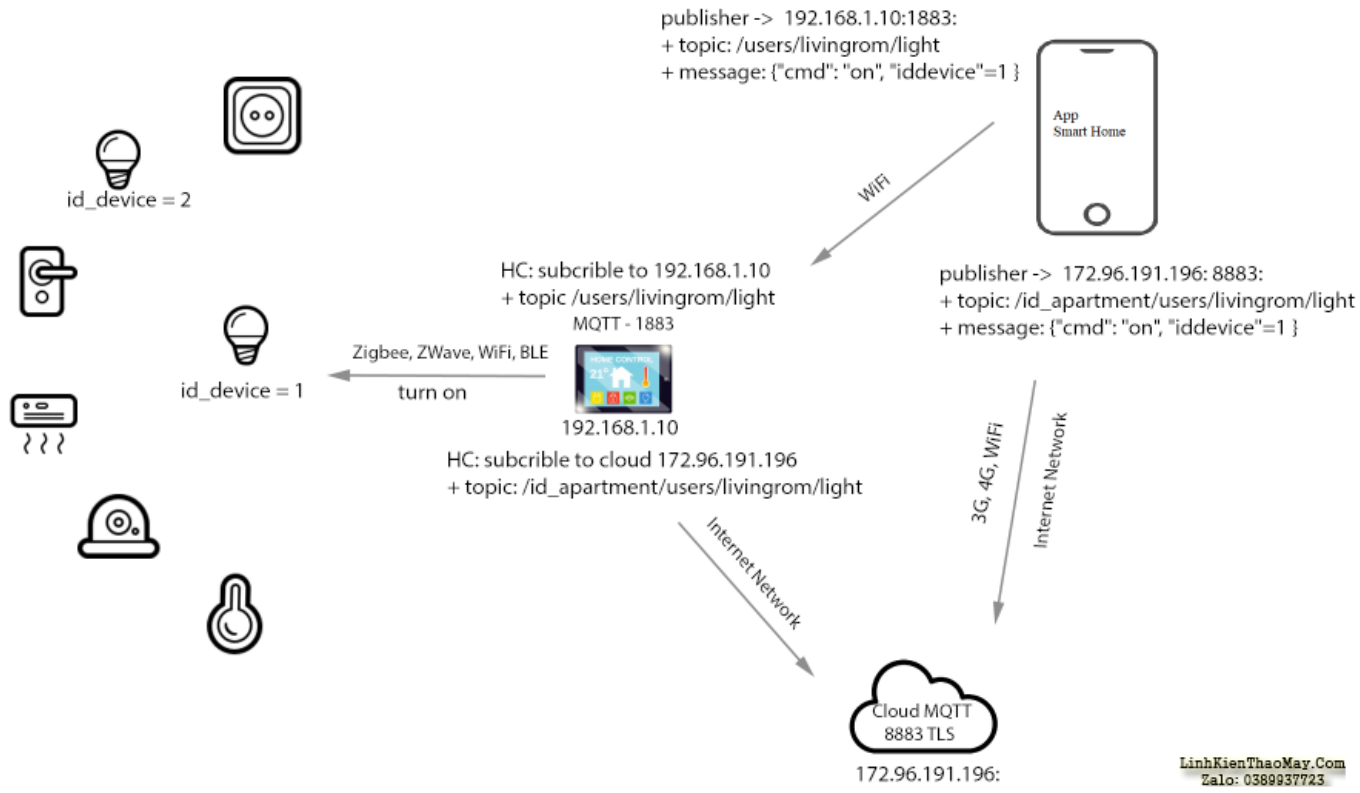
Mục tiêu của mình lần này là hướng tới các thiết bị smarthome, mình chọn target theo tiêu chí là công ty top đầu cung cấp phát triển các giải pháp, thiết bị cho nhà thông minh, các thiết bị thông minh hoặc được sử dụng tại công ty hoặc gia đình mình. Một đơn vị khá có tiếng trong lĩnh vực này. Công ty phát triển các thiết bị như bộ điều khiển trung tâm (Home Controller), Công tắc, Rèm, Hệ thống chiếu sáng và các mạch tích hợp vào khoá cửa, các trợ lý ảo tích hợp của Lumi.

Trong quá trình đánh giá đã tìm ra được một số lỗ hổng bảo mật có ảnh hưởng tới hệ thống, thiết bị và khách như hardcode credential, upload file, access VPN.

Trong đó có lỗ hổng được đánh giá nghiêm trọng nhất liên quan tới giao thức MQTT được sử dụng trao đổi thông tin và ra lệnh cho các thiết bị.

Phân Tích Hướng Tấn Công



- Trường hợp 1: Thiết bị Smartphone cùng mạng (local) với HC như mạng wifi

Hệ thống smarthome sử dụng điện thoại thông minh publish message (turn on light) thông qua mạng wifi local tới thiết bị Home Controller có dịch vụ MQTT port 1883 với topic /user/livingroom/light.

Các bóng đèn subscribe topic /user/livingroom/light sẽ thấy message, chương trình client sẽ xử lý message và thực hiện lệnh tương ứng. Hoặc HC tự mình subscribe topic khi thấy message sẽ gửi lệnh tới thiết được định danh trong HC thông qua mạng zigbee, zwave.

Sau đó các thiết bị client sẽ cập nhật trạng thái để đồng bộ với hệ thống cloud.

- Trường hợp 2: Khác nếu bạn không kết nối với mạng wifi tại nhà. Mà bạn đang ở

ngoài đường muốn bật nóng lạnh trước khi về nhà hoặc mở cửa cho người nhà lên chơi.

Khi đó app smartphone sẽ publish lệnh lên cloud với topic mình ví dụ /id_apartment/user/bathroom/hotcold phía HC subscribe topic đó và nhận message xử lý gửi lệnh tới các thiết bị được định danh tới HC.

Từ phân tích hoạt động ở trên mình chia làm 2 attack vector:

1. Thông qua mạng WiFi local tấn công vào dịch vụ của Home Controller
Ảnh hưởng có thể xảy ra đối với tính huống này là cho phép điều khiển các thiết bị kết nối tới mạng local.

2. Thông qua mang internet tấn công vào dịch phía Cloud.
Ảnh hưởng có thể điều khiển tất cả các thiết bị có kết nối tới Cloud.

Thực Hiện Tấn Công

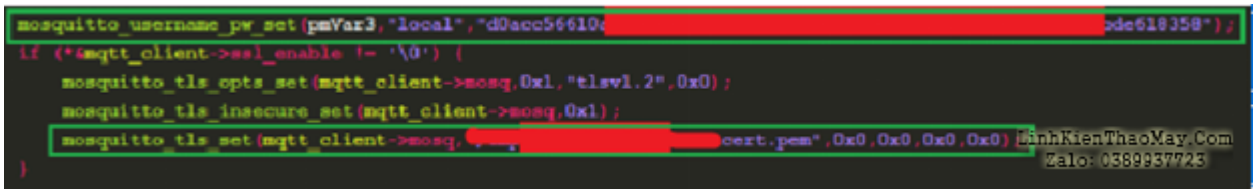
Reverse Firmware

Đầu tiên cần có thông tin tài khoản để truy cập vào dịch vụ MQTT ở phía Home Controller và Cloud. Dịch vụ có cài TLS bảo vệ đường truyền.

Thông tin này được hardcode trong firmware

- Username, password sẽ cho phép bạn truy cập vào dịch vụ.

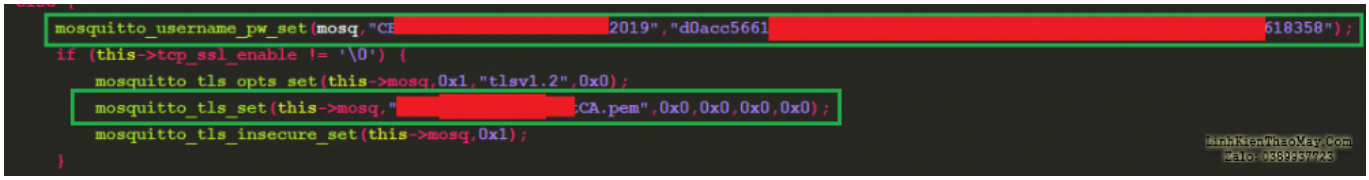
- Certificate sẽ xác minh bạn có đáng tin cậy để truy cập vào dịch vụ hay không, Ngoài ra có còn có tác dụng mã hóa packet tránh trường hợp mạng bị nghe lén hay các tấn công mạng.



Chỉ cần tìm tới hàm *mosquitto_username_pw_set*là ta có thể thấy *username=local và password = d0….58* và *mosquitto_tls_set*certificate được lưu trong filesystem có đường dẫn file cert

Có thể đoán được đây là thông tin truy cập MQTT local được cài trong Home Controller nhớ local.

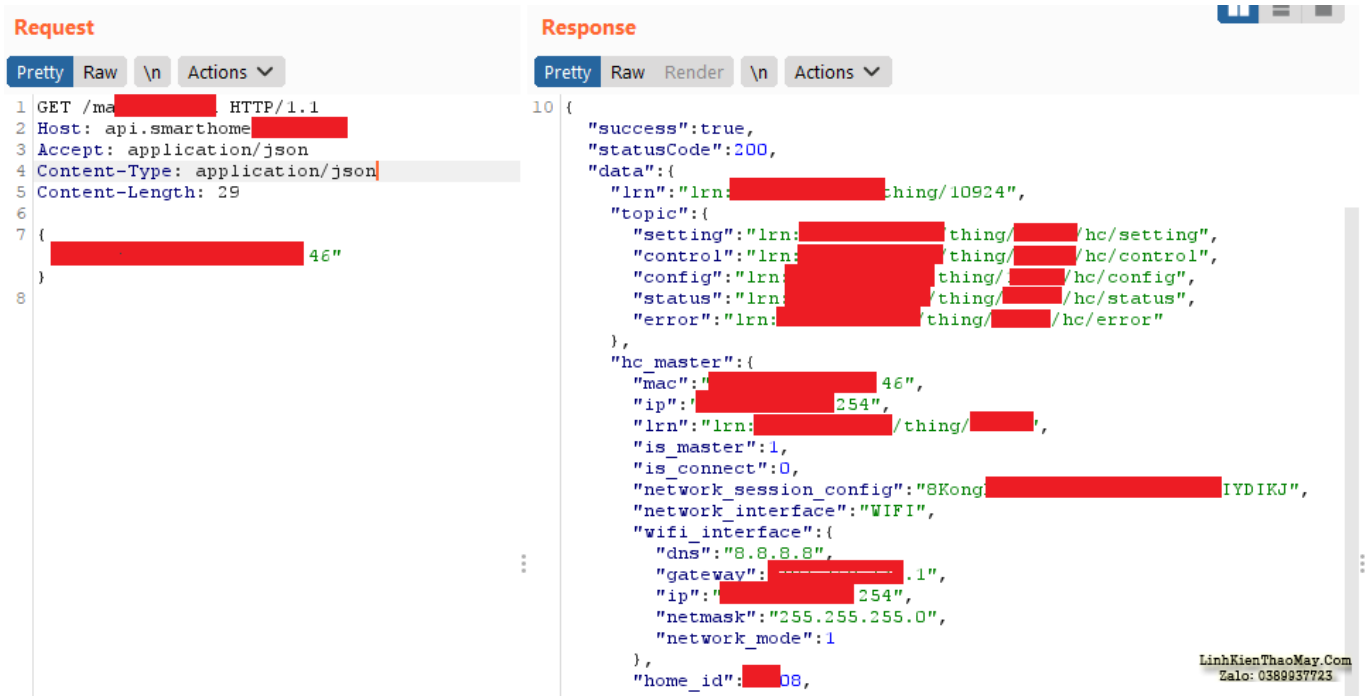
Thế thông tin truy cập phía **cloud** cũng tương tự như vậy



Nhìn là thấy thông tin khác rồi chứ cách lập trình vẫn thế.

DOS thông qua Duplicate Client ID

Lỗi này ở mức có khả năng xảy ra. Cliend ID được lấy từ phía server cloud. Sau khi có client id bạn có thể thực hiện reconnect liên tục để chiếm phiên làm việc dẫn tới không thể ra lệnh do liên tục bị chiếm phiên.



Spoof Client lấy Sensitive Information

DOS thì không có hứng thú lắm bây giờ xem xét hệ thống có thông tin khác như cá nhân hoặc thông tin truy cập tới các hệ thống khác.
Hãy tận dụng những gì đã học đó là sử dụng wildcard +, #, $..để đọc nội dung mà các thiết bị giao tiếp với nhau. Hãy nhớ đây là môi trường mạng internet chứ không đơn thuần là local.

Điều gì xảy ra nếu attacker giả mạo client và subscribe topic “#”.

Hãy xem ví dụ sau:

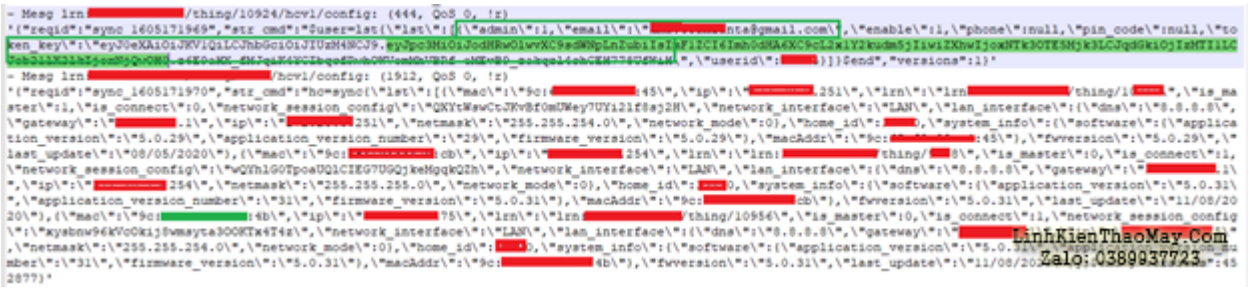
Attacker sẽ thu thập thông điệp các dựa vào subscribe # và filter theo topic /hcv1/config chờ người dùng cấu hình hoặc sửa đổi cấu hình làm lộ thông tin truy cập của của thiết bị và được mình ví dụ như sau:

- ip: 192.168.1.1 – port 80, 8888

- user: admin
- password: 12345678

Từ những thông tin này attacker có thể theo dõi bạn bằng thiết bị được cài đặt.

Ngoài ra con nhiều thông tin khác thu thập được như hình minh hoạ dưới đây.



Truy cập và Điều Khiển Thiết Bị

Để điều khiển các thiết bị có kết nối lên cloud cần các dữ kiện sau:

Đầu tiên attacker sẽ thu thập số điện thoại và email đăng ký trên cloud thông tin này có thể dễ dàng biết được thông qua internet hoặc bạn bè.

Từ đó truy cập các bản ghi thu thập được từ việc lắng nghe trên giao thức từ đó suy ra được địa chỉ MAC.

Từ địa chỉ MAC sử dụng link để lấy ID Client , Topic và ID thiết bị khoá.

- Client_ID có thể lấy các thông qua MAC lrn:…/thing/[ID] ID được tạo ra theo số thứ tự tăng dần khi đăng ký điều đó cho biết tại thời điểm đăng ký hãng đã bán được 10924 bộ sản phẩm.

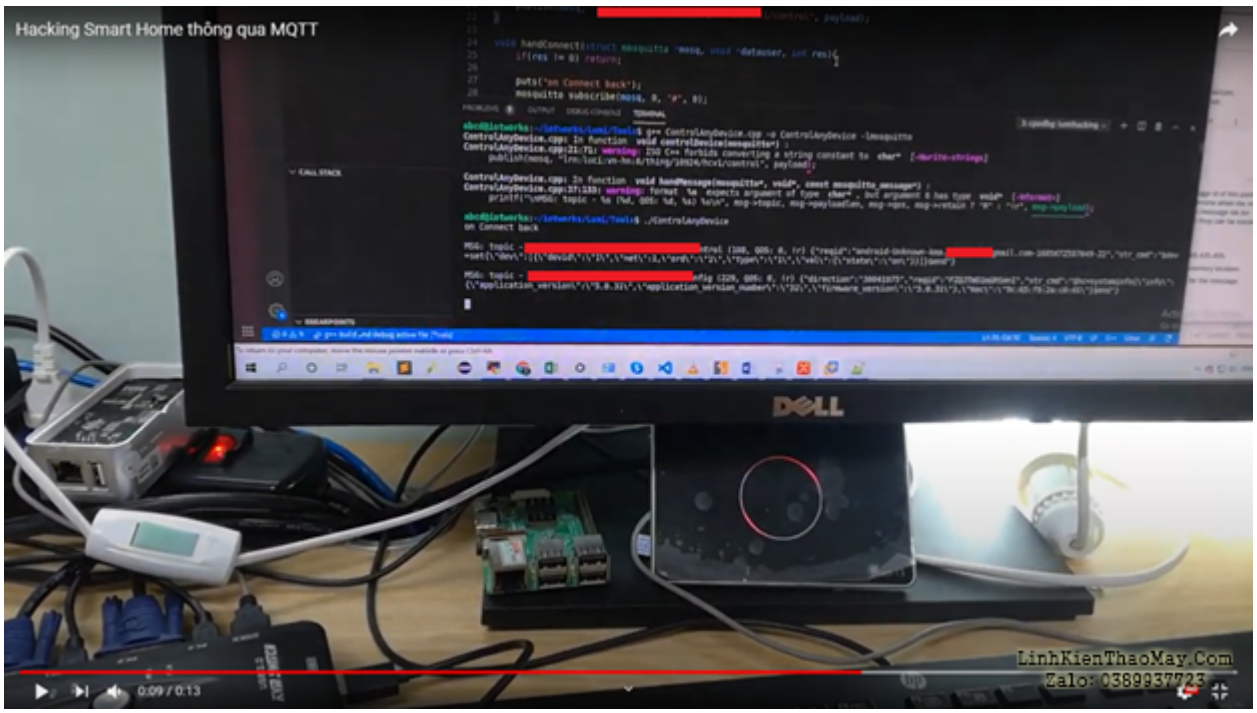
- Topic được map với thiết bị nào và ai sở hữu.
có dạng như sau:
lrn:…/thing/[ID]/hc/control

- Cấu trúc thông điệp chứa lệnh có thể reverse hoặc bắt lại có cấu trúc như sau:
{“reqid”:”ID”,”set”: “devid”:”1″, “net”:1, “type”:”1″,”val”:{“state”:”on”}}

- *state=on* Trạng thái là bật thiết bị.

- *devid=1* id là định danh số thiết bị cho căn hộ.

Minh hoạ lỗi bằng turn on bóng đèn từ xa.



Từ các lỗ hổng trên có thể thấy các thiết bị thông minh tại Việt nam tiềm ẩn một số nguy cơ cho phép tin tặc lợi dụng đánh cắp các thông tin và điều khiển thiết thiết bị và thấy rằng các sản phẩm IoT chưa được chú trọng nhiều về an toàn thông tin.

Phản Hồi

Sau khi Report các lỗ hổng tới đại diện của công ty Lumi đã có những phản hồi tích cực tiếp nhận lỗ hổng, thực tế không nhiều đơn vị ở Việt Nam cởi mở về việc tiếp nhận thông tin lỗ hổng bảo mật. Tới nay lỗi đã được ghi nhận, khắc phục, cập nhật và thấy Thư cảm ơn từ phía công ty Lumi.

Timeline Disclosure

24/11/2020: Thông báo các lỗ hổng và kèm PoC .docx qua email.

24/11/2020: thấy phải hồi từ phía công ty LUMI.

14/12/2020: Thông báo lỗ hổng mới liên quan tới VPN và kèm PoC .docx qua email.

28/04/2021: Cập nhật tình trạng Fix bug và thông báo công bố lỗ hổng cộng đồng.

28/04/2021: Nhận phản hồi rời lịch công bố lỗ hổng phục vụ vá lỗ hổng.

02/07/2021: thấy phản hồi lỗ hổng trong thiết bị, cloud, apps đã được vá.

Tác giả: Hà Văn Toàn

Các bài viết tương tự:

1. cần giúp đỡ âm ly 8 sò 2 ngày vẫn chưa tìm ra bệnh_áp đói xứng +-17vol qua 2 ổn áp 7912 7812 cấp cho rơ le mạch music master mic,,+-52 cho công suất – ban đâu hỏng công suất chết câu chì,,thay thế và kiểm tra các điện áp chân b công suất =nhau 52 vol,các tâng khuyeh đại thúc, đệm, trở tụ tốt,(,bo nguôn ,ổn áp và công suất đi liên),,,tháo đường 52 vol thì rơ le lại đóng cấp vào lại ko đóng ,bỏ 1 câu chì 1 vế lại đóng(vế đã bị nổ câu chì lúc đâu),,,,kiểm tra ko thấy bị sao? 2 trở cân bằng vê rơ le bảo vệ loa em đo 1 đường vê 52vol còn 1 đường vài mili vol,,,ko hiểu là sao lại chênh lệch thế,,,
2. Đâ DVD trung quốc – Nguôn cuả đâù DVD khi đo thì đủ áp nhưng khi căm vào đâu thì lên nhưng lại bị khởi động lại luôn,cứ bị như thế liên tục.(căm nguôn khác thì bình thường)
3. màn hình Acer X203H bị hỏng nguôn – bị nổ dao động nguôn
4. Mấy hôm nay làm có 2 hiện tượng thấy lạ như ma ám.hj. 1là tjvj tq, nên đỏ lè nổj đường hổj, đo đường kR =10v. Tháo vĩ đèn ra đo cũg 10v. Sau đó rút con 4282 trên đg kr ra đo có 150v trên kr, sau đó lăp lạj máy đã chạy bình thường ko pjt bị j lun hehe. 2. Maý trug quôc chj? Bị lỏg mạch nhưg khj đo H thấy 22v. Nhưg vân chay pjh thuog lạ thât. – .
5. panasonic hai chiều – máy không nhận điều khien , đã thay điều khiển khác nhung vẫn khong nhận. khi ấn điều khiển thì màn hình điều khiển bị mờ như kiểu hết pin nhưng thay pin mới vẫn không được .mong các huynh chỉ giáo.
6. quạt điều khiển điện cơ thống nhất – bấm điều khiển ko chạy,bấm phism ko chạy.em đã thay thử thạch anh,mắt nhận đkhiển,ic BA8206,cả tụ khơi động rùi nhưng vẫn ko chạy
7. Thử chiếm quyền kiểm soát các thiết bị thông minh IOT của hãng Akuvox
8. tivi BTV. mất model – bị cao áp đánh vào R(220k) đường ABL, đang sáng thì được 15s thì tối dần và bây giờ đang bị tối màn như giảm độ sáng của mà hình, đã thay cao áp và R(220k) mà màn hình vẫn tối…
9. Tivi LG model 21FU6LR – Chạy ic mành STV 9326, nửa màn hình dưới bình thường,

trên giữa màn hình có vệt sáng hơn và hình bị gấp, phía trên thì hình bị dãn, kiểm tra nguồn 26v đủ, đường ra chân số 5 cao 22v, thay ic mành và các tụ hóa nhưng vẫn chưa ra bệnh

10. toi co may in canon2900 khi ket noi may tinh thi bao co nhan USnhung khong ket noi dc voi may in va may tinh khong tim dc thiet bi B nhung khong ket noi dc voi may in va may tinh khong tim dc thiet bi – toi co may in canon2900 khi ket noi may tinh thi bao co nhan USnhung khong ket noi dc voi may in va may tinh khong tim dc thiet bi B nhung khong ket noi dc voi may in va may tinh khong tim dc thiet bi
11. tủ lanh Daewoo 160L – – ngăn trên làm đá bình thường . quạt chạy , đường gió xuống ngăn mát thông không bị tăc,đã để chăn gió xuống ngăn bảo quản lbes nhất .đã tháo kiểm tra dường hút gió xuống ngăn bảo quản không bị chăn hoặc tăc . vậy mà không có gió lạnh xuống , quạt thổi ra nói chung là tất cả các điều kiện ddeuf tốt vậy mà ngan mát không lạnh gì
12. xin được giúp đỡ từ mọi người,,bếp từ media bị sét đánh hư vỉ chính công suất,,do mạch toàn linh kiện rán nên ko thể phục hồi,,vỉ điều khiển phím ra các lệnh còn sống,,,giờ em cấy vỉ điều khiển của nó sang vỉ chính công suất khác,, – cấy đã xong các lệnh đã tốt nhưng riêng lệnh phát xung IGBT mở tầng khuyech đại thúc(8050,8055)bị yếu,,,,cho nồi lên nhiệt cao nhất mà nghe tiếng mâm từ bắt với đáy xoong nhỏ xíu,,,đáy xong chỉ ấm ấm,,