PAS SAGE EN SEINE

29 JUIN - 02 JUILLET

SOCIÉTÉ ■ INTERNET ■ LIBERTÉ

Comment powned une application bancaire en 30 minutes

@aeris, 29 juin 2017

Aeris

Groupe cyber-terroriste individuel auto-radicalisé sur Internet

Mail / Jabber :
aeris@imirhil.fr
Mastodon :
aeris@social.imirhil.fr

Blog :
https://blog.imirhil.fr/
Conférences :
https://confs.imirhil.fr/

GPG : EFB7 4277 ECE4 E222
OTR : 5769 616D 2D3D
AC72

Devops chez Cozy Cloud

Problématique

Auditer le trafic réseau d'un « truc »

- Logiciel standard (ÉcoFax OVH)
- OS (Windows 10)
- Application Android (Smile & Pay)

Problématique

Auditer le trafic réseau d'un « truc »

- Logiciel standard (ÉcoFax OVH)
- OS (Windows 10)
- Application Android (Smile & Pay)

Quid de TLS ?

Expérimentations

Application desktop

Exécution locale

Wireshark / tcpdump

```
tcpdump -Ani any tcp port not 22 \
        -s 65535 -w /tmp/ecofax.pcap
```

179	0…	10.0.3.15	10.0.3.2	DNS	76	Standard query 0x6c08 A mail.ecofax.fr
180	0…	10.0.3.2	10.0.3.15	DNS	92	Standard query response 0x6c08 A mail.ecofax.fr A 213.186.33.93
181	0…	10.0.3.15	10.0.3.2	DNS	76	Standard query 0x29f7 AAAA mail.ecofax.fr
182	0…	10.0.3.2	10.0.3.15	DNS	130	Standard query response 0x29f7 AAAA mail.ecofax.fr SOA dns11.ovh.net
183	0…	10.0.3.15	213.186.33.93	TCP	76	57912 → imaps(993) [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1
276	0…	213.186.33.93	10.0.3.15	TCP	62	imaps(993) → 57912 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
277	0…	10.0.3.15	213.186.33.93	TCP	56	57912 → imaps(993) [ACK] Seq=1 Ack=1 Win=29200 Len=0
278	0…	10.0.3.15	213.186.33.93	TLSv1	145	Client Hello
279	0…	213.186.33.93	10.0.3.15	TCP	62	imaps(993) → 57912 [ACK] Seq=1 Ack=90 Win=65535 Len=0
337	0…	213.186.33.93	10.0.3.15	TLSv1	1460	Server Hello, Certificate
338	0…	10.0.3.15	213.186.33.93	TCP	56	57912 → imaps(993) [ACK] Seq=90 Ack=1405 Win=30888 Len=0
339	0…	213.186.33.93	10.0.3.15	TLSv1	448	Server Key Exchange, Server Hello Done
340	0…	10.0.3.15	213.186.33.93	TCP	56	57912 → imaps(993) [ACK] Seq=90 Ack=1797 Win=33696 Len=0
341	0…	10.0.3.15	213.186.33.93	TLSv1	254	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
342	0…	213.186.33.93	10.0.3.15	TCP	62	imaps(993) → 57912 [ACK] Seq=1797 Ack=288 Win=65535 Len=0
344	0…	213.186.33.93	10.0.3.15	TLSv1	115	Change Cipher Spec, Encrypted Handshake Message
345	0…	213.186.33.93	10.0.3.15	TLSv1	189	Application Data
346	0…	10.0.3.15	213.186.33.93	TCP	56	57912 → imaps(993) [ACK] Seq=288 Ack=1989 Win=36504 Len=0
1098	6…	10.0.3.15	10.0.3.2	DNS	73	Standard query 0x4bc5 A www.ovh.com
1099	6…	10.0.3.15	10.0.3.2	DNS	73	Standard query 0x1954 AAAA www.ovh.com
1100	6…	10.0.3.2	10.0.3.15	DNS	89	Standard query response 0x4bc5 A www.ovh.com A 198.27.92.1
1101	6…	10.0.3.2	10.0.3.15	DNS	125	Standard query response 0x1954 AAAA www.ovh.com SOA dns.ovh.net
1102	6…	10.0.3.15	198.27.92.1	TCP	76	36364 → http(80) [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TS
1105	6…	198.27.92.1	10.0.3.15	TCP	62	http(80) → 36364 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
1106	6…	10.0.3.15	198.27.92.1	TCP	56	36364 → http(80) [ACK] Seq=1 Ack=1 Win=29200 Len=0
1107	6…	10.0.3.15	198.27.92.1	HTTP	211	GET /update/ecofax.xml HTTP/1.1
1108	6…	198.27.92.1	10.0.3.15	TCP	62	http(80) → 36364 [ACK] Seq=1 Ack=156 Win=65535 Len=0
1109	6…	198.27.92.1	10.0.3.15	HTTP/XML	1494	HTTP/1.1 200 OK
1110	6…	10.0.3.15	198.27.92.1	TCP	56	36364 → http(80) [ACK] Seq=156 Ack=1439 Win=31240 Len=0
1119	6…	10.0.3.15	198.27.92.1	TCP	56	36364 → http(80) [FIN, ACK] Seq=156 Ack=1439 Win=31240 Len=0
1120	6…	198.27.92.1	10.0.3.15	TCP	62	http(80) → 36364 [ACK] Seq=1439 Ack=157 Win=65535 Len=0
1121	6…	198.27.92.1	10.0.3.15	TCP	62	http(80) → 36364 [FIN, ACK] Seq=1439 Ack=157 Win=65535 Len=0
1122	6…	10.0.3.15	198.27.92.1	TCP	56	36364 → http(80) [ACK] Seq=157 Ack=1440 Win=31240 Len=0
1684	9…	10.0.3.15	213.186.33.93	TCP	56	57912 → imaps(993) [FIN, ACK] Seq=288 Ack=1989 Win=36504 Len=0
1686	9…	213.186.33.93	10.0.3.15	TCP	62	imaps(993) → 57912 [ACK] Seq=1989 Ack=289 Win=65535 Len=0
1687	9…	213.186.33.93	10.0.3.15	TLSv1	93	Encrypted Alert
1688	9…	10.0.3.15	213.186.33.93	TCP	56	57912 → imaps(993) [RST] Seq=289 Win=0 Len=0
1689	9…	213.186.33.93	10.0.3.15	TCP	62	imaps(993) → 57912 [FIN, ACK] Seq=2026 Ack=289 Win=65535 Len=0
1690	9…	10.0.3.15	213.186.33.93	TCP	56	57912 → imaps(993) [RST] Seq=289 Win=0 Len=0
1691	9…	213.186.33.93	10.0.3.15	TCP	62	imaps(993) → 57912 [RST, ACK] Seq=4286327295 Ack=289 Win=0 Len=0

```
Frame 1109: 1494 bytes on wire (11952 bits), 1494 bytes captured (11952 bits)
Linux cooked capture
Internet Protocol Version 4, Src: 198.27.92.1, Dst: 10.0.3.15
Transmission Control Protocol, Src Port: http (80), Dst Port: 36364 (36364), Seq: 1, Ack: 156, Len: 1438
Hypertext Transfer Protocol
eXtensible Markup Language
  <update>
    <version>
    <!-- TODO : REMOVE FORCE ON LAST LINUX UPDATE AND PUT VERSION NUMBER RATHER THAN REVERSE DATE ON lastBuild
    <linux
      force="on">
      <deb>
        <lastBuild>
          2012070300
          </lastBuild>
        <file>
          http://mir7.ovh.net/ovh-applications/EcoFax/1.1.2/EcoFax-1.1.2.i386.deb
          </file>
        <md5sum>
          b85d9372b61c772f48bb1d7fb340d0d1
          </md5sum>
        </deb>
    <rpm>
    <i386>
    <x86_64>
```

Application desktop

DNS vers mail.ecofax.fr

IMAPS sur mail.ecofax.fr (chiffré)

DNS vers www.ovh.com

HTTP ( ) vers www.ovh.com (auto-update)

Application desktop

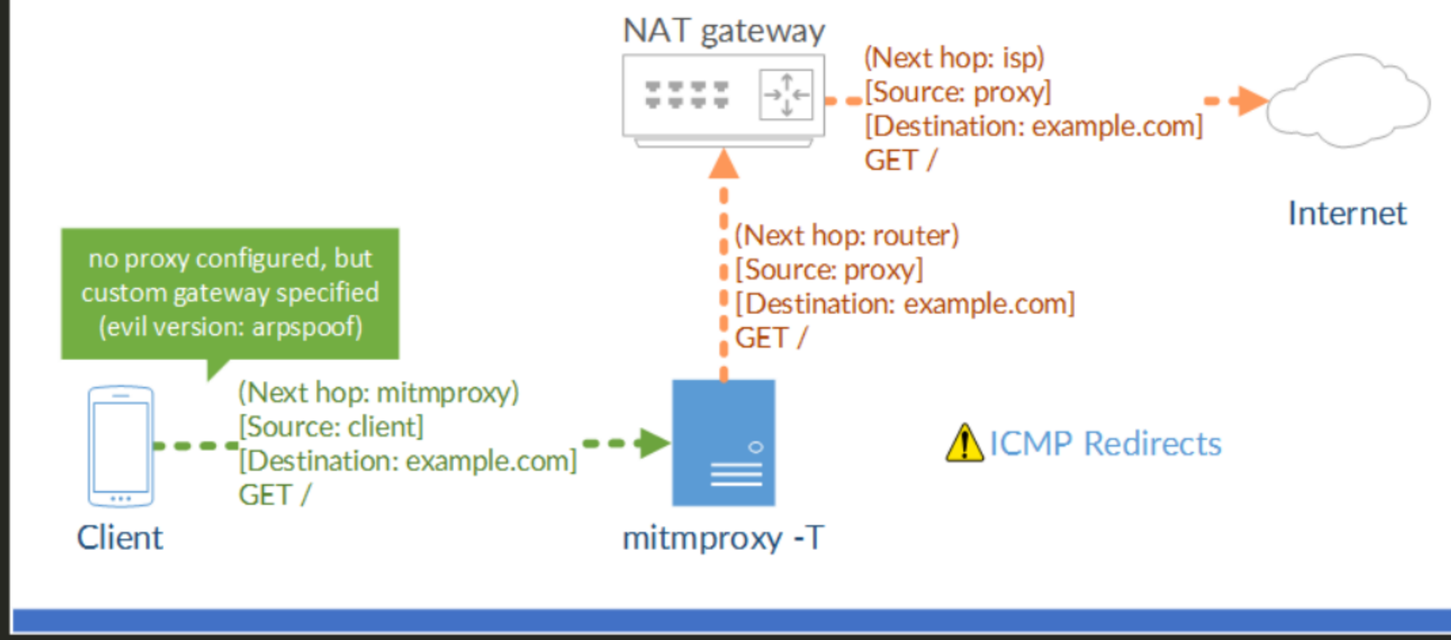
mitmproxy (https://mitmproxy.org/)

mitm_relay (https://github.com/jrmdev/mitm_relay)

Ajout d'une autorité de certification

Agit comme un proxy

Transparent Proxy Variant 2: Custom Gateway



Application desktop

```
apt install mitmproxy
wget https://raw.githubusercontent.com/jrmdev/mitm_relay/maste
        -O mitm_relay && chmod +x mitm_relay

iptables -t nat -A OUTPUT -m owner --uid-owner mitm \
        -p tcp --match multiport --dports http,https \
        -j REDIRECT --to-port 8080
iptables -t nat -A OUTPUT -m owner --uid-owner mitm \
        -p tcp --dport imaps -j REDIRECT --to-port 993
mitmproxy -T
mitm_relay -c .mitmproxy/mitmproxy-ca-cert.pem \
        -k .mitmproxy/mitmproxy-ca.pem \
        -r 993:mail.ecofax.fr:993

ln -s ~/.mitmproxy/mitmproxy-ca-cert.pem \
        /usr/local/share/ca-certificates/mitm.crt
update-ca-certificates

adduser mitm
su mitm Ecofax
```

```
>> GET http://198.27.92.1/update/ecofax.xml
       ← 200 text/xml 823b 257ms
```

```
Event log
10.0.3.15:58144: clientconnect
10.0.3.15:36596: clientconnect
10.0.3.15:58144: Certificate Verification Error for 213.186.33.93:993: hostname 'no-hostname' doesn't match
u'ecofax2.voip.ovh.net'
10.0.3.15:58144: Ignoring server verification error, continuing with connection
10.0.3.15:36596: clientdisconnect
10.0.3.15:58144: Client Handshake failed. The client may not trust the proxy's certificate for 213.186.33.93:993.
10.0.3.15:58144: clientdisconnect
```

```
[1/1]                                                                    ?:help [*:8080]
Warn: 10.0.3.15:58144: Client Handshake failed. The client may not trust the proxy's certificate for
213.186.33.93:993.
```

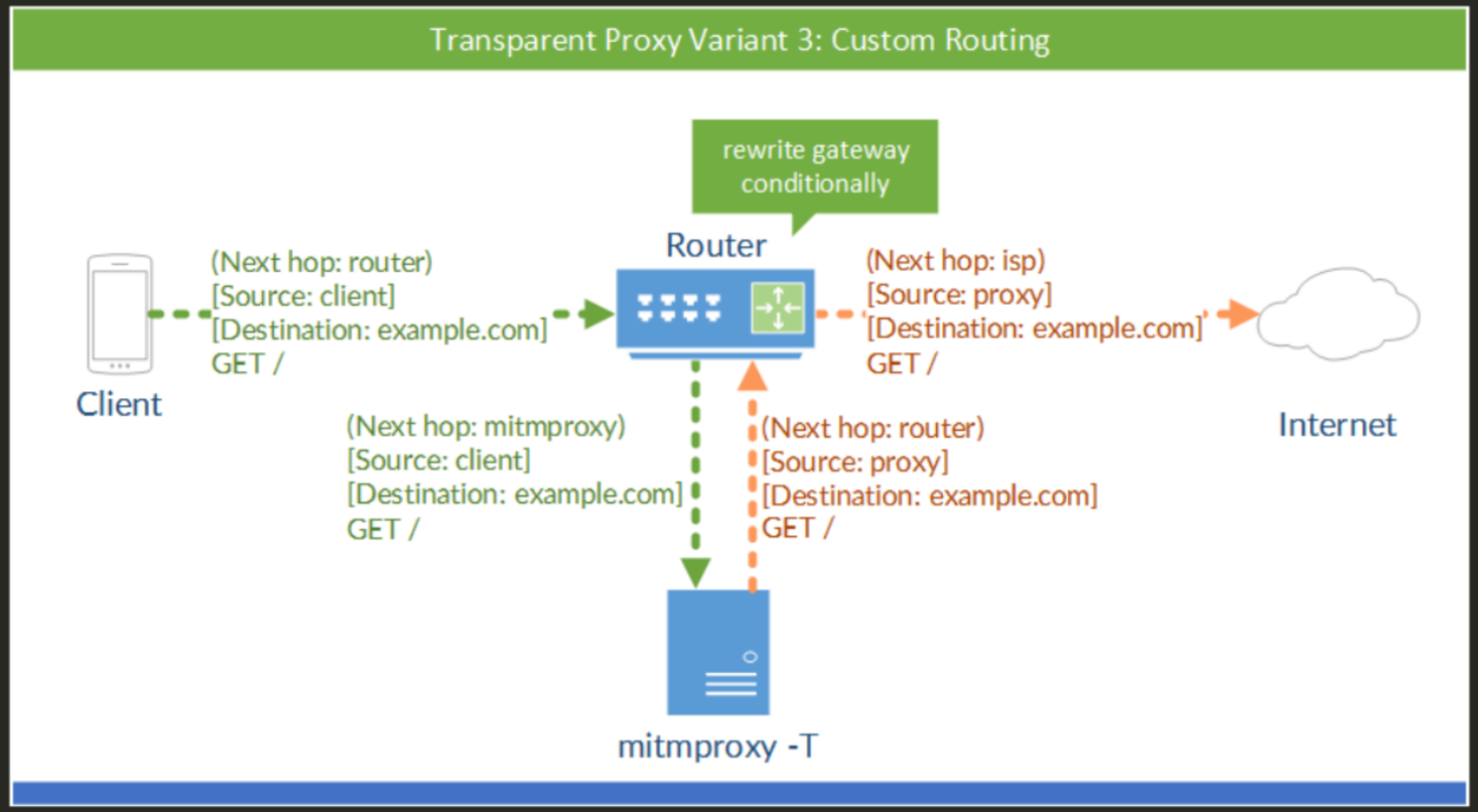
```
┌─[20:53:24] root@testing ~                                                    [15/17]
└─> # ./mitm_relay.py -r 993:mail.ecofax.fr:993 -c .mitmproxy/mitmproxy-ca-cert.pem -k .mitmproxy/mitmproxy-ca.pem
[!] Interception disabled! mitm_relay will run in monitoring mode only.
[+] Relay listening on tcp 993 -> mail.ecofax.fr:993
[+] New client: ('10.0.3.15', 44338) -> mail.ecofax.fr:993
------------------ Wrapping sockets ------------------
S >> C [ 213.186.33.93:993 >> 10.0.3.15:44338 ] [ Sun 18 Jun 20:54:05 ] [ 98 ]
* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE AUTH=PLAIN] Dovecot ready.


C >> S [ 10.0.3.15:44338 >> 213.186.33.93:993 ] [ Sun 18 Jun 20:54:05 ] [ 24 ]
1 LOGIN 00331354 testet


S >> C [ 213.186.33.93:993 >> 10.0.3.15:44338 ] [ Sun 18 Jun 20:54:07 ] [ 52 ]
1 NO [AUTHENTICATIONFAILED] Authentication failed.


C >> S [ 10.0.3.15:44338 >> 213.186.33.93:993 ] [ Sun 18 Jun 20:54:07 ] [ 24 ]
2 LOGIN 00331354 testet


S >> C [ 213.186.33.93:993 >> 10.0.3.15:44338 ] [ Sun 18 Jun 20:54:14 ] [ 52 ]
2 NO [AUTHENTICATIONFAILED] Authentication failed.


C >> S [ 10.0.3.15:44338 >> 213.186.33.93:993 ] [ Sun 18 Jun 20:54:14 ] [ 24 ]
3 LOGIN 00331354 testet
```

Système d'exploitation

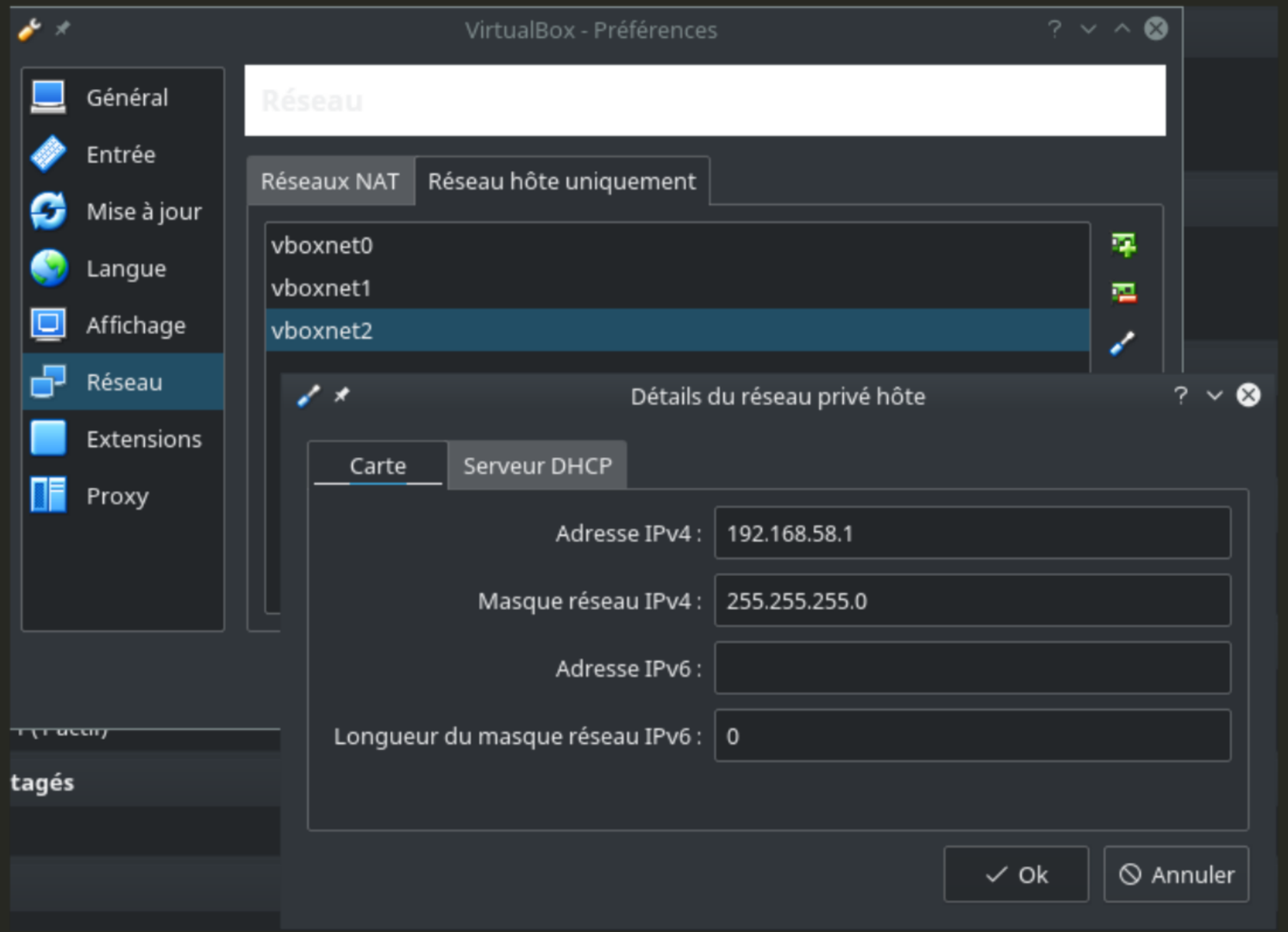
Ne se lance pas comme une application

Pas de configuration réseau « simple »

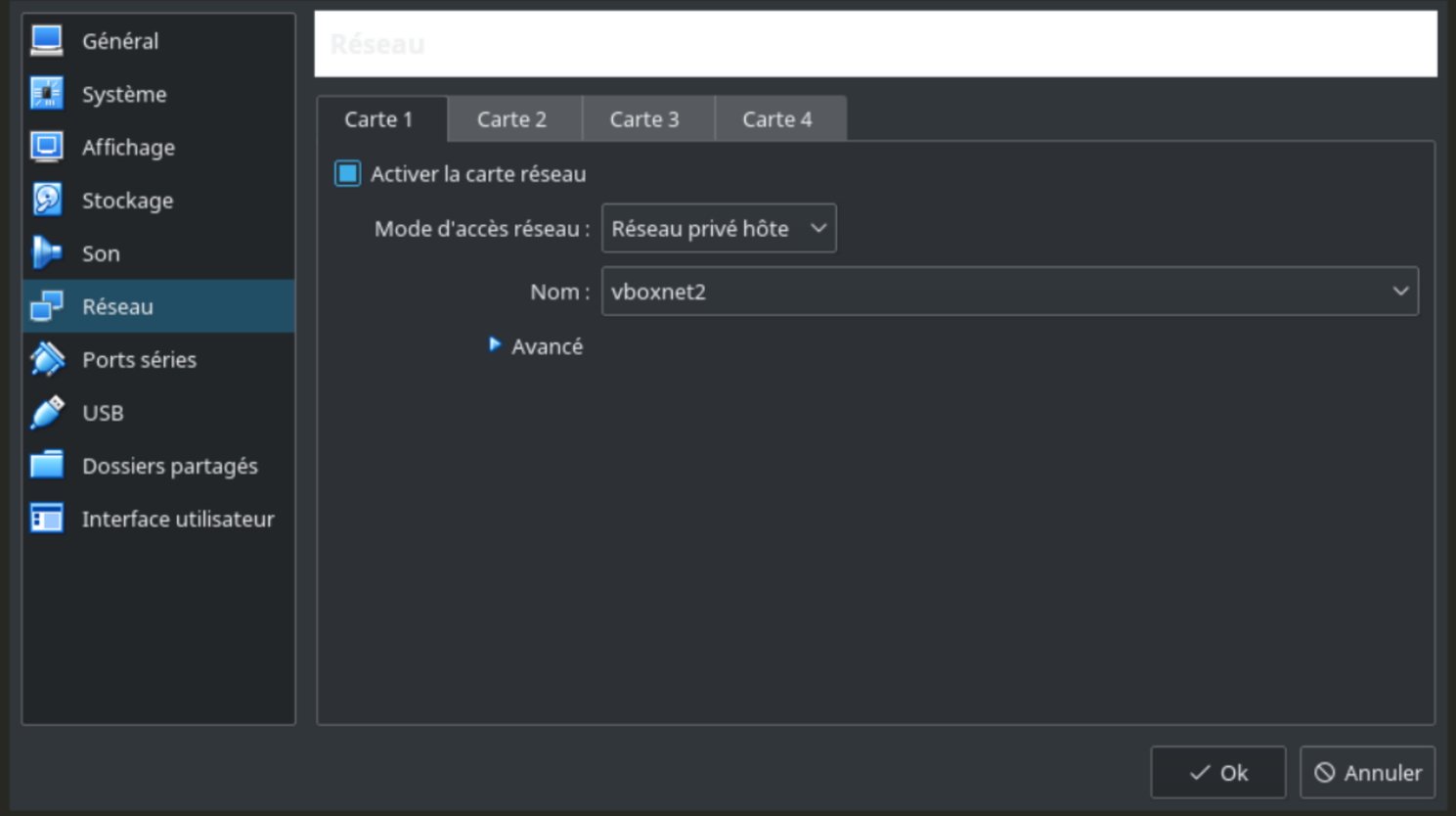
- Early traffic (sauf TLS cause CA)
- DHCP / DNS
- Gateway = mitmproxy 😂



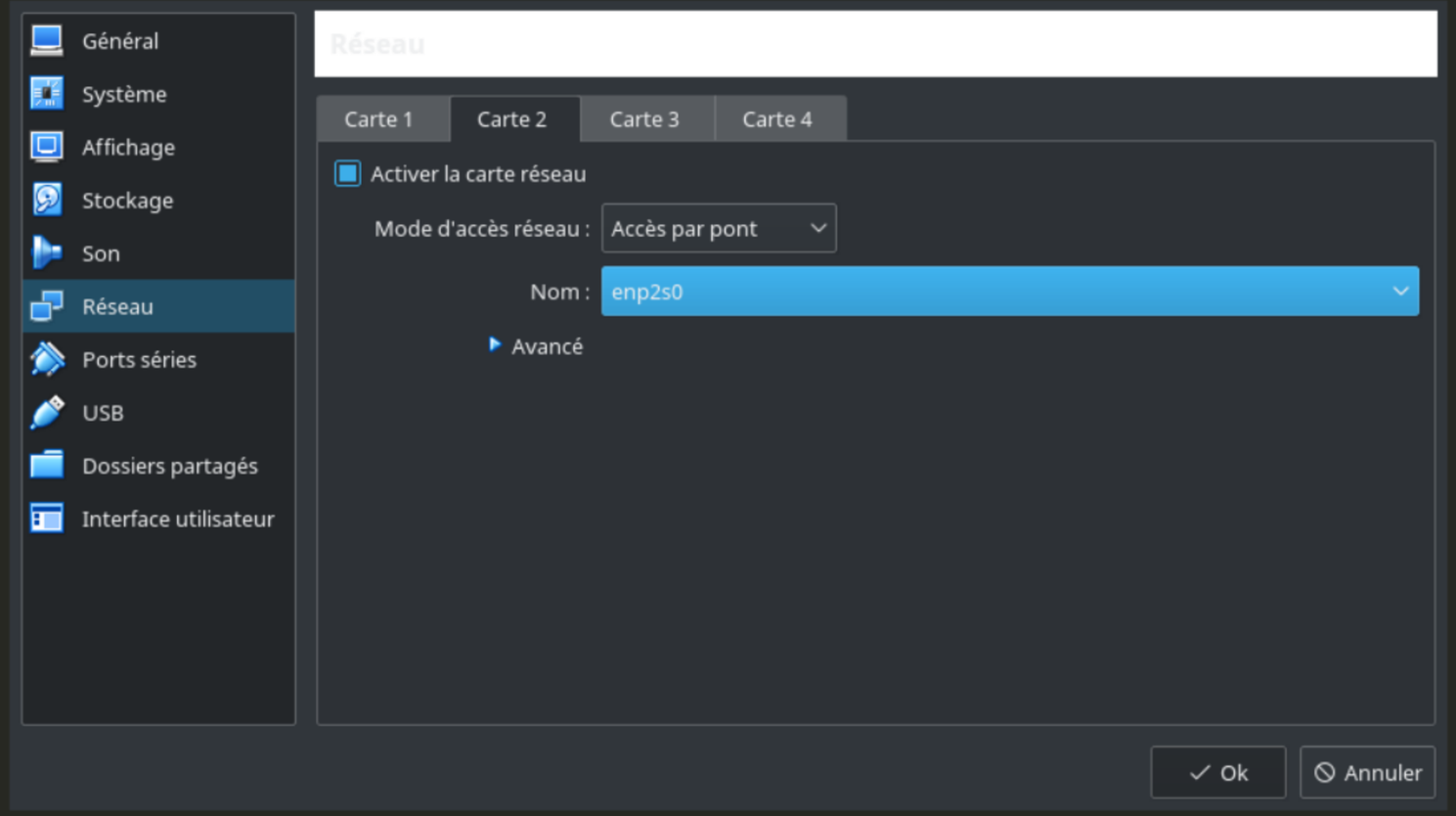
Nécessite un réseau dédié



Création réseau dédié



Association réseau dédié (mitm + cible)



Sortie réseau (mitm)

```
apt install unbound isc-dhcp-server

cat > /etc/network/interfaces.d/enp0s9 <<EOF
allow-hotplug enp0s9
iface enp0s9 inet static
        address 192.168.58.2/24
EOF

cat > /etc/unbound/unbound.conf.d/listen.conf <<EOF
server:
        interface: 127.0.0.1
        interface: 192.168.58.2
        access-control: 127.0.0.1/8 allow_snoop
        access-control: ::1/128 allow_snoop
        access-control: 192.168.58.0/24 allow
EOF
systemctl restart unbound
```

```
cat > /etc/dhcp/dhcpd.conf <<EOF
default-lease-time 600;
max-lease-time 7200;
ddns-update-style none;
subnet 192.168.58.0 netmask 255.255.255.0 {
        range 192.168.58.100 192.168.58.254;
        option routers 192.168.58.2;
        option domain-name "mitm";
        option domain-name-servers 192.168.58.2;
}
EOF
cat > /etc/default/isc-dhcp-server <<EOF
INTERFACESv4="enp0s9"
INTERFACESv6=""
EOF

systemctl restart isc-dhcp-server
```

```
iptables -t nat -A PREROUTING \
        -i enp0s9 -p tcp \
        --match multiport --dports http,https \
        -j REDIRECT --to-port 8080

mitmproxy -T
```

```
2015-08-16 23:21:47 GET https://www.bing.com/AS/API/WindowsCortanaPane/V2/Suggestions?qry=m1tm&c=4&c
                        vid=e0076467122f4cfbbee08ebf088ec0f9&ig=91bd856951984ea4a0514240d0168a3a&cc=F
                        R&setlang=fr-FR
                        ← 200 application/json 332B 234.65kB/s
Request                                                                    Response
Accept:                         */*
X-MSEdge-ExternalExpType:       JointCoord
X-MSEdge-ExternalExp:           d-thshld39,d-thshldspcl40,mystuffqu
X-BM-ClientFeatures:            FontV2, OemEnabled
X-Search-SafeSearch:            Moderate
X-Device-MachineId:             {72AC738B-5E0E-4CDE-9557-F192EC3C8505}
X-BM-Market:                    FR
X-BM-DateFormat:                dd/MM/yyyy
X-Device-OSSKU:                 101
X-Device-NetworkType:           ethernet
X-BM-DTZ:                       120
X-DeviceID:                     01000E2B090064FF
X-BM-DeviceScale:               100
X-Device-Manufacturer:          innotek GmbH
X-BM-Theme:                     ffffff;005a9e
X-BM-DeviceDimensionsLogical:   320x622
X-BM-DeviceDimensions:          320x622
X-Device-Product:               VirtualBox
X-BM-CBT:                       1439760104
X-Device-isOptin:               false
X-Device-Touch:                 false
X-AIS-AuthToken:                AISToken ApplicationId=2529e699-fc8e-4b1b-997c-a778e078aa91&ExpiresOn=
                                1440364835&HMACSHA256=w68KuVtaAfoE%2bqkzX%2bSQ0c9aRknBac%2bwDg%2bK%2fY
                                ynOL4%3d
X-Device-ClientSession:         AE483A6531804B94B22C161CF1E898D3
X-Search-AppId:                 Microsoft.Windows.Cortana_cw5n1h2txyewy!CortanaUI
Referer:                        https://www.bing.com/AS/API/WindowsCortanaPane/V2/Init
Accept-Language:                fr-FR
Accept-Encoding:                gzip, deflate
User-Agent:                     Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0;
                                Cortana 1.4.8.152; 10.0.0.0.10240.21) like Gecko
Host:                           www.bing.com
Connection:                     Keep-Alive
Cookie:                         SA_SUPERFRESH_SUPPRESS=SUPPRESS=0;
                                MUID=A6D4F89E5B6044D092D98A9BB5CEDA4D; _SS=SID=769FA2556DA544D296FF801
                                83C955298&CPID=1439758791964&CPH=d03c1acc&HV=1439760056;
                                _FS=mkt=fr-FR&ui=fr-FR; SRCHD=AF=WNSBOX;
                                SRCHUSR=AUTOREDIR=0&GEOVAR=&DOB=20150816;
                                _EDGE_S=mkt=fr-FR&ui=fr-FR&SID=25C1A7DE29E269A81BE0AFDB28EE68A9;
                                SRCHHPGUSR=IPMH=47f35001&IPMID=1439758791964;
                                SRCHUID=V=2&GUID=3491E524A82D4935BF2691907C44FD8B;
                                MUIDB=A6D4F89E5B6044D092D98A9BB5CEDA4D
No content
```

Envoi des données saisies dans la barre de recherche du menu « Démarrer »

```
2015-08-16 23:21:47 GET https://www.bing.com/AS/API/WindowsCortanaPane/V2/Suggestions?qry=mitm&cp=4&cvid=e0076467122f4cfbbee08ebf088ec0f9&ig=91bd856951984ea4a0514240d016a3a8&cc=FR&setlang=fr-FR
                    ← 200 application/json 332B 234.65kB/s
Request                                                  Response
Accept:                          */*
X-MSEdge-ExternalExpType:        JointCoord
X-MSEdge-ExternalExp:            d-thshld39,d-thshldspcl40,mystuffqu
X-BM-ClientFeatures:             FontV2, OemEnabled
X-Search-SafeSearch:             Moderate
X-Device-MachineId:              {72AC738B-5E0E-4CDE-9557-F192EC3C8505}
X-BM-Market:                     FR
X-BM-DateFormat:                 dd/MM/yyyy
X-Device-OSSKU:                  101
X-Device-NetworkType:            ethernet
X-BM-DTZ:                        120
X-DeviceID:                      01000E2B090064FF
X-BM-DeviceScale:                100
X-Device-Manufacturer:           innotek GmbH
X-BM-Theme:                      ffffff;005a9e
X-BM-DeviceDimensionsLogical:    320x622
X-BM-DeviceDimensions:           320x622
X-Device-Product:                VirtualBox
X-BM-CBT:                        1439760104
X-Device-isOptin:                false
X-Device-Touch:                  false
X-AIS-AuthToken:                 AISToken ApplicationId=2529e699-fc8e-4b1b-997c-a778e078aa91&ExpiresOn=1440364835&HMACSHA256=w68KuVtaAfoE%2bqkzX%2bSQ0c9aRknBac%2bwDg%2bK%2fYynOL4%3d
X-Device-ClientSession:          AE483A6531804B94B22C161CF1E898D3
X-Search-AppId:                  Microsoft.Windows.Cortana_cw5n1h2txyewy!CortanaUI
Referer:                         https://www.bing.com/AS/API/WindowsCortanaPane/V2/Init
Accept-Language:                 fr-FR
Accept-Encoding:                 gzip, deflate
User-Agent:                      Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0; Cortana 1.4.8.152; 10.0.0.0.10240.21) like Gecko
Host:                            www.bing.com
Connection:                      Keep-Alive
Cookie:                          SA_SUPERFRESH_SUPPRESS=SUPPRESS=0;
                                 MUID=A6D4F89E5B6044D092D98A9BB5CEDA4D; _SS=SID=769FA2556DA544D296FF80183C955298&CPID=1439758791964&CPH=d03c1acc&HV=1439760056;
                                 _FS=mkt=fr-FR&ui=fr-FR; SRCHD=AF=WNSBOX;
                                 SRCHUSR=AUTOREDIR=0&GEOVAR=&DOB=20150816;
                                 _EDGE_S=mkt=fr-FR&ui=fr-FR&SID=25C1A7DE29E269A81BE0AFDB28EE68A9;
                                 SRCHHPGUSR=IPMH=47f35001&IPMID=1439758791964;
                                 SRCHUID=V=2&GUID=3491E524A82D4935BF2691907C44FD8B;
                                 MUIDB=A6D4F89E5B6044D092D98A9BB5CEDA4D
No content
```

Envoi du thème utilisé par le bureau

```
2015-08-16 23:09:44 GET https://sls.update.microsoft.com/SLS/%7B9482F4B4-E343-43B6-B170-9A65BC822C77%
                        7D/x64/10.0.10240.0/0?CH=728&L=fr-FR&P=&PT=0x65&WUA=10.0.10240.16384
                        ← 200 application/octet-stream 15.58kB 4.36MB/s
Request                                                                  Response
Connection:  Keep-Alive
Accept:      */*
User-Agent:  Windows-Update-Agent/10.0.10011.16384 Client-Protocol/1.32
Host:        sls.update.microsoft.com
No content
```

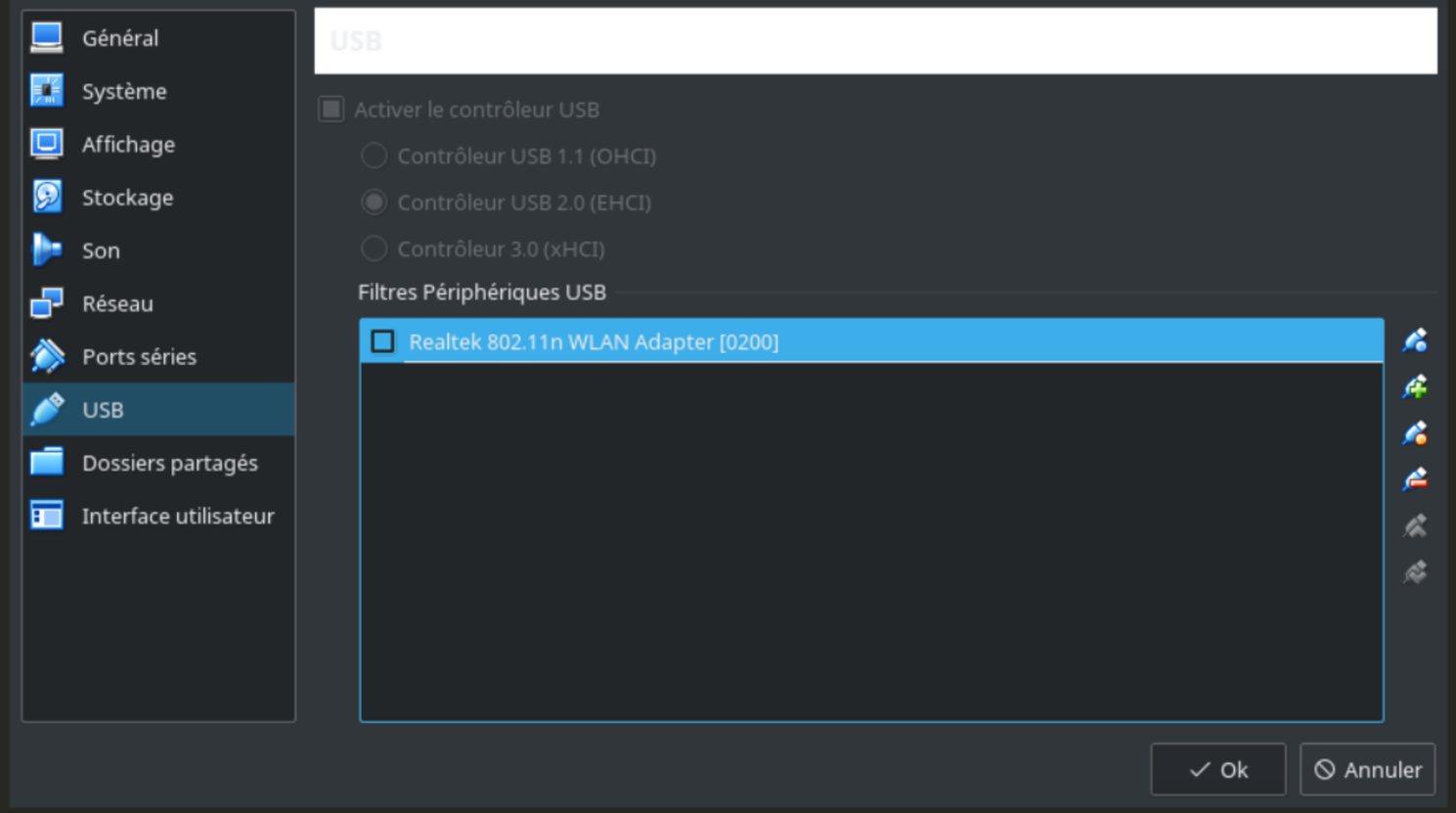
Connexion à Windows Update sans vérification du certificat

Application android

Wifi nécessaire

CA au niveau OS

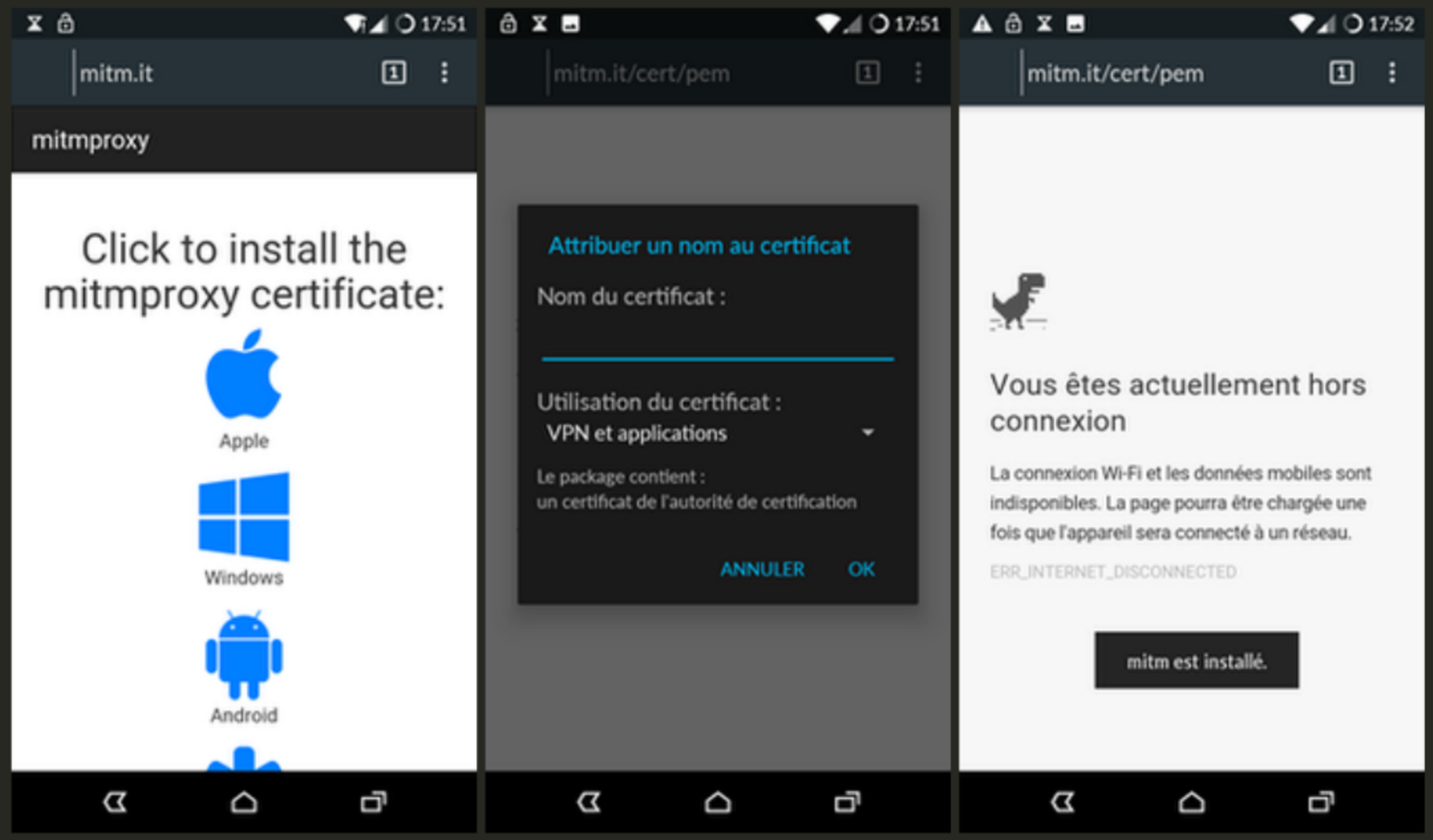
- Donc pas via Firefox



Association du dongle Wifi

```
apt install hostapd

cat > /etc/hostapd/wlxXXX.conf <<EOF
interface=wlxXXX
driver=nl80211
ssid=mitm
hw_mode=g
country_code=FR
ieee80211d=1
ieee80211h=1
channel=6
auth_algs=1
beacon_int=100
dtim_period=2
max_num_sta=255
rts_threshold=2347
fragm_threshold=2346
EOF
```

```
cat > /etc/network/interfaces.d/wlxXXX <<EOF
allow-hotplug wlxXXX
iface wlxXXX inet static
        address 192.168.58.2/24
        hostapd /etc/hostapd/hostapd.conf
EOF
ifup wlxXXX

cat > /etc/default/isc-dhcp-server <<EOF
INTERFACESv4="wlxXXX"
INTERFACESv6=""
EOF

systemctl restart isc-dhcp-server

iptables -t nat -A PREROUTING \
        -i wlxXXX -p tcp \
        --match multiport --dports http,https \
        -j REDIRECT --to-port 8080

mitmproxy -T
```



Installation du certificat CA

```
<?xml version='1.0' encoding='UTF-8'?>
<v:Envelope xmlns:i="http://www.w3.org/2001/XMLSchema-instance" xmlns:d="http://www.w3.org/2001/XMLSchema"
xmlns:c="http://schemas.xmlsoap.org/soap/encoding/" xmlns:v="http://schemas.xmlsoap.org/soap/envelope/">
  <v:Header/>
  <v:Body>
    <n0:XmlRequest xmlns:n0="http://www.nepting.com/nepweb/schemas" id="o0" c:root="1" xmlRequest='
                                                                                                  "/>
  </v:Body>
</v:Envelope>
```

Du base64 dans du XML

```
└─> $ base64 -d < /tmp/foo
<XPDERequest><messageHeader merchantIdentifier="KERNEL" messageType="Login" protocolMode="Production" protocolVersio
n="1" serviceSequenceNumber="1"/><requestBody><transactionDataList appTags="
                                                                                                  "><context sto
reIdentifier=""/><user passwd="[redacted]" preferredLanguage="fr" uid="[redacted].aeris"/><parameterFileList><headerParameterF
ile checksum="4117150854" creationTimestamp="2017-03-21T09:04:24.891" tableName="EMV_ICC_AID_PosMate"/></parameterFi
leList><parameterFileList><headerParameterFile checksum="4835846595" creationTimestamp="2017-03-21T09:04:24.944" tab
leName="EMV_ICC_Key_PosMate"/></parameterFileList><parameterFileList><headerParameterFile checksum="2179966668" crea
tionTimestamp="2017-03-21T09:04:24.998" tableName="Currency"/></parameterFileList></transactionDataList></requestBod
y></XPDERequest>%
```

Du XML encodé base64 dans du XML
Contenant l'identifiant utilisateur et le mot de passe (de 4 chiffres…)

Trop gros, passera pas !

(Réaction entendue généralement)

Ça n'arrive qu'aux autres — Je n'ai rien à cacher

Ça n'arrive qu'aux autres — Je n'ai rien à cacher

Comment SFR viole délibérément la neutralité du Net, et pourquoi c'est grave

Sommaire : *Pour diminuer le trafic sur son réseau, SFR s'est arrogé le droit de modifier les pages HTML et les images des sites web que visitent ses abonnés 3G. Effectuée à leur insu, cette manipulation est une violation caractérisée de la neutralité du Net.*

Par Pierre Col pour Infra | Net | Samedi 16 Mars 2013

Ça n'arrive qu'aux autres — Je n'ai rien à cacher

CLI, INTERNET, MINITEL 2.0, NET NEUTRALITY, NETWORKING, SECURITY

MITM AS A SERVICE 3G EDITION BY BOUYGUES, OU QUAND TON FAI BOUSILLE DNSSEC

FEBRUARY 26, 2017 /DEV/NULL 26 COMMENTS

Ça n'arrive qu'aux autres — Je n'ai rien à cacher

[FRsAG] MiTM Swisscom ?

Florian Siegenthaler florian at siegenthaler.mx
Jeu 9 Avr 23:06:26 CEST 2015

- Message précédent: [FRsAG] mail depuis/vers 1and1 : erreur 550
- Message suivant: [FRsAG] MiTM Swisscom ?
- **Messages triés par:** [date] [thread] [objet] [auteur]

Bonjour à toutes et à tous,

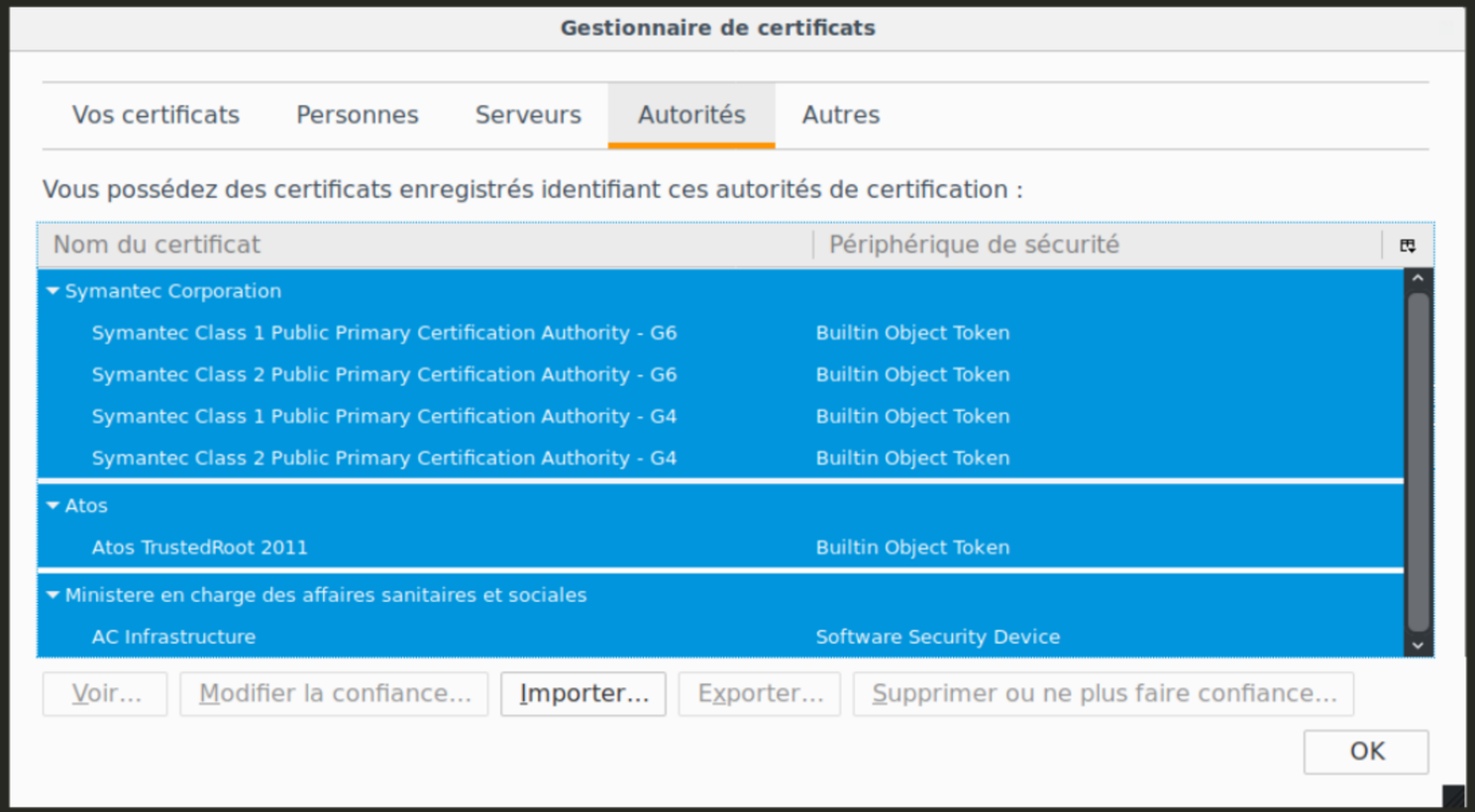
Je ne sais pas si ce message a sa place ici, au cas où je suis preneur d'un endroit plus approprié.

J'ai besoin de faire une investigation sur un faux certificat TLS, j'ai un serveur ownCloud qui a un certificat CAcert pour mon nom de domaine files.siegenthaler.mx et aujourd'hui j'ai reçu une alerte pour un faux certificat émanant de Swisscom (fournisseur d'accès national en Suisse).

Aujourd'hui à deux reprises j'ai reçu ce faux certificat d'une validité de 30 ans, une fois sur l'application ownCloud (fichiers) et une fois sur Thunderbird (contacts), je souhaite savoir si c'est réellement une attaque MiTM de la part de mon fournisseur d'accès ou si c'est un faux-positif, par exemple le routeur qui fait une redirection HTTP 3XX quand il se broute et qu'il présente son propre certificat ?

Ça n'arrive qu'aux autres — Je n'ai rien à cacher

Autorités de certification par défaut



Facilité d'ajout d'une CA

Wifi ouvert

Portail captif pour déployer la CA

Pas d'alerte outre mesure

Facilité d'ajout d'une CA

Wifi ouvert

Portail captif pour déployer la CA

Pas d'alerte outre mesure

La connerie humaine

Quel pourcentage de « continuer » sur une alerte de sécurité ?

Se protéger

Les besoins

Monde de plus en plus « mobile only »

Réseau non fiable (Hostspot wifi, 3G/4G…)

Pas de confiance en les CA

Les besoins

Monde de plus en plus « mobile only »

Réseau non fiable (Hostspot wifi, 3G/4G…)

Pas de confiance en les CA

Arrêter de déléguer sa sécurité

DANE/TLSA

Suppose DNSSec 😭

Suppose TLSA 😭 😭 😭

```
$ dig TLSA _443._tcp.confs.imirhil.fr +short
letsencrypt._tlsa.imirhil.fr.
1 1 2 16ACC40419CEF98984BF7F1BCE354BB0AA3F84AB00
      29E829F36CD3BBE36ED2501B6F22D4EC879B315FA0
      93E0F73C6E7A85FA837582FF41F685C53E4911341451
```

HPKP

TOFU…

HTTP(S) only

Suppose HPKP 😫 😫 😫

```
$ curl -sI https://confs.imirhil.fr | grep public-key-pins
public-key-pins: max-age=5184000;
  pin-sha256="wdkD38iQQzxE7g0RpmN8VoaIqX7YmPWwoueD9Iqawfg=";
  pin-sha256="EswdUzfH2N8sx6Nb4Vr9gamtNF5VWQxLWUG0gDIPVLw="
```

Épinglage manuel

Dispo partout (en théorie)

Gestion du rollover 😫

Réseau non sûr

Aucune transmission de données secrètes

Pas de mot de passe

- Même salé / hashé (rejeu possible)

HMAC (secret partagé)

Signature via bi-clef

Protection anti-rejeu

Question ?