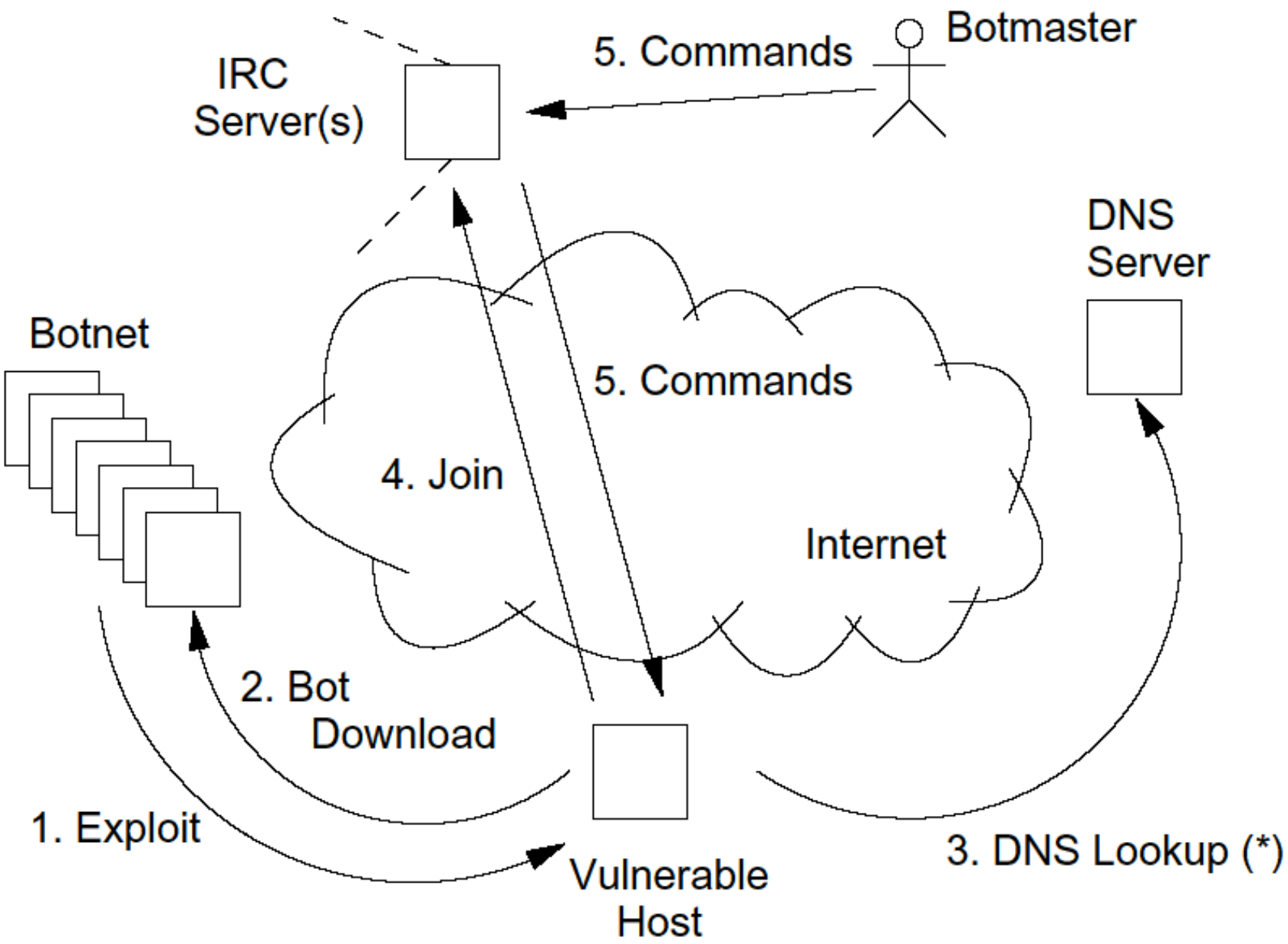
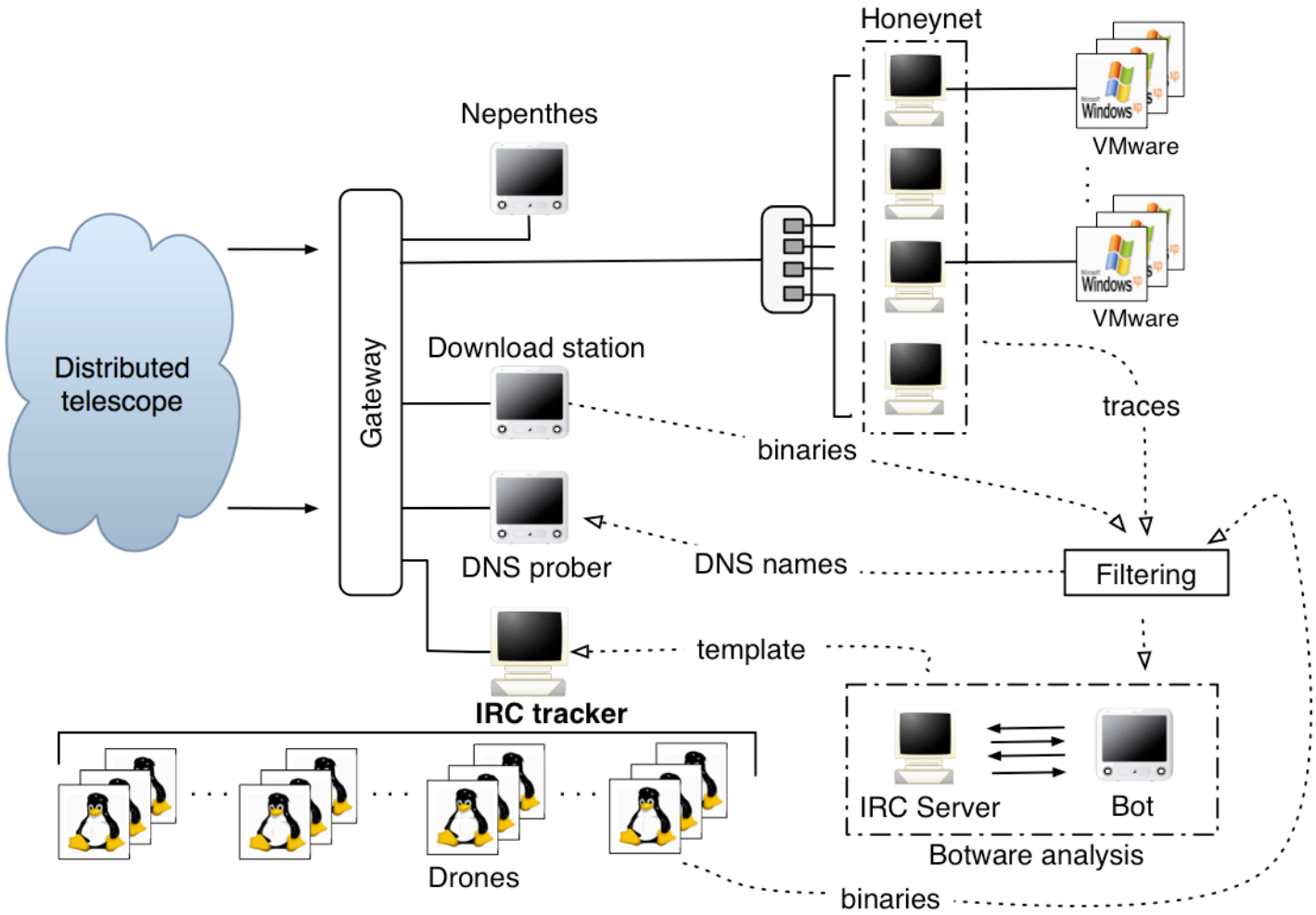

IRC
Server(s)
5. Commands
Botmaster
DNS
Server
Botnet
5. Commands
4. Join
Internet
2. Bot
Download
1. Exploit
Vulnerable
Host
3. DNS Lookup (*)


Honeynet
Nepenthes
VMware
VMware
Distributed telescope
Gateway
Download station
traces
binaries
DNS prober
DNS names
Filtering
template
IRC tracker
IRC Server
Bot
Botware analysis
Drones
binaries

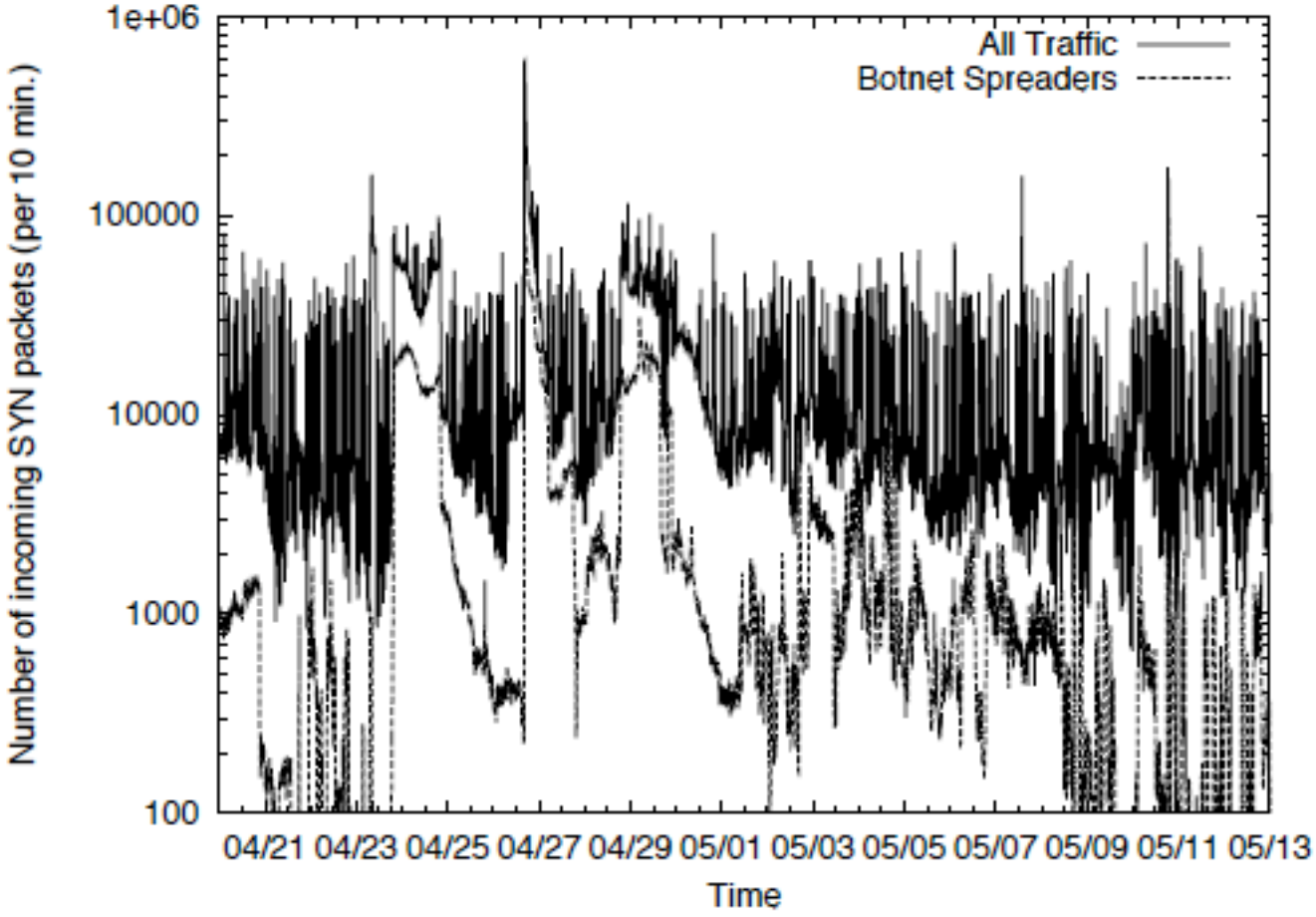


Figure 4: Time series of incoming SYN packets to the darknet.

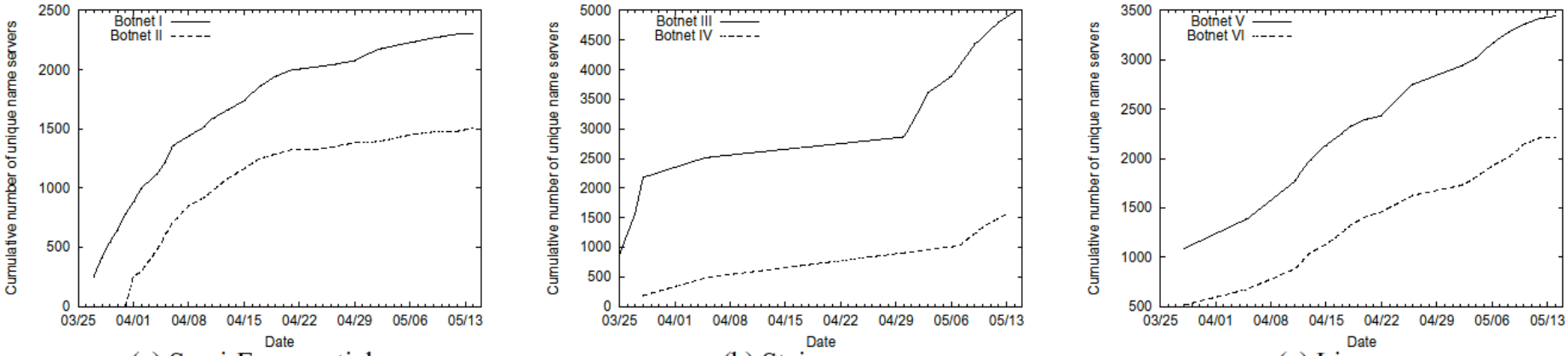
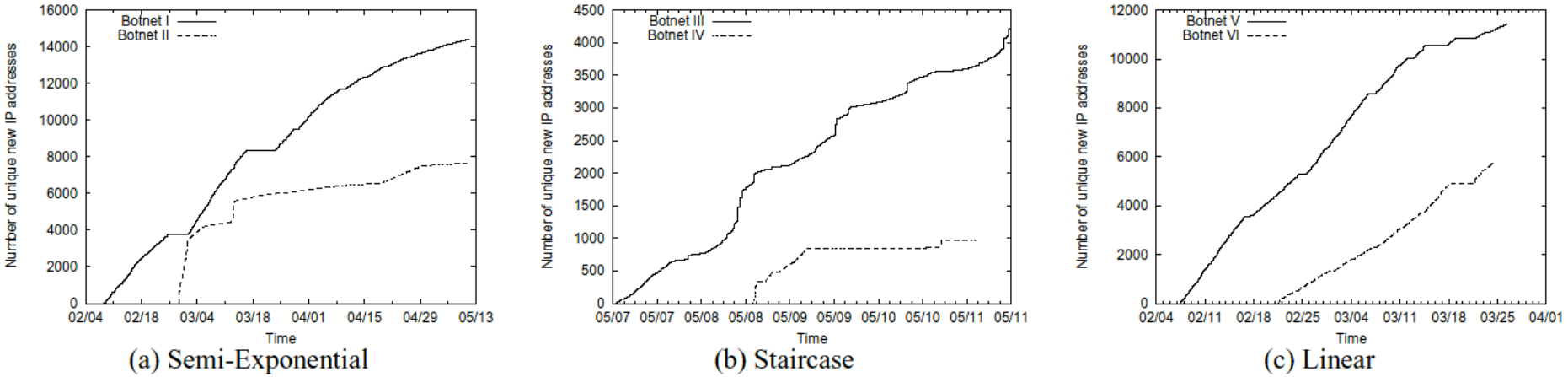


Figure 7: DNS views showing examples from multiple botnets with the three predominant growth patterns.



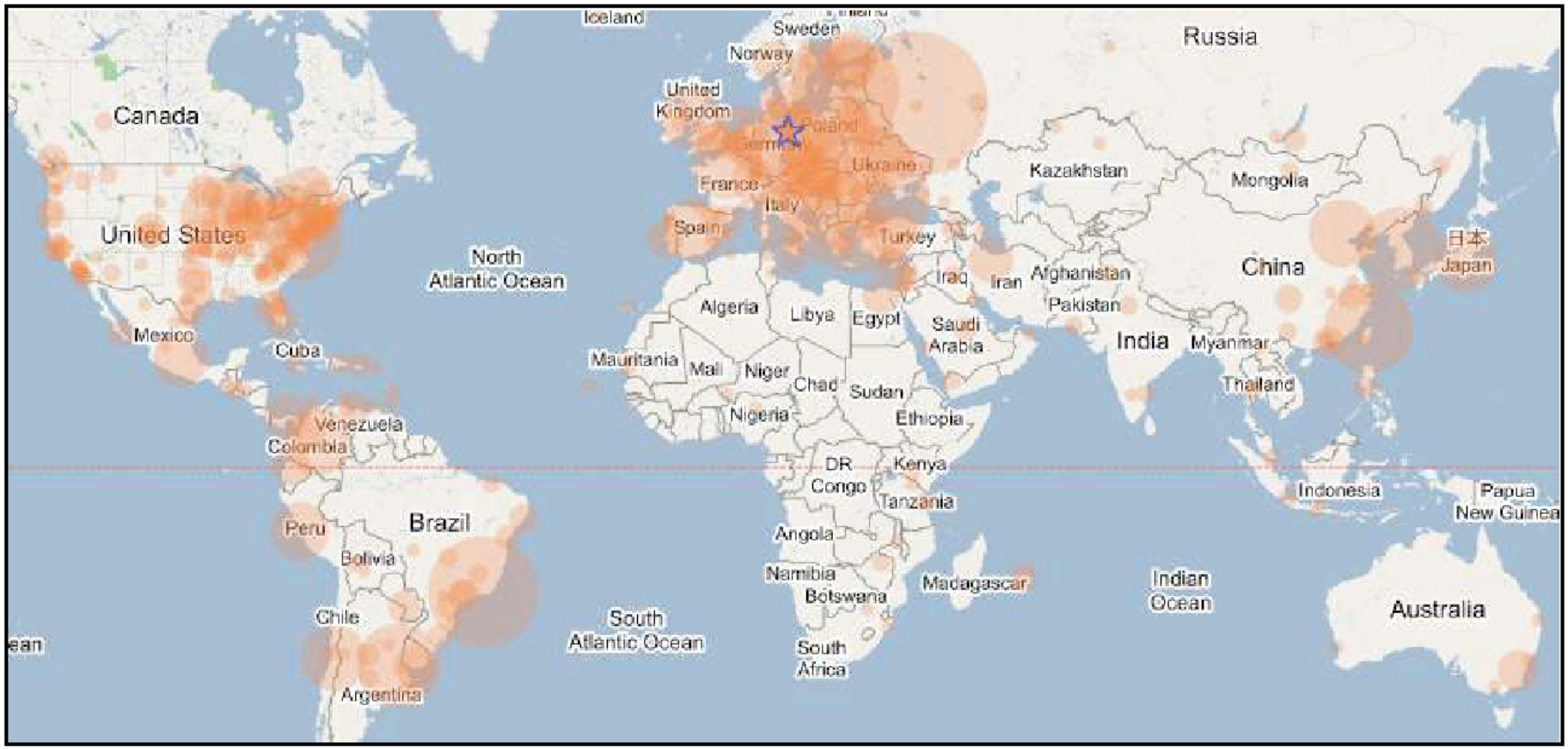


Figure 6: Geographic location of the DNS cache hits for one of the tracked botnets. The star indicates the location of the IRC server.

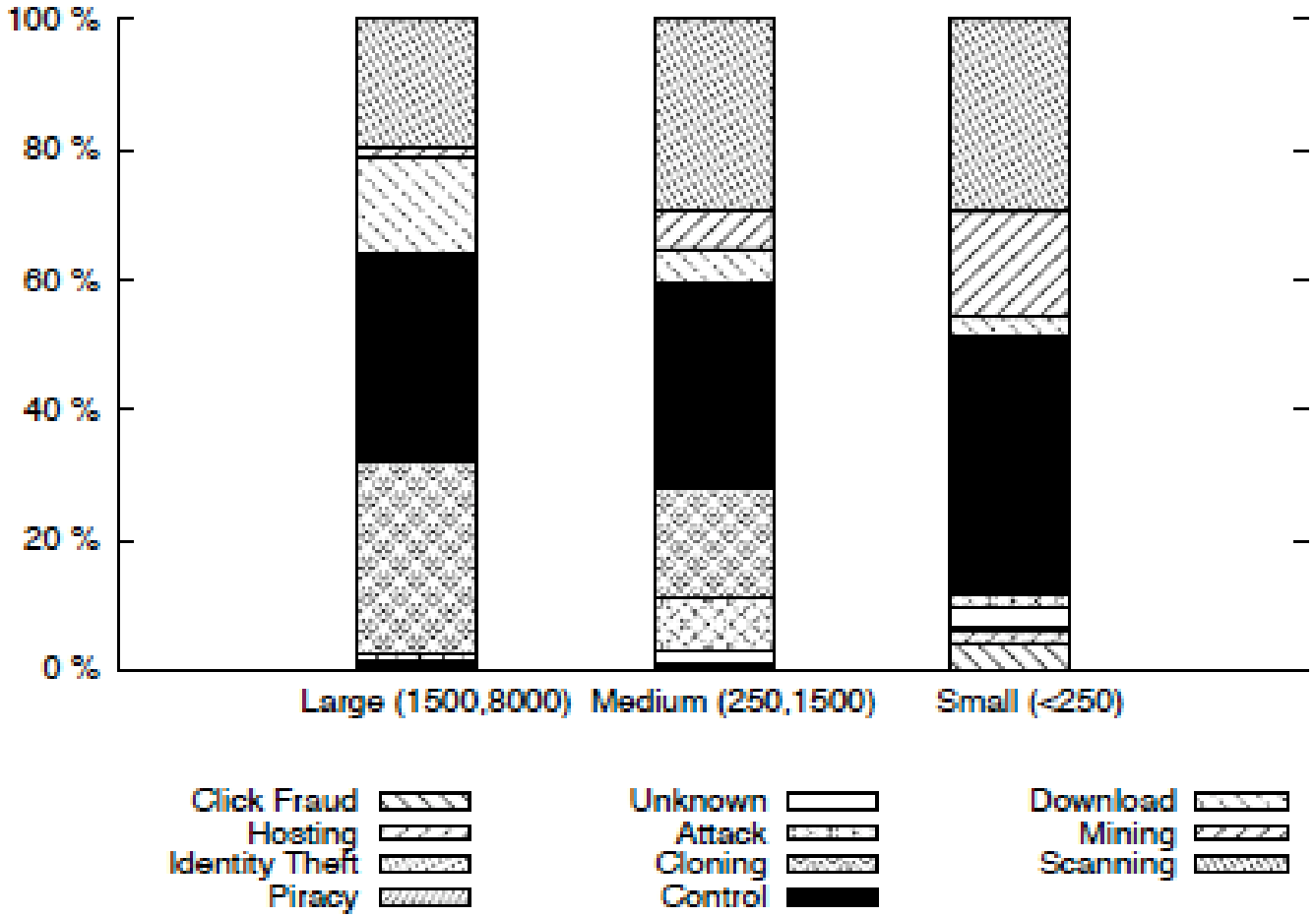


Figure 13: Percentage of command types as a function of observed botnet size.


AwesomePostcard.Com
http://
Google
AWESOMEPOSTCARDS
http://www.awesomepostcards.com
Your download will start in 5 seconds.
If your download does not start, click here
©2000-2008 AwesomePostCard.com - All rights reserved.
Done

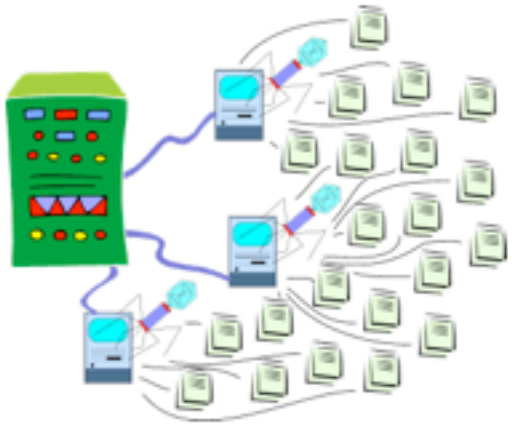
September 6th, 2007

Storm Worm botnet could be world's most powerful supercomputer

Posted by Ryan Naraine @ 8:41 am

Categories: Botnets, Browsers, Data theft, Exploit code, Firefox.....

Tags: Operation, Supercomputer, Malware, Worm, Ryan Naraine



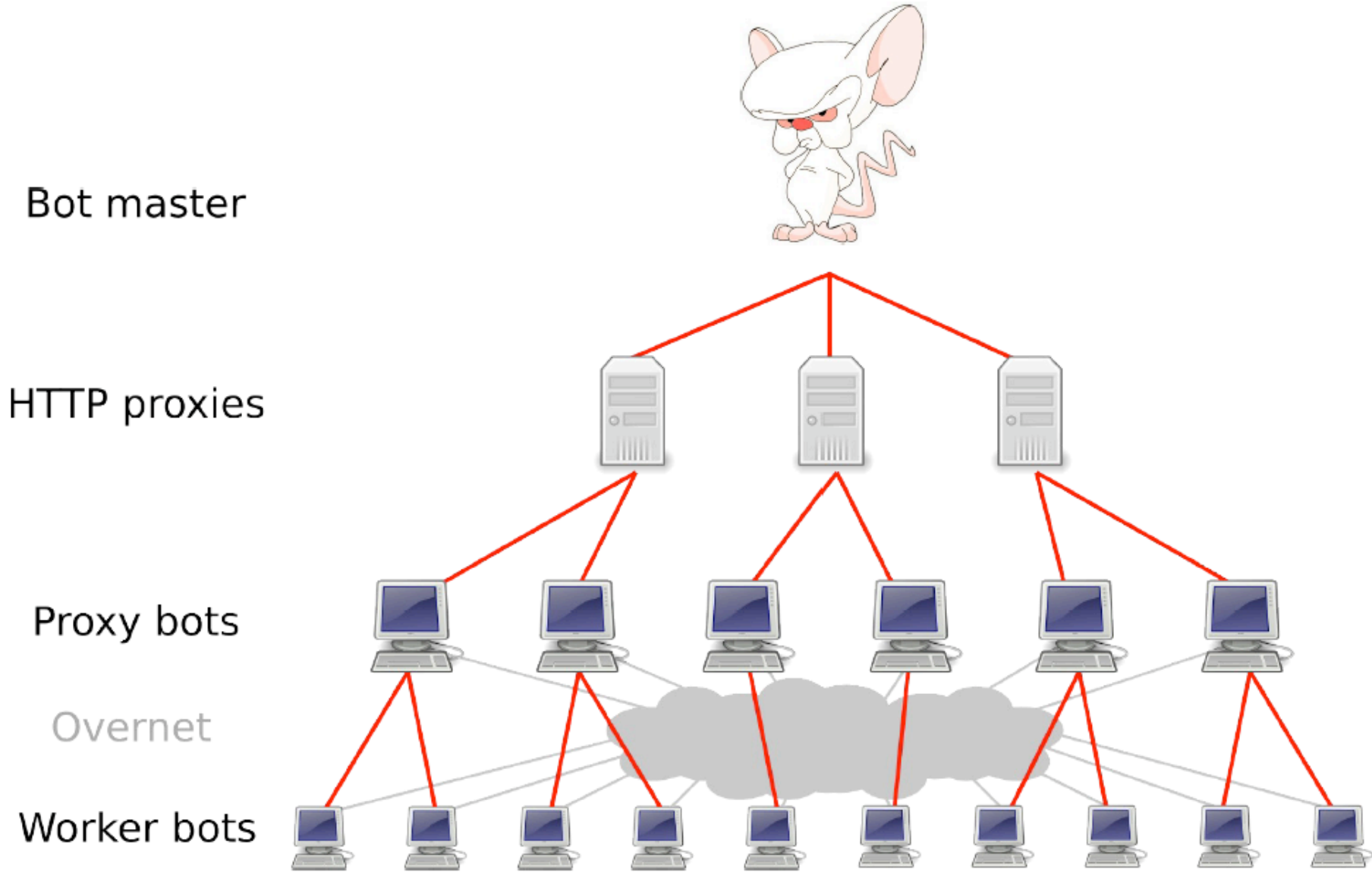
Nearly nine months after it was first discovered, the Storm Worm Trojan continues to surge, building what experts believe could be the world's most powerful supercomputer.

The Trojan, which uses a myriad of social engineering lures to trick Windows users into downloading malware, has successfully seeded a massive botnet — between one million and 10 million CPUs — producing computing power to rival the world's top 10 supercomputers

> *The [Storm] botnet reportedly is powerful enough as of September 2007 to force entire countries off the Internet, and is estimated to be capable of executing more instructions per second than some of the world's top supercomputers. However, it is not a completely accurate comparison, according to security analyst James Turner, who said that comparing a botnet to a supercomputer is like comparing an army of snipers to a nuclear weapon*

If that made you catch your breath a bit, read on...

> *At certain points in time, the Storm worm used to spread the botnet has attempted to release hundreds or thousands of versions of itself onto the Internet, in a concentrated attempt to overwhelm the defenses of anti-virus and malware security firms. According to Joshua Corman, an IBM security researcher, "This is the first time that I can remember ever seeing researchers who were actually afraid of investigating an exploit."*


Bot master
HTTP proxies
Proxy bots
Overnet
Worker bots

(PRNG). Storm generates OIDs using its own PRNG given by the recurrence:

$$I_{i+1} = (a \cdot I_i + b \bmod 2^{32}) \bmod m$$

with $a = 1664525$, $b = 1013904223$, $m = 32767$, and the initial value I_0 is based on the system clock. The generator appears to be based on a well-known linear congruential PRNG described in the *Numerical Recipes*

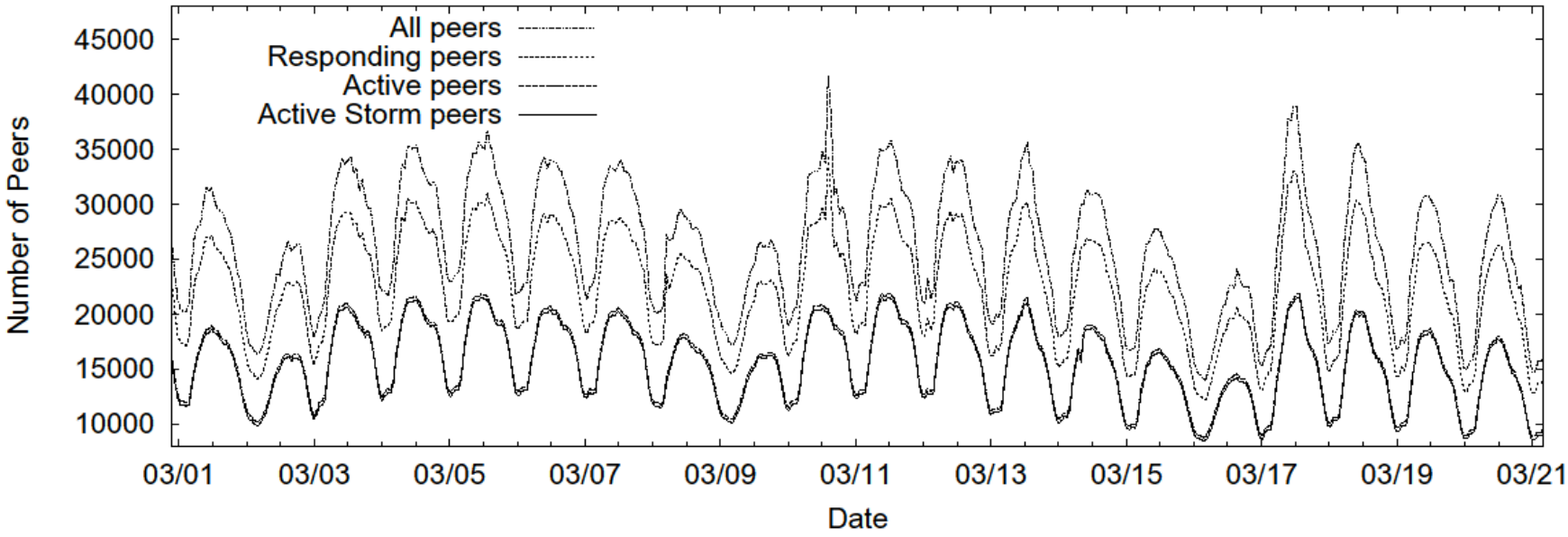
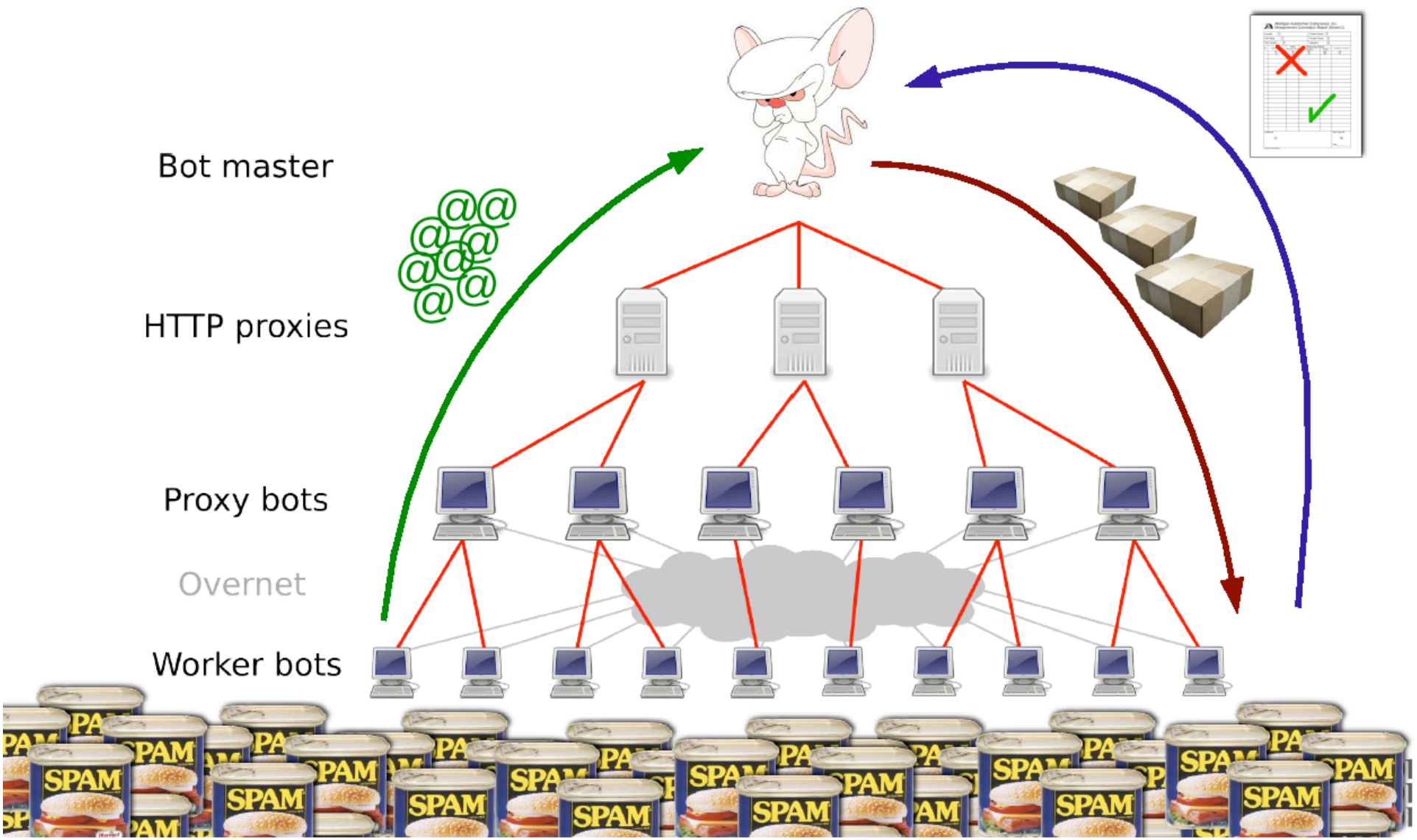


Figure 2: Estimates of the size of the Storm botnet using different notions of liveness over the first three weeks of March 2008 Note that the y-axis does not begin at zero to better separate the curves.

Location	Hallmarks
Germany	Random OIDs with lower 10 bytes constant. Floods the Storm network aggressively with thousands of fake node IPs.
Iran	Random OIDs biased to upper half of space (first bit always set).
Sweden	Random OIDs biased to upper half of space (first bit always set). Does not appear in routing tables of any other peers.
France	One fixed OID, relatively passive crawler, appears to just be sampling Storm.
East Coast, US	257 OIDs evenly distributed in ID space behind one IP, port number used as upper two bytes of the OID.
East Coast, US	Uniform random OIDs, both a Storm implementation and crawler behind the same IP, does not report other peers.
West Coast, US	Random OIDs biased to upper half of space 100:1. Does not report IPs in response to queries.

Table 2: Other parties participating in the "encrypted" Storm network on April 4, 2008.


Bot master
HTTP proxies
Proxy bots
Overnet
Worker bots
SPAM