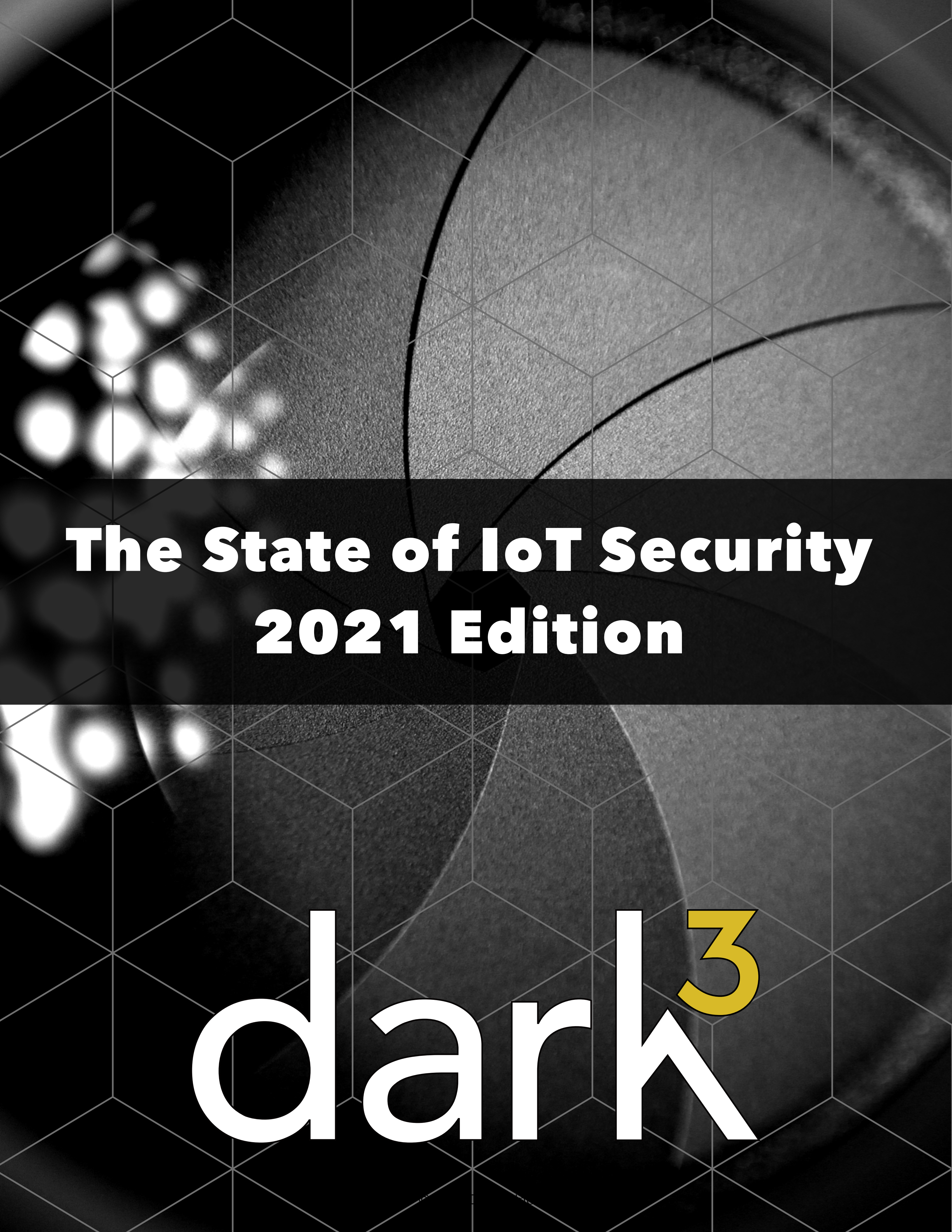


The State of IoT Security 2021 Edition

dark3

“Every IoT device we reviewed had a business connection to China and every product was observed communicating with infrastructure in China, without our permission and void of any transparency from the vendor.”

LETTER FROM THE CEO

More than two years ago, Dark Cubed published the first technical vulnerability assessment report on the "State of IoT Security." Since then, much has changed across the globe and much remains the same. As we reflect on our past research, one thing rings clear—it is necessary to revisit our past discoveries in order to comprehend what we have done in response to address our vulnerabilities and what we must do going forward.

In these two years, we have seen a global pandemic, a massive supply chain-related hack, passage of *The IoT Cybersecurity Improvement Act* here in the United States, and the discovery of a potential hardware supply chain attack involving motherboards and chipsets related to China and Supermicro. We have seen a number of great reports published on IoT risks related to business and the Enterprise, guidance from the National Institute of Standards and Technology (NIST) on securing IoT devices for the Federal Government, and countless news articles focused on privacy and security concerns related to doorbells, baby cameras, and more.

After all of the attention and focus on IoT security in the past few years, one would expect all major US retailers to take the security of consumer IoT devices more seriously, however, we have found that things are actually getting worse. We have more concerns now than we have ever had related to three key issues (1) the implementation of basic security engineering principles, (2) fatal flaws resulting in the leaking of your most personal moments, and (3) an increased role in the command and control of consumer IoT infrastructure in the United States by Chinese companies, surrogaates, subsidiaries, and an array of seemingly deliberately disguised enterprises.

We had hoped that our previous report would be a call to action to take action to protect the American consumer and our cybersecurity infrastructure, but we have not seen meaningful results. As a result, we are more focused than ever on raising our concerns to the general public through this report and will reveal, using facts and real-world observations, the extent to which retail IoT security is a leviathan living just beneath the surface that could cause significant financial and national security impacts in the near future.

As always, we thank you for taking the time to read our report and we very much look forward to your feedback.

Very Respectfully,

Vince Crisler
Founder & CEO

EXECUTIVE SUMMARY

The purpose of this study was to understand the changes that have occurred in the consumer Internet of Things (IoT) market since our last report a little over two years ago. The focus of the study was on several components of this supply chain that is resulting in the largest sensor grid in the history of the world that is getting deployed into every entryway, living room, and bedroom in the United States and is growing in complexity and capability daily.

The key components assessed during this study include:

- The mobile applications used to interact with these devices;
- The communications to and from the actual devices themselves; and,
- The infrastructure these devices communicate with in the cloud from your home network.

Our study did not include any of the following activities:

- We made no attempts to hack, reverse engineer, or otherwise compromise the hardware;
- We did not reverse engineer, brute force, or otherwise attempt to hack the software; and,
- We made no attempts to compromise or exploit related infrastructure components.

Our report is based on plain, simple, and obvious conclusions that can be drawn based on observing how these devices communicate when deployed in your house. This means that every observation or security issue we discovered should have been one of the first things seen by any, and we mean ANY, security-focused individual at any of the companies that produce or sell these devices. Even the most basic security review (if one is even performed) by a major retailer would reveal the issues or concerns we have highlighted here and SHOULD have resulted in some of the devices being deemed unfit for sale to a consumer.

We found:

- Every device had strong supply chain and business connections to China.
- Most devices had at least one network connection to a server based in China.
- Many devices failed basic security checks and had significant, basic vulnerabilities
- Most devices provide complete visibility into private images to anyone in the network path between your house and the IoT provider.
- Most of the Android applications are woefully insecure and sending data to China

In summary, we find it highly unlikely that the retailers are performing any meaningful security due diligence against the hardware, software, and infrastructure components related the IoT devices they are selling. We also strongly suspect that even if retailers are providing security requirements to their suppliers, they are likely being ignored.

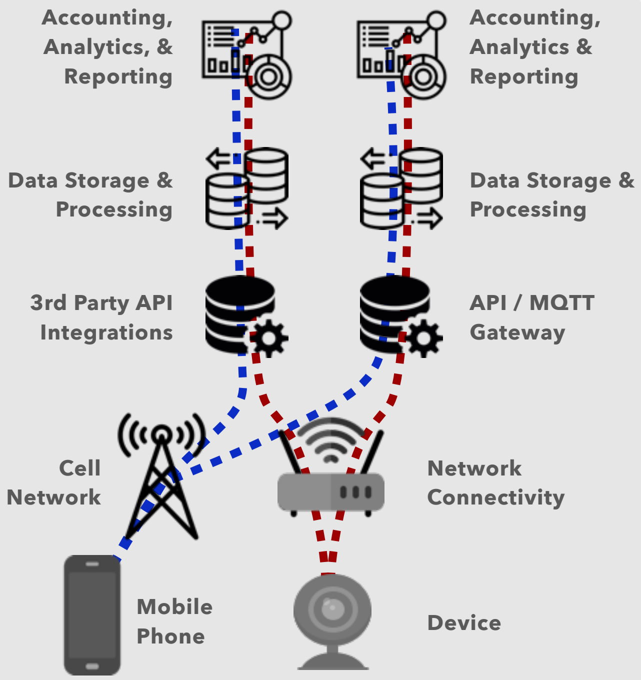
BEHIND THE SCENES

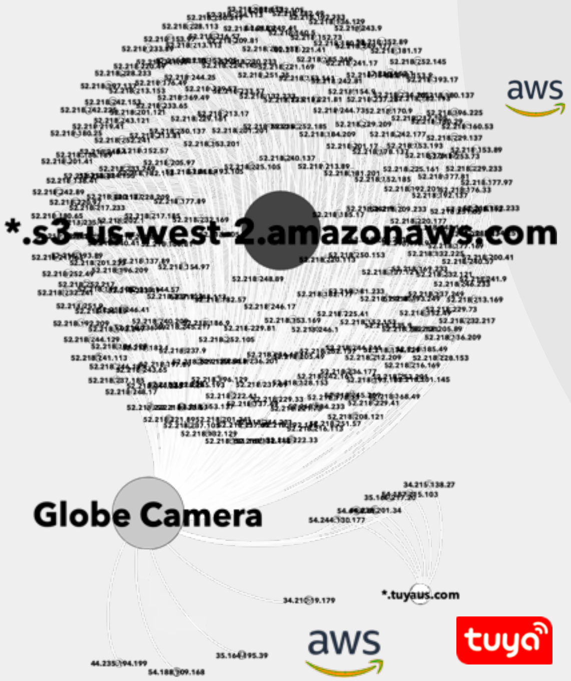
How IoT Works

Just like many technology devices it is easy to ignore the complexity behind the scenes when you plug in that small little camera to watch for someone trying to break into your car or protect your house while you are away. However, the simplicity of these devices covers up the complexity behind the scenes. It is in this complexity that risk is created if the architecture is not engineered with security in mind. The basic elements of an IoT architecture are displayed to the right.

As we can see, in every device we observed not only communications related to the company's own infrastructure, but also to third party applications for integrations with social media, payment platforms, advertising tracking, bug reporting, or other analytics. However, this abstraction simplifies things a little. The image below shows what these communications look like based on actual observed network traffic related to the Globe Camera.

The Technology Behind IoT


Accounting, Analytics, & Reporting
Accounting, Analytics & Reporting
Data Storage & Processing
Data Storage & Processing
3rd Party API Integrations
API / MQTT Gateway
Cell Network
Network Connectivity
Mobile Phone
Device



While the graph is a little overwhelming, we can easily see this camera utilizes Amazon's S3 Storage for data storage. We can also see communications with Tuya-based infrastructure for command and control as well as other services, which are hosted on Amazon's EC2 Platform. By performing this analysis on each of the devices we can produce a single graph of all devices to start to understand where relationships might exist based on shared infrastructure.

It is critical to understand that in the IoT space, the hardware device is only one small aspect of security. We found that the Android devices and the cloud infrastructure itself creates a signficant amount of risk for the consumer and are largely ignored in security discussions.

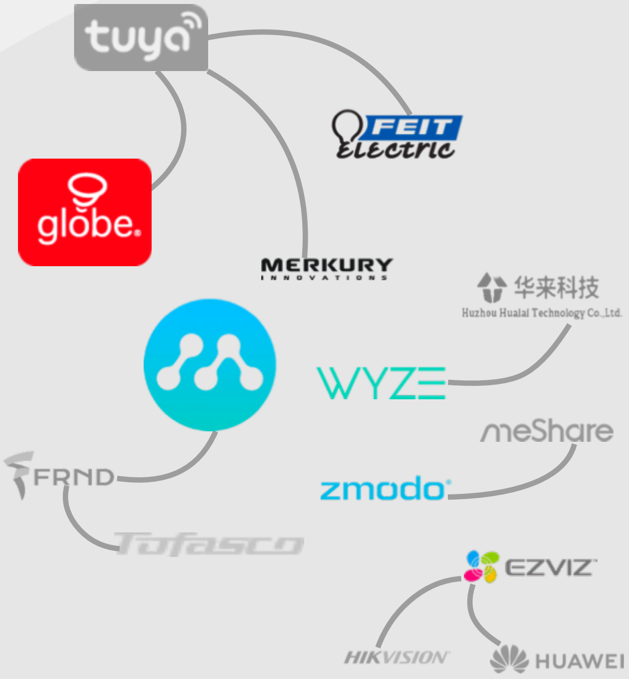
THE SETUP

Devices Reviewed

We purchased our devices at retail prices from major retailers. We focused on getting a representative sample of the consumer-grade IoT devices that appear to be popular items for consumers.

Given the attention devices from Amazon, Google, Ring, and others have received lately, we focused on the second tier of products, typically priced between $20 and $100. The devices we analyzed for our report are listed below.

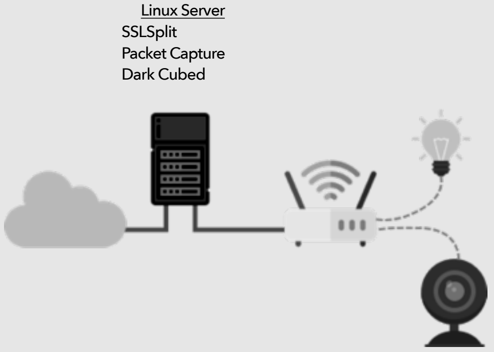
- EZVIZ EZC1C1D2 Camera
- FEIT OM100 RGB Lightbulb
- Globe Smart Indoor Security Camera
- Merkury A21 Smart LED Lightbulb
- Merkury MI-WW218 Smart Outlet
- Merkury Smart WiFi 720P Camera
- Momentum MOCAMIND2K Camera
- Wyze Cam Pan 1080p
- Wyze Cam V3
- Zmodo Pivot



Building on lessons learned from our previous report, an IoT device is never just about one brand. The image above shows connections between these devices and the companies connected with them based on business and technology-based relationships.

The Setup

We used a simple setup for our assessment. There is purpose in this simplicity: to prove a point. Assessing the security of these devices is not difficult. It can be accomplished using open source tools and a little bit of experience. Many assessments of IoT devices rely on complicated reverse engineering tactics, hit or miss brute forcing tactics, or hardware tear-downs. This is not one of those assessments. The most important message for retailers and consumers on our setup is that it would not cost retailers significant amounts of money or time to run some simple validations against the security of these devices or to ensure that the privacy of their consumers is being protected.



dark3 *Threat Analysis*

MobSF *Mobile App Review*

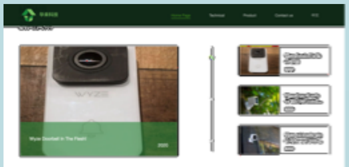
Malcolm *PCAP and Traffic Analysis*

THE COMPANIES

We covered Merkury in depth in a previous report and not much as changed here. The owners of Merkury Innovations are connected to a number of companies to include Targus Digital and appear to do a pretty signficant amount of business by connecting Chinese goods to the US Market. As before, we see they appear to be outsourcing all of their technology work to Tuya.

Based on our analysis, Feit Electric does appear to be a family run business within the Feit family as their website claims. Costco even ran a nice report on the business in a February 2016 version of *The Costco Connection*. While Feit focuses on developing and manufacturing the hardware, it is clear that they are outsourcing the infrastructre and application development to Tuya. Their applicaation is even signed by Tuya, indicating they likely developed it for Feit. One interesting finding is that when we originally setup the Feit lightbulb it automatically registered on the Globe application. This led to some additional testing where we found the Feit, Globe, and Merkury devices were fully interchangeable in the applications, revealing deep connections here that are not transparent to the user. Said another way, because Tuya is running the infrastructure, there is very little difference in these devices other than branding.

We already knew from our previous report of the connection between Wyze and Hualai. Visiting the Hualai website continues to show the connections at play here with the Wyze devices getting "News" postings on the Hualai website. (See: https://www.hualaikeji.com/)



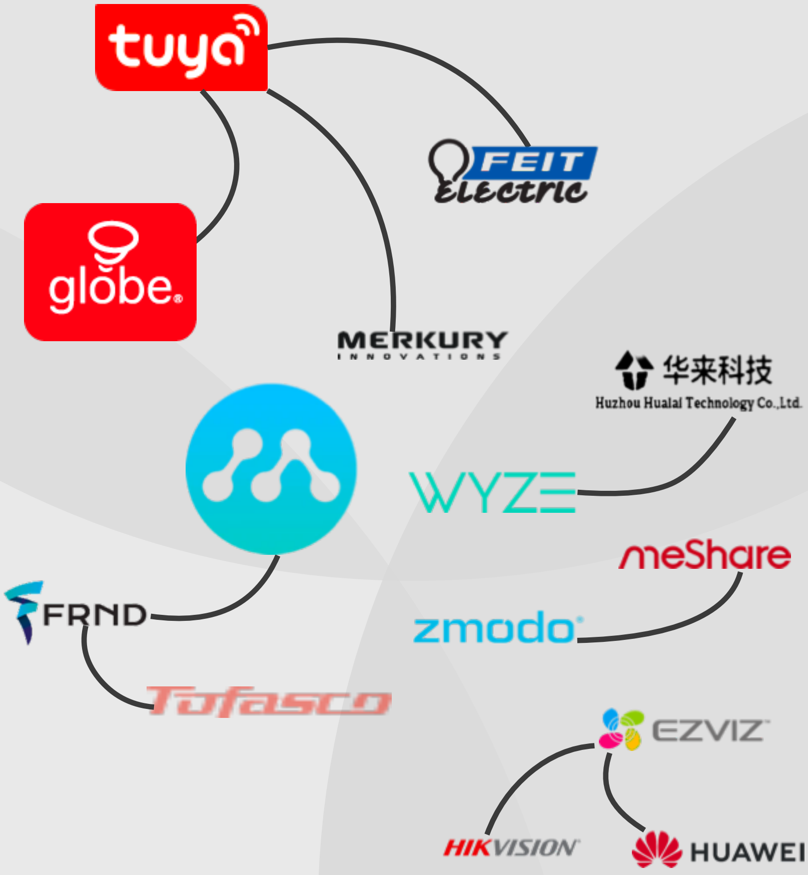
As we also mentioned in our previous report, the name of the Android application remains com.hualai, indicating some form of deeper connection on the development side as well.

What remains concerning about Wyze is their "Story" which focuses on building an innovative team with founders that came from Amazon. This founding story makes it feel like they are creators and designers instead of just repackaging Chinese products for the US Market.

Globe Electric advertises a long history on their website going back to their founding in 1932 in Montreal, Canada. The company has expanded globally with offices in the United States and Hong Kong and advertises the establishment of a wholly owned Subsidiary Keystore International based out of Hong Kong to take advantage of a closer relationship with "the manufacturing base."

All this being said, it is relatively clear that Globe has partnered with Tuya as a platform provider for their IoT Infrastructure.

This being said, we did observe unique communications from this device when compared to the other Tuya devices. These communications were all to IP addresses in the Alibaba Cloud, indicating some other form of command and control which we were unable to attribute but is worth further investigation.



ZModo remains a curious outlier in this group. ZModo's headquarters is clearly listed a in China, but their infrastructure points to just a few IP addresses associated with servers on Comcast in the Chicago area.

We can see that their storage platform relies on meShare, which is advertised to be an IoT platform, however meShare only reports 3 employees on Dun & Bradstreet.

There are also business connections to EP Technology Corporation and EP Surveillance Corporation that all appear to be tied in with common executives and shared addresses. If we had more time to dig here, I am sure some interesting stories could be found.

The EZVIZ story on their website does not align with what we discovered. They describe a small team startup story, when in actuality they are spinout of a large Chinese company, Hikvision.

This is clearly articulated on the Hikvision website, even though it is never stated on the EZVIZ website. (see: https://us.hikvision.com/en/about/about-hikvision-north-america)

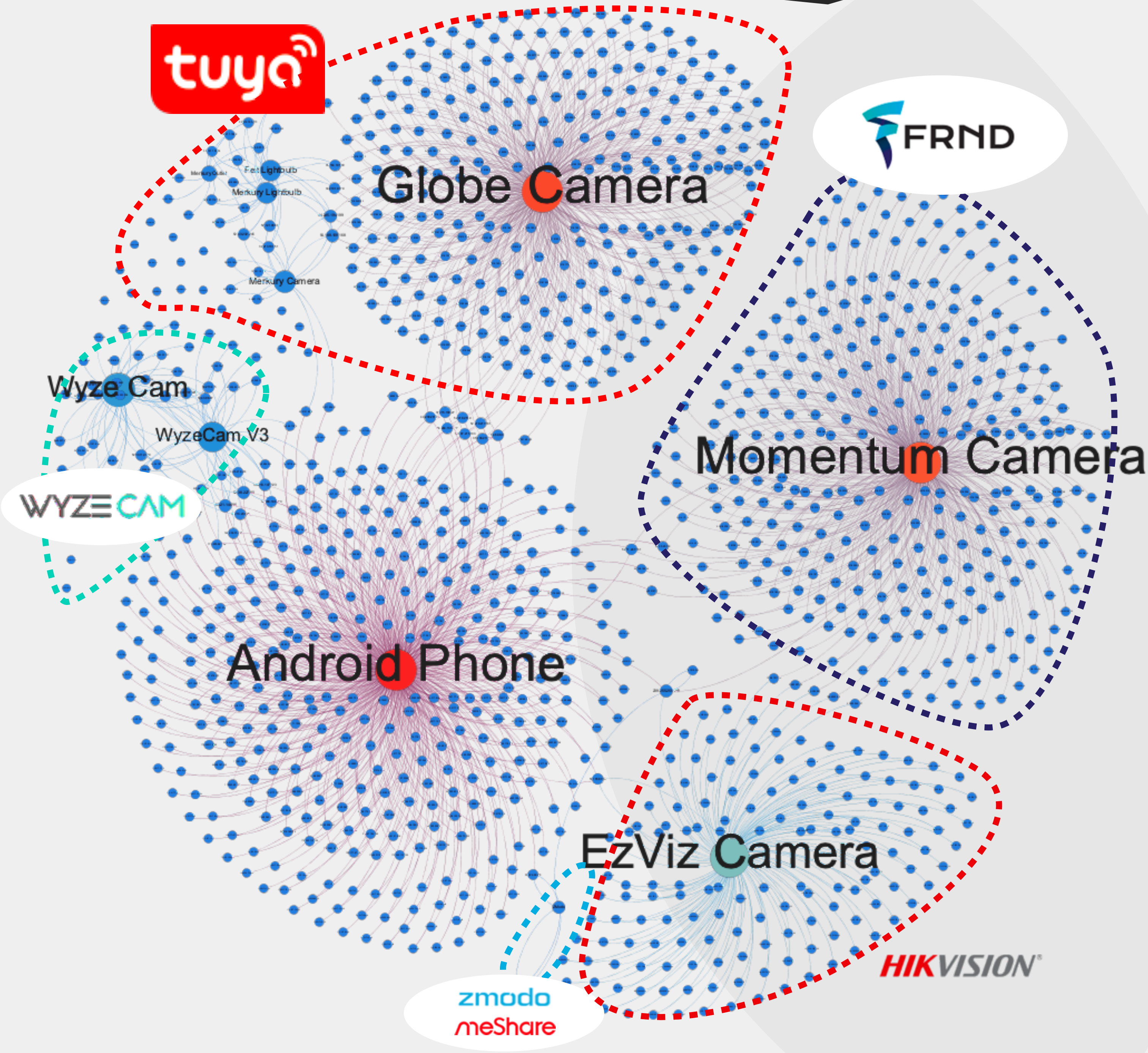
We also clearly see a strong relationship with Huawei in the codebase for their Android Application. It is interesting to note that both Hikvision and Huawei are subject to a ban on procurement from the US Government, but these devices, hidden behind the EZVIZ name remain on the shelves of major retailers.

The Momentum camera remains associated with Apollo Tech USA. However after some digging we found some interesting connections between Apollo Tech USA and a company GD International Inc. which we will come back to later.

It is also clear that the company has changed infrastructure providers since our last review and is now associated with a company FRNDTech. What is fascinating here is that we found a Payrcheck Protection Program result for FRNDTech reporting just a single employee with a loan for just $16,718. Coming back around to GD International, we found that they share a phone number record in common with FRNDTech, making an interesting triangle between these two companies and Apollo Tech USA.

After digging, we found that the domain name for FRNDTech was actually purchased by Tofasco of America. Tofasco just happens to have very strong ties back to China and is primarily known for sourcing Chinese goods (think chairs, tables, sporting equipment) for large retailers such as Costco and Walmart. We find it very concerning that this appears to be an attempt to hide connections between companies from the consumer.

A BIRD'S EYE VIEW



This graph represents every communication we observed between the tested devices, the Android Phone with the associated applications installed, and their related infrastructures. This graph became our "Source of Truth" for understanding how devices are connected behind the scenes and drives the rest of our report. For example, we clearly see that Tuya is behind the Globe, Merkury, and Feit Electric devices, while Momentum is associated with FRNDTech and EZVIZ with Hikvision.

MAN-IN-THE-MIDDLE

About This Technique

The man-in-the-middle attack or MiTM is a pretty simple concept. Basically, we put a device in between the IoT device and the server it is talking to and try to listen in. The communications should be encrypted and often are. However, if the IoT device is poorly configured, this encryption can be rendered useless through the simple of use of a fake certificate. Our device in the middle tells the IoT device that it is the server it is trying to talk to, and then sends that information on to the destination while reading everything that goes on. This is a relatively easy attack to prevent for any security minded company, but just like our last report, we still see devices that fall for this attack. For this testing, we used an old tool called SSLSplit that can easily be installed and up and running in less than five minutes.

The Globe camera easily gave up its secrets, which is interesting because the Merkury camera did not. Even though both are on the Tuya platform, there is something different going on here. In addition to being able to capture the images right off the camera, we see other senstive information such as AWS tokens for the upload of data, device IDs, and other data that could enable us to get access to more data if we put some effort into it.

```
{"result":{"bucket":"ty-us-storage30","endpoint":"s3.us-
west-2.amazonaws.com","pathConfig":{"logPath":"/[REDACTED]/log","detectPath":"/
[REDACTED]/detect"},"msgType":1,"provider":"s3","sk":"[REDACTED]","
expiration":"2021-03-16T21:22:00Z","ak":"[REDACTED]","region":"us-west-2","token":
[REDACTED]
```

In our previous report, Zmodo was the worst of the bunch in terms of information revealed and we see not much has changed. In addition to intercepting images from the camera, we also got a bunch of other information such as visibility into configuration of the device being sent to zmodo, encryption keys, and much more. We also found a number of examples of commands being sent to and from the device using POST commands, meaning an attacker could interact with your device without your knowledge. See below for a signficant finding related to this issue.

```
{"result":"ok","addition":"[REDACTED"],
devconn_port":"6102","session":6000,"devconn_address":"50.226.99.220","img_addre
ss":"uimage.meshare.com","heartbeat_interval":"90","timestamp":1598377393,"encry
pt_key_id":"["REDACTED],"encrypt_key":"[REDACTED]"}

{ "device_channel": "1", "device_ionum": "0", "device_model": "SD-H2002",
"device_version": "V6.4.0.1;V6.4.0.1;V6.4.0.1;V6.4.0.16", "device_capacity":
"1493310209", "device_extend_capacity": "1861032823", "temperature_channel":
"1", "humidity_channel": "1", "resolution": "{ \"HD\": \"1920*1080\", \"SD\":
\"640*480\", \"LD\": \"320*240\" }", "aes_key": "[REDACTED]' }
```

SIGNIFICANT SECURITY RISK FINDING

In our testing we found an item of significant concern related to the Zmodo camera. Based on our analysis, the camera uses a simple GET request to a server, https://dev.meshare.com. This request includes a "physical_id" for the device and requires no authentication or special codes. In response, the requester is provided with details on a meshare server to post images to along with an encryption key. We found that by changing the physical_id we received different responses with respect to encryption keys.

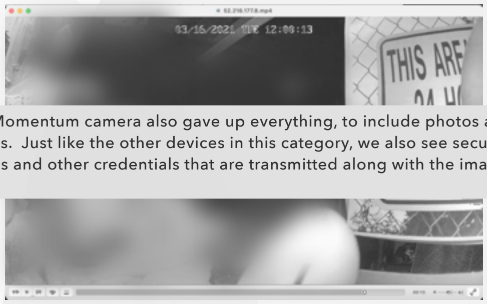
Based on what we have seen, we think this issue has the potential to allow an attacker to decrypt any image stored on the meshare servers.

REQUEST

```
https://dev.meshare.com/[redacted]?physical_id=[redacted]
```

RESPONSE

```
{"result":"ok","addition":"[REDACTED]","
devconn_port":"6102","session":6000,"devconn_address":"50.226.99.220
","img_address":"uimage.meshare.com","heartbeat_interval":"90","time
stamp":1615956303,"encrypt_key_id":"[REDACTED]","encrypt_key":"[REDA
CTED]"}
```



The Momentum camera also gave up everything, to include photos and videos. Just like the other devices in this category, we also see security tokens and other credentials that are transmitted along with the image.

```
PUT /rfprods3.frndtech.com/10890/CI2K-[REDACTED]/1/notify/
2021-03-16/1615921086693 HTTP/1.1
Host: s3.us-west-2.amazonaws.com
User-Agent: Mozilla/4.0 (Compatible; s3; libs3 4.1; Linux mips)
Accept: */*
Content-Length: 15673
Content-Type: application/octet-stream
Authorization: AWS4-HMAC-SHA256 Credential=[REDACTED]/us-west-2/s3/
aws4_request,SignedHeaders=content-type;host;x-amz-content-sha256;x-amz-
date;x-amz-security-token;x-amz-server-side-
encryption,Signature=[REDACTED]
x-amz-server-side-encryption: AES256
x-amz-date: 20210316T185806Z
x-amz-security-token: [REDACTED]
```

Wyze was an interesting one. We were unable to intercept any communications on the V3 camera, which is a good sign. However, on the original camera, we saw some interesting traffic. While we weren't able to capture any images, we did capture some certificates related to their infrastructure, which should be concerning to the company. These certificates appear to be the private key associated with the device and used for future encryption. This means, once you have this private key, you can see everything that happens. There is a chance we are mistaken here, but anytime we see BEGIN RSA PRIVATE KEY we get concerned. To take matters further, we see them using temporary credentials for downloading files, however we were able to replicate these commands to change the date on the credentials and download the file again at a later date.

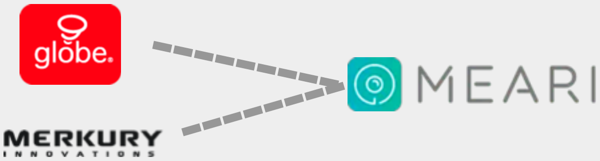
```
GET /iot_cert_files/client/wyzecp1_jef/[redacted]-private.pem.key?X-Amz-
Expires=1200&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=[redacted]/20210222/
us-west-2/s3/aws4_request&X-Amz-Date=20210222T192154Z&X-Amz-SignedHeaders=host&X-Amz-
Signature=[REDACTED] HTTP/1.1
Host: wyze-iot.s3-us-west-2.amazonaws.com
Accept: */*

HTTP/1.1 200 OK
x-amz-id-2: [REDACTED]
x-amz-request-id: [REDACTED]
Date: Mon, 22 Feb 2021 19:21:56 GMT
Last-Modified: Fri, 20 Mar 2020 17:56:56 GMT
ETag: "[REDACTED]"
Accept-Ranges: bytes
Content-Type: application/octet-stream
Content-Length: 1679
Server: AmazonS3

-----BEGIN RSA PRIVATE KEY-----
[REDACTED]
-----END RSA PRIVATE KEY-----
```

DEVICE CONNECTIONS TO CHINESE INFRASTRUCTURE

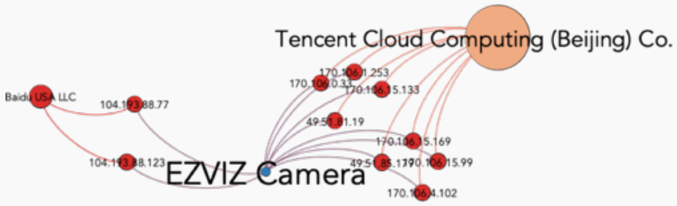
Tuya cameras connected to Chinese company Meari for a license validation process



3rd.meari.com.cn/device/license/third/validation?

It is clear that the Globe and Merkury cameras are simply rebranded Meari devices. Even worse, they still phone home to infrastructure in China when first powered up.

EZVIZ Camera regularly communicates with Tencent Cloud and Baidu



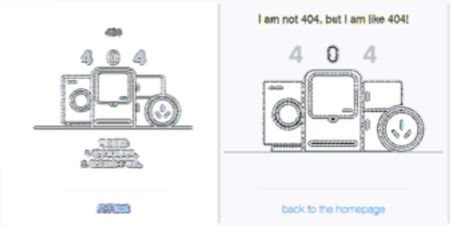
While other devices primarily communicated with AWS infrastructure, the EZVIZ camera, associated with Hikvision and Huawei regularly communicated with a number of servers related to Tencent and Baidu.

Concerns with Data Segregation in Tuya's Infrastructure

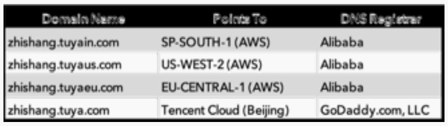
We saw a number of warning signs when mapping out the infrastructure utilized by Tuya that their US-based infrastructure is only a symbolic gesture at segregating data.

```
Server certificate
subject=C = US, ST = California, L = San Jose, O =
Tuya Global Inc., CN = *.tuyacn.com, CN =
*.tuyaeu.com, CN = *.tuyarf.com, CN =
*.tuyajp.com, CN = *.tuyain.com, CN =
*.tuyaas.com, CN = *.tuyaaf.com, CN =
*.tuyasa.com, CN = *.wgine.com, CN = *.tuya-
inc.cn, CN = *.tuyaus.com, CN = *.tuya.com, OU =
Tuya, emailAddress = iot_world@tuya.com,
subjectAltName = *.tuyaus.com, subjectAltName =
*.tuyacn.com, subjectAltName = *.tuyaeu.com,
subjectAltName = *.wgine.com, subjectAltName =
*.tuya-inc.cn, subjectAltName = *.tuyajp.com,
subjectAltName = *.tuyain.com, subjectAltName =
*.tuyaas.com, subjectAltName = *.tuyaaf.com,
subjectAltName = *.tuyasa.com, subjectAltName =
*.tuyarf.com, subjectAltName = *.tuya.com
```

We found wildcard certificates that could be used for all related infrastructure, to include servers in China, Europe, and the US. This is lazy at best, but more likely points to concerning questions around data segregation.



A US-based AWS server provided a 404 error in Chinese when browsing to the IP address. Browsing to the related domain name on that server, gave a 404 error in English.



Domain Name	Points To	DNS Registrar
zhishang.tuyain.com	SP-SOUTH-1 (AWS)	Alibaba
zhishang.tuyaus.com	US-WEST-2 (AWS)	Alibaba
zhishang.tuyaeu.com	EU-CENTRAL-1 (AWS)	Alibaba
zhishang.tuya.com	Tencent Cloud (Beijing)	GoDaddy.com, LLC

We found numerous examples of copy and paste infrastructure such as shown above. For what it is worth, based on a few attempts to translate Zhishang, we found it translates to the ideas of IQ, supreme, paramount, or "above all else."

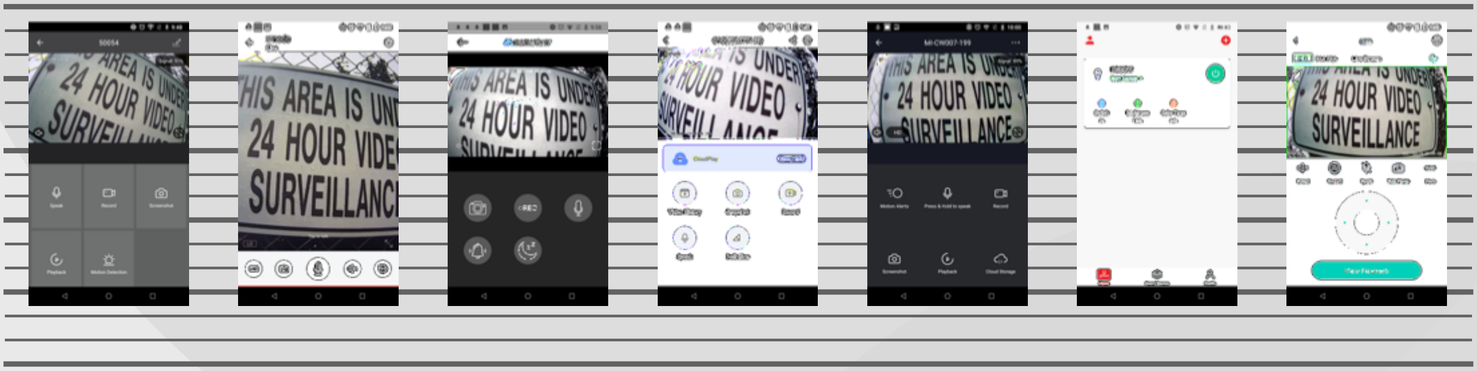
These are just a few examples of the large number we found where it is clear that the separation between Tuya's global infrastructure is not as clear as they make it out to be. ***If retailers are asking the question "Where are your servers located?" they are completely missing the point.*** The real issue here is getting visibility and transparency into how the data is used and where it goes once it has been collected. It is plainly obvious here that Tuya is only focused on the image of data staying in the US versus really caring about data privacy and security.

MOBILE APPLICATIONS

Why care about the mobile applications?

While connections from the hardware devices may seem the most important, we found that the mobile phone applications should receive just as much attention, if not more. The lightbulb is in a fixed location in your house and has minimal functionality, but to turn that lightbulb on and off you have to install an application on a device that goes with you everywhere and has access to your entire life...and most of the ones we looked at are horribly insecure and every single one had connections to China.

The Lineup



		Z	momentum		ee	globe	WYZE
APPLICATION PERMISSIONS REQUESTED	19	29	20	34	17	21	45
TRACKERS REPORTED BY EXODUS PRIVACY & MOBSF	Google	Google (x5) Facebook (x3)	Bugly Google	Facebook (x3) Flurry Google (x4)	AutoNavi Facebook (3) Tencent Umeng	Google (x5)	Facebook (x4) Google Braze Segment
SECRETS HARDCODED INTO APPLICATION	"umeng_key" : [redacted] "umeng_secret" [redacted]				"umeng_key" : [redacted] "umeng_secret" [redacted] "googleAppKey" : "749461155379-hfecsbl0mggs "googleAppSecret" : "749461155379-hfecsbl0mg		
CHINESE INFRASTRUCTURE	a.app.qq.com airtakeapp.com (x2) tuyacn.com (x5) smartapp.tuya.com	mob.com (x3) up.sharesdk.cn	android.bugly.qq.com	api.map.baidu.com appgallery.cloud.huawei.com ys7.com (x27)	a.app.qq.com airtakeapp.com (x2) tuyacn.com (x5) smartapp.tuya.com	a.app.qq.com airtakeapp.com (x2) tuyacn.com (x5) smartapp.tuya.com	iot.espressif.cn wyze-static-temperature-ex.s3.cn-north-1.amazonaws.com.cn

Bottom Line: We often see IoT security discussions focused on the hardware, the actual camera or lightbulb, however **it is crystal clear that to truly assess the security of these devices one must look at the device, the device-to-cloud connections, the cloud infrastructure AND the mobile applications.** Our analysis proves that these applications are the weak link and are exposing consumers to signficant amounts of risk.

MOTHER MAY I?

One of the most obvious and critical things to observe about any mobile application is the permissions it requires and uses. Each of these applications has the ability to capture screenshots, trigger based on audio events, send audio through the device, record video and set up schedules or automations. These functionalities all obviously require extensive permissions to function. One would expect the permissions requested by these applications to be similar from one application to another. The table below shows what we found.

		FEIT	Zmodo	Momentum	EZVIZ	Geeni	Globe	Wyze
Permission	Status	19	29	20	34	17	21	45
ACCESS_BACKGROUND_LOCATION	Dangerous	■					■	■
ACCESS_COARSE_LOCATION	Dangerous	■	■	■	■	■	■	■
ACCESS_FINE_LOCATION	Dangerous	■	■	■	■	■	■	■
ACCESS_LOCATION_EXTRA_COMMANDS	Normal			■				
ACCESS_NETWORK_STATE	Normal	■	■	■	■	■	■	■
ACCESS_WIFI_STATE	Normal	■	■	■	■	■	■	■
ANSWER_PHONE_CALLS	Dangerous							■
AUTHENTICATE_ACCOUNTS	Dangerous		■					
BLUETOOTH	Normal	■	■	■	■	■	■	■
BLUETOOTH_ADMIN	Normal	■	■	■		■	■	■
CALL_PHONE	Dangerous							■
CAMERA	Dangerous	■	■	■	■	■	■	■
CHANGE_CONFIGURATION	Signature/System				■			
CHANGE_NETWORK_STATE	Normal	■	■	■	■	■	■	■
CHANGE_WIFI_MULTICAST_STATE	Normal	■	■	■	■	■	■	■
CHANGE_WIFI_STATE	Normal	■	■	■	■	■	■	■
CONNECTIVITY_INTERNAL	Unknown							■
DISABLE_KEYGUARD	Normal		■		■			■
EXPAND_STATUS_BAR	Normal		■					
FLASHLIGHT	Normal			■	■			■
FOREGROUND_SERVICE	Normal	■			■	■	■	■
GET_ACCOUNTS	Dangerous		■					
GET_TASKS	Dangerous		■		■			■
GET_TOP_ACTIVITY_INFO	Unknown							■
INTERNET	Normal	■	■	■	■	■	■	■
INTERACT_ACROSS_USERS	Unknown							■
INTERACT_ACROSS_USERS_FULL	Unknown							■
MANAGE_ACCOUNTS	Dangerous		■					
MODIFY_AUDIO_SETTINGS	Normal	■			■		■	■
MOUNT_UNMOUNT_FILESYSTEMS	Dangerous				■			■
PEERS_MAC_ADDRESS	Unknown							■
READ_CALL_LOG	Dangerous							■
READ_CONTACTS	Dangerous		■					■
READ_EXTERNAL_STORAGE	Dangerous	■	■	■	■	■	■	■
READ_LOGS	Dangerous			■				■
READ_MEDIA_IMAGES	Unknown							■
READ_MEDIA_VIDEO	Unknown							■
READ_PHONE_STATE	Dangerous							■
READ_SETTINGS					■			
READ_SMS	Dangerous							■
READ_SYNC_SETTINGS	Normal		■					
READ_SYNC_STATS	Normal		■					
RECEIVE_BOOT_COMPLETED	Normal				■			■
RECEIVE_SMS	Dangerous							■
RECORD_AUDIO	Dangerous	■	■	■	■	■	■	■
REORDER_TASKS	Normal							■
REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	Normal				■		■	
REQUEST_INSTALL_PACKAGES	Dangerous			■	■			
RESTART_PACKAGES	Normal				■			
SYSTEM_ALERT_WINDOW	Dangerous		■		■			■
SYSTEM_OVERLAY_WINDOW	Unknown				■			■
TRANSMIT_IR	Normal							■
USE_CREDENTIALS	Dangerous		■		■			■
USE_FINGERPRINT	Normal				■			
USE_FULL_SCREEN_INTENT	Normal	■	■		■		■	
VIBRATE	Normal		■	■	■	■	■	■
WAKE_LOCK	Normal	■	■	■	■	■	■	■
WRITE_EXTERNAL_STORAGE	Dangerous	■	■	■	■	■	■	■
WRITE_OWNER_DATA	Unknown				■			
WRITE_SECURE_SETTINGS	Signature/System							■
WRITE_SYNC_SETTINGS	Normal		■					
WRITE_SETTINGS	Dangerous				■			

Many DANGEROUS permissions come with the territory on these IoT applications, however, some devices used far more than others.

What is most concerning is when applications just request permissions without any concern as to if the user will be using those permissions. For example, the Feit application was only used to control our lightbulb, yet asked for all of the permissions necessary to record audio, interact with storage on your phone, and more.

The EZVIZ application had the second most number of permissions among the group to include a number of unique DANGEROUS permissions such as WRITE_SETTINGS and the CHANGE_CONFIGURATION Signature Permission, which should not be used by third party applications.

Another area of concern showed up with the Momentum and EZVIZ applications where they are granted the permission to install packages or applications on the phone. This permission was added to Android to enable a way for application developers to create safer alternatives to an App Store concept, however, why an IoT app would require this is beyond us.

Signature Permissions are explicitiy called out by the Android developers as being "NOT FOR USE BY THIRD-PARTY APPLICATIONS." These should not be used by any application.

The Wyze application had significantly more permissions than any other application, to include some very strange capabilities such as sending and receiving phone calls and SMS messages. We assume this is related to their monitoring capabilities, however those cost extra and must be added on.

The Wyze application was also the only one that had the WRITE_SECURE_SETTINGS permissions, which should not be used by third-party applications such as this due to security concerns.

This device also had some very unique permissions, which are concerning. For example:

- PEERS_MAC_ADDRESSES: Allows this application to get the MAC address of other wifi and bluetooth devices nearby, even if location settings are disabled.

- INTERACT_ACROSS_USERS(_FULL): Based on our research, this allows an application to cross user boundaries on a device, but there is no clear reason why this would provide any benefit and no other application uses these permissions. To make matters worse, the FULL version of this permission should not be used by third-party developers.

The ZModo Application has a number of unique permissions that all appear to be associated with very old versions of Android indicating they probably have not changed portions of their codebase for a very long time. Examples include WRITE_SYNC_SETTINGS, READ_SYNC_SETTINGS, READ_SYNC_STATS, MANAGE_ACCOUNTS, and AUTHENTICATE ACCOUNTS.

APPLICATION SECURITY

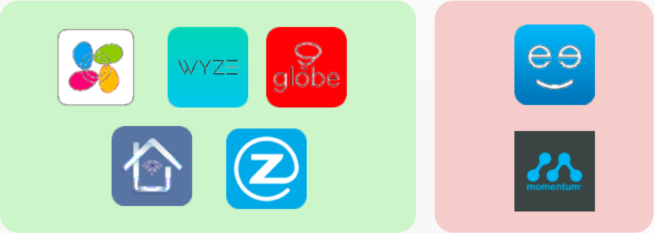
WebView Insecurities

Within an Android Application a developer may want to allow a user to view web content without having to use a browser. This is relatively normal, however it can create some significant vulnerabilities as shown below.

- Geeni, Globe & Feit: These application were all flagged for an insecure configuration of WebView AND a HIGH risk vulnerability of having debugging still enabled, which could allow the user to be tracked remotely. This vulnerability came from Tuya Code (TuyaWebView.java)
- EZVIZ: This device was flagged for having webview that ignores SSL errors, meaning it is vulnerable to a simple MITM attack.

SSL Pinning to prevent Man-in-the-Middle Attacks

We would expect security measures such as preventing MITM attacks to be a basic functionality on all of these applications, however that was not true. Kudos to the developers from Wyze, Zmodo, Globe, EZVIZ, and Feit for including this, bad marks for Momentum and Geeni for not.



Other Notes

- **Weak encryption and hashing:** We saw a large number of issues associated with weak encryption and hashing protocols in most of the applications. These point to concerns with the security of a user's data on the device and the lack of security oversight by the developers.
- **Old Signature Scheme:** All of these applications have a vulnerability associated with being signed with the V1 signature scheme making them vulnerable to the Janus Vulnerability. This could allow the application to be compromised without being detected. A fix for this was deployed in December of 2017 and V2 of the signature scheme has been available since Android 7 and V3 has been available since Android 9.
- **Strange Artifacts:** The Momentum code had a couple of strange artifacts left over to include a yahoo.com email address associated with a "Chat Activity" and a gmail address for a likely independent developer in code associated with Google Wallet. These are strong indicators of a lack of rigor in the management of the software code.
- **Use of SQLite Databases:** The Momentum, Globe, Geeni, Feit, Zmodo, and Wyze apps all use SQLite to store user data in a database, the commands to interact with this are all raw queries, making these apps susceptible to SQL Injections.
- **Encryption of SQL Database:** In the plus column, the Wyze, Globe, and Momentum applications all use add-on code called SQLCipher to encrypt the database to protect user data.

Bottom Line: It is very difficult to get into the details on application vulnerability scanning in a report like this, but based on what we observed, there is very little discipline or focus on security with respect to these applications. We would be surprised if the applications from Geeni, Globe, Feit, or EZVIZ have gone through any form of a security review. The Momentum, Zmodo, and Wyze applications appear to have some focus on security, but there is still significant room for improvement.

FINAL OBSERVATIONS

This report is the culmination of countless hours of analysis and hundreds of pages of notes. If we went into details on all of our findings and concerns this report could have been significantly more detailed, however we made an attempt to cover the highlights as best we could. After looking at the last five years, we are discouraged at the lack of progress in the IoT security space and see little signs of good news ahead. We see no indication of a move to cut ties with Chinese companies in IoT due to an extreme focus on cost above all else.

Business and Supply Chain Connections to China: We understand that the supply chain for IoT and electronics runs through countries like China based on cheap labor and materials costs. We expect there to be connections for sourcing purposes, however, when we start to see more intricate business connections and software development relationships, we get concerned. This is not about making China the "Boogeyman;" it is about a proven pattern of behavior clearly called out by the US Government and other governments related to corporate espionage, intellectual property theft, significant national security concerns, and clear evidence of a long-term, patient play for data supremacy. Based on our research, the low cost associated with Chinese-based infrastructures such as Tuya is not driven by a lower cost to operate, but rather this is a strategic play for control of the global IoT market. We strongly believe this to be the case. When capabilities are being offered below cost, there is a reason to dig deeper. Retailers and policy makers must decide if they want to abdicate the IoT market in their country to a foreign power that has shown a propensity to conduct corporate espionage and large-scale intellectual property theft operations. This discussion is made even more serious by recent developments with cybersecurity laws in China where the Chinese government can demand data from Chinese companies and those companies are forced to comply.

Failure to Implement Basic Security Controls: We saw countless examples of failures to implement basic security controls, the failure to fix vulnerabilities that have been known about for years, and the poor implementation of security and privacy techniques allowing an attacker to view your most private moments. It is unacceptable that devices with these flaws can be found on the shelves of major retailers. You can not buy toys with broken glass in them or building materials with asbestos in these stores due to safety concerns and regulations, but you can buy an IoT device like a Zmodo camera that has significant security flaws and has likely never gone through a meaningful security audit.

Flagrant Lack of Concern for Privacy: All of the applications we observed require deep and intimate access into your mobile phone for functions you may never use. There is no clear or simple way to manage your privacy in these applications, putting consumers at the mercy of the developers. This flagrant lack of concern around consumer privacy is deeply troubling, especially given the fact that these applications have been downloaded and installed millions of times on the devices of unsuspecting consumers that are completely unaware of the risks to which they are being exposed.

RECOMMENDATIONS

#1 Consumers Must Demand Accountability From Major Retailers

Major retailers understand that consumers do not really care about security or privacy of IoT devices based on how consumers are voting with their wallets. They will not care about security and privacy until they are forced to by the government or consumers. If consumers do actually care about preventing unknown people from spying on them through their camera, or monitoring the activities in their home through lightbulbs and smart outlets, then you need to make your voice heard. Small actions go a long way here. Take to Twitter, Facebook, or other online platforms to make your voice heard.

#2 Consumers Should Focus on Functionality Over Cost

Given the extreme state of insecurity in these IoT devices, consumers should be willing to spend a few more dollars for brands that take a stand on transparency and security. Saving $40 on a camera that you might have for two years is really only saving about $1.60 per month…giving up your privacy is priceless. Seek out resources for getting better visibility into which devices are secure. To make matters worse, we are accepting all of these privacy and security risks for a device that simply lets you dim a lightbulb or change its color from your phone. Most of these applications are poorly designed and have extremely limited functionality given the risk to which they expose consumers. Demand better and buy accordingly.

#3 The Government Should Take Action to Protect Consumers

The US Government has already taken action to address vulnerabilities in IoT with the Internet of Things Cybersecurity Improvement Act of 2020, however this is not nearly enough. This law focuses on federal information systems, not on the general consumer. The National Institute of Standards and Technology (NIST) has already made significant strides in publishing guidance and recommendations on IoT, we just need to get these recommendations teeth to protect consumers.

#4 Industry Needs to Increase Transparency

Every company we investigated in this report has a public story that feels good to the consumer, but behind the scenes their relationships to Chinese partners and Chinese infrastructure providers are obscured. For family run businesses like Feit Electric, we understand cost driving you towards the Tuya platform, but cost should not and can not be your only consideration. For “startups” like Wyze, we need to understand the deeper connections to Hualai and how you are securing the software development lifecycle and the data you are collecting.

#5 It Is Time for an Independent Oversight Body in IoT Like Underwriter Labs

Over the years we have heard discussions about the need for something like an Underwriter Labs for IoT devices and we think it is well past the time when this is needed. This approach meets a nice balance between government regulation and industry standards and could help elevate a focus on consumer safety, security, and privacy in the IoT market to the forefront.

dark³

Dark Cubed is an innovative Software-as-a-Service Cybersecurity Company delivering automated protection to small and medium businesses through partnerships with Managed Service Providers. To learn more about Dark Cubed check us out online or e-mail us at info@darkcubed.com

https://www.darkcubed.com