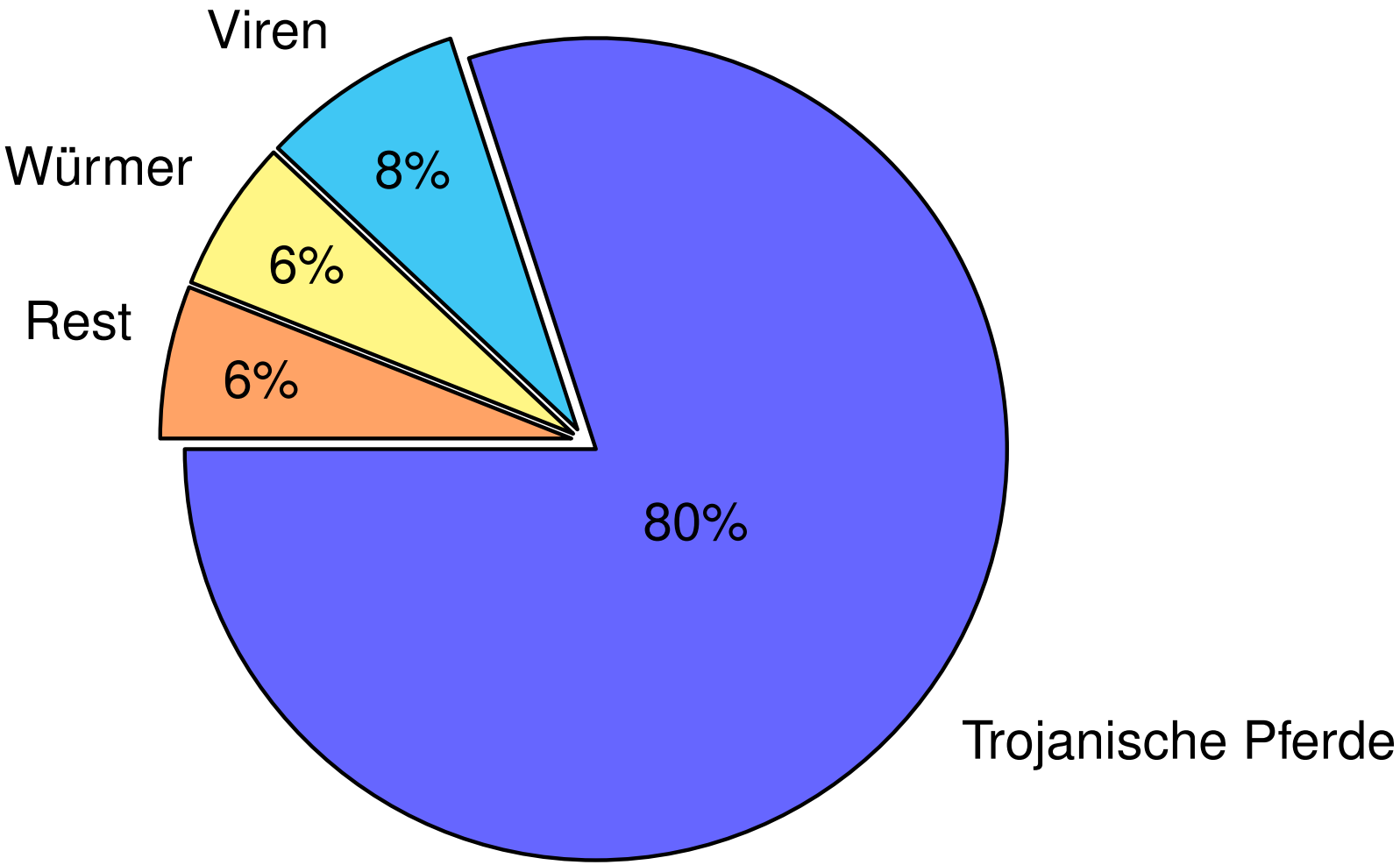
Ein paar Zahlen aus 2015

- 142 Mio. neue Malware-Programme (390.000 pro Tag)
- ca. 25% aller Computer sind befallen (weltweit: ca. 32%)
- 8,3% aller Websites mit Malware (weltweit) kommt aus Deutschland
- ca. 5,9% aller Mails sind Spam
- ca. 5% aller Straftaten mit “Tatmittel Internet”

Quelle: `https://www.netzsieger.de/ratgeber/malware-statistiken`

IT-Sicherheit – Deutschland

Malwareverteilung 2015

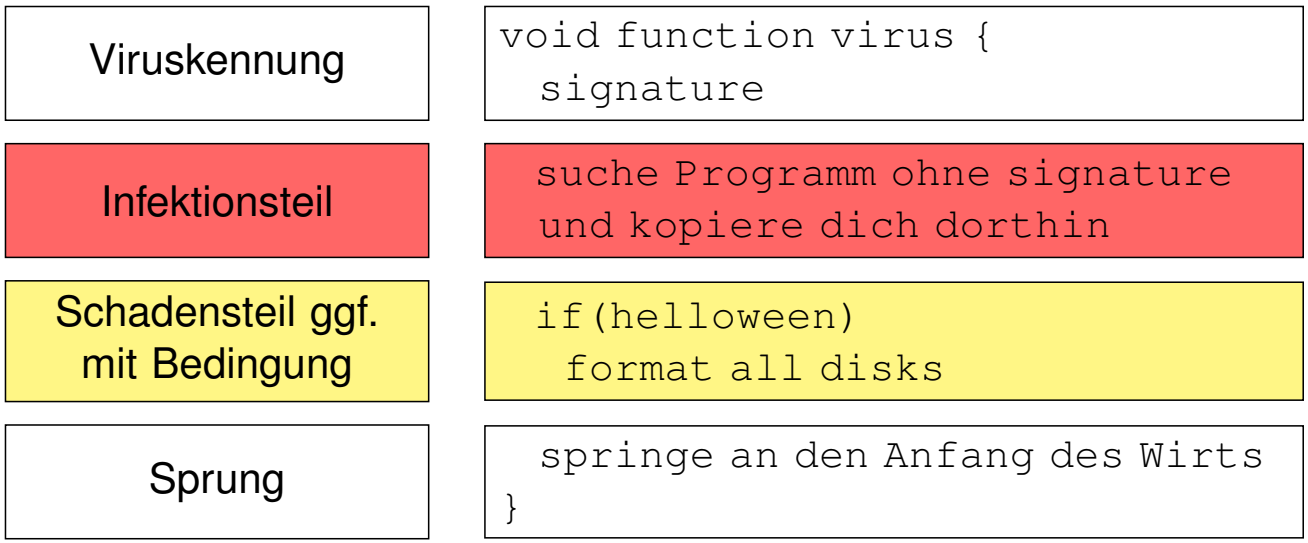


8.1: Viren

Virus

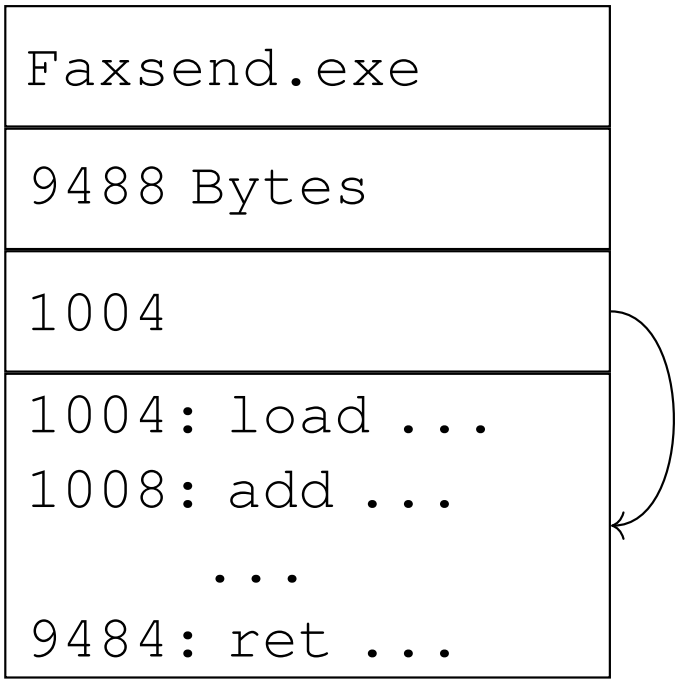
- Kein selbstständig ablauffähiges Programm.
- Benötigt Wirtsprogramm zur Ausführung.
- Selbstreplikation (Infektion weiterer Wirte (Programme))

Allgemeiner Aufbau

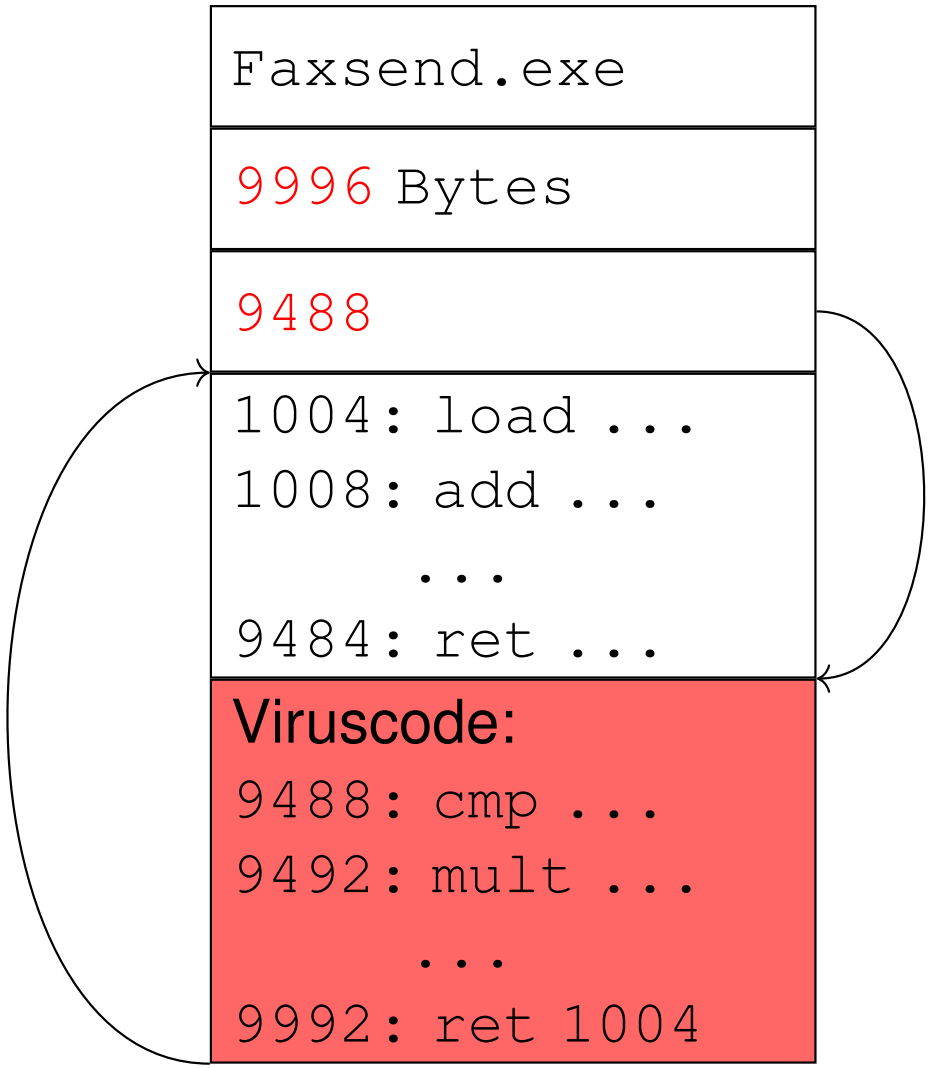


Program-Viren: Infektion

Dateiformat vor der Infektion



Dateiformat nach der Infektion



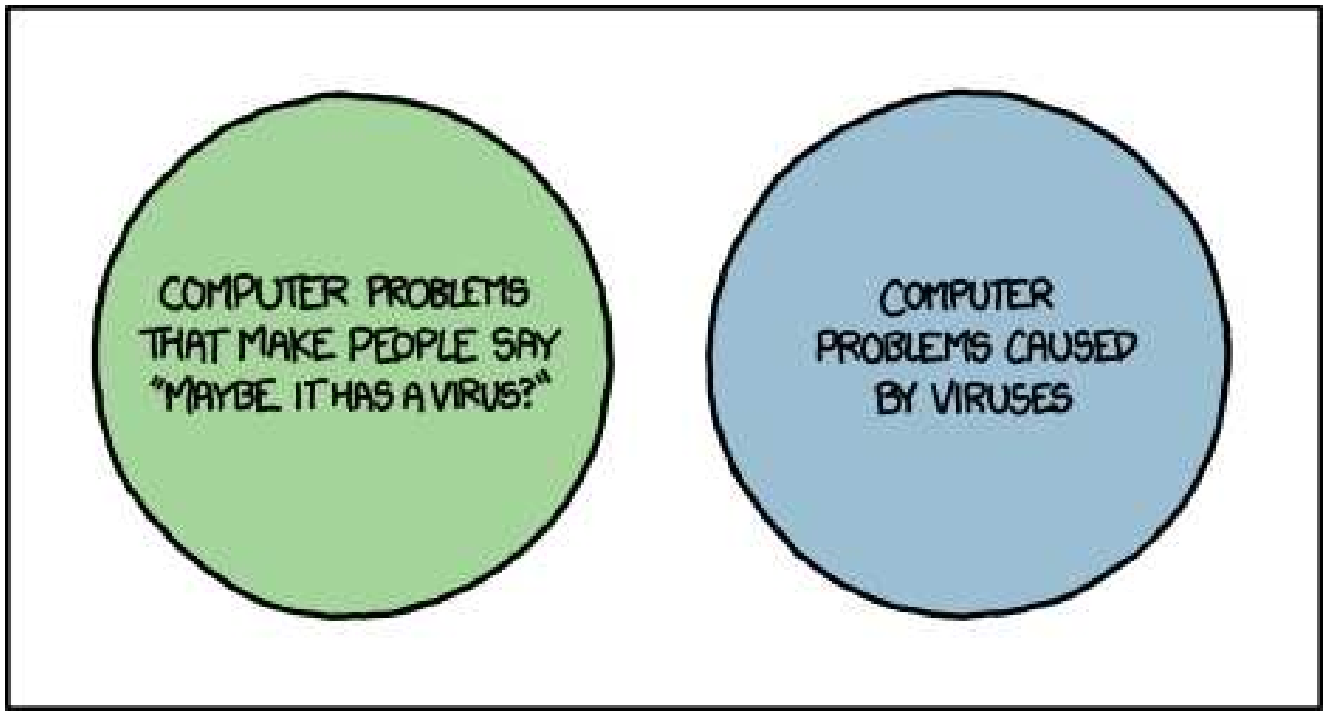
Viren: Klassifikation I

- **Programm-Virus (Link-Virus)**
  Infiziert ausführbare Dateien (MS-DOS/Windows: .exe, .com).
- **Bootsektor-Virus**
  Infiziert den Bootsektor von Festplatten oder Disketten.
- **Makro-, Daten-Virus**
  Makro-, Daten-Virus Infiziert „Daten-Dateien“ mit eingebetteten Makro-Sprachen (z.B. Visual Basic in MS Office, Flash, . . .).
- **Multipartiter bzw. hybrider Virus**
  Infiziert mehr als ein Ziel, z.B. Bootsektor + Programme.

Viren: Klassifikation II

- **Polymorpher Virus**
  Verschlüsselt den Viruscode; damit für Anti-Viren-Software (AV) schwerer zu finden.
- **Retro-Virus**
  Greift aktiv AV an; versucht Scanner so zu verändern, dass er unentdeckt bleibt.
- **Stealth-Virus**
  Virus versucht, sich vor AV zu verstecken. Sobald AV Dateien scannt, entfernt der Virus seinen Code aus den infizierten Dateien (Wiederherstellung des Orginalzustandes)
- **Tunneling-Virus**
  Virus mit Superuser-Rechten der sich versteckt, in dem er Systemcalls des AV unterbricht die zu seiner Entdeckung führen können.

Virus, der default Schuldige



Quelle: `https://xkcd.com/1180/`

8.2: Würmer

Wurm

- Eigenständig lauffähiges Programm - benötigt keinen Wirt!
- Selbstreplikation (z.B. über Netz oder USB-Sticks (mit „Autorun“)).
- Einzelne infizierte Maschinen werden als Wurm-Segmente bezeichnet.

Internet Worm: Historischer Rückblick, 1988

Chronologie der Vorfälle an der University of Utah

Mittwoch 2. November 1988

- 17:02: Test oder Start des Wurms
- 17:04: Maschine an der Cornell University "befallen"
- 20:49: Wurm infiziert VAX 8600 an der Univ. Utah (cs.utah.edu)
- 21:09: Wurm versucht von VAX aus andere Maschinen zu infizieren
- 21:21: Load (Anzahl der rechenbereiten Prozesse) von 5
- 22:01: Load von 16
- 22:06: Es können keine Prozesse mehr gestartet werden, Benutzer können sich nicht mehr anmelden.
- 22:20: Systemadministrator terminiert den Wurm Prozess
- 22:41: Der Wurm ist zurück; Load 27
- 22:49: System shutdown, reboot
- 23:21: Der Wurm ist zurück; Load 37

Internet Worm: Globale Sicht, 1988

- Mittwoch 2. Nov. 1988
  - 17:02: Test oder Start des Wurms
  - 21:00: Stanford University; ca. 2500 Unix Maschinen infiziert
  - 21:30: MIT infiziert
  - 22:54: University of Maryland
  - 23:00: University of California, Berkeley
- Donnerstag, 3. Nov. 1988
  - 2:28: E-mail Warnung; erreicht aber die meisten nicht vor Samstag
  - 5:58: Bug fix posting aus Berkeley
    - Sendmail's `debug` Kommando deaktivieren
    - C Compiler umbenennen
    - Linker umbenennen
  - 10:30: TV Teams am MIT
  - 11:00: Titel-Story in den Nachrichten:
    Mehr als 6000 hosts im Internet infiziert (10%)

Internet Worm: "How it works (1/2)"

- Befall neuer Maschinen
  - `sendmail`
  - `finger` Bug; Buffer Overflow (nur VAX werden befallen)
  - Remote execution (`rsh, rexec`)
- Finden von neuen Zielen
  - `/etc/host.equiv` (list of trusted hosts)
  - Gateways aus der Routing-Tabelle
  - Endpunkte von Point to Point Verbindungen
  - Zufällig geratene Adressen
  - Datei gebrochener Accounts
    - `.rhosts` (Users `/etc/hosts.equiv`)
    - `.forward` (Email forwarding information)

Internet Worm: "How it works"(2/2)

- User Accounts öffnen
  - Offensichtliche Passwörter (Bentzername, Nachname, . . .)
  - Build-In Wörterbuch Angriff (432 Wörter)
  - `/usr/dict/words` (24.474 Wörter)
  - Trusted Host Beziehung (.rhosts)

- Was der Wurm NICHT tut
  - Versuchen *root* access zu erhalten
  - Well-known Accounts angreifen
  - Daten zerstören
  - "Zeitbomben" zurücklassen

Internet Worm: Programm Struktur

```
int main(int args, char *args[]) {
  argv[0] = "sh";                  /* rename process */
  if ( infected() ) return 0;  /* faults here causes mass
    infection */
  Initialize clock();

  while (true) {
    cracksome(); /* attack accounts, try to find hosts */
    sleep(30);                     /* hide the worm */
    if ( infected() ) return 0;  /* faults here causes
    mass infection */
    if (fork()) return 0;          /* Camouflage */
    try to attack some machines;
    sleep(120);                    /* hide the worm */
    if (running > 12 hours)
      cleaning host List;          /* reduce memory
    consumption */
    if (pleasequit) return 0;
```

Internet Worm: Lessons Learned

- (lange) bekannte Bugs fixen.
- Starke Passwörter benutzen.
- Least privilege Prinzip (sowenig Rechte wie nötig) einhalten.
- Strenge Zugriffskontrolle implementieren.
- Logging und Auditing Dienste benutzen.
- Keine reflexartigen Reaktionen.
- Kontinuierliche Informationfluß aufrecht erhalten.
- „Zentrales“ Security Repository CERT (Computer Emergency Response Team) wurde gegründet `www.cert.org`.

Internet Worm: Der Verursacher

- Robert T. Morris, 23, Cornell Student (Sohn des NSA Chief Scientist)
- Morris wollte mit dem Wurm die Computer im Internet zählen. :)
- Suspendierung von der Cornell University
- Verurteilt zu 10.000 USD und 400 Stunden gemeinnütziger Arbeit.
- 1995 gründet Morris das Softwareunternehmen Viaweb
- 1998 verkauf Morris Viaweb für 49 Millionen USD an Yahoo.
- Seit 1999 ist Morris Professor am MIT.

SQL Slammer: Historischer Rückblick, 2003

- Schnellster Wurm in der Geschichte.
- Beginn Samstag, 25. Januar 2003.
  - 5:30: Start des Wurms
  - Pro Minute: Verdopplung der Population alle 8,5 Sekunden ($\pm$ 1 s)
  - $>$ 3 Minuten: etwas verringerte Verbreitungsrate; Netzbandbreite wird zum beschränkenden Faktor
  - 5:40: ca 90% aller anfälligen Hosts sind infiziert.
  - 6:00: alle 75.000 anfälligen Hosts sind infiziert.
  - 07:11: Bugtraq Posting MS SQL WORM IS DESTROYING INTERNET BLOCK PORT 1434!".
- Folgen
  - Große Teile des Internets nicht mehr erreichbar.
  - Steuerungssysteme für die Stromversorgung gestört.
  - Funktionsstörungen bei Geldautomaten.
  - Wurm legt Sicherheitssystem des Davis-Besse Atomkraftwerks für 5 Stunden lahm (WTF?!?).

SQL Slammer: Infektion

- Infektion fand über den Monitor Port (UDP 1434) des MS SQL Servers 200 statt.
- Die Schwachstelle war seit längerem bekannt.
- Microsoft hatte Patch bereits 6 Monate zuvor (sic!) veröffentlicht.
- Problem
  - SW von Drittanbietern beinhaltet SQL-Server
  - Dies ist nicht allgemein bekannt

SQL Slammer: Funktionsweise

- Slammer passt in ein UDP Packet.
  - 376 Byte groß, geschrieben in Assembler.
  - Mit Header Informationen 404 Byte.
- Slammer nutzt Buffer-Overflow an UDP Port 1434
- Nach Infektion
  - *Rate*zufälliger IP-Adresse
  - Sende SQL-Slammer als UDP-Packet an Port 1434.
- Keine Schadfunktionalität im eigentlichen Sinn
- Charakteristika
  - Keine persistente Speicherung (Slammer lebt nur im RAM).
  - UDP verbindungsloses Protokoll; wird nur durch Bandbreite beschränkt
  - Höchste beobachtete „Probing“-Rate: 26.000 Scans pro Sekunde
  - Aggressive Verbreitungsstrategie führt dazu, dass der Wurm mit anderen Würmern um Netzbandbreite konkurriert

SQL Slammer: Lessons Learned

- Grundproblematik: kein Einspielen von Patches.
- Bundling von Software; Anwender weiß u.U. nichts von Sicherheitsproblemen und notwendigen Patches.
- Angriffe über UDP können zu extrem schneller Verbreitung führen.
- Gegenmaßnahmen
  - Sicherheitsupdates einspielen
  - Nicht benötigte Dienste deaktivieren.
  - Filtern des entsprechenden Verkehrs (UDP Port 1434) über Firewall.

Stuxnet: Deutsches Presse-Echo 2010

- Stuxnet-Wurm kann Industrieanlagen steuern (heise.de, 16.09).
- Digitale Bedrohung Virus könnte Akw übernehmen (taz.de, 17.09).
- Der digitale Erstschlag ist erfolgt (FAZ, 22.09).
- Rätselhafte Schadsoftware – Cyberkrieg: Sabotageziel Iran (SZ.de, 23.09).
- Geheimnisvolle Cyber-Attacke: Stuxnet – Wurm befällt Rechner in iranischem AKW (Spiegel Online 26.09).
- Iran im Krieg 2.0 (zeit.de, 30.09).
- Stuxnet breitet sich weiter aus (Financial Times, 4.10).
- Stuxnet: Vorgeschmack auf den Cyber-Krieg? (DW, 5.10).
- ...

Der Computerwurm Stuxnet

- Bei Stuxnet handelt es sich um einen sehr ausgreiften Wurm.
- Angriffsziel: Simatic S7-Anlagen (Industrieanlagen).
- Angriffsvektor: WinCC Software zum Management von Industrieanlagen.
- Zu diesem Zweck befällt Stuxnet Windows-Rechner.

Stuxnet – Infektion von Windows Rechnern

- Versucht sich über LAN zu verbreiten, in dem nur eingeschränkte. oder keine Internet-Konnektivität besteh.t

- Installation von RPC-Server und Client.
- Peer-to-Peer Kommunikation zwischen infizierten Rechnern.
- Damit Update-Möglichkeit für neuere Versionen.

- Versuch Datei-Freigaben für Weiterverbreitung zu nutzen

- Installation eines Windows-Rootkit.

Stuxnet – Infektionsvektoren (1/2)

- `autorun.inf`-Dateien können von Windows auch als EXE-Datei intepretiert werden.

- Windows Server Service RPC Handling vulnerability, aka. Conficker Bug (CVE-2008-4250)
- Der Conficker Bug ist bekannt seit 25.09.08 (Patch 26.10.08).

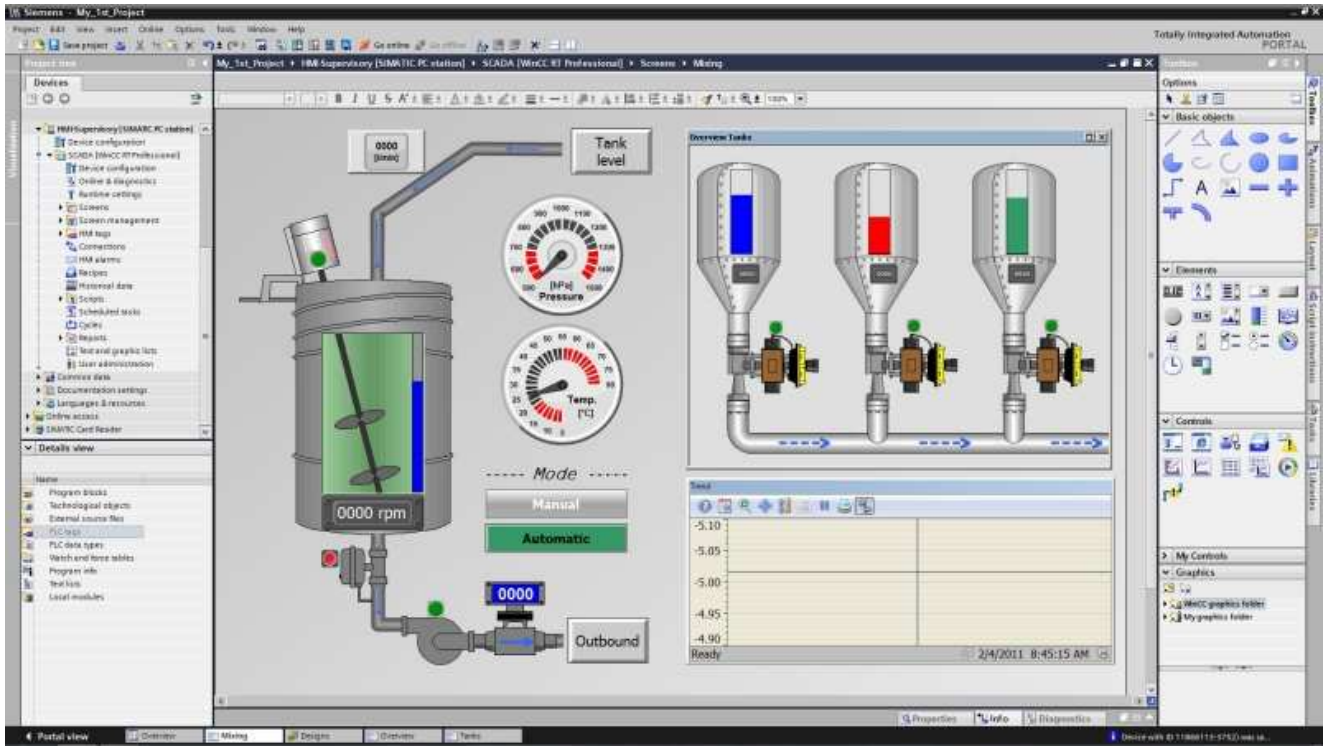
- LNK / CLINK: LNK-Datei auf USB Stick;
- Beim Lesen des Icons einer LNK-Datei wird Code ausgeführt (CVE-2010-2568)
- Der Bug ist bekannt seit 30.06.10 (Patch 02.08.10).

Stuxnet – Infektionsvektoren (2/2)

- Payload-Dateien; Treiber (MrxCls.sys, MrxNet.sys) sind digital signiert mit Zertifikaten von Realtek bzw. JMicron.
- Print Spooler Bug: Fehler in Druckerwarteschlange erlaubt Schreiben in Systemverzeichnis (CVE-2010-2729)
- Print Spooler Bug ist bekannt seit 14.07.10 (Patch 14.09.10).
- Privilege escalation über Keyboard layout file (Patch 12.10).
- Privilege escalation über Task Scheduler (Patch 14.12.10).

Stuxnet – Ziel: Infektion von WinCC

- Ziel von Stuxnet ist es zunächst WinCC zu infizieren.
- WinCC (Windows Control Center) ist ein Prozessvisualisierungssystem von Siemens.



Quelle: `http://www.ohlendorf.eu`

Angriff auf WinCC vom infizierten Windows Rechner

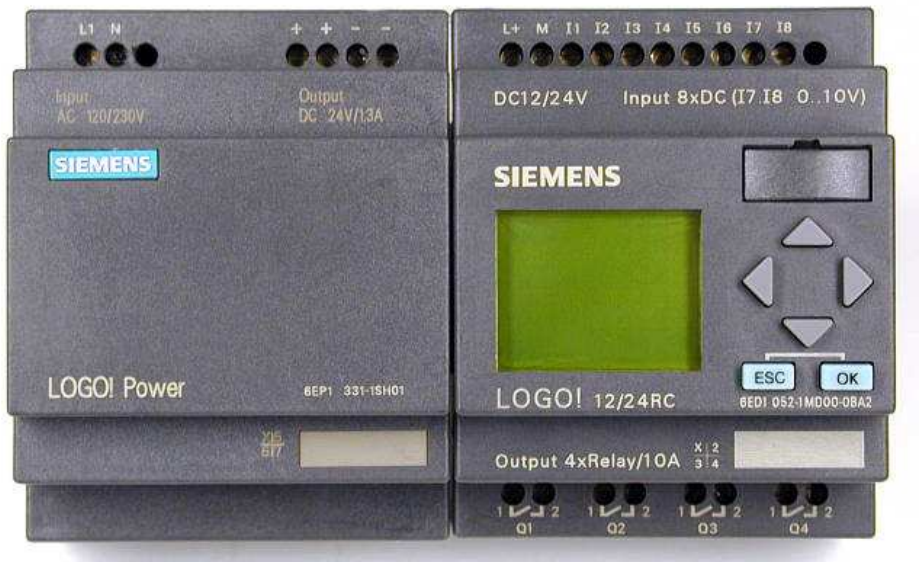
- Suche nach WinCC oder Siemens Step7 Software in Registry.

- Verbindung zum WinCC Datenbank-Server mit fest-kodiertem Account und Passwort (uid= WinCCConnec pwd= 2WSXcder).
- Siemens empfiehlt, wegen Stabilität der Steuerung, diesen Account nicht zu verändern.
- Mittel eines Malicious SQL-Statement infiziert Stuxnet die Datenbank.

- Stuxnetz ersetz die zentralen DLL (`s7otbxdx.dll`).
- Orginaldatei wird in `s7otbx`**`s`**`x.dll` umbenannt.

Angriff auf PLC von infiziertem WinCC

- Stuxnet überwacht alle Lese- und Schreibzugriffe auf PLCs. (Programmable Logic Device Contoller).
- Infektion eines PLC mit eigenen Code Blöcken.
- Masquerading einer PLC Infektion (PLC-Rootkit).
- Infizierter PLC arbeitet auch ohne Verbindung zum Steuerrechner.



Quelle: `https://degraveemiel.files.wordpress.com`

Stuxnet – Schadcode

Manipulation der Geschwindigkeit von Zentrifugen zur Urananreicherung.

- Normalwert 1064 Hz
- Stuxnet erhöht die Frequenz für 15 Min. auf 1.410 Hz
- Nach 27 Tagen Reduzierung auf wenige hundert Herz
- Folge: Zerstörung der Zentrifugen
- Wiki-Leaks meldet nuklearen Störfall in Natans (17.07.2009)
- Von 4.700 Zentrifugen arbeiten zu der Zeit nur 3.900

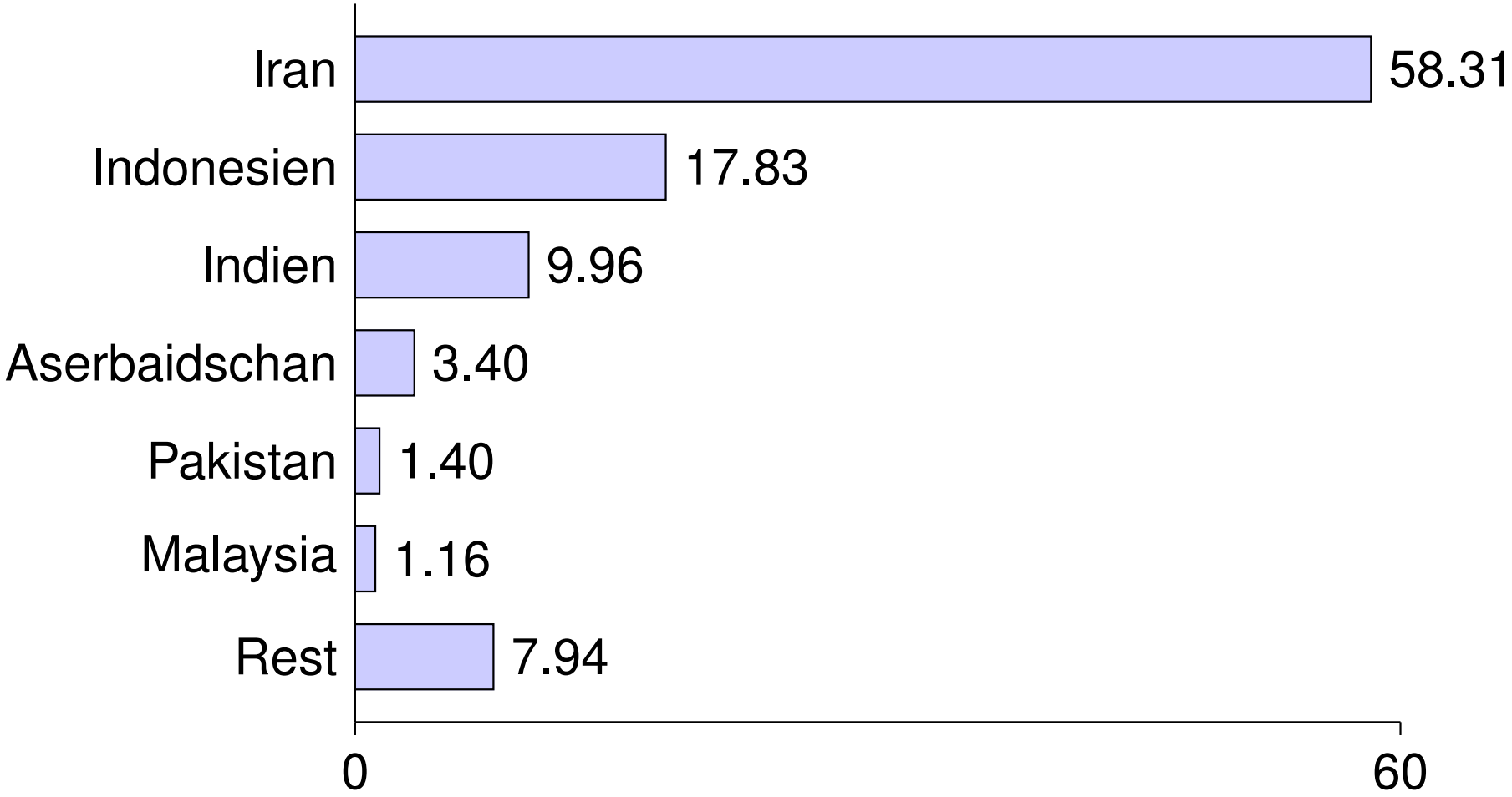
Stuxnet Analyse

- Viele verschiedene Exploits um Hostrechner anzugreifen
  - Vier Zero-Day Vulnerabilities.
  - Maskierungäls Treiber mit legalerSSignatur.
- Verschlüsselte Konfigurationen.
- Ïnfektion"von Dynamischen Bibliotheken (dll)
  - Systembibliotheken (Ntsys.dll).
  - ca. 10 Anti-Viren Programme (Kaspersky, McAffee, F-Secure,....).
- Komplexer Angriffs- und Installationsvektor.
- Installation einer Backdoor; Command and Control Server.
- Funktion eines Windows Rootkits.
- Injektion von Code in PLCs.
- Masquerading der Infektion auch der PLCs (PLC-Rootkit).

Ursachen und Ziele

- Bush startete Programm mit Code-Namen Ölympic Games".
- Obama entscheidet über Fortsetzung und beschleunigt Aktion.
- Experten vermuten bei Stuxnet handelt es es sich um die komplexeste und teuerste Malware in der Geschichte.
- Fachleute aus unterschiedlichen Bereichen notwendig
- Amerikaner, Europäer und Israelis sind beteiligt.
- Wurm wurde von ßecret Israeli unitünd Ämerican intelligence officialsprogrammiert.
- Angriffsziel: Zentrifugen in der Anreicherungsanlage Natanz.

Stuxnet: Geographische Verbreitung



(Quelle: w32_stuxnet_dossier.pdf)

Verteilung der insgesamt ca. 100.000 infizierten Rechnern.

Stuxnet: Fazit

*Stuxnet has highlighted **direct-attack attempts on critical infrastructure are possible** and not just theory or movie plotlines.*

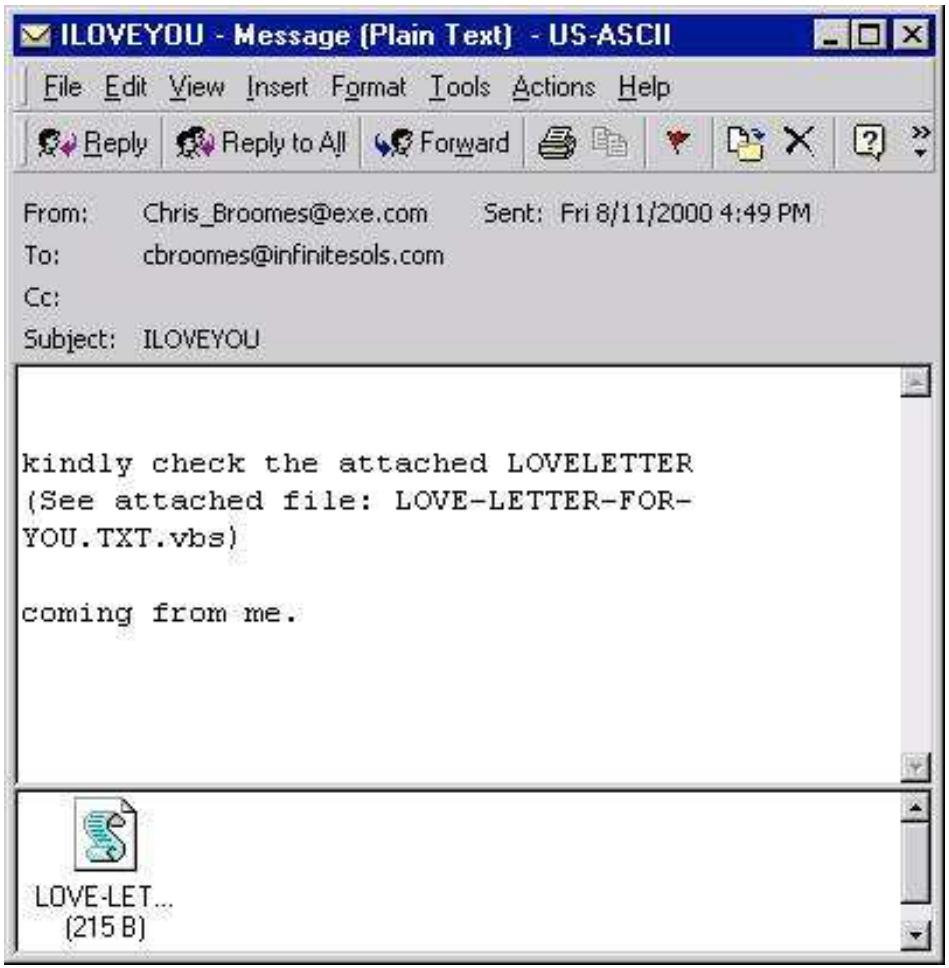
The real-world implications of Stuxnet are beyond any threat we have seen in the past. Despite the exciting challenge in reverse engineering Stuxnet and understanding its purpose, Stuxnet is the type of threat we hope to never see again.

(Symantec: w32_stuxnet_dossier.pdf)

Weitere Wurm Beispiele

- Mai 2000: ILOVEYOU (ausführbares E-Mail-Attachment, verschickt sich an alle im Adressbuch eingetragenen E-Mail-Adressen)
- Juli 2001: Code Red (Defacement von Microsoft IIS Webservern)
- November 2008: Conficker (Windows-Exploits + Wörterbuch-Angriff; infizierte Maschinen formen Botnet, weltweit > 15 Mio. infizierte Rechner)
- Juni 2010: Stuxnet
- August 2011: Morto (Wörterbuch-Angriff via Remote Desktop Protocol)
- September 2012: NGRBot (Messanger link zu `.exe`, tarnt sich per Rootkit, späht Daten aus, blockt Updates)
- ...

Beispiel: ILOVEYOU



8.3: Malicious Code: Trojanisches Pferd

Trojanisches Pferd

Ein Programm, welches neben gewünschter Funktionalität noch unerwartete/unbekannte und unerwünschte Funktonalität anbietet.

- Sinnvolle oder attraktive„ Nutzfunktionalität“
- Versteckte (Schad-) Funktionalität
- Keine selbständige Vervielfältigung

Trojanische Pferde: Beispiele

- Folklore: Rundung bei der Zinsberechnung
  - Nutzfunktion: Zinsberechnung mit drei Stellen Genauigkeit
  - Versteckte Funktionalität: Abgerundete Beträge ab der 4. Stelle aufsummieren und auf definiertes Konto buchen.
- 1998: T-Online Power Tools
  - Nutzfunktion: Unterstützende Werkzeuge für den T-Online Decoder
  - Versteckte Funktionalität: Bei der Registrierung (Shareware) werden T- Online-Zugangsdaten übermittelt
- 2001: Data Interception by Remote Transmission (D.I.R.T)
  - Integrierbar in (Nutzfunktion) wie Word, Exel und Powerpoint.
  - Versteckte Funktionalität: Keyboard-Logger, Screenshots, . . .
- 2011: *Staatstrojaner*

Der Staatstrojaner, 2011

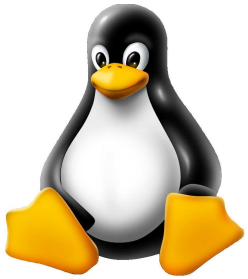
8.10.2011: Chaos Computer Club (CCC) veröffentlicht Analyse. `http://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf`

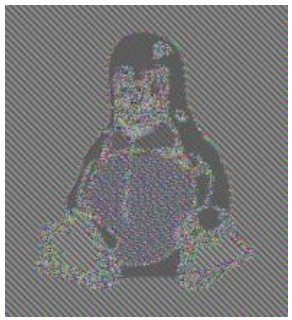
- CCC analysiert zugespielte DLL: `mfc42ul.dll`
  - Wird per Registry-Eintrag geladen
  - Klinkt sich bei der Initialisierung in `explorer.exe` ein
- Funktionen
  - Screenshots
  - Nachladen weiterer Module (sic!)
  - Abhören von Skype- und VoIP-Gesprächen
  - Kommunikation mit Command and Control (C&C) Server

Photo: mellowbox / flickr

Der Staatstrojaner: Die Kommunikation

- Einseitig AES-Verschlüsselung zwischen Malware und C&C-Server mit unsicherem ECB Mode unter konstatem Schlüssel.





- *Authentisierung* über konstanten Banner-String `C3PO-r2d2-POE`.
- Kommando-Kanal (C&C $\rightarrow$ Malware) unverschlüsselt; keine Authentisierung.
  - Malware somit durch Dritte steuerbar
  - Durch Nachladefunktion der Malware kann komplettes System durch Dritten übernommen werden
  - Zielperson kann durch gefälschte Beweise belastet werden
- Fest kodierte Adresse des C&C Servers : 207.158.22.134. (Hosting Provider Web Intellects in Ohio, USA)

Der Staatstrojaner: Der Befehlssatz

Eine kleine Auswahl der 18 unterstützten Befehle.

- `cmd3`: Screenshot geringer Qualität.
- `cmd 4`: Registrieren eines Kernelmode-Treibers.
- `cmd 6`: Löschen der Malware aus dem Dateisystem und Reboot.
- `cmd 8`: Liste aller Softwarekomponenten.
- `cmd 13`: Screenshot von Webbrowser und Skype.
- `cmd 14`: Nachladen eines Programms und unmittelbare Ausführung

Hardware-basierte/-nahe Trojanische Pferde

- Manipulierte Hardware / Firmware.

- BadUSB: Z.B. Manipulierte USB Memory-Sticks mit Tastaturemulation zum Absetzen von beliebigen Befehlen

Weitere Formen von Malicious Code

- Vordergründig oft kostenlose, interessante Anwendung
- Im Hintergrund:
  - Übermitteln des gesamten Adressbuchs an Hersteller
  - Übermitteln der eindeutigen Gerätekennung an Werbenetzwerke
  - Umleiten des Internet-Traffic über Server des Herstellers
  - Mining von Bitcoins o. ähnl.
  - Versand von Premium-SMS o.ähnl.
- Ohne Analyseumgebung (z.B. Simulator, Netzmonitoring) für Anwender nicht erkennbar

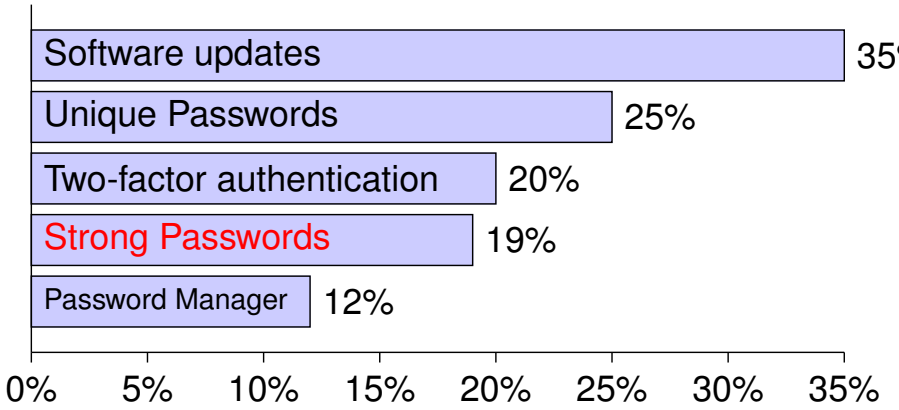
8.4: Schutz- und Gegenmaßnahmen

- Auf allen Systemen (Desktop + Server):
  - Nicht als Administrator anmelden
  - Verwendung von starken Passwörter
  - Regelmäßig Softwareupdates einspielen
  - Nicht benötigte Dienste deaktiveren/deinstallieren
  - Getrennt gelagerte, regelmäßig erstellte Daten-Backups
  - Keine Software zweifelhafter Herkunft installieren
  - Anti-Viren-Software installieren und aktuell halten
- Auf Desktop-Systemen
  - Automatische Makro-Ausführung, Autorun etc. deaktivieren
  - Mit Ad- und Scriptblocker surfen
- (Primär) auf Server-Systemen:
  - Integrity-Checker einsetzen ($\rightarrow$ Host Intrusion Detection Systeme)
  - Zugriffsrechte sehr restriktiv vergeben (Need-to-know-Prinzip)
  - Bei Verwundbarkeiten ohne andere Lösung: Impfen, d.h. in die Programme wird bewusst die Signatur des Virus eingetragen

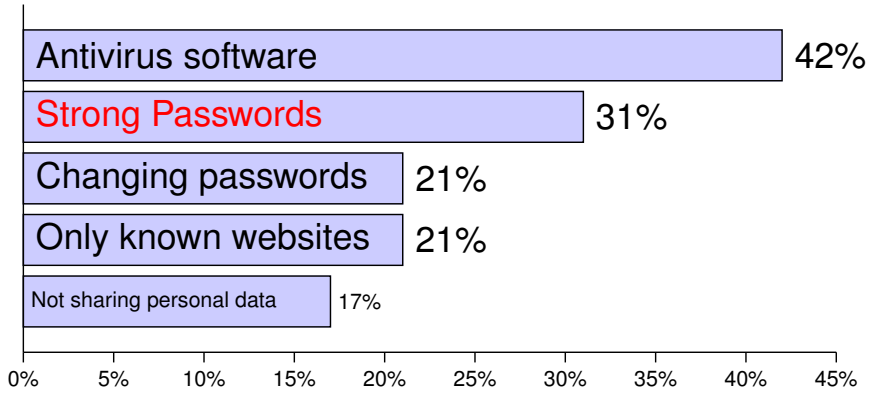
Top 3 Schutzmaßnahmen gegen Online Angriffen

Google hat 231 Sicherheitsexperten und 294 Internetlaien nach ihren Top 3 IT-Sicherheitspraktiken gefragt.

Quelle: `https://www.usenix.org/system/files/conference/soups2015/soups15-paper-ion.pdf`



IT-Sicherheitsexperten



Internetlaien

False-Positives bei Virensignaturen (1/2)

26.10.2011 13:36

heise Security « Vorige | Nächste »

Avira verdächtigt sich selbst

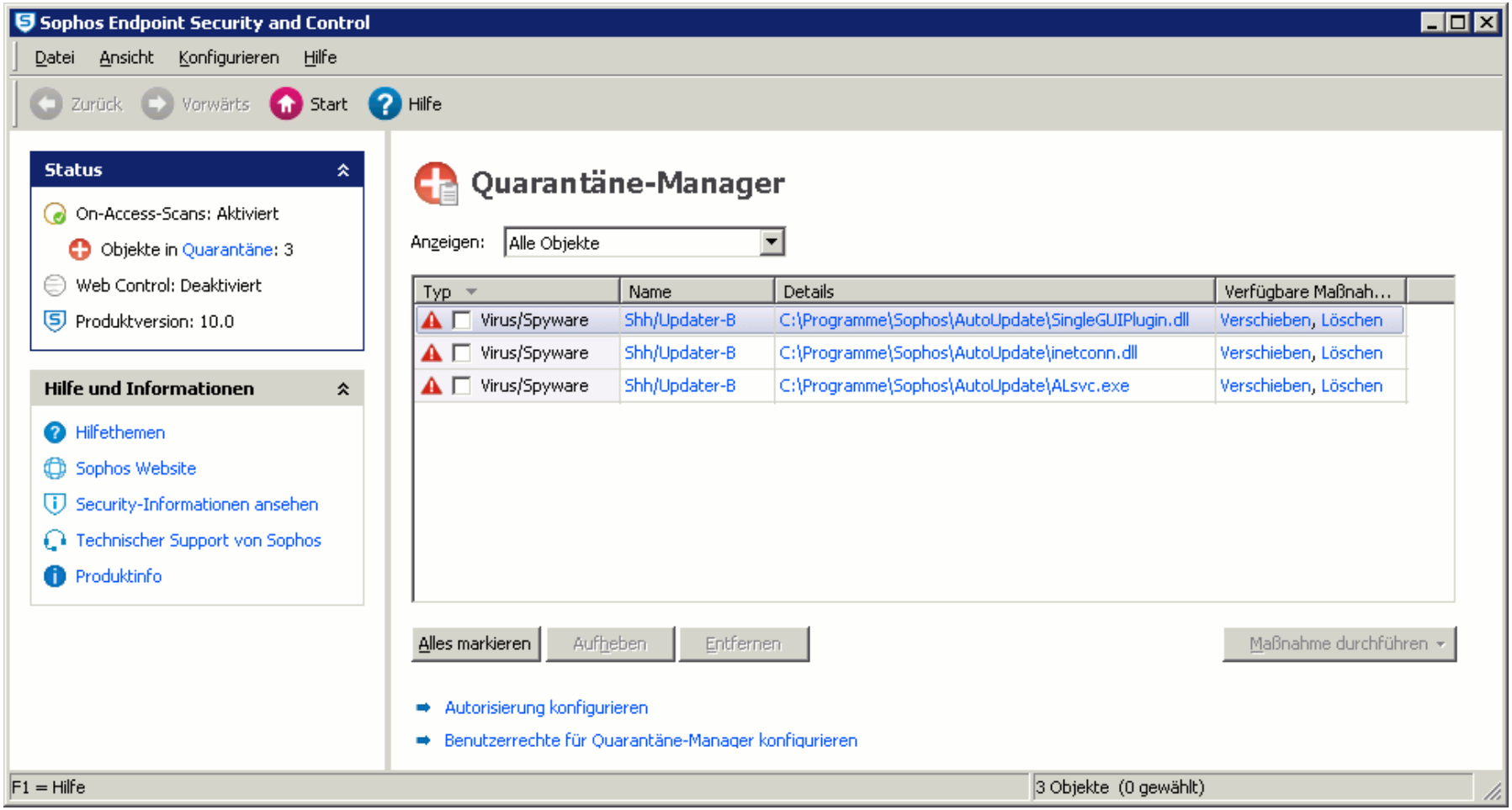
vorlesen / MP3-Download

Ein reguläres Update der Antiviren-Software von Avira lieferte eine Signatur, die auf eine der eigenen Dateien ansprang. Die Bibliothek AESCRIPT.DLL wurde dann plötzlich als "TR/Spy.463227" erkannt und gemeldet.

Ein Avira-Mitarbeiter bestätigte in den Support-Foren das Problem und erklärte, dass deshalb die Auslieferung des Updates bereits gestoppt wurde. Eine weitere Aktualisierung soll das Problem auch wieder beheben. (ju)

Quelle: `http://www.heise.de/-1367031`

False-Positives bei Virensignaturen (2/2)



Quelle: `https://tinyurl.com/owhe2dj`

20.09.2012: Sophos verschiebt sich selbst in Quarantäne, lässt keine Updates mehr zu.

Manipulierte Virensignaturen

Zwei Haupt-Angriffsvektoren

1. Angreifer bringen bekannte Viren-Signaturen in harmlosen Dateien unter und lassen diese über Online-Virenscanner testen
   $\Longrightarrow$ Im Worst Case werden z.B. die entsprechenden Files auf eine Blacklist gesetzt und von den Anwendersystemen gelöscht.
2. Antivirus-Softwarehersteller erstellt Fake-Signaturen, die von der Konkurrenz ungetestet übernommen werden.

Schwere Vorwürfe gegen Firmenchef Eugene Kaspersky

heise online 15.08.2015 14:38 Uhr – Dorothee Wiegand vorlesen

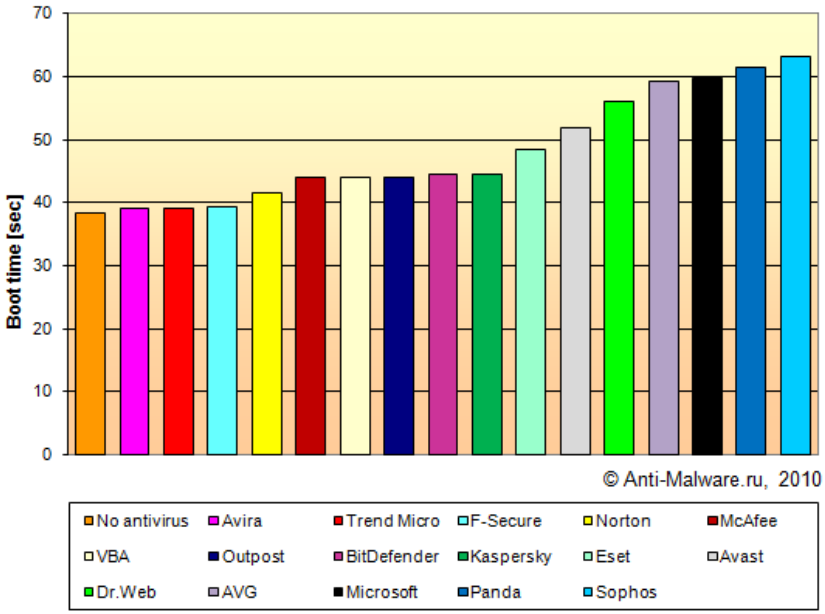
Zwei Ex-Mitarbeiter des Antiviren-Herstellers Kaspersky beschuldigen ihren ehemaligen Chef, er habe sie damit beauftragt, Konkurrenzprodukte zu sabotieren.

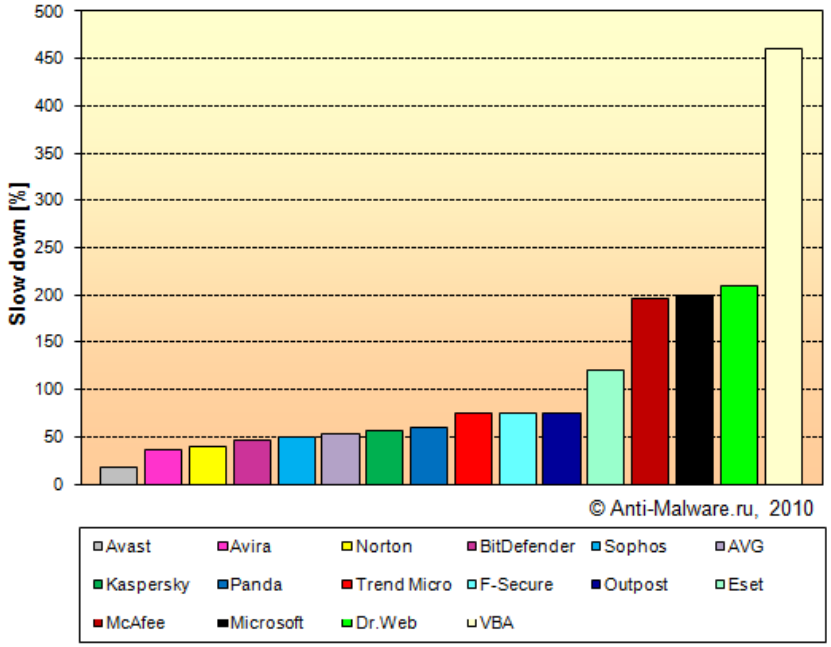
Zwei ehemalige Mitarbeiter des Antiviren-Herstellers Kaspersky beschuldigen den Firmenchef persönlich. In einem Bericht der amerikanischen Nachrichtenagentur Reuters werden die beiden namentlich nicht genannten Personen zitiert. Demnach habe Kaspersky einige Mitarbeiter damit beauftragt, Konkurrenzprodukte zu sabotieren. Konkret hätten sie den Auftrag bekommen, indirekt Produkte anderer AV-Hersteller so zu manipulieren, dass sie bei harmlosen Dateien Probleme melden, also Fehlalarme hervorrufen – die sogenannten False-Positive-Fälle. Aktionen dieser Art soll es über 10 Jahre gegeben haben.

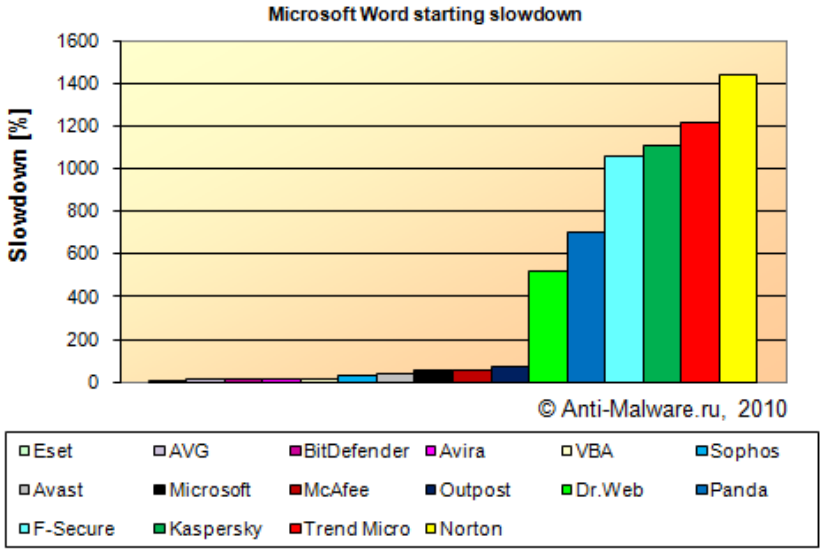
Die beiden Ex-Kaspersky-Mitarbeiter sagten gegenüber der Nachrichtenagentur, dass sie einem kleinen Kreis von Kollegen angehört hätten, der immer wieder solche Sabotage-Aufträge erhielt; die restlichen Mitarbeiter seien nicht eingeweiht gewesen. Ihr Chef habe die Manipulationen verlangt, da er verärgert über die Arbeitsweise der Konkurrenz gewesen sei. Statt eigene Verfahren zu entwickeln, würden die Mitbewerber nur Kaspersky-Produkte kopieren - so soll sich der Firmengründer geäußert haben. Mit den Manipulationen sollten laut Reuters-Bericht vor allem Microsoft, AVG and Avast geschädigt werden, aber auch weitere Antiviren-Hersteller.

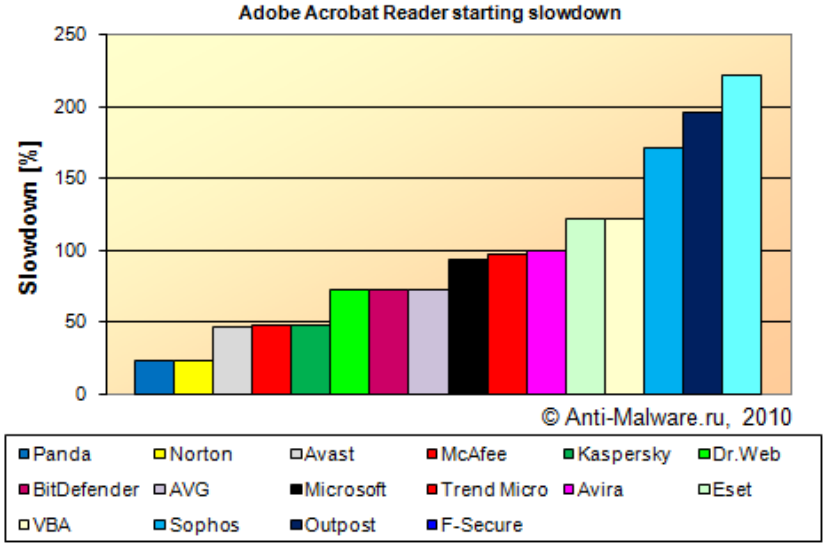
Quelle: `http://www.heise.de/-2779946`

Anti-Viren-Software: Performance Impact



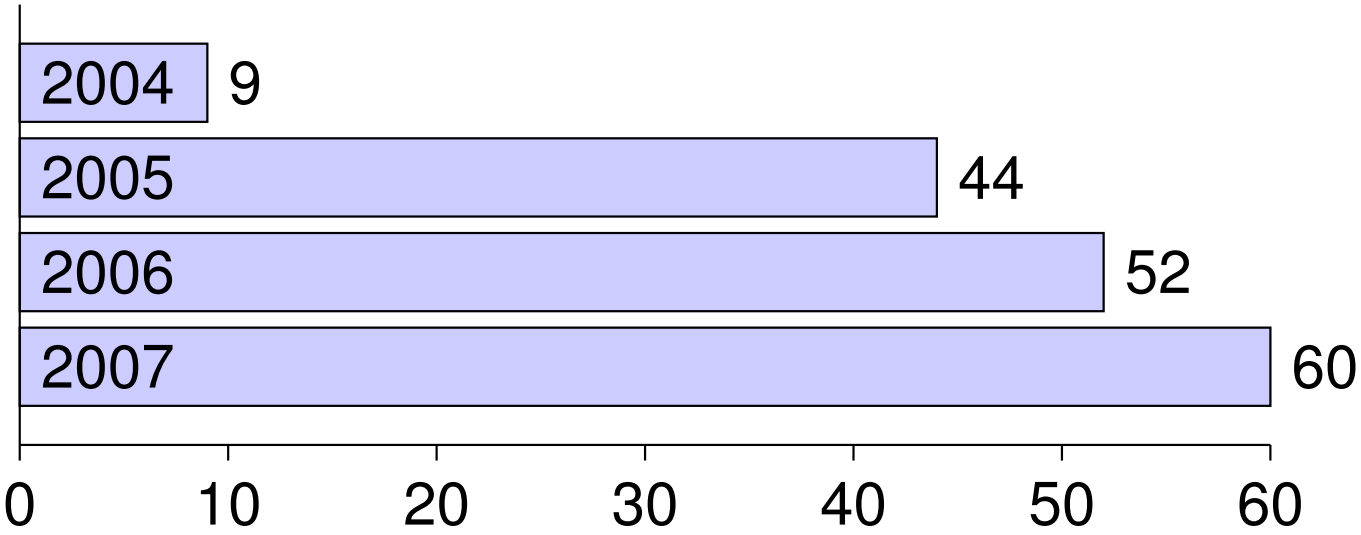






Auch AV-Software haben Sicherheitslücken (1/3)

Attacking The Antivirus, Blackhat 2008



Sicherheitslücken in AV-Software (National Vulnerability Database)

. . . , end users have been putting too much faith in antivirus solutions, and have ignored the fact that antivirus software itself can be compromised. People have scanned everything suspicious in the past. But now, it's better to think twice before doing so.

Quelle `https://tinyurl.com/nrfqwr3`

Auch AV-Software haben Sicherheitslücken (2/3)

Werden die Wächter selber angegriffen, haben sie dem oft wenig entgegenzusetzen. Und Fehler, die einen solchen Angriff ermöglichen, gibt es nach wie vor zu Hauf, bilanziert ein Sicherheitsforscher seine Analyse von 17 Antiviren-Programmen.

Antiviren-Software soll die Sicherheit erhöhen – trägt aber mitunter auch wesentlich dazu bei, dass ein System erst angreifbar wird, bilanziert Joxean Koret in seinem Vortrag Breaking Antivirus Software auf der Syscan-360-Konferenz.

Quelle: `http://heise.de/-2277782`

Auch AV-Software haben Sicherheitslücken (3/3)

Microsofts Antivirensoftware gefährdet Windows-Nutzer

- Microsoft hat eine Malware Protection Engine (MPE).
- Die AV-Software Defender benutzt MPE.
- Um Schadsoftware in Javascript-Code zu finden, simuliert die MPE dessen Ausführung ...
  - ... mit Systemprivilegien,
  - ... ohne Sandbox-Funktionalität
- Bug im MPE-Javascript Simulator ermöglicht das Ausführen von beliebigen Code mit Systemrechten
- MPE durchsucht auch E-Mails und deren Anhänge

  $\Longrightarrow$ Remote Code Excecution

`Quelle:https://tinyurl.com/ko4etqa(09.05.2017),`

Viren-Scanner für Android ist nutzlos (1/2)

Die beliebte Android-App Virus Shield schützt angeblich vor Malware und Datenklau. Ein Blick in den Quellcode verrät: In Wirklichkeit macht die App fast gar nichts. Das kostet dann vier Dollar.

Die angebliche Android-Virenscanner Virus Shield wurde tausendfach installiert und schaffte es sogar an die Spitze der Bezahl-Apps bei Google Play. Nach Untersuchung des Quellcodes stellte sich allerdings heraus, dass das Programm rein gar nichts macht. Und das für stolze 3,99 US-Dollar.

Quelle: `http://heise.de/-2166224`, 08.04.2014

Viren-Scanner für Android ist nutzlos (2/2)

Quelle: `http://www.androidpolice.com`, 06.04.2014

Antivirenschutz: AVG kann Nutzerdaten verkaufen

AVG kann Nutzerdaten, wie etwa den Browser- und Suchverlauf, an Dritte verkaufen. Das legt die überarbeitete Datenschutzerklärung nahe, die laut AVG am 15. Oktober in Kraft tritt.

Die gesammelten Daten sollen dem Anbieter zufolge anonymisiert sein und keine Rückschlüsse auf Nutzer zulassen. AVG könne aber schon länger Daten wie den Suchverlauf erfassen und verkaufen, nur haben sie das in älteren Versionen der Datenschutzerklärung nicht so eindeutig formuliert.

Quelle: `http://heise.de/-2822516`, 21.09.2015

Breaking Antivirus Software

Angriffsfläche

- Fakt: Die Installation von Software vergrößert die Angriffsfläche.
- Programme die als Admin laufen und Gerätetreiber sowie Paketfilter installieren erhöhen die Angriffsfläche dramatisch.

Mythos und Realität

- Propaganda: Wir machen deinen Rechner sicherer ohne spürbaren Leistungseinbußen. Wir schützen euch sogar vor unbekannten 0-Day Angriffen.
- Realität:
  - AV Software macht ihren Rechner verwundbarer, mit spürbaren Leistungseinbußen ist zu rechnen.
  - The AV-Software ist verwundbar gegenüber 0-Day Angriffen. Einige AV-Programme deaktivieren moderne Schutzmaßnahmen wie Data Execution Prevention (DEP) und Address Space Layout Randomization (ASLR).

Antivirus is dead, says maker of Norton Antivirus

. . . he estimates traditional antivirus detects a mere 45 percent of all attacks. That's not good.

Making matters more difficult . . . security provider FireEye says that 82 percent of all malware it detects stays active for a mere hour, and 70 percent of all threats only surface once, as malware authors rapidly change their software to skirt detection from traditional antivirus solutions. The function signature-based AV serves has become more akin to ghost hunting than threat detection and prevention,the firm says.

Quelle: `https://tinyurl.com/mbyuw2x`, May 5, 2014

Die 8 Goldene Regeln des Herrn Forler, 2004

1. *OE ist böse.*
2. *IE ist böse.*
3. *Active Scripting ist böse.*
4. *Keine Updates einspielen ist böse.*
5. *Sich als Administrator anmelden ist böse.*
6. *Auf alles klicken was sich bewegt ist böse.*
7. *Software aus nicht vertrauenswürdigen Quellen ist böse.*
8. *Dienste die sich an ein externes Interface binden sind böse.*

Diese Regeln bringen mehr als die trügerische Sicherheit eines Virenscanner/PFW.

Quelle: `http://de.comp.security.misc.narkive.com/DbKPebfb/on-acces-scanner`

8.5: E-Mail-Security (Hoaxes, Spam und Phising)

Hoax

Falschmeldungen die per E-Mail verbreitet werden um Nutzer zu erschrecken.

Spam, Junk

Unerwünschte Werbemails werden oft als SPAM oder Junk-Mails. Der Begriff SPAM stammt von einem Monty Python Sketch. `https://www.youtube.com/watch?v=anwy2MPT5RE`

Phising

Phising E-Mail fordert den Empfänger auf vertrauliche Benutzerinformationen wie Zugangsdaten (Benutzername und Passwort) oder Kreditkarteninformation zu verraten.

Hoax: GEZ-Gebührenerstattung, 1998

GEZ-Gebührenerstattung

Die öffentlich-rechtlichen Rundfunkanstalten ARD und ZDF haben im Frühjahr einen Gewinn von über 1 Mrd. DM erwirtschaftet. Dieses ist gemäß Bundesverfassungsgericht unzuläßig. Das OLG Augsburg hat am 10.01.1998 entschieden, daß an diesem Gewinn der Gebührenzahler zu beteiligen ist. Es müssen nach Urteil jedem Antragsteller rückwirkend für die Jahre 1997, 1998 und 1999 je Quartal ein Betrag von DM 9,59 (insgesamt 115,08 DM) erstattet werden.

ACHTUNG! Dieses Urteil wurde vom BGH am 08.04.98 bestätigt.[....] Bitte möglichst viele Kopien an Verwandte, Freunde und Bekannte weiterleiten, damit die Gebühren auch ihnen erstattet werden.

Hoax: Angeblich geplante Terroranschläge, 2002

Geplanter Terroranschlag auf Weihnachtsmärkten
Mein Kollege hat grad was erzählt, was uns zu denken geben sollte. Seine Tochter hat vor einigen Tagen in Hannover in einem großen Kaufhaus (Horten glaub ich) eine Brieftasche gefunden. Sie hat sie oben abgegeben, Adresse stand drin, türkisch klingender Name, der Mann wurde ausgerufen, kam dann auch und fragte dann die Tochter meines Kollegen, was er ihr denn als Finderlohn geben könnte. Sie sagte darauf hin, gar nichts, das wäre doch selbstverständlich und so.... daraufhin beugte er sich zu ihr vor und flüsterte ihr zu MMeiden Sie Weihnachtsmärkte!SSie noch am selben Tag zur Polizei und das erzählt, und die meinten dann nur, sie wüßten davon, daß Anschläge geplant sind, aber sie können es ja nicht erzählen, sonst gäbe es Panik... na toll!!! Oh gott, und ich wollte dieses Jahr so einige Weihnachtsmärkte abklappern :-(

Also, bitte bitte erzählt es allen weiter und meidet Weihnachtsmärkte!! Das ist kein Scherz oder Fake

Hoax, mögliche Erkennungszeichen

- Warnung vor „extrem gefährlichem Virus“
- “Keine AV-Software kann diesen Virus erkennen”
- “Warnen Sie alle Bekannten und Freunde”
- Nicht plausible Bedrohung
  (z.B. physische Zerstörung des Rechners)
- Verweis auf namhafte Unternehmen oder Institute/Unis
- Kettenbriefe im klassischen Sinn:
  - Gewinnspiele oder Glücksbriefe
  - „Geld zurück“
  - E-Petitionen
  - Pyramidensysteme
  - „Tränendrüsenbriefe“
- Schutzmaßnahmen: Hoax-Mail löschen und NICHT verbreiten
- `http://hoax-info.tubit.tu-berlin.de/list.shtml`

SPAM, Unsolicited Bulk Email (UBE)

E-Mail-Spam-Aufkommen am Beispiel Leibniz Rechenzentrum (LRZ), ein Tag im Oktober 2008.

- Zustellversuche für 14.556.000 Mails
- Spam und Viren-Mails: 14.436.000 ($\approx 99,18\%$)
- Abgelehnte Mails: 14.400.000 ($\approx 99\%$)
- Als Spam markiert: 35.000 ($\approx 0,24\%$)
- Viren-Mails: 1.000 ($\approx 0,01\%$)
- Gewünschte Mails („Ham“): 120.000 ($\approx 0,82\%$)

Probleme

- Eingangs-Mailbox wird mit Spam überflutet.
- Zusätzlicher Aufwand (Speicherplatz, Arbeitszeit).
- Zusätzliche Kosten (Infrastruktur, Übertragung, Personal,....).
- Extrem störend, oft „gefährlicher“ Inhalt.

Zielgruppenorientierter Spam: Beispiel

Subject: UNIVERSITY DIPLOMAS
Date: Tue, 08 Aug 1996 18:47:06 -0400 (EDT)

Obtain a prosperous future and secure the admiration of all for as little as $125.

Diplomas from prestigious non-accredited universities based on your life experience.

No tests, no classes, no interviews. All diplomas available including bachelors, masters, and doctorates (PhD's).

No one is turned down. Your diploma puts a University Job Placement Counselor at your disposal.

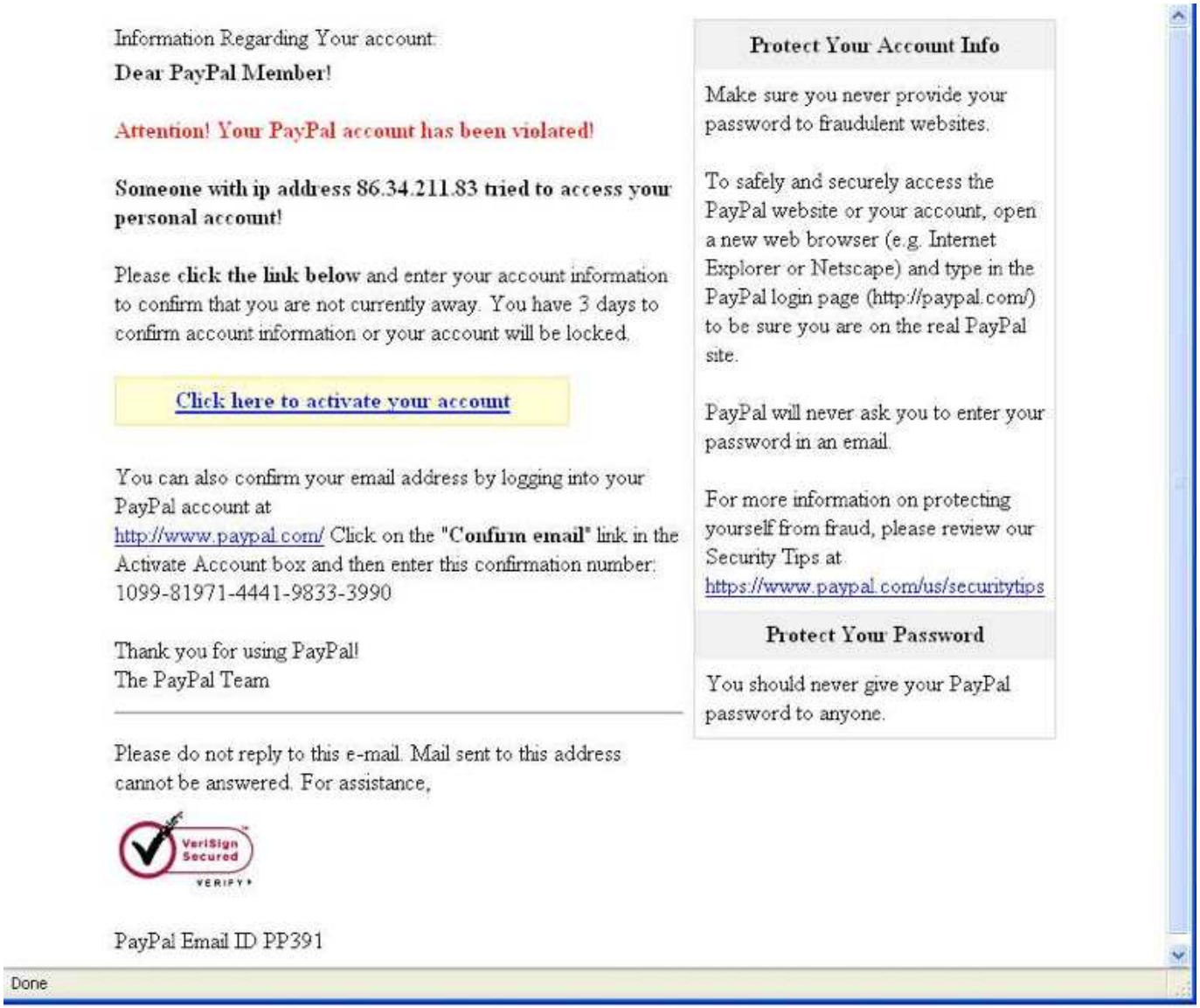
Confidentiality assured.

CALL NOW to receive your diploma within days!!!

1-603-623-0033, Extension 307

Open Every Day Including Sundays and Holidays.

Beispiel: PayPal-Phishing, 2013



Information Regarding Your account:

Dear PayPal Member!

Attention! Your PayPal account has been violated!

Someone with ip address 86.34.211.83 tried to access your personal account!

Please **click the link below** and enter your account information to confirm that you are not currently away. You have 3 days to confirm account information or your account will be locked.

Click here to activate your account

You can also confirm your email address by logging into your PayPal account at http://www.paypal.com/ Click on the "**Confirm email**" link in the Activate Account box and then enter this confirmation number: 1099-81971-4441-9833-3990

Thank you for using PayPal!
The PayPal Team

Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance,

VeriSign Secured VERIFY

PayPal Email ID PP391

Protect Your Account Info

Make sure you never provide your password to fraudulent websites.

To safely and securely access the PayPal website or your account, open a new web browser (e.g. Internet Explorer or Netscape) and type in the PayPal login page (http://paypal.com/) to be sure you are on the real PayPal site.

PayPal will never ask you to enter your password in an email.

For more information on protecting yourself from fraud, please review our Security Tips at https://www.paypal.com/us/securitytips

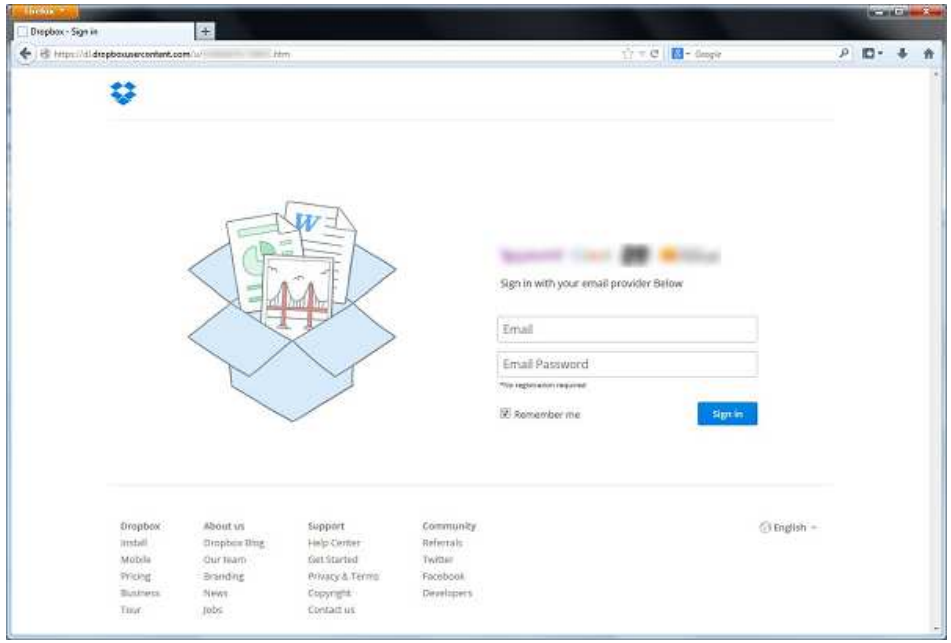
Protect Your Password

You should never give your PayPal password to anyone.

Done

Beispiel: Dropbox-Phishing, 2014

- Phishing-Mail mit Dropbox als vermeintlichem Absender
- Angreifer betreibt Phishing-Website über offizielle Dropbox-Domain `dropboxusercontent.com`
- Zugriff auf Phishing-Website über HTTPS somit mit offiziellem Dropbox-Serverzertifikat



Quelle: Symantec

- Diverse Logos von E-Mail-Providern motivieren zur Eingabe weiterer Accounts und Passwörter.
- Ähnlicher Angriff im März 2014 über Google Docs.

Beispiel: Porno-Abmahn-Mails fordern Bitcoins, 2014

Eine aktuelle Welle von gefälschten Abmahnschreiben fordert Schadenersatz in Bitcoins für vermeintliches Streaming eines Pornovideos. Verbraucherschützer warnen davor, die Mails zu beantworten und auf die darin enthaltenen Links zu klicken.

Die Verbraucherzentrale Rheinland-Pfalz warnt vor einer aktuellen Welle gefälschter Abmahnschreiben, die Schadenersatz in Bitcoins für Urheberrechtsverletzungen fordern. Ëmpfänger solcher E-Mails sollten diese nicht beantworten und auf keinen Fall die angegebenen Links öffnen", raten die Verbraucherschützer.

Quelle `http://heise.de/-2437348`, 28.10.2014.

Spam, klassische Gegenmaßnahmen: Spamfilter

- Software, die eingehende Mails nach Spam durchsucht
- Es gibt drei Arten von Spam-Filtern
  1. Blacklist / Whitelist Ansatz
     Aussperren von Mail-Servern und Mail-Domänen, die üblicherweise von Spammer benutzt werden.
  2. Regelbasiert
     Nachricht wird inhaltlich nach Spam-Merkmalen durchsucht; sowohl im Header als auch im Body der Mail.
  3. Filtersoftware lernt aus Beispielen: Neuronale Netze oder Bayes-Filter bewerten Mailinhalte.
- Vor- u. Nachteile dieser Spam-Filter
  1. Effizient zu implementieren;
     aber grobgranular, keine inhaltliche Prüfung.
  2. Sehr hohe Erkennungsraten; aber E-Mail muss vollständig entgegen genommen werden, kontinuierlicher Aufwand für Konfigurationspflege.
  3. Gut in Mail-Clients zu integrieren; aber Erkennungsrate abhängig von Training (NN) bzw. Modellierung (Bayes).

Spamfilter

- Fehlerarten bei der Erkennung
  - **Falsch positiv**: Mail wird als Spam erkannt, obwohl sie Ham ist
  - **Falsch negativ**: Mail wird als Ham bewertet, obwohl sie Spam ist
- Welche Fehlerart ist problematischer?
- Policy für Spambehandlung
  - Spam-Mail löschen und Empfänger ggf. benachrichtigen
  - Spam-Mail markieren und dann ausliefern
  - Welche Variante bevorzugen (unter Beachtung der Fehlerarten)?
  - Vgl. auch Urteil Landgericht Bonn, 15 O 189/13
  - SpamAssassin (`http://spamassassin.apache.org/`)
    - Implementiert alle Filterarten (Blacklist, Regelbasis, Bayes-Filter)
    - Zentral und dezentral einsetzbar, fein-granular konfigurierbar
  - Spamfilter als Cloud-Dienst: Mail-Gateway mit Spamfilter bei externem Dienstleister - kein eigener Konfigurationsaufwand, aber “Mitleser”...

Greylisting

- Eingehender Mailserver *Y* überprüft das Tripel (`<E-Mail-Adresse des Absenders>, < Ausgehender Mailserver>, < E-Mail-Adresse des Empfängers >`)
- Falls bereits bekannt, akzeptiert *Y* die Mail
- Falls unbekannt, schickt *Y* typischerweise den Fehlercode 451.
- Typische Fehlermeldung: `451 4.7.1 Greylisting in action, come back in 25 minutes .`
- Nach der Wartezeit wird die E-Mail beim erneuten Versuch akzeptiert.
- Greylisting funktioniert überraschend gut. Warum?

Epilog: Best of Top 20 Internet Security Problems

SANS System Administration, Audit, Networking and Security)/FBI Annual Top 20 Internet Security Vulnerability List (bis 2007)

- Client-seitig
  1: Schwachstellen in Web-Browsern
  2: Schwachstellen in Office-Programmen
  3: E-Mail (Phishing, Spam, DoS, Malware)
  4: Media Players (u.a. Flash Player, Quicktime, ...)
- Server-seitig
  1: Webanwendungen (u.a. XSS, SQL Injection, ...)
  4: Angriffe über Backup-Software
  (lokale Berechtigungen; zentrale Ablage)
  5: Programmierfehler in Anti-Virus-Software
  (code execution vulnerabilities)
  6: Unzureichend gesicherte Management-Server
  (u.a. Monitoring, Softwareverteilung, ...)

Epilog: Die Lage der IT-Sicherheit 2015

Berlin (Reuters) - Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat schwere Vorwürfe gegen die großen Software-Hersteller erhoben.

"Die Anzahl kritischer Schwachstellen in Standard-IT-Produkten hat sich gegenüber den bereits hohen Werten in den Vorjahren im Jahr 2015 noch einmal massiv erhöht", heißt es in dem am Donnerstag veröffentlichten Jahresbericht zu IT-Sicherheit in Deutschland.

Besonders schlecht schneiden in der BSI-Aufstellung für kritische Schwachstellen die Produkte Adobe Flash, Microsoft Internet Explorer, Apple Mac OS X und Microsoft Windows ab. Bei ihnen wurde bis September 2015 jeweils weiter mehr als 100 kritische Schwachstellen registriert.

Quelle: `http://de.reuters.com/article/companiesNews/idDEKCN0T80RS20151119`, 19.11.2015

Zusammenfassung

Sie sollten . . .

- . . . wissen wie ein Virus funktioniert.
- . . . wissen wie ein Wurm funktioniert.
- . . . wissen was ein trojanisches Pferd ist.
- . . . wissen was ein Hoax ist.
- . . . wissen was SPAM ist.
- . . . wissen wie man sich gegen Malware schützt.