Impact Analysis of Botnet Infection on Networked Systems using Timed Automata

SYSC 5500
Group 8

Alvi Jawad
Luke Newton

Outline

Brief Overview

- Previous Work

Extending the Botnet

- Major Changes
- Extension Efforts
- Hardware and OS limitations

Rebooting as a Solution

- Device Type 2 – Reboot Capable
- Why Rebooting?

Results

- Reboot Frequency
- "Active" vs "Stealthy" bots
- Network Speed Variation
- Next steps!

Previous Work

Modeling

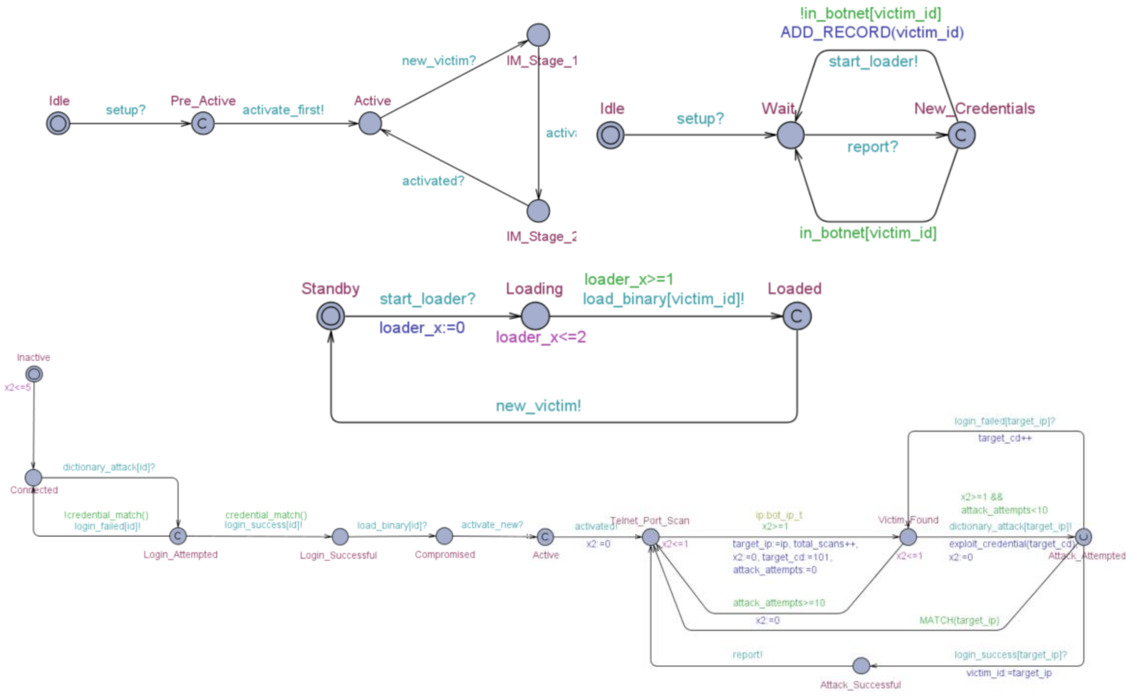
- Modeling the Mirai botnet infrastructure and individual device behavior

Modeling Formalism

- Timed Automata

Modeling Tool

- UPPAAL 4.1.24



Objective

- Observing the behavior of individual entities in the botnet
- Perform experiments to examine the infection rate and generated network traffic

Major Changes

Extended Dictionary

- Bots now make use of the full dictionary of the original Mirai codebase
- Each device has a pseudo-randomly generated ID (IP, credentials) at the start

Modeling Workarounds

- Extreme state-space reduction
- Compact data structure
- Removal of a few secondary committed states

Target

- Extend the network to simulate thousands of devices simultaneously

Extension Efforts

Extending the Botnet

- Initial efforts focused on extending the size of the botnet by a small margin

20 Devices

- Simulations were extremely fast
  - Simulation time (10 runs): ~**2 seconds**
- Very low resource consumption
  - Verification memory: ~**17 MB/29 MB**
- Very small network; not representative of the IoT

100 Devices

- Simulations were relatively fast
  - Simulation time (10 runs): ~**3 minutes**
- Very low resource consumption
  - Verification memory: ~**157 MB/188 MB**
- Small network; still not representative of the IoT

Extension Efforts

Extending the Botnet

- Subsequent efforts emphasized creating networks of over a hundred devices

500 Devices

- Simulation times were **infeasible**
  - Simulation time (10 runs): ~ **11 hours**
- Highest resource consumption
  - Verification memory: ~ **3500 MB/3700 MB**
- A good representation of a small IoT network

250 Devices

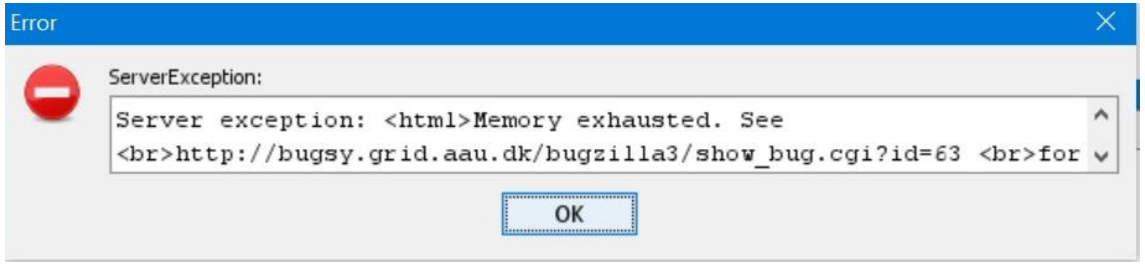
- Simulations were still rather slow
  - Simulation time (10 runs): **75 minutes**
- Moderate resource consumption
  - Verification memory: ~**580 MB/650 MB**
- The best overall compromise in terms of simulation speed and network size

We chose to use networks of 250 and 100 devices for most simulations

Limitations

Extending the Botnet

- Extending the network beyond 500 devices would never work

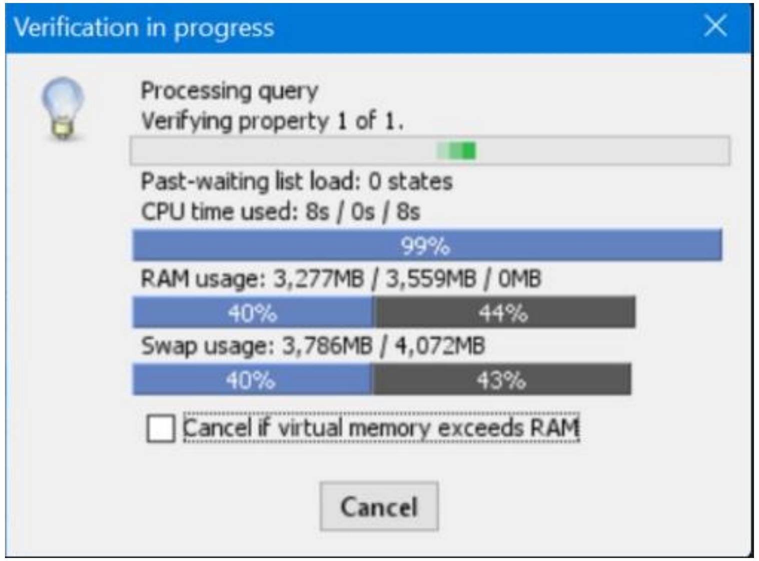


ServerException:

```
Server exception: <html>Memory exhausted. See
<br>http://bugsy.grid.aau.dk/bugzilla3/show_bug.cgi?id=63 <br>for
```

Hardware Limitations

- Verification memory: ~ 3500 MB/3800 MB -> **40%**
- Graphical simulator: ~ 3600 MB/4072 MB -> **44%**



Processing query
Verifying property 1 of 1.

Past-waiting list load: 0 states
CPU time used: 8s / 0s / 8s

99%

RAM usage: 3,277MB / 3,559MB / 0MB

40% 44%

Swap usage: 3,786MB / 4,072MB

40% 43%

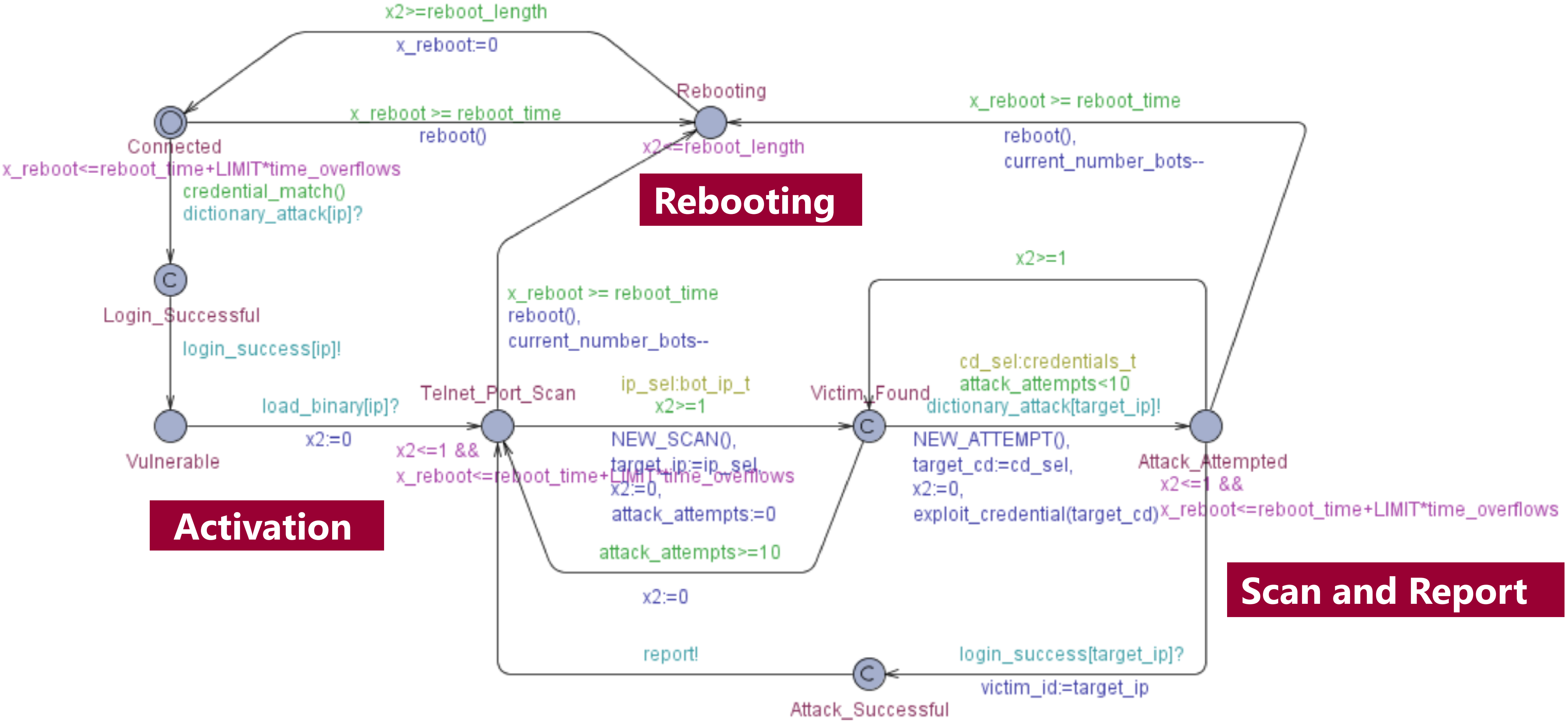
☐ Cancel if virtual memory exceeds RAM

OS Restrictions

- Only 32-bit version of UPPAAL available for MS Windows
- The verifier can only access at most 4 GB of memory

We decided to leave extending the network further as part of our future work

Device type 2 – Reboot Capable



Rebooting

Activation

Scan and Report

Why Rebooting?

Extending the Botnet

- Mirai lives in the dynamic memory; cleared when the device is rebooted
- Device credentials must be changed to prevent secondary infection

Target Clusters

- Devices that reboot either periodically or manually by the user
- Class **E1** - Devices with a periodic battery (primary) replacement interval
- Class **P0** – Devices that are normally off and only reattached to the network when needed

New Objective

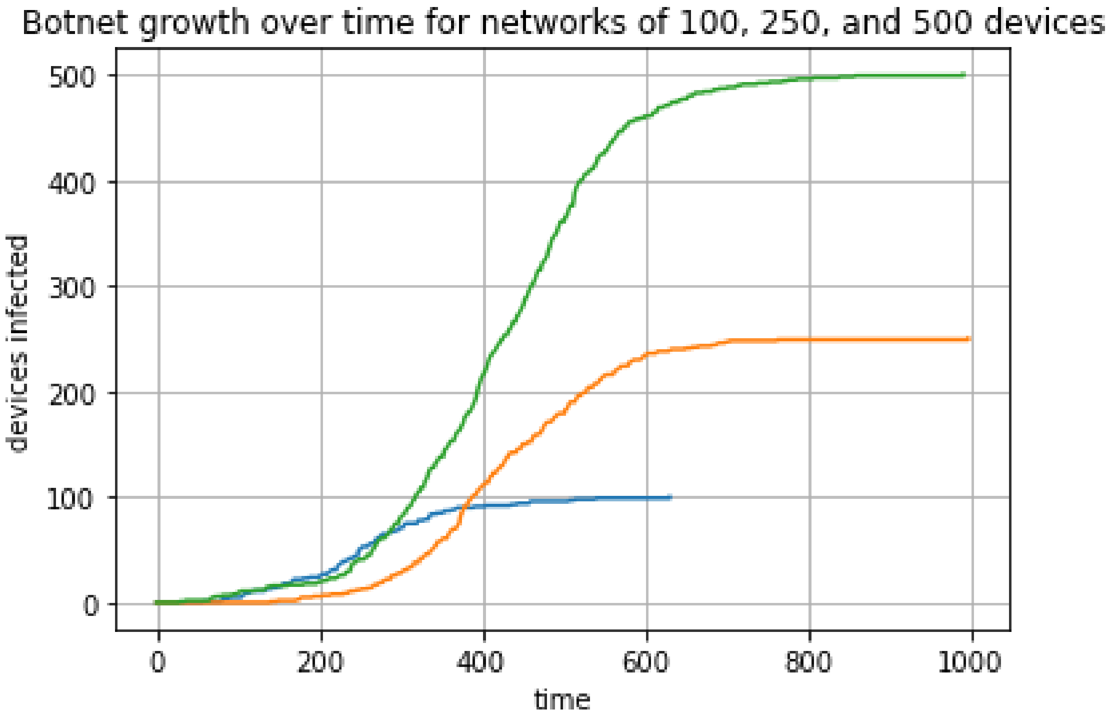
- **Can rebooting prevent** the accumulation of a **large-enough botnet**?
- If so, what **rate of frequency** is needed to achieve such results?
- Is the rate **feasible**?

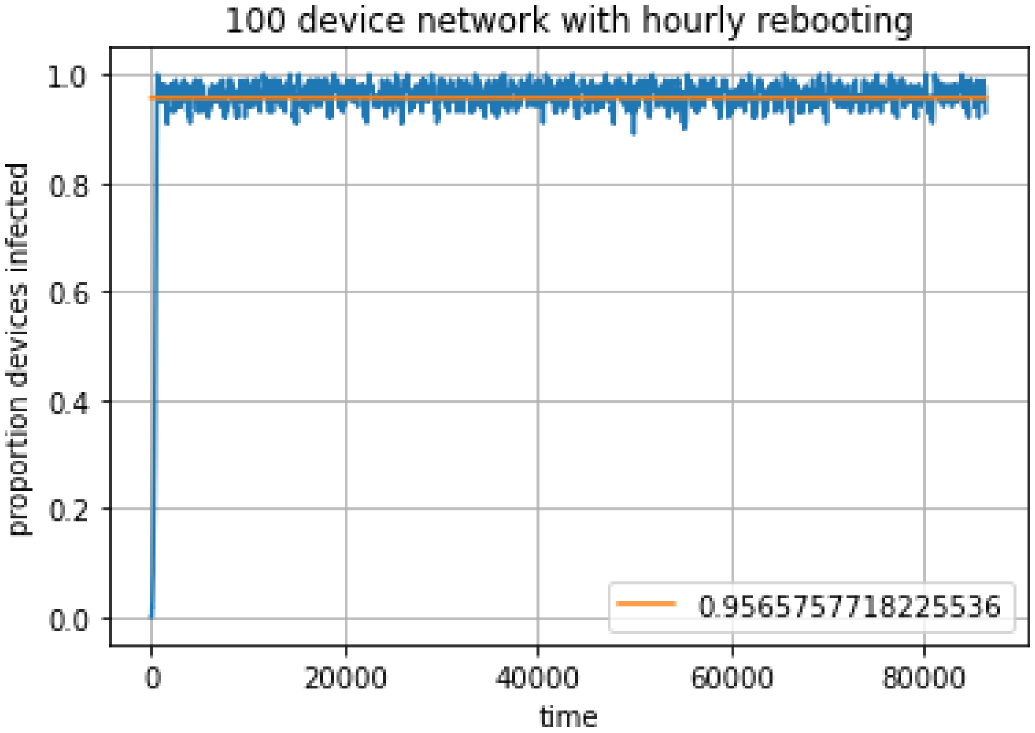
C. Bormann and A. Keranen. Terminology for Constrained-Node Networks. https://www.ietf.org/rfc/rfc7228.txt

Simulation Parameters

Parameter	Default Value	Other values used
Number of devices	100	250, 500
Round Trip Delay	100ms	1s
Simulation time	1 day	1 week
Dictionary length	62	-
Percentage of devices with weak credentials	100%	-
Reboot frequency	Hourly	Daily, every 30 minutes, every 10 minutes, every 5 minutes
Duration of device reboot	60s	-
Percentage of time bots propagate malware	100%	50%, 10%, 1%
Proportion of “always connected” devices to rebooting devices	0:100	100:0

“Always-Connected” vs “Reboot Capable”



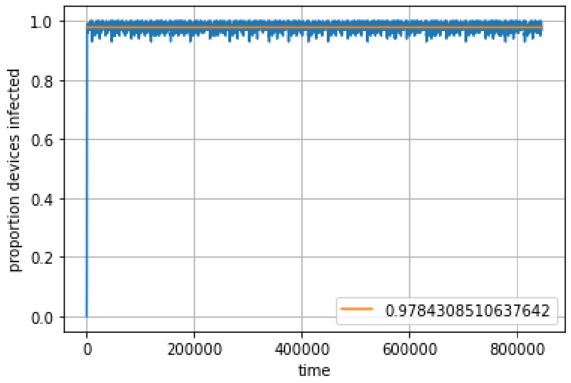


How does period affect botnet size?

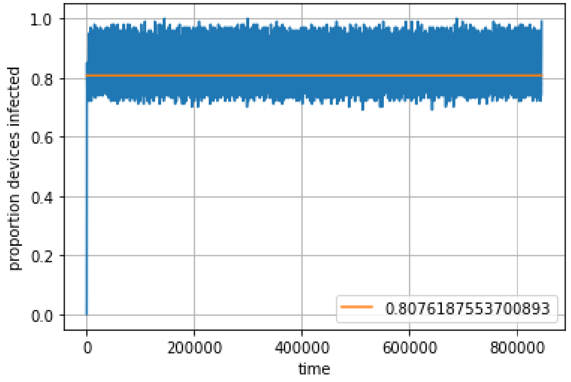
- 100 device network
- 1 minute to reboot a device
- Once a device is infected, it only propagates malware

Reboot Frequency	Uptime	Average botnet size
Daily	99.93%	99.9%
Hourly	98.33%	97.8%
Every 30 minutes	96.67%	96.0%
Every 10 minutes	90%	89.6%
Every 5 minutes	80%	80.7%

Hourly reboots over one day



Reboot every 5 minutes over one day



“Active” vs “Stealthy” bots

- 100 device network
- 1 minute to reboot a device
- Vary the percentage of time a bot propagates malware

Percentage of time propagating malware	Percentage of time stealthing	Reboot Frequency	Average botnet size
100%	0%	Hourly	97.8%
50%	50%	Hourly	97.7%
10%	90%	Hourly	95.8%
1%	99%	Hourly	71.5%
100%	0%	Daily	99.9%
50%	50%	Daily	99.7%
10%	90%	Daily	99.4%
1%	99%	Daily	97.4%

How does network speed affect botnet size?

Reboot Frequency	Uptime	Average botnet size (100ms RTT)	Average botnet size (1s RTT)
Daily	99.93%	99.9%	99.0%
Hourly	98.33%	97.8%	95.6%
Every 30 minutes	96.67%	96.0%	92.1%
Every 10 minutes	90%	89.6%	76.3%
Every 5 minutes	80%	80.7%	46.9%

How does network speed affect botnet size?

Percentage of time propagating malware	Percentage of time stealthing	Reboot Frequency	Average botnet size (100ms RTT)	Average botnet size (1s RTT)
100%	0%	Hourly	97.8%	95.6%
50%	50%	Hourly	97.7%	93.2%
10%	90%	Hourly	95.8%	69.6%
1%	99%	Hourly	71.5%	0.0067%
100%	0%	Daily	99.9%	99.0%
50%	50%	Daily	99.7%	98.7%
10%	90%	Daily	99.4%	97.8%
1%	99%	Daily	97.4%	86.0%

Conclusion

- Rebooting and slowing the network down can reduce botnet size, but are only effective at levels that would deteriorate functionality
- The most effective strategy is to change default credentials
- A botnet's level of stealthing can be very high before it's ability to grow is severely impacted
- Even a botnet of relatively small size can still send 10 000s of messages over a network hourly

Thank You!

Questions?