Calculating Consumer Costs of Insecure IoT Devices

Kim Fong, Kurt Hepler, Rohit Raghavan, Peter Rowland

MIMS Final Project Presentation

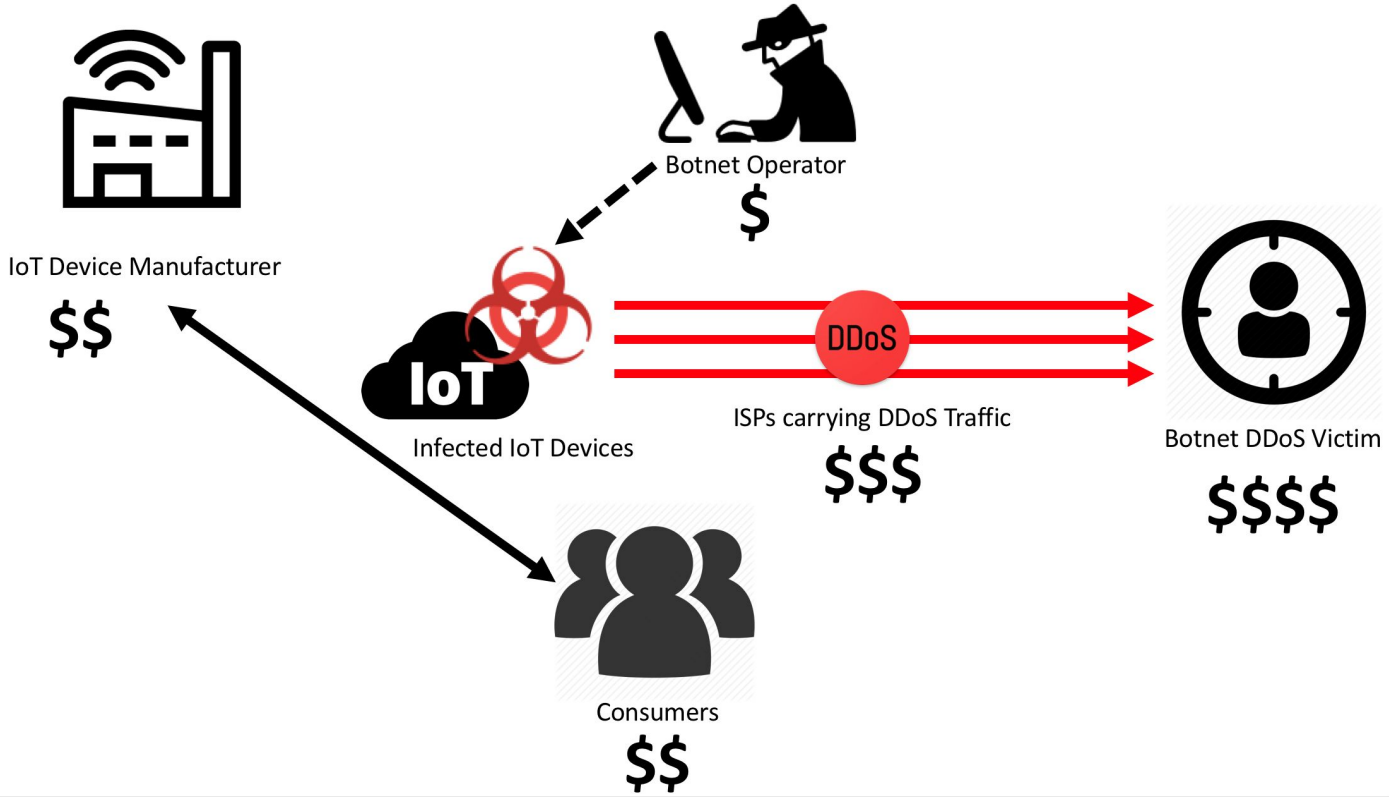
2018

Berkeley SCHOOL OF INFORMATION

CLTC Center for Long-Term Cybersecurity UC Berkeley

DDoS, Botnets, and Consumers

A Model of Incentives and Costs in DDoS Attacks



What Costs Do Consumers Incur?

Direct costs	Indirect costs	Defense costs
• Additional energy consumption • Bandwidth consumption • Packet loss • Non-functioning or reduced functioning of device • Clean up and repair costs • Frustration or lost productivity from inability to access disabled services	• Competition • Innovation	• Anti-virus software • Installing updates

Research Hypotheses

Hypothesis 1

Increased Energy Consumption

IoT devices infected with Mirai malware have increased electricity consumption. The amount of the increase, when aggregated across a large botnet, is consequential.

Hypothesis 2

Increased Bandwidth Consumption

IoT devices infected with Mirai malware consume additional bandwidth. The additional bandwidth consumption is substantial when aggregated across a large botnet.

Hypothesis 3

Degraded User Experience

IoT devices infected with Mirai malware interfere with the legitimate use of a consumer's device and network. Although measuring the additional cost of degraded service is beyond the scope of this project, the fact that this cost is likely non-zero turns the costs incurred because of electricity and bandwidth consumption into lower bounds for overall consumer costs.

Methods: Measuring Energy and Bandwidth Consumption

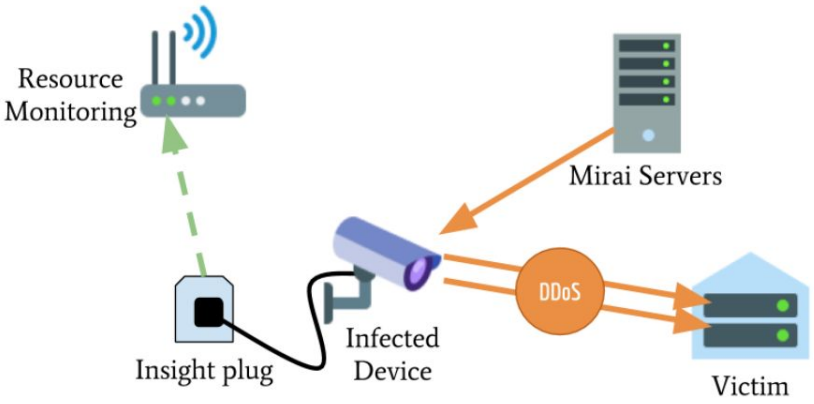
Device Selection

- Mirai malware targets IoT devices such as IP Cameras, DVRs and Routers.
- Mirai source code (on GitHub) contains 68 username password pairs.
- Acquired 8 devices suspected to have been involved in Mirai botnet attacks.*
- Successfully infected 2 devices.

IP Cameras	Digital Video Recorders (DVRs)	Routers
Samsung Smartcam SNH-1011N	**Dreambox DM500-C**	SMC Barricade SMCWBR14-G2
Dahua Camera HAC-HDW1200EM	Dahua DVR DHI-HCVR7104H-S2	ZyXEL Prestige 643
Dahua Camera IPC-HDW4431C-A		MikroTik hEX PoE lite RS750UPr2
		Buffalo WHR-300HP2

* https://krebsonsecurity.com/2016/10/who-makes-the-iot-things-under-attack/

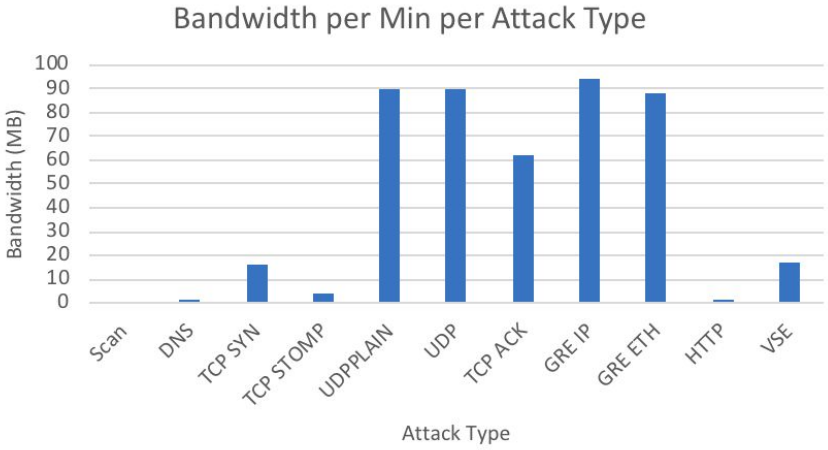
Network Setup & Measurements

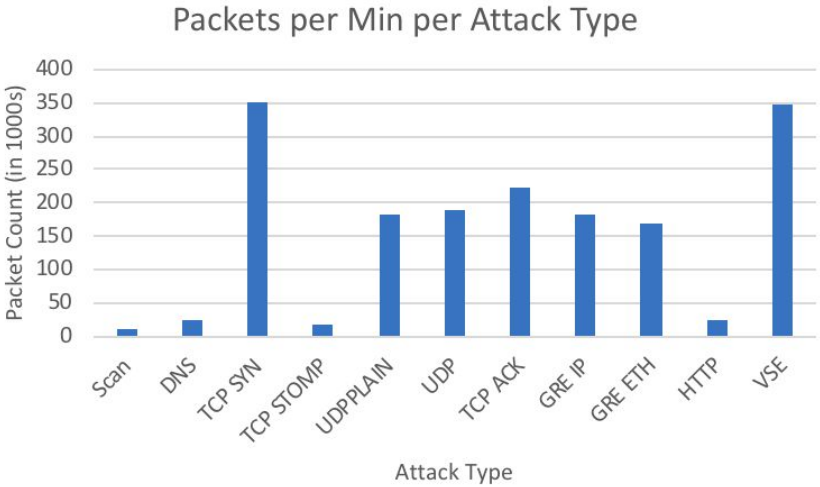


- **Network Setup**
  - Isolated network with no internet access.
  - Router as central hub and logging server for connected devices.
- **Measuring Energy Consumption**
  - Mirai Infected device plugged into Wemo Insight smart plug for energy monitoring.
  - Developed Python script to invoke Insight API to retrieve the instantaneous power consumption and write to log every min.
- **Measuring Bandwidth Consumption**
  - Added iptables (kernel level firewall) rules on router to log bandwidth and packets transferred by infected device.
  - Developed shell script to query iptables and write to log every min.

Testing Procedure

- Test consisted of 4 phases, each lasting 30 mins:
  - **Powered On (Control) phase**
  - **Scan phase**
  - **TCP SYN Attack phase**
  - **UDP Attack phase**
- Tested over WiFi and Ethernet connections.
- Results averaged over 5 tests.



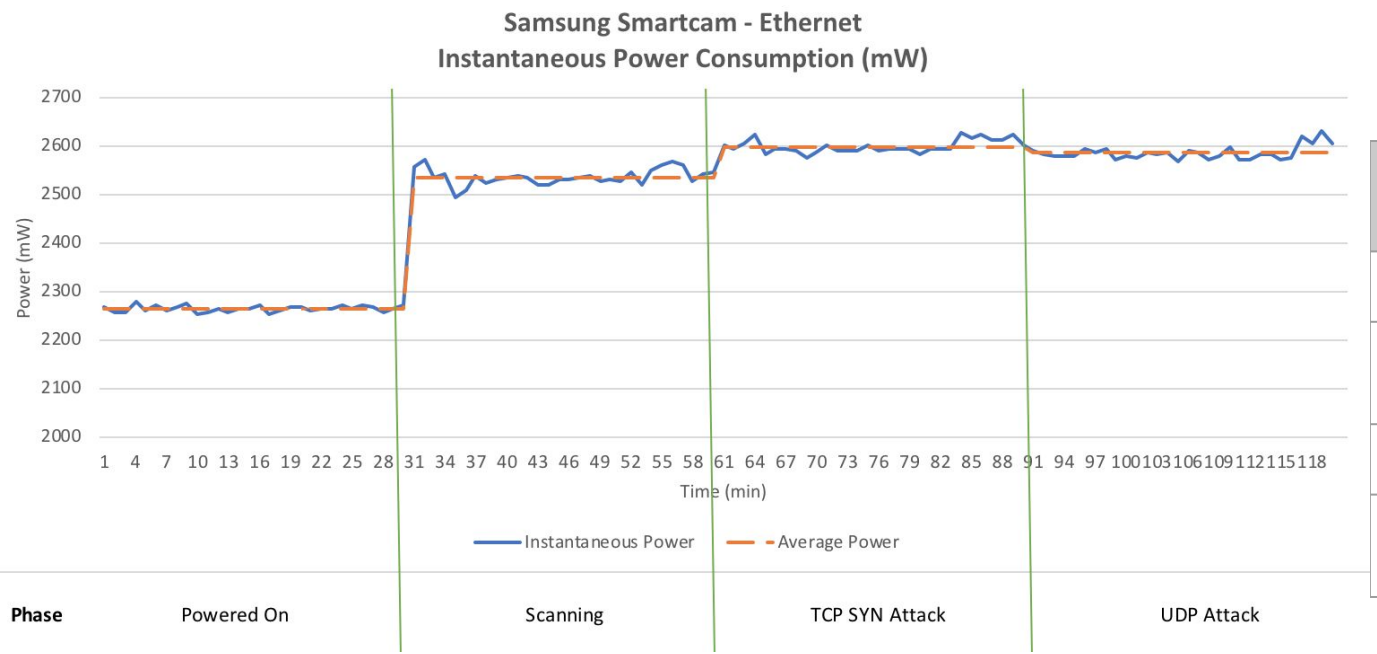


Results

H1: Increased Electricity Consumption

- Inconsequential increase in electricity consumption.
  - IoT devices do not use much electricity
- Across all devices and tests, increase of about 0.0001 kilowatts per hour.
  - Measurable, but miniscule

H1: Increased Electricity Consumption

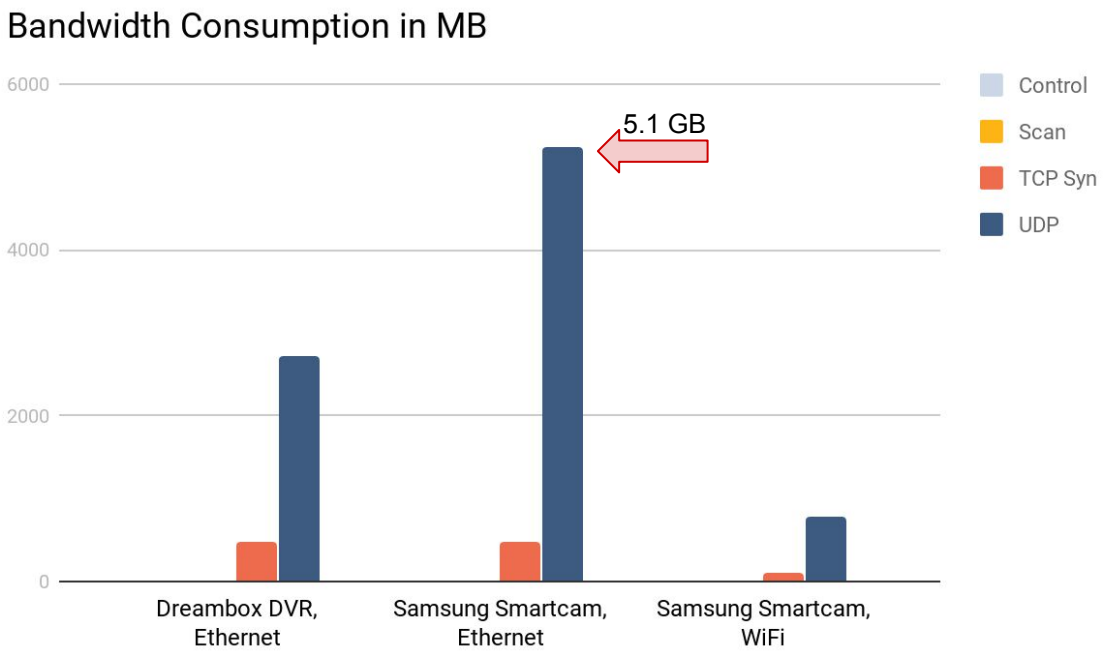


Phase	Energy (kWh)	% Change
Control	0.001104	—
Scan	0.001254	**↑ 13.59%**
TCP Attack	0.001284	**↑ 16.31%**
UDP Attack	0.00125	**↑ 13.22%**

H2: Increased Bandwidth Consumption

- Hacked devices use significant bandwidth during attacks.
- Bandwidth usage depends on a few factors.
  - Attack type (TCP vs. UDP)
  - Connection type (Ethernet vs. WiFi)
  - Device type (PPC vs. ARM)
- If the user has a bandwidth cap, a single infected device could devour a consumer’s entire monthly allowance in a few hours (especially for wireless and satellite customers).

H2: Increased Bandwidth Consumption



H3: Degraded User Experience

- Increased network latency
  - During UDP attacks, increased from around 0.3 ms to over 200 ms
  - Intermittent packet loss
  - Router CPU utilization reached nearly 100 percent
- Device crashes
  - Several test devices shut down unexpectedly and repeatedly when participating in attacks
    - Samsung Smartcam
    - Dahua DVR
    - Buffalo Router

Implications

Scenarios

Based on our results for energy and bandwidth consumption, we developed a calculator to estimate the costs incurred by consumers when their devices are used in DDoS attacks.

KrebsOnSecurity

Date: September 20, 2016

Duration: **77 hours**

Size of botnet: **24,000**

Total estimated externalized cost:
$323K

DYN

Date: October 21, 2016

Duration: **6 hours**

Size of botnet: **107,000**

Total estimated externalized cost:
$115K

Worst-Case

Date: Doomsday

Duration: **50 hours**

Size of botnet: **600,000**

Total estimated externalized cost:
$68M

Public Policy

How do you regulate this problem?

Federal Trade Commission 2017 unfairness claim against D-Link dismissed; failed to show “any actual consumer injury in the form of a monetary loss or an actual incident where sensitive personal data was accessed or exposed.”

Methods for determining costs contribute to this debate.

KrebsOnSecurity

KrebsonSecurity

In-depth security news and investigation

ADVERTISING/SPEAKING | ABOUT THE AUTHOR

07 MAY 18 Study: Attack on KrebsOnSecurity Cost IoT Device Owners $323K

A monster distributed denial-of-service attack (DDoS) against KrebsOnSecurity.com in 2016 knocked this site offline for nearly four days. The attack was executed through a network of hacked "Internet of Things" (IoT) devices such as Internet routers, security cameras and digital video recorders. A new study that tries to measure the direct cost of that one attack for IoT device users whose machines were swept up in the assault found that it may have cost device owners a total of $323,973.75 in excess power and added bandwidth consumption.

My bad.

I School Courses That Informed Our Research

Privacy, Security, and Cryptography

Distributed Computing Applications and Infrastructure

Privacy Law for Technologists

Privacy and Security Lab

Information Law and Policy

Information Technology Economics, Strategy, and Policy

Quantitative Research Methods

Information Organization Lab

```
        $$$$$$\     $$$$$$$$\
        \_$$  _|     \__$$  __|
 $$$$$$\ $$ | $$$$$$\ $$ |
$$  __$$\$$ |$$  __$$\$$ |
$$ |  \__$$ |$$ /  $$ $$ |
$$ |     $$ |$$ |  $$ $$ |
$$ |   $$$$$$\$$$$$$  $$ |
\__|   \______\______/\__|
```

Special Thanks To

CLTC
Center for Long-Term Cybersecurity
UC Berkeley

Project advisor
Chris Hoofnagle

Berkeley SCHOOL OF INFORMATION