邮件加密普及之日就是欺诈邮件消亡之时

根据美国联邦调查局(FBI)互联网犯罪投诉中心(IC3)发布的《2023 年互联网犯罪报告》显示，商业邮件攻击(Business Email Compromise, BEC)在 2023 年给美国企业造成了 29 亿美元的损失，成为第二大最具破坏性的互联网犯罪。2013 年 10 月至 2023 年 12 月期间，BEC 攻击事件给美国和全球组织造成了近 555 亿美元的损失。为此，FBI 针对降低 BEC 攻击提出了以下建议：

(1) 使用多重身份验证 (MFA) 和多人双重验证来确认更改付款账户信息的请求。
(2) 为每项在线服务使用独特的密码，并尝试定期更改密码。
(3) 确保电子邮件中 URL 与其声称来自的企业/个人相关联。
(4) 注意可能包含真实域名拼写错误的假冒网站超链接。
(5) 切勿通过电子邮件提供登录凭证或个人身份信息(PII)，即使请求看似合法。
(6) 验证发件人的电子邮件地址，尤其是在使用移动或手持设备时，确保其与发件人相符。
(7) 确保员工计算机设置允许查看完整的电子邮件头等扩展信息。
(8) 定期监控财务账户是否存在异常情况，例如存款丢失。

英国国家网络安全中心(NCSC)也专门针对 EBC 攻击设计了一个通俗易懂的 PDF 宣传页，并详细解释了什么是 BEC 攻击和如何防范。EBC 攻击是一种网络钓鱼攻击形式，犯罪分子试图诱骗高级管理人员（或财务人员）转移资金或泄露敏感信息。BEC 攻击背后的犯罪分子发送看起来令人信服的电子邮件，这些电子邮件可能会要求不寻常的付款，或包含指向假冒网站的链接。某些电子邮件可能包含伪装成无害附件的病毒，这些病毒在打开时会被激活。与不加选择地向数百万人发送的网络钓鱼电子邮件不同，BEC 攻击旨在吸引特定个人，并且更难被发现。BEC 攻击对各种规模和所有部门的所有组织都构成威胁，包括非营利组织和政府。

笔者通过对 BEC 攻击给受害者发送的各种电子邮件案例分析，特撰写此文，明确告诉大家：只有普及应用 S/MIME 邮件加密技术才能防范所有 BEC 攻击，FBI 和 NCSC 的建议只能起到一定的帮助作用，不能彻底解决问题。只有普及了邮件加密，才能真正有效防范 BEC 攻击，彻底消灭邮件欺诈。

一、电子邮件数字签名，能保证邮件发件人可信身份，确保收件人不会上当受骗！

BEC 攻击的第一个特点就是假冒公司高管给财务人员发邮件要求付款或者更改已审批的收款方信息，这是攻击者利用电子邮件的设计漏洞发起的攻击，因为邮件发件人的邮件地址是可以随意编写的，可以写成公司 CEO 一样的邮件地址发送欺诈邮件，虽然目前已经有了 SPF、DKIM、DMARC 等验证发件人身份的相关标准，但是并不是所有邮件系统和邮件客户端支持这些标准，即使支持也并不能有效拦截所有攻击。

即使邮件服务器依据这些标准严格验证发件人身份后真的拦截了假冒邮件地址的邮件，但是攻击者还可以注册一个类似真实域名的假冒身份域名来通过这些严格的验证而成功送达欺诈邮件。如下图 1 所示，看起来是真实的邮件地址发送的邮件(图示为模拟效果)，下图 2 则是看起来很像真实域名的假冒域名的邮件地址发送的电子邮件(注意 0 和 o 的不同)，下图 3 是利用了邮件客户端(如 Outlook)无法完整显示长邮件地址的问题而显示看起来是真实的邮件地址，其实隐藏了后面的假冒域名。可以看出，这些看起来真实的邮件地址，一般人是无法识别出真伪的。这就是为何 NCSC 要求确保所有重要的电子邮件请求都使用其他方法进行验证（例如短信、电话、登录账户或通过邮寄或亲自确认）。

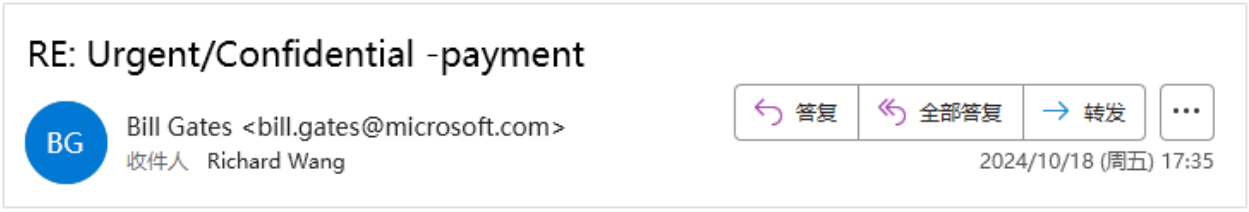

图 1 看起来没有问题的假冒身份邮件发件人

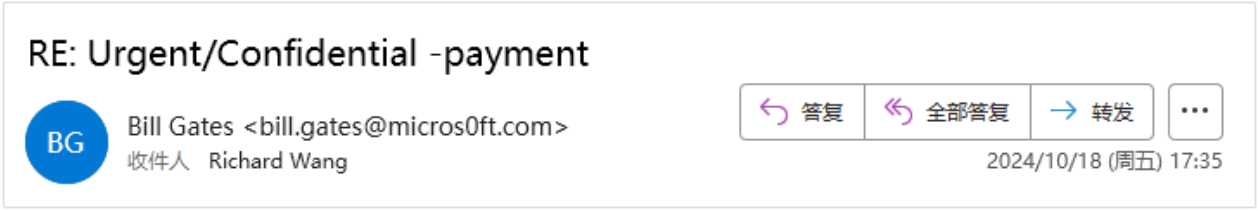

图 2 使用假冒域名的邮件地址

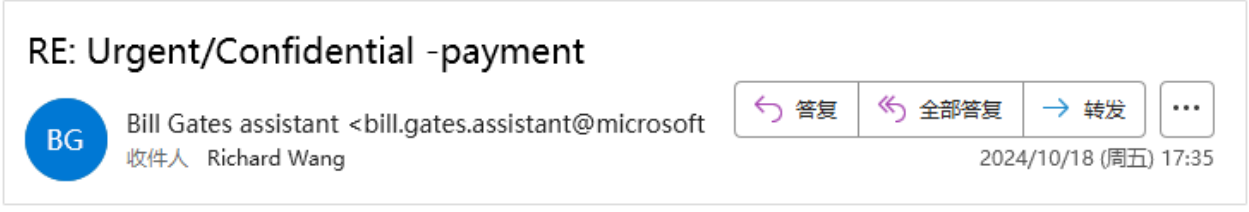

图 3 Outlook 无法展示完整邮件地址

但是，如果使用零信浏览器收发电子邮件，零信浏览器不显示发件人设置的姓名，因为这个自己设置的姓名不是可信的身份信息，所以仅显示邮件地址。凡是没有数字签名和加密的邮件都会在收件人邮件地址行下面显示一个警告惊叹号标识和一个黑色开锁，表示此邮件没有数字签名和没有加密，以提醒用户注意发件人身份是否可信，如下图 4 所示。而如果有数字签名，则会增加显示签名者的邮件证书绑定的邮件地址和证书中验证的身份信息。对于仅验证邮件地址的发件人，会显示 T1 认证标识和仅显示已验证的发件人邮件地址，如下图 5 所示。

图 4 无数字签名和加密的邮件 UI 展示

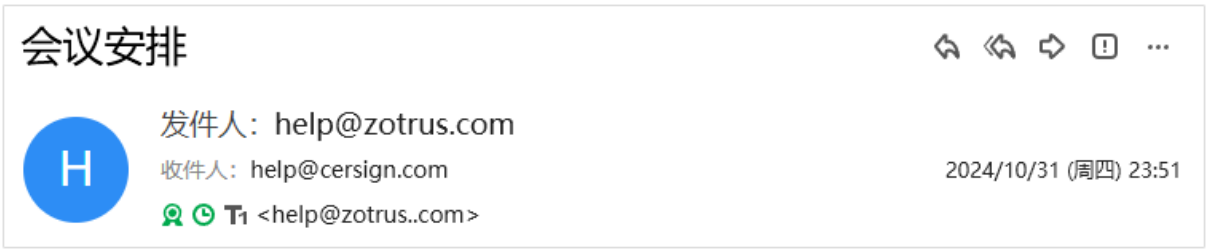

图 5 有数字签名的邮件 UI 展示(MV 认证用户)

对于已经完成个人身份认证的发件人，数字签名邮件会显示 T2 认证标识和显示发件人已认证的姓名和邮件地址，如下图 6 所示。对于已完成单位身份认证的发件人，数字签名邮件则显示 T3 认证标识、发件人邮件地址和单位名称，不会显示发件人姓名，因为发件人身份并没有认证，如下图 7 所示。对于已完成单位身份认证和单位员工身份认证的发件人，数字签名邮件则显示 T4 认证标识、发件人姓名、邮件地址和发件人所属单位名称，如下图 8 所示。

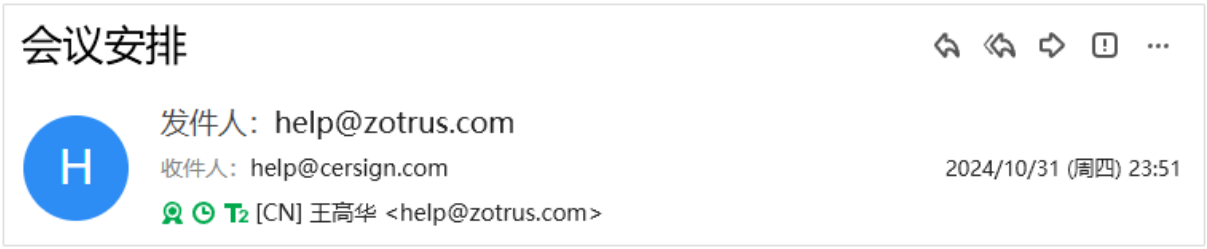

图 6 有数字签名的邮件 UI 展示(IV 认证用户)

图 7 有数字签名的邮件 UI 展示(OV 认证用户)

图 8 有数字签名的邮件 UI 展示(SV 认证用户)

由于所有 CA 必须验证用户邮箱控制权才会签发邮件证书，所以假冒邮件地址是无法申请到绑定没有控制权的真实邮件地址的邮件证书的，所以，即使假冒者能把发件人邮件地址写成真实的邮件地址，但是零信浏览器会展示其邮件证书中绑定的邮件地址，并在发件人邮件地址后面增加一个警告惊叹号标识，以提醒用户注意所声称的邮件地址与邮件证书绑定的邮件地址不一致，如下图 9 所示。

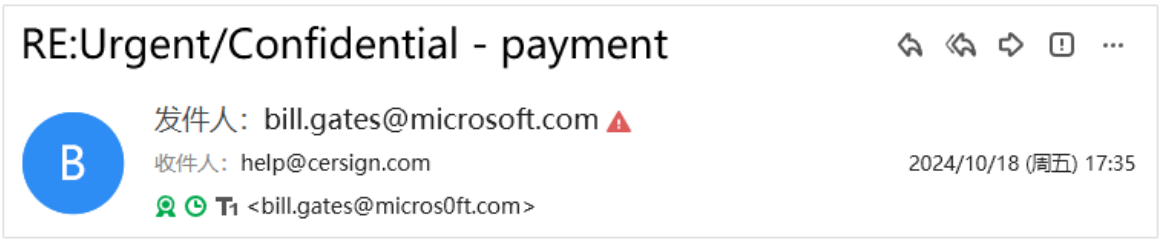

图 9 发件人声称的邮件地址与证书绑定的实际邮件地址不一致时 UI 提醒

这就是数字签名的火眼金睛威力！相信用户看到这些不同的认证标识、相关警示信息和展示已认证信息一定不会再上当受骗了，假冒身份欺诈将不再得逞，这就是 S/MIME 加密技术的魅力，其他不关心邮件发件人身份认证仅重视邮件加密的解决方案是达不到的这种防止身份欺诈的效果的，先进的邮件加密解决方案必须同时注重发件人身份认证和加密，才能保证邮件安全。

用户还可以点击每个标识，查看具体含义，如下图 10 所示，点击数字签名标识，会显示：邮件已数字签名(SM2)，括号里面显示签名算法。并且明确告诉用户：电子邮件内容在收发过

程中没有被非法篡改，这是数字签名的核心功能。如果邮件内容被篡改，则数字签名无效，零信浏览器会显示显示签名有问题标识和显示“数字签名有问题，邮件内容已被篡改，请勿相信邮件内容!”，如下图 11 所示，相信任何人看到这样的警示信息都不会执行邮件中要求转账的指示的。如下图 12 所示，Outlook 也会对已篡改的电子邮件有提示。

图 10 点击签名图标查看详情

图 11 邮件内容有篡改的 UI 提醒

图 12 Outlook 显示数字签名有问题

之所以有这样的 UI 展示，是因为数字签名邮件是不允许篡改的，即使篡改了一个字节，数字签名失效，这就是密码的魅力。而仅有数字签名的邮件是有可能被篡改的，因为电子邮件内容并没有加密。只有电子邮件加密了，才不会被非法篡改，如果一个加密邮件被篡改了，那收件人就极有可能收不到这封邮件了，也就是不会上当受骗了。而即使收件人能收到邮件(很高技术手段的篡改)，零信浏览器也一定会通过验证数字签名无效而显示上面的警告信息，从而可以避免收件人上当受骗。

二、电子邮件加密，能保证邮件内容不会被非法篡改和非法窃取，也就保证了收件人不会上当受骗！

BEC 攻击的第二个特点更有攻击性，不假冒发件人身份发送欺诈电子邮件，电子邮件的确是真实的发件人如公司 CEO 发出的，但是由于电子邮件没有采用加密技术，使得电子邮件在传输过程中被攻击者非法篡改，修改 CEO 的要求转账给 A 公司的邮件内容改为转账到 B 公司账户，这种攻击即使是有高度警惕意识的财务人员也是无法防范的。

但是，如果电子邮件已加密，则攻击者根本无法篡改邮件内容，无法实施 BEC 攻击，也就不会有高达 555 亿美元的损失了，这就是邮件加密的重要性。电子邮件仅有数字签名还是不够的，因为攻击者还有可能篡改已签名邮件的内容，而收件人有可能会忽视邮件客户端的警告信息，因为电子邮件在传输过程中数据有可能会丢包，而导致邮件内容不完整而显示为“数字签名有问题”。

这就是为何使用零信浏览器发送的每一封电子邮件都是默认加密的，以保证电子邮件在传输过程不会被非法篡改，在存储过程中不会被非法窃取邮件内容，只有每一封电子邮件都加密了，才能保证收件人不会遭遇 EBC 攻击而上当受骗。如下图 13 所示，会在邮件加密状态栏显示加密标识，如果是采用国密算法加密，还有增加显示国密加密标识。

图 13　UI 显示邮件国密加密、数字签名、时间戳和 T4 认证信息

用户还可以点击加密标识，会显示“邮件已端到端加密(SM2)”，括号后显示加密算法，同时显示“从发件人发出邮件到您收到邮件的全程都是加密的”，这就能让用户坚信电子邮件内容是真实的，是不可能被篡改的，如下图 14 所示，用户还可以点击“证书有效”，查看邮件加密证书详情。

图 14 点击加密锁标识查看详情

三、电子邮件时间戳，保证邮件发送时间可信，彻底解决了邮件发送时间欺诈难题。

BEC 攻击还有一种情况是笔者独家发现的，那就是假冒邮件发送时间，这是同邮件发送者的邮件地址可以随便设置一样的问题，邮件发送时间也是可以随便设置的，这就给需要证明邮件发送时间的欺诈有了钻空子的机会，这类欺诈邮件非常有隐蔽性，普通用户根本无法发现这个问题，因为目前所有邮件客户端都是直接显示邮件头中声称的邮件发送时间。

如下图 15 所示，使用 Outlook 查看这封邮件，看到的邮件时间为 10 月 31 日 23 点 34 分。但是，如果使用零信浏览器查看这封邮件，如下图 16 所示，看到的邮件时间是 11 月 1 日 0 点 14 分，这是用户使用零信浏览器发送邮件时自动附署的时间戳时间，这才是真实的邮件发送时间。可以看出：邮件发送者电脑时间比标准时间晚 40 分钟。

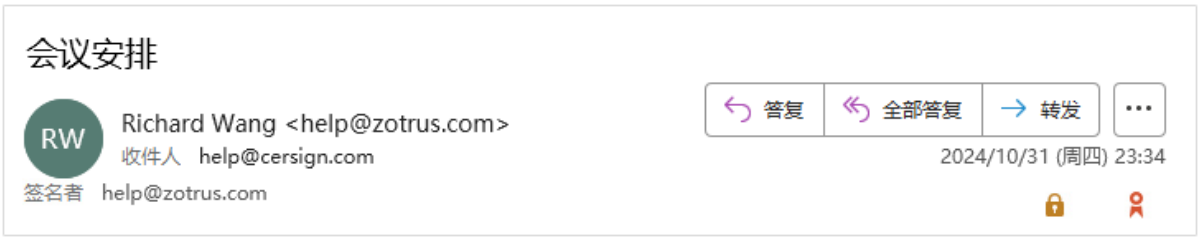

图 15 Outlook 显示的邮件时间是不可信时间

图 16 零信浏览器显示时间戳标识，表明所显示的邮件时间是可信时间

从这个演示案例可以看出，如果 10 月 31 日是某个事件要求发送邮件的截至时间的话，则

只有零信浏览器才能正确识别出用户的发送邮件时间已经过了截至时间，其他所有邮件客户端都只是读取邮件头中的不可信时间而会认为邮件发送者发送邮件的时间是符合要求的。这就是零信浏览器免费提供的电子邮件时间戳服务的威力，让电子邮件发送时间可信，不可假冒和不可否认，因为有时间戳数字签名可以证明真实的邮件发送时间。用户还可以点击时间戳标识查看详情，如下图 17 所示。

图 17 点击时间戳标识查看详情

零信浏览器全球独家创新提供的电子邮件时间戳服务能有效地杜绝邮件发送时间欺诈，能保证每一封电子邮件的发送时间是可信时间，这个功能可用于各种需要证明邮件发送时间的应用场景，这就彻底解决了电子邮件发送时间的原始设计缺陷，让欺诈者无法钻空子而实施邮件发送时间欺诈。

四、邮件加密普及之日就是欺诈邮件灭亡之时

相信大家通过阅读上面的内容已经充分体会到了电子邮件数字签名、加密和时间戳的威力和魅力，为何这么好的技术并没有得到普及应用，从而可以有效地防止 BEC 攻击呢？因为要实现电子邮件数字签名和加密非常难，不仅有购买邮件证书的金钱成本，而且还有费时费力去配置使用的时间成本和学习成本。目前全球只有零信技术实现了电子邮件数字签名和加密的自动化，用户只需下载安装零信浏览器，设置自己的邮箱账户启用零信邮件加密自动化服务，即可像发送明文邮件一样完全无感地发送加密邮件，并且这个邮件加密服务是完全免费的，非常有利于普及邮件加密应用，以杜绝 BEC 攻击。

也许马上就有人质疑零信技术的动机了，为何这么好的服务会免费提供？是否有其他目的？笔者作为公司创始人也必须在这里把这个问题讲清楚。正如笔者在博文《邮件加密，任重道远》中所讲，采用密码技术实现电子邮件加密是笔者二十年来的不断追求，无论这个过程中遇到了

多大的挫折，笔者始终坚信这个技术方向能彻底解决邮件安全难题，也只有这个方案才能真正彻底解决邮件欺诈这个世纪难题。所以，只要有机会，笔者就一直不忘初心，继续探索邮件加密难题的解决之道。

笔者坚信：现在的基于零信浏览器的邮件加密自动化解决方案能彻底解决以前遇到的各种技术难题，能最终实现笔者一直在追求的普及邮件加密之梦想。至于盈利模式，大家已经看到，零信技术在提供免费服务的同时提供收费服务，免费服务仅自动化验证用户邮箱控制权，未验证用户身份，所以也就无法告知发件人的真实身份，只能收件人自己根据发件人邮件地址判断是否可信了，免费服务只能保证发件人的邮件地址是真实的，只能保证电子邮件内容没有被篡改，只能保证电子邮件内容不会被非法窃取。为了让收件人放心处理您的电子邮件，欢迎选购收费服务，能明确显著地向收件人展示真实可信的发件人姓名和/或单位名称等身份信息，增强在线信任，促成更多在线交易。

笔者既欢迎大家免费使用零信电子邮件加密自动化服务，也非常欢迎选购收费服务，共同为普及电子邮件加密做贡献，共同努力彻底消失邮件欺诈，从而让古老的电子邮件焕发新生机，继续更好地造福人类。

王高华

2024 年 11 月 14 日于深圳

欢迎关注零信技术公众号，实时推送每篇精彩 CEO 博客文章。
已累计发表中文 191 篇(共 54 万 7 千多字)和英文 80 篇(10 万 3 千多单词)。