Verunsichert

Schädlingsbekämpfung
auf dem Windows-PC

Humboldt-Universität zu Berlin
Computer- und Medienservice

einige „High-lights“ in 2006

- Stration-Wurm (lädt ständig veränderte Kopien von sich herunter)
- Microsoft: 133 kritische und wichtige Sicherheitslücken behoben (2005 ca. 60)
- MPEG-Dateien ans Malware-Träger
- 73 Malware-Angriffe auf Smartphones
- Professionalisierung der Szene und Einstieg organisierter und krimineller Banden
- Versteigerung von Sicherheitslücken

Computer-Viren

Viren sind destruktive Programme, die andere Programme verändern („infizieren“) können, wobei es eine (möglicherweise mutierte) Kopie von sich selbst einfügt, sich somit von einem Speichermedium zu einem anderen kopieren können und Schäden an Daten, Programmen, Rechnerkonfigurationen und Arbeitsabläufen verursachen können.

Struktur eines Virus

- Infektion: Zum Infektionsmechanismus zählen die Art oder Arten, auf denen sich ein Virus verbreitet
- Payload: Der Payload-Mechanismus ist das, was der Virus zusätzlich zur Replikation tut (falls er etwas Zusätzliches tut)
- Trigger: Der Trigger-Mechanismus (Auslöser) ist die Routine, die bestimmt, ob es der richtige Zeitpunkt ist, den Payload auszuführen (falls dieser existiert)

Würmer (1)

Würmer sind keine Viren im eigentlichen Sinne, da sie keine Wirtsprogramme benötigen, sondern ausschließlich sich selbst kopieren. Im Gegensatz zu Viren und Trojanischen Pferden infizieren sie keinen fremden Code, um sich fortzupflanzen.

Trojanische Pferde

Trojanische Pferde (Trojaner) sind auch keine Viren im eigentlichen Sinne (da sie sich i. d. R. nicht selbst reproduzieren), sondern Programme mit Virenfunktionalität, die sich hinter dem Namen von bekannter (harmloser) Software verstecken. Der Begriff Trojaner wird gelegentlich synonym für Spionage-Software verwendet. Besondere Kennzeichen sind, dass sie oftmals lange Zeit unentdeckt bleiben und von „innen nach außen“ wirken.

Beispiele für Trojaner

Korgo (2004):

Korgo ist gleichzeitig ein Wurm (Verbreitung) und ein Trojaner (Aufzeichnung von Tastatureingaben und Weiterleitung über Internet).

TROJ_PGPCODER (2005):

Verschlüsselung von .DOC, .XLS u.a. Dateien, Schlüssel für Entschlüsselung gegen 200 $

Hoax (1)

W I C H T I G
== == == ==
Wir sind informiert worden, dass unser Computer von dem Virus
jdbgmgr.exe
infiziert worden ist, der sich per e-mail automatisch ausbreitet, da er sich im e-mail Adressbuch versteckt. Er kann nicht mit Norton oder McAfee Antivirus entdeckt werden, und bleibt 14 Tage inaktiv, bevor er das komplette Computer-System beschädigt.
Er kann aber gelöscht werden, bevor er Ihre Daten beschädigt.
Bitte gehen Sie wie folgt vor:
KLICKEN SIE AUF " START "
KLICKEN SIE AUF " SUCHEN " UND SUCHEN SIE DIE DATEI:
JDBGMGR.EXE
VERGEWISSERN SIE SICH, DASS IN C:\ GESUCHT WIRD
KLICKEN SIE AUF " SUCHEN "
WENN IHR PC DEN VIRUS GEFUNDEN HAT (ES HAT EIN KLEINES
BÄREN-SYMBOL)
BITTE NICHT ÖFFNEN !!!!!!!!!!!!
KLICKEN SIE MIT DER RECHTE MOUSE-TASTE AUF DAS KLEINE
BÄREN-SYMBOL UND
WÄHLEN SIE " LÖSCHEN " (DER VIRUS WIRD IN DEN ORDNER "
PAPIERKORB " VERSCHOBEN)
KLICKEN SIE MIT DER RECHTEN MOUSE-TASTE AUF DEN PAPIERKORB UND WÄHLEN SIE
" PAPIERKORB LEEREN ".
WENN SIE DEN VIRUS AUF IHREM COMPUTER GEFUNDEN HABEN, SCHICKEN SIE DIESE MITTEILUNG SCHNELLSTMÖGLICH AN ALLE ADRESSEN IN IHREM E-MAIL ADRESSBUCH.

MFG

Hoax (2)

>>>Dieser Bericht enthält eine Bitte: Könnt ihr so gut sein, diese Mail weiterzuleiten? Dadurch könnt ihr einem kleinen Jungen (Brian) aus Buenos Aires helfen. Brian hat mit einer schweren Erkrankung an seinem Herzmuskel zu kämpfen und wartet dringend auf eine Transplantation. Doch es gibt ein "Aber": Diese Operation kostet 115.200 US Dollar. Der ISP (Internet Service Provider) bezahlt 0,01 Dollar für jede Mail, die für diesen Zweck versendet wird und mit dem Titel: "Solidarida con Brian" über den Server gehen. Es ist wichtig, schnell zu handeln! Neben Brians Krankenbett steht ein Notebook mit Modem um zu zählen. Es sind 11,5 Mill. Mails nötig, um die Operation finanzieren zu können. Könnt ihr, wenn möglich, an jeden den ihr kennt, eine Kopie von dieser Mail senden? Das kostet max. 2 Minuten eurer sicherlich kostbaren Zeit, während es für Brian lebenswichtig ist. Zerstöre die Kette bitte nicht und vergesse vor allem nicht den Titel "Solidarida con Brian", der unter Subjekt/Betreff stehen muss, denn das ist die Kontrollmöglichkeit des Servers. Vielen Dank im Namen von ida van Kampen-Damsma und Betty Meyboo de Jong, Hochschullehrerinnen für Allgemeinmedizin an der Rjks Universität in Groningen. Tipp: Kopiere diesen Bericht und forwarde ihn an dein ganzes Adressbuch. … Danke!!! Solidarida con Brian <<<

Spyware (1)

- Spyware sind Programme, die persönliche Daten von Computer-Nutzern ohne deren Wissen versenden.
- Die am häufigsten vorkommende Spyware sind Adware-Cookies bzw. Adware-Programme. Diese stellt nach dem Start einer Applikation Anzeigenwerbung dar und übermittelt dabei unerlaubt Daten an Dritte.

Spyware (2)

- Spyware hat vordergründig keine zerstörerische Funktion, kann in vielen Fällen aber zu Problemen (Systemabstürzen, Ressourcenverbrauch) führen.
- Spyware kann auch aktiv werden und das Verhalten des Anwenders beeinflussen:
  - Suchen auf vorgegebene Seiten umlenken
  - Funktionen des Browsers verändern
  - Bannerwerbung und Pop-Ups in andern Programmen

Phishing

- Phishing ist Trickbetrug per E-Mail.
- Es wird versucht, über fingierte E-Mails auf gefälschte Bank- oder eBay nachempfundene Webseiten zu locken, um dort die Zugangsdaten abzunehmen.

AV-Software - Kostenlos für Privat

(kostenlos für den Privatgebrauch)

- AntiVir Personal Edition http://www.free-av.de
- F-Prot für DOS http://www.f-prot.com
- Bitdefender Free Edition http://www.bitdefender.de
- Weitere Informationen über kostenfreie Scanner: http://www.heise.de/security/dienste/antivirus/links.shtml

AV-Software - Kostenlos und online

- VirusTotal
  http://www.virustotal.com/
- Jotti
  http://virusscan.jotti.org/de/
- Ikarus
  http://www.ikarus-software.at/portal/modules.php?name=Content&pa=showpage&pid=4
- Weitere Informationen über kostenfreie Online-Scanner:
  http://www.heise.de/security/dienste/antivirus/links.shtml

Anti-Spyware-Software

- Ad-Aware SE Personal
  http://www.lavasoft.com
  für den Privatgebrauch kostenfrei
- Spybot Search&Destroy
  http://www.spybot.info/de/download
  für den Privatgebrauch kostenfrei, mit Aufforderung zur Spende

Weitere Empfehlungen (1)

Firewall nutzen und testen

- Windows XP SP2:
  Systemsteuerung - Sicherheitscenter
- für ältere Windows-Versionen:
  http://www.kerio.com
  http://www.zonelabs.com
  (nicht parallel zur Windows-Firewall!)
- Test der Firewall
  http://www.heise.de/security/dienste/portscan/auswerten/faq.shtml

Weitere Empfehlungen (2)

Überprüfungen:

- Passwort-Check
  https://passwortcheck.datenschutz.ch/check.php?lang=de
- Demonstration von Browser-Sicherheitslücken:
  http://www.heise.de/security/dienste/browsercheck/
- Browserinformationen, Traceroute u.a.
  http://www.it-sec.de/vulchk.html
- Browser-Check
  http://www.pc-magazin.de/aktionen/browser/check.php

Weitere Empfehlungen (3)

Windows aktualisieren

- passende Service-Packs installieren (online): http://www.windowsupdate.com
- automatisches Suchen nach Windows-Updates Systemsteuerung - Leistung und Wartung - System - Automatische Updates
- passende Service-Packs downloaden: http://v4.windowsupdate.microsoft.com/catalog

Weitere Empfehlungen (4)

E-Mail-Sicherheit

- Keine HTML-Mails zulassen
- E-Mail in sicheren Zonen lesen
- kein automatisches Speichen und Öffnen von Attachments
- kein automatisches Hinzufügen zum Adressbuch

Weitere Empfehlungen (5)

Sicherheitseinstellungen in Windows

- Rechte vergeben (NTFS verwenden)
- Verschlüsselung von Dateien
- „Run as“ – sichere Accounts verwenden
- sichere Verbindungen (SSL)
- sichere Passwörter

Weitere Empfehlungen (6)

Schutz vor Spyware:

- Windows-Update, Sicherheitseinstellungen
- Misstrauen beim Surfen
- Mistrauen in Tauschbörsen
- Informationen über zu installierende Software
- regelmäßige Überprüfung des PCs mit entsprechender Sicherheitssoftware

Weitere Empfehlungen (7)

Schutz vor Phishing:

- Banken und andere Unternehmen verschicken i.d.R. keine Mails mit der Aufforderung, persönliche Kontodaten preiszugeben
- Keinen Links in Mails folgen, sondern die sichtbare Adresse im Browser eintippen
- Versicherung, dass eine SSL-Verschlüsselung verwendet wird
- Quelltext einer solchen Mail nach den tatsächlichen Links überprüfen

Weitere Empfehlungen (8)

MS Baseline Security Analyzer

- kostenloses Tool von Microsoft zum Test auf Sicherheitslücken
  http://www.microsoft.com/technet/security/tools/mbsahome.mspx

Weiterführende Informationen

http://agn-www.informatik.uni-hamburg.de/vtc/

http://www.heise.de/security/dienste/antivirus/

http://www.buerger-cert.de

http://www.bsi.de/

http://www.tu-berlin.de/www/software/hoax.shtml

http://www.mcafee.com/de/

stange@cms.hu-berlin.de