Mirai and the Future of IoT Malware

Paul Royal
College of Computing
Georgia Institute of Technology
There is no Internet of Things, only other people's computers in your house.

-Jacob Hoffman
About

● What is GTISC?
  – Georgia Tech Information Security Center
  – Multi-unit, campus-wide organization at Georgia Tech, with a dual mission of research and education

● Who am I?
  – Affiliate researcher at GTISC
  – Build large-scale malware analysis systems
Mirai Overview
Motivation

Why study Mirai?

– October 2016 Dyn attack
  • 50,000 Mirai-compromised devices participated in > 1Tbps DDoS attack
  – Disrupted Dyn’s managed DNS service
Mirai Client Structure

- **Multi-arch software written in C**
  - ARM, MIPS, PPC, SH4, and others
    - Statically linked to avoid libc ABI compatibility issues
  - Targets busybox-based Linux typically found on embedded platforms
    - Examples: CCTVs, DVRs, routers
  - Self-propagates by brute-forcing telnet passwords

```cpp
// Set up passwords
add_auth_entry("\x50\x40\x40\x56", "\x5A\x41\x11\x17\x13\x13", 10);
// root  xc3511
add_auth_entry("\x50\x40\x40\x56", "\x54\x48\x58\x54\x54", 9);
// root  vizxv
add_auth_entry("\x50\x40\x40\x56", "\x43\x46\x4F\x48\x44", 8);
// root  admin
add_auth_entry("\x43\x46\x4F\x48\x44", "\x43\x46\x4F\x48\x44", 7);
// admin  admin
add_auth_entry("\x50\x40\x40\x56", "\x1A\x1A\x1A\x1A\x1A\x1A", 6);
// root  888888
```
Mirai Target Identification

- Hard-coded credentials reveal specific devices that are vulnerable

Mirai Client Notes

- Prevents introduction of other malware via telnet, SSH, and HTTP
- Identifies/terminates other malware
Mirai C&C

- **Software written in Go**
  - Instructs what/how to attack
    - Whitelists subnets belonging to DoD, USPS, GE and HP
- **Attacks Supported**
  - GRE Floods
  - UDP, TCP Floods
  - DNS Floods

```go
func (this *Attack) Build() ([]byte, error) {
    buf := make([]byte, 0)
    var tmp []byte

    // Add in attack duration
    tmp = make([]byte, 4)
    binary.BigEndian.PutUint32(tmp, this.Duration)
    buf = append(buf, tmp...)

    // Add in attack type
    buf = append(buf, byte(this.Type))

    // Send number of targets
    buf = append(buf, byte(len(this.Targets)))

    // Send targets
    for prefix, netmask := range this.Targets {
        tmp = make([]byte, 5)
        binary.BigEndian.PutUint32(tmp, prefix)
        tmp[4] = byte(netmask)
        buf = append(buf, tmp...)
    }
}
```
Mirai Development

- **July 10, 2016** – Author announces that Mirai will begin terminating QBot instances

- **August 6, 2016** – Author boasts about success in brute forcing telnet logins
Mirai Development Cont’d

- September 30, 2016 – Author releases Mirai source code

**Preface**

Greetings everybody,

When I first go in DDoS industry, I wasn't planning on staying in it long. I made my money, there's lots of eyes looking at IOT now, so it's time to GTFO. However, I know every skid and their mama, it's their wet dream to have something besides qbot.

So today, I have an amazing release for you. With Mirai, I usually pull max 380k bots from telnet alone. However, after the Kreb DDoS, ISPs been slowly shutting down and cleaning up their act. Today, max pull is about 300k bots, and dropping.

So, I am your senpai, and I will treat you real nice, my hf-chan.

And to everyone that thought they were doing anything by hitting my CNC, I had good laughs, this bot uses domain for CNC. It takes 60 seconds for all bots to reconnect, lol.
Mirai Trivia

- Mirai’s name was decided by its author.
- Name is based on a popular Japanese comic/cartoon series titled 「未来日記」
  - Romanizes to Mirai Nikki
  - Translates to Future Diary
Trends

- IoT malware will continue to flourish until device makers stop repeating the security mistakes of the late 20\textsuperscript{th}/early 21\textsuperscript{st} century
- Malware creation for IoT will undergo commoditization that enables a variety of general purpose computing
- Hardware evolution and attacker creativity will repurpose “other people's computers in your house” into powerful weapons
Data Sharing and DHS IMPACT
Introduction

- GTISC will soon begin sinkholing some Mirai C&C domains
  - A Mirai sinkhole dataset may subsequently appear in IMPACT
  - Currently available datasets include Kraken and Flashback
- Also shares several large-scale malware analysis datasets
Motivation

- Malware analysis is the basis for understanding the intentions of malicious programs
  - Cyber threat discovery, analysis
  - Compromise detection
  - Forensics and asset remediation

- Large-scale malware analysis data has both research and operational utility
Challenges

- Sensitive nature of data
  - Many in security industry continue to treat malware samples as a currency
  - Redistribution of raw malware carries risk

- Volume of samples
  - Number of new (unique, previously unseen) malware samples makes analysis an HPC activity

- Analysis resistance inherent to modern malware
  - Anti-analysis techniques previously in more sophisticated malware now a commodity
Opportunity

- GTISC has extensive malware collection and analysis experience
  - Collects over 100,000 unique, previously unseen samples each day
  - Samples collected from web crawlers, mail filters, and malware exchanges

- Has built large-scale, transparent malware analysis systems
  - Daily processing capacity on the order of hundreds of thousands of samples
  - Analysis infrastructure gathers malware network information
IMPACT

Through IMPACT, GTISC makes a safe representation of malware analysis data widely available.

Share network-level actions of samples, along with supporting metadata.

- DNS (domain name) data
  - Can be used to identify C2 domains and detect compromised assets

- SMTP (email) data
  - Can be used to improve spam and phishing detection
GTISC Data Users

- **Academia**
  - George Washington University, Texas A&M University, University of California Berkeley, Dalhousie University (Canada), Tel Aviv University (Israel)

- **Industry**
  - Security – Symantec, Intel Security (McAfee), Trend
  - Financials – Bank of America, Capital Group Companies, Lloyds Banking Group (UK)
  - Healthcare – Pfizer, Athena Health, Emdeon

- **Government**
  - DoD Cyber Crime Center, DARPA, DHS, RCMP (Canada), CSE (Canada), INCB (Israel)
Invitation to Participate

Do you need data to power your research?
- Visit the IMPACT website at impactcybertrust.org to search available datasets and learn more

Want to share data, but don’t have the time/infrastructure/legal framework?
- IMPACT can host, process requests for, and share your data at no cost to you
- Email info@impactcybertrust.org to begin a discussion
Questions?