台湾地区政府APT组织借新型肺炎发起网络攻击

Original 微步情报局 安全威胁情报 Today

还记得台湾当局对口罩限制出口、在海关拦截口罩的新闻吗？他们的情报机构正在对大陆政府部门以新型肺炎相关的“疫情防控日报表”、“社会维稳”和“献药方”等主题为诱饵，发起网络攻击。

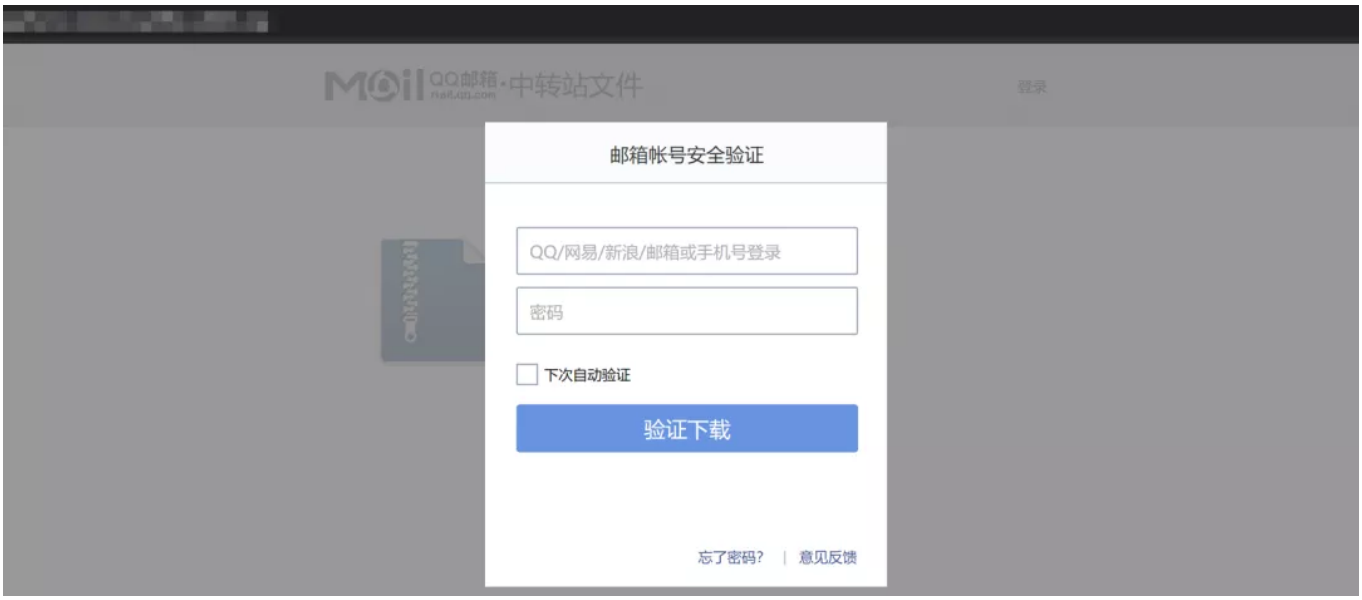
新冠肺炎疫情之下，网络空间已成为承载人民基本生活保障的重要基础设施，各个国家和地区负责网络间谍和网络战的黑客组织都不约而同一般盯上这片战场，前有印度背景黑客组织“白象”以疫情文件作饵攻击我医疗部门，现又有台湾情报机构属下黑客组织“绿斑”伸出黑手。

微步在线旗下安全研究团队“微步情报局”从1月下旬开始监测到三个用于钓鱼的文件：

经溯源和研判后，微步情报局认定这三个文件为同一个黑客组织所发布，属于同一轮攻击。微步情报局自设立以来，累计率先发现数十个境外高级APT黑客组织，并长期监控全球APT组织针对我国关键基础设施和金融、能源、政府、高科技等行业的定向攻击行动，经过对IOC和作案手法、攻击链等信息的分析，微步情报局判定，这个黑客组织，就是台湾情报机构属下APT组织“绿斑”，即GreenSpot。该组织自2007年来，持续针对大陆政府、军事、科技、教育和海事机构等部门进行攻击，试图窃取各种机密数据、进行情报活动。

攻击目标	政府部门、医疗机构
攻击时间	2020年1月下旬至今
攻击向量	网络钓鱼
攻击复杂度	低
攻击目的	窃取邮箱账密，收集情报

“绿斑”的主要攻击手法是利用仿冒QQ和163邮箱的域名发起钓鱼攻击。攻击者通过邮件等方式发送“疫情防控日报表”、“社会面维稳组工作简要总结”和“《南部杜氏中医》献方”等诱饵文档下载链接，一旦受害者点击链接，则会弹出要求验证邮箱账号的页面，诱导输入账号密码，而账号和密码则会被回传到攻击者的服务器：



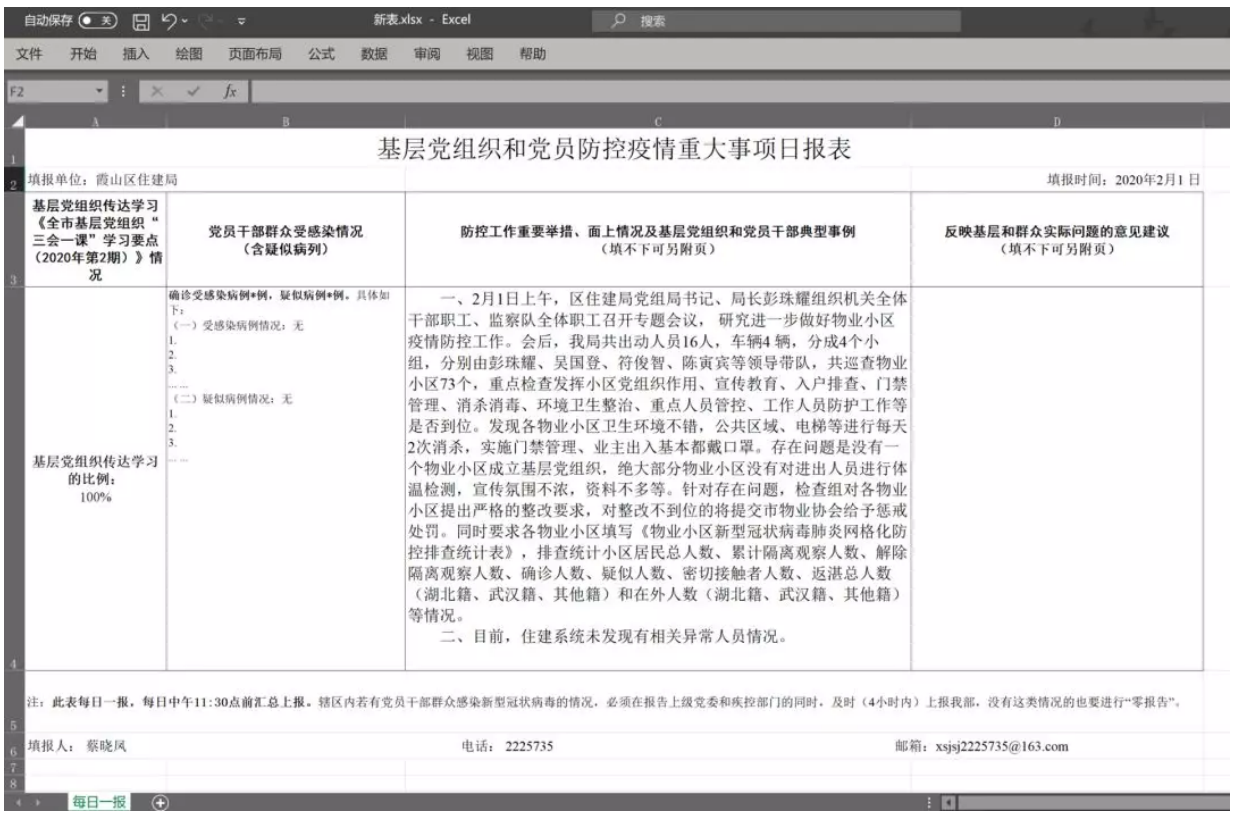

```
<div class="login_form">
    <form id="loginform" autocomplete="off" name="loginform" action="login.php" method="post" target="_parent" style="margin:0px">
        <div class="uinArea" id="uinArea">
            <label class="input_tips" id="uin_tips" for="u"></label>
            <div class="inputOuter">
                <input type="email" class="inputstyle" id="u" name="id" placeholder="QQ/网易/新浪/邮箱或手机号登录" value="" tabindex="1" pattern="^\w+@\w+(\.com)" required>
                <a class="uin_del" id="uin_del" href=""></a>
            </div>
            <!--ul class="email_list" id="email_list"></ul-->
        </div>
        <div class="pwdArea" id="pwdArea">
            <label class="input_tips" id="pwd_tips" for="p"></label>
            <div class="inputOuter">
                <input type="password" class="inputstyle" id="p" name="pass" value="" maxlength="16" tabindex="2" placeholder="密码" pattern="^[\S]{6,18}$" required>
            </div>
            <div class="lock_tips" id="caps_lock_tips">
                <span class="lock_tips_row"></span>
                <span> 大写锁定已打开 </span>
            </div>
        </div>
```

Body

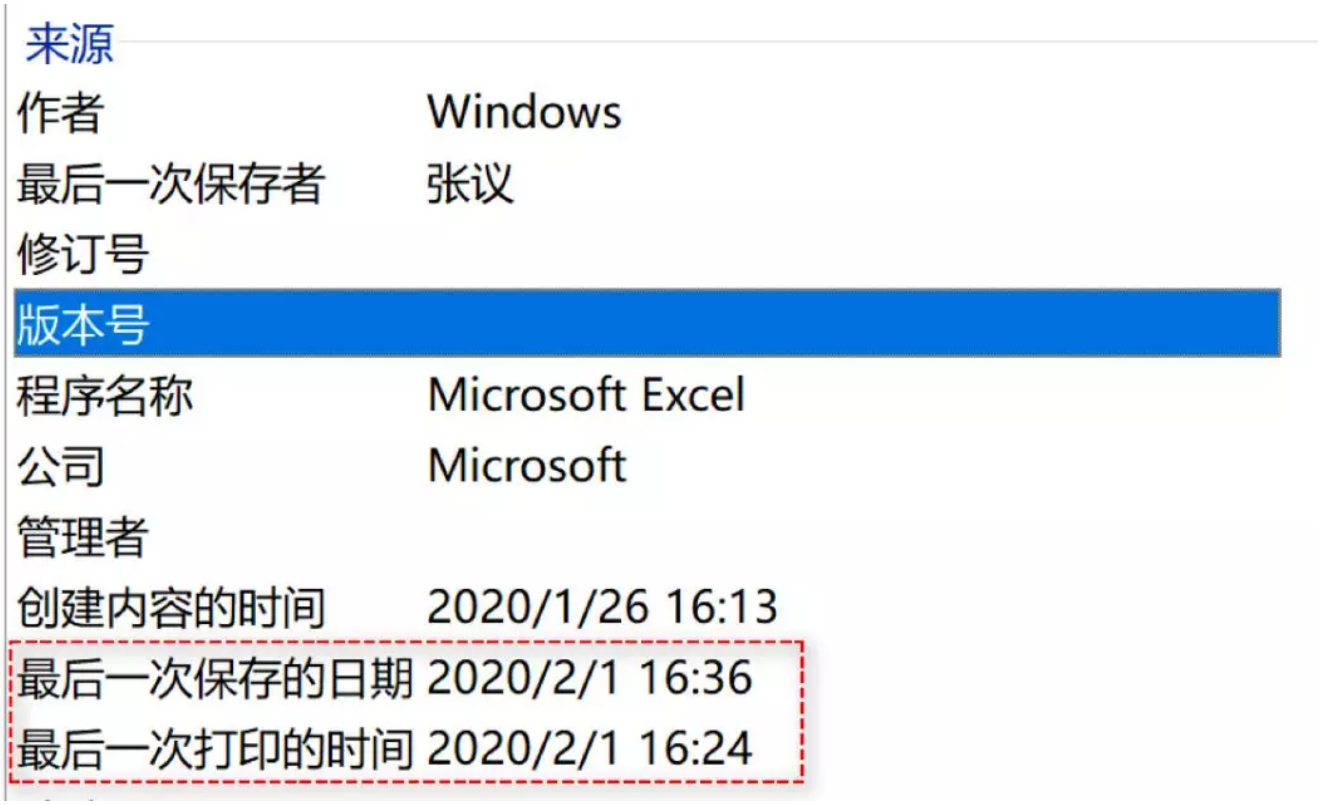
Name	Value
id	33213@qq.com
pass	tef123456
verifycode	

下图为第一个钓鱼文件。

打开后，标题竟然是“基层党组织和党员防控疫情重大事项日报表”。



这说明，该文件很可能是通过破解相关部门的邮箱，截获往来邮件得来。“绿斑”将所截获的文件制成诱饵，似针对某市区政府住建局及疾控部门发起钓鱼攻击，旨在窃取相关人员的QQ、网易、新浪等邮箱账密，以及通过窃取的邮箱账密进一步窃取邮箱数据进行情报收集和利用发起鱼叉攻击。诱饵文档为一白文件，但极可能是内部文件。



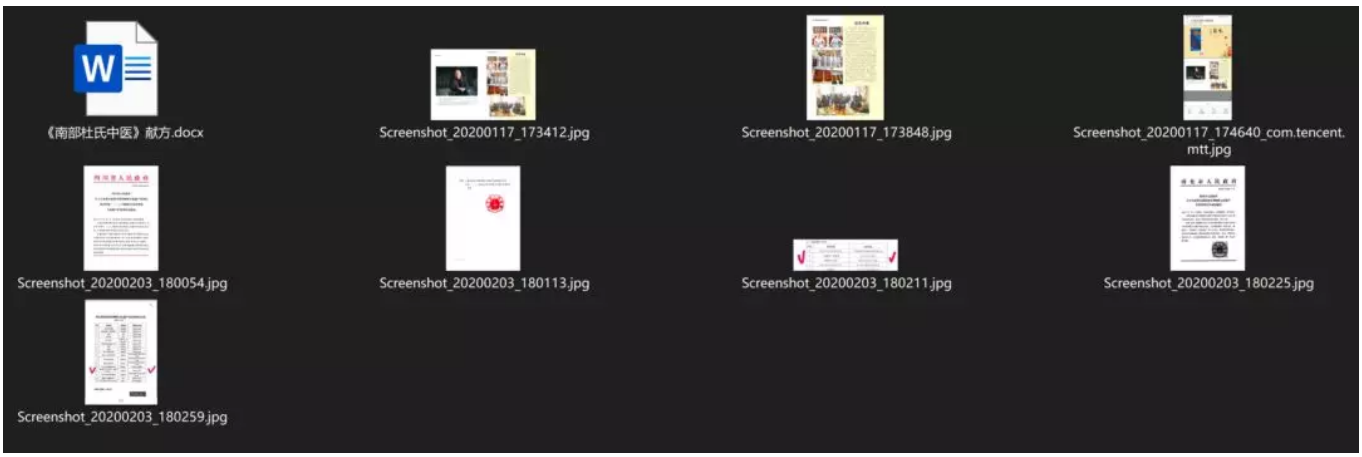
微步情报局认为，从文件内容、文件最后保存日期和文件最后打印日期来看，不排除存在邮箱账密被窃取的可能。

第二个文件则名为“社会面维稳组工作简要总结”。诱饵文档目前无法下载，但从攻击时间节点和诱饵主题推测，这应同是利用疫情针对政府相关部门发起的钓鱼攻击。

第三个文件名为“《南部杜氏中医》献方.7z”。同样结合攻击时间节点以及诱饵主题猜测，这是台湾黑客组织“绿斑”在给大陆恶意“献方”，利用疫情中人们希望平安的心理，使用带有病

毒的文件进行网络钓鱼攻击。两岸本一衣带水，但自新冠病毒爆发以来，台湾当局不仅封锁物资，还对大陆展开网络间谍活动，可谓毫无情义、恶劣至极。

看似是普通的Word文档，实则暗藏着重重恶意。



根据微步情报局的提供的信息显示，该文件于2月5日制作完毕，开始投入攻击。

针对此次攻击，微步情报局提出如下建议：

1、 在输入邮箱账号和密码时，一定注意查看地址栏的网站是否是合法网站。此外，建议使用强密码策略并定期更换密码。如果已经遭遇此类钓鱼攻击，应立即修改相关密码并进行排查。

2、 警惕邮件钓鱼，不要轻易点击和打开未知邮件中的链接和附件，对安全性存疑的邮件通过其他方式进行二次确认，使用微步云沙箱对可疑链接和附件进行分析。

目前，微步在线旗下安全DNS防护产品OneDNS入选中关村发布首批抗击疫情的新技术新产品新服务清单。疫情环境下的远程办公同样面临各类网络威胁，OneDNS能够有效防护勒索软件、钓鱼、木马、病毒、蠕虫和APT攻击等多种网络威胁，从而保障远程办公中员工个人设备和企业数据的安全。此外，微步在线旗下产品TDP、TIP和API都能对本次攻击做出检测和防范。

疫情汹汹，保卫网络空间也十分重要。在目前的紧要关头，微步情报局建议相关部门引起重视，并进行对邮箱等个人账号的严格排查，我们相信，借助扛疫舆情发起攻击的卑劣行为，

无法扰乱中国军民扛疫的决心，更无法扰乱社会和民心的稳定。每一次定期排查、甚至每一个强密码，都可能挡住一次来自外部的黑客攻击。

你若不慎，别有用心者就会见缝插针；你若安全，就是给国家的安全贡献力量。

关于“微步情报局”

微步情报局，即微步在线研究响应团队，负责微步在线安全分析与安全服务业务，主要研究内容包括威胁情报自动化研发、高级APT组织&&黑产研究与追踪、恶意代码与自动化分析技术、重大事件应急响应等。

微步情报局由精通木马分析与取证技术、Web攻击技术、溯源技术、大数据、AI等安全技术的资深专家组成，并通过自动化情报生产系统、云沙箱、黑客画像、威胁狩猎系统、自动追踪溯源系统、威胁感知系统、大数据关联知识图谱等自主研发的系统，对微步在线每天新增的百万级样本文件、千万级URL、PDNS、Whois数据进行实时的自动化分析、同源分析及大数据关联分析。微步情报局自设立以来，累计率先发现了包括数十个境外高级APT组织针对我国关键基础设施和金融、能源、政府、高科技等行业的定向攻击行动，协助数百家各个行业头部客户处置了肆虐全球的WannaCry勒索事件、BlackTech定向攻击我国证券和高科技事件、海莲花长期定向攻击我国海事/高科技/金融的攻击活动、OldFox定向攻击全国上百家手机行业相关企业的事件。

政府

新华社 | 农业部 | 国家信息中心

海淀区政府 | 浦口信息中心

金融

人民银行清算中心

工商银行 | 农业银行 | 中国银行 | 交通银行

招商银行 | 民生银行 | 光大银行 | 微众银行

中国银联 | 农信银资金清算中心 | 蚂蚁金服

渤海银行 | 南京银行 | 浦发银行

厦门国际银行 | 江苏农信 | 山东农信

山东城商行联盟

中国平安 | 安邦保险 | 前海人寿 | 太平洋保险

银河证券 | 安信证券 | 国信证券 | 证通股份

广发证券 | 东方证券 | 中信建投证券 | 凡普金科

兴业证券 | 光大证券 | 中信集团 | 华泰证券

中信证券 | 国泰君安证券 | 东方花旗证券

能源

中国石油 | 国家电网 | 南方电网

互联网

腾讯 | 百度 | 字节跳动 | 金山云 | 爱奇艺 | 京东 | 美团

唯品会 | 汽车之家 | 瓜子二手车 | Bilibili | 太极云

更多

VIVO | 顺丰速运 | 中国移动

千寻位置 | 中兴通讯 | 波司登 | OPPO

THREATBOOK PARTNERS

合作伙伴

以下企业或产品中集成了微步威胁情报：

阿里云态势感知

情报模块(需单独采购)

互联网域名系统北京市工程研究中心

DNS硬件防火墙

以下企业或产品**没有集成**微步威胁情报：

深信服

安恒信息

绿盟科技

瀚思科技

等其他企业

产品合作信息以微步在线官方披露为准

我们将随时更新合作伙伴名单及合作类别