SEXTOYS CONNECTÉS : LA DÉBANDADE ?

@MaliciaRogue
Forensic bitch
RS Strategy - Managing uncertainty with data

SALUT !

Chui Rayna

@MaliciaRogue

rayna.st@protonmail.com

about.me/raynast

MAIS… ÇA SERT VRAIMENT ?

(Oui)

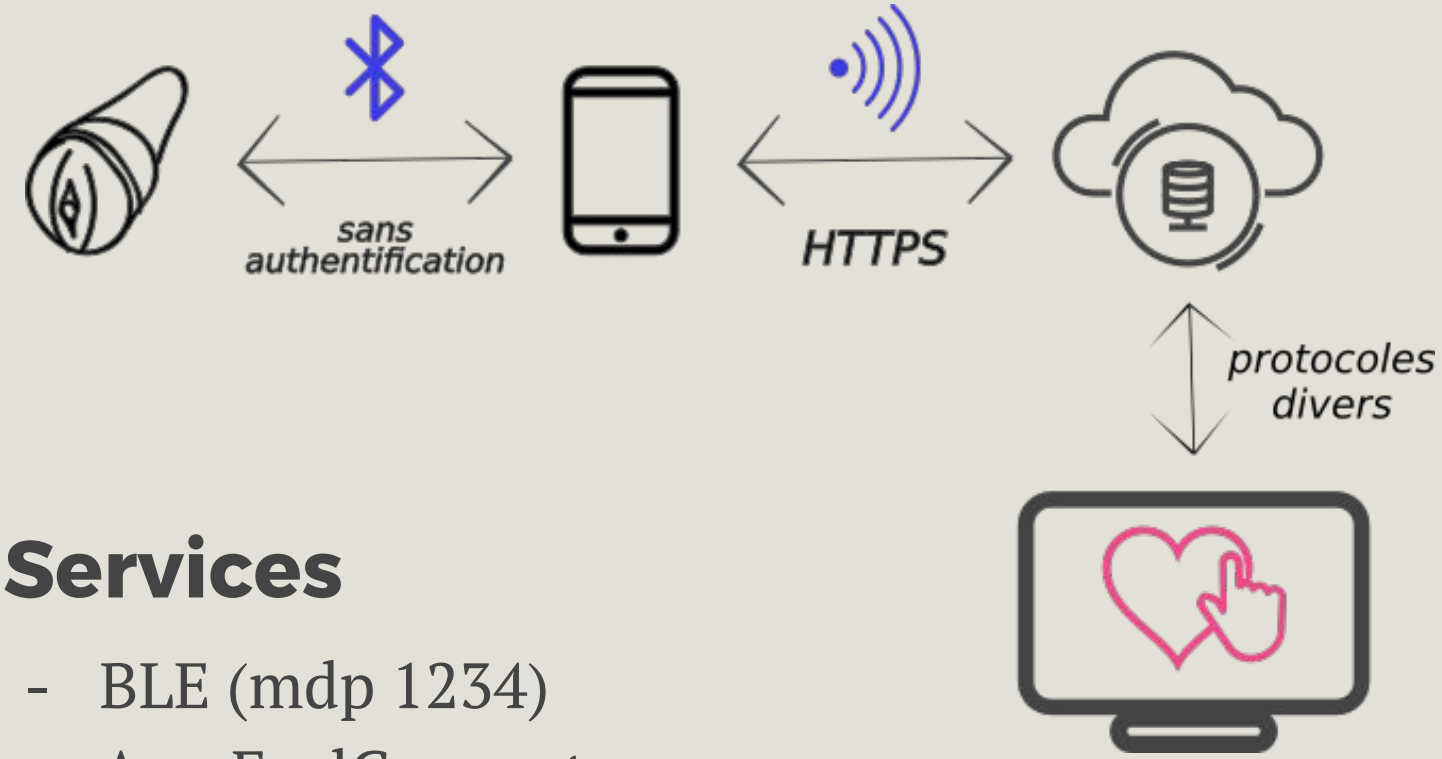
- 56 sextoys avec au moins du Bluetooth (aussi WiFi/3G/4G).
- 46 applis Android
- 31 applis iOS

FLESHLIGHT LAUNCH

Un vagin à piles, quoi

EN GROS...

EN GROS...



Services

- BLE (mdp 1234)
- App FeelConnect
- Site FeelMe.com

Bluetooth

(positions des parties mobiles pour mouvement à venir et de la vitesse de mouvement + interactions boutons)

```
module.exports = {
    service: '88F80580-0000-01E6-AACE-0002A5D5C51B',   // UUID principal
    command: '88F80583-0000-01E6-AACE-0002A5D5C51B',   // Spécification du mode de
mouvement
    data: '88F80581-0000-01E6-AACE-0002A5D5C51B',      // Écriture des données
    touch_channel: '88F80582-0000-01E6-AACE-0002A5D5C51B',  // Notifications type
status
};
```

SOUS LE CAPOT

App (JS Cordova ; l'identifiant de l'objet, la position des parties mobiles et leur vitesse de mouvement)

```
function onDeviceData(deviceId, percentValue, speed) {
    var devices = MyDevicesStore.getDevices();
    for (var i = 0; i < devices.length; i++) {
        var device = devices[i];
        if (!device || device.id === deviceId) {
            // Don't send to the same device
            continue;
        }
        BluetoothActions.sendToDevice(device.id, percentValue, speed);
    }
}
function start() {
    // Subscribe to device data events
    BluetoothDevicesStore.addDeviceDataListener(null, onDeviceData);
    Dispatcher.dispatch({ eventName: Constants.LOCAL_CONNECTION_ON });
    GoogleAnalyticsActions.bluetoothLocalMode();
}
function stop() {
    BluetoothDevicesStore.removeDeviceDataListener(null, onDeviceData);
    Dispatcher.dispatch({ eventName: Constants.LOCAL_CONNECTION_OFF });
}
module.exports = {
    start: start,
    stop: stop,
};
```

App <-> site web

(requestToken par le site, accessToken par l'API)

```
function handleAuthorize(urlComponents) {
    var requestToken = urlComponents.query.token;
    // go to Websites page
    history.push('/websites');
    var devices = MyDevicesStore.getDevices();
    var message = devices.length
        ? T('Connect to this website?')
        : T('Connect to this website and devices?');
    if (!confirm(message)) {
        hideTheApp();
        return;
    }
    addWebsite(requestToken);
}
```

- Hidashhi.com (marque blanche) : flux vidéo ;
- Pubnub.com : événements de changement de vitesse ;
- Google Analytics : métriques de visite

PLUTÔT BIEN AU FINAL

- Autorisations excessives
- Certif X.509 OK depuis 23/02/17
- Durée de conservation des données ?
- pubnub.com et hidashhi.com utilisent toujours du SSLv3 (=> /!\ POODLE)
- hidasshi.com en WordPress 3.9.2 (v4.8)

… mais Kiiroo a un programme de disclo

#NSFW

Âmes sensibles, toussa

AVEC ASSEZ DE LUBRIFIANT TOUT RENTRE

Fabricant US

- (6 pour ♀, 2 pour ♂ et 2 🤷)
- 3 applis mobiles (Java)
- Cert X.509 auto-signé (“F”), vuln. à OpenSSL Padding Oracle

Extrait de `classes.dex`

(les fichiers .dex contiennent la totalité du code exécutable + toutes ses ressources et certificats. Modification impact directement le .apk)

```
public final class Config
{
// snip
  public static String CY_APP_KEY = "f20e6f99c74d4cbfaae0f2868f320201";
  public static String CY_HTTP;
  public static final String DATE = "date";
  public static final String DEVICE_ADDRESS = "device_address";
  public static final String DEVICE_NAME = "device_name";
  public static final String EMAIL = "email";
  public static final String FIRST_PAIRING = "first_pairing";
  public static String HTTP = "http://api.masqué.tld";
  public static final String HTTP_IP = "http://74.xxx.xxx.xxx";
```

Pourquoi avoir un bon certif quand on ne s'en sert pas ?

```
GET /Services/GetAccessToken.aspx?appid=10001&appsecret=xxtoy HTTP/1.1
User-Agent: Dalvik/2.1.0 (Linux; U; Android 6.0.1; ASUS_Z00UD Build/MMB29P)
Host: api.masqué.tld
(...)
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: application/json; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 10 May 2017 20:27:38 GMT
Content-Length: 87

{"AccessToken":"F6F66EB078A0958A59C9E2CF09FCABF9","StatusCode":200,"Message":"succes
s"}

POST /Services/User/SignUp.aspx HTTP/1.1
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
(...)
n=rayna.st%40xxxxxx.com&sc=FC7996F1A4974AA30F92B400C4187D35&t=2&access_token=F6F66EB
078A0958A59C9E2CF09FCABF9&p=74F5CFB03AA9ECB3B40DC7FFBFB8D2C5&e=rayna.st%40xxxxxx.com
&HTTP/1.1 200 OK
(...)
{"StatusCode":200,"Message":"success"}

POST /Services/User/SignIn.aspx HTTP/1.1
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
(...)
Set-Cookie: ASP.NET_SessionId=vty2hhhoev1qigdipwq2dmcw; path=/; HttpOnly
Set-Cookie: impron_userinfo=uid=5ed1a49c-38d4-43fa-b01d-4d34a936b327&token=;
expires=Thu, 10-May-2018 20:27:38 GMT; path=/
(...)
{"UserID":"5ed1a49c-38d4-43fa-b01d-4d34a936b327","UserName":"rayna.st@xxxxxx.com","R
oleName":"","UserPoint":0.00,"Email":"rayna.st@xxxxxx.com","PhotoPath":"","Address":
"","EquipID":"","EquipConnectStatus":1,"LastLogin":"2017-05-10
20:27:38","Token":"","StatusCode":200,"Message":"success"}
```

PCAP or it didn’t happen

- Remonte en clair des données vers une machine Windows
- avec un FTP en clair sur le port 21
- le serveur web (IIS) est accessible en clair sur le port 80

Il y a de la cohérence...

Création de compte, token, données

```
n=rayna.st%40xxxxxx.com&sc=FC7996F1A4974AA30F92B400C4187D35&t=2&access_token=F6F66EB
078A0958A59C9E2CF09FCABF9&p=74F5CFB03AA9ECB3B40DC7FFBFB8D2C5&e=rayna.st%40xxxxxx.com
&

//

Set-Cookie: impron_userinfo=uid=5ed1a49c-38d4-43fa-b01d-4d34a936b327&token=;
expires=Thu, 10-May-2018 20:27:38 GMT; path=/
```

- Umeng plutôt que GA ;
- Adware Android.Igexin (2015, *Low risk* pour Symantec)
- IMEI, IMSI, versions de l'OS, du noyau, autres applis installées + en cours d'exécution, etc.

LEAKY APPS,
STICKY SITUATION

- X.509, le retour : service déployé sur Apache (port 443, login VirtualSVN…) et avec RDP sur le port 3389

=> test/dév/prod au même endroit + société US mais données collectées et traitées en Chine


THE INTERNET OF
RANSOMWARE
THINGS IS UPON US

MERCI !

Des questions ?

@MaliciaRogue

rayna.st@protonmail.com

about.me/raynast