Einleitung
Motivation
Objekt der Untersuchungen
Technische Grundlagen
Messungen
Messwerkzeuge
Messung: KaZaA
Messung: Gnutella & OpenFT
Ergebnisse
Messergebnisse: KaZaA
Messergebnisse: Gnutella & OpenFT
Schaden, Maßnahmen
Literatur
Fazit

A Study of Malware in Peer-to-Peer Networks / Malware Prevalence in the KaZaA File-Sharing Network

Gregor Kopf

Seminar „Internet Measurement“,
Technische Universität Berlin

25. Juli 2007

Inhalt

Einleitung
Motivation
Objekt der Untersuchungen
Technische Grundlagen
Messungen
Messwerkzeuge
Messung: KaZaA
Messung: Gnutella & OpenFT
Ergebnisse
Messergebnisse: KaZaA
Messergebnisse: Gnutella & OpenFT
Schaden, Maßnahmen
Literatur
Fazit

1 Einleitung
- Motivation
- Objekt der Untersuchungen
- Technische Grundlagen

2 Messungen
- Messwerkzeuge
- Messung: KaZaA
- Messung: Gnutella & OpenFT

3 Ergebnisse und Interpretation
- Messergebnisse: KaZaA
- Messergebnisse: Gnutella & OpenFT

4 Schaden und Gegenmaßnahmen

5 Literatur

6 Fazit

Motivation

Einleitung
Motivation
Objekt der Untersuchungen
Technische Grundlagen
Messungen
Messwerkzeuge
Messung: KaZaA
Messung: Gnutella & OpenFT
Ergebnisse
Messergebnisse: KaZaA
Messergebnisse: Gnutella & OpenFT
Schaden, Maßnahmen
Literatur
Fazit

- Zunehmende Verbreitung von Malware
- Malware verursacht enormen Schaden:
  - Verteilte Angriffe auf Strukturen (z.B. DNS, Websites)
  - Versand von Spam
  - Diebstahl oder Manipulation von Daten
- Peer-to-Peer-Netze können Verbreitung begünstigen
  - Download von Dateien unbekannter Herkunft
  - Möglichkeit zum Tausch von Executables begünstigt Ausbreitung von Viren

Objekt der Untersuchungen

Einleitung
Motivation
Objekt der Untersuchungen
Technische Grundlagen
Messungen
Messwerkzeuge
Messung: KaZaA
Messung: Gnutella & OpenFT
Ergebnisse
Messergebnisse: KaZaA
Messergebnisse: Gnutella & OpenFT
Schaden, Maßnahmen
Literatur
Fazit

Untersuchte Netze

In [KAM 06]:

- KaZaA (Fasttrack)

In [SJB 06]:

- Gnutella
- OpenFT

Untersuchte Malware

Der Einfachheit halber: nur Viren

Objekt der Untersuchungen

Einleitung
Motivation
Objekt der Untersuchungen
Technische Grundlagen
Messungen
Messwerkzeuge
Messung: KaZaA
Messung: Gnutella & OpenFT
Ergebnisse
Messergebnisse: KaZaA
Messergebnisse: Gnutella & OpenFT
Schaden, Maßnahmen
Literatur
Fazit

Untersuchte Netze

In [KAM 06]:

- KaZaA (Fasttrack)

In [SJB 06]:

- Gnutella
- OpenFT

Untersuchte Malware

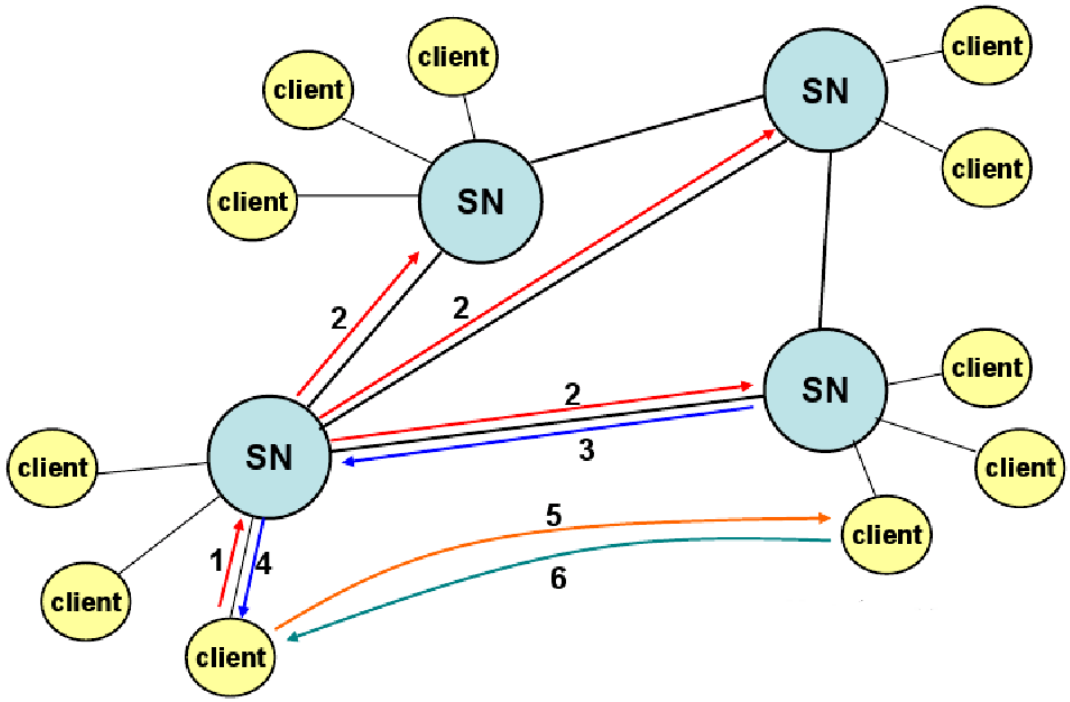
Der Einfachheit halber: nur Viren

Technische Grundlagen

Einleitung
Motivation
Objekt der Untersuchungen
Technische Grundlagen
Messungen
Messwerkzeuge
Messung: KaZaA
Messung: Gnutella & OpenFT
Ergebnisse
Messergebnisse: KaZaA
Messergebnisse: Gnutella & OpenFT
Schaden, Maßnahmen
Literatur
Fazit

- Suchmechanismus der Netze wird zum Auffinden von Malware verwendet
- Supernode-Architektur

Abbildung: Supernode-Architektur



Messwerkzeuge

Einleitung
Motivation
Objekt der Untersuchungen
Technische Grundlagen
Messungen
Messwerkzeuge
Messung: KaZaA
Messung: Gnutella & OpenFT
Ergebnisse
Messergebnisse: KaZaA
Messergebnisse: Gnutella & OpenFT
Schaden, Maßnahmen
Literatur
Fazit

Fasttrack

- Client nicht quelloffen
- Eigener Client namens ,,Krawler”
  - Verbindet sich als Supernode
  - Sendet Anfragen an alle bekannten Supernodes
  - Aktualisiert Supernode-Liste über ,,supernode refresh list”
  - Aktive Suche im Netz
  - Lädt möglicherweise infizierte Dateien herunter

Gnutella und OpenFT

Veränderungen an den Clients Limewire und giFT

- Verbinden sich als Supernode
- Passives Monitoring von Suchanfragen und Ergebnissen
- Herunterladen möglicherweise infizierter Dateien

Messwerkzeuge

Einleitung
Motivation
Objekt der Untersuchungen
Technische Grundlagen
Messungen
Messwerkzeuge
Messung: KaZaA
Messung: Gnutella & OpenFT
Ergebnisse
Messergebnisse: KaZaA
Messergebnisse: Gnutella & OpenFT
Schaden, Maßnahmen
Literatur
Fazit

Fasttrack

- Client nicht quelloffen
- Eigener Client namens ,,Krawler”
  - Verbindet sich als Supernode
  - Sendet Anfragen an alle bekannten Supernodes
  - Aktualisiert Supernode-Liste über ,,supernode refresh list”
  - Aktive Suche im Netz
  - Lädt möglicherweise infizierte Dateien herunter

Gnutella und OpenFT

Veränderungen an den Clients Limewire und giFT

- Verbinden sich als Supernode
- Passives Monitoring von Suchanfragen und Ergebnissen
- Herunterladen möglicherweise infizierter Dateien

Messung: KaZaA

Einleitung
Motivation
Objekt der Untersuchungen
Technische Grundlagen
Messungen
Messwerkzeuge
Messung: KaZaA
Messung: Gnutella & OpenFT
Ergebnisse
Messergebnisse: KaZaA
Messergebnisse: Gnutella & OpenFT
Schaden, Maßnahmen
Literatur
Fazit

- Durchsuchen des Netzes nach beliebten Anfragen auf download.com
- Messungen: 2 mal 3 Tage (Februar und Mai 2006)

Suchbegriffe

Ad, Spyware, LimeWire, ICQ, Registry, SpyBot, WinZip, Morpheus, All, iMesh, IrfanView, WinRar, DivX, BitComet, RealPlayer, PC, Adobe, Trillian, Camfrog, SmartFTP, Nero, MSN, Quick, Knight

Messung: Gnutella & OpenFT

Einleitung
Motivation
Objekt der Untersuchungen
Technische Grundlagen
Messungen
Messwerkzeuge
Messung: KaZaA
Messung: Gnutella & OpenFT
Ergebnisse
Messergebnisse: KaZaA
Messergebnisse: Gnutella & OpenFT
Schaden, Maßnahmen
Literatur
Fazit

- Passive Überwachung des Netzes
- Messungen 45 Tage Gnutella, 37 Tage OpenFT
- Scan der Downloads mit ClamAV

Downloadkriterien

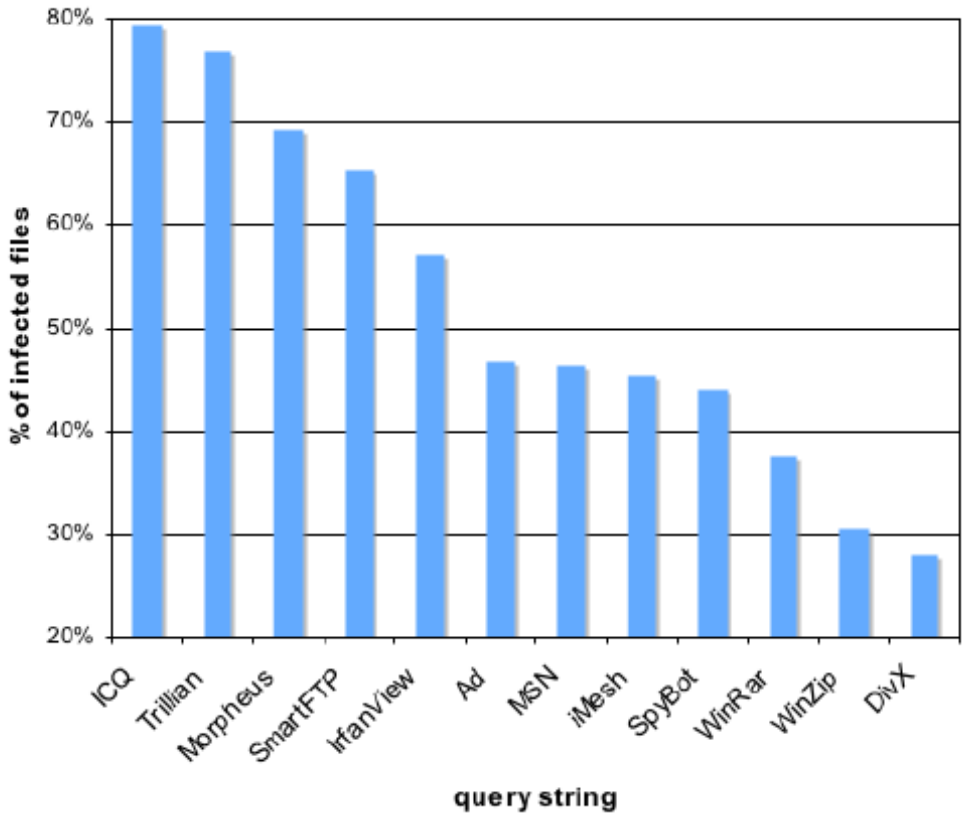
Ausführbare Dateien, Archive, Microsoft-Office-Dokumente

Messergebnisse: KaZaA

Einleitung
Motivation
Objekt der Untersuchungen
Technische Grundlagen
Messungen
Messwerkzeuge
Messung: KaZaA
Messung: Gnutella & OpenFT
Ergebnisse
Messergebnisse: KaZaA
Messergebnisse: Gnutella & OpenFT
Schaden, Maßnahmen
Literatur
Fazit

- Sehr hoher Anteil infizierter Dateien
- Messung nicht repräsentativ

Abbildung: Anteil infizierter Dateien

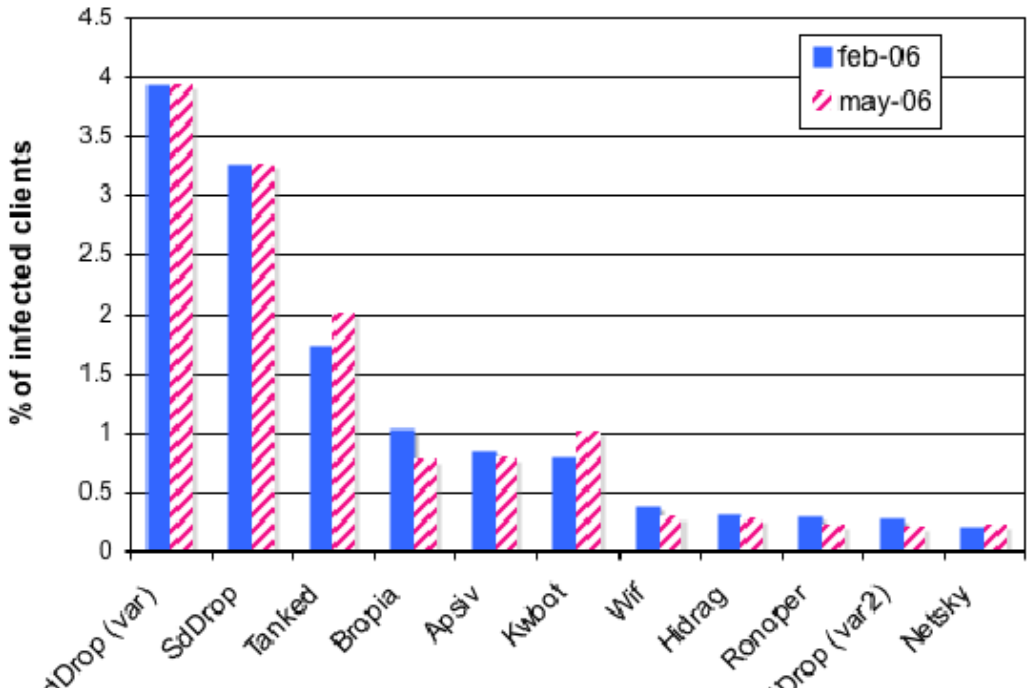


Häufigste Schädlinge

Einleitung
Motivation
Objekt der Untersuchungen
Technische Grundlagen
Messungen
Messwerkzeuge
Messung: KaZaA
Messung: Gnutella & OpenFT
Ergebnisse
Messergebnisse: KaZaA
Messergebnisse: Gnutella & OpenFT
Schaden, Maßnahmen
Literatur
Fazit

- Situation ist stabil
- Häufigste Schädlinge speziell für Einsatz in Peer-to-Peer-Netzen entwickelt
- Viren mit vielen Binärvarianten verbreiten sich besser

Abbildung: Häufigste Schädlinge im KaZaA-Netz



Schädlinge im KaZaA-Netz

Einleitung
Motivation
Objekt der Untersuchungen
Technische Grundlagen
Messungen
Messwerkzeuge
Messung: KaZaA
Messung: Gnutella & OpenFT
Ergebnisse
Messergebnisse: KaZaA
Messergebnisse: Gnutella & OpenFT
Schaden, Maßnahmen
Literatur
Fazit

Art der Schädlinge im KaZaA-Netz (der Häufigkeit nach):

1. Backdoors
2. Spamversand
3. Ausführen von DDoS
4. Datendiebstahl

Tabelle: Art der Malware in KaZaA

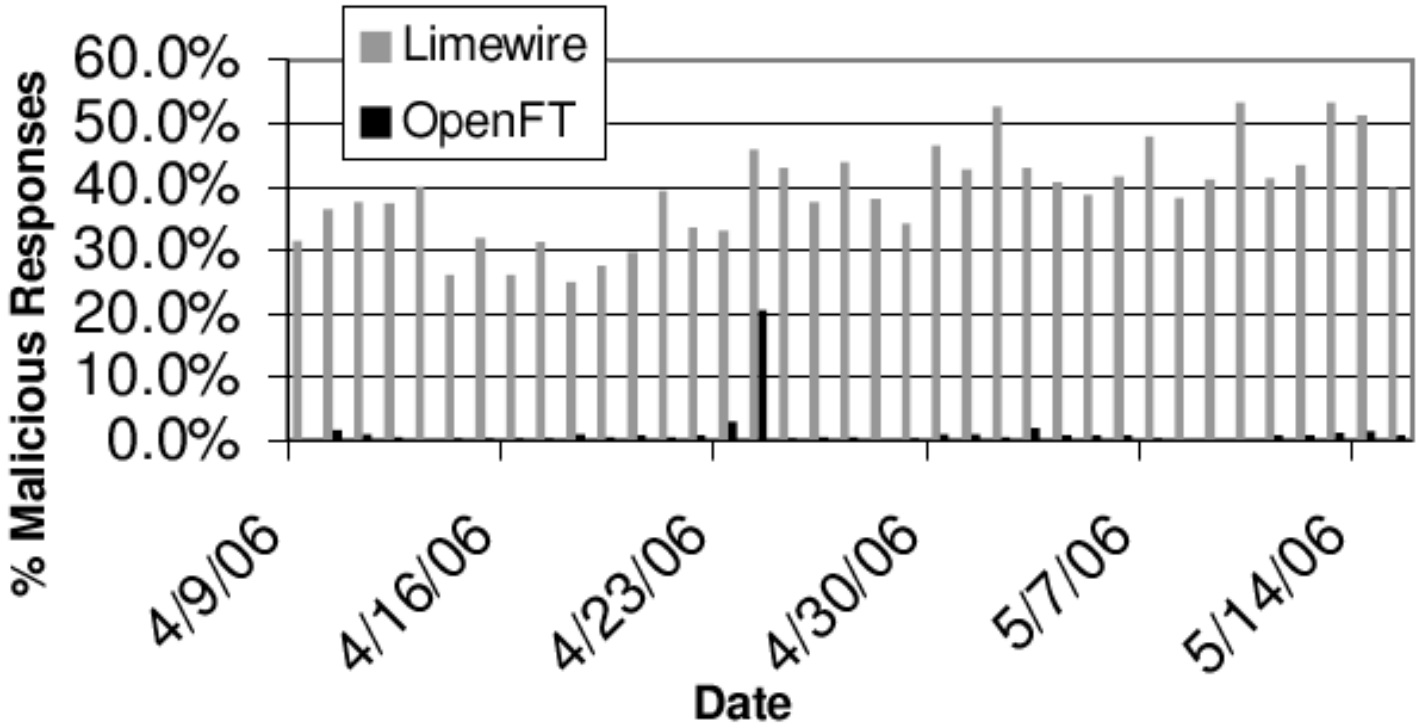
Attack	Virus list
Backdoor	Sndc, Tanked, Kwbot, Bagle, Darby, SdBot, SpyBot, Swen, IRCBot, Agent.Gen, Delf, Dropper
Spam (email)	Bagle, Darby, Mapson-A, Ronoper, Swen, NetSky
Spam (messenger)	Bropia, Supova
DDoS	Darby, Kindal, SdBot
Information stealing	Darby, SdBot

Messergebnisse: Gnutella & OpenFT

Einleitung
Motivation
Objekt der Untersuchungen
Technische Grundlagen
Messungen
Messwerkzeuge
Messung: KaZaA
Messung: Gnutella & OpenFT
Ergebnisse
Messergebnisse: KaZaA
Messergebnisse: Gnutella & OpenFT
Schaden, Maßnahmen
Literatur
Fazit

- Hoher Befall im Gnutella-Netz
- Sehr geringer Befall im OpenFT-Netz

Abbildung: Anteil infizierter Dateien



Kritische Suchanfragen

Einleitung
Motivation
Objekt der Untersuchungen
Technische Grundlagen
Messungen
Messwerkzeuge
Messung: KaZaA
Messung: Gnutella & OpenFT
Ergebnisse
Messergebnisse: KaZaA
Messergebnisse: Gnutella & OpenFT
Schaden, Maßnahmen
Literatur
Fazit

- P2P-Viren benennen sich nach aktuellen Trends
- Daher erhöhte Infektionsrate bei bestimmten Suchbegriffen

Kritische Suchbegriffe: Gnutella

scary movie 4, ice age 2, 2006, lost, silent hill, ice age, sex, ...

Kritische Suchbegriffe: OpenFT

crack, adobe, sims, limewire, games, windows xp, macromedia, ...

Spezielle Situation im OpenFT-Netz

Einleitung
Motivation
Objekt der Untersuchungen
Technische Grundlagen
Messungen
Messwerkzeuge
Messung: KaZaA
Messung: Gnutella & OpenFT
Ergebnisse
Messergebnisse: KaZaA
Messergebnisse: Gnutella & OpenFT
Schaden, Maßnahmen
Literatur
Fazit

- Einsatz häufig unter UNIX-Systemen
- Tausch von Windows-Binaries daher seltener
- Ausführen von Windows-Binaries oft nicht möglich, daher Umbenennung von Viren (z.B. in Filmnamen) selten

Schaden

Einleitung
Motivation
Objekt der Untersuchungen
Technische Grundlagen
Messungen
Messwerkzeuge
Messung: KaZaA
Messung: Gnutella & OpenFT
Ergebnisse
Messergebnisse: KaZaA
Messergebnisse: Gnutella & OpenFT
Schaden, Maßnahmen
Literatur
Fazit

Ausbreitung der Viren erfordert Nutzerinteraktion

- Herunterladen und Ausführen von Binaries Vorraussetzung für Infektion
- Herunterladen von Medien (Musik/Filmen) stellt nur geringe Gefahr dar:
  - Infektion solcher Dateien erfordert Kenntnis des Players

Verursachter Schaden schwer zu messen

- Backdoors sind universell, Schaden schwer einzuschätzen
- Beteiligung an DDoS im Nachhinein kaum nachweisbar
- Auch Datendiebstahl selten nachzuweisen
- Emailspam ist leichter zu verfolgen
  - 70% der infizierten Hosts an Spamversand beteiligt (laut verschiedener Blacklists)

Schaden

Einleitung
Motivation
Objekt der Untersuchungen
Technische Grundlagen
Messungen
Messwerkzeuge
Messung: KaZaA
Messung: Gnutella & OpenFT
Ergebnisse
Messergebnisse: KaZaA
Messergebnisse: Gnutella & OpenFT
Schaden, Maßnahmen
Literatur
Fazit

Ausbreitung der Viren erfordert Nutzerinteraktion

- Herunterladen und Ausführen von Binaries Vorraussetzung für Infektion
- Herunterladen von Medien (Musik/Filmen) stellt nur geringe Gefahr dar:
  - Infektion solcher Dateien erfordert Kenntnis des Players

Verursachter Schaden schwer zu messen

- Backdoors sind universell, Schaden schwer einzuschätzen
- Beteiligung an DDoS im Nachhinein kaum nachweisbar
- Auch Datendiebstahl selten nachzuweisen
- Emailspam ist leichter zu verfolgen
  - 70% der infizierten Hosts an Spamversand beteiligt (laut verschiedener Blacklists)

Gegenmaßnahmen

Einleitung
Motivation
Objekt der Untersuchungen
Technische Grundlagen
Messungen
Messwerkzeuge
Messung: KaZaA
Messung: Gnutella & OpenFT
Ergebnisse
Messergebnisse: KaZaA
Messergebnisse: Gnutella & OpenFT
Schaden, Maßnahmen
Literatur
Fazit

Heuristik: Dateigröße

Identifizieren von Malware anhand von Dateigröße:

- Liefert heutzutage akzeptabele Ergebnisse
- Dennoch naiv, da leicht auszuhebeln
  - Viren mit variabler Dateigröße einfach zu implementieren
  - Durch Blacklisting vieler Dateigrößen viele False-Positives

Virenscanner

Einbau von Virenscanner in Peer-to-Peer-Client

- Leicht zu realisieren
- Würde sehr gute Ergebnisse liefern
- Benutzer könnte das aber auch selbst erledigen

Gegenmaßnahmen

Einleitung
Motivation
Objekt der Untersuchungen
Technische Grundlagen
Messungen
Messwerkzeuge
Messung: KaZaA
Messung: Gnutella & OpenFT
Ergebnisse
Messergebnisse: KaZaA
Messergebnisse: Gnutella & OpenFT
Schaden, Maßnahmen
Literatur
Fazit

Heuristik: Dateigröße

Identifizieren von Malware anhand von Dateigröße:

- Liefert heutzutage akzeptabele Ergebnisse
- Dennoch naiv, da leicht auszuhebeln
  - Viren mit variabler Dateigröße einfach zu implementieren
  - Durch Blacklisting vieler Dateigrößen viele False-Positives

Virenscanner

Einbau von Virenscanner in Peer-to-Peer-Client

- Leicht zu realisieren
- Würde sehr gute Ergebnisse liefern
- Benutzer könnte das aber auch selbst erledigen

Gegenmaßnahmen

Einleitung
Motivation
Objekt der Untersuchungen
Technische Grundlagen
Messungen
Messwerkzeuge
Messung: KaZaA
Messung: Gnutella & OpenFT
Ergebnisse
Messergebnisse: KaZaA
Messergebnisse: Gnutella & OpenFT
Schaden, Maßnahmen
Literatur
Fazit

Verteiltes System

Im Netz verteiltes System zur Abstimmung über ,,Gefährlichkeit" von Dateien

- Bringt viele mögliche Schwierigkeiten mit sich
  - ,,Böswillige" Clients
  - Gemeinsame Kriterien zur Abstimmung müssen gefunden werden
  - Verteiltes Aktualisieren von Signaturen anfällig für Angriffe
- Wäre aber universell einsetzbar (zur Bewertung anderer Kriterien)
- Insbesondere für soziale Netze interessant

Literatur

Einleitung
Motivation
Objekt der Untersuchungen
Technische Grundlagen
Messungen
Messwerkzeuge
Messung: KaZaA
Messung: Gnutella & OpenFT
Ergebnisse
Messergebnisse: KaZaA
Messergebnisse: Gnutella & OpenFT
Schaden, Maßnahmen
Literatur
Fazit

 Andrew Kalafut, Abhinav Acharya, Minaxi Gupta. A Study of Malware in Peer-to-Peer Networks. IMC'06, October 25-27.

 Seungwon Shin, Jaeyeon Jung, Hari Balakrishnan. Malware Prevalence in the KaZaA File-Sharing Network. IMC'06, October 25-27, 2006.

 Sepandar D. Kamvar, Mario T. Schlosser, Hector Garcia-Molina. The EigenTrust Algorithm for Reputation Management in P2P Networks. WWW2003, May 20–24, 2003.

Fazit

Malware in P2P-Netzen

Einleitung
Motivation
Objekt der Untersuchungen
Technische Grundlagen
Messungen
Messwerkzeuge
Messung: KaZaA
Messung: Gnutella & OpenFT
Ergebnisse
Messergebnisse: KaZaA
Messergebnisse: Gnutella & OpenFT
Schaden, Maßnahmen
Literatur
Fazit

- Hoher Anteil infizierter Dateien
- P2P-Malware wird auch benutzt (zumindest für Spamversand)
- Gegenmaßnahmen bleiben bisher dem Benutzer überlassen
- OpenFT stellt eine Ausnahme dar