Understanding Large-Scale Spamming Botnets From Internet Edge Sites

Tatsuya Mori, Holly Lovely, Aditya Akella, Akihiro Shimoda, Shigeki Goto
NTT, University of Wisconsin-Madison, Waseda University

Goal

Better understanding of the large-scale spamming botnets from both global and local view points

Approach

- Leverage TCP fingerprint technique
- Correlate SMTP logs and tcpdump traces collected at multiple vantage points

Contributions

1.We extract new variants of TCP fingerprint of the Srizbi bot

2.We evaluate the effectiveness of the C&C (McColo) shut down from Internet edge-sites

3.We reveal the long-term growth and transition of the botnet

Lessons learned

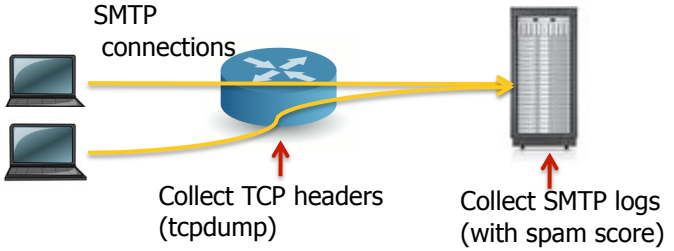
- Temporal but significant effectiveness of C&C attack at Internet edge sites.
- Rapid response (version transition) of spamming botnet operation
- Differences of spam contribution from botnet among receiver domains

→ need for global correlation / localization

Data sets

SMTP logs collected at 3 vantage points
TCPDUMP traces collected at 4 vantage points

	tcpdump	SMTP log
UW	Feb 9, 2008 – Jul 11, 2008	Feb 1, 2008 – Apr 30, 2008
CORP	Apr 7, 2008 – Jul 31, 2008 Dec 26, 2008 – Dec 31, 2009	Apr 7, 2008 – Jul 31, 2008 Jan 1, 2009 – Dec 31, 2009
GEM	–	Aug 1, 2008 – Apr 30, 2009
WAS	Oct 16–22, 2008, Mar 7–16, 2009	–
MAWI	Jul 1, 2007 – Nov 31, 2009	–



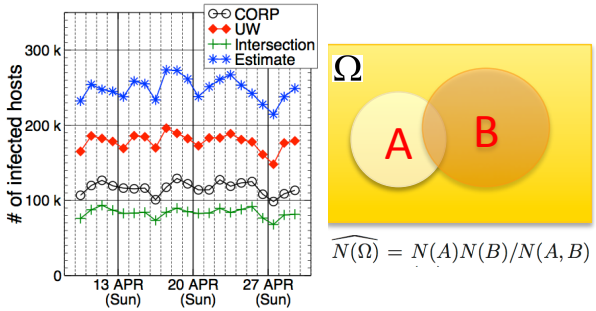
The known and newly extracted TCP fingerprints for Srizbi botnet

Signature	#spam	#ham	#senders
[24000:128:0:44:M536:.]	14,495,869	2,708	260,955
[24000:128:0:44:M51360:.]	262,077	21	3,147
[24000:128:0:44:M528:.]	223,246	3	2,662
[24000:128:0:44:M1452:.]	56,589	9	774
[24000:128:0:44:M1414:.]	20,504	7	251

Effectiveness of C&C Shutdown (2008/11)

data set	#total spam	Srizbi (%)	Windows (%)
Before shutdown			
UW Feb 2008	110,959,667	12,602,852 (11%)	83,333,645 (61%)
UW Mar 2008	136,572,281	17,813,844 (13%)	101,094,771 (74%)
UW Apr 2008	101,131,663	15,185,849 (15%)	71,106,454 (70%)
CORP Apr 2008	20,107,288	7,530,864 (37%)	11,220,937 (56%)
CORP May 2008	25,079,293	10,694,254 (43%)	13,286,069 (53%)
CORP Jun 2008	25,088,872	11,349,148 (45%)	12,707,436 (51%)
CORP Jul 2008	17,562,162	5,434,277 (30%)	10,682,847 (60%)
After shutdown			
CORP Jan 2009	10,886,153	607,499 (6%)	9,487,679 (87%)
CORP Feb 2009	11,604,039	951,914 (8%)	9,849,693 (85%)
CORP Mar 2009	13,545,628	246,862 (2%)	12,211,121 (90%)

Size estimation of botnets with "mark and recapture" method



Long-term trends