Varianzanalyse

Cooler Untertitel, den wir uns noch ausdenken

Henri Neumann & Robert Feldhans

15. Dezember 2016

Experimentelle Psychologie für Nichtpsychologen

Inhalt

1. Henri
2. Robert
3. Historische Einordnung
4. Malware und ihre Hauptverteilwege
5. Antiviren-Programme
6. Wirksame Maßnahmen gegen Viren

Henri

Robert

Historische Einordnung

Beginn des Schlangenöls

- aus Mythologie des Wilden Westens
- von Wunderheilern eingesetzt
- Heilmittel für Gebrechen aller Art

Schlangenöl allgemein

- versprochenes Wundermittel
- unübersichtliche Bereiche, oft in Technik
- wenig Wirkung
- Heutige Anwendungen oft in Kryptografie und Antiviren-Software

Malware und ihre Hauptverteilwege

Malware

Malware

Software, welche schädliche Funktionen ausführen

- Viren
- Würmer
- Trojanische Pferde
- Ransomware
- ...
- nicht: fehlerhafte Software

Verschiedene Malware

Virus

Schadprogramm, welches sich verbreitet, in dem es sich in andere Software einschleust. Durch das Kopieren dieser wird der Virus passiv verbreitet (und dabei oft nur lokal)

Wurm

Schadprogramm, welches sich aktiv ausbreitet, in dem es Sicherheitsprobleme ausnutzt. Für Nutzer kaum unterschiedlich zu Viren

Trojanisches Pferd

Schadprogramm, welches sich als nützliche Anwendung tarnt und ohne Wisse des Anwenders (auch) schädliche Funktionen ausführt

Anzahl Malware

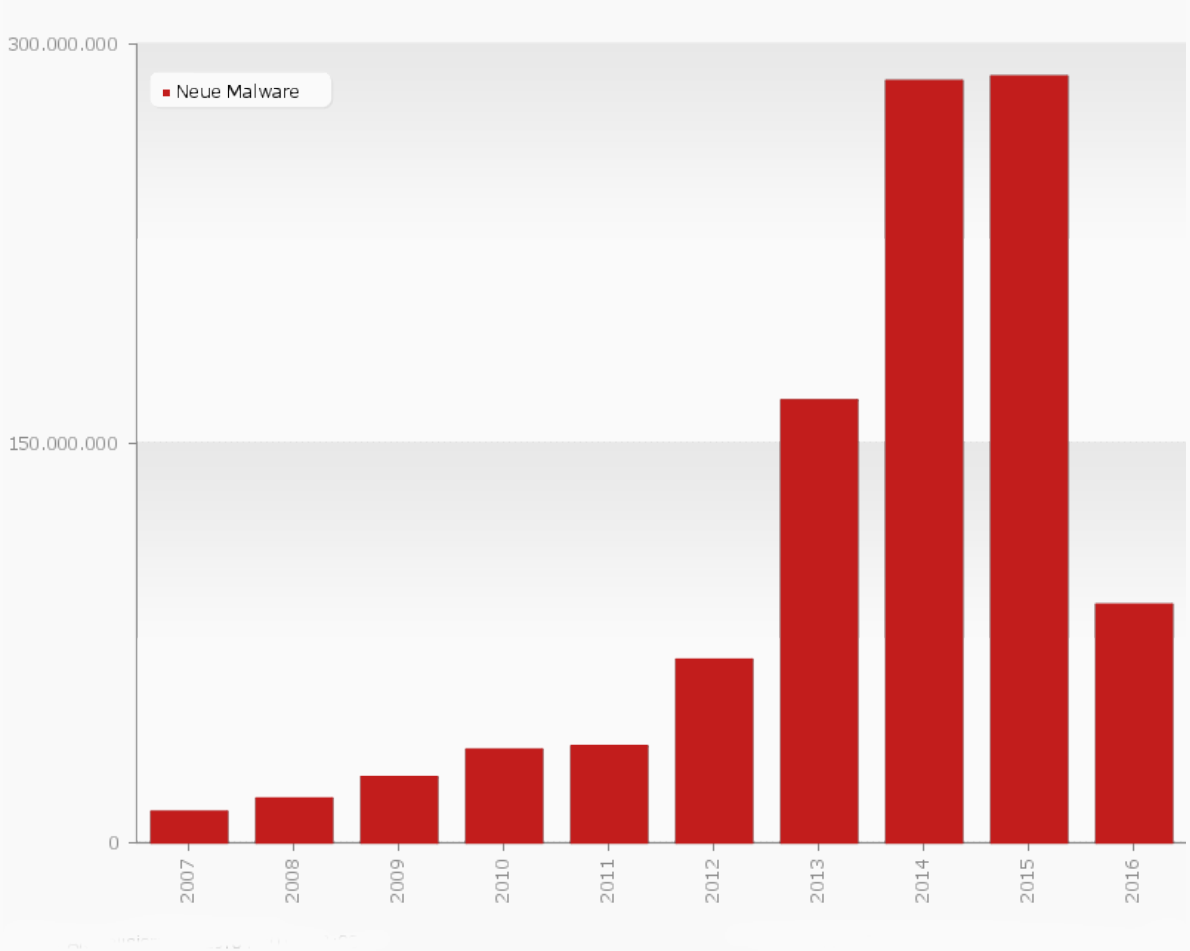

Abbildung 1: Registrierung neuer Schadprogramme in den letzten 10 Jahren. Quelle: avtest

Verteilwege von Malware

- E-Mail-Dateianhänge
- Drive-by-Downloads
- Datenträger
- Netzwerke

Statistiken

Problem

Viele Statistiken zu Malware und ihren Verteilwegen werden von Antiviren-Software-Firmen angeboten

- wenige unabhängige Quellen
- Quantität schwer einzuschätzen
- nur bekannte Probleme aufgelistet

Antiviren-Programme

Vermeintliche Lösung

Wie schützen wir uns vor Viren?

Wir installieren ein Antiviren-Programm!

Verbreitung von AV-Programmen

Zahlen zu AV-Installationen

- AVG Antivirus Free (32 & 64 bit) 22.3M
- avast Free Antivirus 19.4M
- Ad-Aware Free Antivirus 9.2M

jeweils in Millionen Downloads bei Chip (Windows)

Virtualisierung I

Virtualisierung

Idee: Wir tun nur so, als würden wir verdächtigen Code laufen lassen, überwachen tatsächlich seine Verhaltensweise

Firewalls I

Firewall

Idee: Ein- und ausgehende Kommunikation überwachen, um Kommunikation von Malware zu verhindern/ Malware zu finden

Problem

Sobald die Kommunikation verschlüsselt abläuft, wird die Überwachung beliebig kompliziert

AV-Browser I

Antiviren-Browser

Idee: Wir halten den Nutzer davon ab, schädliche Dateien herunterzuladen, indem wir einen Browser bereitstellen, der gefährliche Websites u.Ä. blockiert

Wirksame Maßnahmen gegen Viren

Zitat

„We cant write secure software. Why are people suprised that we also can not write secure security software?“

Fragen?

Quellen I

- blog.fefe.de
- sherpablog.marketingsherpa.com/wp-content/uploads/2016/02/Snake-Oil-Cures-All.jpeg
- itwissen.info/definition/lexikon/ (diverse Definitionen)
- de.wikipedia.org/wiki/Schadprogramm
- av-test.org/de/statistiken/malware/
- netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0
- bsi.bund.de/DE/Publikationen/Lageberichte/bsi-lageberichte.html
- Chip.de (diverse AV-Downloadseiten)
- bugs.chromium.org/p/project-zero/issues/detail?id=769
- de.urbandictionary.com/define.php?term=Startkeylogger

Quellen II

- bugs.chromium.org/p/project-zero/issues/detail?id=564&redir=1
- news.softpedia.com/news/avast-safezone-browser-lets-attackers-access-your-filesystem-499990.shtml
- imgur.com/Smwnzx3
- www.heise.de/security/meldung/Authentifikation-von-McAfees-Enterprise-Security-Manager-loechrig-3036068.html
- www.heise.de/security/meldung/Symantec-Endpoint-Protection-Gefaehrlicher-Sicherheitsluecken-Cocktail-2768461.html
- thehackernews.com/2015/07/bitdefender-hacked.html?m=1
- www.heise.de/mac-and-i/meldung/Apple-Anti-Viren-Apps-fuer-iOS-irrefuehrend-2581916.html
- www.heise.de/security/meldung/Antiviren-Software-und-Apples-Schutzmechanismen-fuer-Mac-OS-X-nutzlos-2620049.html