Computerwürmer

und deren Infektionswege

Ravinder Sangar, Philip Fraunlob, Jonas Winkler

31.01.2020

Inhalt

Was ist ein Computerwurm?

Computerwurm

- Ein Computerprogramm, das sich selbständig verbreitet
- Gehört zur Malware (Schadsoftware)
- Bei der Verbreitung dupliziert er sich
- Erstmals 1988 programmiert: *Morris-Wurm*

Computerwurm

- Ein Computerprogramm, das sich selbständig verbreitet
- Gehört zur Malware (Schadsoftware)
- Bei der Verbreitung dupliziert er sich
- Erstmals 1988 programmiert: *Morris-Wurm*

Quelle: *https://www.kaspersky.de/blog/der-morris-wurm-wird-25*

Wurm vs. Virus

Virus

- Braucht ein Wirtsprogramm als Träger des Virus
- Verbreitet sich nicht selbstständig

Wurm

- Ist ein eigenständiges Programm
- Verbreitet sich selbstständig

Payload

- Schaden kann sowohl minimal als auch verheerend sein
- Häufig werden Daten gestohlen oder manipuliert (z.B. Kreditkartennummern, Passwörter)

Email-Wurm

Funktionsweise des Email-Wurms

- Übertragung:
  - Ursprünglich über Email
  - Heute immer häufiger über soziale Medien
- Benötigen normalerweise ein Hilfsprogramm
- Bezeichnet als Social-Engineering-Attacken
- Aktivierung durch Täuschungstechniken
- Auswirkungen je nach Art unterschiedlich

Loveletter

- Verbreitung in den 2000er
- Geschrieben in *Visual Basic Script*

Loveletter

- Verbreitung in den 2000er
- Geschrieben in *Visual Basic Script*

Quelle: *https://www.f-secure.com/v-descs/love.shtml*

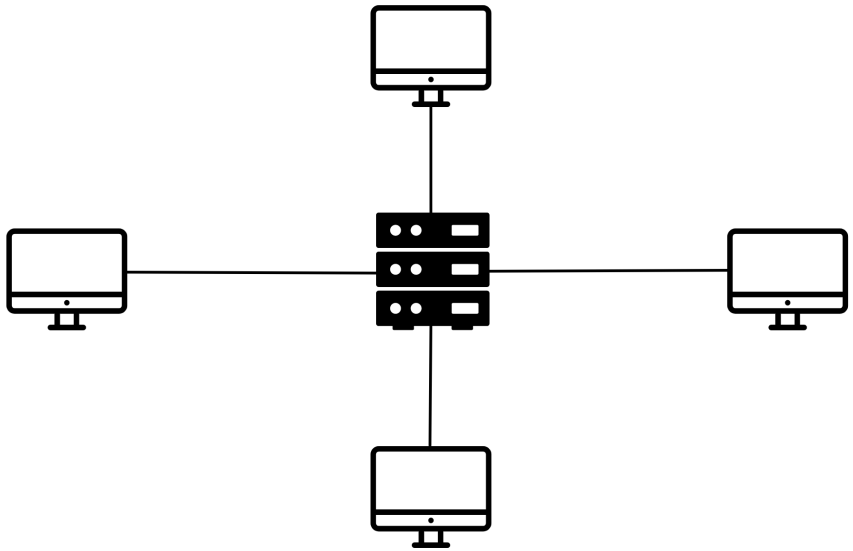
Algorithmus

1. Initialisiere (Ermittle wichtige Informationen wie das Win-Verzeichnis)
2. Kopiere dich selbst in das System-Verzeichnis
3. Schreibe dich in die Registry, sodass du beim Booten auf jeden Fall ausgeführt wirst.
4. Verbreite dich via E-Mail
   - Lies alle Personen aus dem Adressbuch von Outlook aus und verschicke dich selbst.
5. Infektion
   - Ersetze bestimmte Dateien auf der Festplatte

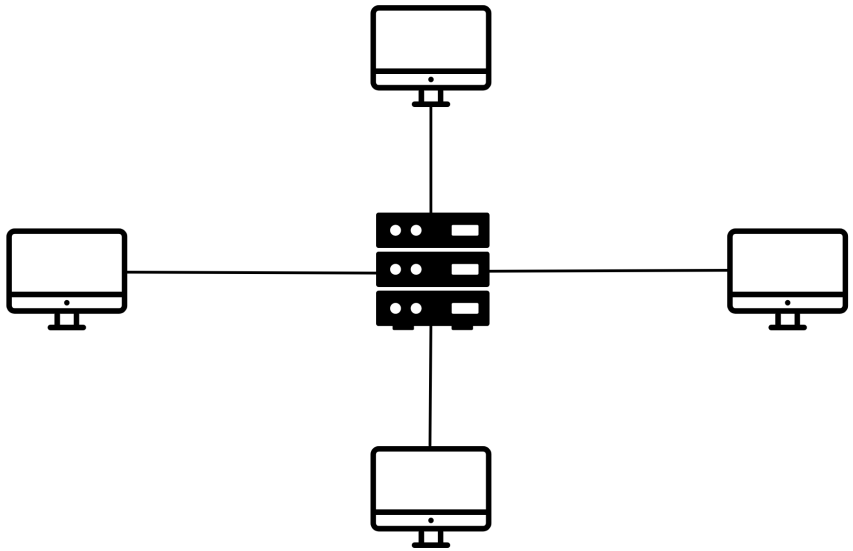
P2P-Wurm

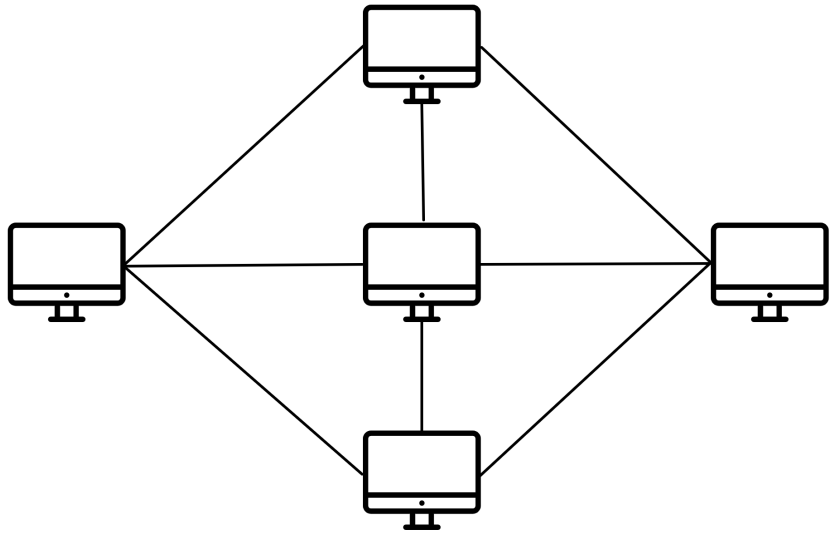
Peer-To-Peer Netzwerk

Peer-To-Peer Netzwerk



Peer-To-Peer Netzwerk





P2P-Wurm vs. Scanning-Wurm

P2P Wurm

- IP Adressen bekannt
- Verbindungsaufbau zum Rechner bereits vorhanden
- Passen sich dem Verkehr an

Scanning-Wurm

- Sucht IP Adressen zufällig
- Verbindungsaufbau zum Rechner erforderlich
- Suchen nach Sicherheitslücken erforderlich

Klassen des P2P-Wurms

Topological

- Infiziert selbst die Nachbarn
- Hit-List

Passiv

- Bleibt im Shared-Folder
- Wartet auf Nutzer

Vielen Dank für Ihre Aufmerksamkeit