Cyber Attack in IoT on the rise
- Observing attacks in IoT using IoTPOT -

Koji Nakao
Distinguished Researcher – NICT
Guest Professor – Yokohama National University
Adviser – KDDI

2017/1/24
Cyber attacks in IoT on the rise
Devices attacked our honeypot during Jan–June 2016

600,000+ IPs

500+ device types

†inferred by telnet and web responses
Categories of Inferred Infected devices (2016.9)

- **Surveillance camera**
  - IP camera
  - DVR
- **Network devices**
  - Router, Gateway
  - Modem, bridges
  - WIFI routers
  - Network mobile storage
  - Security appliances
- **Telephone**
  - VoIP Gateways
  - IP Phone
  - GSM Routers
  - Analog phone adapters
- **Infrastructures**
  - Parking management system
  - LED display controller
- **Control system**
  - Solid state recorder
  - Sensors
  - Building control system (bacnet)
- **Home/indivisuals**
  - Web cam, Video recorders
  - Home automation GW
  - Solar Energy Control System
  - Energy demand monitoring system
- **Broadcasting**
  - Media broadcasting
  - Digital voice recorder
  - Video codec
  - Set-top-box,
- **Etc**
  - Heat pump
  - Fire alert system
  - Medical device (MRI)
  - Fingerprint scanner

Devices are inferred by telnet/web banners
ROUTE CAUSES OF THE MASS-INFECTION

Telnet
Telnet

From Wikipedia, the free encyclopedia

Not to be confused with Telnet.

This article needs additional citations for verification. Please help improve this article by adding citations to reliable sources. Unsourced material may be challenged and removed.

(April 2014) (Learn how and when to remove this template message)

Telnet is an application layer protocol used on the Internet or local area networks to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection. User data is interspersed in-band with Telnet control information in an 8-bit byte oriented data connection over the Transmission Control Protocol (TCP).

Telnet was developed in 1969 beginning with RFC 15, extended in RFC 854, and standardized as Internet Engineering Task Force (IETF) Internet Standard STD 8, one of the first Internet standards.

Historically, Telnet provided access to a command-line interface (usually, of an operating system) on a remote host, including most network equipment and operating systems with a configuration utility (including systems based on Windows NT). However, because of serious security concerns when using Telnet over an open network such as the Internet, its use for this purpose has waned significantly in favor of SSH.

https://en.wikipedia.org/wiki/Telnet
They are everywhere in Internet

BCM96328 Broadband Router

OpenPLI 3.0 dm800se

Netgear login:

Air5450v2 login:

Advantys login:

Router CLI User Access Verification

Hikvision login:

MX120 VoIP AG login:

BCM96328 ADSL Router

BCM96328 xDSL Router

TL-40N login:

Netgear login:

Netgear TL-WR740N login:

dm800se login:

et4x00 login:
With default/weak id and password

[shogo@www9058up ~]$ telnet x.x.243.13
Trying x.x.243.13...
Connected to x.x.243.13.
Escape character is '^]'.

openpli.3.0.dm800s
dm800se.login: root
Password: 12345

BusyBox v1.1.2 (2007.05.09-01:19+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.
Search for "default" "password" "list"
Devices attacked our honeypot during Jan–June 2016

Those devices attacked us also run telnet and we believe it is via which they got infected

Devices are inferred by telnet and web banners of these devices
HOW WE MONITOR ATTACKS
Two approaches to monitor attacks

- **Passive monitoring**
  Prepare network to monitor attacks and wait
  - Darknet monitoring
  - Honeypot

- **Active monitoring**
  Search for device/vulnerability/backdoors
  - Accessing Web, Telnet, FTP, etc to decide what devices they are
  - Checking for backdoor ports
  - Measuring clock skew for tracing individual devices
Darknet monitoring

Darknet: unused but routable IP address(es) or net blocks

Many researchers/organization utilize darknet to monitor malicious activities like scanning, remote exploits, back scatters, etc
Recently, “scanning to Port 23 (telenet)” is getting larger!!

- Capturing packets through dark-net in real time basis.
- Color indicates the protocol types.

- **UDP**
- **TCP SYN**
- **TCP SYN/ACK**
- **TCP Other**
- **ICMP**
Increases of telnet attacks

10 years observation of NICTER darknet (23/tcp only)
To monitor in depth

Darknet monitoring is simple and great to monitor wider networks but limited as it only gets the first packet of each attack.
Our system: IoTPOT = IoT Honeypot

We use decoy system (honeypot) to emulate vulnerable IoT devices to monitor the attacks in depth.

Observation result (last year)
Period: 2015/4/1 ~ 2015/7/31 (122 days)

150,000 IPs attempted to login, 100,000 actually did send us malware binaries

Binaries with 11 different CPU architectures
93% of the binaries were new in VT (as of 2015/9/24)
Increase of attacks

Num. of IP addresses

IPs/month

2016

Jan: 35508
Feb: 55592
Mar: 78726
Apr: 121632
May: 242835
Jun: 407357
Jul: 380957
Source countries

Period: 2015/05/01 – 2016/02/21

- China 21%
- Turkey 12%
- Russia 9%
- Brazil 5%
- India 5%
- South Korea 5%
- US 4%
- Costa Rica 4%
- Vietnam 2%
- Argentina 2%
- Taiwan 2%
- Hong Kong 2%
- Mexico 2%
- Thailand 1%
- Malaysia 1%
- Israel 1%
- Philippines 1%
- Ukraine 1%
- Colombia 1%
- Spain 1%
- France 1%
- Guernsey 1%
- Poland 1%
- Others 15%
Log-Compromise Devices

Thank you to Prof. Michel van Eeten of TU Delft for providing ISP data.
**Telnet-based malware infection**

1. Dictionary attacks on telnet
2. Check and customize environment
3. Malware download
4. C2 commands
5. Various attacks

**Targets**

- Malware download server
- C2

- Attackers/infected devices
Dictionary used in 2015

root/root
root/admin
root/1234
root/12345
root/123456
root/1111
root/password
root/dreambox

root/root
root/admin
root/12345
root/123456
admin/root
...

admin/admin
admin/263729
admin/m6h3
admin/new/porra
admin/263297
admin/2m0r
admin/114
root/123

guest/guest
guest/12345
admin/
root/root
root/admin
root/
root/1234
root/123456
root/1111
root/password
root/dreambox
root/vizxv

root/root
root/toor
root/admin
root/user
...

Increase of id/password pairs

Increase of id/password pairs
→ Increase of targeted devices

Total #pairs

# new pairs

2015/11 2016/3 2015/6
Telnet-based malware infection

1. Dictionary attacks on telnet
2. Check and customize environment
3. Malware download
4. C2 commands
5. Various attacks

Malware download server
Binaries

Targets

Attackers/infected devices
Eg. Malware binary downloads

Binaries of MIPS, MIPSEL, ARM, PPC, SUPERH, MIPS16 are all downloaded and executed
Latest IoT malware

<Mirai (未来 = Future)>

• More than 500,000 IoT devices were infected by Mirai through telnet service.

  — Characteristics:
    • SCAN to 23/TCP, 2323/TCP
    • Dictionary Attack
    • Destination IP address = TCP sequence Number
    • Destination IP, Window size, Source port may be random

  — Source code of Mirai was uploaded to Hackforums and GitHub in September 2016 by Anna-senpai
【 Digression 】Anna-senpai?

- Anna-senpai was a Japanese animation
- Broadcasted from July to September in 2015.

[FREE] World's Largest Net: Mirai Botnet, Client, Echo Loader, CNC source code release

Yesterday, 12:50 PM (This post was last modified: Yesterday 04:29 PM by Anna-senpai.)

Anna-senpai
L33t Member

Preface
Greetz 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 all about scale and leverage. 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, 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.
The Attacker may be very OTAKU (Comic fanatic).
Further information on “Mirai”

DDoS Attacks

- Krebs on Security (16/9/20)
  - Akamai Service

- DNS of DYN (16/10/21)
  - Netflix
  - Twitter
  - Amazon

- Types of Infected:
  - Printer
  - Camera
  - Router
  - DVR and etc.

- Architecture used:
  - ARM
  - ARM7
  - MIPS
  - PowerPC
  - SH4
  - SPARC
  - X86
"Mirai" observed by Darknet
(by Destination IP address = TCP sequence Number)

Starting from 1st of August. After source code uploaded, scan was jumped up
Countries infected by Mirai from Source IPs

- Other: 49%
- VN: 15%
- BR: 15%
- TR: 8%
- IN: 5%
- Other: 49%

Countries infected by Mirai
After August 2016

- Other: 55%
- CN: 14%
- BR: 10%
- IN: 9%
- VN: 7%
- TW: 5%

Courtiers infected by IoT malwares
Before August 2016

- Other: 55%
- CN: 14%
- BR: 10%
- IN: 9%
- VN: 7%
- TW: 5%
Telnet-based malware infection

1. Dictionary attacks on telnet
2. Check and customize environment
3. Malware download
4. C2 commands
5. Various attacks

Targets

Malware download server
Binaries

C2

Attackers/infectected devices
Dinial of Service (DoS)

Cache DNS at ISPs

No resource

9a3jk.cc.zmr666.com?
elirjk.cc.zmr666.com?
pujare.cc.zmr666.com?
oiu4an.cc.zmr666.com?

Slow response

Auth DNS for “zmr666.com”

Infected devices
Propagation

Infected devices
The matching result is provided by Arbor Networks ASERT Japan
Two approaches to monitor attacks

- **Passive monitoring**
  Prepare network to monitor attacks and wait
  - Darknet monitoring
  - Honeypot

- **Active monitoring**
  Search for device/vulnerability/backdoors
  - Accessing Web, Telnet, FTP, etc to decide what devices they are
  - Checking for backdoor ports
  - Measuring clock skew for tracing individual devices
Inferring infected device

We check telnet/web banners and more to find out which devices are attacking us.
Examples of web interfaces of infected devices
Device categories

60+ categories are observed (top 20 listed below)

- DVR: 10734 IPs
- Router: 4856 IPs
- IP Camera: 1391 IPs
- Web Camera: 787 IPs
- Set-Top-Box: 430 IPs
- Modem: 411 IPs
- Network Video Recorder: 337 IPs
- Ethernet Over Coax Adaper: 206 IPs
- CPE: 206 IPs
- VoIP Gateway: 174 IPs
- Heat Pump: 60 IPs
- DVS: 20 IPs
- WiFi Extender: 19 IPs
- Personal Video Recorder: 15 IPs
- Hybrid Video Recorder: 11 IPs
- Environment Monitoring Unit: 10 IPs
- Peer-to-peer Communication Controller: 9 IPs
- IP Phone: 6 IPs
- Digital Attached Storage: 6 IPs

2015/5/01–9/30
Categories of Inferred Infected devices (2016.9)

- **Surveillance camera**
  - IP camera
  - DVR

- **Network devices**
  - Router, Gateway
  - Modem, bridges
  - WIFI routers
  - Network mobile storage
  - Security appliances

- **Telephone**
  - VoIP Gateways
  - IP Phone
  - GSM Routers
  - Analog phone adapters

- **Infrastructures**
  - Parking management system
  - LED display controller

- **Control system**
  - Solid state recorder
  - Sensors
  - Building control system (bacnet)

- **Home/individuals**
  - Web cam, Video recorders
  - Home automation GW
  - Solar Energy Control System
  - Energy demand monitoring system

- **Broadcasting**
  - Media broadcasting
  - Digital voice recorder
  - Video codec
  - Set-top-box

- **Etc**
  - Heat pump
  - Fire alert system
  - Medical device (MRI)
  - Fingerprint scanner

Devices are inferred by telnet/web banners
Infected devices in Japan (Daily count)

Increase since May 2016
Potential victims?

195.36.2.28 (static-028.mi.telnet.demosdata.it)
- TELNET-ITALY - TELNET S.r.l., IT (5392) - Italy
- 23/telnet
- autonomous_system.name: TELNET-ITALY
- autonomous_system.organization: TELNET S.r.l., IT

120.50.16.120 (NEW-ASSIGNED-FROM-APNIC-20-03-2008.telnet.net.bd)
- TELNET-AS-BD-AP - Telnet Communication Limited (38712) - Bangladesh
- 23/telnet
- autonomous_system.name: TELNET-AS-BD-AP
Other vulnerabilities?
Other vulnerabilities

- IoTpot implements following vulnerabilities exploited in the wild
  - DVR configuration leak
    Config files of Several DVR manufacturers can be accessed from WAN [7]
  - Backdoors on routers [8]
    Arbitrary code can be executed through backdoors of Chinese routers (53413/udp)
  - IP cameras accessible shodan, insecam [9]

Insecam

United States(4916)
Turkey(2392)
Japan(1555)
Italy(1107)
France(987)
Russian Federation(739)
United Kingdom(651)
Netherlands(604)
India(604)
Germany(329)
Sweden(290)
Spain(288)
Czech Republic(268)

Japan was No 3 (2016/9/15)
Honey IP cam at YNU
Access to honey cam

1) First access after 5 days from Germany
2) Confirmed the exposed ID/pass in the camera image is used for accessing other service of the honey cam
   → Not only machines but humans are watching
Honey cam was on Insecam!

Honey cam in YNU
Insecam attracts 1000+ times accesses

- After our honey cam is on Insecam, accessing hosts are 1000+ times more!

- 80% from Japan

People do not scan for cameras but simply look at those sites (insecam, shodan, etc)
Monitoring, analysis, alert system at YNU

- Passive monitors
- Active Monitors
- Analysis/Alert/Data Sharing

Other organizations (CERTs, ISPs, Universities, Security Vendors)

Feedback

Alerts
Monitoring, analysis, alert system at YNU

- Passive monitors
- Active Monitors
- Analysis/Alert/Data Sharing
  - Internet
  - Other organizations (CERTs, ISPs, Universities, Security Vendors)
  - Feedback
  - Alerts
More sensors!

Netherlands: Done
Japan: done

USA
UK
Germany
Spain
France
Thailand
India
Australia
Hong Kong
Singapore
China: Done
Taiwan: Done
Monitoring, analysis, alert system at YNU

Internet

Passive monitors

Active Monitors

Analysis/Alert/Data Sharing

Alerts

Feedback

Other organizations (CERTs, ISPs, Universities, Security Vendors)
Enhancement of active monitors

• With TU Delft team
  – Enriching device signatures to infer device manufacturers and models
  – Fingerprinting individual devices

• Usage of Censys, shodan data
Monitoring, analysis, alert system at YNU

- Passive monitors
- Active Monitors
- Analysis/Alert/Data Sharing
  - Other organizations (CERTs, ISPs, Universities, Security Vendors)
  - Feedback
  - Alerts

Internet
Analysis/Alert/Data sharing

• **Infra**
  – Big data handling infra, Use of cloud,

• **Analysis capabilities**
  – Sandbox/Static analysis
  – Vulnerability analysis

• **Alerting**
  – NISC, JPCERT/CC, KRCERT/CC, TWCERT/CC,

• **Countermeasures**
  – **Cleaning up of infected devices**, Patching, Penetration tools for IoT devices
Monitoring, analysis, alert system at YNU

- Passive monitors
- Active Monitors

Analysis/Alert/Data Sharing

Other organizations (CERTs, ISPs, Universities, Security Vendors)

Feedback

Alerts

Internet
We share samples, observation, insights, proxy sensors with more than 30 research institutes/organizations.
What can we learn from telnet-based infection?

It is technically easy to solve a problem of individual devices
Stop Telnet at any time before in use
If telnet is necessary, use better password

It is difficult to solve at mass
Various manufacturers, installers, users in different locations, no traces of devices after sales, too many of them, firmware updates never really done, aggressive info sharing with systems like censys and shodan
Summary

• Various IoT devices are infected and joining botnets, causing real-world problems like DoS.

• It is too optimistic to expect the problem will be solved by solo efforts of manufacturers as the problem is already too big.

• Need mechanism to find, trace, notify, clean-up, and keep patching these devices.
Thank you for listening

Implement & use Security *

Design Security *

Monitor & review Security *

Maintain & improve Security *