Detection of peer-to-peer botnets

Matthew Steggink, Igor Idziejczak

February 6, 2008

Introduction & theory

Research question

Peacomm case study

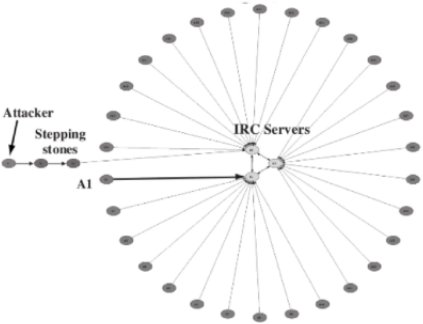
Detection

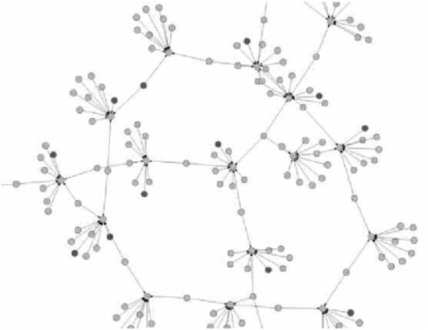
Conclusion & future work

Peer-to-peer botnets

- What are botnets . . . and peer-to-peer botnets?
- What's the purpose of bots and botnets?

Botnet topology





Research question?

in cooperation with SURFnet

Detection of peer-to-peer botnets

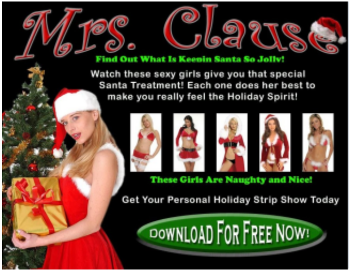
- Why this research
- Goal of this research
- Previous work . . .

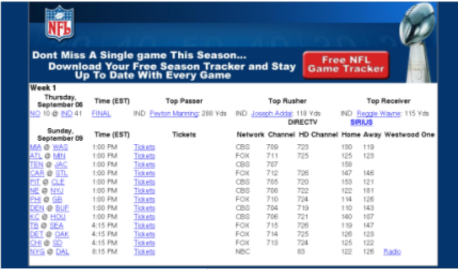
Peacomm

Peacomm

- What is Peacomm
- DHT: Usage of the Overnet protocol

How do users get infected?


Mrs. Clause
Find Out What Is Keepin Santa So Jolly!
Watch these sexy girls give you that special Santa Treatment! Each one does her best to make you really feel the Holiday Spirit!
These Girls Are Naughty and Nice!
Get Your Personal Holiday Strip Show Today
DOWNLOAD FOR FREE NOW!



Dont Miss A Single game This Season...
Download Your Free Season Tracker and Stay Up To Date With Every Game

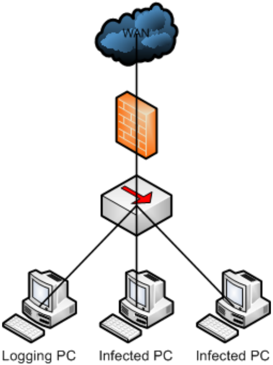
Week 1

Thursday, September 06	Time (EST)	Top Passer	Top Rusher	Top Receiver
NO 10 @ IND 41	FINAL	IND Peyton Manning: 288 Yds	IND Joseph Addai: 118 Yds	IND Reggie Wayne: 115 Yds

				DIRECTV		SIRIUS		
Sunday, September 09	**Time (EST)**	**Tickets**	**Network**	**Channel**	**HD Channel**	**Home**	**Away**	**Westwood One**
MIA @ WAS	1:00 PM	Tickets	CBS	709	723	130	119	
ATL @ MIN	1:00 PM	Tickets	FOX	711	725	125	123	
TEN @ JAC	1:00 PM	Tickets	CBS	707		158		
CAR @ STL	1:00 PM	Tickets	FOX	712	726	147	146	
PIT @ CLE	1:00 PM	Tickets	CBS	705	720	153	121	
NE @ NYJ	1:00 PM	Tickets	CBS	708	722	122	181	
PHI @ GB	1:00 PM	Tickets	FOX	710	724	114	126	
DEN @ BUF	1:00 PM	Tickets	CBS	704	719	110	143	
KC @ HOU	1:00 PM	Tickets	CBS	706	721	140	107	
TB @ SEA	4:15 PM	Tickets	FOX	715	726	119	147	
DET @ OAK	4:15 PM	Tickets	FOX	714	725	126	123	
CHI @ SD	4:15 PM	Tickets	FOX	713	724	125	122	
NYG @ DAL	8:15 PM	Tickets	NBC		83	122	126	Radio

Peacomm experimental setup

- Peer to peer botnet study
- Test environment
- Experimenting (CW Sandbox, PerilEyez, Rootkit Unhooker, Wireshark)



Infection

- Executable copy (noskrnl.exe)
- Time configuration
- Initial peer list (noskrnl.config)
- Creates a rule in the Windows Firewall
- Rootkit noskrnl.sys

Secondary injections

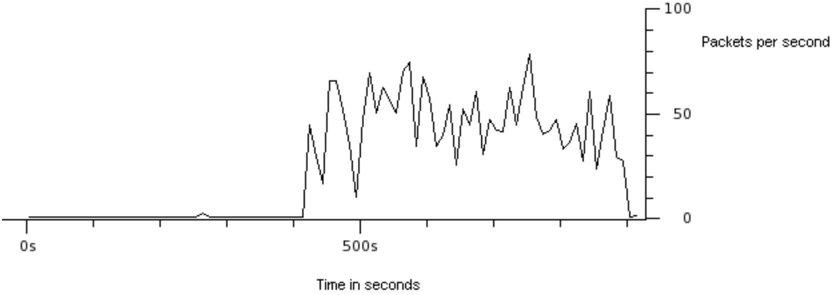
- Duplicate on the desktop
- Update malware through TCP connection
- Updates peer list and downloads spam message

Network analysis

UDP

- Very noisy: 55 %
- Always same high numbered port (different on every host)
- Packet length (40-79): 98 %, in total: 51 %

Network analysis
SMTP

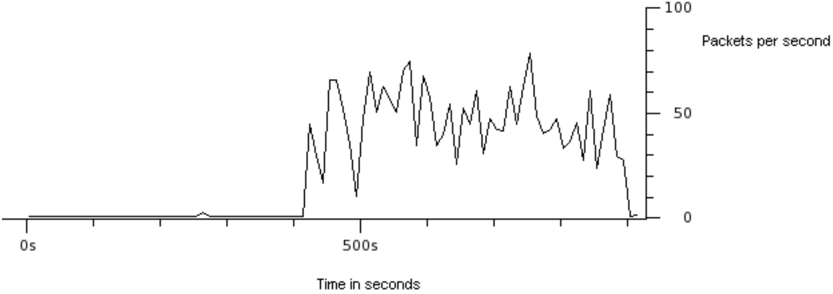


- 5 % of total traffic → < 0,5% [1]
- 33 packets / second

📄 ipoque.com, *Internet Study 2007*, August - September 2007

Network analysis

MX queries



- 1 % of total traffic
- 4 packets / second → isolated case?
- Host MX queries are suspicious

Detection

- Protocol traffic
- SMTP
- MX queries
- Connection

Detection

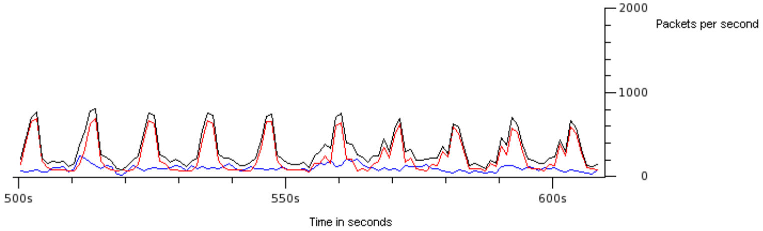


Figure: Comparison between all traffic (black), Peacomm traffic (red) and other traffic (blue) (generated with Wireshark)

Conclusion & future work

- Unique characteristics
- Hard to predict the future?
- Future Peacomm developments: less noisy, what now?
- New bots in the future: Agobot?

Questions?

- Matthew Steggink: matthew.steggink@os3.nl
- Igor Idziejczak: igor.idziejczak@os3.nl