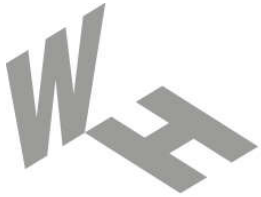


Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Botnetze

Prof. Dr. (TU NN)
Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
http://www.internet-sicherheit.de

if(is) internet-sicherheit.

Inhalt

- Einleitung
- Malware und seine Infektionsvektoren
- Netzwerkstrukturen in Botnetzen
- Schadfunktionen durch Bots
- Gegenmaßnahmen
- Ausblick
- Fazit

Inhalt

- **Einleitung**
- Malware und seine Infektionsvektoren
- Netzwerkstrukturen in Botnetzen
- Schadfunktionen durch Bots
- Gegenmaßnahmen
- Ausblick
- Fazit

Vom Virus zum Botnetz

- Der erste PC-Virus wurde im September 1986 entwickelt
- Codename: ©Brain

- *„Welcome to the Dungeon*
  *© 1986 Basit * Amjad (pvt) Ltd. BRAIN COMPUTER SERVICES 730 NIZAM BLOCK ALLAMA IQBAL TOWN LAHORE-PAKISTAN PHONE: 430791,443248,280530.*
  Beware of this VIRUS....
  Contact us for vaccination...“

Vom Virus zum Botnetz

- Die Motivation hat sich gewandelt
  - Früher: Entwicklung von Viren für Ruhm
  - Heute: Entwicklung von Viren für Reichtum
- Finanzieller Anreiz führte zur organisierten Kriminalität

Vom Virus zum Botnetz

- Botnetz: Steuerbares Netzwerk mehrerer infizierter Systeme
- Vorteile aus Perspektive des Angreifers
  - Infizierte Systeme können gesteuert werden
  - Leistung mehrerer Bots kann gebündelt werden
  - Wechselnde Angriffsquellen möglich
  - **Hoher finanzieller Nutzen**

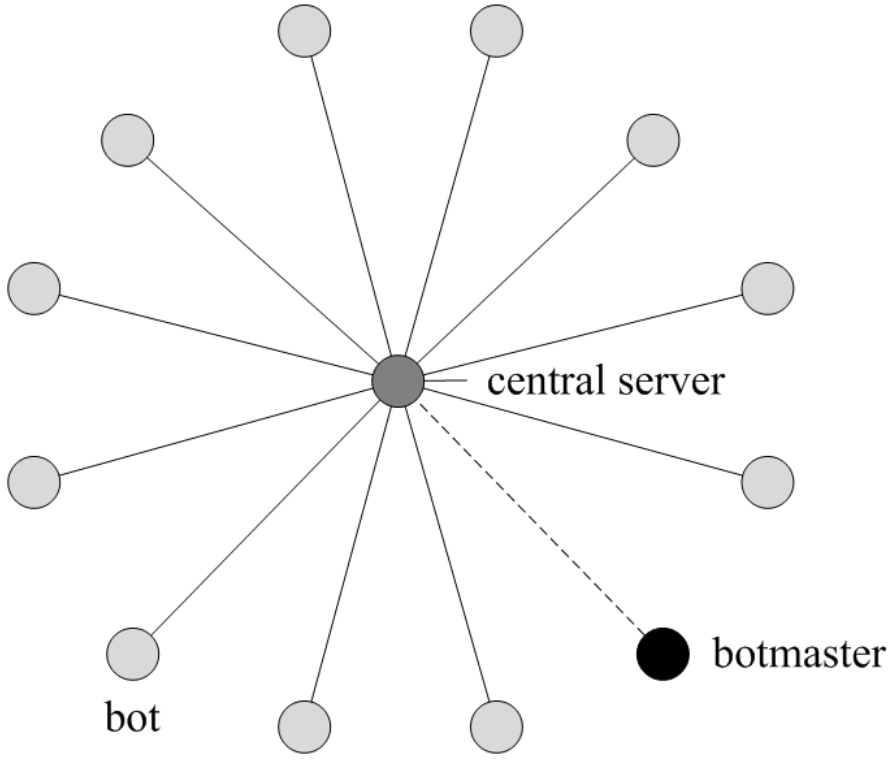
Vom Virus zum Botnetz

- Trend zu immer mehr Botnetzen hält an

- Anzahl infizierter Systeme ist ungewiss, aber gewiss hoch
- Mittlerweile sehr großes Interesse von vielen Parteien

Vom Virus zum Botnetz
→ Definitionen

- ***Malware***: Malicious Software, d.h. Schadsoftware jeglicher Art
- ***Bot***: System, das mit Schadsoftware infiziert ist und durch eine entfernte Seite steuerbar ist
- ***Botnetz****:* Zusammenschluss von Bots in einem vom Botmaster kontrollierbaren Netzwerk
- ***Botmaster:*** Person mit Kontrolle über das Botnetz (Angreifer)
- ***C&C-Kommunikation***: Netzwerk-kommunikation zur Steuerung und Kommandierung von Bots (engl.: *Command & Control*)



Inhalt

- Einleitung
- **Malware und seine Infektionsvektoren**
- Netzwerkstrukturen in Botnetzen
- Schadfunktionen durch Bots
- Gegenmaßnahmen
- Ausblick
- Fazit

Infektionsvektoren
→ Wege zum Aufbau eines Botnetzes

- Ein Botnetz schließt mehrere infizierte Systeme zusammen
  - Systeme müssen infiziert werden
  - Gemeinsames Kommunikationsprotokoll
- Mehrere potentielle Infektionsvektoren
- Wahl ist entscheidend für den Erfolg eines Botnetzes
- Oft nur kurzzeitiger Erfolg für jeden Exploit
- Schnelligkeit des Angreifers ist wichtig!

Infektionsvektoren
→ Externe Medien

- ©Brain verbreitete sich per Diskette
- Heute Verteilung über USB-Sticks
  - Schnell und geräuschlos wiederbeschreibbares Medium
  - Autoplay-Funktion
- Infektion erfordert physische Verbreitung des Mediums
- Langsame Ausbreitung
- Beispiel: Zeus-Toolkit

Infektionsvektoren
→ Spam

- Malware im Spam-Anhang oder auf verlinkten Webseiten
- Meist unter Vorwand getarnt
- Erfordert „Mitarbeit“ des Benutzers
- Spamfilter zunehmend besser in der Erkennung
- Beispiele: Storm Worm

Fourth of July Party

All-Yours.Net [acjz@elp.rr.com]

Extra line breaks in this message were removed.

To: [redacted]

Hi. Neighbor has sent you a greeting ecard.
See your card as often as you wish during the next 15 days.

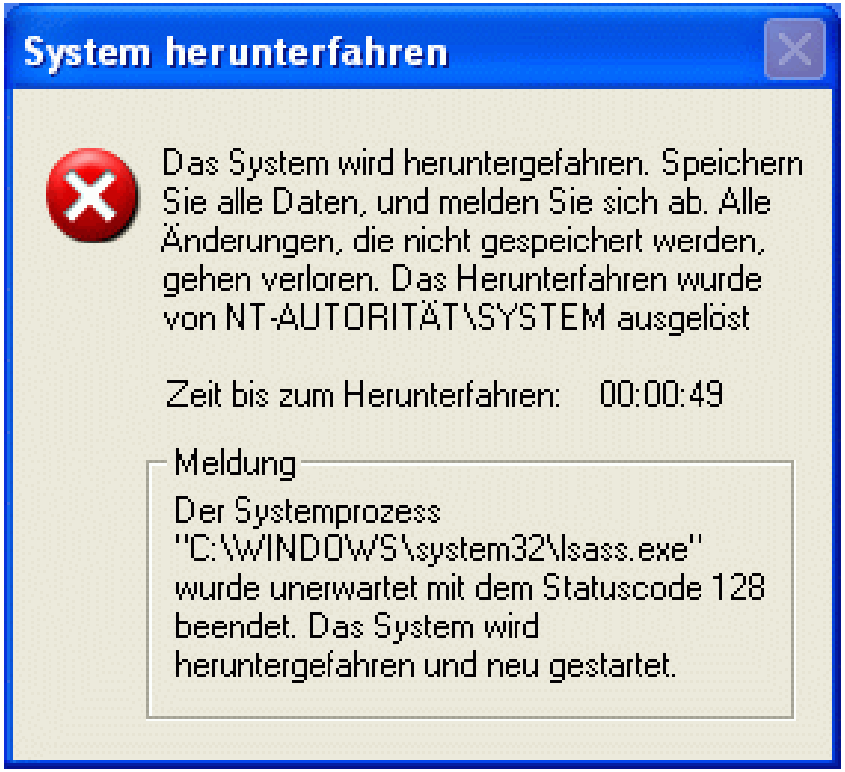
SEEING YOUR CARD

If your email software creates links to Web pages, click on your card's direct www address below while you are connected to the Internet:

http://75.23.42.46/?c775ed2175ee0c2a4c1c8a8a

Infektionsvektoren
→ Schwachstellen im Betriebssystem

- Keine Software ist perfekt
- Schwachstellen sind oft über das Netzwerk/Internet ausnutzbar
  - Insbesonders Systeme ohne Firewall / NAT
- Bekanntestes Beispiel: Sasser (2004)
- Keine Benutzerinteraktion notwendig
- Sehr schnelle Verbreitung möglich!
- Nur ein Teil der Systeme ist öffentlich erreichbar (NAT)



Infektionsvektoren
→ Sicherheitslücken in Anwendungen

- Neben dem OS sind auch installierte Anwendungen angreifbar
- Bestimmte Programmklassen sind prävalent
  - E-Mail-Clients: MS Outlook, Mozilla Thunderbird, ...
  - Web-Browser: MS Internet Explorere, Mozilla Firefox, ...
- Je mehr Nutzer eine Anwendung einsetzen, desto attraktiver

- **Vielseitige Angriffe durch Zero-Day-Exploits möglich**
  - Drive-By-Downloads auf präparierte Webseite
  - Präparierte E-Mails mit aktivem Inhalt
  - PDF-Dateien mit integriertem Exploit
  - Bilddateien mit integrierten Exploits

Infektionsvektoren
→ Social Engineering

- Social Engineering wird bei gezielten Angriffen eingesetzt
- Umfeld einer Zielperson wird ausgespäht
- Speziell präparierte „Angriffe“ bspw. per Mail
- Sehr effektiver Angriff mit hoher Erfolgswahrscheinlichkeit

- Einige Beispiele
  - Physikalischer Zugang
  - Authentisch wirkende E-Mails
  - Forging der Telefonnummer

Infektionsvektoren
→ Mehrfachinfektion

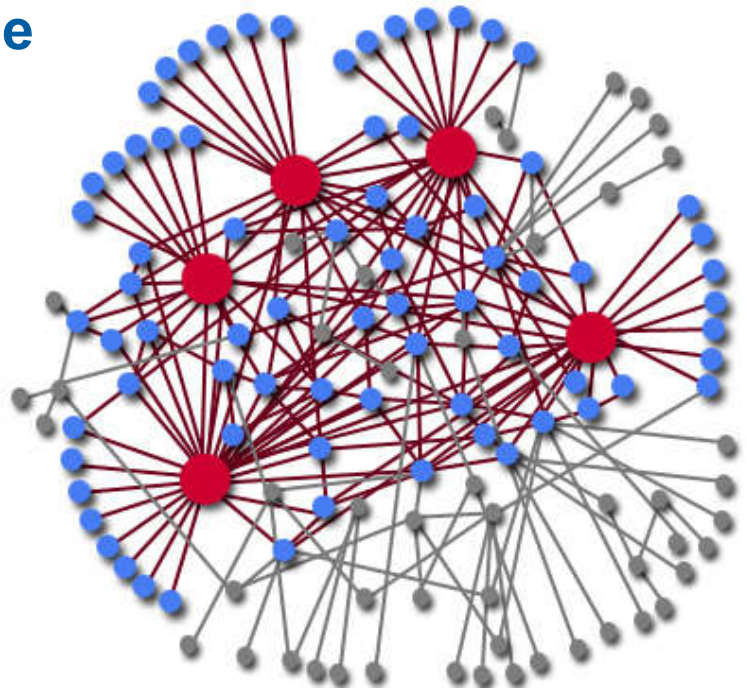
- Sicherheitslücken bleiben nach der Infektion bestehen
- Malware-Autoren stehen in Konkurrenz zueinander
- **Mehrfachinfektion kann nicht ausgeschlossen werden**
  - Gängige Praxis auf unsicheren Systemen
  - Doppelinstallation der selben Malware wird teilweise erkannt
- Trend: „Bereinigung“ von konkurrierender Malware

Inhalt

- Einleitung
- Malware und seine Infektionsvektoren
- **Netzwerkstrukturen in Botnetzen**
- Schadfunktionen durch Bots
- Gegenmaßnahmen
- Ausblick
- Fazit

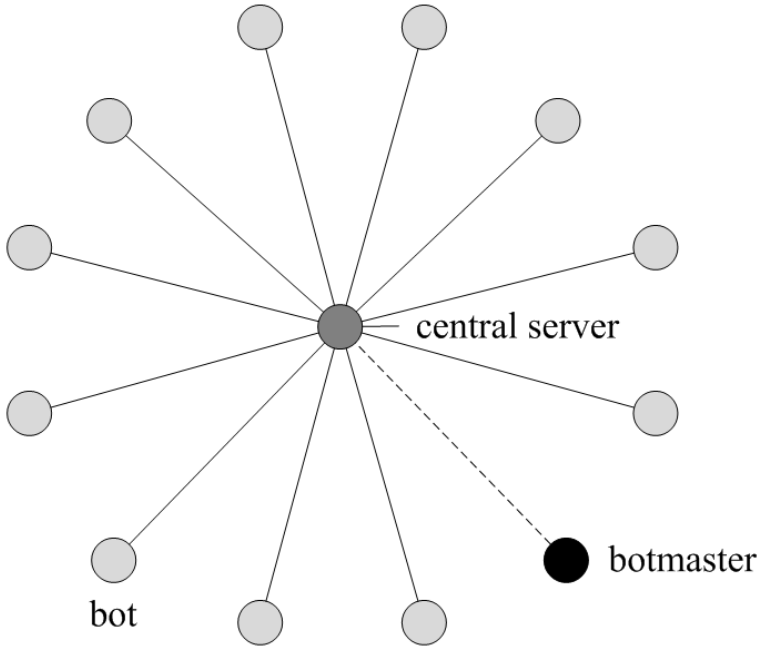
Netzwerkstrukturen in Botnetzen
→ Von der Infektion zum Netzwerk

- Nach der Infektion schließt sich das System dem Botnetz an
  - Statusinformationen werden mitgesendet
  - Botmaster erhält Kontrolle über das System
- Gemeinsames Kommunikationsprotokoll
  - Kommunikationsprotokolle im Malware-Binary verankert
  - **Command and Control (C&C) - Kanäle**
- Verschiedene Botnetz-Topologien
  - Zentralisiertes Botnetz
  - Verteiltes Botnetz
  - Hybrides Botnetz



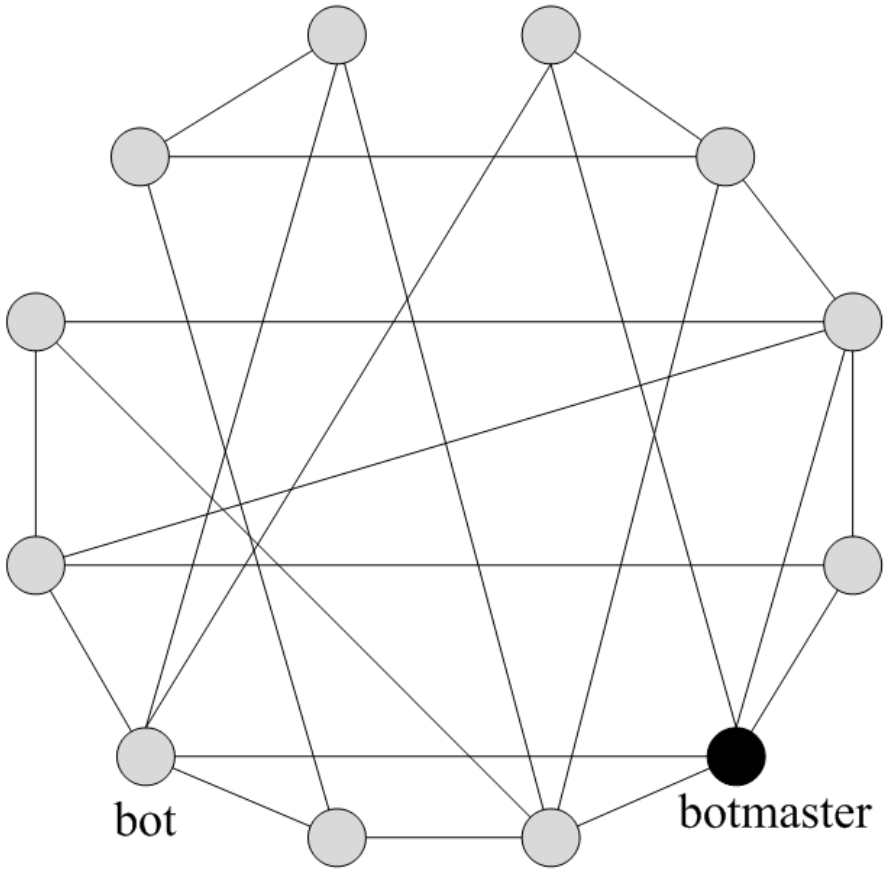
Netzwerkstrukturen in Botnetzen
→ Zentralisiertes Botnetz

- Zentraler Kommunikationsserver
- Historisch oft basierend auf Internet Relay Chat (IRC)
- Botmaster verbindet zum Server und steuert von dort
- **Vorteile:**
  - Einfache Client-Server-Implementierung
  - Zugangskontrolle zu Kommunikationsserver
- **Nachteile:**
  - C&C-Server muss gehostet werden
  - Single point of failure
- Bekanntes Beispiel: IRC SDBot



Netzwerkstrukturen in Botnetzen
→ Verteiltes Botnetz

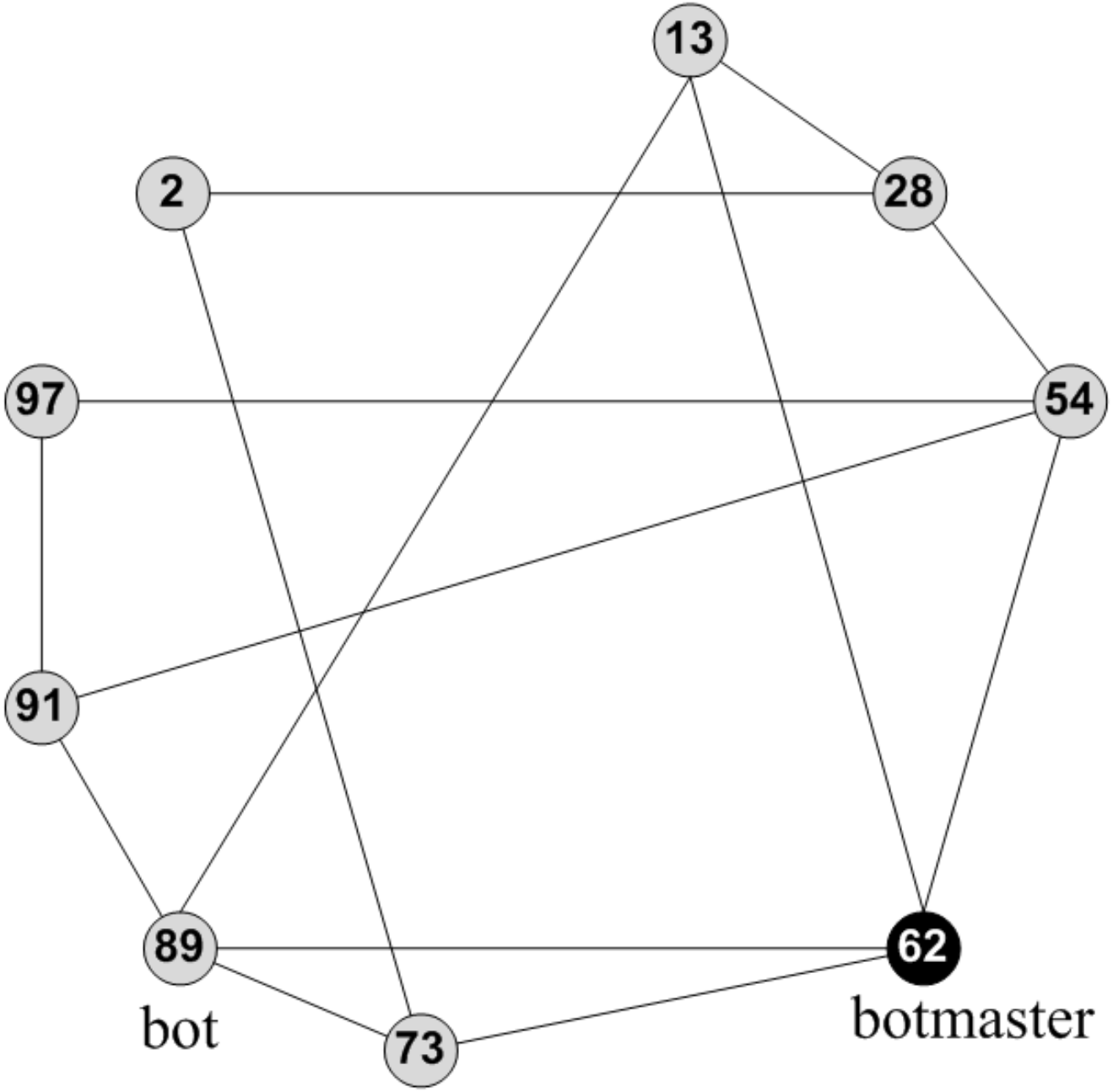
- Zusammenschluss der Bots mittels Peer-To-Peer (P2P)
- Kein C&C-Server
- **Vorteile:**
  - Kein single point of failure
  - Kein C&C-Server notwendig
- **Nachteile:**
  - Komplexere Implementierung
  - Schlechte Zugangskontrolle
  - NATing verhindert Peerings
- Bekanntes Beispiel: Storm



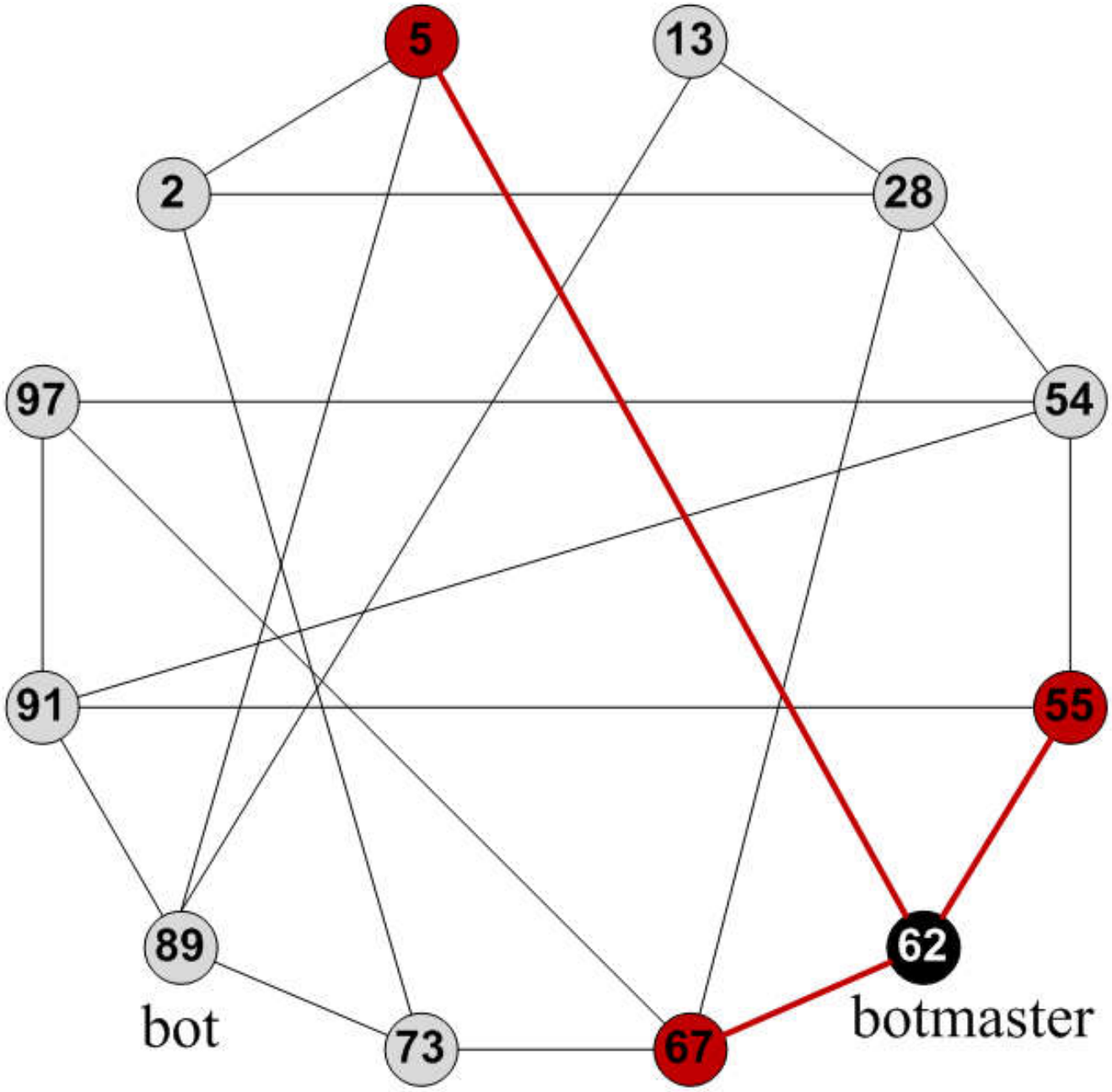
Netzwerkstrukturen in Botnetzen
→ Verteiltes Botnetz

- Weiterer Nachteil: P2P – Sicherheit

Netzwerkstrukturen in Botnetzen
→ Verteiltes Botnetz

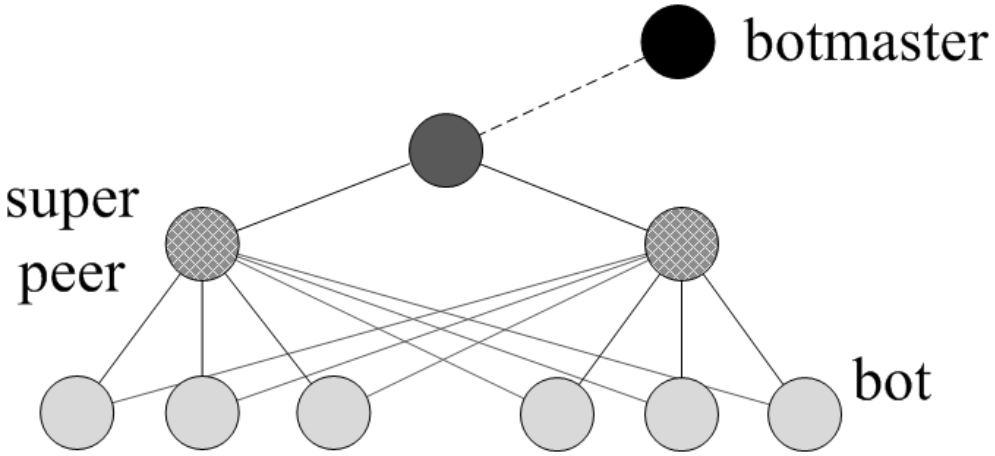


Netzwerkstrukturen in Botnetzen
→ Verteiltes Botnetz



Netzwerkstrukturen in Botnetzen
→ Hybride Botnetz

- Mehrere Kommunikationsserver
- Ähnlich wie zentrales Botnetz, jedoch ausfallsicherer
- **Vorteile:**
  - Kein single point of failure durch Redundanz
  - Einfache Client-Server-Implementierung
  - Zugangskontrolle zu Kommunikationsserver



- **Nachteile:**
  - C&C-Server müssen gehostet werden
- Bekanntes Beispiel: Waledac

Inhalt

- Einleitung
- Malware und seine Infektionsvektoren
- Netzwerkstrukturen in Botnetzen
- **Schadfunktionen durch Bots**
- Gegenmaßnahmen
- Ausblick
- Fazit

Schadfunktionen
→ Vom Botnetz zum Geld

- Botnetze sind meistens rein finanziell motiviert
- Angriffe können in Geld umgesetzt werden
- **Beliebtheit der Angriffe hängt von mehreren Faktoren ab**
  - Wieviel Geld kann eingenommen werden?
  - Wie hoch ist die Erfolgswahrscheinlichkeit?
  - Auf welchem Weg kommt das Geld zum Botmaster?
  - Wie auffällig ist der Angriff?
- Dabei werden Botnetze sogar entgeltlich vermietet

Schadfunktionen
→ Spreading

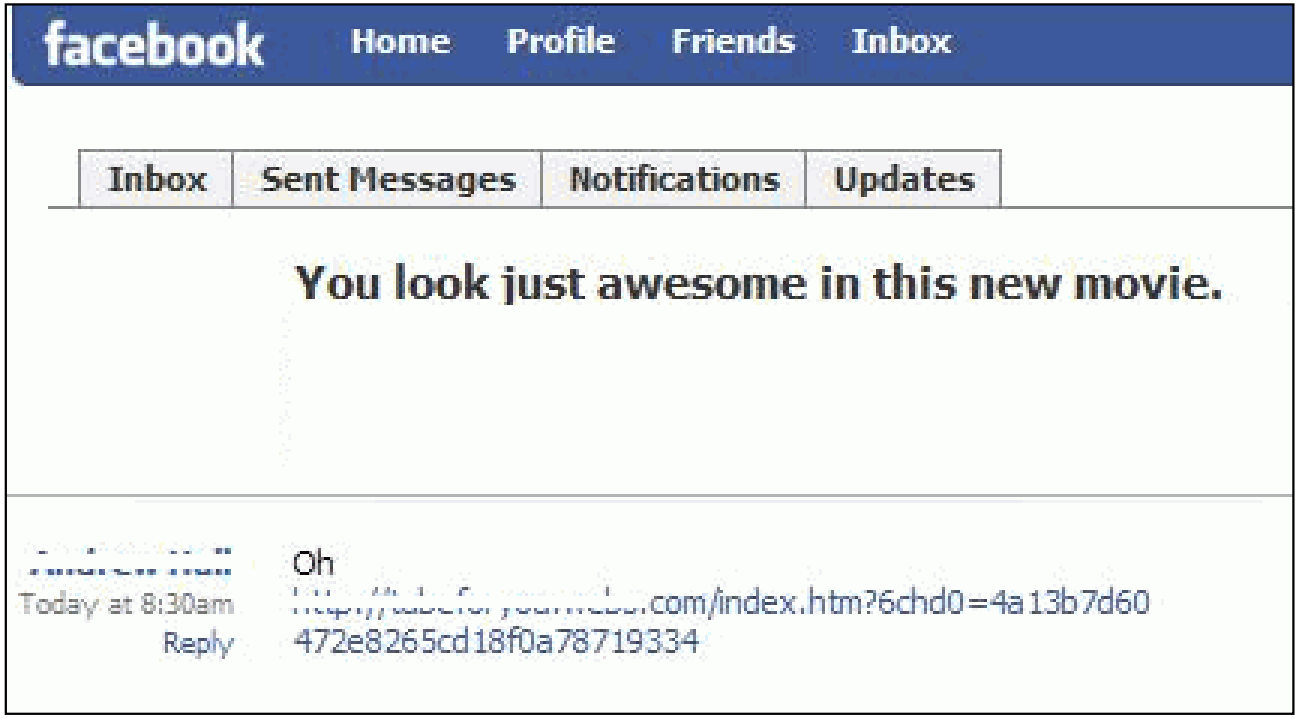
- **Spreading ist die Verbreitung des Botnetzes mittels Infektionen**
- Art des Spreadings ist abhängig von Infektionsvektor
- Potentielle Angriffe:
  - Port-Scans zum Aufdecken von Schwachstellen im OS
  - FTP-Bruteforce-Angriffe als Vorbereitung für Drive-By-Downloads
  - SSH-Bruteforce-Angriffe zur Aquise von neuen C&C-Server
  - E-Mail-Harvesting für das Spreading via Spam
- Spreading kann im Datenverkehr schnell entdeckt werden

Schadfunktionen
→ Spam

- E-Mails mit unaufgeforderter Werbung ist Spam
- Ursprünglich wurde Spam von Open-Relays versendet
- IP-Adress-Blacklisten sehr effektive Spam-Abwehr
- Bots haben jedoch häufig wechselnde IP-Adressen
  - Spam-Versand wurde durch Botnetze wieder möglich
  - Hohe Anzahl infizierter Systeme führt zu vielen Spam-Quellen
- **Bots verantworten 80% - 95% des globalen Spam-Volumens**
- Versand von Spam ist bei Endbenutzern sehr auffällig

Schadfunktionen
→ Spam

- Trend zum Web 2.0 – Spam
  - Blog-Kommentare
  - Spam in Social Networks
- Beispiel: Koobface



Schadfunktionen
→ Distributed Denial of Service

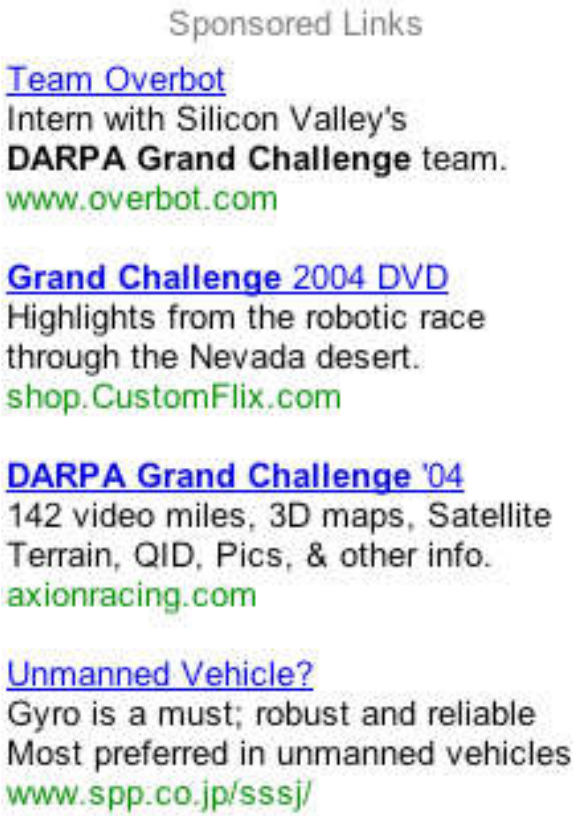
- Botnetze heben Denial of Service auf die nächste Stufe
  - Viele Systeme nehmen gleichzeitig an DoS-Angriff teil
  - Distributed Denial of Service (DDoS) – Angriffe
- Erpressung als mögliche finanzielle Motivation
- Teilweise auch politische Hintergründe
- Technisch vielfältige DoS-Möglichkeiten
  - SYN-Floods
  - Connection-Floodings

Schadfunktionen
→ Identity Theft

- Identität des Benutzers wird gestohlen
- Bekannt geworden durch Kreditkartendiebstahl
- Weitere Beispiele sind Banktrojaner oder Keylogger
- **Identity Theft ist kaum im Datenverkehr aufzuspüren**
- Direkter finanzieller Nutzen des Angriffs
- Angriff kann jedoch je Infektion nur begrenzt oft durchgeführt werden und ist selten wiederholbar

Schadfunktionen
→ Klickbetrug (Click fraud)

- Pay-per-click ist auf regulären Webseiten verbreitet
  - Webseitenbetreiber bindet Werbung Dritter ein
  - Bezahlung für jeden Klick des Besuchers
- Methode wird von Botnetzen missbraucht
  - Botnetz-Betreiber registrieren sich als Werber
  - Bots täuschen Klicks auf Werbelinks vor
- Eher unauffällig, da HTTP-basiert
- Direkter finanzieller Nutzen



Inhalt

- Einleitung
- Malware und seine Infektionsvektoren
- Netzwerkstrukturen in Botnetzen
- Schadfunktionen durch Bots
- **Gegenmaßnahmen**
- Ausblick
- Fazit

Gegenmaßnahmen
→ Lösung des Botnetz-Problems

- Großes Interesse, die allgemeine Gefahr einzudämmen
- Es gibt leider kein Allheilmittel
- Gegenmaßnahmen aus vielen Bereichen
- Nicht weniger Maßnahmen können umgangen werden
- Schwierigkeitsgrad für Angreifer erhöhen

Gegenmaßnahmen
→ User-Awareness

- Benutzer kennen das Problem Botnetze nicht
- Infektion hat keine direkten negativen Konsequenzen
- Problem muss publik gemacht werden
- Einfache Gegenmaßnahmen von Endbenutzern
  - Einsatz von Firewall und Virenscanner
  - Betriebssystem und Anwendungen regelmäßig updaten
  - Minimierung des Risikos durch NATing
  - Verhaltensregeln aufstellen

Gegenmaßnahmen
→ Regulatorische Maßnahmen

- Infektion von Systemen in Deutschland illegal
- Infrastruktur für Botnetze in Deutschland illegal
- **Botnetze sind jedoch ein globales Problem**
  - Andere Nicht-EU-Staaten sind weniger restriktiv
  - Grenzübergreifende Regeln sind komplex und zeitintensiv
  - Täter und Opfer bleiben geografisch getrennt
- Regulationen behindern leider auch „die gute Seite“
  - Technische Restriktionen bei der Erkennung (Datenschutz)
  - Direkter Eingriff in Botnetz-Infrastrukturen schwierig

Gegenmaßnahmen
→ Technische Abwehr von Angriffen

- Schaden der Botnetze kann limitiert werden
- Gegenmaßnahmen je Schadfunktion – z.B.:
  - Spam
  - Web 2.0 Spam
  - DDoS
  - Spreading
- **Lediglich Bekämpfung der Symptome – Ursache bleibt**
  - Angriffe werden potenziert (Bsp: Spam)
  - Latente Gefahr der Umgehung dieser Gegenmaßnahmen

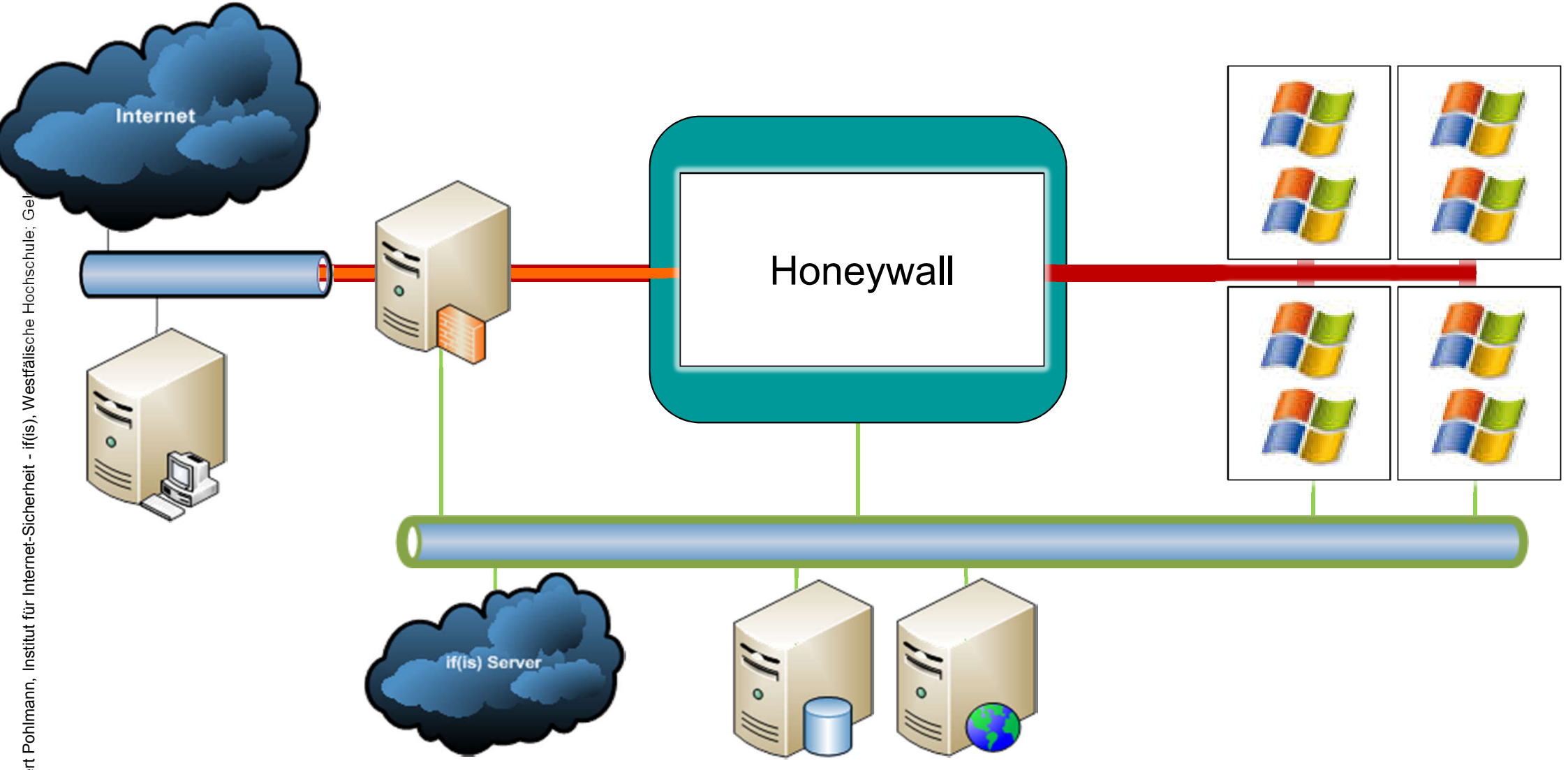
Gegenmaßnahmen
→ Organisatorische Sicherheit

- **Wenige Umstellungen minimieren das Risiko enorm**
- Minimierung des Infektionsrisikos
  - Eingeschränkte Benutzerrechte (d.h. kein Administrator)
  - Ausschließlich seriöse Webseiten besuchen
- Minimierung des Schadensrisikos
  - Banktrojaner scheitern bisher an mTAN
  - 2-Faktor-Authentisierung statt Passwörter
  - Regelmäßiges Ändern der Passwörter
- Minimierung des finanziellen Potentials von Botnetzen
  - Nicht auf DDoS-Erpressungen eingehen
  - Werbung: Paradigmenwechsel von *Pay per Click* auf *Pay per Sale*

Gegenmaßnahmen
→ Systemintegrität wiederherstellen

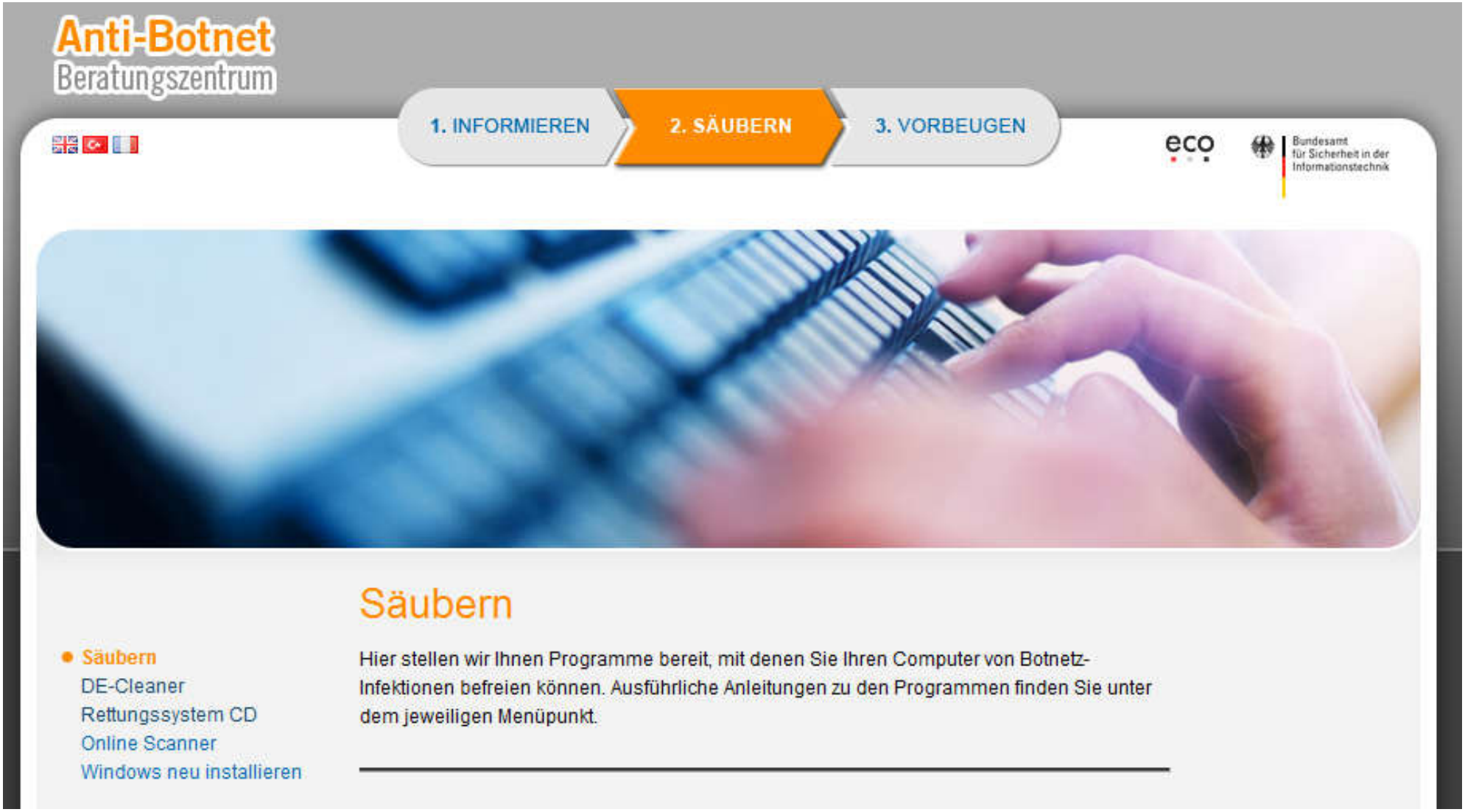
- Benutzer hat oft keine Kenntnis über Infektion
- Wissen über Infektion ist Grundvoraussetzung für Bereinigung
- **Mechanismen zur Erkennung von Botnetzen benötigt**
- Verschiedene Blickwinkel der Erkennung
  - Endbenutzer: Ist mein System infiziert?
  - Internet Service Provider: Welche Kundensysteme sind infiziert?
  - Hosting-Provider: Beinhaltet mein Netzwerk C&C-Server?
  - Unternehmen: Welche Unternehmenssysteme sind infiziert?

Exkurs
→ Das Sandnet des if(is)



Gegenmaßnahmen
→ Systemintegrität wiederherstellen

- Initiative in Deutschland: botfrei.de



Gegenmaßnahmen
→ Systemintegrität wiederherstellen

- Erfolg der Desinfektion hängt stark vom Reinfektionsrisiko ab
  - Sicherheitsniveau wird nicht automatisch mit Desinfektion erhöht
  - Den direkten Schaden von Infektion tragen oft andere
  - Zu geringe Motivation des Benutzers zur Wahrung der Integrität
- Konzept des **Walled Garden** erhöht die Motivation
  - Walled Garden kann vom Provider eingerichtet werden
  - Kunde erhält direkt Nachricht über die Infektion seines Systems
  - Infizierte Systeme haben nur beschränkt Internet-Zugang
  - Erst nach Bereinigung und weiteren Sicherheitsmaßnahmen
- Enormer personeller Aufwand (Support / Hotlines)

Gegenmaßnahmen
→ Takedown eines Botnetzes

- Botnetze haben typischerweise kritische Infrastruktur
  - C&C-Server sowie deren Integritäts- und Zugangsschutz
  - Domains zur Auflösung der IP-Adressen der C&C-Infrastruktur
- Erfordert Kooperation mit Behörden und/oder Hostern
  - Teilweise Bürokratie und Korruption bei Behörden
  - Insbesondere Bullet-Proof-Hoster vermeiden eine Kooperation
- Infrastruktur ist zudem meistens redundant ausgelegt
- Dennoch sind Takedowns erfolgreich
  - Waledac: Deregistrierung der Domains, P2P-Angriff (02/2010)
  - Rustock: Konfession von C&C-Servern (03/2011)

Inhalt

- Einleitung
- Malware und seine Infektionsvektoren
- Netzwerkstrukturen in Botnetzen
- Schadfunktionen durch Bots
- Gegenmaßnahmen
- **Ausblick**
- Fazit

Ausblick
→ Erwartete Trends

- Großes Potential für die Entstehung weiterer Botnetze
- Weiterentwicklung der Gegenmaßnahmen und Malware
  - Gegenmaßnahmen werden besser
  - Malware wird reifer und ausgefeilter
- Mehr und mehr Geräte werden dem Internet angeschlossen

Ausblick
→ Mobile Malware

- Malware zielt bisher primär auf den PC ab
  - Bedingt durch Erfahrungen in der Implementierung
  - Windows XP/Vista/7 findet eine weite Verbreitung
- **Mobile Malware zielt auf mobile Endgeräte ab**
  - Nur vereinzelte Fälle bekannt
  - Kein Botnetz basierend auf Mobile Malware bekannt
- Solche Botnetze werden aber wahrscheinlich entstehen
  - Neue Angriffstechniken (Dialler, Diebstahl Geo-Infos)
  - Wachsender Markt an Smartphones

Ausblick
→ Steganographie

- C&C-Kommandos waren traditionell unverschlüsselt
- Botnetze setzen vermehrt auf eine Verschlüsselung der Daten
- **Steganographie erschwert zusätzlich die C&C-Erkennung**
- Kreativität sind kaum Grenzen gesetzt
- Zwei bekannte Beispiele für HTTP:
  - Integration von Daten im Kommentarattribut von GIF-Bildern
  - Codierung von Daten in Reihenfolge der HTML-Attibute

```
<img src="test.jpg" width="13" height="37" alt="Test"
  title="Test" border="0" style="none;">
```

→ 7 Attribute, 5040 Kombinationen, 12 Bits!

Ausblick
→ Gezielte Angriffe

- Paradigma: Qualität vor Quantität
  - Kleinere Botnetze
  - Bestimmte Aufgabe
  - Hohe Tarnung wird angestrebt
- Stuxnet war ein Vorgeschmack
- Verschiedenartige Motivationen
  - Spionage
  - Sabotage
  - Erpressung von mächtigen Personen
- Gezielte Angriffe sind weniger auffällig und schwer erkennbar

Ausblick
→ Trusted Computing

- Malware unterwandert die Systemintegrität
- **Trusted Computing kann die Systemintegrität wahren**
  - TPM signiert und verifziert Systemdateien
  - Neue Applikationen müssen signiert werden
- Trusted Computing Hardware bereits in Systemen integriert
- Praktikable Software-Lösungen stehen noch aus

Inhalt

- Einleitung
- Malware und seine Infektionsvektoren
- Netzwerkstrukturen in Botnetzen
- Schadfunktionen durch Bots
- Gegenmaßnahmen
- Ausblick
- **Fazit**

Fazit

- Botnetze stellen eine immense Bedrohung des Internets dar
- Genaues Potential ist unklar, jedoch groß und zunehmend
- Infektionsvektoren bestimmen die Verbreitung von Botnetzen
  - Angreifer sucht möglichst große Angriffsfläche
  - Infektionsvektoren oft sehr kurzlebig
- Netzwerkstrukturen bestimmen die Stabilität von Botnetzen
  - Tarnung erschwert C&C-Erkennung
  - Hohe Redundanz erschwert Takedown

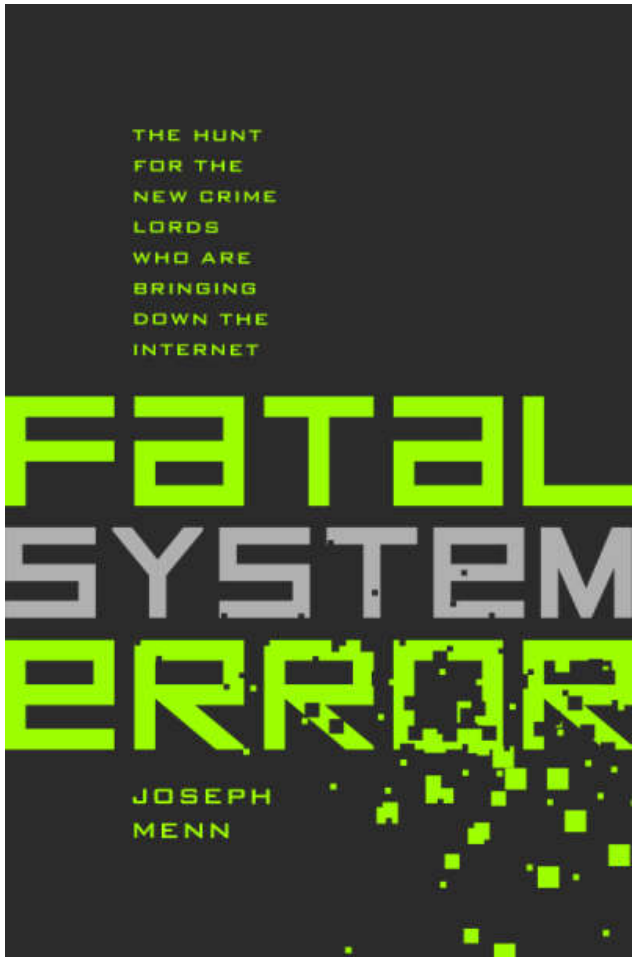
Fazit

- Gegenmaßnahmen sind vorhanden und werden populärer
  - Wiederherstellen der Systemintegrität
  - Takedown des Botnetzes
  - Awareness
  - Regulatorische und organisatorische Maßnahmen
- Angreifer versuchen die Gegenmaßnahmen zu umgehen
- Entwicklung hin zu ausgefeilten Botnetzen
  - Verschlüsselung und Steganographie
  - Gezielte Angriffe

Buchempfehlungen

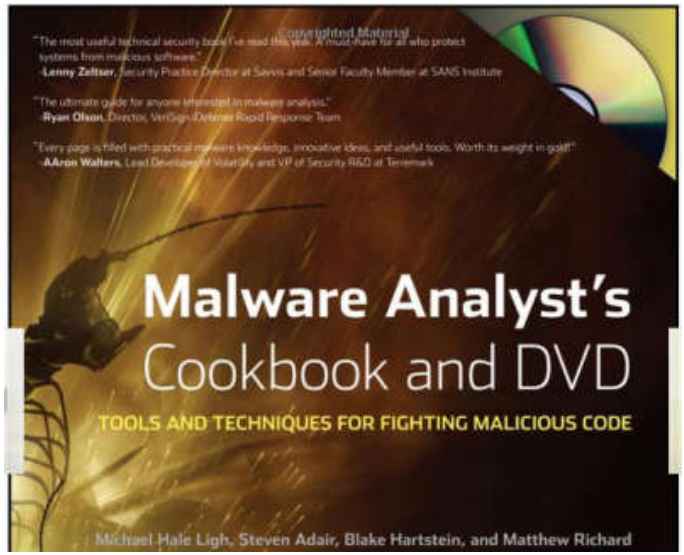
Fatal System Error

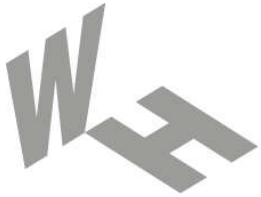
von Joseph Menn



Malware Analyst´s Cookbook

von Ligh et al.





Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Botnetze

Vielen Dank für Ihre Aufmerksamkeit
Fragen?

Prof. Dr. (TU NN)
Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
http://www.internet-sicherheit.de