Panoptes: Detecting Malware Activity in Home Networks

Sarthak Grover, Nick Feamster
School of Computer Science, Georgia Tech

Problem

- Hosts on home networks can be compromised.
- Users don't always install anti-virus.
- Some devices do not have anti-virus.
- ISPs can only detect that a compromise has occurred inside the home, not which specific device has been compromised.

Approach

- Outsource security and home network management to a trusted and skilled third party.
- Passively monitor traffic inside the home, *behind the NAT*
  - Monitor suspicious traffic exchanged with each device
  - Allows for identifying individual devices

Demonstration

Server

dp4.gtnoise.net

```
./bloom
malware_domains
```

Client

Ubuntu 13.04

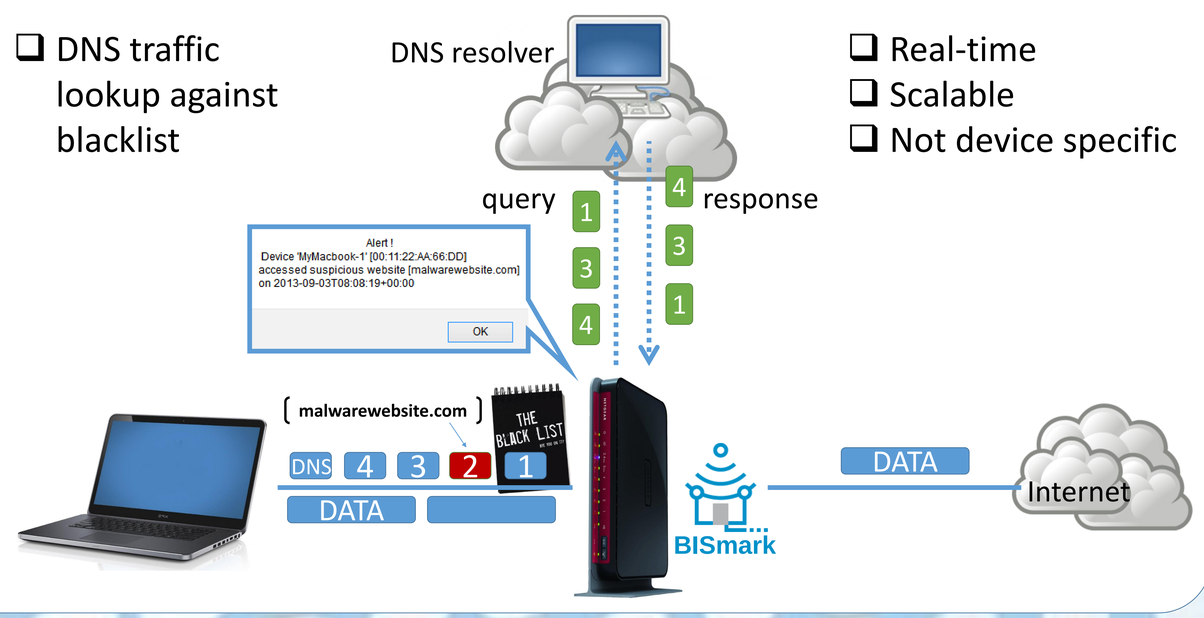
```
curl
server:filter.bin
sudo ./bloom-
passive.bin eth0
dig <domains>
```

Panoptes

- Scalable and efficient Bloom-filter based malware traffic detection system.
- Monitor customer traffic passing through a gateway device in real-time.
- Compare DNS queries against extensive blacklist compiled from third party expert sources.
- On detection of malicious traffic
  - Log access information: time, duration, compromised devices' ID, port numbers, bytes transferred and malware website(s) accessed.
  - Notify the owner of (home) network about device information.

Implementation

- DNS traffic lookup against blacklist
- Real-time
- Scalable
- Not device specific



Server

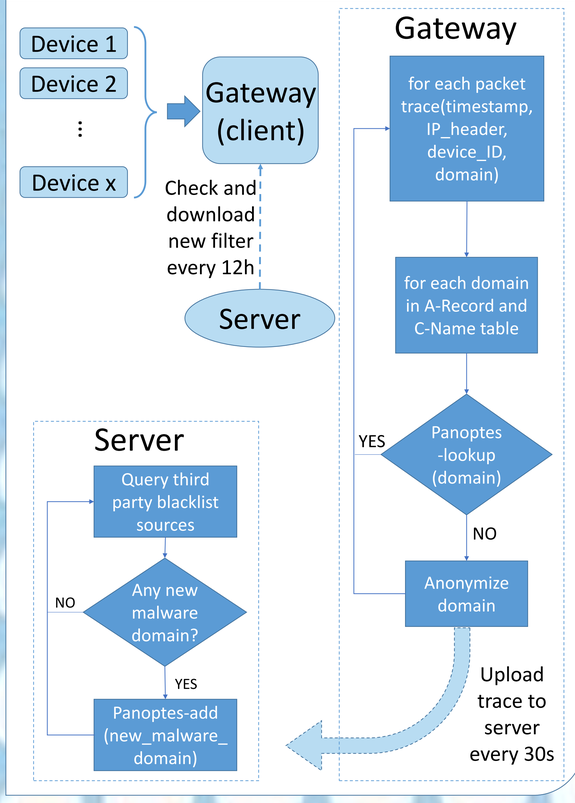
- Download recent malware domain list
- Create bloom-filter at server [gtnoise.net]

https://github.com/shahifaqeer/bismark-passive
https://github.com/shahifaqeer/bloom_filter

Client

- Download filter.bin if new
- Start bismark-passive with Panoptes
- Generate traffic using `dig` command or browser
- Log traces into /tmp/bismark-uploads/
- Upload log to server for detailed analysis

System Overview



Future Work

- **Take action on suspicious traffic [Comcast SAZO].** ISP alert to trigger VPN at gateway to redirect traffic for device showing suspicious activity, followed by deep packet inspection of malicious traffic.
- **Early detection and malware prediction.** Analysis of DNS traces at server to predict malicious traffic for user.

Contact: sgrover@gatech.edu