我叫 AMEER FIRZA，来自马来西亚。我和其他几个伙伴一直从事于发送钓鱼邮件给中国的公司。到目前为止，我们从中国的公司这里大概获得了 400 多万美金。当然，其中一部分的钱我们给了政府官员。

现在我打算放弃这个工作，因为我觉得终有一天我会被逮捕。为了表示道歉我写了一些我们常见的手法，给大家参考，希望中国的公司能看到。我们东南亚这里从事这样的人很多，你们随时随地都存在威胁。

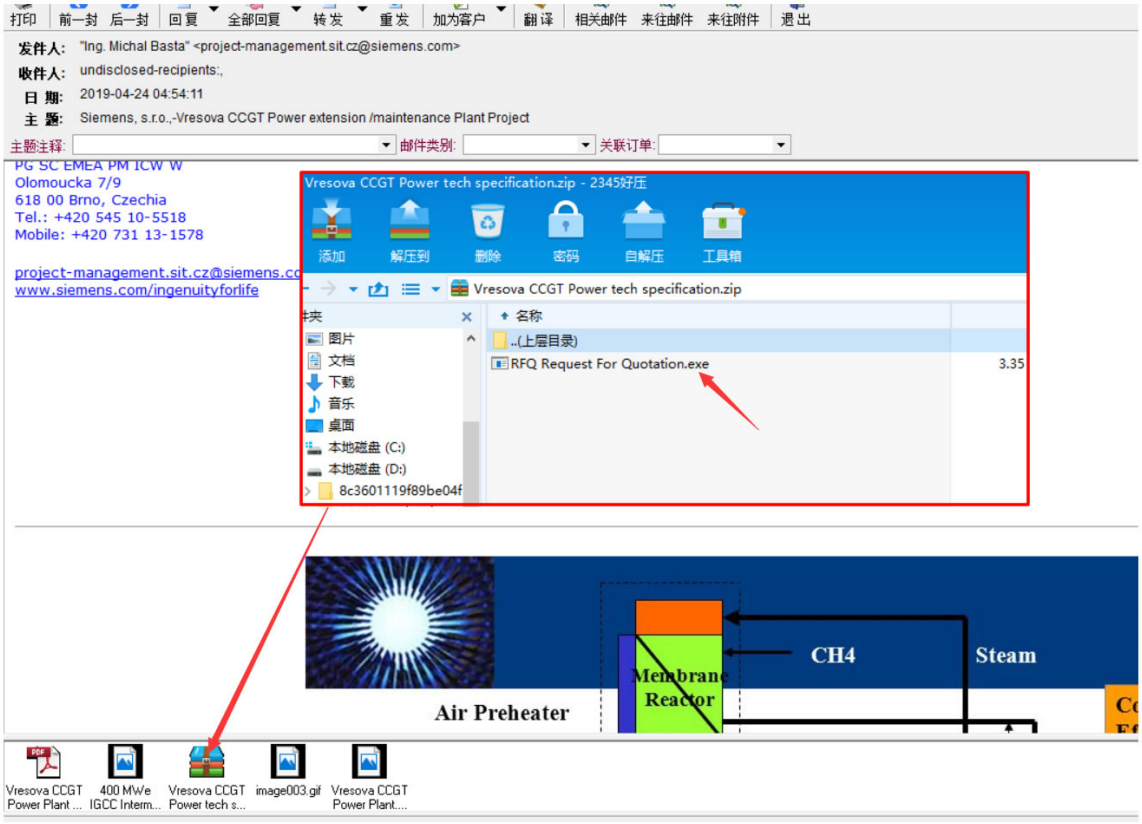
我节选了一些我的日记，公开给你们参考。

2018 年 1 月 9 日

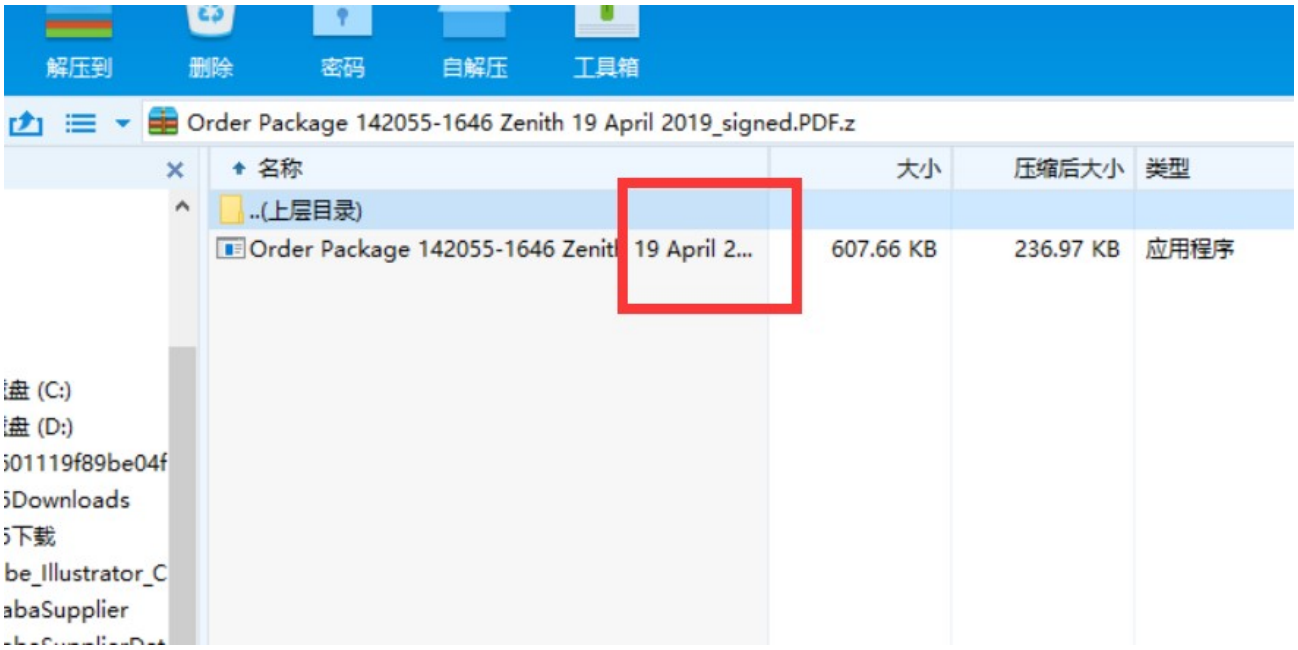
今天我们团队购买到了一个中国公司的邮箱数据库，大概有 20G。真的没想到现在的数据公司会如此强大，对数据的整理如此完善。

我们晚上就进行群发。

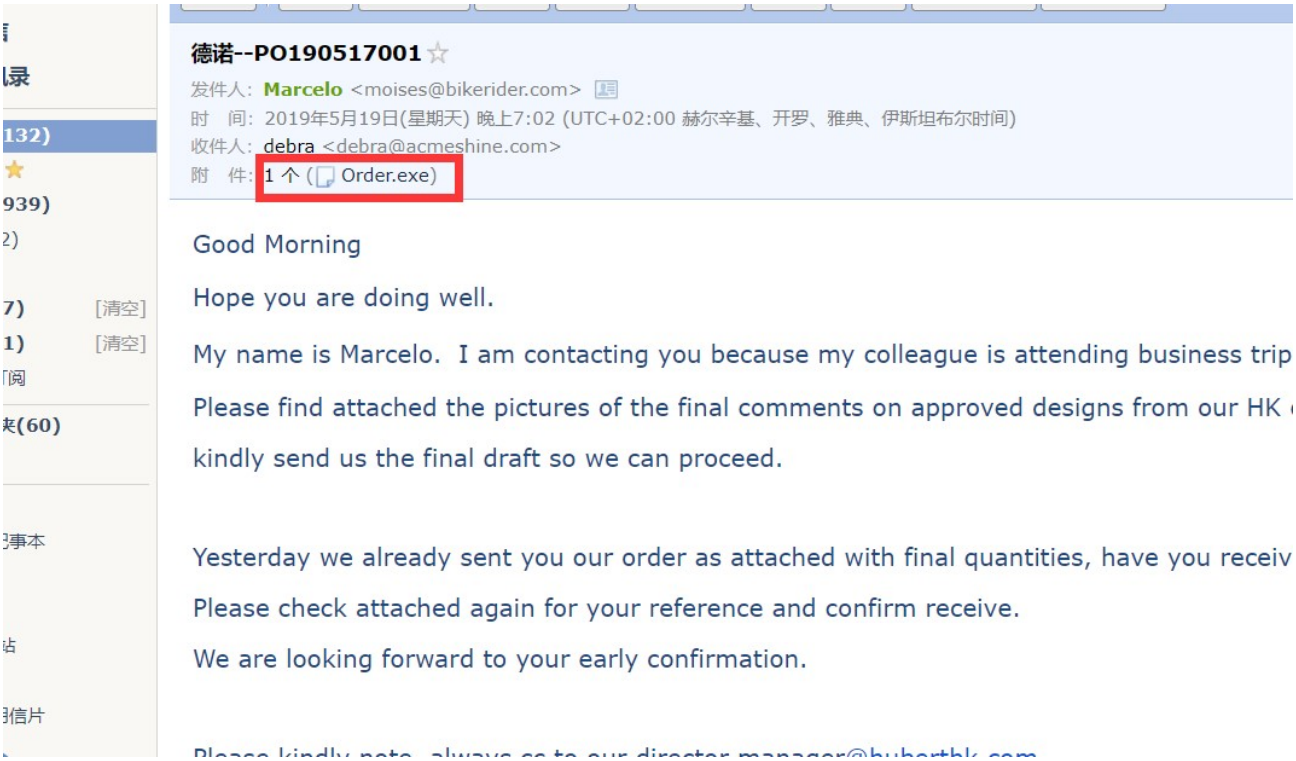
今天我的工作是找到一些新的 TOPIC，这次我找了个“大公司询盘”，西门子公司项目。其他的文件都是正常的，里面有个压缩文件嵌入了 exe 可执行文件木马。



在邮箱附件的压缩文件里放入木马是最常见的做法了。有的时候，为了防止对方看到这个 .exe 文字，我们会把文件名称取得很长，这样他们在解压到时候，不能看到这个文件属性。



有一次我直接做了一个 order.exe，也还是有人会去点开看。



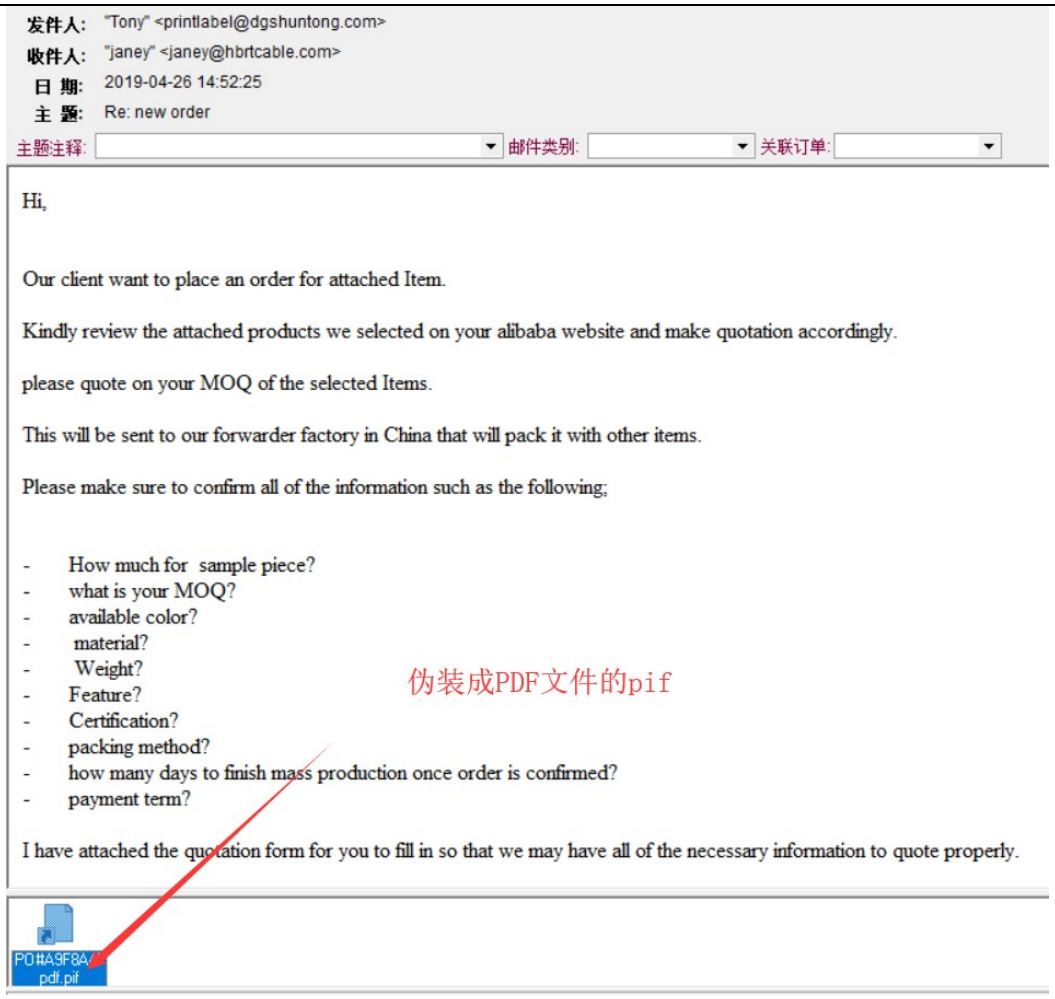
发出后，我在管理后台看到大概有 200 多个木马种植确认。这个木马的主要功能是侦测用户在网页里输入密码的时候，返回相关的数据。

这是我另外一个伙伴开发的程序，这个文件它可以绕过病毒检测程序，然后会扫描整个电脑的常见的程序的密码，比如中国人经常用的 QQ，以及一些邮箱软件。

我们的管理后台收到各类的密码后，我们的另外一组人马，会去做探测，看看能不能登陆，若成功登录，他们就会阅读里面的资料。当然，我们会做潜伏，很长时间的潜伏，主要是看他们的邮件往来，熟悉他们的邮件内容，然后在汇款的时候，他们发出 INOVICE 的时候，我们立刻做一个相同的 INVOICE，用我们这里的公司的账号，告诉客人银行账户做了修改。

当然大部分的客户他们会来确认一次，若客户比较警觉，我们一般就会被发现。然后我们会暂停行动。但是只要他们汇款过来，那基本上这个钱就到我们手里了。

还有一个文件格式我也经常用到，那就 pif 格式，我也用它来种植木马。



2018 年 3 月 9 日

今天我负责了一个新的 case，邮件跟踪小组的人说快钓到一条大鱼，我开始负责“切换”，切换什么呢，就是我们去注册一个新的域名，和被跟踪者的类似的域名，比如把 i 变成 l，或者 l 变成 i，或者 s 变成 z，或者域名后面就增加一个 s，反正让人基本上一眼看过去是一样的，很难一下子辨识出来不同的。

“切换”完成后，我们这里就有了一个和被跟踪者“一样”的邮箱，我们会设置里面的所有的发件人名称，公司资料，所有的一切都是和原来的邮箱一样的。

等被跟踪者发送银行付款的资料后，我们会马上接管过去，用新的邮箱发送过去一份新的修改后的 INVOICE 资料。这样，客户若有疑问，回复过来再次确认，我们会做一个邮件的回复做确认。同时，我们会监控老的邮箱，如客人有发过去老的邮箱，我们立刻做删除。

这次切换很成功，我们账号里汇进来 3 万多美金。。。

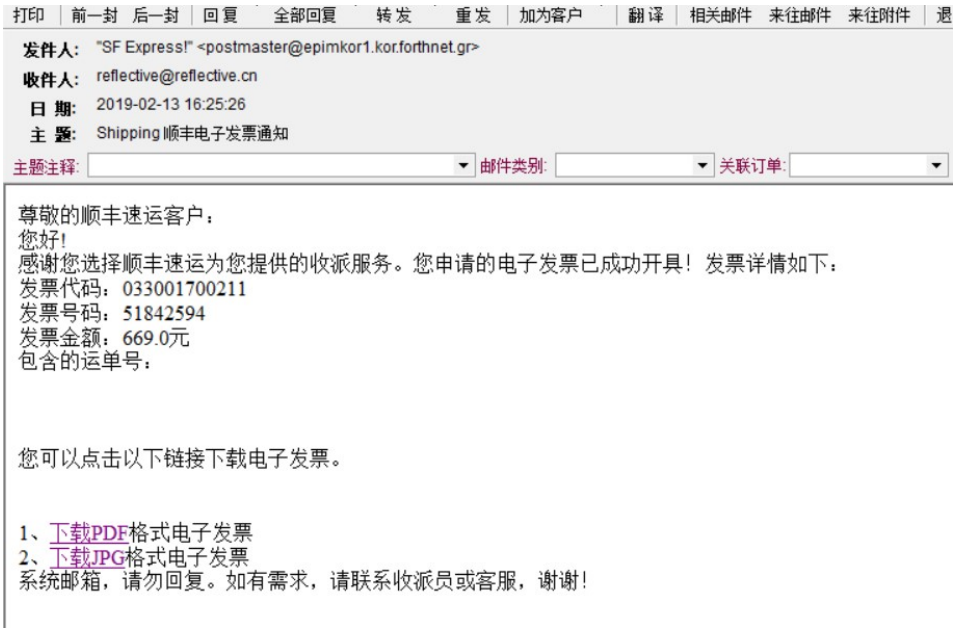
“切换”有个弱点就是若客户打电话给被跟踪者或者用其他社交聊天工具确认，我们就会被暴露。

2018 年 5 月 1 日

这个月我需要做新的文案，找一些新的“鱼饵”。

现在中国很多地方可以用电子发票来做财务，这倒是一个好机遇，我可以做做一些电子发票的对账单下载链接来让一些人输入邮箱密码。

今天做了一个顺丰发票的模板：


打印 | 前一封 后一封 | 回复 全部回复 转发 重发 | 加为客户 | 翻译 | 相关邮件 来往邮件 来往附件 | 退

发件人: "SF Express!" <postmaster@epimkor1.kor.forthnet.gr>
收件人: reflective@reflective.cn
日 期: 2019-02-13 16:25:26
主 题: Shipping 顺丰电子发票通知
主题注释: 邮件类别: 关联订单:

尊敬的顺丰速运客户：
您好!
感谢您选择顺丰速运为您提供的收派服务。您申请的电子发票已成功开具！发票详情如下：
发票代码：033001700211
发票号码：51842594
发票金额：669.0元
包含的运单号：

您可以点击以下链接下载电子发票。

1、下载PDF格式电子发票
2、下载JPG格式电子发票
系统邮箱，请勿回复。如有需求，请联系收派员或客服，谢谢!

下载链接点进去就是输入邮箱密码。这样的钓鱼只对一些头脑简单的人的。但总是会有人去输入密码。

以及另外几个：


« 返回 | 回复 | 回复全部 | 转发 | 删除 | 彻底删除 | 举报 | 拒收 | 标记为... | 移动到...

SF- Express送货服务

发件人：Express Shipment <turbofui@hotmail.com>

时　间：2019年4月19日(星期五) 上午9:23

收件人：liningyao <liningyao@msn.com>

Dear liningyao@msn.com 您的包裹已于2019年3月25日到达我们的邮局，追踪号码是91175

审核地址

其实光看看发件人的邮箱就会被发现，因为顺丰的网址是 sf-express.com，但总会有人不仔细看的。

2018 年 5 月 2 日

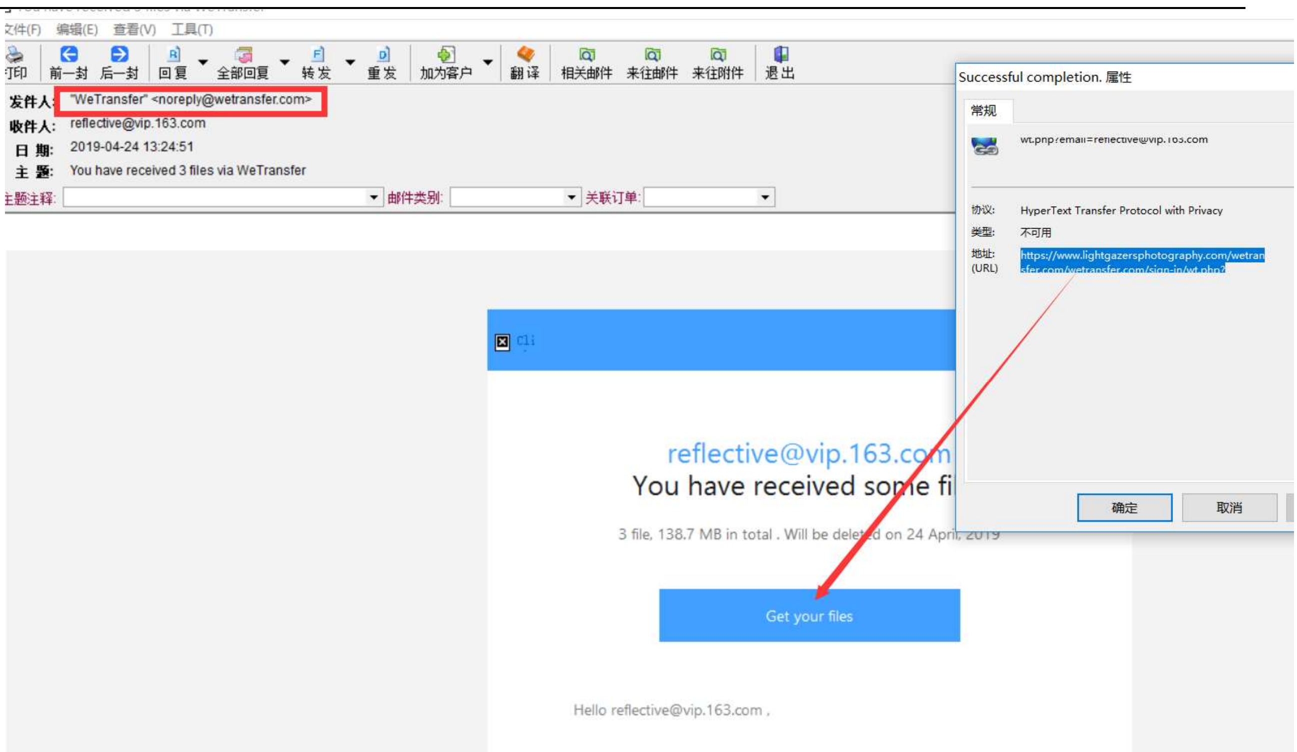
昨天的顺丰钓鱼邮件，我感觉有点太 low，发件人是很容易被看到。

今天我用匿名邮件服务器，做了一个新的模板。

Wetransfer.com 是广泛被被用来大文件转发。我找到了一个服务器，可以任意配置发件人的名称和邮箱。

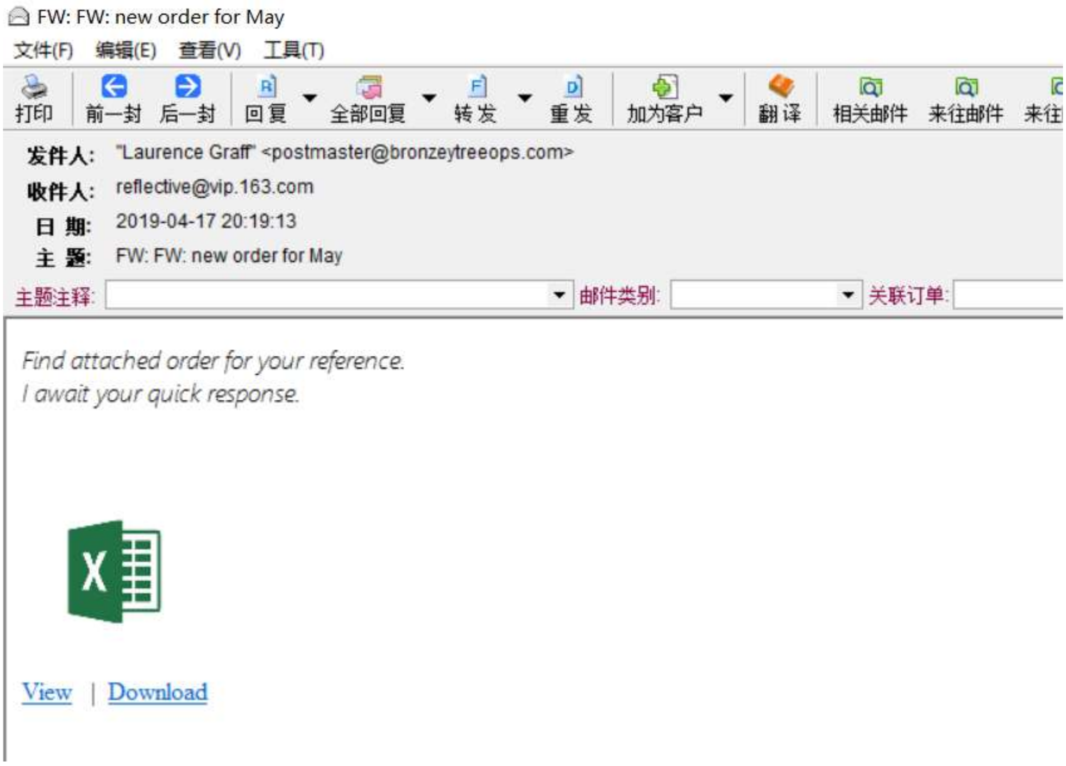
在内容里面，我做了一个输入密码的链接。这个链接是无法改变的，因为它是我们密码收集服务器上的。

还是那句话：总是会有人输入的。

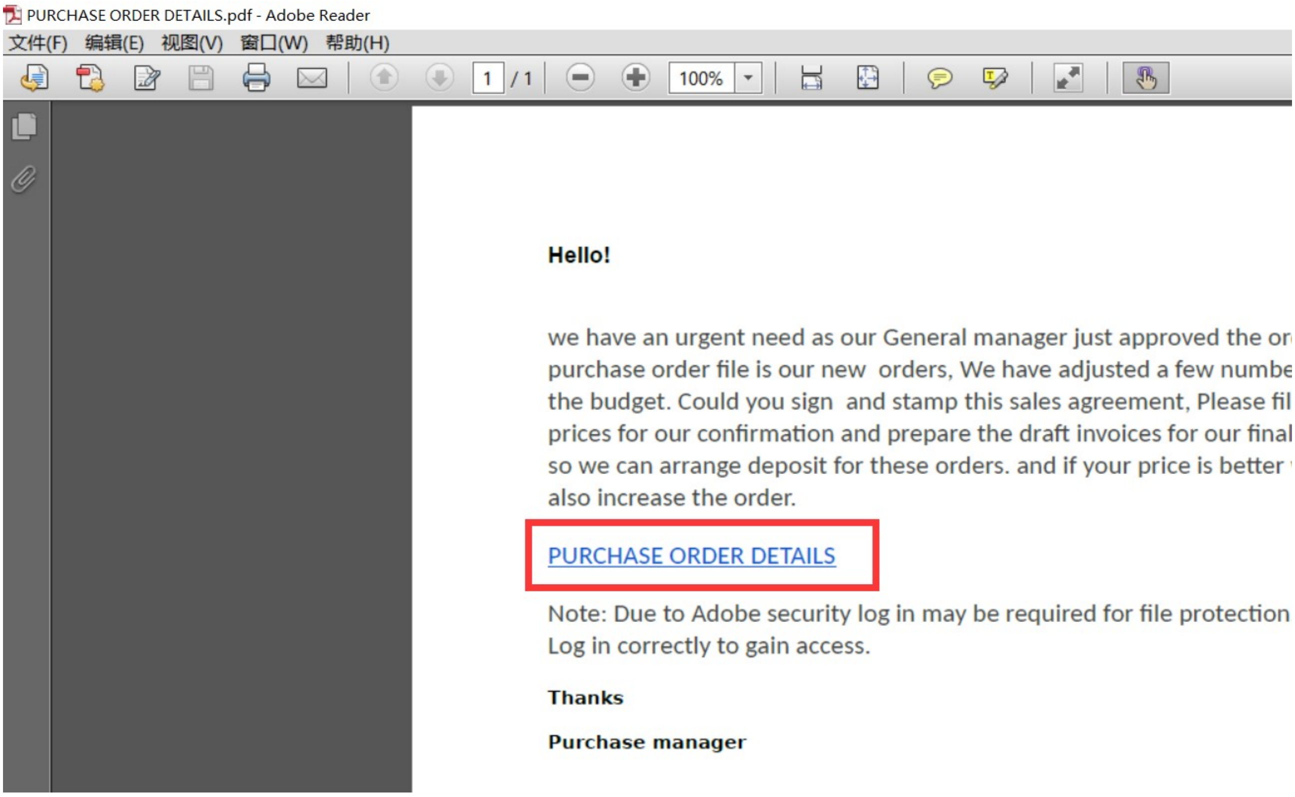


或者有的模板加个下载的文件的图标：

下载链接点进去就是输入邮箱密码。这样的钓鱼只对一些头脑简单的人的。但总是会有人去输入密码。



有的时候，我也会做一些 PDF 的询盘，附件是没有什么病毒的，只是里面有个链接，让收件人点进去“报价”。



事实上，像上面这样的附件，有 2 个问题，一个是邮件的内容是泛泛的，没有任何的针对性的信息，另外一个就是，没有一个公司的采购会发一个附件然后再让你进去点击链接去下载什么其他文件的

还是那句话：总是会有人去下载和输入的。

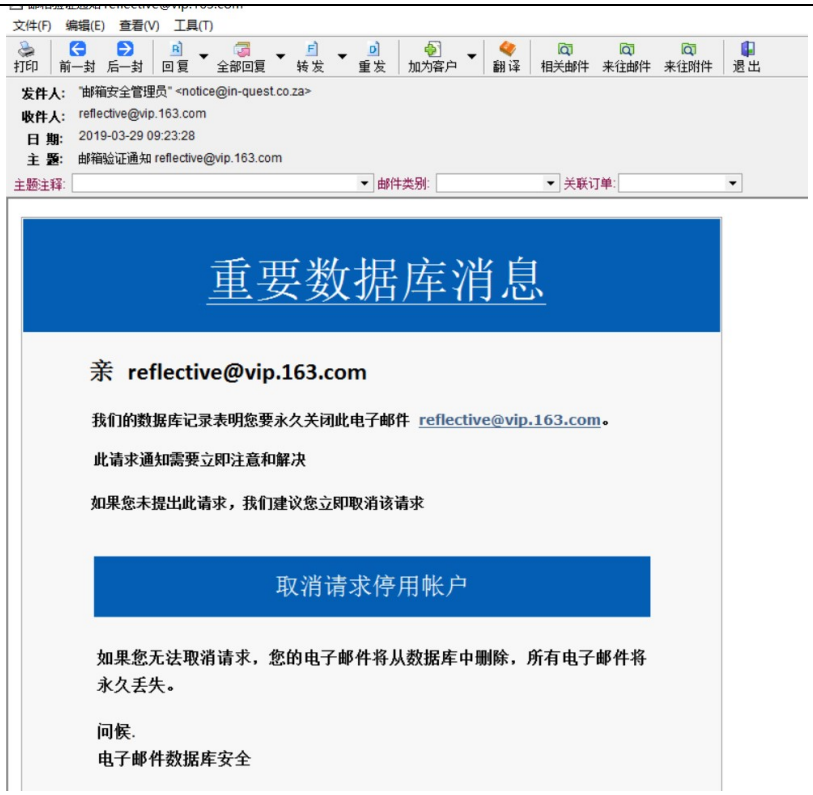
2018 年 7 月 9 日

今天我又做了一个新的文案。就是用警告信，比如告诉对方你的邮箱满了，被禁用。

有的还真的会输入密码进去查看到底有没有禁用。

不过现在很多浏览器也多了一些拦截功能，我们的一些钓鱼链接都被他们侦测到了，用户进入浏览器就会发出警报。

但是这有怎么样呢，我们可以不断制造新的连接。

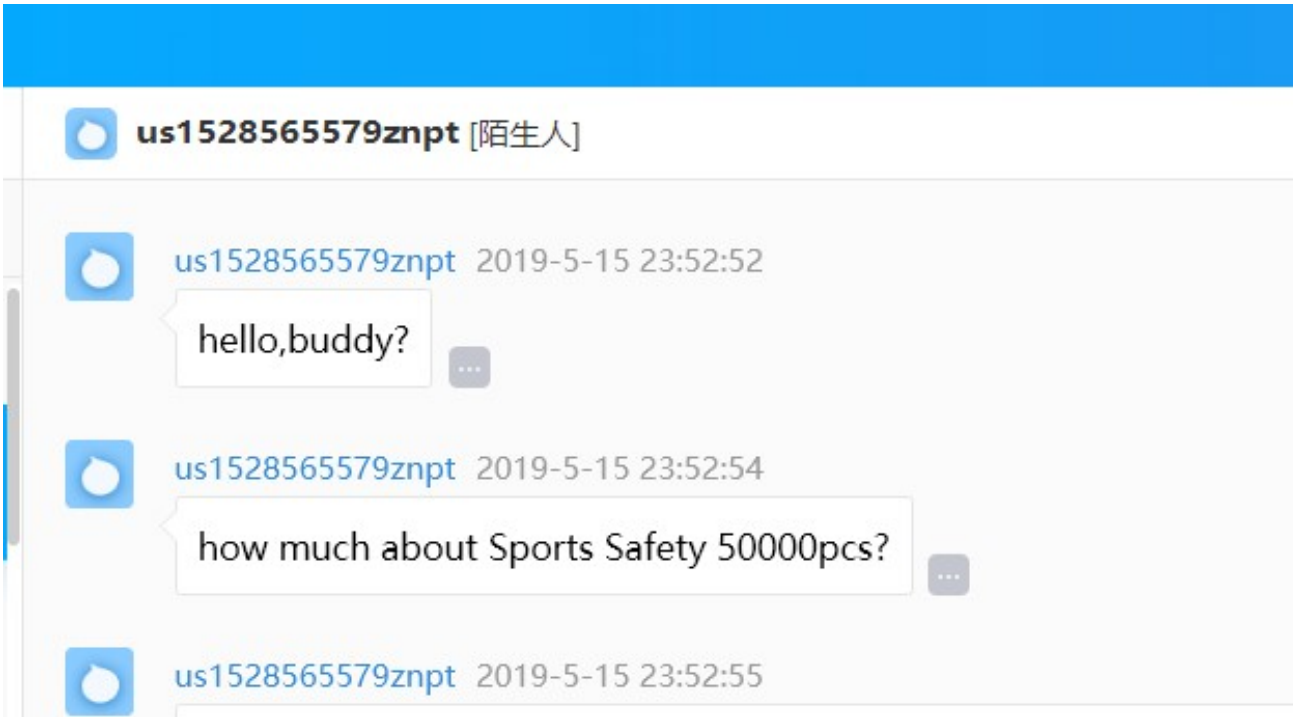


2018 年 9 月 9 日

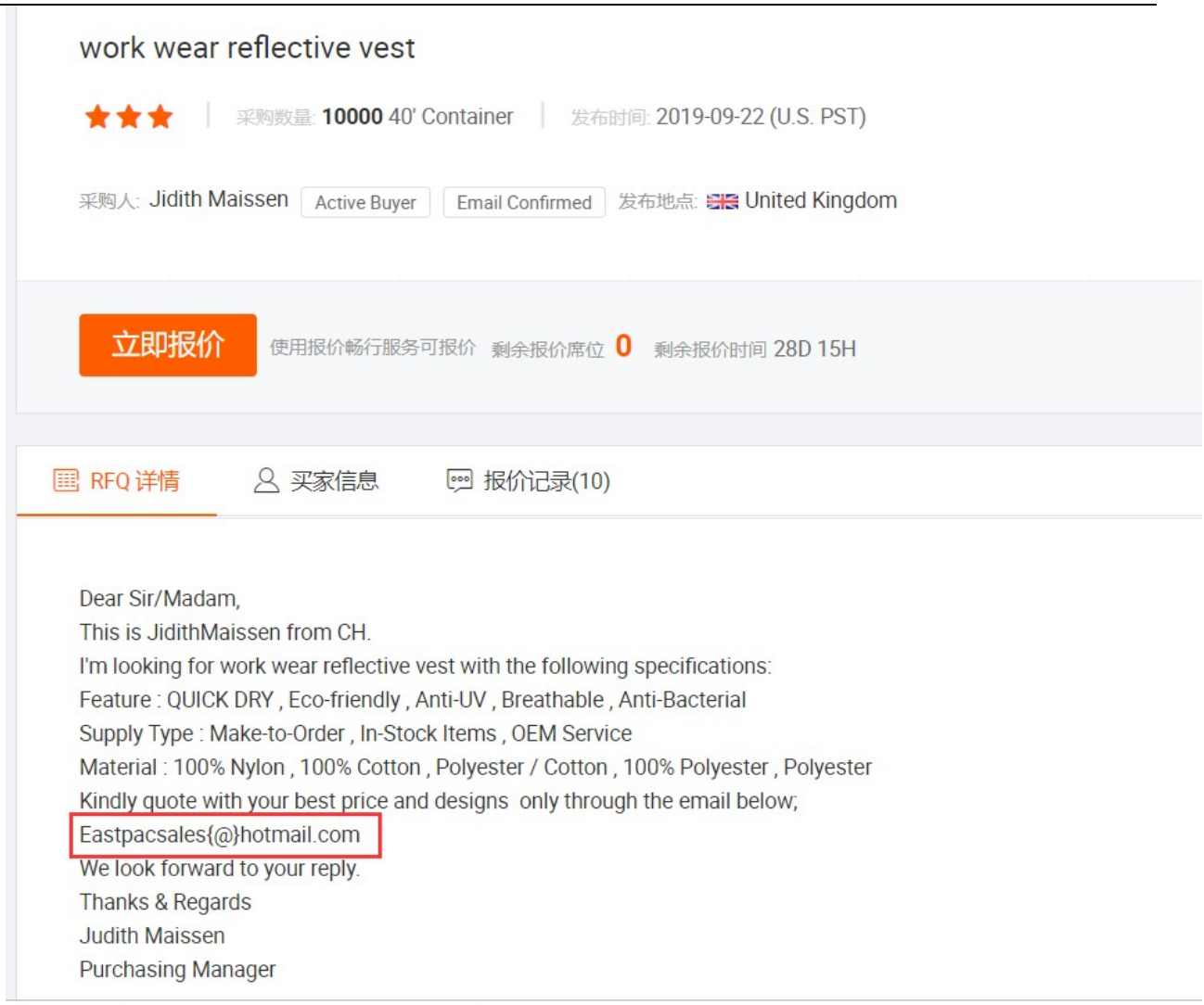
今天在别的团队这里学到了新的内容，发送木马的渠道。

我们发送了很多询盘在中国的电商平台，比如阿里巴巴，中国制造这里，要他们的销售加我们的 QQ 或者微信来发送更多内容。

果然是很多的他们的 sales，加了我们。我们就把木马包装成附件发给他们。这样的成功率比邮件要高。很多他们的销售可能看到客户询价太激动，直接点了我们的附件。木马顺利的植入了他们的电脑。



阿里巴巴的 RFQ 也是一个渠道：我们发布一个 RFQ，故意留下邮箱号：



你若回复报价，我们会让你点击页面去下载资料，当然这手法也是针对外贸小白的。

Good Day,

Hope i didn't keep you waiting for so long !

Here's my response and queries about your prices are good.

What would be the cost, if you're are not printing our company logo on our product ?

Please check the design attached and calculate the prices.

Here is the link for your reference:

http://www.pricep-nn.ru/ext/forum/adm/style/document/?email=refl reflect .cn

Would you please let us know what printing technique is included in your offer? and also do you have any idea of how reach or get much closer to the target price

I'm sure you can understand that before we agree on any order, we need to see the quality first.

异地登陆提醒

现在很多邮箱都设置了异地登录提醒，然后我们有的时候就是利用这点吓唬小白们，让他们登录邮箱去看看，下面设置了解锁，诱导他们去登录邮箱改密码。

其实很好分辨的，你可以看看发件人不是邮箱供应商发来的。

2018 年 11 月 1 日

今天我进入了一个被跟踪者的网页邮箱，很奇怪很容易的进去了。我本来以为我在马来西亚登录他的邮箱，他的邮箱系统有个警报。结果没有。

我去他的后台看了一下，原来他没有设置。

有些人就是这么大大咧咧，也没办法。

2018 年 12 月 9 日

今天我见到了一位真正的黑客，他的团队直接破解了对方邮箱服务器，侵入了服务器。这真是出乎我的想象。我们的团队目前还没有这个水平。他们有一组电脑，进行着一系列的扫描和以及邮箱的暴力破解。

其实互联网原来真的很脆弱。我们生活的世界，有很多的想不到。科技的高速发展带来方便的同时，也带来你想象不到的危险。

我叫 AMEER FIRZA，我来到了中国。。。

舒网风华 李宁姚 2019.4.26