No IOUs with IoT

Bryson Bort

Founder & CEO
SCYTHE
@brysonbort
Who has IoT devices in their office or home?
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?
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

Attacker 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

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

Was: $59.99
Price: $34.99  ✔️prime | FREE One-Day
Delivered tomorrow for FREE with qualifying orders over $50. Details
You Save: $25.00 (13%)

Get $10 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/UHS-I, Class 10) for local storage

Compare with similar items
New (6) from $34.99  ✔️prime
☐ Report incorrect product information.

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

Price: $79.00  ✔️prime | Try Fast, Free Shipping *

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

Only 17 left in stock - order soon.
Want it Monday, April 9 to 23017? Choose Same-Day Delivery at checkout.
Sold by myGKcloud 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 | 8 languages on Web interface | ONVIF conformant

Compare with similar items
New (1) from $79.00  ✔️prime shipping. Details
☐ Report incorrect product information.
Insert Video 1 (Set-up camera)
No IOUs with IoT

Demonstration:
• Recon
• Enumeration
• Compromise
• Pivot
• Steal
• DDOS
No IOUs with IoT

Recon and Enumeration

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

Port forwarding on the router
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 - Unauthorized Access

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

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
manufacturer accountability

design for security lifecycle
References for more information

www.icsvillage.com
www.iotsecurityfoundation.org
www.iamthecavalry.org
Thank you for your time!

Bryson Bort
@brysonbort
info@scythe.io