2016 中国企业邮箱安全性研究报告

2016 年 12 月 8 日

摘　　要

- 根据艾瑞相关报告分析及预测：到 2016 年底，中国企业邮箱用户规模将达到 1.12 亿，并且仍将持续高速增长，至 2017 年底，将有望达到 1.35 亿。在企业办公应用中，电子邮件仍然发挥着不可替代的作用。
- 服务器端口对外开放，发送邮件不受限制，安全管理水平低下，易于发动精准攻击等因素，是企业邮箱容易遭到黑客攻击的主要原因。
- 垃圾邮件、邮箱盗号、钓鱼邮件和带毒邮件是企业邮箱遭到网络攻击最主要的四种形式。
- 全国企业用户的邮箱系统平均每天接到的各类垃圾邮件的数量高达 2000 余万封，预计全年总量约为 73 亿封。这些垃圾邮件约占到企业用户收到邮件总量的 69.8%。
- 国内企业邮箱用户平均每天遭遇疑似盗号攻击事件约 1.0 万件，全年预计总量约为 365 万件。邮箱被盗后，会产生诸如密码被篡改，对外发送垃圾邮件，对内发送欺诈邮件等多种异常现象。
- 用户使用弱密码，仍然是邮箱被盗号的首要原因。统计显示，企业邮箱帐号使用弱密码的比例高达 16.0%，且占总量 9.8%的邮箱账户使用的是 10 个最流行的企业邮箱密码。据此估算，攻击者仅需尝试 10 次，全国就有约 1097.6 万个企业邮箱可能被成功破解。
- 对于企业用户来说，OA 钓鱼邮件是最具危险性的钓鱼邮件。攻击者冒充系统管理员发送邮件，以邮箱升级、邮箱停用等理由诱骗企业用户登录钓鱼网站，并进而骗取企业员工的帐号、密码、姓名、职务等信息。
- Coremail 论客与 360 的联合监控平台每天仍能截获 6000 封左右的带毒邮件，最高峰时期可达单日数万封。在所有带毒邮件的木马附件中，PE 文件（可执行文件）占 3.8%，非 PE 文件占比为 96.2%。在邮件携带的 PE 文件木马中，远控木马最多，占到了 61.8%，其次是下载者，占 14.5%；而在带毒邮件携带的非 PE 文件木马中，下载者占到了 99.1%。

关键词：企业邮箱、邮箱盗号、钓鱼邮件、OA 钓鱼、带毒邮件

目　　录

第一章　综述

一、　企业邮箱安全性的重要地位

在中国当前的互联网环境下，伴随着社交网络的日益发达，电子邮箱对于普通个人用户的重要性已经大大下降。但是，对于企业用户来说，电子邮箱仍然是网络办公最主要的“办公用品”。

根据艾瑞相关报告分析及预测：2014 年，中国企业邮箱用户规模仅为 6000 万左右，但到 2016 年底，中国企业邮箱用户规模将达到 1.12 亿，并且仍将持续高速增长，至 2017 年底，将有望达到 1.35 亿。可见，在企业办公应用中，电子邮件仍然发挥着不可替代的作用，并且其重要性正在逐年提高。

来源：艾瑞咨询根据企业财报、公开数据及行业访谈估算。

对于一些 IT 化程度较高的企业来说，企业用户的电子邮箱往往承担着以下重要的办公功能：

1） 企业内网权限管理中的身份标识。

2） 企业内部重要办公信息的沟通渠道，并且具有一定的保密性质。

3） 企业与外部沟通的正式平台，交互信息具有一定的法律效力。

所以，一旦企业用户的邮箱遭到攻击，发生邮件的内容被窃取、帐号被仿冒，电脑因此感染病毒等情况，遭受威胁的将不仅仅是企业的某个员工个体或个别终端设备，而也有可能危及企业的整个内网系统，以及企业的各种外部商务合作。

二、　攻击者为什么喜欢攻击企业邮箱

尽管企业邮箱在企业的网络系统中承担着如此重要的职责，然而不幸的是，企业邮箱通常也是黑客对企业发动网络攻击的首先攻击途径，这主要是由于以下几方面的原因：

1） 邮件服务器端口是企业内网唯一对外公开暴露的网络端口

企业内网防护的基本方法之一是隐藏或屏蔽内部服务的各种网络端头。但是，为了保证

互联互通，邮箱服务器的收发端口必须公开，企业即便使用私有的邮箱服务系统，也必须如此，否则就无法与外部网络之间进行正常的邮件往来。

2） 企业级邮箱发送垃圾邮件一般没有数量限制

普通的个人邮箱服务通常都是由专业的邮件服务公司来免费提供的。出于成本和安全的考虑，个人邮箱通常都会对用户群发邮件的数量进行严格的限制，而且一旦某个个人邮箱被发现用来发送垃圾邮件，邮箱帐号及发送人 IP 通常都会被立即封锁。

但是，企业邮箱，特别是完全私有的企业邮箱系统，其服务规则都是由企业自己定制的，而绝大多数企业都不会对邮箱发送邮件的数量进行限制。所以，一个普通企业用户邮箱被黑客盗用后，一次性发送几千封，甚至上万封垃圾邮件的事情屡见不鲜。

事实上，通过对大量被盗号的企业邮箱监控发现，发送垃圾邮件是黑客盗取企业邮箱帐号的首要原因。

3） 企业对邮箱的安全管理水平一般远远不及专业邮件服务商

邮箱系统供应商通常都会为邮箱系统配置大量的安全管理功能，正确使用这些功能，通常可以有效防范 95%以上邮件攻击。但从实际使用情况来看，即便是最为必要的安全规则，如弱密码检测、SSL 传输加密等，也有 50%以上的企业会选择不开启。这也就导致了企业邮箱系统，特别是完全私有的邮箱服务系统，其安全管理水平事实上远远低于一般的商业邮箱，所以更容易入侵。这也就形成了一个非常客观的矛盾：一方面，企业为了防止信息泄漏，会选择搭建完全私有的邮箱服务系统；但另一方面，由于其安全管理能力不足，导致其邮箱系统更容易被入侵和泄密。

4） 电子邮箱更容易被用于发动精准攻击

普通的网络黑客喜欢发起群体式攻击。但对于高级攻击者来说，对于特定目标发动精准攻击，尽可能避免自己的暴露，则是更加优选的攻击策略。但通常来说，要从外部网络对内网系统中的特定终端或个人进行精准定位是非常困难的，但如果知道了攻击目标的电子邮箱，给其发送一封带毒邮件或钓鱼邮件，则往往是轻而易举的事情。这也就是为什么在 APT 攻击中，鱼叉邮件是首选攻击手法的主要原因。

三、 企业邮箱攻击的主要方法

综合网络大数据分析与客服反馈情况来看，针对企业用户的邮箱攻击主要有以下四种常见手段：

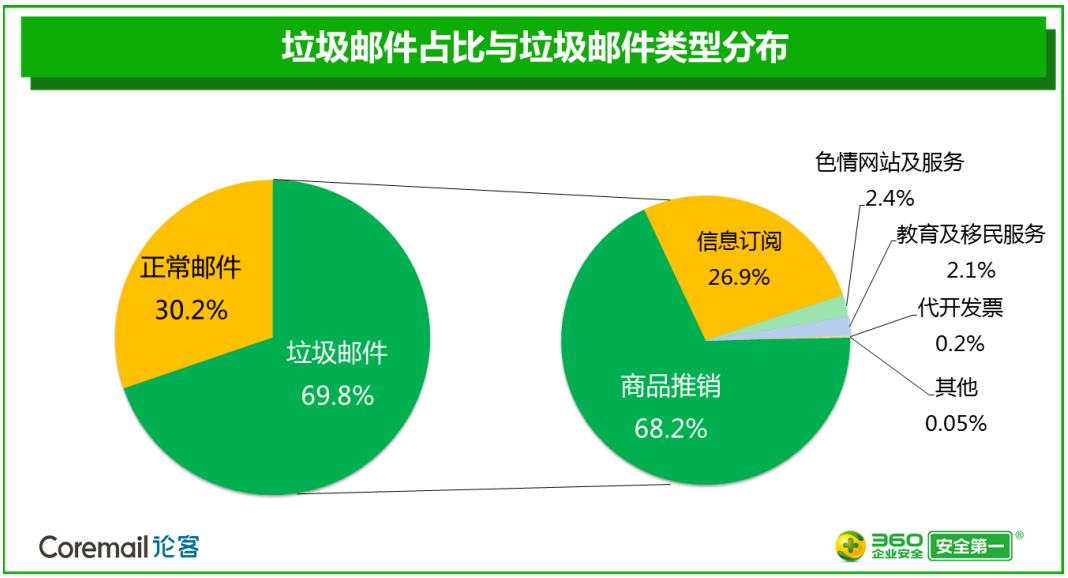
（一） 垃圾邮件

垃圾邮件是最为普遍存在的一种邮箱攻击现象。这里所说的垃圾邮件，特指以宣传推广为目的垃圾邮件，不包括带有显著攻击性质的恶意邮件，如钓鱼邮件或带毒邮件。

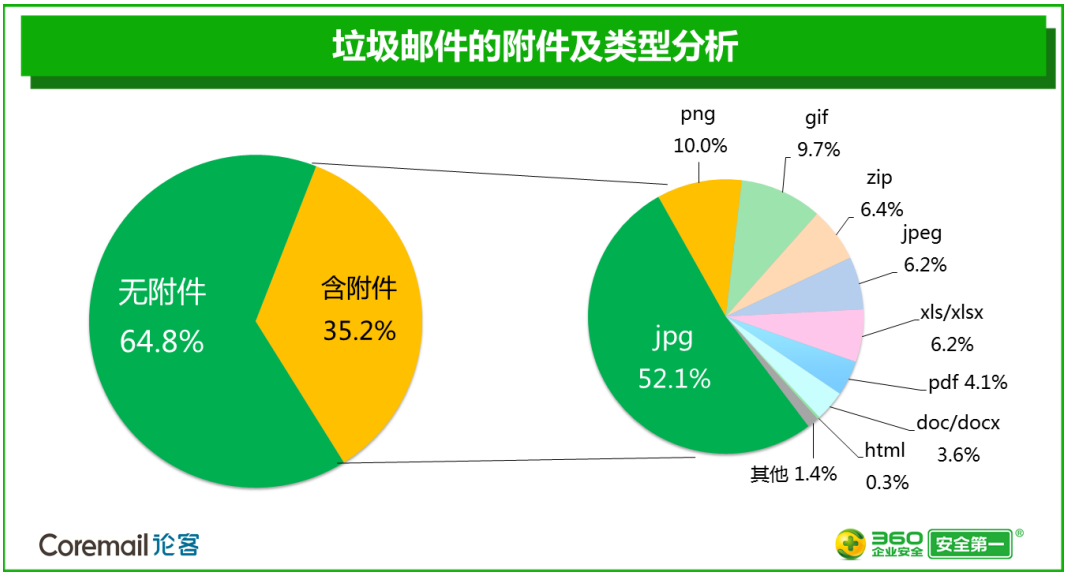
监测分析显示，2016 年以来，全国企业用户的邮箱系统平均每天接到的各类垃圾邮件的数量高达 2000 余万封，预计全年总量约为 73 亿封。这些垃圾邮件约占到企业用户收到邮件总量的 69.8%。也就是说，如果没有反垃圾邮件过滤系统的话，那么企业用户平均每收到三封邮件，就至少有两封为垃圾邮件。

从类型上来看，商品推销类垃圾邮件最多，占垃圾邮件的 68.2%；其次是信息订阅类，

占比 26.9%；第三是色情网站及服务，占 2.4%。



从附件角度看，约有 35.2%的垃圾邮件会携带附件，其中，图片附件最为常见，约占携带附件邮件总量的 80%，包括机票 jpg 占 52.1%，png 占 10.0%，gif 占 9.7%，jpeg 占 6.2%。



考虑到垃圾邮件的主要危害是给用户和邮件系统增加负担，而造成实质性损失的风险相对较小，所以在本报告的后续研究中将不做重点讨论。

（二） 邮箱盗号

邮箱盗号攻击，是指攻击者通过拖库、撞库、暴力破解、木马盗号、钓鱼盗号等手段盗取用户电子邮箱的账户和密码，随后再利用盗取的邮箱账户进行其他恶意攻击。

用户邮箱账户被盗后，通常有以下几种可能的结果：

1） 被盗邮箱被用于大量发送垃圾邮件，最终导致被盗邮箱被其他邮件系统列入黑名单，无法正常发信。

2） 被盗邮箱被用于向企业内部发送欺诈邮件，以盗取更多的邮箱账户，或对特定目标

人进行鱼叉攻击。

3） 被盗邮箱被用于向企业客户或合作方发送欺诈邮件，进行商业欺诈。

4） 被盗邮箱被用于企业内网攻击，黑客利用被盗邮箱所持有的企业内网访问权限，对企业内网实施攻击。

（三） 钓鱼邮件

钓鱼邮件攻击是指攻击者仿冒特定身份的人或组织，对企业用户或企业用户的邮件联络对象进行欺诈；而攻击者所使用的邮箱发件人的显示名、前缀和后缀都有可能经过精心伪装，进而迷惑被攻击者。

钓鱼邮件经常伪装的发件人身份有以下几个主要类型：

1) 冒充系统管理员，以系统升级、身份验证等为由，通过钓鱼网站等方式骗取企业员工的内网帐号密码或邮箱帐号密码。

2) 冒充特定组织，如协会、机构、会议组织者或政府主管部门等身份发送邮件，骗取帐号密码或钱财。

3) 冒充客户或冒充自己，即攻击者会冒充企业客户或合作方对企业实施诈骗，或者是攻击者冒充某企业员工对该企业的客户或合作方实施诈骗。当然也有可能 是冒充某个企业的管理者对企业员工实施诈骗。

需要说明的是，同样是身份冒充，其针对性也有所不同。如冒充管理员和冒充特定组织这类邮件诈骗，往往会群发给企业中的很多员工。而冒充客户或冒充自己，实施专门的商业欺诈的邮件，则往往只会定向发送给特定人群，如公司财物人员，公司高管等。

（四） 带毒邮件

带毒邮件是一种比较传统，但十分有效的攻击方式。攻击者主要是通过在邮件中夹带带有病毒的邮件附件，并诱骗攻击目标打开附件的方式实施攻击。从攻击目的来看，在针对企业用户的攻击中，邮件携带的病毒通常可以分为如下三类：

1) 远控木马，完全控制被攻击的电脑。

2) 盗号木马，主要用于盗取用户的各种帐号和密码。

3) 下载者：木马本身并不具备明显的破坏性，但却会把更多的木马下载到用户电脑中。

此外，2016 年以来，敲诈者木马也比较流行，这类主要通过对用户电脑上的办公文件、图片、视频等文件进行高强度加密的方式，向被攻击者进行敲诈勒索。

需要说明是，邮箱盗号、钓鱼邮件和带毒邮件这三类邮箱攻击手段并不是特别严格区分的，它们中间可能存在很多交叉或关联。比如，有的邮件攻击可能即仿冒了身份，又携带了病毒，而邮箱被盗号也完全可能是由于被钓鱼或电脑中毒所导致的。

本报告后面章节，将主要针对邮箱盗号、钓鱼邮件和带毒邮件这三类邮箱攻击方式进行详细分析和案例分析。此外，由于针对普通人的欺诈邮件也可能会危及到企业用户，所以后文也会对典型的民用欺诈邮件举例分析。

四、 邮箱攻击事件的四个层次

上一小节介绍了邮件攻击的主要方法。但攻击方法的选择，实际上与攻击的目的和层次有很大的关系。有些攻击是群体性的，而有些攻击则具有很强的针对性。对于不同层次的攻击，需要采取的防御手段也有所不同。本小节将对邮件攻击事件的层次进行一个粗略的分析描述。

一般来说，根据攻击的针对性不同，我们大致可以将针对邮箱的攻击事件分为如下表中的几个层次：垃圾邮件、个人攻击、商业欺诈和 APT 攻击。

事件层次	针对性	攻击量	主要攻击目的	主要攻击手段
垃圾邮件	弱	大	发送商业推广信息	群发邮件
个体攻击	弱	大	盗号发送垃圾邮件 骗取个人财物	仿冒邮箱、钓鱼邮件、盗号木马、 敲诈者木马、盗号、撞号
商业欺诈	强	中	骗取公司财物	仿冒邮箱、盗号、撞号
APT 攻击	强	小	情报窃取、系统破坏	邮件携带专用木马

表 邮件攻击的三个层次

垃圾邮件是针对性最弱，但攻击量最大的一类邮箱攻击。攻击者通常来说甚至完全不考虑收件人的个体差异，也不在乎收件人使用的是民用邮箱（由商业网站提供的，可以开放注册并免费使用的邮箱）还是企业邮箱。

个体攻击的针对性要比垃圾邮件强，但其危害往往只影响个别用户。此类攻击包括利用邮件进行钓鱼盗号、木马盗号、邮箱撞库攻击、网络诈骗、敲诈者木马等。但是，个体攻击有时也会产生群体性影响。例如，某个企业用户的邮箱被盗，并被用于大量发送垃圾邮件时，有可能导致整个企业的邮箱被其他邮箱系统识别为黑名单，最终导致整个企业的邮箱都无法对外发送。

商业欺诈是针对性极强的一种邮箱攻击方式。攻击者通过仿冒邮箱、盗号等方式对企业员工进行欺诈。但与一般的个体攻击不同，攻击者的目标是企业而不是员工个人，最终目的是欺骗企业的财物人员向攻击者的银行帐号进行汇款。相比于个体攻击，商业欺诈一旦成功，往往金额特别巨大。

高级持续性攻击，也就是 APT 攻击，则是针对性最强，也最不易被发现的一种邮件攻击。根据 360 威胁情报中心发布的《2015 中国高级持续性威胁（APT）研究报告》显示，在针对国内目标发动的 APT 攻击中，79.2%的攻击使用的是鱼叉攻击，也就是向特定目标发送攻击邮件，而这些邮件绝大多数都是携带了专用木马的带毒邮件。与前述几个层次的攻击不同，APT 攻击的目的通常不是经济利益，而是窃取情报或恶意破坏。而从攻击的结果和数量上看，窃取情报是 APT 攻击最主要的目的。

第二章　邮箱盗号

盗号攻击，是企业邮箱用户经常遭遇的一类网络攻击。根据 Coremail 论客与 360 的联合监控分析显示，2016 年 1-10 月，国内企业邮箱用户平均每天遭遇疑似盗号攻击事件约 1.0 万件，全年预计总量约为 365 万件。

邮箱发生的很多种异常现象都与盗号有关。而黑客盗取企业用户邮箱帐号的方法其实有很多种，如果不能正确的应对盗号攻击，企业就会面临员工邮箱频繁被盗，修改密码后再次被盗的情况。

一、　邮箱被盗号的主要现象

企业邮箱被盗号之后的外在表象有很多种。下面逐一进行介绍。

（一） 密码被篡改

密码被篡改，是最为明显的邮箱帐号被盗现象。不过，通常情况下，对于经常被使用的企业邮箱账户，攻击者一旦篡改密码，就会很快被原使用者发现，并且邮箱的原使用者一旦成功重置了密码，那么攻击者一般也就无法继续使用这个邮箱了。所以，绝大多数的邮箱攻击者通常不会轻易修改企业邮箱原有的密码。

不过也有一些例外的情况。因为，如果企业用户将邮箱与某些支付账户、游戏账户或苹果设备等相绑定，那么攻击者一旦盗号成功，很有可能就会修改邮箱密码，目的是窃取与邮箱绑定的实际财富或虚拟财富。

下面两张图就是我们接到的企业邮箱用户举报的，由于密码被篡改导致的邮箱无法正常登录的截图。左图是来自山东某高校的用户举报，右图是来自某电信运营商用户的举报。

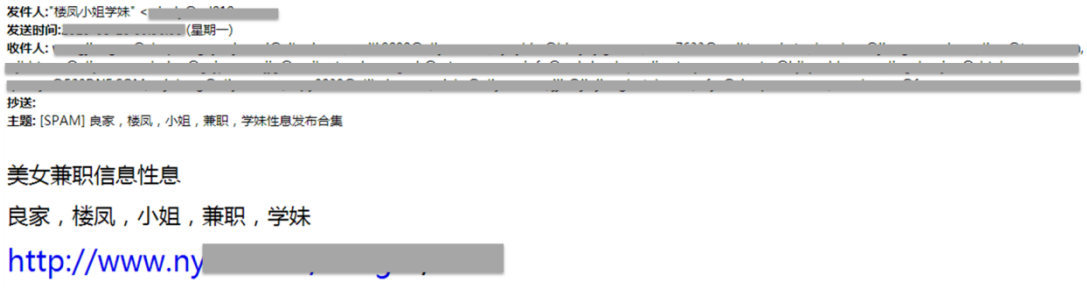
（二） 发送垃圾邮件及引发次生灾害

当邮箱在用户不知情的情况下突然发出大量垃圾邮件，那么一定是该邮箱帐号被盗了。下图是某企业用户邮箱被盗后，大量对外发送代开发票垃圾邮件的用户界面截图。

Time	subject	content
November 21st 2016, 15:19:23.000	开★发 QQ:1449814623	您 好！需要全国各地（普通国税、地税）（增值7%点开）(普通1%-2%点开)的发&票请电:★&~税 ¥~★"票"¥★"代"★开★刘小姐136 7015 9601 QQ:1449814623
November 21st 2016, 15:18:44.000	开★发 QQ:1449814623	您 好！需要全国各地（普通国税、地税）（增值7%点开）(普通1%-2%点开)的发&票请电:★&~税 ¥~★"票"¥★"代"★开★刘小姐136 7015 9601 QQ:1449814623
November 21st 2016, 15:18:38.000	开★发 QQ:1449814623	您 好！需要全国各地（普通国税、地税）（增值7%点开）(普通1%-2%点开)的发&票请电:★&~税 ¥~★"票"¥★"代"★开★刘小姐136 7015 9601 QQ:1449814623
November 21st 2016, 15:16:11.000	开★发 QQ:1449814623	您 好！需要全国各地（普通国税、地税）（增值7%点开）(普通1%-2%点开)的发&票请电:★&~税 ¥~★"票"¥★"代"★开★刘小姐136 7015 9601 QQ:1449814623
November 21st 2016, 15:14:33.000	开★发 QQ:1449814623	您 好！需要全国各地（普通国税、地税）（增值7%点开）(普通1%-2%点开)的发&票请电:★&~税 ¥~★"票"¥★"代"★开★刘小姐136 7015 9601 QQ:1449814623
November 21st 2016, 15:14:23.000	开★发 QQ:1449814623	您 好！需要全国各地（普通国税、地税）（增值7%点开）(普通1%-2%点开)的发&票请电:★&~税 ¥~★"票"¥★"代"★开★刘小姐136 7015 9601 QQ:1449814623
November 21st 2016, 15:13:50.000	开★发 QQ:1449814623	您 好！需要全国各地（普通国税、地税）（增值7%点开）(普通1%-2%点开)的发&票请电:★&~税 ¥~★"票"¥★"代"★开★刘小姐136 7015 9601 QQ:1449814623
November 21st 2016, 15:13:29.000	开★发 QQ:1449814623	您 好！需要全国各地（普通国税、地税）（增值7%点开）(普通1%-2%点开)的发&票请电:★&~税 ¥~★"票"¥★"代"★开★刘小姐136 7015 9601 QQ:1449814623
November 21st 2016, 15:11:56.000	开★发 QQ:1449814623	您 好！需要全国各地（普通国税、地税）（增值7%点开）(普通1%-2%点开)的发&票请电:★&~税 ¥~★"票"¥★"代"★开★刘小姐136 7015 9601 QQ:1449814623
November 21st 2016, 15:10:30.000	开★发 QQ:1449814623	您 好！需要全国各地（普通国税、地税）（增值7%点开）(普通1%-2%点开)的发&票请电:★&~税 ¥~★"票"¥★"代"★开★刘小姐136 7015 9601 QQ:1449814623

下面两图分别是某企业用户邮箱被盗后，大量对外发送色情服务垃圾邮件的用户界面截图。

Time	subject
November 18th 2016, 19:26:37.000	和刚认识几天的情人去开房间
November 18th 2016, 19:25:28.000	粉色小短裙的同事，讓我去她家玩
November 18th 2016, 19:25:08.000	粉色小短裙的同事，讓我去她家玩
November 18th 2016, 19:25:08.000	和刚认识几天的情人去开房间
November 18th 2016, 19:24:10.000	好身材美女爱自拍
November 18th 2016, 19:24:08.000	好身材美女爱自拍
November 18th 2016, 19:17:53.000	妹子口活很棒
November 18th 2016, 19:16:23.000	妹子口活很棒

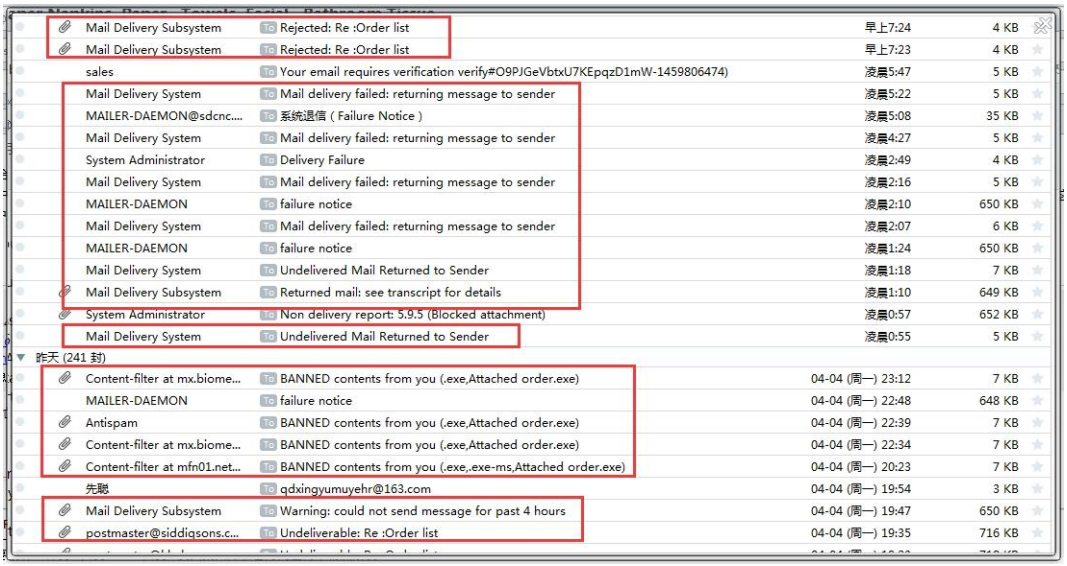


下图是我们近期截获的某公司用户邮箱被盗后，向外发出的推广赌博信息的垃圾邮件。

企业邮箱被盗用发送垃圾邮件，不仅会危及其他邮箱的用户，同时，由垃圾邮件引发的“次生灾害”也会直接危及该企业自身的邮件服务。当用户遇到这些次生灾害时，一般也就意味着其邮箱账户被盗了。

1） 邮箱无故收到大量退信

垃圾邮件一旦被其他邮件系统拦截或拒绝，该用户的邮箱就会突然收到大量的退信。下面两图分别是某个企业用户邮箱由于被盗后发送大量垃圾邮件而导致突然收到的大量退信的截图。



2） 被盗邮箱，乃至整个企业的所有邮箱都无法对外发送邮件

一旦其他邮箱系统发现了某个邮件服务器在大规模的发送垃圾邮件，就会拉黑该邮件服务器的 IP，使得由该服务器发出的该企业的所有邮件都被其他邮件系统拒绝，结果就是该公司所有员工都无法对外发送邮件。

下面给出两个由于发送垃圾邮件，邮箱帐号被系统查封的相关提示信息截图。

3） 即便修改密码，邮箱仍然大量对外发送垃圾邮件

造成这种情况的原因有很多种。其中最常见的三种原因是：一、邮箱设置被改动；二、邮箱设置了其他登录认证方式；三、用户电脑感染了病毒。

首先来看邮箱设置被改动的问题。

最为简单的一种连续盗号方式就是攻击者给邮箱设置一些密码找回问题，这样即便用户修改了密码，攻击者仍然可以轻易的找回这些密码，之后继续用该邮箱发送垃圾邮件。

还有一种通过修改邮箱设置用于发送垃圾邮件的方法更为高明，使得攻击者即便不登录受害者邮箱，也能持续对外发送垃圾邮件。如果受害者不明其中机巧，那么无论怎么修改密码或密码找回问题，都无法阻止垃圾邮件的发出。这种巧妙的修改方法就是：给邮箱设置批量的自动转发，并且将某个攻击者指定的邮箱设置为信任邮箱，无条件转发该邮箱发来的所有内容。如此一来，攻击者只要向受害者的邮箱发信，该邮箱就会自动的把攻击者发来的垃圾邮件群发给预先设定好的所有转发对象，而攻击者则无需长期掌握受害者的邮箱密码。下图就是一个邮箱系统的自动转发设置界面截图。

再来看邮箱设置其他登录认证方式的问题。

如果我们假定用户只能在邮箱登录系统中输入帐号和密码进行登录，那么修改了账户密码后，在确保不会再次被盗号的情况下，理论上说攻击者就无法再次登录了。但问题在于，很多企业为了方便办公，会为邮箱设置其他的登录认证方式。

例如：在某些企业的网络系统中，员工使用内部账号或域帐号登录办公网后，系统就会

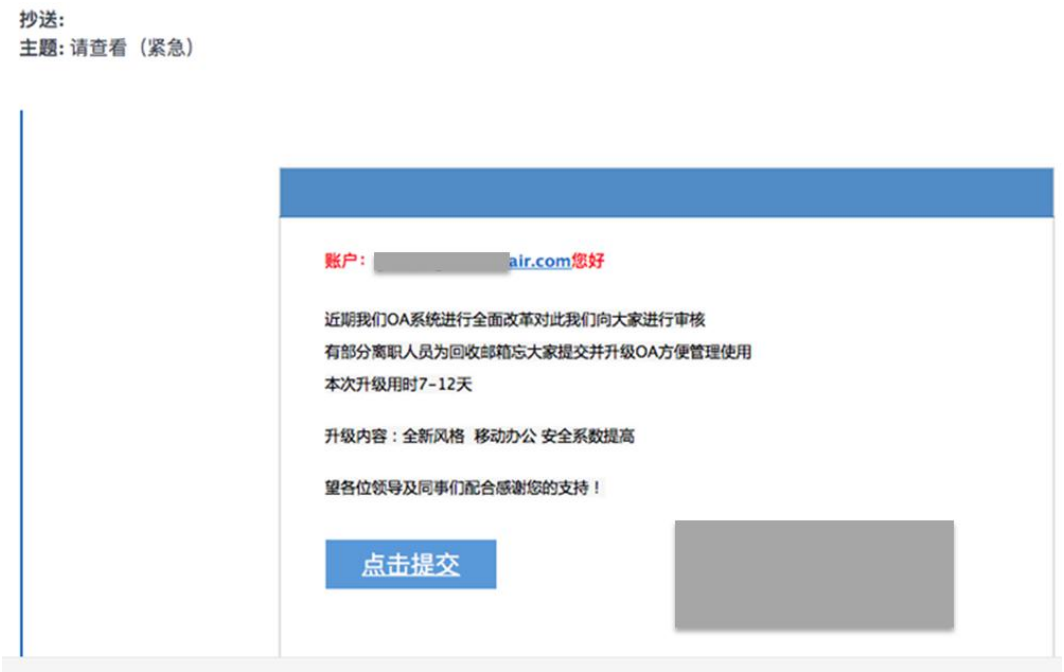
默认该员工邮箱也同时登录成功，而不再进行邮箱密码的验证。如果员工登录办公网的密码没有被强制与邮箱密码同步修改，那么么攻击者就有可能凭借对内部账号或域帐号的登录控制，绕过修改后的邮箱密码，直接操作邮箱系统。

通过我们对企业邮箱安全事件的监测显示，类似问题在企业用户中实际上经常发生。

（三） 内外邮件欺诈

对于攻击者来说，盗取企业邮箱的另外一个重要作用，就是用来对该企业的更多邮箱用户实施欺诈，以盗取该企业更多用户的邮箱。特别值得注意的是：对于安全意识较强的用户来说，比对邮箱后缀是最重要的防骗手段之一；但如果攻击者是使用企业内部邮箱欺诈内部员工，可信度和成功率都会大幅提高。

下图是我们 2016 年 7 月截获的某航空公司员工邮箱被盗后，向整个公司发出的一份冒充管理员身份 OA 钓鱼邮件。



事实上，即便是用一个企业的邮箱对另外一个企业的邮箱发送这种诈骗邮件，同样具有一定的迷惑性，如果后缀是 edu、org 或 gov 等时，收件人对邮件的信任度也会明显提高。下图是我们 2016 年 9 月截获的某组织机构邮箱被盗后，向某教育机构发送钓鱼邮件截图。

还有个别胆大妄为的攻击者，会直接使用内部邮箱，冒充管理员，给企业内部的各个下

设管理机构或邮件组发送此类钓鱼欺诈邮件。一旦企业中某个下设的管理机构中招，将直接威胁内网系统中最敏感的信息资料安全。

下图是我们于 2016 年 7 月截获的，某个互联网公司被盗邮箱后向该企业各管理机构邮箱发送的 OA 钓鱼邮件，收件人中不乏 IT 管理、人力资源、财务管理等高度敏感部门的邮箱。

当然，在某些特殊情况下，被盗的企业邮箱还会被用于更加高级的商业欺诈，如诱骗财务人员汇款，给合作伙伴或客户发送虚假信息等。但这类事件已经接近 APT 攻击，攻击过程也非常的复杂，本次报告就不进行详细分析了。

（四） 第三方帐号被盗

由于某些网络服务，如游戏、支付、iCloud 等，会与电子邮箱进行绑定，而很多犯罪分子在盗取了被绑定的邮箱后，就会利用相关网络服务提供的基于邮箱的密码找回、密码重置等功能盗取其他网络服务的帐号和密码，进而盗取用户的游戏装备，网银资产、网上资料（如照片，视频等）。这种攻击在个人邮箱领域经常发生。但如果企业用户使用公司邮箱注册了这些第三方服务，也会面临相同的攻击。

2016 年下半年，频繁被媒体曝光的苹果设备锁屏攻击，实际上就是一种非常典型的邮箱盗号攻击。其攻击原理是：苹果设备的帐号，特别是 iCloud 功能通常是与电子邮箱绑定的；同时，苹果安全中心还为用户提供了一种锁屏防盗功能，即用户的 iPhone 手机或 iPad 如果被偷走后，用户可以登录安全中心将设备锁死，使盗窃者设备无法正常使用；而苹果锁屏敲诈，则是犯罪分子反向利用了此项防盗功能，在首先盗取用户邮箱账户后，利用 iCloud 的邮箱密码找回功能，登录苹果安全中心，之后再把用户的所有与该 iCloud 帐号绑定的苹果设备锁死，并在通知信息中留下自己的电话或 QQ，要求用户支付赎金后为其解锁。

下面两张图是我们在网上找到的一些用户苹果手机遭遇此类锁屏敲诈后开机界面。

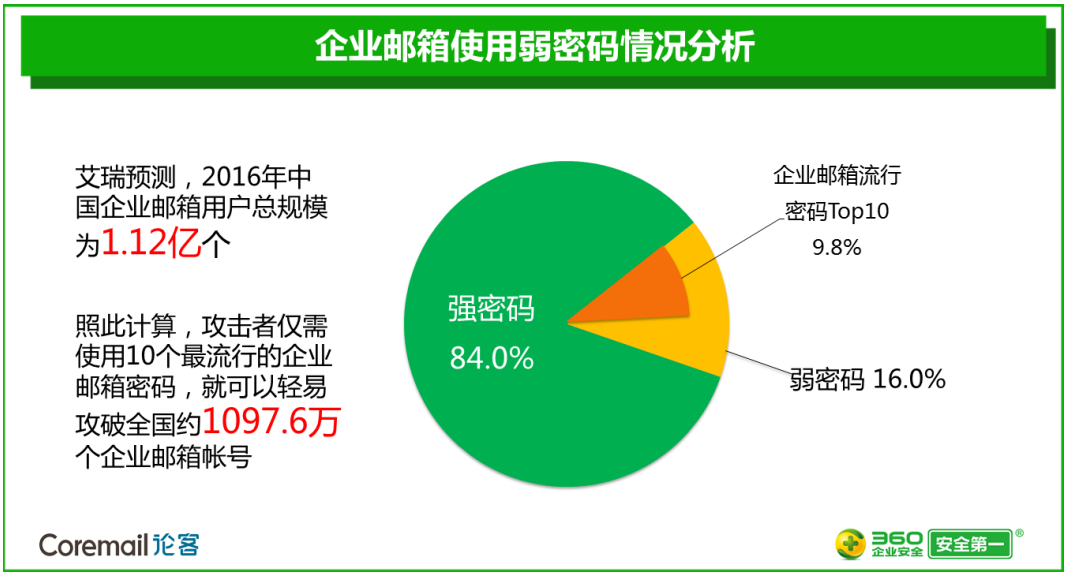
二、 邮箱盗号原因分析

电子邮箱被盗号的方式方法有很多，有一些方式还会比较巧妙和复杂。不过，从大的方面来看，最主要的原因有以下四种：一是因为使用弱密码而被暴力破解；二是收到带毒邮件后感染木马；三是收到钓鱼邮件被钓鱼盗号；四是邮箱服务器遭遇拖库或撞库攻击。

关于带毒邮件和钓鱼邮件的问题，将在接下来的两章中详细讨论，这里就不详细分析了。而至于拖库和撞库攻击，目前还缺乏比较全面的企业邮箱相关统计，这里也不做展开分析。下面仅就弱密码问题也就是暴力破解问题进行讨论。

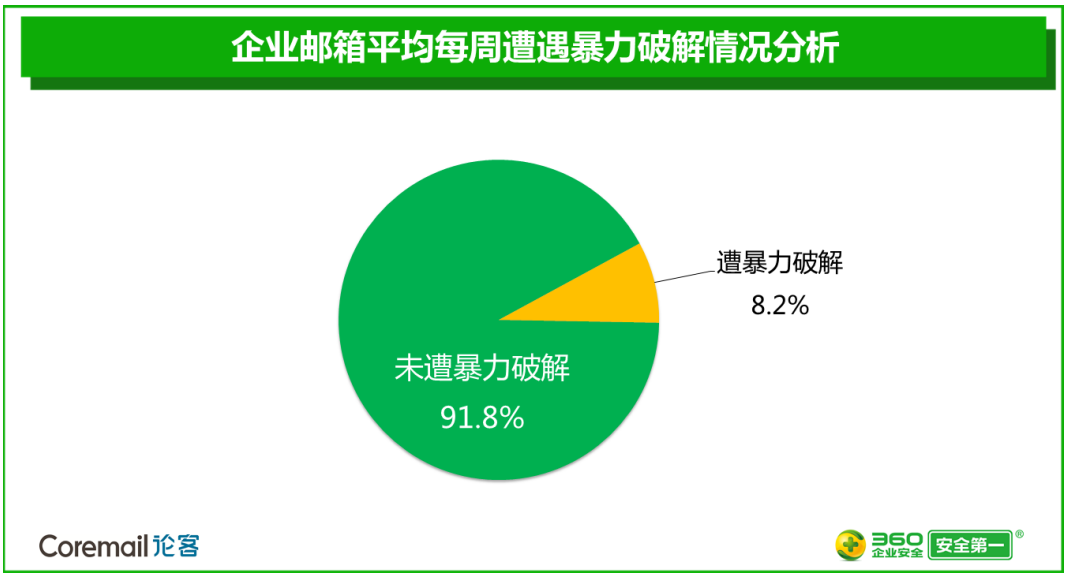
从安全性的角度来看，企业邮箱必须具备弱密码检测及弱密码被强制改密功能。但我们的监测发现，即便是在哪些采购了由专业邮箱服务商提供的企业邮箱系统的企业中，也有相当数量的企业没有开启系统自带的弱密码检测及弱密码强制改密功能。而在那些完全使用开源系统自建邮箱服务的企业中，这种危险情况更加普遍。

为了能够确切的掌握企业邮箱使用弱密码的情况，我们在得到了相关企业授权的情况下，对部分企业的用户邮箱进行了弱密码抽样检测，结果发现：使用长度不足或密码结构过于简单的弱密码的企业邮箱帐号，占到了所有被测试的企业邮箱帐号的 16.0%。而更为可怕的是，约占所有被测试的企业邮箱帐号总量 9.8%的邮箱账户，使用的是企业邮件系统最常见的 10 个流行密码。也就是说，如果攻击者已经通过钓鱼、木马等盗号手段获取了大量企业用户的邮箱账号和密码，并据此准确的推算出了 10 个最流行的企业邮箱密码，那么，在约 1.12 亿总规模的企业邮箱用户中，就可能有约 1097.6 万个企业邮箱帐号属于暴力破解的高危帐号——攻击者最多仅需尝试 10 次，就有可能攻破这些邮箱。

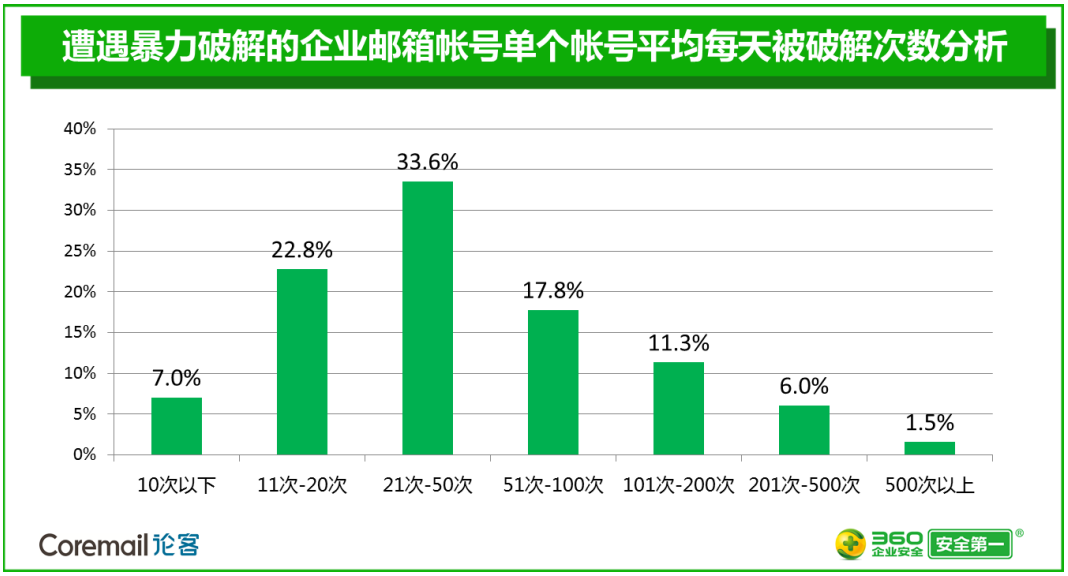


事实上，针对用户使用弱密码的情况，攻击者们每天都在对大量用户进行着不断的暴力尝试。抽样统计显示，每个星期至少有 8.2%的企业邮箱帐号会遭遇暴力破解猜测（这些邮箱帐号在一周内至少被使用不同密码尝试登录 50 次以上），平均每个账户每天被使用不同密码尝试登陆 85 次以上，甚至有个别完全不设任何防暴力破解措施防护的企业邮箱每天会遭到 3000 次以上的暴力破解猜测。

下图给出了企业邮箱帐号遭遇暴力破解的比例情况。



下图给出了企业邮箱在遭遇暴力破解的情况下，每个邮箱平均每天被破解的次数。需要说明的是，邮箱每天被破解的次数，除了与邮箱密码的本身强度相关外，也与企业邮箱具体的防暴力破解安全策略有关。所以，邮箱被破解的次数不能完全说明邮箱密码的强度，它仅体现黑客相关攻击活动的活跃程度。

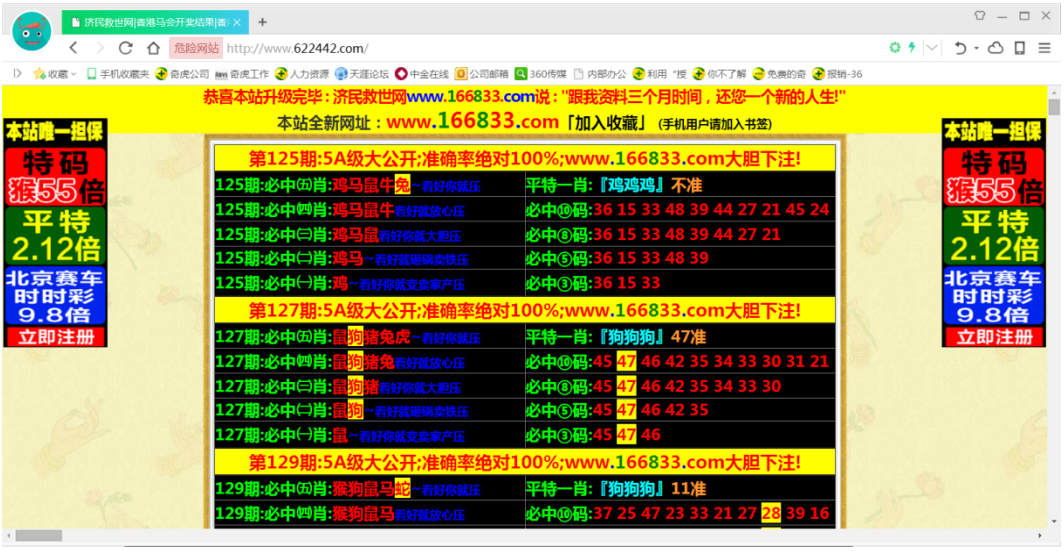


三、 邮箱盗号典型案例

本小节以一次大规模邮箱盗号攻击事件为例，说明邮箱盗号事件的手法及危害。

2016 年下半年，Coremail 论客服务系统接到某大型企业客户举报，其邮箱服务系统中的 300 余个邮箱帐号在某日夜间出现异常 IP 登陆，并几乎同时对外发送垃圾邮件的情况。。邮件内容均为某境外赌博网站的推广信息。邮件内容示例如下。

经查，涉案赌博网站域名共有三个，相关赌博网站的页面截图如下：

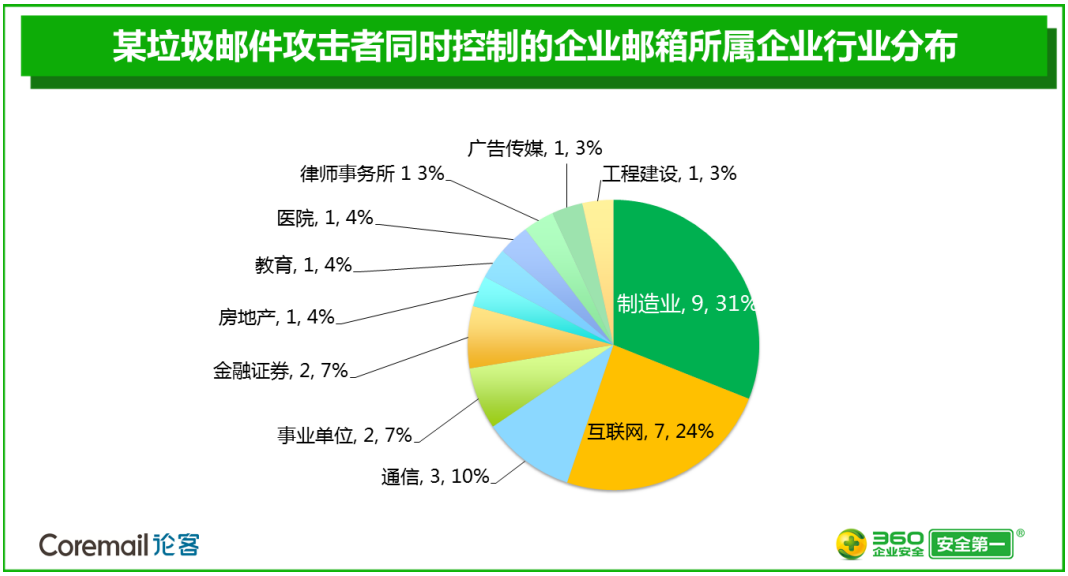


应该大型企业客户的协查要求，Coremail 论客与 360 追日团队成立了联合调查小组，对该事件的起因、背景及相关影响展开调查。

调查显示，这 300 余个被盗号并被用来集中发送垃圾邮件的电子邮箱，其盗号过程并不在此次事件案发前后发生的，事件的起因实际上一直可以追溯到 2015 年上半年。当时，该公司的很多用户都接到一封冒充 OA 系统管理员的钓鱼欺诈邮件，有相当数量的该企业员工被骗，并在钓鱼网站上填写了真实的邮箱帐号和密码，从而帐号被盗。自 2015 年上半年至今，除极少数邮箱曾经被攻击者偶尔使用过之外，一直没有发生其他类似的大规模垃圾邮件外发事件。

而引起调查小组关注的是，在 2015 年上半年发生的那次钓鱼邮件攻击事件中，相关邮件实际上又是由攻击者使用其他企业的邮箱帐号发送出来的。通过进一步对钓鱼盗号邮件及相关博彩信息邮件进行不断的追踪、溯源分析后发现：攻击者最早期的活动迹象出现在 2014 年 8 月，此后，攻击者通过钓鱼盗号，再钓鱼再盗号的循环攻击，至少先后盗取和使用了 29 家企业的数千个企业邮箱，而且还另外使用了一个攻击者自己独立注册的邮箱系统。而最早被攻陷的企业，是一家北京的通信服务公司，该公司邮箱是所有后续 OA 钓鱼攻击的总起点。不仅如此，该公司的官网也被攻击者篡改挂马，植入了大量赌博、博彩类的钓鱼信息。

下图给出了此次“OA 钓鱼+赌博推广”攻击事件中，攻击者同时控制的所有企业邮箱所属企业的行业分布情况。可以看出，被这个攻击者控制的企业邮箱，有 9 家属于制造业企业，7 家属于互联网公司，另有通信企业 3 家，事业单位和金融证券类企业各 2 家。



从这起案例中可以看出，垃圾邮件攻击者的攻击有以下特点：

1） 从钓鱼盗号攻击到发送垃圾邮件攻击之间，攻击者的潜伏和准备周期特别长。攻击者这样做的主要目的是为了增加事后追查难度，更好的隐藏自己。如果没有完整的历史数据存留，我们就很难复原整个攻击过程。

2） 攻击者会不断的以新盗取的企业邮箱为跳板，对更多的企业邮箱发起攻击。

3） 一个垃圾邮件攻击者的手中，往往会同时掌握成千上万个企业邮箱帐号资源。

这起案例也再次告诉我们在企业安全领域的一个基本事实：即便没有显著的或重大的安全事件发生时，也不等于企业的系统就是安全可靠，攻击者可能早已完成了入侵和控制。而一旦破坏性攻击事件真的发生了，再进行防护可能早就为时已晚。

四、 企业邮箱防盗号建议

客户服务监测显示，尽管如前所述，盗号攻击的技术方法有很多，但盗号并非不可避免。企业邮箱系统只要采用某些基本的技术防护措施和管理方法，实际上就可以非常有效的避免 95%以上的邮箱盗号事件发生。下面就对这些基本的技术方法和管理措施进行简要的介绍。

（一） 技术措施

利用技术手段对邮箱安全性进行监测是十分必要的，不能指望员工能很好的执行公司的各项安全规定。从反盗号的角度看，企业用户的邮箱系统除了应当具备一般反垃圾邮件功能外，至少还应具备以下基本安全功能，才有可能在最大程度上阻止盗号攻击：

1） 双因子认证

双因子认证仍然是目前比较容易部署，并且比较安全可靠的一种安全登录认证方法。在邮件系统中，其主要工作方式是在邮箱的帐号和密码之外，生成动态口令，并通过邮件登录系统以外的方式传送给登录者。双因子认证的方法，可以在很大程度上避免邮箱的帐号密码被盗后，攻击者直接入侵邮件系统或企业内网。但如果攻击者进一步使用钓鱼网站或木马程序窃取动态口令，则仍有可能突破双因子认证的防线。

除了动态口令之外，目前还有一些基于数字认证技术或生物识别技术等其他形式的双因子认证技术也正在逐渐的普及开来。

特别需要说明的一点是，对于动态口令，传统的技术实现方案大多需要使用一个单独的硬件电子令牌。虽然电子令牌的体积一般很小，但携带和使用仍然有一定的不便。而目前，已经有一些新型的技术方案可以将电子令牌制作成一个手机上的 APP，这样使用起来就相对比较方便。下图是 360 研发的一套可运行于普通智能手机上的动态口令 APP 界面截图。

2） 弱密码检测

如前所述，弱密码是企业邮箱被盗号的最主要原因。所以，企业邮箱系统应具备弱密码检测功能，并对员工邮箱进行强制检测，并通过技术规则强制员工邮箱密码满足如下要求：

初始密码只能用于首次登陆，之后必须强制修改密码；

密码长度大于 15 位；

密码包括数字、字母和特殊符号；

密码中不能包括姓名拼音或姓名拼音缩写，也不能包括生日的各种数字组合；

使用弱密码库和暴力破解方式对员工邮箱密码进行碰撞，限定时间内破解成功，则强制员工修改密码。

3） 周期性强制改密

密码定期强制更换，建议周期为 3 个月或 6 个月，更换后的新密码也要进行弱密码检测。

4） 垃圾邮件阻断

当有企业邮箱被用于发送垃圾邮件时，系统应具备检测发现和阻断发送的功能，并能向用户及管理员发送邮箱异常预警。这种对垃圾邮件的阻断，既是对攻击者的一种防范，同时也是对邮件系统的保护，以免邮件系统 IP 被其他邮件系统列入黑名单。

5） 异常登录监测

邮件系统应对每一个用户的日常使用行为进行特征分析，并对异常登录行为进行预警和阻拦，包括短时间内跨地域登录，频繁异地登录，短时连续密码错误等。

6） 反钓鱼引擎

邮件系统应具备反钓鱼引擎，能够对邮件中的钓鱼网址，特别是专门用于盗号的钓鱼网址具备较强的识别能力，并且系统应具有足够大的恶意网址库和足够快的恶意网址更新能力，从而能够更加有效的实时拦截钓鱼邮件。

7） 反病毒引擎

邮件系统应具备恶意程序扫描引擎，并且恶意样本库应足够大，且更新速度足够快，如此才能有效的识别邮件中携带的盗号木马程序。不仅如此，从前一章中还可以看出，反病毒引擎还可以在更多的层面保护邮件系统，及邮箱使用者的安全。

（二） 员工教育

当然，不是所有的问题都能够通过技术手段解决，特别是当邮件系统的监控能力被局限在内网环境中的时候，如果不进行有效的员工教育，难免出现各种不可预期的问题。特别是在盗号攻击方面，需要做好以下几方面的员工教育。

1） 企业邮箱密码必须单独设置，不能与任何其他第三方网站或应用使用相同的密码。

制定这样的规范主要是为了防止企业邮箱被撞库。因为当第三方网站被黑客攻破，用户的登录密码被泄漏时，黑客就有可能用已经窃取的密码来尝试登录企业用户的邮箱，从而实现对企业内部网络的入侵。

2） 不用企业邮箱注册第三方网站或应用。

很多网站或应用的注册环节都会使用电子邮箱，而一旦这些第三方网站或应用的后台系统被攻破，就可能造成企业用户邮箱地址的泄漏，这就为垃圾邮件和钓鱼邮件的攻击提供了标靶。事实上，使用企业邮箱注册第三方应用或服务，正是企业邮箱被大量曝光的主要原因。

如果用户在第三方网站或应用上使用的密码与企业邮箱密码相同，则攻击者便可一次性窃取到完整的企业邮箱地址和密码，危害极大。

（三） 综合管理

除了技术手段和员工教育外，邮箱帐号的安全性还与企业的内部管理关系密切。例如员工离职、工作调动、一人多账户等因素，都有可能造成邮件帐号管理与监控的疏漏。如果邮件系统长期存在当销号未销号，当变更未变更，闲置邮箱数量庞大的情况，那么该企业的邮件系统，甚至是企业的内部网络都将处于极其脆弱和极其危险的环境。

第三章　钓鱼邮件

钓鱼邮件是指含有虚假欺诈信息的电子邮件。不过，客观的说，几乎所有的带毒邮件也都是含有虚假欺诈信息，因此也应该都属于钓鱼邮件。为了便于区别分析，在本报告中，钓鱼邮件特指那些单纯使用欺诈手段，而没有使用任何木马病毒的电子邮件。而对于带有木马病毒的邮件及其相应的欺诈手法，将在下一章“带毒邮件”中 专门分析和论述。

在中国，由于电子邮件并非普通个人网民经常使用的网络沟通方式，所以，钓鱼邮件在中国并不十分发达。在欧美、拉丁美洲和非洲等地区比较流行的，利用邮件进行的信用卡诈骗、中奖诈骗等，在中国都非常少见。

不过，对于国内企业用户而言，以冒充系统管理员为代表的 OA 钓鱼邮件还是十分流行的。此外，也有一些国外非常经典的民间骗术，如“冒充富人求帮助”诈骗或“装成穷人扮可怜”诈骗会以英文（少数为中文）电子邮件的形式发给中国的企业邮箱用户。本章将主要以 OA 钓鱼和部分民间骗术为例，分析企业邮箱用户可能遭遇的钓鱼邮件风险。

当然，还有一些高级攻击者会使用电子邮箱进行商业欺诈，主要针对企业的财务人员或合作伙伴。但这种攻击比较少见，而且攻击过程也比较复杂，已经十分接近 APT 攻击。此类攻击不在本次报告的讨论之内。

一、 OA 钓鱼邮件

攻击者冒充系统管理员发送邮件，以邮箱升级、邮箱停用等理由诱骗企业用户登录钓鱼网站，并进而骗取企业员工的帐号、密码、姓名、职务等信息，这是企业用户最为经常遭受的一种钓鱼邮件攻击，我们一般称之为 OA 钓鱼邮件。

OA 钓鱼邮件的具体形式和欺诈理由也是多种多样，下面就给出一组攻击实例。

（一） 虚假邮箱升级

邮箱需要升级，这是冒充管理员的钓鱼邮件最为经常使用的欺诈手法。一旦用户点开邮件中所谓的升级链接，就会进入一个钓鱼网站页面，并被要求输入帐号、密码和其他个人信息。从形式上来看，虚假升级邮件最经常使用的升级借口包括：提升邮箱安全性、邮箱容量不足、员工离职或邮箱到期等。下面分别举例进行说明，案例中的所有截图均为我们截获的实际攻击邮件样本。

1） 提升邮箱安全性

安全邮箱升级Mail

尊敬的用户[ ]

由于你目前使用的安全连接协议版本存在漏洞，可能导致帐户的相关数据可被窃听，我们暂时阻止你登录邮箱使用功能，给您带来不便敬请谅解,本次需要您在72验证升级完成激活邮箱才能解除困扰，超时系统将对您的账号冻结!，

时间	地点	事件
2016-5-6 - 2:23:59	本地局域网	邮箱异常操作
2016-5-6 - 2:23:59	本地局域网	邮箱异常操作

（1）.请配合我们相关工作

（2）.点击这里解除 立即恢复正常

注：此邮件72小时内有效,请及时验证信息恢复正常使用，解除安全隐患!

Copyright ? 2005 - 2016 Tencent. All Rights Reserve

Mail Outlook WEB 邮件升级系统提醒

尊敬的用户:

您的帐号 由于你目前使用的OA版本存在漏洞,请尽快升级OA恢复正常使用！我们暂时阻止你登录Email使用功能！

邮箱帐号:

邮箱密码:

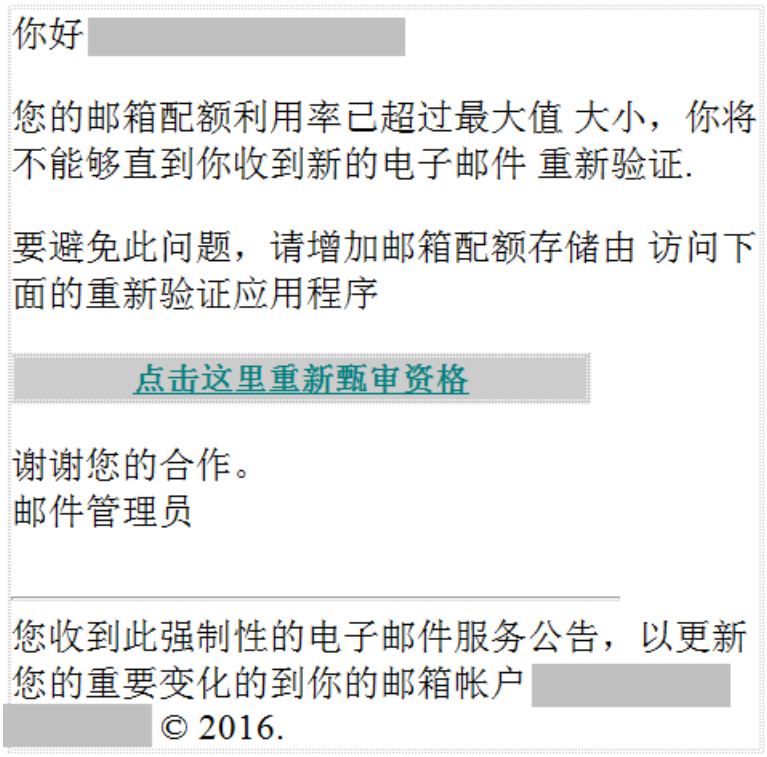
历史密码:

工　　号:

此邮件24小时内有效,请及时验证信息将邮件回复到:
qiyeyouxiangkefu@foxmail.com

°æÈ¨ËùÓÐ¡£ÇëÅä¶ÎÒÃÇÍà¹Ø¹¤×÷

2） 邮箱容量不足



你好 [redacted]

您的邮箱配额利用率已超过最大值 大小，你将不能够直到你收到新的电子邮件 重新验证.

要避免此问题，请增加邮箱配额存储由 访问下面的重新验证应用程序

点击这里重新甄审资格

谢谢您的合作。
邮件管理员

您收到此强制性的电子邮件服务公告，以更新您的重要变化的到你的邮箱帐户 [redacted] © 2016.

关于邮箱公告!	
一	根据相关用户和员工反映：邮箱容量不够日常使用，邮箱登录使用存在卡顿的现象！
二	为保证邮箱系统的稳定运行和正常使用，现在需要对部分邮箱进行升级！
三	请收到此邮件的员工请进行测试
	进行测试

您的邮箱配额已满
这可能会导致您的邮箱故 障或您可能无法再接收更 多的电子邮件

要继续使用您的邮箱，您 需要立即升级您的邮箱配 额。 这项服务是免费的。

升级邮箱配额这里

一旦升级完成，您的邮 箱将有效地工作。

邮件管理员 2016

[redacted],

您的邮箱配额已满
这可能会导致您的邮箱故障或您可能无法再接收更多的电子邮件

要继续使用您的邮箱，您需要立即升级您的邮箱配额。 这项服务是免费的。

升级邮箱配额这里

一旦升级完成，您的邮箱将有效地工作。

邮件管理员 2016

3） 员工离职或邮箱到期

各位同事	
用户	[redacted]
维护原因	由于离职人员较多，导致内部邮箱被他人使用，登陆存在卡顿发信速度比较慢，特此升级该邮箱！
维护时间	维护虚耗时1-6小时，为保证邮箱能正常使用，请立即升级
注意事项	请收到此邮件的人员立即升级以免总要数据丢失，**否则我公司，会按离职人员删除该邮箱账户**
操作指示	请点这里进行升级

尊敬的[redacted]，

访问到您的邮箱即将到期，

我们建议您升级您的帐户，以避免临时账户停牌。

使用以下链接更新您的电子邮件帐户。

升级邮箱这里

邮件管理员 © 1997-2016

4） 其他升级理由

尊敬的领导以及同事：您的管理员已经启动"邮箱搬家"，这将助于邮箱升级。

在收到通知的第一时间，将下列信息填写完毕回复本邮箱!
姓名：
职位：
邮箱：
邮箱密码：
历史密码：

从上面的例子可以看出，绝大多数虚假升级邮件都是会使用钓鱼网站来回收用户的个人信息，但也有个别钓鱼邮件会要求用户直接在邮件中回复姓名、职位、邮箱和邮箱密码等信息。对于缺乏基本的安全意识的企业员工来说，此类虚假升级钓鱼邮件的中招率还是很高的。

（二） 恐吓邮箱停用

邮箱即将停用，是除了邮箱升级之外，攻击者第二喜欢使用的理由。而且攻击者往往会将邮箱能够继续使用的期限设置的非常短，使收件人来不及细想便赶紧去申请续用邮箱。此类攻击的主要目的仍然是盗取企业员工的个人信息及邮箱帐号和密码。

[redacted]您好:

由于您长期未验证邮件系统账号信息,导致系统无法识别信息，或超过三个月未登录!（现需要重新采集用户信息)

为确保合理使用系统资源，若是收到此通知当天下班前没有回复或者校验用户信息,后台将自动识别此用户或是无人使用的邮箱，将被自动删除，感谢您的配合!

点击进行升级 <http://click.bes.baidu.com/adx.php?c=cz02YTQ3MWE3OGFjMTA2NTA0AHQ9MTQxMzc0MzM4NABzZT0xAGJ1PTY3Nz

请于2015.3.28 星期三 之前登陆内部网 <http://click.bes.baidu.com/adx.php?c=cz02YTQ3MWE3OGFjMTA2NTA0AHQ9MTQxMzc0

还有一种比较特殊的邮件停用理由，即邮件内容说用户邮箱由于某种原因，如发现危险行为，发送垃圾邮件等，已经被系统列入黑名单或禁止发邮件，之后再诱导用户在钓鱼页面上申请解封。这种钓鱼邮件也有很强的迷惑性，因为很多企业的内网管理规则确实会在某些情况下暂时禁用某些员工的内网帐号或邮箱帐号。如果企业用户没有认真甄别邮件的真伪，便直接申请“解封”，就很可能会中招。

Dear User [redacted],

4 收到的消息进行排队和等待传递
因为你的邮箱 ([redacted]) 是不可用（黑名单）。
在其他接收邮件，必须加入白名单您的邮箱。

白名单邮箱

Thanks,
QIYE.163.COM

二、 民间典型邮件骗术举例

民间流传的一些经典的邮件骗术虽然不是专门针对企业用户的，但也是企业用户可能经常接触到的一类钓鱼邮件。我们在这里也举几个比较典型例子供读者参考。

（一） 冒充富人的求帮助诈骗

某个生命垂危的老人或病人，希望能通过您的帮助把巨额财产捐献给国外的慈善机构或需要帮助的人；或者是某个有钱的贪官或地下组织希望通过您的帮助向异国转移货物或财产；而当您以为就要拿到巨额财产或提成的时候，对方却要求您必须先支付一定付费用来完成某些琐碎但必要的手续——这就是在西方国家已经流行了多年的有钱人求助骗局。而如今，我们在国内也截获了不少类似的诈骗邮件样本，不过其中绝大多数是英文邮件。

在有钱人求助骗局中，最为有名的一个骗局是上世纪 80 年代开始，起源于尼日利亚的尼日利亚骗局，也称为尼日利亚黑水骗局。在这个骗局中，受害者如果表示同意协助骗子管理或转移财产后，骗子首先会邮寄给受害者一些黑色的纸片和一瓶药水，受害者将药水滴在纸片上以后，纸片上的黑色就会褪去，变成美元。骗子解释说，直接邮寄现金是违法的，所以必须先将美元染黑之后再邮寄，而只有使用这种特殊的药水，黑纸才能变成美元，但由于前期投入太大，剩余资金不足，需要受害者帮忙出钱制作更多的药水。受害者一旦汇出制作药水的钱，就会与骗子失去联系。

此类骗术大多是由一封文词优美的，来自境外的电子邮件开始，之后通过多次的邮件往复，使受害人逐渐陷入骗局并向骗子的境外账户汇钱。而这些文词优美的诈骗邮件大多是用英文撰写的，在英语国家一直很流行。

好在中国人的英语平均水平相对较低，所以此类骗术在中国的成功率较低。但此类骗术对于在中国工作的外籍员工，或者是英文程度较高精英阶层，还是很具欺骗性的。特别是其优美的文词，往往让人很难相信它们会是出自骗子之手。

下面给出一个我们截获的一封尼日利亚骗局邮件的全文。

****

I am glad you responded to my email. My name is Ruby Jiro Hotarubi.I am 71 years of age and I lived in Willmar(Minnesota) until recently. I am diagnosed with a terminal case of laryngeal cancer which has defied all forms of treatment. Due to the rate at which it has spread through my body, I have been told that I have only a few more weeks to live. I don't want you to feel sorry for me in anyway,because I believe we all will die someday. What matters most is what we have done with the time given to us and how we have lived our lives.

I gave a lot of thought before i sent you the email, Whilst reading various topics from medicine, religion, economics i saw your email, i don't recall the exact site, at the time it did not occur to me to save it.I assumed there is a lot of energy that makes up life itself, i also believe this energy is never random. It is always focused and we need to make sure the focus is always positive. Negativity harms the sender.

This disease has changed my approach to life and how things work. There have been a few times in my life when something appeared to be so solid, so unbreakable, so much a part of life that I never dreamed it would change – only to later find myself living in what seemed to be a whole new world. I remember well the first time I experienced the loss of a friend. Jim Gross is the person who stepped in when my father stepped out. He was a gifted businessman in our community. My sister and i regularly babysat for his children, and Jim would often drive us home filling the car with a voice of encouragement met with listening ears. In many ways, it was Jim who had tucked the pillow of God under my head when i was prepared to give up on God. Jim was fit and trim. He played basketball almost every day. And still, Jim's life was stripped short, stopped in the middle of an ordinary game on the basketball court when he suffered a heart attack and died at the age of 42. At that time, the world as i knew it seemed to be turned upside down. I learned that life is not always fair – that bad things happen to good people – that some questions arise that will never be answered.

For many of us, the times we are experiencing are unlike anything we have experienced before. Each week i learn of someone else whose economic security blanket has been pulled from beneath them. Individuals who have worked for the same company for 15-20 years are being asked to leave. People who thought there was no doubt that they would be retiring from this same company have been given pink slips. Women and men with master's degrees and extensive experience in a myriad of fields are working for minimum wage. Countless others are pounding the pavement, resumes in hand, eager to see what door might open. And while all of this is happening, those who have retired are wondering if their hard-earned investments will ever rise to the level where they were before the economy started to weaken. The World's economy that once seemed to strong – so indestructible – has been spun around with us all holding on tight, praying that we have seen the worst of it and that recovery is on the way. It does not take much for the world to be changed.

One senseless death.

One lost job.

One parent leaving.

One diagnosis at the doctor's office.

One closed company.

One plane hitting a tower.

One broken heart.

One accident.

One empty tomb.

My own world changed after one diagnosis at the doctor's office.

The reason i sent you the email is to know if you have a heart for charity, thus would not have any problem locating deserving charity and human aid groups.

I believe if God gives me a second chance to come to this world again, I will live my life in a different way from how I have lived it now; but now that God has called me, I have willed and given most of my property and assets to my immediate and extended family members, as well as a few close friends. So far, I have successfully distributed money to some charity organizations in the U.A.E, Algeria and Malaysia. But my health has deteriorated so badly that I cannot do this by myself anymore. I once asked members of my family to close one of my accounts and distribute the money which I have there to charity organizations in Bulgaria and Pakistan, but they kept the money for themselves. Hence, I do not trust them anymore as they are clearly not contended with what I have left for them.

I intend to grant you access to my last possession on earth.The disbursement of this fund would be entirely in your hands. (I want atleast 80% given to charity)

I need to know if you can help me achieve this last desire of mine. I want to give to the needy, the widows, orphans and victims of disasters. The reference i gave you, i coined it Let Love reign.

Let me know if you are capable and willing to do this for me. It would be wonderful if you could tell me what charities you may have in mind as well. I will wait to hear from you.

Ruby

****

下面是另外一封非常有趣的，冒充国外银行管理人员的英文诈骗邮件，基本上也可以算是一种变形了的冒充富人求帮助诈骗。其邮件大意是：我是阿拉伯某国一家银行的管理人员。有一位与您姓氏相同，原籍相同的人在我们银行存了一大笔钱的定期存款，价值 1840 万美元。但存款到期之后，我们银行一直联系不上这个存款人。结果最后发现，这个存款人已经死于 2008 年 5 月 12 日的汶川大地震（作者注：英文钓鱼邮件能写出汶川大地震，也算煞费苦心）。由于您和存款人同姓同籍，所以如果我们俩内外联手，就能将这笔钱取出来，之后咱们俩对半分，我得到的那一半将会被用于慈善事业。

****

主题: i need your coopration

Dear Sir

I am sorry to contact you unannounced through this medium. I am Mr. Abdulkarim Alzarouni, Deputy General Manager-Audit & Compliance at National Bank of Abu Dhabi here in UAE . I write you this proposal in good faith hoping that I will rely on you . In 2006, one Mr. Omar Gerard who has same surname as yours and who has your country in his file as his place of origin, made a fixed deposit for 36 calendar months, valued at $18,400,000.00 with my bank. I was his account officer before I rose to the position of the auditor general now. The maturity date for this deposit contract was 16th of January 2009. Unfortunately, while on a business trip , he died in a deadly earthquake that occurred on May 12, 2008 in Sichuan province of China which killed at least 68,000 people.

Since the last quarter of 2009 until today,the management of my bank have been finding a means to reach him so as ascertain if he will want to roll over the Deposit or have the contract sum withdraw . Since September 2009,when I discovered that this will happen , I learnt of his death ,so I have tried to think up a procedure to preserve this fund and use the proceed for charity .

Some directors here have been trying to find out from me the information about this account and the owner, but I have kept it closed because, I know that if they become aware that Mr Omar is now late, they will corner the funds for themselves. Therefore, I am seeking your co-operation to present you as the one to benefit from his fund at his death since you have the same name, so that my bank head quarters will pay the funds to you. I have done enough inside bank arrangement and will only have to put in your details into the information network in the bank computers and reflect you as his next of kin.

I am not a greedy person, so I am suggesting we share the funds equal,50/50% to both parties My share will assist me to start a charity organization to help the poor and also own a company which has been my dream. Let me know your mind on this and please do treat this information as TOP SECRET. At the receipt of your reply, strictly through my personal email address, abdualzaruni@gmail.com I will give you details of the transaction. And a copy of the Deposit certificate of the fund and also the incorporation certificate of the company that generated the fund.

Anticipating your communication.

Mr Abdulkarim Alzarouni

****

（二） 装成穷人的扮可怜诈骗

与前述的冒充富人求帮助诈骗恰恰相反，也有骗子会专门把自己描述为无钱求学或急病求医的穷人来实施诈骗，目的是利用人们的同情心骗取钱财。下面就是一封我们近期在国内截获的扮可怜诈骗邮件。以下是邮件正文：

****

尊敬的女士/先生：

你好！

我是蓝蓝，一个可爱的女生，来自农村，目前在上海，我今年 7 月份高中毕业，并参加了高考，现在已经被上海对外经贸大学录取，将学习国际商务英语专业。

我有一个残缺但温暖的家庭，妈妈在我高三的时候抛弃了我和爸爸，跟着另外一个男人走了，现在音讯全无。爸爸在一家企业上班，是个小职员，工作非常辛苦，但是，每个月的薪水去掉房租和各种生活费后所剩无几。现在无力支付我的大学学费以及生活费（2016 年 9 月份入学时需要缴纳各种费用约 2 万多元，4 年大学期间一共需要花费大约 10 万元）。

我非常渴望学习，不想因此而辍学。所以，请你在收到这封邮件后，能够支持我一部分费用，帮助我完成我喜爱的学业。无论多少，哪怕一元、一角，都是你对蓝蓝的爱。并且请留下你真实有效的电话号码或其他联系方式，在我完成学业并且开始工作后，我将会联系你并且将你的资助资金全部归还给你。

谢谢。

我不是在开玩笑，也不是诈骗，这完全是真实的， 我想借助互联网寻求能帮助我的人。如果您是有缘人，想真心帮我的话， 我可以提供更多详细信息供您核实。
如果需要了解更加多的内容，请您回复。

抱歉，打扰了。。。

蓝蓝

2016-0X-XX 凌晨

****

从上面的邮件中可以看出，诈骗分子实际上是群发的邮件，并没有写出特定的收件人姓名；而且邮件使用的显然是假名或笔名，并没有留下自己的联系方式；信中虽然说明了自己将要上哪所大学，但却没有说明自己毕业于哪所中学。骗子这样做其实就是为了防止被人举报，防止收件人到其所谓的毕业中学去核实相关信息。而一旦收件人动了善心回复邮件给对方，就会逐步落入骗子的陷阱。

三、 企业邮箱反钓鱼建议

钓鱼邮件的识别与防范，同样需要技术方法的运用与员工素质的提高这两方面因素的共同作用。

（一） 技术措施

1） 选择使用上一章中介绍的各种邮箱防盗号技术措施，就可以最大限度的降低 OA 钓

鱼邮件带来的危害。

2） 选择具有较强反钓鱼能力的安全引擎配合垃圾邮件过滤。

（二） 员工教育

教育员工养成以下的良好邮件阅读习惯。

1） 收到类似邮箱升级、邮箱停用等办公信息通知类邮件时，一定要注意查看邮件的发件人的邮箱后缀是否为企业邮箱后缀，如果不是，则一定是钓鱼邮件。

2） 不要轻信发件人邮箱地址中默认的“显示名”，因为显示名实际上是可以随便设置的，要注意阅读发件邮箱的全称。

3） 对于陌生人发来的邮件，不要轻易点开邮件中的链接。如果接到的邮件是邮箱升级、邮箱停用等办公信息通知类邮件，在点开链接时，还应认真比对链接中的网址是否为企业内网网址，如果不是，则为钓鱼欺诈。

第四章　带毒邮件

从电子邮件刚刚普及的年代，就已经出现了携带病毒附件的邮件攻击形式。不过，随着安全软件的普及和反垃圾邮件系统的不断升级，群发带毒邮件的攻击方式越来越难以成功。但尽管如此，2016 年以来，Coremail 论客与 360 的联合监控平台每天仍能截获 6000 封左右的带毒邮件，最高峰时期可达单日数万封。

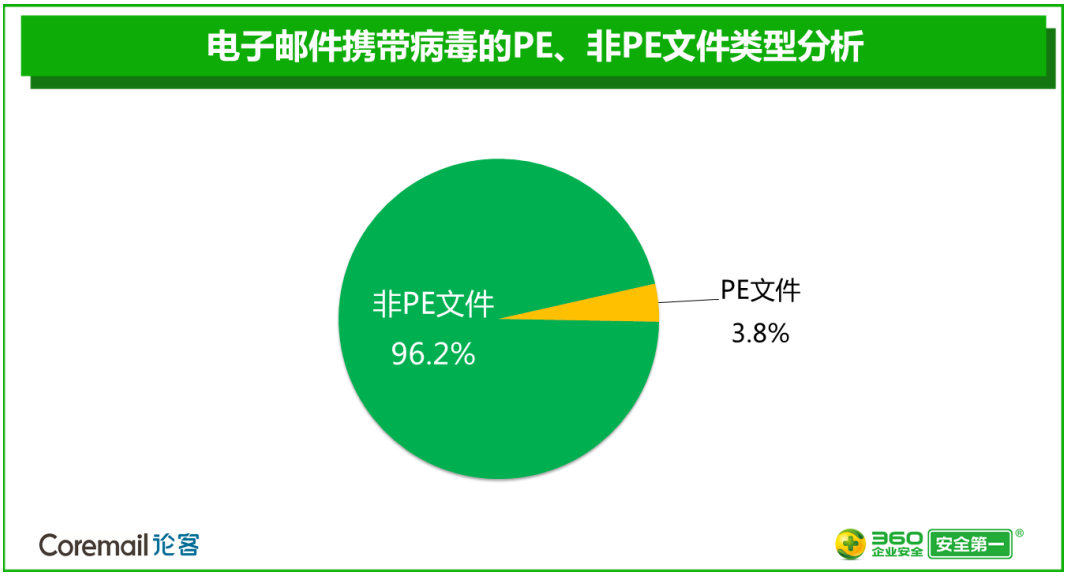
此外，利用邮件进行有针对性的攻击，特别是结合了社会工程学手法的邮件攻击，也仍然十分流行。特别值得注意的是，对于只针对有限目标发送的，针对性很强的带毒邮件，普通的垃圾邮件过滤系统往往很难识别。因为这些邮件并不具备一般垃圾邮件所具有的海量群发、或使用大量推广语汇的特点，而且病毒样本的传播范围也非常有限。

识别带毒邮件，一般需要在普通的垃圾邮件过滤系统之上，再增加一套恶意程序识别系统，并且该系统具有较强的特种木马识别能力。

本章主要针对带毒邮件的带毒类型，攻击目的，伪装方法和一些很难识别的典型攻击手法进行分析说明。

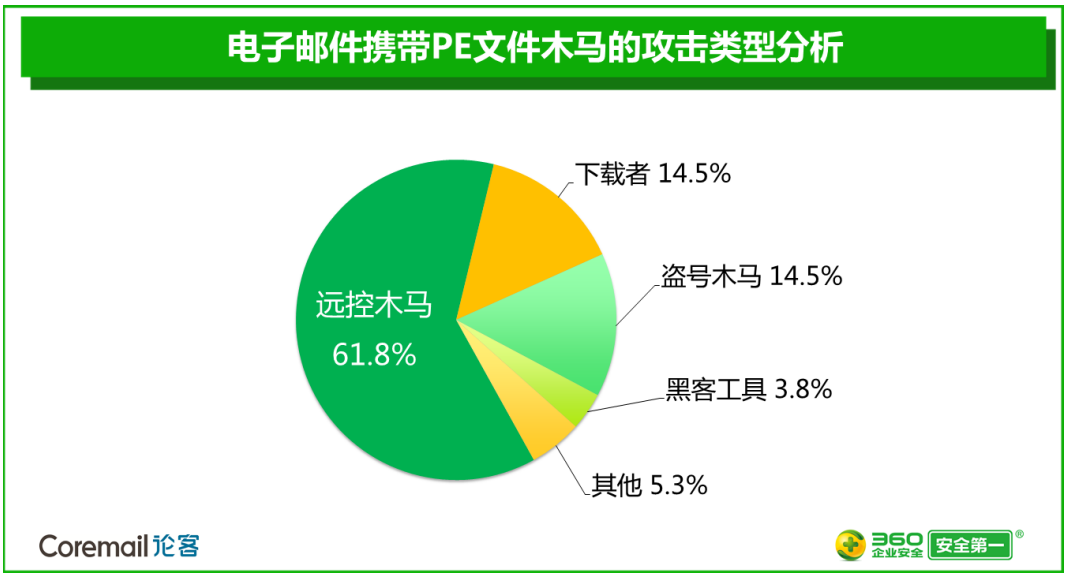
一、　带毒邮件的带毒类型

本次报告针对 2016 年 10 月截获的一大批带毒邮件进行了抽样分析。统计显示，所有的带毒邮件都是以附件形式携带的木马病毒。而在所有带毒邮件的病毒附件中，PE 文件（可执行文件）占 3.8%，非 PE 文件占比为 96.2%。可见，非 PE 文件是绝对的主流。而这也正是带毒邮件最让人担忧的问题。因为对于有防毒经验的人来说，如果邮件附件是可执行文件，轻易是不会去打开的。但如果邮件附件是非 PE 文件，则用户的警惕性通常都会大大降低。

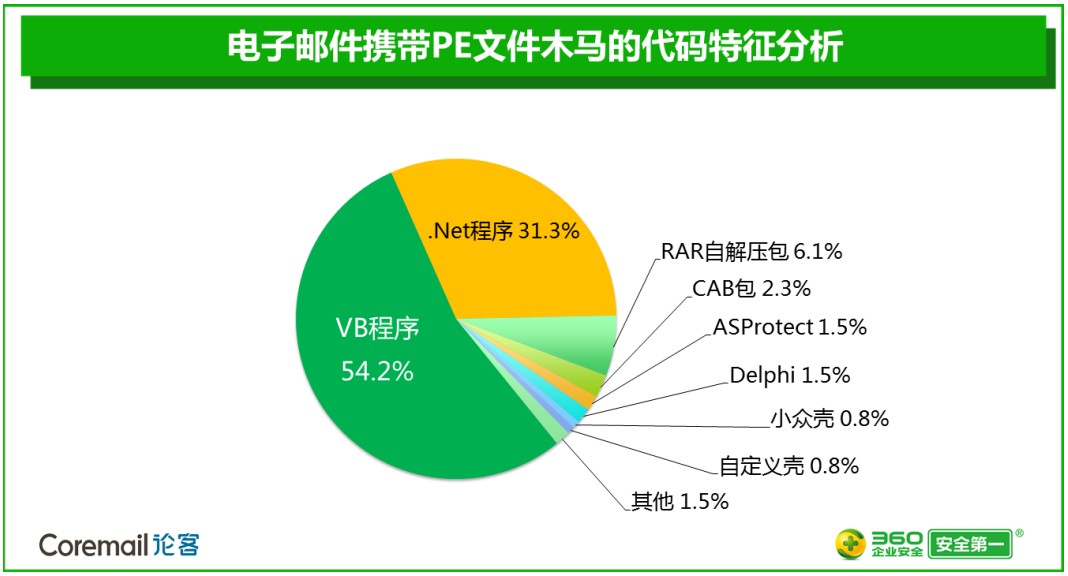


（一） PE 文件

从攻击类型上来看，在邮件携带的 PE 文件木马样本中，远控木马最多，占到了 61.8%，其次是下载者（将更多的木马病毒下载到电脑中的一种木马程序），占 14.5%

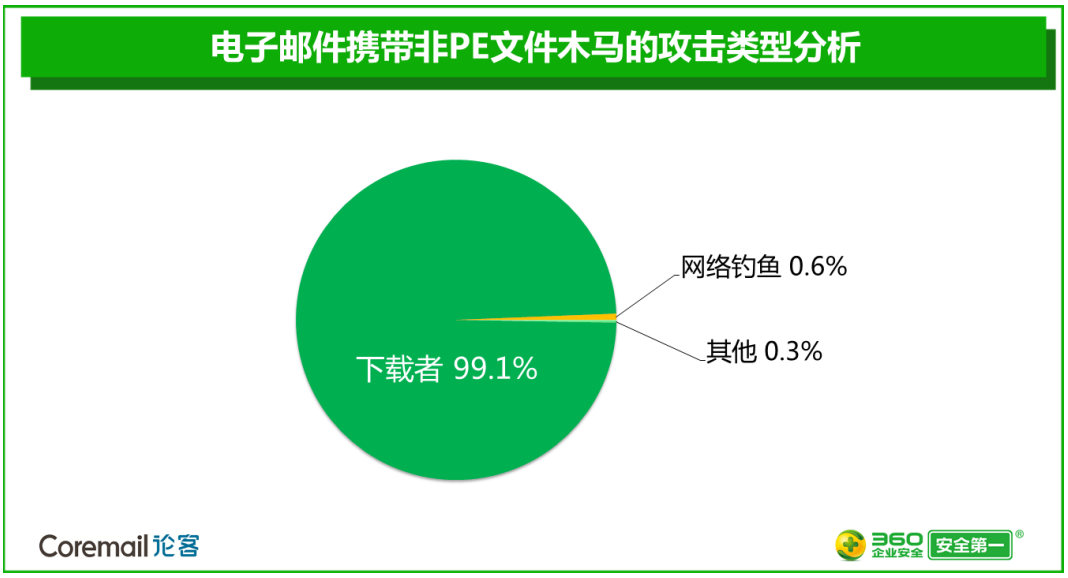


从代码特征上来看，在邮件携带的 PE 文件木马样本中，VB 程序最多，占 54.2%；其次是.Net 程序，占 31.3%；RAR 自解压包排名第三，占 6.1%。

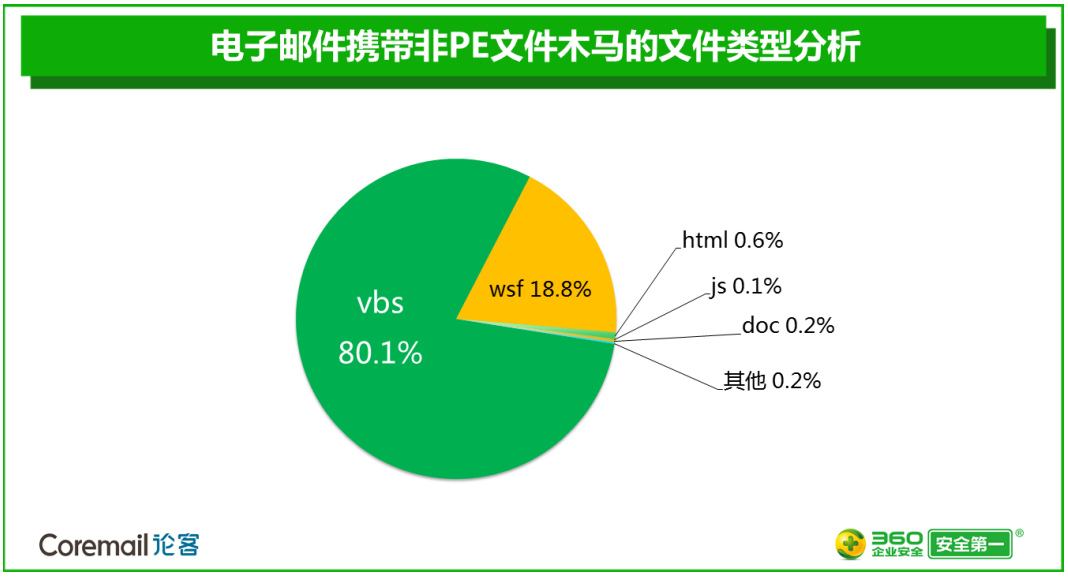


（二） 非 PE 文件

非 PE 文件木马程序的类型相对来说就比较单一了。从下图中可见，下载者木马占到了邮件携带的非 PE 文件木马程序的 99.1%；而其他类型的非 PE 木马的总和不足 1%。



从文件的类型来看，在邮件携带的非 PE 文件木马样本中，vbs 程序最多，占 80.1%；其次是 wsf 程序，占 18.3%；其他类型的非 PE 木马在邮件出现比例都非常低。



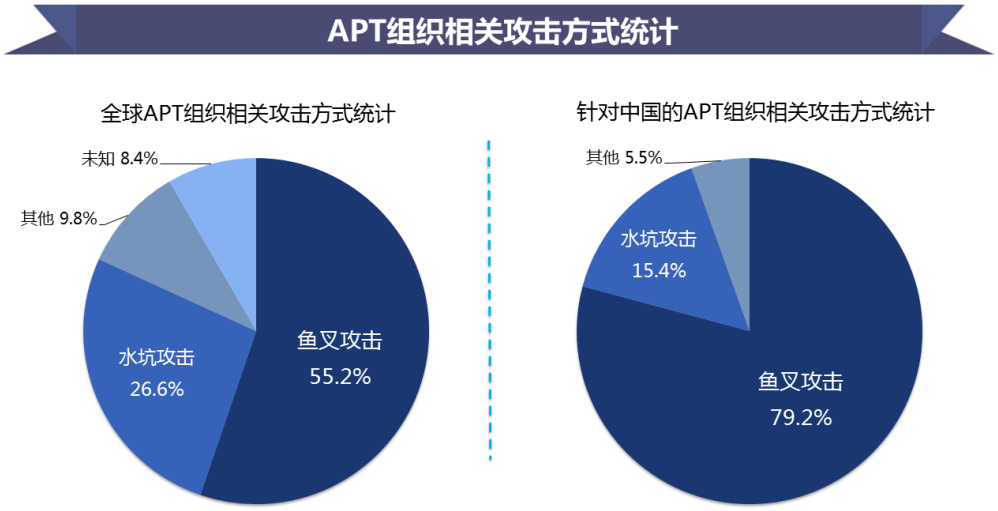
二、 APT 攻击中的鱼叉邮件

带毒邮件的一种比较特殊的形态是鱼叉邮件，特指在高级持续性攻击，即 APT 攻击中，攻击者专门发送给特定攻击目标的一种带毒邮件。鱼叉邮件与普通的带毒邮件有两点最主要的不同：一是鱼叉邮件通常不会群发给很多人，而是非常精确的发送给某一个人或几个人；二是鱼叉邮件通常不是以获取经济利益为目的。其攻击目的主要是窃密情报机密，另外就是在极少数情况下会以破坏为目的。

APT 攻击会采用的手法很多，但鱼叉攻击是被使用最为频繁的。不过，特别值得注意

的是，根绝 360 威胁情报中心发布的《2015 中国高级持续性威胁（APT）研究报告》显示，在针对国内目标发动的 APT 攻击中，79.2%的攻击使用的是鱼叉攻击；而从全球来看，APT 攻击中使用鱼叉邮件的仅占 55.2%。

下图援引自《2015 中国高级持续性威胁（APT）研究报告》。



为什么在针对中国的 APT 攻击中，鱼叉邮件的使用比例会远远高于全球平均水平呢？这主要是因为：鱼叉邮件的实施成本要明显低于水坑攻击等其他攻击手段，但相比之下，鱼叉邮件也是最容易被识破的攻击，而中国的企业用户的安全意识水平普遍不及西方国家用户，所以，使用鱼叉邮件对中国用户实施攻击的成功率要高于西方国家，所以攻击者在攻击中国时，更乐于选择使用成本较低，但收益不低的鱼叉邮件。

三、 企业邮箱防毒建议

（一） 技术措施

1） 企业邮箱的服务系统应当配备反病毒引擎，并且应确保该反病毒引擎为国内用户普遍使用的主流引擎，这样才能保证病毒样本收集更快，更全面。

2） 企业用户办公电脑上，应安装统一管理的反病毒软件，以做到针对新生病毒样本第一时间发现，第一时间查杀。

3） 在企业内网系统中，构建终端安全软件与邮箱服务端反病毒引擎的协同联动机制，使终端安全软件能够成为邮件服务系统的恶意样本探测器，一旦在终端上捕获新的恶意样本，立即上报给邮件系统的反病毒引擎，从而可以立即阻止同类病毒样本继续通过邮件系统对用户发动攻击。

在上述三点中，第三点目前还很少有企业在实践中使用。特别是目前绝大多数的邮件服务商并不具备专业的反病毒能力，而专业的反病毒厂商往往又普遍缺乏在邮箱服务系统中采集恶意样本的能力。而 Coremail 论客与 360 的合作则为这一长期矛盾提供了深层次的解决方案。

（二） 员工教育

在防范带毒邮件攻击方面，企业应当对员工进行以下几方面的基本教育：

1） 对于陌生人发来的邮件，不要轻易点开邮件附件。

2） 下载邮件附件，一定要先查毒，再打开。

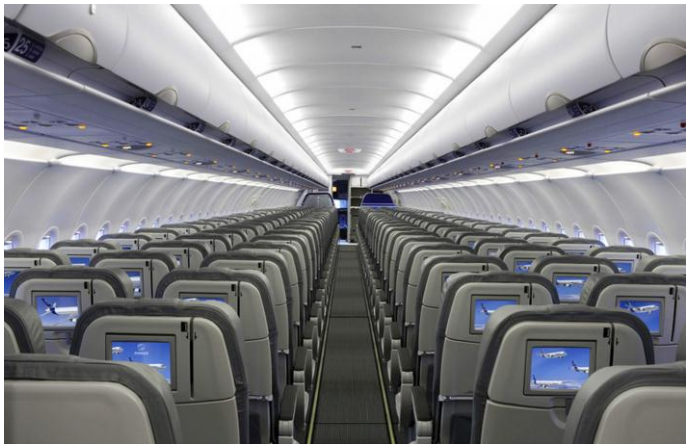
3） 可以将安全性存疑，或安全性不确定的邮件附件，放在电脑安全软件提供的沙箱功能中打开或运行，从而即能看到附件中文件的内容，又可以最大限度的保护电脑不受侵害。

4） 遇到邮件附件为可执行文件时，绝对不能直接点开，特别想打开看的话，也一定要放在沙箱中运行。

附录 2016 年全球电子邮件十大安全事件

以下事件，按照发生时间排序。

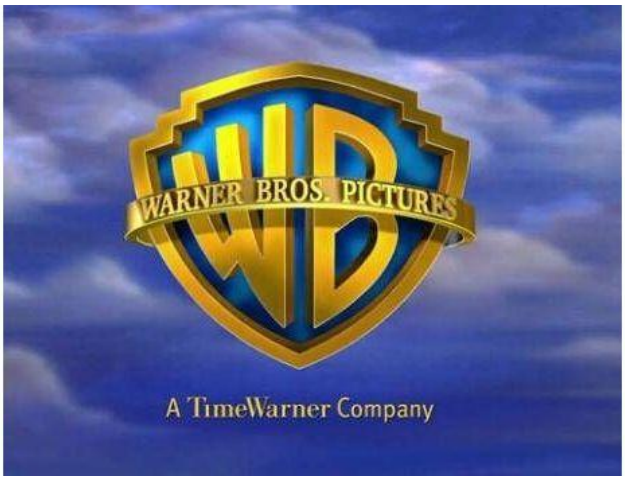
一、 FACC CEO 遭邮件诈骗 5000 万欧元



2015 年 12 月到 2016 年 1 月，被中航工业集团收购的奥地利飞机零部件制造商（FACC）陆续向多个海外账户汇出 5000 万欧元。这次诈骗是个典型的身份造假诈骗，也被称为“商务电子邮件攻击”。攻击者冒充其他员工或合作伙伴，给首席执行官发送电子邮件，要求紧急汇款。2016 年 5 月，FACC 公司 CEO 沃尔特•史蒂芬（Walter Stephan）因此被解雇。

尽管 FACC 公司已设法追回了被盗的 1090 万欧元，但其余的资金仍然不翼而飞，或分布于斯洛伐克和亚洲各地的银行中。

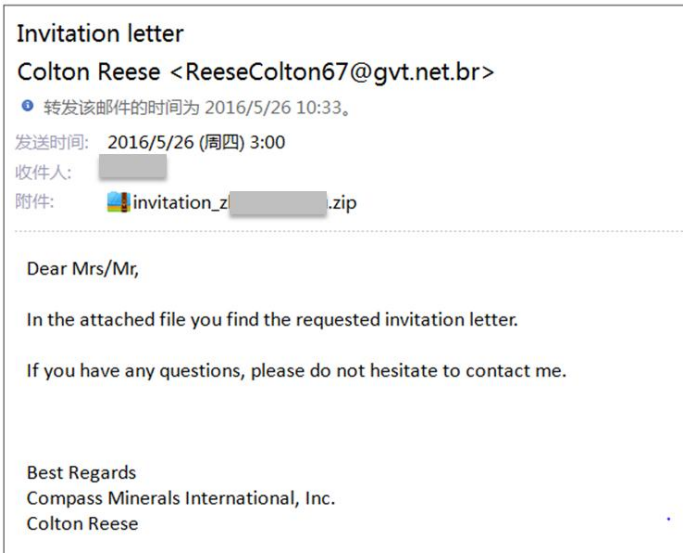
二、 时代华纳 30 多万客户邮箱泄漏



据国外媒体 2016 年 1 月 8 日报道，美国最大的有线电视公司时代华纳表示，旗下约有 32 万用户的邮件和密码信息已被黑客窃取。据悉，这些邮件和密码信息很有可能是通过网络钓鱼的方式获得，同时也可能是保存了时代华纳用户数据的第三方合作商信息泄露所致。FBI 已经介入调查，尽管还没有确定信息泄露的最终原因，但时代华纳并不认为有迹象显示

其内部系统出现了漏洞。

三、 敲诈者木马通过邮件大规模攻击



2016 年 2 月中旬，一种名为“Locky”新型病毒开始伪装成电子邮件附件的形式，在全世界各地迅速传播，并很快成为最流行敲诈者病毒之一。一旦电脑用户点击携带病毒的附件，则计算机上的办公文档、照片、视频等文件就会被恶意加密。用户要想重新解开数据的密码，就必须向这款病毒的发布者缴纳一定数量的赎金。

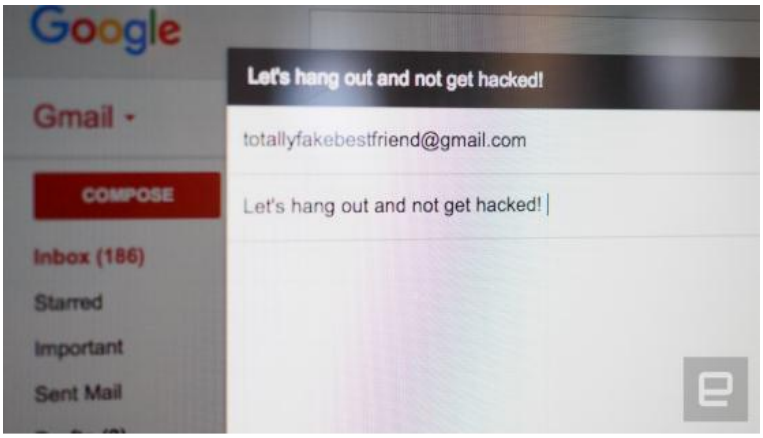
根据 360 互联网安全中心的监测，以“Locky”为代表的敲诈者木马在 2016 年大规模爆发，并先后于 4-5 月及 9-10 月形成两次集中高发期。全年攻击电脑用户多达 497 万次。而根据 2016 年上半年的监测情况来看，恶意电子邮件约占敲诈者木马传播总量的 14%。

四、 通灵邮件诈骗百万美国人 1.8 亿美元

2016 年 5 月 9 日，美国纽约联邦检察官表示，目前已与一宗算命诈骗案的多个被告达成和解，这些被告涉嫌从超过 100 万美国人身上骗取逾 1.8 亿美元（约 11.7 亿元人民币）。

检察官卡珀斯表示，被告包括来自法国的“灵媒”杜瓦尔(Maria Duval)与格林(Patrick Guerin)、加拿大直销公司 Infogest 及香港公司 Destiny Research Center Ltd.，他们被指通过邮件向美国老人及其他弱势消费者推销虚假声明。这些诈骗者声称，通灵者有特别视力，知道如何发财，包括如何中彩票。借此要求收件人购买有关产品和服务。这些大量内容相同的信件目标是“绝望及年老体弱者”。

五、 俄罗斯 2 亿电子邮件账号被售卖



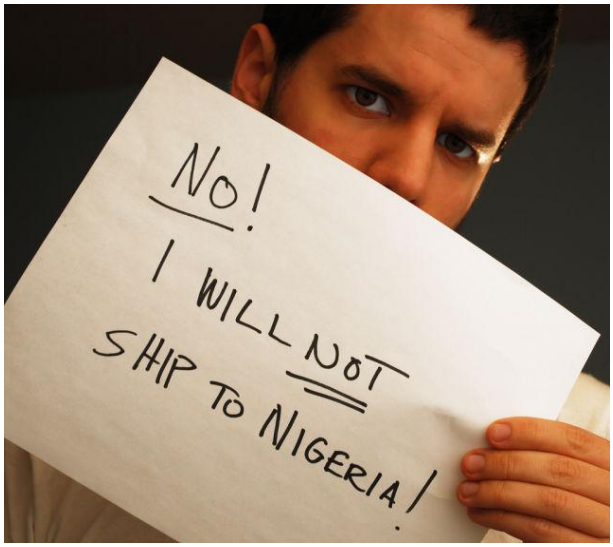
2016 年 5 月，在俄罗斯黑市上，大约有超过 2.72 亿个被盗的电子邮箱和其它网站登录凭证被售卖，其中大部分是俄罗斯本地的电子邮箱服务 Mail.ru 的用户名和密码，此外还包括了少部分 Google、雅虎以及微软的电子邮箱登录凭证。据了解，许多账号被盗用户都是美国最大银行、制造商以及零售商的员工。

令人意外的是，这样一个庞大的被盗邮箱数据正在以 50 卢布（不到 1 美元）的超低价格对外销售。这一大规模的被泄露数据可以用于进一步非法获取用户信息，或是进行钓鱼攻击，导致用户的财务信息或名誉受损风险增长。

六、 带毒邮件盗取日大型旅社 800 万用户资料

2016 年 6 月，日本大型旅行社 JTB 宣布，因员工打开钓鱼邮件导致网路遭到非法入侵，有近 800 万客户资料外泄，包括姓名、地址及护照号码等。办案人员称，该钓鱼邮件伪装成全日空（ANA）发来的电子邮件。邮件地址包含「ana」，内容为提醒确认机票预定。员工打开该邮件后，导致电脑及服务器中毒，大量资料被泄露。警方以违反《禁止非法入侵电脑法》进行调查，从邮件 IP 位置得知，该邮件发送源头在海外，最后发送地则是香港。

七、 尼日利亚电邮诈骗 6000 万美元



2016 年 8 月、尼日利亚抓获一名涉嫌在全球范围内利用数千封电子邮件实施诈骗的跨国犯罪团伙头目。这名嫌犯为 40 岁的尼日利亚籍男子，人称“迈克”。据信该嫌烦已使全球数百网民蒙受 6000 万美元（约合 3.98 亿元人民币）损失。其中一人被骗金额高达 1540 万美元（约合 1.02 亿元人民币）。

嫌犯的作案手法包括：篡改供应商的电子邮件，给采购商发去虚假信息，要求其向该团伙控制的银行账户打钱；控制企业高管的电子邮箱，利用该邮箱要求负责财务的雇员电汇款项等。

八、 德国莱尼集团遭邮件诈骗 4000 万欧元

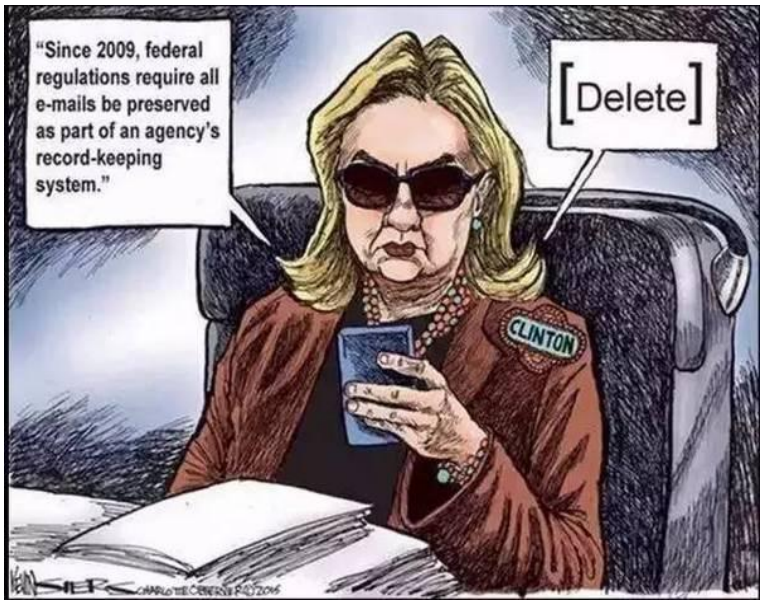
2016 年 8 月 12 日，作为欧洲最大的电线电缆制造商，全球第四大供应商的德国莱尼集团在北罗马尼亚的分公司收到了骗子模仿官方支付需求发出的诈骗邮件。莱尼在北罗马尼亚分公司的财务官认为，这封邮件是莱尼德国总部的顶级高管发来的，而且该公司的信息系统也是欧洲最安全的系统之一，于是 4000 万欧元就这样被汇到了骗子的账户上。这一消息致使该家公司股票下跌 5 至 7 个百分点。

九、 雅虎逾 5 亿用户资料两年前被窃

2016 年 9 月 22 日，即将谢幕的美国互联网公司雅虎证实，至少 5 亿用户的账户信息在 2014 年遭黑客盗取，这创造了史上最大单一网站信息遭窃的纪录，也让正在出售核心业务的雅虎再受重创。

雅虎在一份声明中表示，受影响用户的姓名、邮箱地址、电话号码、出生日期、密码以及部分取回密码时的安全问题，都遭到了泄露。雅虎相信，盗取信息的黑客是“受到国家支持的”，但没有具体点名哪个国家。

十、 希拉里邮件门影响美国大选



2016 年 11 月，希拉里因“邮件门”最终落败美国总统竞选。希拉里在担任国务卿期间，从未使用域名为“@state.gov”的政府电子邮箱，而是使用域名为“@clintonemail.com”的私人电子邮箱和位于家中的私人服务器收发公务邮件，涉嫌违反美国《联邦档案法》关于保存官方通信记录的规定。希拉里被美国联邦调查局（FBI）调查，民众支持率节节下降。

希拉里承认在任职美国国务卿期间使用私人邮箱处理约 6 万封邮件，称其中 3 万封因涉及私人生活已被其团队删除，剩余约 3 万封与工作相关邮件已全部上交美国国务院。

“邮件门”让希拉里呈现出非常负面的形象：蔑视规则、凌驾于法律之上、受到舞弊体系的保护。