Tumbling Down the Rabbit Hole:

Exploring the Idiosyncrasies of Botmaster Systems in a Multi-Tier Botnet Infrastructure

Chris Nunnery
Greg Sinclair
Brent ByungHoon Kang
[University of North Carolina at Charlotte]

Our Work

- Forensic investigation of botmaster components
- Interpreting functionality and management using network traces and file-system artifacts
  - Obtained through ISP cooperation

Purpose

- Refine notions of how advanced botnets are deployed and managed
- Reveal mechanisms and techniques to perform malicious activities
- Expose the systems in the highest tiers, providing a complete view of Waledac's infrastructure

Overview

- Context
- Topology
- Components and Deployment
- Activities, Operations, and Management

Context

- Waledac: a successor to Storm
- Emerged mid-2008
- Multi-tier architecture, single-tier peering
- Leveraged for *spamming*, *data harvesting*, and *phishing*

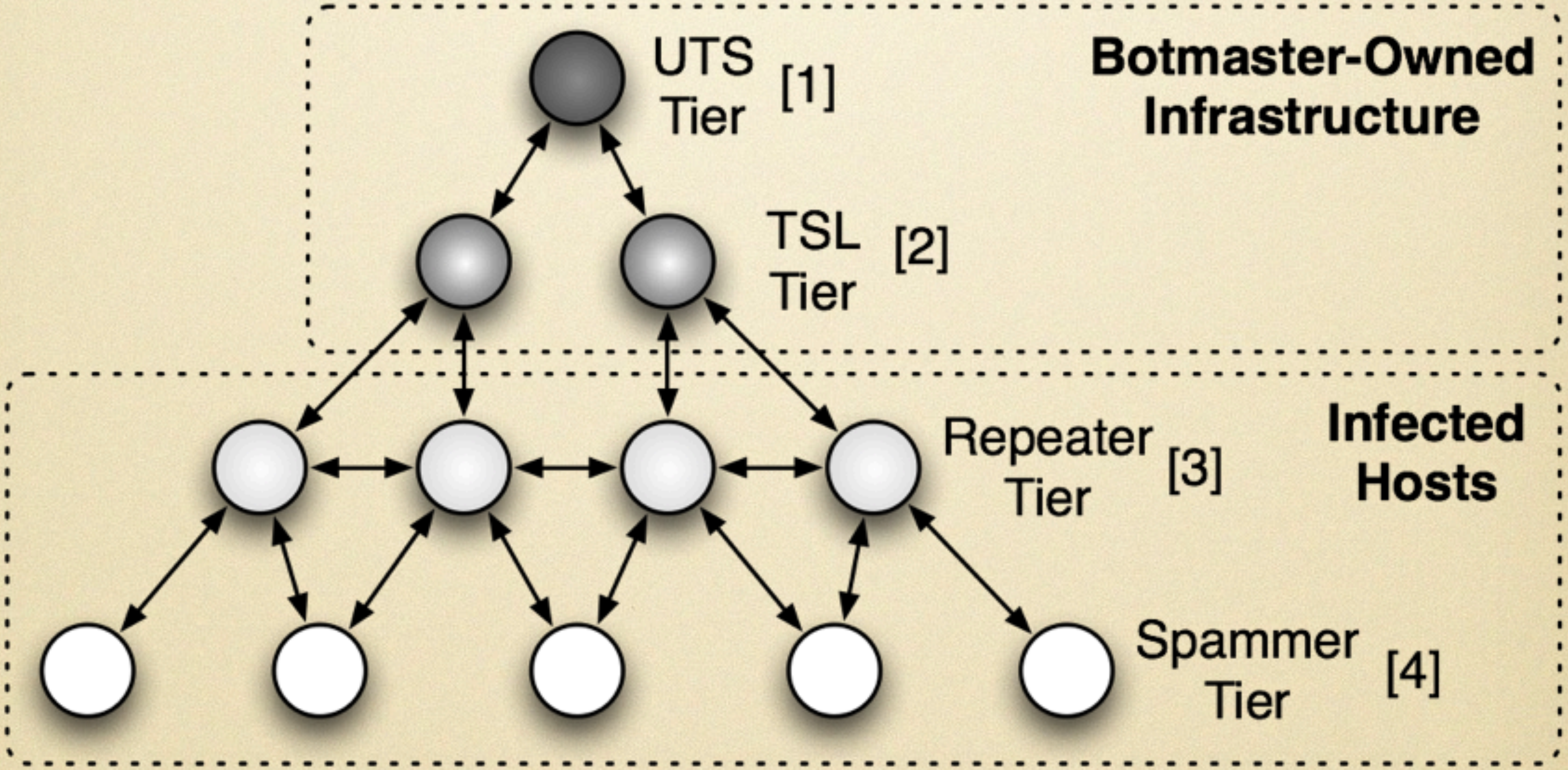
Waledac's Components

- Botmaster-deployed systems (*1:6*[*] *ratio*):
  - UTS (single system)
  - TSLs
- Infected-host tiers (*1:7*[*] *ratio*)
  - Repeater Layer
  - Spammer Layer

[*]on average

Topology

4 layers, 2 sections



Infected-Host Tiers

layers 3 and 4

- Roles
  - Local data harvesting, spamming
  - HTTP proxying, fast-flux DNS
- Communication
  - HTTP-based, similar to Storm
  - Limited P2P functionality
  - Certificates + AES

TSLs

layer 2

- Purpose
  - Hide UTS from Repeaters
  - Initiate targeted spam campaigns

- Configuration
  - CentOS
  - ntp, BIND, PHP, nginx, proxychains
  - *src* (package archives) and *pack* (specific configs)
  - php_mailer

UTS

layer 1

- Purpose
  - Autonomous C&C
  - Credentials repository
  - Hosts binaries and bootstrap lists
  - Monitors population, vitality statistics
  - Affiliates interface (*FairMoney*)
  - Interacts with underground 3rd parties (*spamit.com, j-roger.com*)
- Configuration
  - CentOS
  - Flat-files, no central DB
  - CLI

Audit Methodology

@UTS layer

- ERP- Executable Request Proxy
  - Is a repeater hosting a particular file?

request

```
GET /readme.exe HTTP/1.0
  Host: 99.56.197.58
```

reply

```
HTTP/1.1 200 OK
Server: nginx/0.8.5
Date: Fri, 28 Aug 2009 09:26:11 GMT
Content-Type: application/octet-stream
Connection: close
Content-Length: 2
Last-Modified: Sun, 26 Jul 2009 10:49:55 GMT
Accept-Ranges: bytes

MZ
```

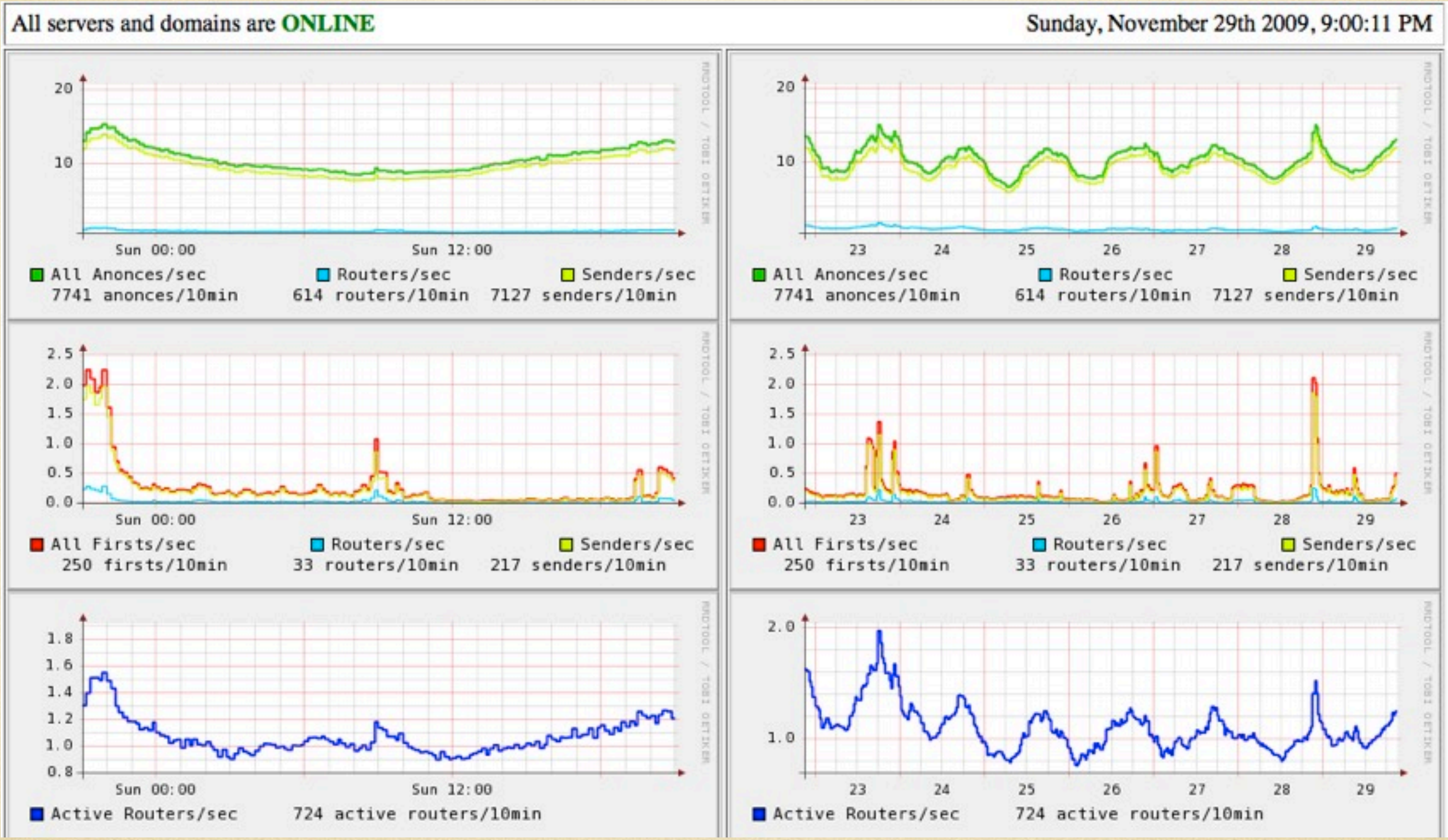
- DR - Domain Response
  - Can a repeater resolve *hellohello123.com*?
  - A fast-flux domain without a *.com* TLD entry

Third-Party Repacking

@UTS layer

- *crypt.j-roger.com* and *cservice.j-roger.com*
- UTS sends a POST to:
  `/api/apicrypt2/[16 hexadecimal digit hash]`
  ...followed by a binary to repack
- Repacked binaries returned in ~*4* seconds
- *157* binaries repacked during a 2-hour observation

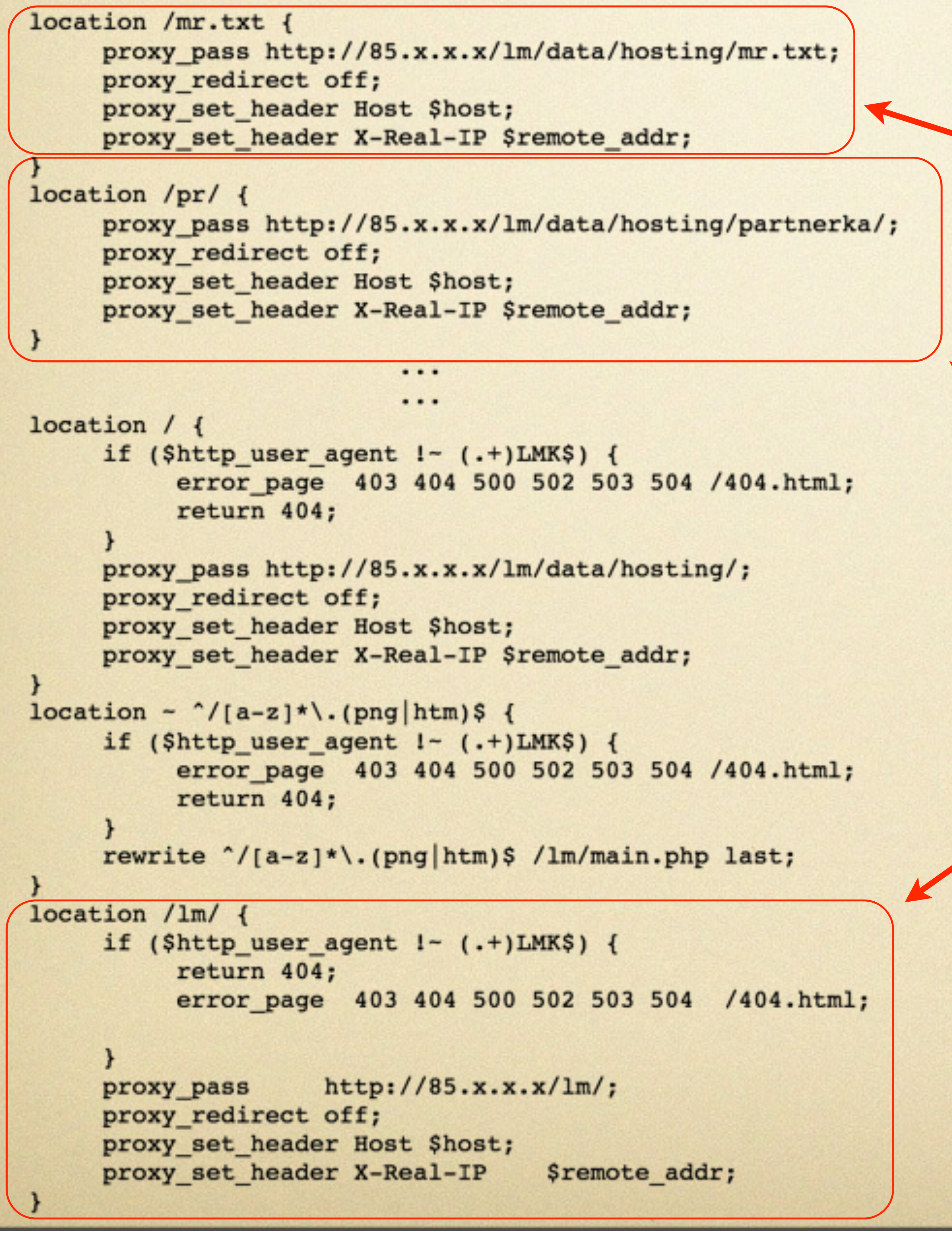
Monitoring @UTS



All servers and domains are **ONLINE** Sunday, November 29th 2009, 9:00:11 PM

nginx Config

@TSL layer



```
location /mr.txt {
     proxy_pass http://85.x.x.x/lm/data/hosting/mr.txt;
     proxy_redirect off;
     proxy_set_header Host $host;
     proxy_set_header X-Real-IP $remote_addr;
}
location /pr/ {
     proxy_pass http://85.x.x.x/lm/data/hosting/partnerka/;
     proxy_redirect off;
     proxy_set_header Host $host;
     proxy_set_header X-Real-IP $remote_addr;
}
                                   ...
                                   ...
location / {
     if ($http_user_agent !~ (.+)LMK$) {
          error_page  403 404 500 502 503 504 /404.html;
          return 404;
     }
     proxy_pass http://85.x.x.x/lm/data/hosting/;
     proxy_redirect off;
     proxy_set_header Host $host;
     proxy_set_header X-Real-IP $remote_addr;
}
location ~ ^/[a-z]*\.(png|htm)$ {
     if ($http_user_agent !~ (.+)LMK$) {
          error_page  403 404 500 502 503 504 /404.html;
          return 404;
     }
     rewrite ^/[a-z]*\.(png|htm)$ /lm/main.php last;
}
location /lm/ {
     if ($http_user_agent !~ (.+)LMK$) {
          return 404;
          error_page  403 404 500 502 503 504  /404.html;

     }
     proxy_pass     http://85.x.x.x/lm/;
     proxy_redirect off;
     proxy_set_header Host $host;
     proxy_set_header X-Real-IP    $remote_addr;
}
```

- */mr.txt* - list of repeater nodes; used for targeted spam proxying
- */pr/* - partnerka; interface to obtain binaries; access affiliates program
- */lm/* - access to the UTS control scripts

Affiliates

partnerka

- The *FairMoney* system
- Developers create multiple versions of binaries with different affiliate IDs
- Distribution (URLs) handled by 3rd parties
- Pricing based on *downloads* and *lifetime*

Activities

malicious throughput

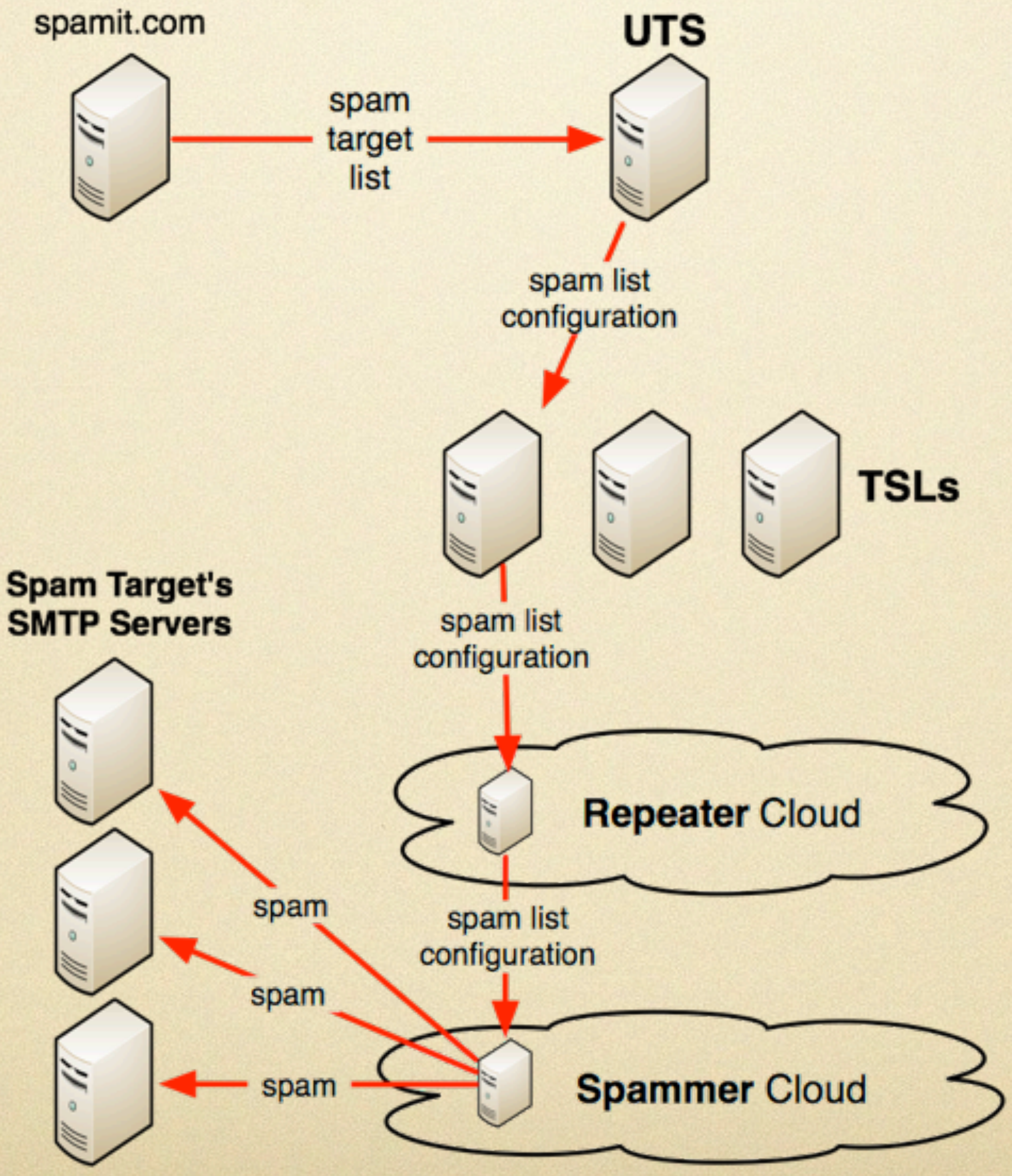
- Differentiated spamming
  - *High* and *Low* quality (*HQS*/*LQS*)
  - *Authenticated* and *targeted* v. *bulk*
- Data harvesting
  - Network traffic (*winpcap*)
  - HDD Scanning (*email regex*)

Differentiated Spamming

- **HQS** (*High* Quality Spam)
  - Utilizes credentials to send authenticated mail(SMTP-AUTH)
  - ‘test’ campaign
- **LQS** (*Low* Quality Spam)
  - Autonomous, bulk, sent by *spammer* tier
  - Transmission success statistics are reported

LQS

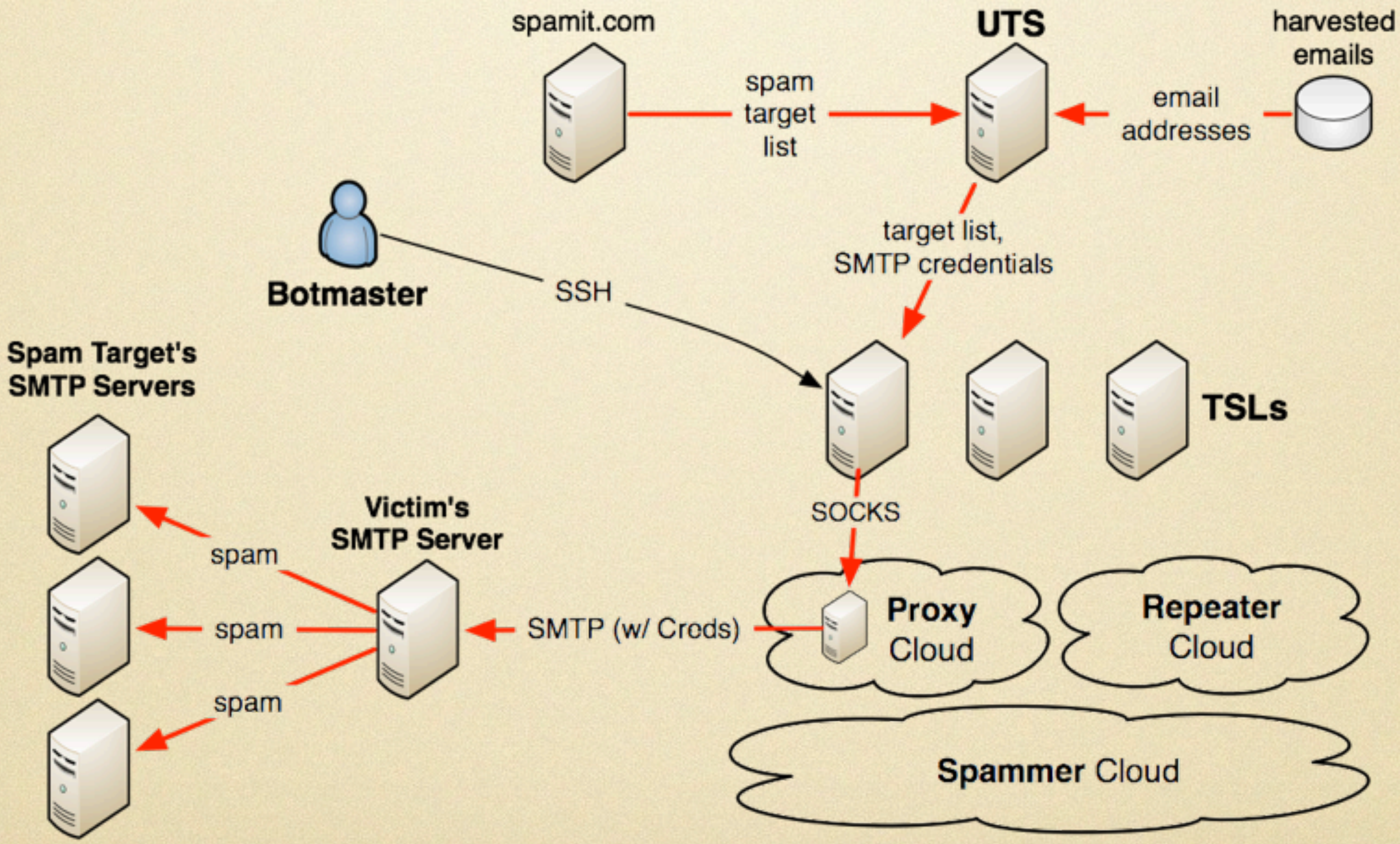
low quality spam



Wednesday, April 28, 2010

HQS

high quality spam



Challenging Notions

- Differentiated Spamming
- 3rd-Party Repacking
- Node Auditing

Questions