
# I ALWAYS FEEL LIKE SOMEBODY'S WATCHING MY IOT

## An Analysis of Ring LLC. Data breaches

Fullstack Academy


2203-FTB-ET-CYB-PT

**FAB FIVE**

Joel Beck, Caleb Brackens, Mahmoud Nobakhti, Christopher Watson , Ashley Ricketson

WE WILL DISSECT SECURITY RISKS, DESCRIBE HOW MALICIOUS ACTORS WERE ABLE TO CARRY OUT THE ATTACK, AND INVESTIGATE WAYS RING ATTEMPTED TO MITIGATE ITS SECURITY ISSUES.

THE PURPOSE OF THIS PROJECT IS TO EXAMINE THE SECURITY VULNERABILITIES POSED BY DEVICES FROM RING LLC


# THERE ISN'T A MORE VIOLATING FEELING THAN HAVING YOUR PRIVACY INVADED

# IT'S UNDOUBTEDLY DISTURBING WHEN DEVICES DESIGNED TO PROTECT OUR PRIVACY ARE HACKED

Ring security devices, like so many entities that make up the "Internet of Things" (IoT), can be hacked. And if something can be hacked, chances are there is someone out there trying to do that right now. It's up to companies like Ring to stay ahead of the hacker game and keep their product safe.

# ATTACK VECTORS

Compromised Credentials

Brute Force

Poor Encryption

Third-Party Vendors

**POOR CREDENTIALS AND BRUTE FORCE**

Due to the frequency with which individuals reuse passwords and other login information, a hacker with a large set of stolen credentials will invariably find a number of accounts that they can breach

**POOR ENCRYPTION**

Previously, IoT security cameras sent data over the network via HTTP. This posed a security risk as HTTP traffic is unencrypted and, thus, insecure

**THIRD PARTY VENDORS**

If a would-be victim is tricked into installing a malicious app, it would allow the attackers to obtain authentication cookies. With these cookies, an attacker could access a user's account without their password, allowing the malicious app to steal PII

# THE BRUTE FORCE ATTACK

| | |
|---|---|
| Amount of People Affected | OVER 3,600 |
| Method Used | RING VIDEO DOORBELL CONFIG |
| How the Information Was Accessed | ON NULLEDCAST |

# THE PURPOSE OF RING IS TO HAVE SECURITY BUT THEY LEAVE ALL THEIR USERS EXPOSED

On a desktop web browser, someone who is logged in can watch historical, archived footage, meaning that if a hacker gains access to a user's account, the hacker can watch live and historical footage of a family inside their home without providing any additional identity verification.

Some of the unauthorized hacks were further publicized via the podcast NulledCast. NulledCast streams on Discord. On the NulledCast, hackers take over peoples' Ring and Nest smart-home cameras, then use the two-way talk feature to harass their unsuspecting owners.

Hackers share "Ring Video Doorbell Config" which was used to brute force attack Ring cameras. The config has a "High CPM," or high "check per minute," meaning it can test if a username and password allows access to a Ring camera quickly, until they get a hit.

# THE REAL - LIFE EXPERIENCES OF BEING SPYED ON

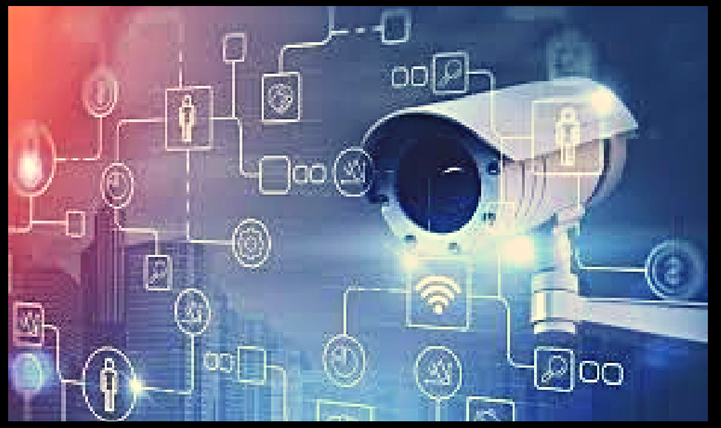

## DECEMBER 4TH, 2019

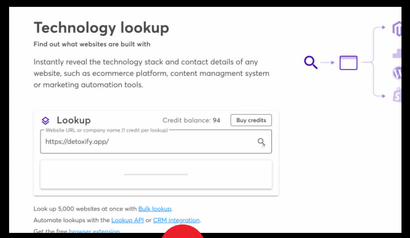
Ring cameras installed in a family's home began live-streaming, and played Tiny Tim cover of "Tiptoe Through the Tulips". A hacker had the ability to see, hear, and speak to an 8-year-old girl inside her own room. The hacker began shouting racial slurs and encouraging her to misbehave. He continued to say, "I'm your best friend. I'm Santa Claus. Don't you want to be my best friend?".

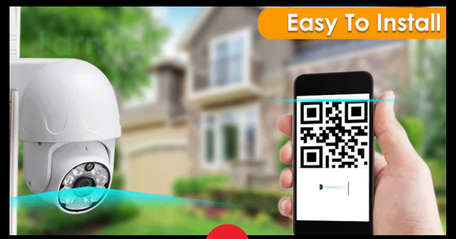
## DECEMBER 9TH, 2019

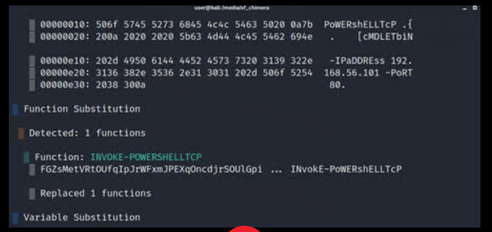
A family was interrupted by a voice laughing and shouting, "Ring support! Ring support!" A stranger had hacked their Ring system and was spying on them inside their home. The hacker then accessed their doorbell camera and told them, "I'm outside your front door." The voice also threatened the couple with "termination" if they did not pay a ransom of 50 bitcoin.

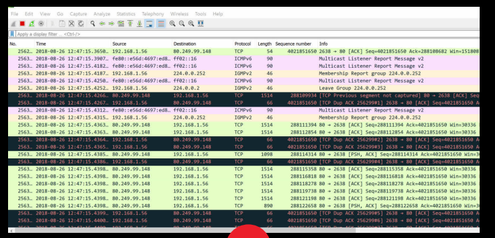
# TESTS PERFORMED





## TEST 1

Passive Reconnaissance

## TEST 2

Account Creation and Device Set-Up

## TEST 3

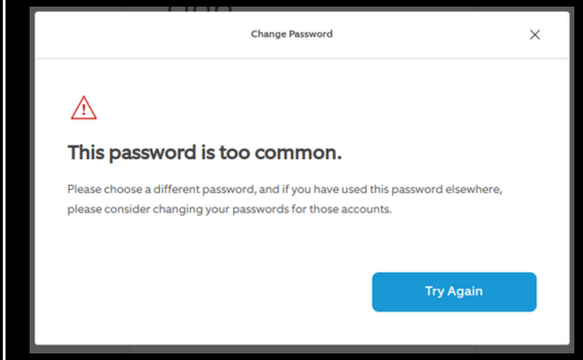
Scans: Port, Vulnerability & Web Content

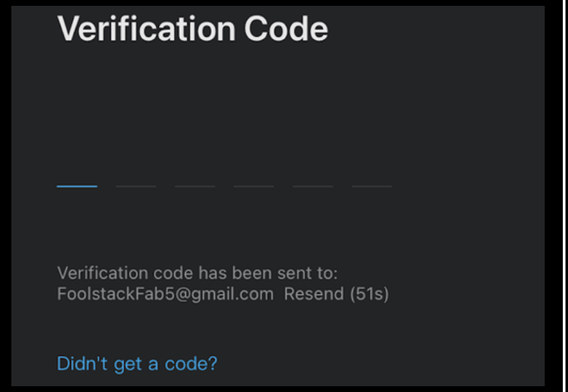
## TEST 4

Packet Sniffing

# WHAT'D WE FIND?

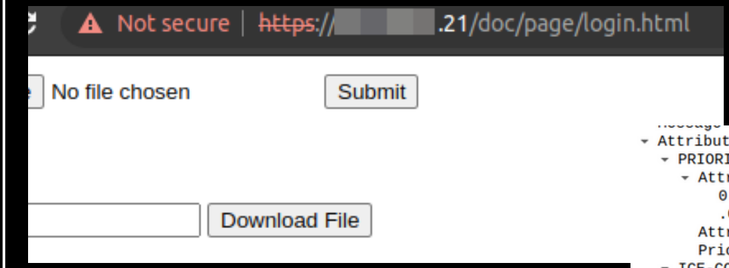
## SECURE PRACTICES



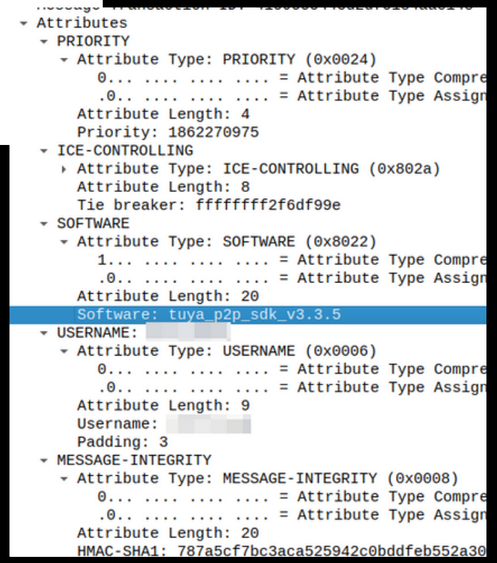




```
caleb@          :~$ sudo nmap -sS -p-          .17-21
Starting Nmap 7.80 ( https://nmap.org ) at 2022-08-26 13:56 CDT
Nmap scan report for          .17
Host is up (0.046s latency).
All 65535 scanned ports on          .17 are closed
MAC Address: 9C:76:13:          (Unknown)
```

## UNSECURE PRACTICES




```
Nmap scan report for          .21
Host is up (0.012s latency).
Not shown: 65525 closed ports
PORT      STATE SERVICE
443/tcp   open  https
554/tcp   open  rtsp
1300/tcp  open  h323hostcallsc
6060/tcp  open  x11
6061/tcp  open  x11
7000/tcp  open  afs3-fileserver
8012/tcp  open  unknown
8089/tcp  open  unknown
8699/tcp  open  vnyx
45936/tcp open  unknown
MAC Address: 54:2B:57:          (Night Owl SP)
```



# POTENTIALS FOR COMPROMISE

Obscure Security Transparency

Potential Malicious Apps

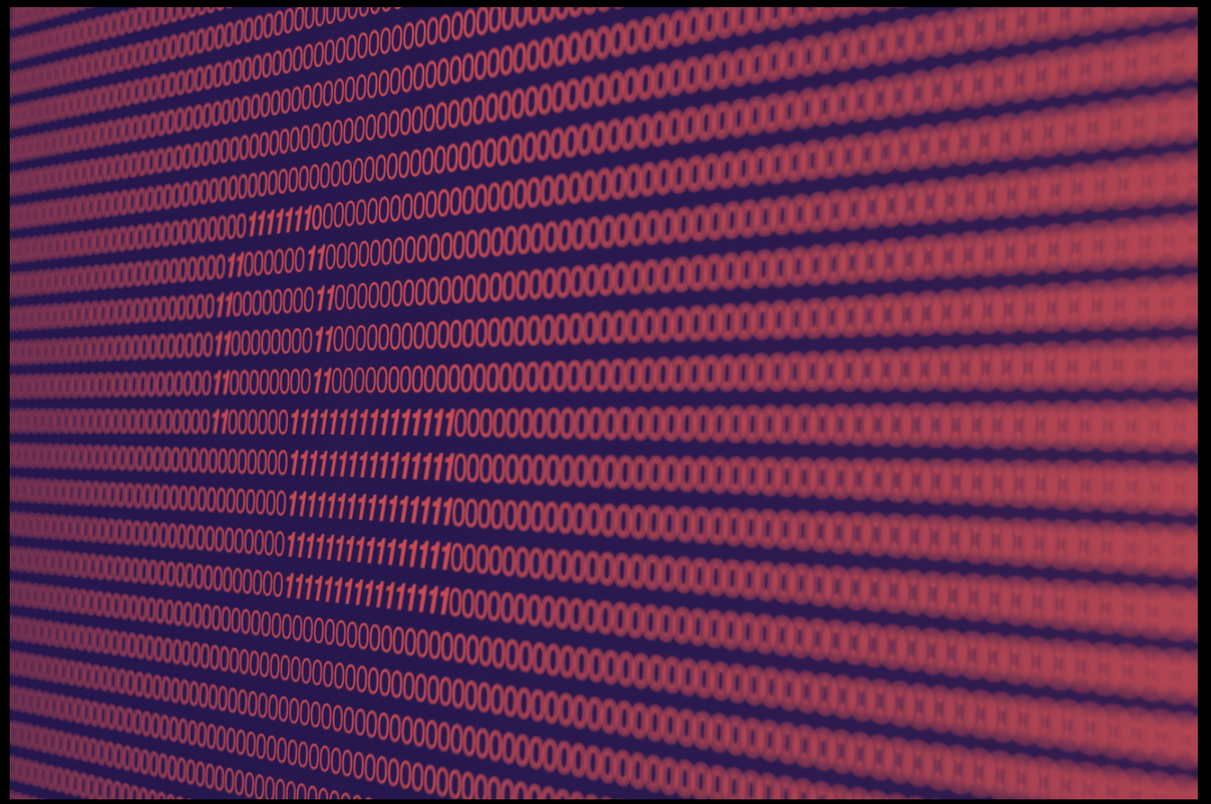
Incomplete Port Hardening

Vulnerable Services

Weak User Credentials

UDP Protocols

**OVERALL, RING PERFORMED WELL**
**THIS DOES NOT MEAN THE RING CAMERA DOES NOT HAVE VULNERABILITIES - ONLY THAT IT HAS BEEN PROPERLY SECURED AGAINST OUR SPECIFIC TESTS**



# STEPS TOWARDS MITIGATION

| INDUSTRY CHANGES | CONSUMER CHANGES | BOTH |
| --- | --- | --- |
| Constant application updates | Create Strong Password | Utilize Ring 2-Step Verification |
| Safeguards Against Malicious Apps | Switch passwords regularly | Delete Old Footage |
| Discontinue Sharing Customer Footage | Use separate passwords for different accounts | Strong Password Requirements |
| | Network Segmentation | |

# FINAL THOUGHTS

## WHAT HAVE WE LEARNED?

GREAT **STRIDES** HAVE BEEN MADE.

**RING HAS DONE THE MOST** TO PROTECT ITS IOT DEVICES FROM MALICIOUS ACTORS.

INDUSTRY MUST **REMAIN VIGILANT** IN STAYING AHEAD OF THE HACKER GAME.

CONSUMERS SHOULD **STAY INFORMED** ON HOW PROTECT THEIR OWN SECURITY.