RSA®Conference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: SBX4-W2

No IOUs with IoT

Bryson Bort

Founder & CEO
SCYTHE
@brysonbort

Who has IoT devices in their office or home?

CES 2018

Honeywell
ShadeCraft
ROBOTICS
SUNFLOWER™
with other
INTEGRATE YOUR FAVORITE CONNECTED THINGS
good to know.
ShadeCraft

No IOUs with IoT

“The ongoing problem with all of these Internet-connected accessories is security, or the complete lack thereof.”

If it could be Internet connected... **IT WAS**

If it could be voice enabled... **IT WAS**

No IOUs with IoT

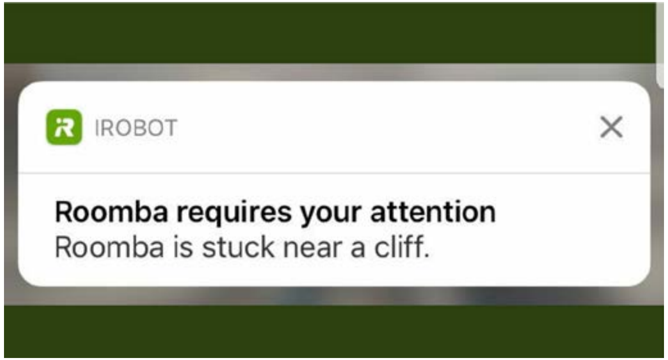
Today you will learn:

- IoT Threat Landscape
- IoT Attack Types
- How to defend / consider for your house and the enterprise

No IOUs with IoT

What is IoT?

Heard of IIoT?



Roomba requires your attention
Roomba is stuck near a cliff.

State of Affairs

Threat Landscape

- DDoS
- Ransomware
- Crypto-jacking

History of attacks

Mirai

- Factory defaults with script

Reaper / IoTroop

- N-Days: Netgear, Linksys, AVTech, D-Link like cell phones

GoScan SSH

7000 username/password pairs

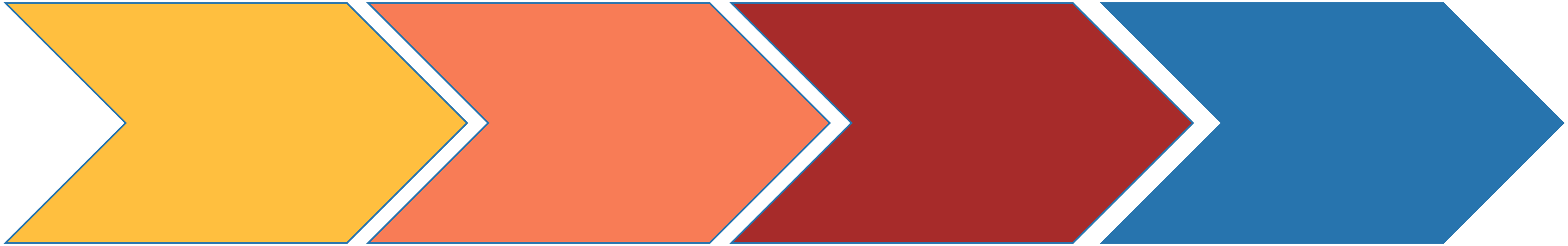
70 samples

Multiple architectures

- Open Embedded Linux Entertainment Center - Kodi derivative, Home Theater
- Open Source Media Center - Kodi derivative
- Raspberry Pi
- Jailbroken iPhones

No IOUs with IoT

Attack Lifecycle



Scan

Automate

Hijack

Execute

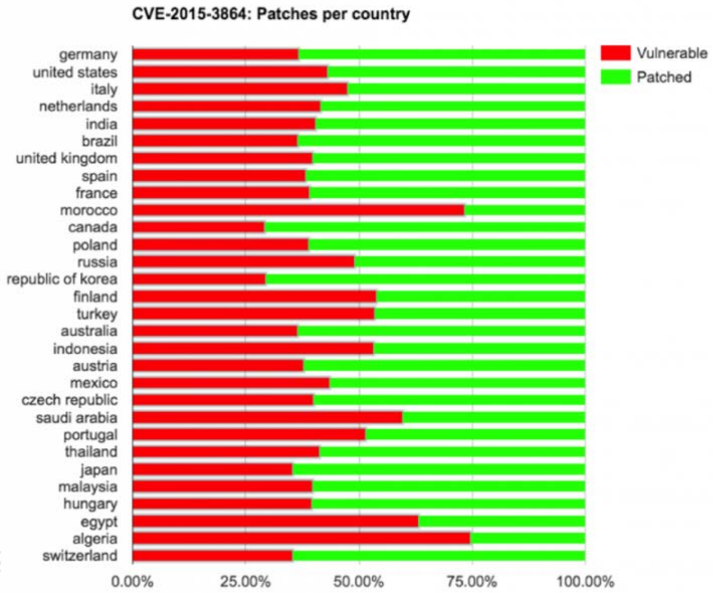
No IOUs with IoT

Patch History (phones)

Patch rates for Stagefright 9 months after discovery

Support Lifecycle

- Android 3 years
- Apple 5 years



https://www.miradore.cc

Howdy Neighbor

Howdy Neighbor

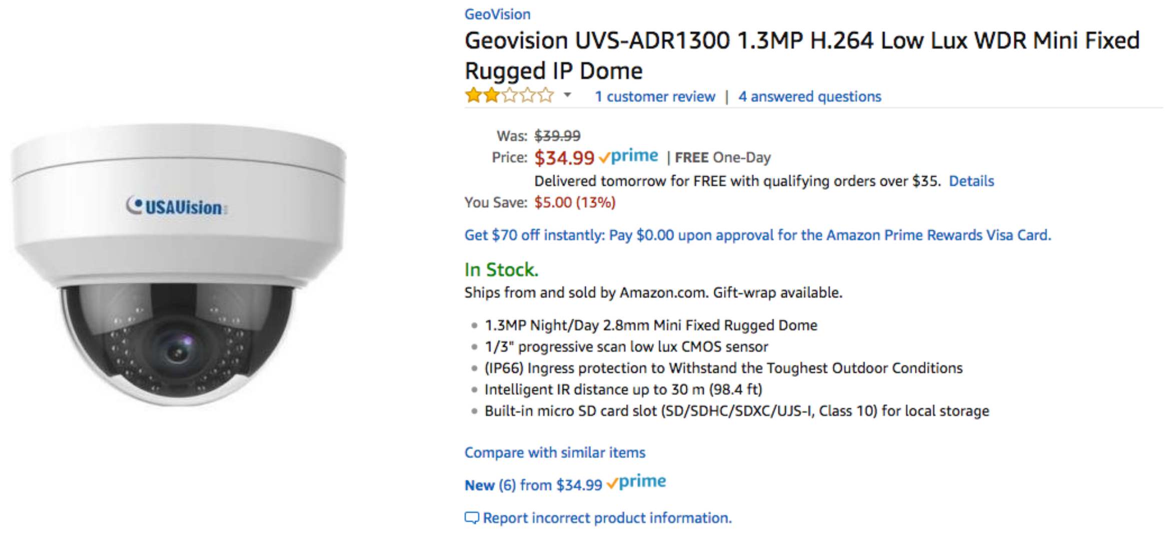
A model "smart" house

Interactive home products

- Webcams
- Smoke detectors
- Smart TVs
- HVAC systems
- Locks

No IOUs with IoT

- Alarm systems are expensive
- People want to secure their homes
- Cost is a major factor
- People purchase security cameras



GeoVision

Geovision UVS-ADR1300 1.3MP H.264 Low Lux WDR Mini Fixed Rugged IP Dome

★★☆☆☆ 1 customer review | 4 answered questions

Was: ~~$39.99~~

Price: $34.99 ✓prime | FREE One-Day

Delivered tomorrow for FREE with qualifying orders over $35. Details

You Save: $5.00 (13%)

Get $70 off instantly: Pay $0.00 upon approval for the Amazon Prime Rewards Visa Card.

In Stock.

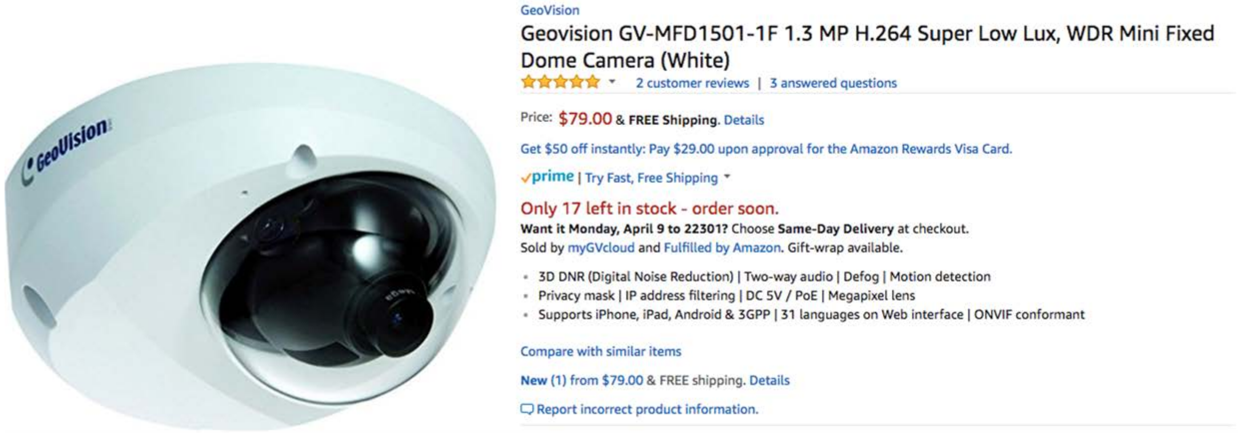
Ships from and sold by Amazon.com. Gift-wrap available.

- 1.3MP Night/Day 2.8mm Mini Fixed Rugged Dome
- 1/3" progressive scan low lux CMOS sensor
- (IP66) Ingress protection to Withstand the Toughest Outdoor Conditions
- Intelligent IR distance up to 30 m (98.4 ft)
- Built-in micro SD card slot (SD/SDHC/SDXC/UJS-I, Class 10) for local storage

Compare with similar items

New (6) from $34.99 ✓prime

Report incorrect product information.



GeoVision

Geovision GV-MFD1501-1F 1.3 MP H.264 Super Low Lux, WDR Mini Fixed Dome Camera (White)

★★★★★ 2 customer reviews | 3 answered questions

Price: $79.00 & **FREE Shipping**. Details

Get $50 off instantly: Pay $29.00 upon approval for the Amazon Rewards Visa Card.

✓prime | Try Fast, Free Shipping

Only 17 left in stock - order soon.

Want it Monday, April 9 to 22301? Choose **Same-Day Delivery** at checkout.

Sold by myGVcloud and Fulfilled by Amazon. Gift-wrap available.

- 3D DNR (Digital Noise Reduction) | Two-way audio | Defog | Motion detection
- Privacy mask | IP address filtering | DC 5V / PoE | Megapixel lens
- Supports iPhone, iPad, Android & 3GPP | 31 languages on Web interface | ONVIF conformant

Compare with similar items

New (1) from $79.00 & FREE shipping. Details

Report incorrect product information.

Insert Video 1 (Set-up camera)

No IOUs with IoT

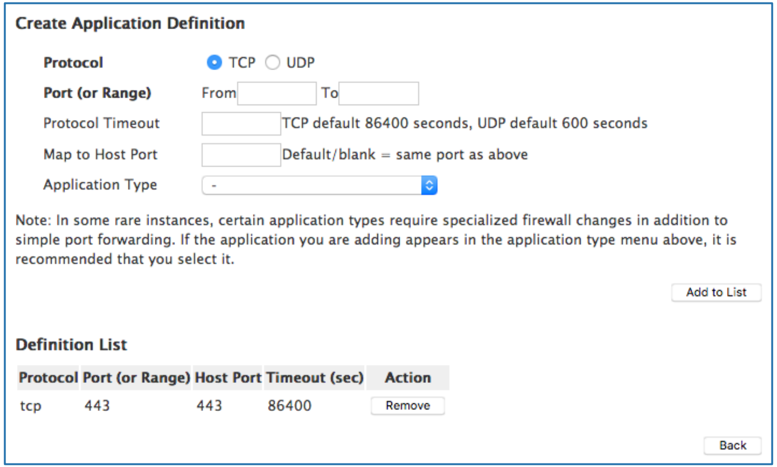
Demonstration:

- Recon
- Enumeration
- Compromise
- Pivot
- Steal
- DDOS

Recon and Enumeration

To access the camera, it needs to be connected to the Internet

Port forwarding on the router



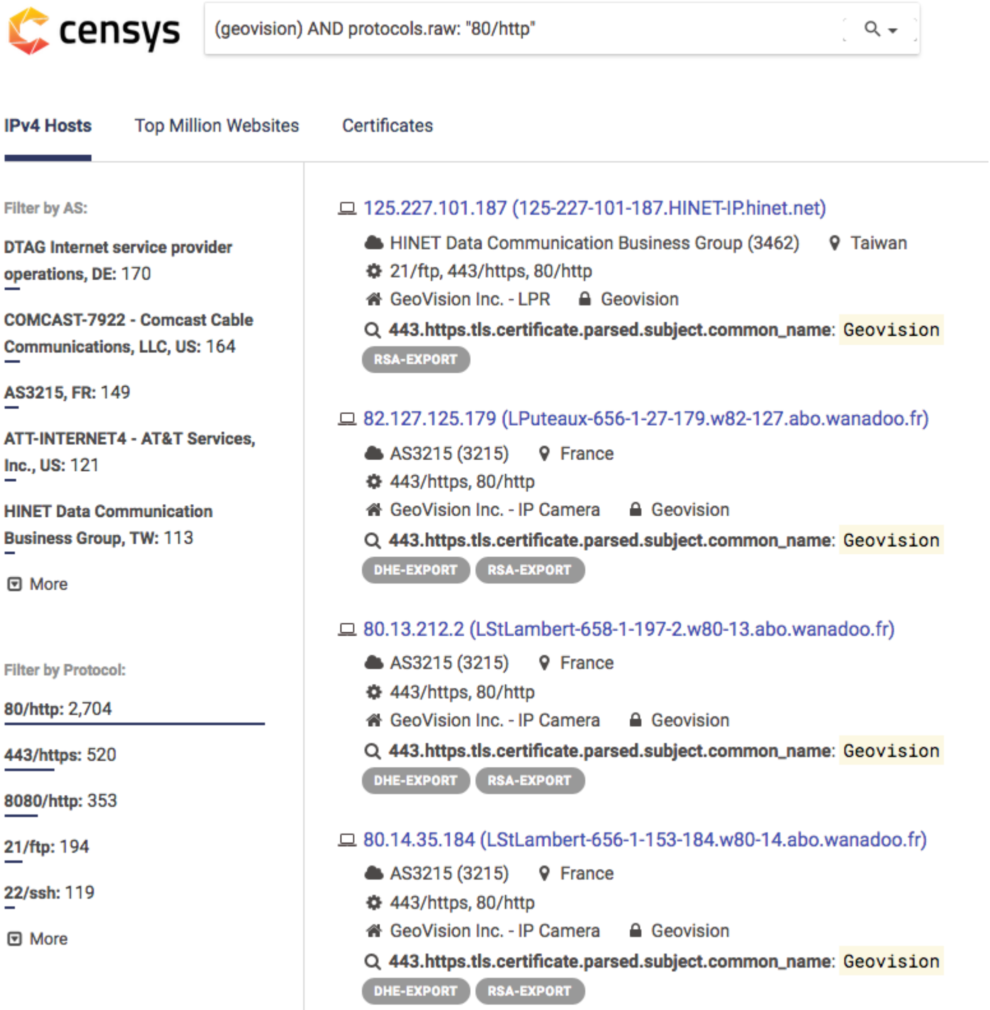
Create Application Definition

Protocol	● TCP ○ UDP
Port (or Range)	From ___ To ___
Protocol Timeout	___ TCP default 86400 seconds, UDP default 600 seconds
Map to Host Port	___ Default/blank = same port as above
Application Type	-

Note: In some rare instances, certain application types require specialized firewall changes in addition to simple port forwarding. If the application you are adding appears in the application type menu above, it is recommended that you select it.

Definition List

Protocol	Port (or Range)	Host Port	Timeout (sec)	Action
tcp	443	443	86400	Remove



censys

(geovision) AND protocols.raw: "80/http"

Filter by AS:

DTAG Internet service provider operations, DE: 170

COMCAST-7922 - Comcast Cable Communications, LLC, US: 164

AS3215, FR: 149

ATT-INTERNET4 - AT&T Services, Inc., US: 121

HINET Data Communication Business Group, TW: 113

More

Filter by Protocol:

80/http: 2,704

443/https: 520

8080/http: 353

21/ftp: 194

22/ssh: 119

More

125.227.101.187 (125-227-101-187.HINET-IP.hinet.net)
HINET Data Communication Business Group (3462) Taiwan
21/ftp, 443/https, 80/http
GeoVision Inc. - LPR Geovision
443.https.tls.certificate.parsed.subject.common_name: Geovision
RSA-EXPORT

82.127.125.179 (LPuteaux-656-1-27-179.w82-127.abo.wanadoo.fr)
AS3215 (3215) France
443/https, 80/http
GeoVision Inc. - IP Camera Geovision
443.https.tls.certificate.parsed.subject.common_name: Geovision
DHE-EXPORT RSA-EXPORT

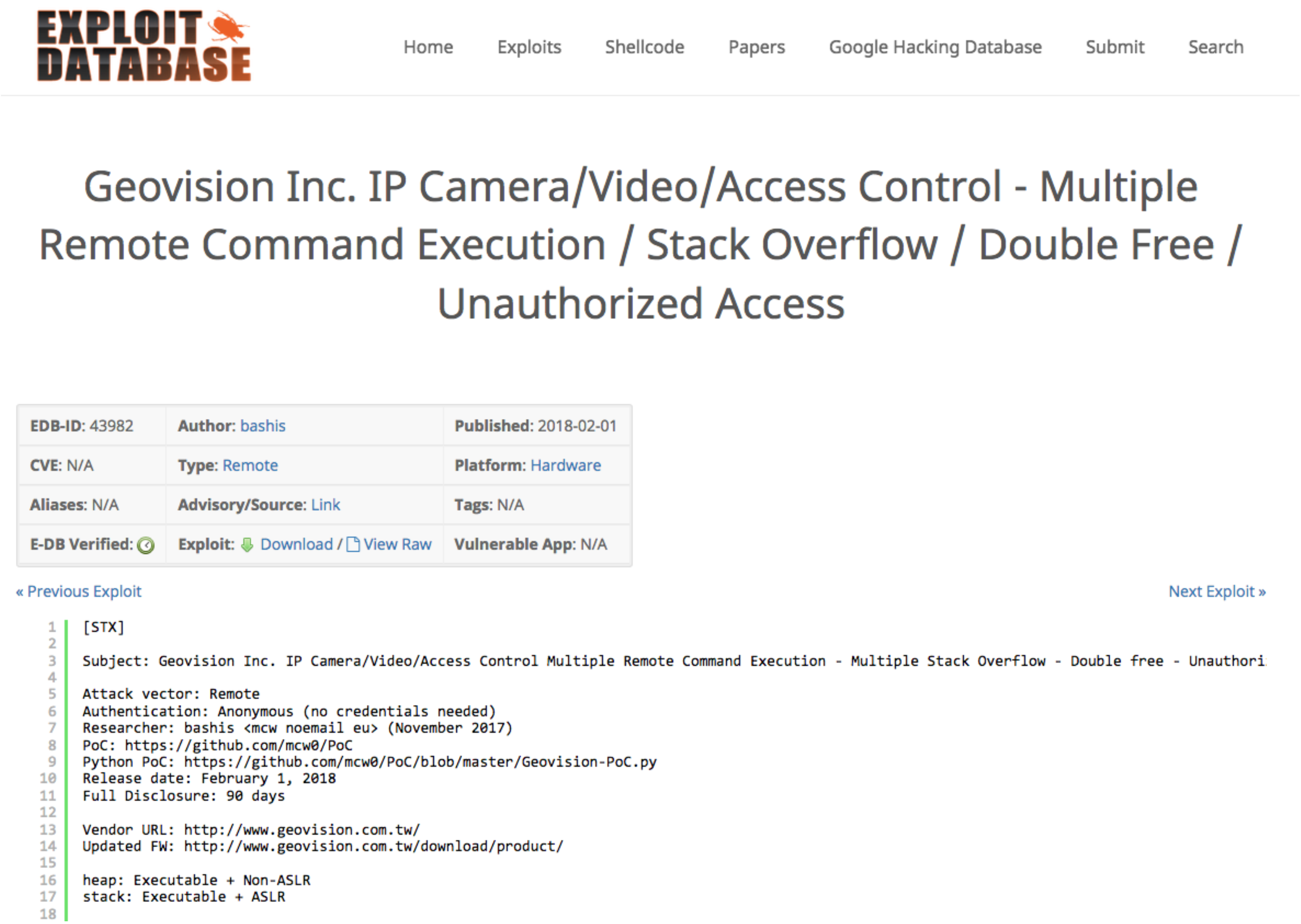
80.13.212.2 (LStLambert-658-1-197-2.w80-13.abo.wanadoo.fr)
AS3215 (3215) France
443/https, 80/http
GeoVision Inc. - IP Camera Geovision
443.https.tls.certificate.parsed.subject.common_name: Geovision
DHE-EXPORT RSA-EXPORT

80.14.35.184 (LStLambert-656-1-153-184.w80-14.abo.wanadoo.fr)
AS3215 (3215) France
443/https, 80/http
GeoVision Inc. - IP Camera Geovision
443.https.tls.certificate.parsed.subject.common_name: Geovision
DHE-EXPORT RSA-EXPORT

Zee Hackers

CC-BY MakeHackVoid / devdsp

Insert Video 2 (Find Cameras and Attempt Default Password)



Geovision Inc. IP Camera/Video/Access Control - Multiple Remote Command Execution / Stack Overflow / Double Free / Unauthorized Access

EDB-ID: 43982	**Author:** bashis	**Published:** 2018-02-01
CVE: N/A	**Type:** Remote	**Platform:** Hardware
Aliases: N/A	**Advisory/Source:** Link	**Tags:** N/A
E-DB Verified: ◷	**Exploit:** Download / View Raw	**Vulnerable App:** N/A

```
[STX]

Subject: Geovision Inc. IP Camera/Video/Access Control Multiple Remote Command Execution - Multiple Stack Overflow - Double free - Unauthori

Attack vector: Remote
Authentication: Anonymous (no credentials needed)
Researcher: bashis <mcw noemail eu> (November 2017)
PoC: https://github.com/mcw0/PoC
Python PoC: https://github.com/mcw0/PoC/blob/master/Geovision-PoC.py
Release date: February 1, 2018
Full Disclosure: 90 days

Vendor URL: http://www.geovision.com.tw/
Updated FW: http://www.geovision.com.tw/download/product/

heap: Executable + Non-ASLR
stack: Executable + ASLR

```

Insert Video 3 (Remote Admin Account Password Change/Hacker Access Camera + Camera Communicates Back to Attack Server, Presents Root Shell + Attacker Enumerates Network to Find More Devices)

No IOUs with IoT

Pivot

Scan the network again

Look for other devices

No IOUs with IoT

Steal

Can we obtain anything?

Videos, pictures, audio, or files???

No IOUs with IoT

DDoS attack

So what can I do?

- BEHIND a firewall
- Change Default Credentials
- Patches
- Segregate Wi-Fis

BONUS for SMB: UTM - Unified Threat Management

Call to Action

- Manufacturer Accountability
- Design for Security Lifecycle

References for more information

www.icsvillage.com

www.iotsecurityfoundation.org

www.iamthecavalry.org

Questions?

Thank you for your time!

Bryson Bort

@brysonbort

info@scythe.io