Malware Prognosis

Recommendations for Doing Malware Research in the Medical Domain

Sai R. Gouravajhala, Amir Rahmati, Peter Honeyman, Kevin Fu

SPQR

COLLEGE OF ENGINEERING
COMPUTER SCIENCE & ENGINEERING
UNIVERSITY OF MICHIGAN

Background

Malware in the medical domain is an important concern.

- Regulatory [FDA Cybersecurity Draft Guidance, 2013; MAUDE Database]
- Academia [Halperin et al., IEEE S&P 2008; Clark et al., HealthTech 2013]
- Media

Why are medical devices vulnerable in the first place?

What IT policies are currently being utilized?

- Isolated networks
- VLANs
- Access Control Lists (ACLs)

Research Questions

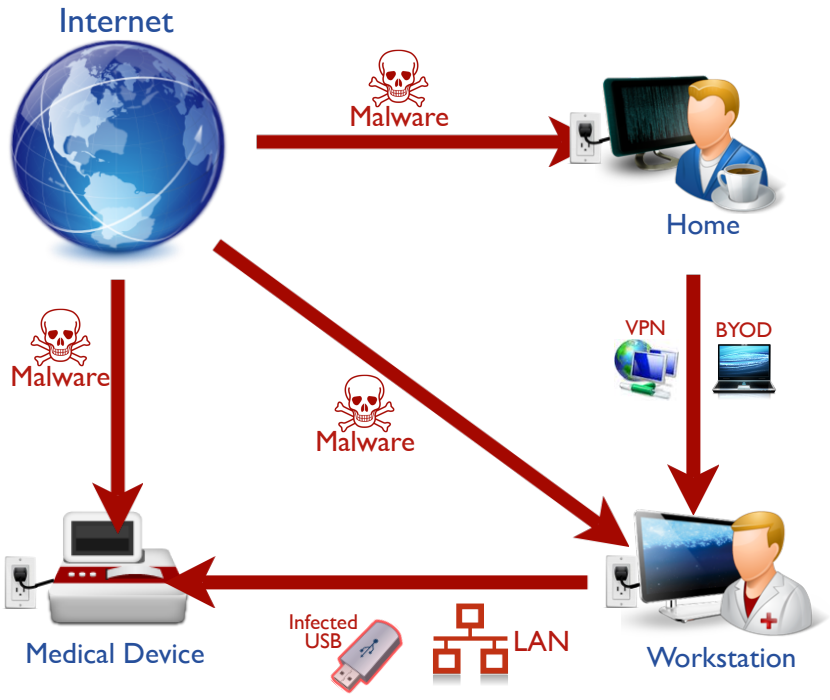
What are the dominant vectors for malware infections?

How can we mitigate these vectors?

To address those, need to know how to:

- Detect infections
- Quantify the infection rate
- Qualify the types of malware infections

We focus on *detection*.

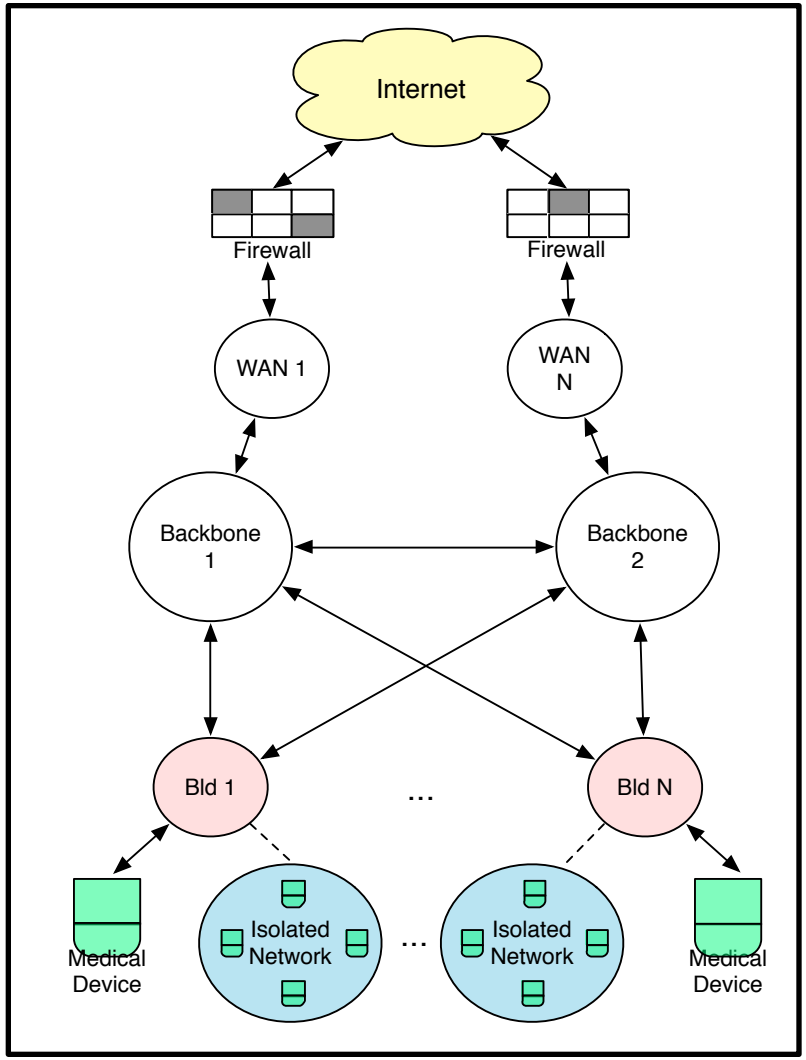


Hypothesis

We can detect compromised medical workstations and devices using the network perspective.

Data:

- Darknet
- NetFlow
- Blacklist



Experiments

Comb through network traces to find malware fingerprints, then zero-in on suspicious source IPs.

Experiment 1: Darknet

Experiment 2: NetFlow

Experiment 3: NetFlow + Blacklist

Heuristic approach:

- Port scanning, odd port behavior, botnet-like behavior
- Timing analysis

Diagnosis?

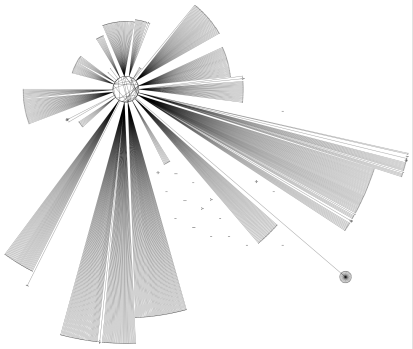
Experiment 1: Darknet has been of little use

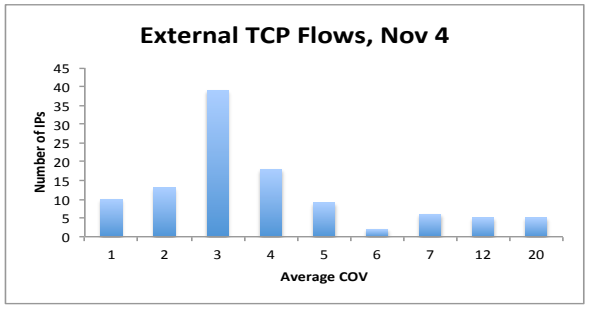
Experiment 2: anomalous behavior seen

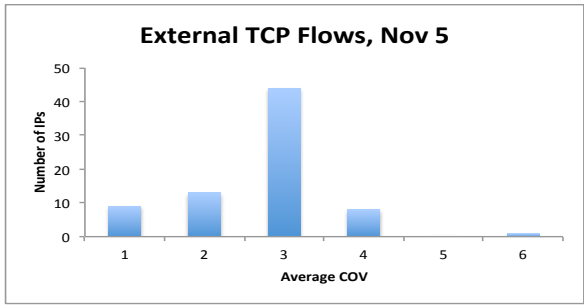
At least two workstations in radiology that seem to be infected with adware; a couple of hosts operating over BitCoin ports; a machine that was contacting a Tor exit node over IRC port 6667;

Timing analysis showed a few machines with unusually low average coefficients of variation.

Experiment 3: tens of devices with more than 300 blacklisted IPs contacted.







Evaluation

We know that medical devices are vulnerable…

…and that hospital networks have malware…

…but why aren't we seeing those "gotcha" signs?

Potential reasons why →

℞ 1: Longitudinal data

Network traces need to either be targeted to specific events or be longitudinal in nature.

℞ 2: Network administration

Effective network administration is a potent means of limiting both the number and scope of malware incidents.

℞ 3: Device-level investigations

Looking for vulnerabilities at the device level is both productive and important for understanding how easily systems can become infected.