Rishi

Identifizierung von Bots durch Auswerten der IRC Nicknamen

Jan Göbel & Thorsten Holz

goebel@rz.rwth-aachen.de

thorsten.holz@informatik.uni-mannheim.de

13. Februar 2008

DFN Workshop 2008

Inhalt

Inhalt

Einleitung

Was ist Rishi?

- Der Begriff „Rishi“ kommt aus dem Hinduismus und bezeichnet einen Seher oder Weisen. Ihnen wird zugesagt Wunder zu bewirken oder Krankheiten zu heilen.
- Hier: eine Software zur Erkennung von IRC Bot infizierten Rechnern
- Netzwerk basierte Erkennung, d.h. keine zusätzliche Software auf den Clients notwendig
- Kleines Python Skript (ca. 2280 Zeilen Code), welches passiv den Netzwerkverkehr belauscht und analysiert.
- Nutzt eine Eigenschaft des IRC Protokolls zur Erkennung von Bots (Eindeutigkeit des Nickname)

Einleitung

Grunprinzip

- IRC Protokoll besitzt eine Reihe von Schlüsselwörtern
- Rishi sucht nach Vorkommen der folgenden Schlüsselwörter: JOIN, NICK, USER, MODE
- Alle zu den Schlüsselwörtern gehörigen Parameter werden extrahiert
- Besonderes Augenmerk liegt auf dem verwendeten Nickname, der zusammen mit dem Kommando NICK übertragen wird.

Inhalt

Analyse Funktion

Einleitung

- Jeder Nickname wird analysiert und bewertet (Punktesystem)
- Je höher die Punktzahl am Ende ist, desto wahrscheinlicher handelt es sich um einen Bot
- Derzeitiger Schwellwert liegt bei 10 Punkten
- Für die Berechnung der Endpunktzahl werden verschiedene Kriterien herangezogen, die unterschiedliche Gewichtung haben

Analyse Funktion

Bewertung des Nickame

- Prüfen gegen statische und dynamische Whiteliste/Blackliste (N-Gramm Analyse)
- Entfernen bekannter Nickname Extensions: ^essen, _away
- Prüfen auf ...
  - verdächtige Zeichenketten: DEU, r00t3d
  - verdächtige Anfangs- oder Endzeichenketten: l33t-, p0w, _13
  - Nickname besteht nur aus Ziffern
  - Anzahl aufeinanderfolgender Ziffern und verdächtige Zeichen: |, [,]
- Prüfe gegen 77 reguläre Ausdrücke, die durch die Auswertung von ca. 4000 IRC Bots und bis heute entdeckten Varianten entstanden sind

Analyse Funktion

Zusätzliche Faktoren

- Prüfen auf ...
  - bekannte Command and Control Server
  - bereits gesehenen Botnet Channel
  - nicht-standard IRC Server Port
  - Clients die nicht zum IRC verbinden sollten

Analyse Funktion

Beispiel

- Beispiel: [00|DEU|048651]
  - 2 Punkte für: [und]
  - 2 Punkte für zwei |
  - 1 Punkt für die Zeichenkette: DEU
  - 4 Punkte für die Ziffernpaare
  - 10 Punkte für passenden regulären Ausdruck
- Ohne passenden regulären Ausdruck: 9 Punkte / mit 19 Punkte

Analyse Funktion

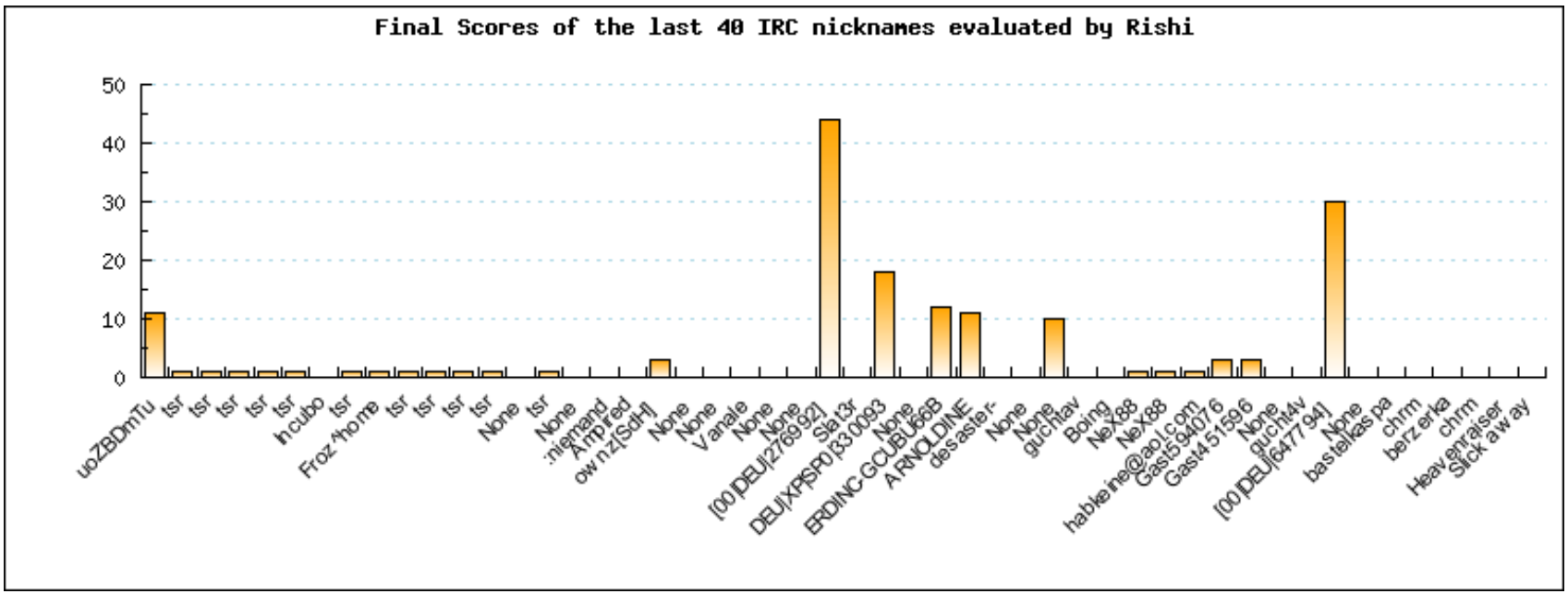
Beispiel

- Ohne und mit regulärem Ausdruck (Webinterface)

23.01.2008 07:05:19	134.130	218.229.156.212	7676	[DEU][12]91G-BW	18
23.01.2008 06:41:17			6669	[Soma]	3
23.01.2008 06:37:22	134.130	218.229.156.212	7676	[DEU][12]91G-BW	8

Analyse Funktion

Ausgabe



Inhalt

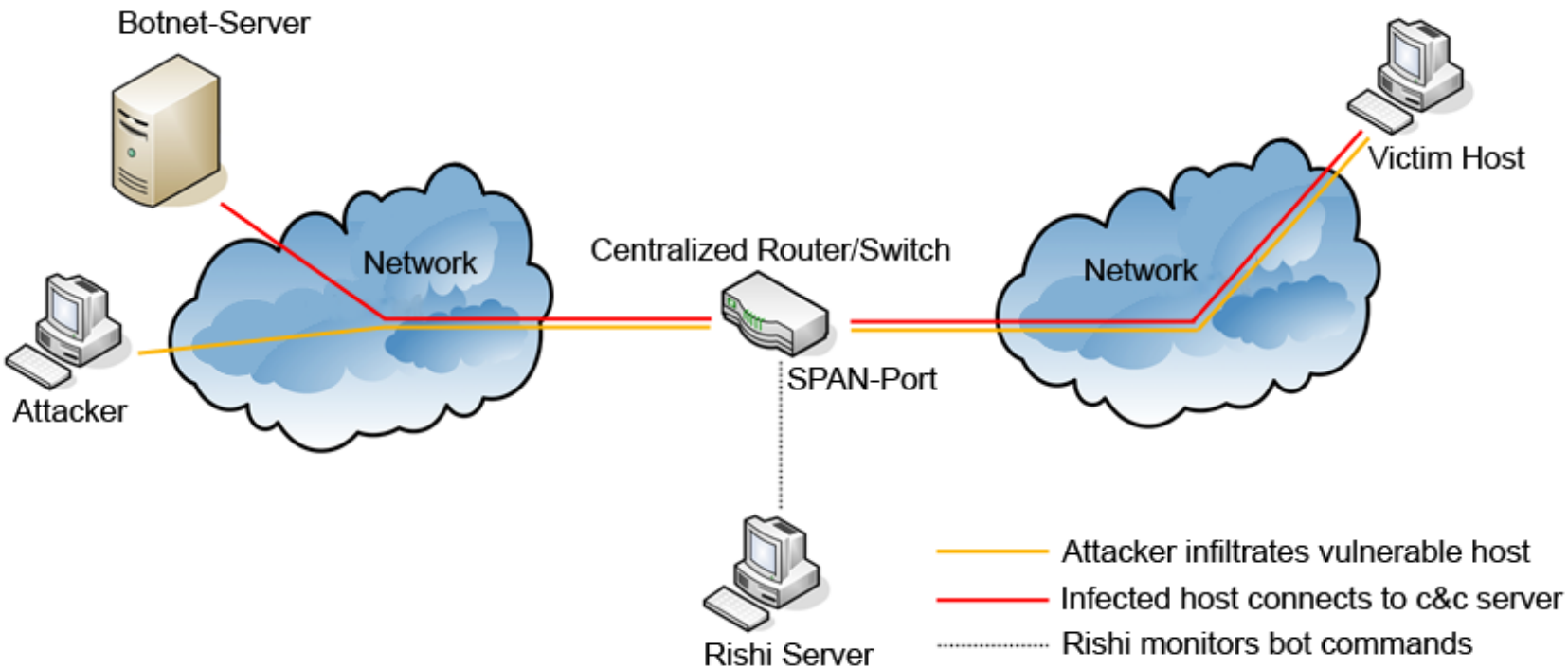
Rishi im Netzwerk

Aufbau

- Rechner an einem zentralen SPAN Port
- Passives mitlesen des Netzwerkverkehrs
- Sammeln von Payload mit IRC Protokoll Schlüsselworten (ngrep)
- Analysieren der Daten
- Extrahieren von IRC Informationen (Nickname, Channel, etc.)

Rishi im Netzwerk

Aufbau



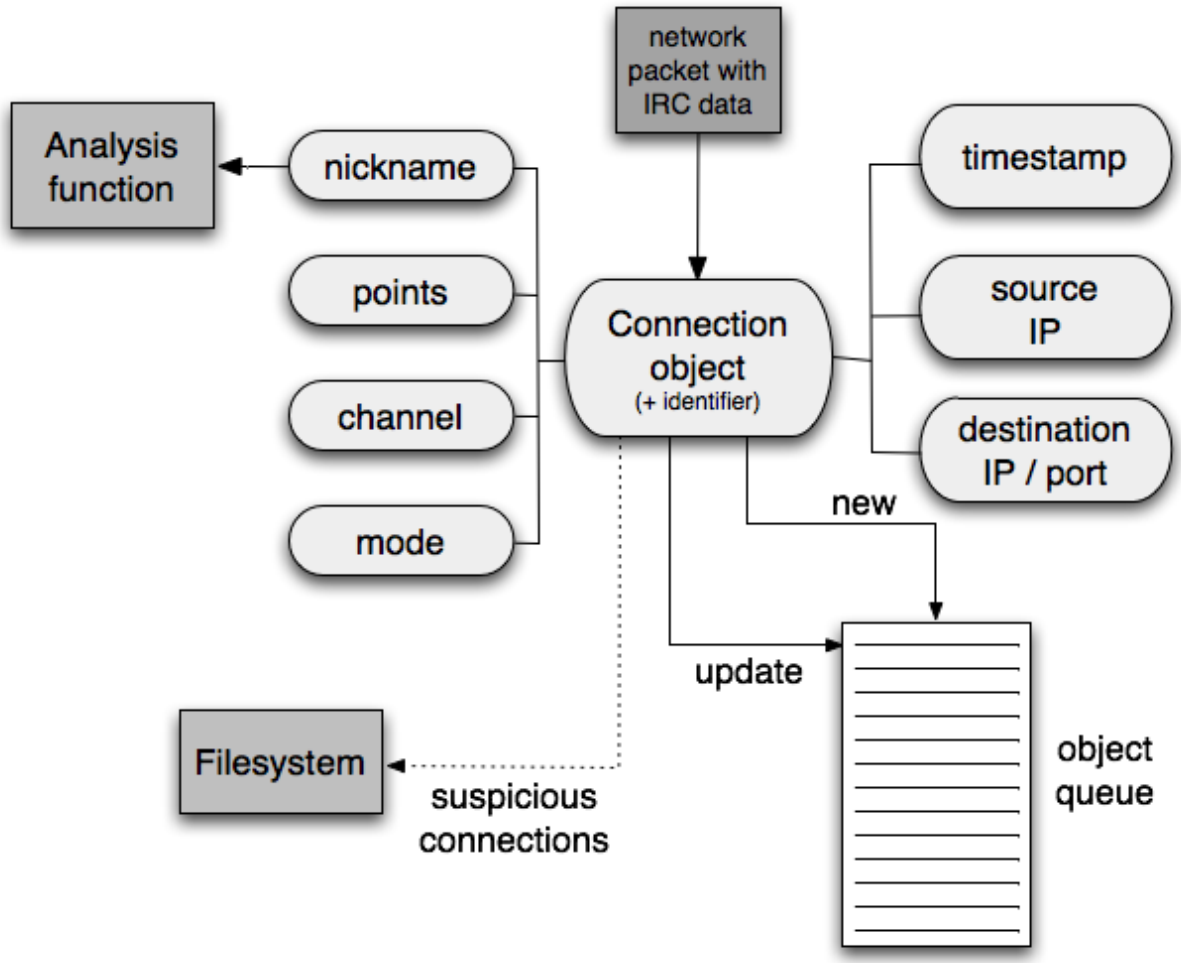
Rishi im Netzwerk

Funktionsweise

- Rishi ist Thread-basiert
- Ein Thread (Collector) sammelt ausschliesslich Netzwerkpakete mit Hilfe von ngrep (Vorfilterung)
- Passende Pakete kommen in eine Queue
- 3 Threads (Worker) analysieren die Paketinhalte

Rishi im Netzwerk

Funktionsweise



Rishi im Netzwerk

Log Ausgabe

- bots.log

2008-01-26 22:23:47,424 INFO
2008/01/26 22:23:47 Identifier: xxxxxx194126174x POSSIBLE BOT DETECTED !!!
srcIP: 134.130.xxx.xxx srcPort: 1026 dstIP: 194.126.174.116 dstPort: 3306
Nick: FQ[DEU-0H-vdobbhjbl Value: 41
Channel: ['#.nigger0']
User: ['heh heh heh :kakap']
Parameter: []
Old Nicknames: []
Analysis Function: 'uncomPort': 1, 'susString': 1, 'blacksimi': 'FQ[DEU-0H-vdobbhjbl', 'whitenick': 0, 'hostblack': 0, 'blacknick': 1, 'botChan': 0, 'onlydigit': 0, 'whitesimi': 0, 'srvblackl': 0, 'whiteregx': 0, 'dynblsimi': 0, 'somedigit': 0, 'susBeginn': 0, 'susEnding': 0, 'regxmatch': 'exp76', 'susCharac': 1

Rishi im Netzwerk

Webinterface Overview

08.11.2007 19:22:15	134.[redacted]	64.86.133.15	83	[M00|ESP|521005088]	58	details	Wohnheim
08.11.2007 19:22:11	137.[redacted]	67.202.25.195	6668	None	0	details	Wohnheim
08.11.2007 19:21:56	134.[redacted]	194.124.229.58	6667	NeX88	1	details	Wohnheim
08.11.2007 19:21:50	134.[redacted]	140.211.166.3	6667	NeX88	1	details	Wohnheim
08.11.2007 19:21:49	134.[redacted]	64.86.133.15	83	VICTOR	1	details	Wohnheim
08.11.2007 19:21:18	137.[redacted]	195.124.74.154	6667	der_MaJa	1	details	Wohnheim
08.11.2007 19:20:46	134.[redacted]	64.86.133.13	83	[M00|ESP|753943859]	30	details	Wohnheim
08.11.2007 19:20:35	137.[redacted]	216.52.240.155	6667	None	0	details	022000
08.11.2007 19:18:56	137.[redacted]	206.53.56.55	6667	None	0	details	Wohnheim
08.11.2007 19:18:50	134.[redacted]	64.86.133.15	83	VICTOR	1	details	Wohnheim
08.11.2007 19:17:47	134.[redacted]	64.86.133.13	83	[M00|ESP|028079243]	30	details	Wohnheim
08.11.2007 19:16:03	134.[redacted]	72.51.18.254	7000	None	0	details	Wohnheim
08.11.2007 19:16:00	137.[redacted]	83.140.172.211	6667	:WiR	0	details	Wohnheim
08.11.2007 19:15:52	134.[redacted]	64.86.133.15	83	[M00|ESP|678597638]	30	details	Wohnheim
08.11.2007 19:15:01	137.[redacted]	194.124.229.58	6667	f|yer	1	details	Wohnheim
08.11.2007 19:14:49	134.[redacted]	64.161.255.20	6667	ToXedVirus2	0	details	022000
08.11.2007 19:14:49	134.[redacted]	64.86.133.13	83	[M00|ESP|586835787]	30	details	Wohnheim
08.11.2007 19:14:38	134.[redacted]	195.22.174.130	6667	ToXedVirus2	0	details	022000
08.11.2007 19:14:23	137.[redacted]	217.160.109.17	6667	dvgsghehj	0	details	022000
08.11.2007 19:13:55	137.[redacted]	83.140.172.212	6668	MfG_Linus	1	details	Wohnheim
08.11.2007 19:13:27	134.[redacted]	64.86.133.13	83	[M00|ESP|213685479]	30	details	Wohnheim
08.11.2007 19:13:16	134.[redacted]	64.86.133.15	83	[M00|ESP|512664464]	30	details	Wohnheim
08.11.2007 19:09:52	134.[redacted]	64.86.133.15	83	[M00|ESP|375375211]	30	details	Wohnheim
08.11.2007 19:09:32	134.[redacted]	82.96.64.4	6667	Unknown	0	details	Wohnheim
08.11.2007 19:08:49	134.[redacted]	64.86.133.13	83	[M00|ESP|843658416]	58	details	Wohnheim
08.11.2007 19:08:35	137.[redacted]	140.186.244.235	6667	None	0	details	022000
08.11.2007 19:07:27	134.[redacted]	64.86.133.13	83	[M00|ESP|969095663]	30	details	Wohnheim

Rishi im Netzwerk

Webinterface Details

Details for 134.[redacted]

Firstseen:	21.10.2007 14:18:58
Lastseen:	03.11.2007 11:09:28
IP Address:	134.[redacted]
Hostname:	[redacted]RWTH-Aachen.DE
IKZ:	none
IRC Nickname:	[00|DEU|771273]
Value:	44
Old Nickname:	None
IRC Server:	221.11.6.203 : 57
DNS Name:	221.11.6.203
Channel:	['#fucku .']
Usermode:	['XP-4071 * 0 :MICHAELMOBIL']
Additional Parameter:	['#fucku ']
Analysis Result:	{'uncomPort': 1, 'susString': 1, 'blacksimi': '[00|DEU|771273]', 'whitenick': 0, 'hostblack': 0, 'blacknick': 1, 'botChan': 0, 'whitesimi': 0, 'srvblackl': 0, 'onlydigit': 0, 'dynblsimi': 0, 'somedigit': 1, 'susBeginn': 0, 'susEnding': 0, 'regxmatch': 'exp43', 'susCharac': 1}
Point Distribution:	Nick on Blacklist: Set to 10 Points Similar to Blacklist: +1 Point for each similar charackter Uncommon Port: +1 Point Suspicious Strings: +1 Point each Suspicious Charackters: +1 Point each Every Two Digits: +1 Point Match Regular Expression: +10 Points
DNS Replication:	221.11.6.203
Alive Test:	Server is running
Write eMail:	VPN/DialUP Rechner
Mark: [automatic]	is Bot / no Bot

back

Rishi im Netzwerk

Ergänzung

- Rishi läuft seit Ende 2006 an der RWTH Aachen, seit Anfang 2007 am Georgia Institute of Technology und seit Anfang/Mitte 2007 an der Universität Karlsruhe
- Hilfreiches Feedback, insbesondere von Björn Weiland (Karlsruhe)
- Es gibt einen Regelsatz zur Integration von Rishi mit dem IDS Prelude
- `https://trac.prelude-ids.org/attachment/ticket/246/rishi.rules`

Inhalt

Einschränkungen

Netzwerkverkehr

- An der RWTH lauscht Rishi an einem 10GBit SPAN Port
- Das Netzwerkinterface ist mehr als überlastet
- RX packets:3237373912 errors:712274218 dropped:712184466 overruns:712184466
- Durch Paketverlust gehen auch Informationen über infizierte Rechner verloren
- Ein Bot verbindet sich aber durchaus öfters, so dass wir ihn in der Regel doch erwischen
- Lösung: verteiltes Setup mit Logging in eine gemeinsamme MySQL Datenbank

Einschränkungen

IRC Protokoll

- Rishi funktioniert nur solange wie die IRC Schlüsselworte sich nicht ändern
  - SENDN NTH-6993
  - SENDU NTH-6993 * 0 :NTH-6993
  - JOIN #netthrottle bob
  - SENDM #netthrottle :[Exploit Scanner] DCOM135: Exploited IP: 134.130.xxx.xxx OS: 2
- Aufgefallen durch join ohne Nicknamen und User

Einschränkungen

Nicknamen

- Nicknamen die aus echten Personennamen bestehen (Zapchast.AU)
  - Liste mit 32.000 Nicknamen
  - Robert, larisa_18, yoshiaki, ...
  - komischerweise auch sowas: botnet
  - Fällt nur auf wenn der Rechner eigentlich kein IRC machen sollte: Wiki-Server/Sekretärin
- Willkürliche Buchstabenkombinationen
  - QmfuyKXM, nwPDnNnn, eYQyuKNr
  - Hier hilft das menschliche Auge (Webinterface)
  - Fallen meist durch ungewöhnliche Serverports auf

Einschränkungen

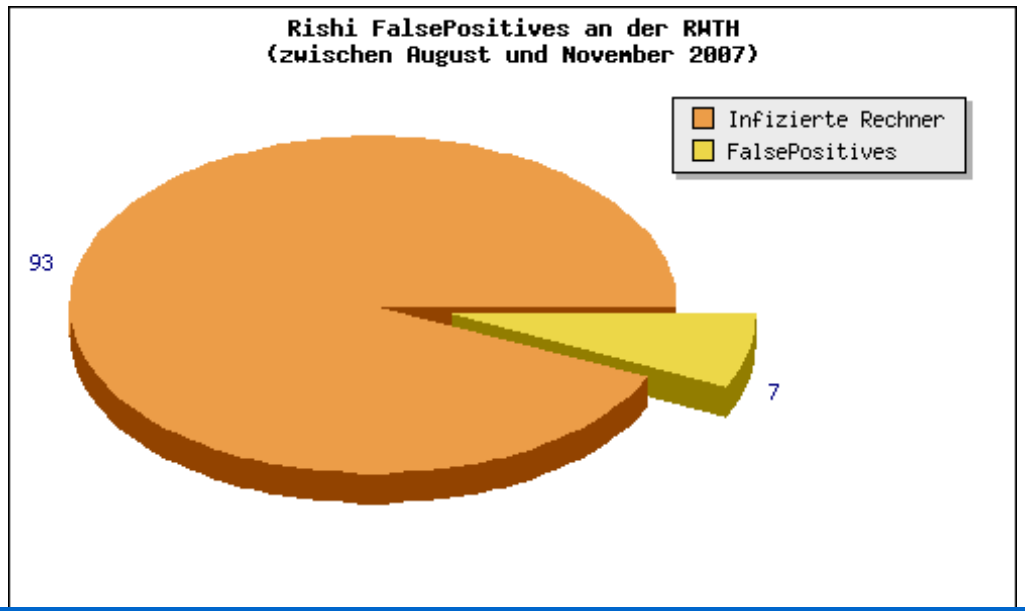
Nicknamen

23.11.2007 06:07:02	137.[redacted]	84.33.1.236	6667	jipjvf	0
23.11.2007 06:07:01	137.[redacted]	67.43.236.69	5190	KFmSVGtz	1
23.11.2007 06:07:01	137.[redacted]	66.252.13.195	1728	[AUT]00|XP|SP2|L|2199	40
23.11.2007 06:07:01	137.[redacted]	72.10.166.178	1863	iecxIvEv	1
23.11.2007 06:07:01	137.[redacted]	67.43.236.68	1863	UcYjhqvB	1
23.11.2007 06:07:01	137.[redacted]	209.205.196.11	80	[P00|AUT|73442536]	67
23.11.2007 06:07:01	137.[redacted]	67.43.232.38	10324	tZLJsqit	1
23.11.2007 06:07:01	137.[redacted]	66.252.13.250	1728	][l4m3r][gqaowo	40
23.11.2007 06:07:01	137.[redacted]	67.43.236.66	5190	KDTAqzzp	28
23.11.2007 06:07:01	137.[redacted]	193.77.90.253	3159	AUT|XP|SP2|923696	43
23.11.2007 06:07:01	137.[redacted]	124.2.130.194	3921	[XP]|1975606643	43
23.11.2007 06:06:59	137.[redacted]	67.43.236.98	2293	StNtVVWR	1
23.11.2007 06:06:59	137.[redacted]	83.149.86.193	7175	awk-7262056	4

Inhalt

Ergebnisse

- Rishi läuft an der RWTH Aachen seit Ende 2006
- Im Schnitt entdecken wir 1-3 infizierte Rechner pro Woche
- Inzwischen fester Bestandteil bei der Identifizierung von infizierten Rechnern
- Im Zeitraum August bis November 2007 wurden 100 Rechner als infiziert erkannt (7 FalsePositive)



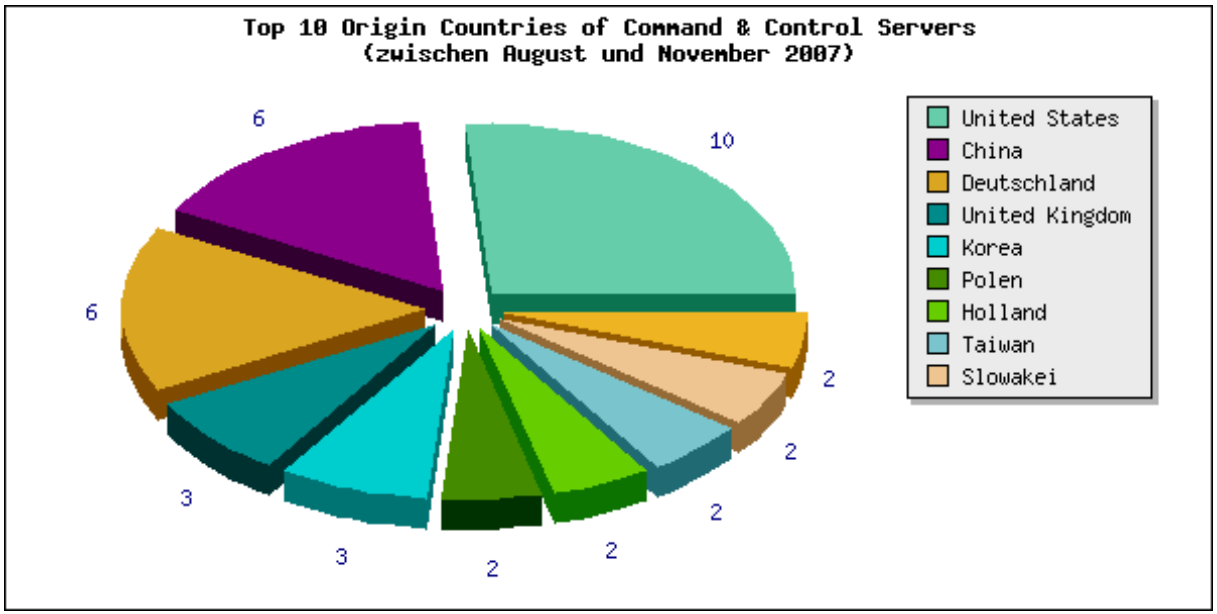
Ergebnisse

FalsePositives

- asikoreczka|000000
- S000000000000??40783624570
- ustreamer|4595
- 000000
- h1234
- b3450497
- o5175

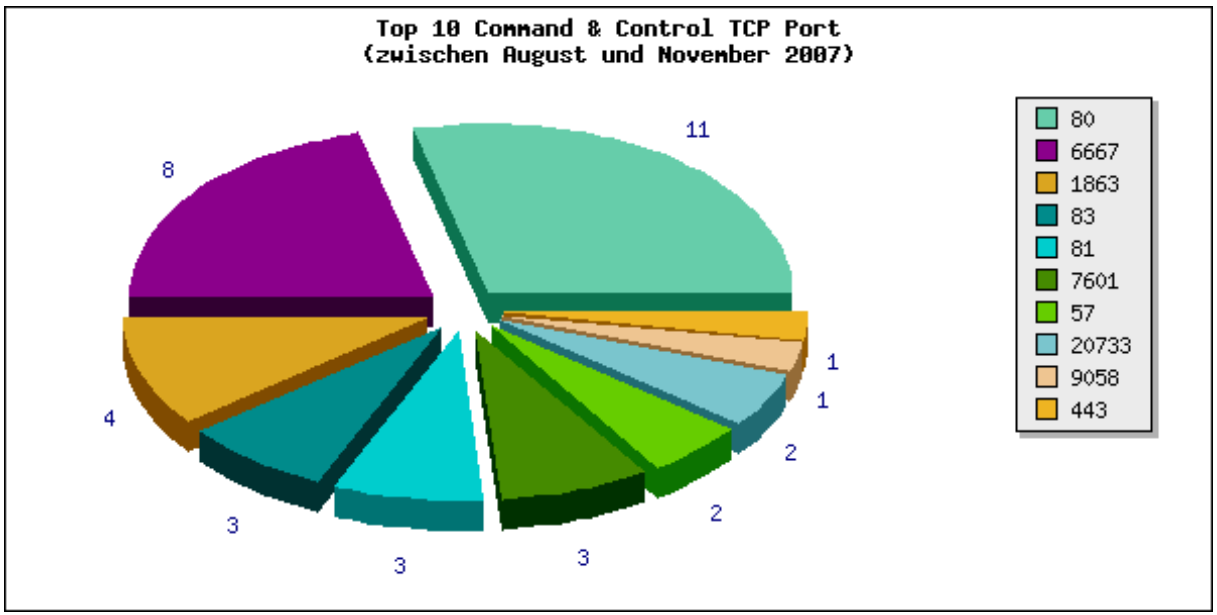
Ergebnisse

- Verteilung der Command & Control Server



Ergebnisse

- Command & Control Server Ports



Ergebnisse

- Erkennung von Bots die sich nicht durch auffällige Mechanismen verbreiten wie PortScans
- z.B. durch Drive-By Downloads oder wie derzeit sehr aktiv durch Microsoft Messenger
- Die Botnetz-Informationen sind sehr Hilfreich um neue Binaries zu gewinnen (siehe BotSpy)

File **pdf.pdf.exe** received on **11.09.2007 17:04:44 (CET)**
Current status: **finished**
Result: **1/32 (3.13%)**

Compact Print results

Antivirus	Version	Last Update	Result
AhnLab-V3	2007.11.9.1	2007.11.09	-
AntiVir	7.6.0.34	2007.11.09	-
Authentium	4.93.8	2007.11.09	-
Avast	4.7.1074.0	2007.11.08	-
AVG	7.5.0.503	2007.11.09	-
BitDefender	7.2	2007.11.09	BehavesLike:Win32.Malware

Inhalt

Zusammenfassung

- Rishi ist ein recht simples aber effektives Tool um IRC Bot infizierte Rechner zu entdecken
  - basiert auf der Auswertung von Nicknames
  - verwendet ein flexibles Punktesystem
  - Erweiterbar durch eigene reguläre Ausdrücke (Update Funktion)
- Es fehlt noch ein Automatismus, vielleicht mit Prelude IDS möglich
- Rishi ist OpenSource (http://zero.ram.rwth-aachen.de/rishi/)

Vielen Dank für Ihre Aufmerksamkeit
Fragen ???