Summer Live

CIS夏日版

网络安全创新大会

Cyber Security Innovation Summit

攻防实战—邮件钓鱼实践

3vilK4li

FREEBUF

Summer Live

CIS夏日版

网络安全创新大会

Cyber Security Innovation Summit

攻防实战—邮件钓鱼实践

精准布控&快速上线&主动防御

3vilK4li

FREEBUF

About Me

3vilK4li

@斗象科技-高级安全服务工程师

网安漏洞研究员

攻防钓手

邮箱信息收集

常见的邮箱收集工具

SNOV
https://app.snov.io/domain-search

hunter
https://hunter.io/

VP微匹
http://veryvp.com/

skymen
http://www.skymem.info/

https://github.com/Taonn/EmailAll

theHarvester
https://github.com/laramies/theHarvester

EMAIL GUESS
邮箱穷举猜测工具

邮箱信息收集

邮箱存活清洗

EmailCamel

https://www.emailcamel.com/

EmailVerify.

http://www.emailverify.site/

邮箱侦探
MAIL-VERIFIER.COM

https://www.mail-verifier.com/

VERIFY-EMAIL.ORG
by Emailable

https://verify-email.org/

邮服的选择

现成邮服？

自建邮服？

邮服的选择

现成邮服

使用邮件服务提供商提供的邮件服务器或账号

- ✓ 快速部署
- ✓ 送达率高
- ✓ 隐蔽性高
- ✗ 用户限制
- ✗ 发件频率限制

自建邮服

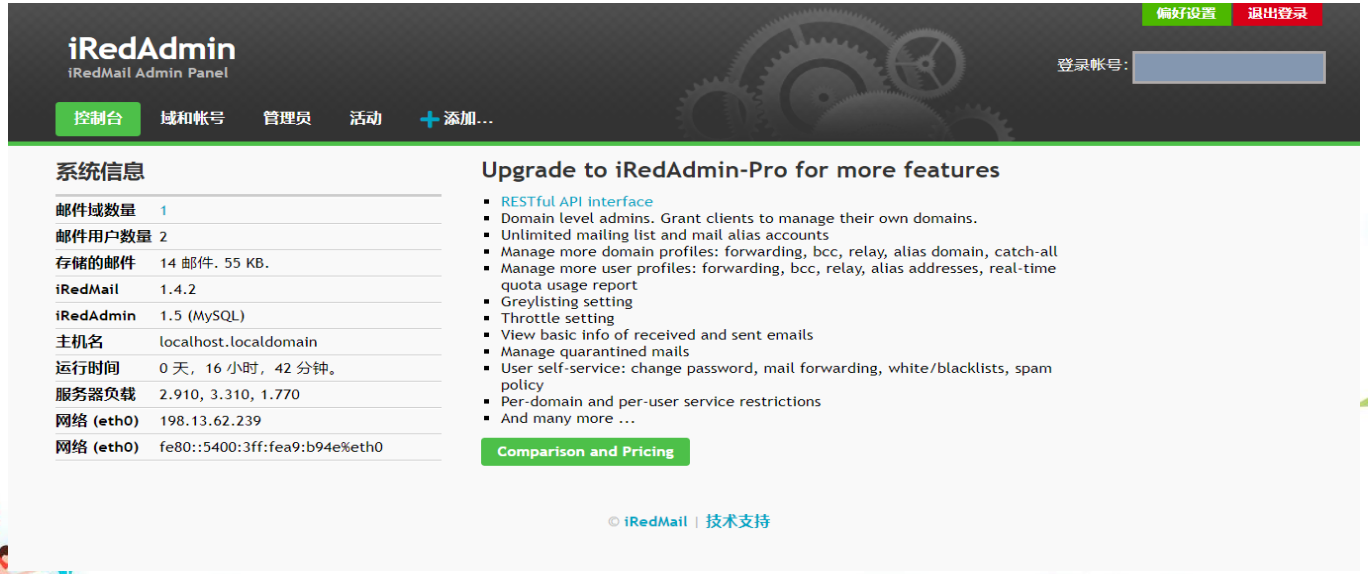
使用自定义的域名进行搭建邮件服务器

- ✓ 发件频率高
- ✓ 发件用户自定义
- ✓ 可变发件IP
- ✗ 邮服配置复杂，25端口开放受限
- ✗ 多因素影响送达率

邮服的搭建

邮件服务的选择

https://reurl.cc/KrDpvg



邮服的搭建

为什么我的邮件发不出去？？

IP信誉度

域名选择

域名信誉

SPF/DKIM/DMARC/PTR

SSL证书、S/MIME证书

邮服的搭建

为什么我的邮件还是被拒收?

可能是TLDs 顶级域名惹的祸!

邮服的搭建

SpamAssassin觉得你可以改进一下 -2

著名的垃圾邮件过滤器 SpamAssassin。得分: -2。
得分低于 -5 通常被认为是垃圾邮件。

-0.1	DKIM_SIGNED	Message has a DKIM or DK signature, not necessarily valid **This rule is automatically applied if your email contains a DKIM signature but other positive rules will also be added if your DKIM signature is valid. See immediately below.**
0.1	DKIM_VALID	Message has at least one valid DKIM or DK signature **太棒了！你的签名是有效的。**
0.1	DKIM_VALID_AU	Message has a valid DKIM or DK signature from author's domain **太棒了！你的签名是有效的，并且和你的域名相匹配。**
0.1	DKIM_VALID_EF	Message has a valid DKIM or DK signature from envelope-from domain
-0.499	FROM_SUSPICIOUS_NTLD	From abused NTLD
-1.725	PDS_OTHER_BAD_TLD	Untrustworthy TLDs URI: mail.n[redacted].space (space)
-0.001	SPF_HELO_NONE	SPF: HELO does not publish an SPF Record
0.001	SPF_PASS	SPF: sender matches SPF record **太棒了！你的SPF记录是有效的。**

邮服的搭建

换个域名试一下!

邮服的搭建

成功了！！

测试测试

Thx_xhT

发给 [redacted]

发件人: [redacted]

收件人: [redacted]

时间: 2022年5月19日 (周四) 12:17

大小: 3 KB

这是一封来自mail.[redacted].com的测试邮件。

文案设计

超链接

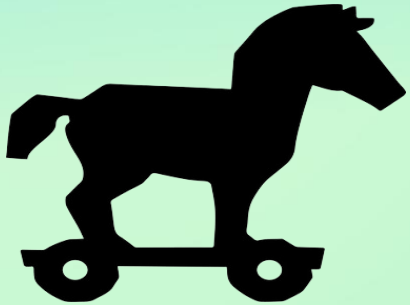
相信页面真实性

输入账号密码

页面停留

获取账号权限

获取主机权限



打开附件

宏（office or wps）

下载文件

文件运行

文案设计

几个重要的文案设计方向

用户利益

公司事务

时事热点

文案设计

诱惑：一封掉钱的邮件！

XX市卫健委关于2021年春节期间留X过年补贴通知

为了积极响应国家政策，减少国家防控压力，XX市卫健委提倡2021年春节期间尽量不离开XX市，对过年期间留在XX市的人员给予生活补贴1500元/人。一定要离开XX市的，需提前报备做好登记工作。为了对自己和身边的人负责，望大家在假期期间做好自身防护防控。不要前往任何中高风险地区，在假期期间因个人原因导致医学隔离或强制性隔离不能正常上班的，全程费用自理且不带薪。

注意事项:

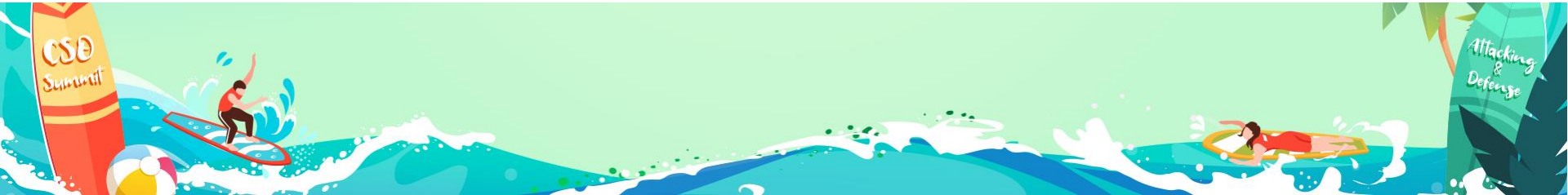
1. 各企业自行安排员工在X的记录情况，春节放假期间全程留X欢度春节的员工奖励1500元/人。(还需提供常用手机行程码和健康码，必须证明是未离开过XX市的)
2. 春节假期结束后（2月19日），各企业对在X过年人员进行统计，汇总后发送到XX市卫健委官方邮箱：wjw.XX@foxmail.com
2. 假期返X上班，每一位员工需提供健康码行程数据以做记录，任何行程异常的个人（去过中高风险地区的同事）需执行隔离14+7并做核酸检测的规定，核酸检测试阴性者方可正常复工。
3. 如疫情新情况，公司会另行通知，盼大家都能留X过年!

为了更好配合国家防疫工作和统计在XX公司2021年留X过年的人员信息，请所有人按照自己情况进行填写:

留X过年的人员点击下载"XX市卫健委关于2021年春节留X人员信息统计表.xlsx";

返乡过年人员请点击下载"XX市卫健委关于2021年春节返乡人员信息统计表.xlsx"。

信息填写完成后请点击发送到wjw.XX@foxmail.com，最晚填报时间为1月29日。



文案设计

几个重要的文案设计方向

用户利益

公司事务

时事热点

文案设计

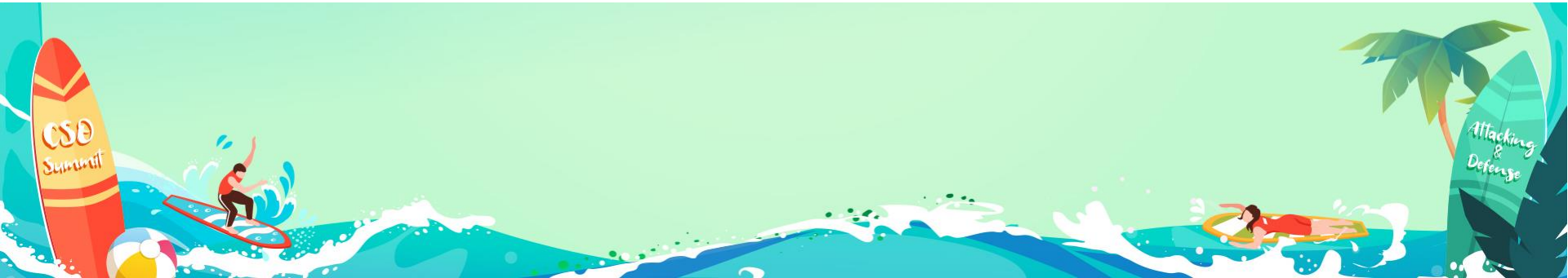
核酸检测的福利

各位好：

据XX疾控和XX卫健委通知，1月26日，XX新增一例新冠肺炎输入病例。目前仍存在23名确诊的无症状，和177例密切接触者，XX新冠肺炎防控工作依旧严峻。为响应XX市核酸检测号召，XX企业与XX疾控中心进行合作，将组织大家进行统一核酸检测。核酸检测要求如下：

1. **点击**下方链接，通过邮箱登陆自己的账户进行下载
   https://oa.xxxxx.com/核酸检测/
2. 或者点击"XX企业核酸检测个人信息登记表.xlsx"下载
3. 如实填写表中的个人信息，重点包括**联系电话，居住小区和紧急联系人信息**
4. **点击**行末的邮件账户，将登记表信息发送到XX企业核酸检测账号hsjc@xxxx.com

由于安排核酸检测人员数量较多，请所有人员在1月28号下班前完成。若逾期未完成填报的人员，将视为放弃核酸检测。



文案设计

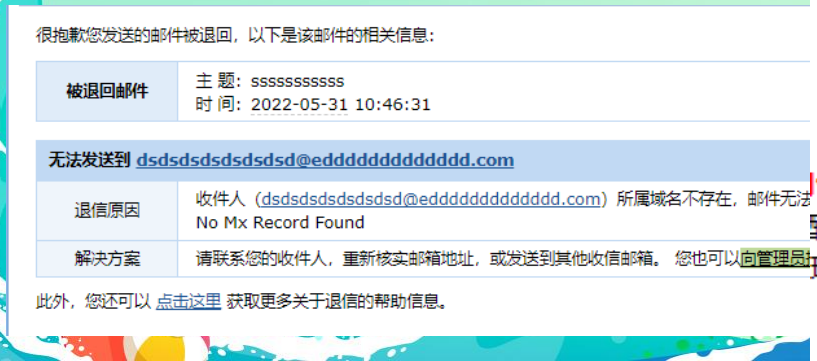
到底要不要让受害者回邮件呢？

增加邮件内容的真实性

更加符合现代办公的要求

受害者可能提高警惕

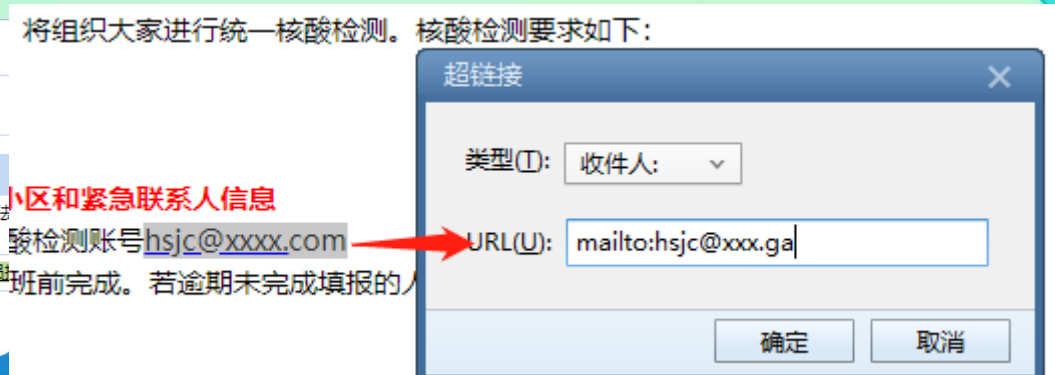
通知类的邮件操作显得多余



很抱歉您发送的邮件被退回，以下是该邮件的相关信息：

被退回邮件	主 题：sssssssssss 时 间：2022-05-31 10:46:31
无法发送到 dsdsdsdsdsdsdsd@eddddddddddddd.com	
退信原因	收件人（dsdsdsdsdsdsdsd@eddddddddddddd.com）所属域名不存在，邮件无法 No Mx Record Found
解决方案	请联系您的收件人，重新核实邮箱地址，或发送到其他收信邮箱。 您也可以向管理员

此外，您还可以 点击这里 获取更多关于退信的帮助信息。



文案设计

几个重要的文案设计方向

用户利益

公司事务

时事热点

文案设计

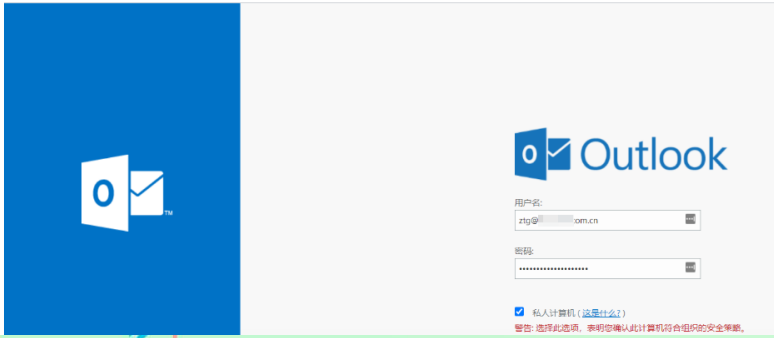
一封完整却又不完整的邮件！

近期攻防演练在即，最近有技术人员发现部分员工的邮箱疑似被泄露，被黑客攻击，向他人发送不当言论。为了杜绝在攻防演练期间再次出现此类问题，上级领导决定，于12月3日（周四）对大家的密码进行重置。重置密码操作由技术支持部进行进行统一操作，请大家配合技术支持部的工作。如有问题，请与技术支持部联系。

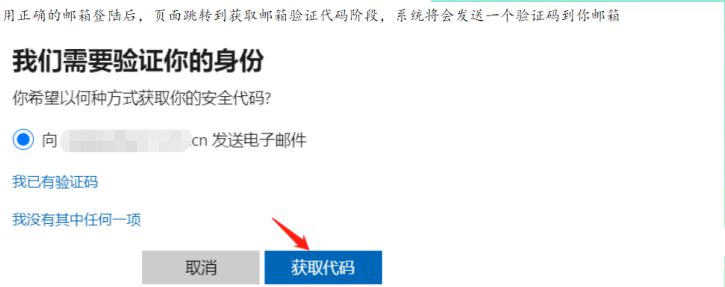
以下是邮件重置的流程：

1. 登陆XX企业统一邮件后台中心，使用用自己的邮箱密码进行登陆

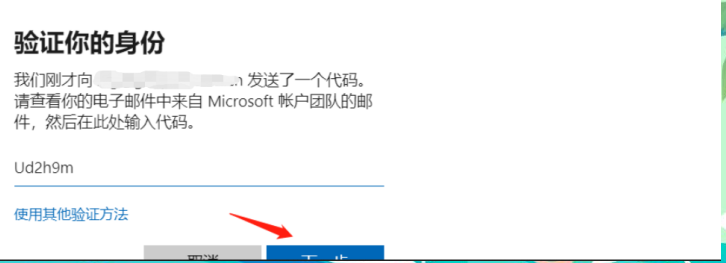
   http://mail.XXXXX.cn



2. 使用正确的邮箱登陆后，页面跳转到获取邮箱验证代码阶段，系统将会发送一个验证码到你邮箱



3. 获取验证码后在下方输入框输入后即可重置密码。重置的密码要求至少8位以上，且必须是大小写和数字的组合，否则重置不会成功。



文案设计

时间魔术

回复： [redacted]**重置企业邮箱的通知** ☆

发件人：**技术支持部** <[redacted]>

时　间：2020年12月3日（星期四）下午3：54

收件人：[redacted]

各位同事：

技术支持部发现部分同事的邮箱还未进行重置密码，麻烦还未对邮箱进行重置密码的同事于今天内进行重置工作。谢谢各位的配合。

如有问题，请与技术支持部联系。

文案设计

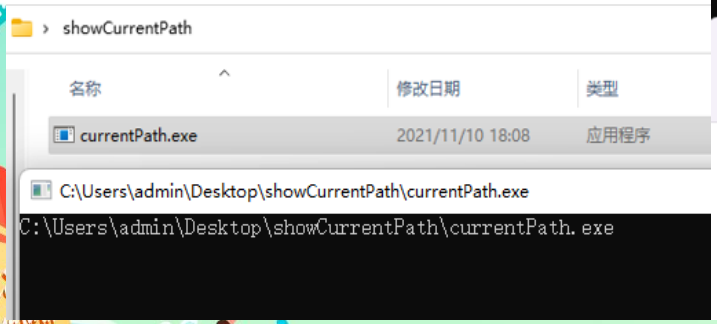
容易忽略的几点

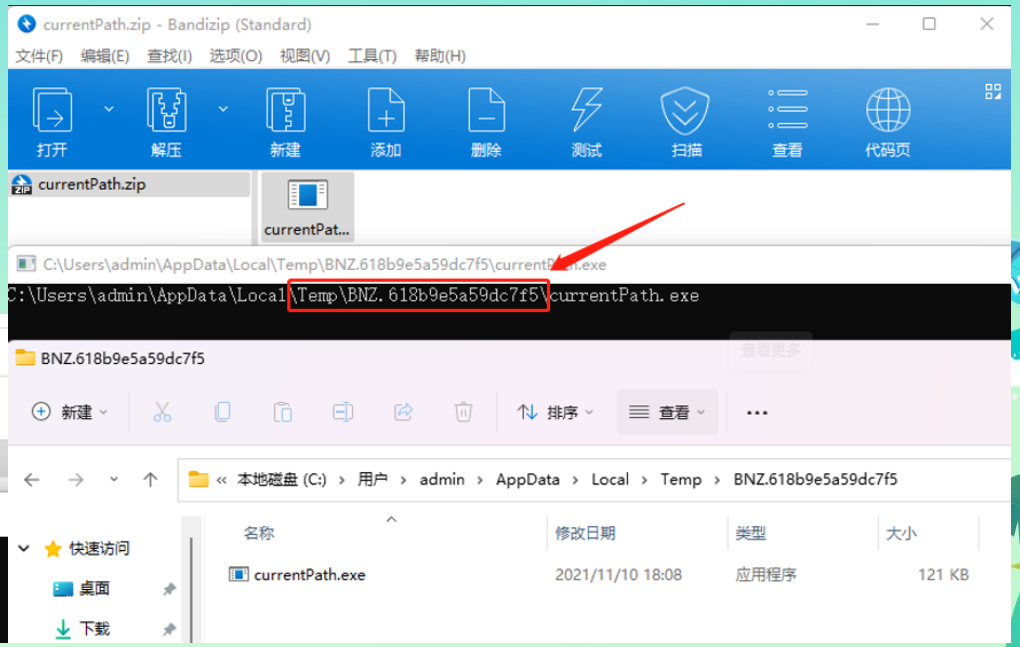
- 发件时间
- 惰性心理
- 发件内容合理性
- 暗示性动词
- 企业签名

附件木马的设计

压缩包的秘密（EXE）

```
#include<stdio.h>

void main(int argc, char* argv[])
{
        printf("%s\n", argv[0]);
        getchar();
}
```



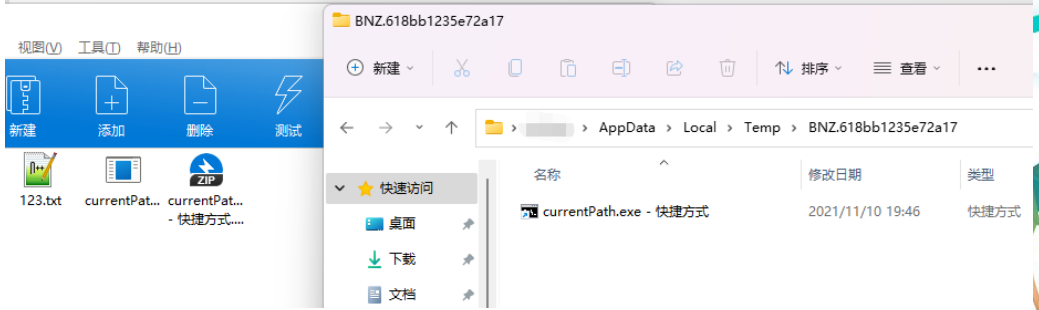


附件木马的设计

压缩包的秘密（LNK）

```
C:\Windows\System32\cmd.exe /c  dir >>
C:\Users\admin\Desktop\showCurrentPath\
123.txt && pause
```

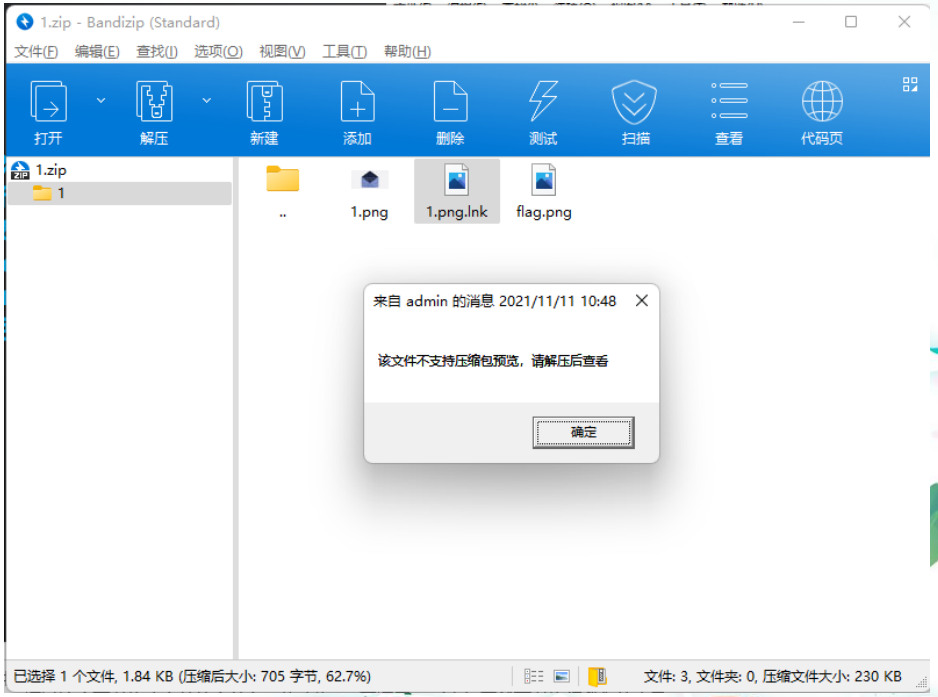
```
 驱动器 C 中的卷没有标签。
 卷的序列号是 7C08-21AB

 C:\Users\admin\AppData\Local\Temp\BNZ.618bb1235e72a17 的目录

2021/11/10  19:46    <DIR>          .
2021/11/10  19:46    <DIR>          ..
2021/11/10  19:46               880 currentPath.exe - 快捷方式.lnk
               1 个文件            880 字节
               2 个目录 31,410,606,080 可用字节
```



附件木马的设计

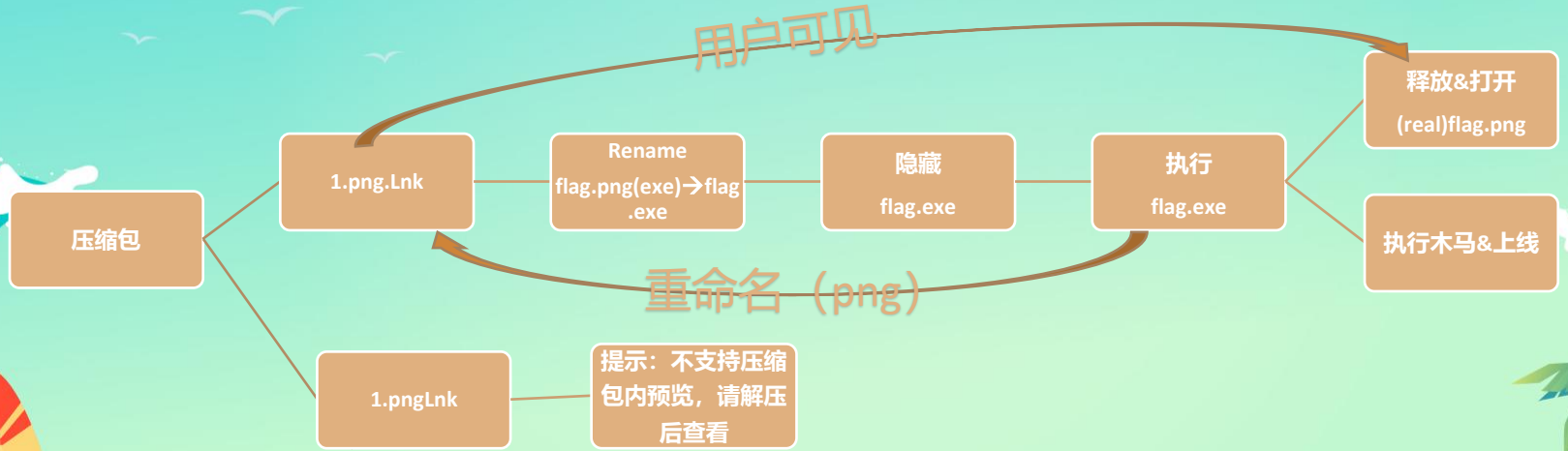
Lnk – 双击“图片”也能上线

```
%windir%\system32\cmd.exe /c  if exist “flag.png” ( ren flag.png flag.exe && attrib +s +h flag.exe && start flag.exe && ren flag.exe flag.png ) else ( msg %username% /time:10 "该文件不支持压缩包预览，请解压后查看")
```



附件木马的设计

Lnk – 双击“图片”也能上线

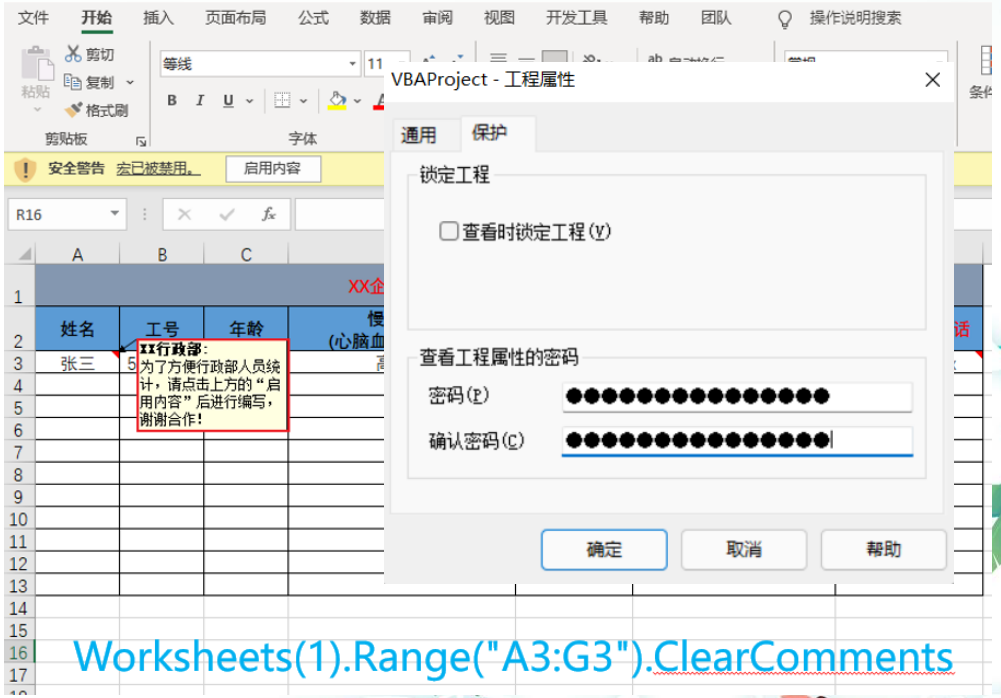


附件木马的设计

Office Macro—批注也疯狂

https://github.com/outflanknl/EvilClippy

https://github.com/PDWR/3vilMacro




```
Worksheets(1).Range("A3:G3").ClearComments
```

附件木马的设计

解压密码的艺术

Dear All:

近段时间，我司开展了一次模拟真实攻击的网络攻防演练活动，本次活动旨在全面提升我局人员的安全意识，以及我局网站的安全。在前期的摸排工作中，发现大部分同时所使用的终端都没有安装公司统一采购的杀毒防护软件，或者安装了杀毒防护软件后未按照最新的要求去配置，采用了宽松的安全防护措施。现接到集团总部的要求，在本次攻防演练期间，所有人的电脑必须安装公司统一采购的杀毒防护软件，并按照要求开启"严格"等级的防护模式。

软件统一安装方法：

1. 下载本邮件附件--"终端安全防护EDR"（解压密码为："2022安全"，拼音全称）
2. 双击软件，选择安装位置后，下一步，进行安装
3. 安装后请第一时间在软件设置--安全等级中，选中"严格模式"。

（软件运行后会自动检测是否已经开启严格模式，如果显示已经开启"严格模式"，

水坑 or 直接投递木马?

兵贵不一定神速!

水坑 or 直接投递木马?

水坑钓鱼的魅力

使用受害者企业邮服内部发件

获取企业邮箱通讯录

增加信任度

防！几招教抵御钓鱼邮件

两个原则!

四观察:

- 邮件来源
- 邮件标题
- 正文措辞
- 正文签名

两戒备:

- 正文链接
- 邮件附件

防！几招教抵御钓鱼邮件

两个稳妥！

心态要稳

- 沉着冷静
- 及时上报
- 梳理经过
- 防患未然

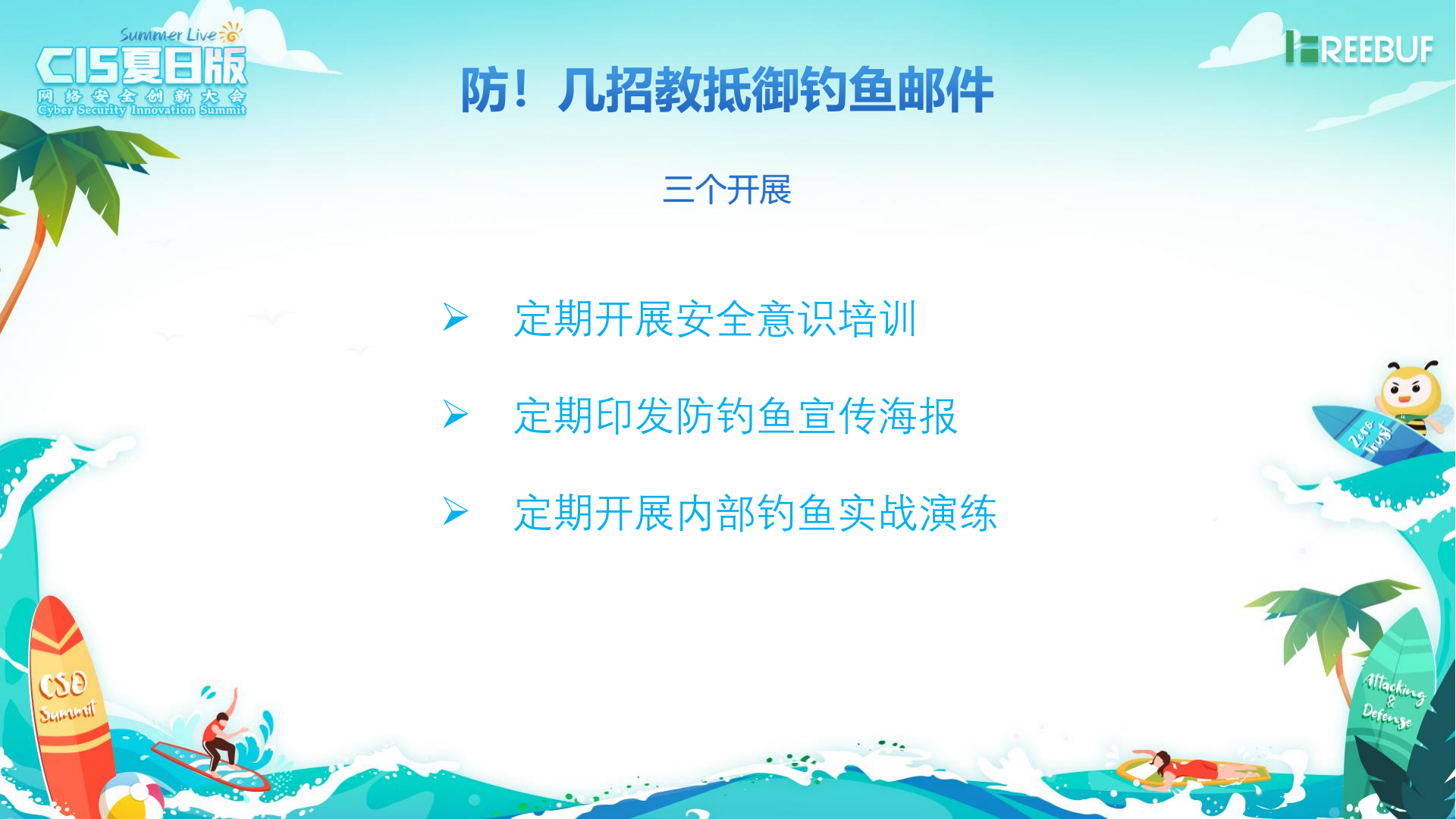
操作要稳

- 安装杀毒软件
- 不在非官方站点输入账号密码
- 确认链接来源
- 做好登录辅助认证

防！几招教抵御钓鱼邮件

三个开展

- 定期开展安全意识培训
- 定期印发防钓鱼宣传海报
- 定期开展内部钓鱼实战演练




Summer Live
CIS夏日版
网络安全创新大会
Cyber Security Innovation Summit
Thanks!
FREEBUF
CSO Summit
Zero Trust
Attacking & Defense