简译版

邮件平台及安全工具与威胁激烈对抗

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	Email Security Tools Try to Keep Up with Threats		
原文作者	Kelly Sheridan	原文发布日期	2018 年 5 月 9 日
作者简介	Kelly Sheridan 是 Dark Reading 的编辑。https://www.darkreading.com/author-bio.asp?author_id=837		
原文发布单位	Dark Reading		
原文出处	https://www.darkreading.com/endpoint/email-security-tools-try-to-keep-up-with-threats/d/d-id/1331769		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

邮件平台及安全工具与威胁激烈对抗

Kelly Sheridan

2018 年 5 月 9 日

长期以来，电子邮件一直是网络攻击的主要媒介之一，而且黑客只会越来越狡猾。电子邮件平台和安全工具能跟得上吗？

无论企业中充斥着多少即时消息和协作应用，大多数（如果不是全部的话）员工还是会继续使用电子邮件来工作。网络犯罪分子深谙这一点，他们越来越多地利用这种依赖性，寻找新的方法来绕过电子邮件安全保护措施。

Mimecast 公司的网络安全专家鲍勃·亚当斯（Bob Adams）解释了电子邮件威胁是如何演变的。“了解邮件攻击的历史，预测它们的演进方向，这一点很重要。”他说。较老的网络钓鱼诈骗经常出现拼写和语法错误，很容易识别。受害者一旦上钩，很可能就任凭攻击者为所欲为了。

“钓鱼诈骗如此成功的原因之一在于它采用了即使聪明人都不会发现异常的方法。”他说。如今，威胁源拥有充足的资源来创建邮件，使其邮件看起来非常可信，从而欺骗更多的受害者。以前能轻松识别钓鱼邮件伎俩的人，正在成为鱼叉式或者 BEC 邮件攻击的受害者。

在《电子邮件安全风险评估》（ESRA）报告中，Mimecast 收到了 9590 万封邮件，这些邮件通过企业邮件管理平台接收并经过了邮件安全系统过滤，Mimecast 对这些邮件进行了扫描。经过扫描，Mimecast 发现了 1420 万封垃圾邮件（510 万封被退回，910 万封被隔离），近 1 万个危险文件类型，1.25 万个恶意软件附件和 2.3 万起伪装攻击。

垃圾邮件确实令人讨厌，但大多数人都能识别，并不致命。然而，伪装攻击是很狡猾的。“这些攻击更容易、投资回报率更高的原因是，所有公司和个人都被曝光了大量的信息。”Wickr 公司首席执行官约珥·沃仑斯特罗姆（Joel Wallenstrom）表示。

“攻击者需要做的就是挑选一个目标；并根据从 Facebook、LinkedIn、数据中间商以及泄露的个人身份信息（PII）数据库收集到的信息定制一封邮件；然后就可以进行诈骗了。”他补充道。BEC 攻击已经成为一个非常有利可图的行业，FBI 在 2017 年将其归类为一个新的犯罪类型，自此 BEC 攻击创造了高达 50 亿美元的利润。

“我们看到越来越多的鱼叉式钓鱼攻击，攻击者利用各种社会工程手段，欺骗人们提供帐户凭证。”谷歌产品经理蕾娜·纳德卡尔尼（Reena Nadkarni）表示。

亚当斯指出，BEC 攻击依赖于简单性、可信性、受害者心理和紧迫性来说服受害者采取行动。他们不会使用太多的细节：他们不会说“上周三在星巴克见到你很高兴”，而是会说“前些日子和你谈话很高兴”，这样更有可能骗到目标。攻击者可能会利用员工不敢质疑管理人员的心理。“我现在很忙，无法详谈，但我需要你立即这样做”是攻击者可能使用的另一句台词。

在 ESRA 测试中，12500 个恶意软件附件绕过了邮件安全系统，其中有 11653 个包含已知恶意软件，849 个包含未知恶意软件。如果无法检测到邮件中的未知恶意软件，后果可能会非常严重，因为大多数常见的反病毒系统都不会检测到它，这样一来攻击者就可以驻留在网络中或进行横向移动。

邮件安全跟得上吗？

重要的电子邮件提供商微软和谷歌一直在努力为其邮件平台创建更强大的安全性。纳德卡尔尼解释了网络攻击的演变如何给邮件安全带来挑战；现在，攻击者正在伪造网站并创建与正规域名类似的域名。

“有趣的是，这些邮件没有附件，”她说，“许多能够捕获附件的传统方法都行不通。”

谷歌最近添加了一些新的 Gmail 安全功能，作为更广泛的重新设计的一部分。用户可以通过为邮件创建过期日期或撤回发送的邮件（在邮件被查看之前或之后），来保护敏感内容。收件人可能需要提供一些额外信息才能查看邮件，这是一种数据保护措施，即使收件帐户被黑客入侵也无妨。

微软也为其电子邮件平台添加了新的安全功能。但是，一些安全专家指出，在数据安全方面还有很多工作要做。沃仑斯特罗姆说，Gmail 的保密计算是“朝着正确方向迈出的一步”。用户必须知道如何为每封邮件设置过期日期，但这些设置仅限于收件人一端。他指出，发件人应尽量减少关键和敏感信息，这也是一种有用的防护措施。

对于最近的 Gmail 更新，特别是关于企业安全的问题，亚当斯说：“有点迟了，而且在我看来，还有点欠缺。”他说，对小型企业来说，这可能会有好处；但对于大型企业来说，“目前我看不到它的安全性和有效性”。

Safe-T 公司产品副总裁艾坦·布莱姆勒（Eitan Bremler）指出，Exchange 仍然限制发送文件的大小（除非通过 OneDrive 发送），并且没有与数据丢失防护（DLP）和反病毒软件集成。他担心 Gmail 缺乏诸如文件加密、DLP 或反病毒集成等高级安全功能。

“在过去的 20 年中，黑客越来越成熟，并且创造了更巧妙的方法，但是从技术角度来看，电子邮件技术本身并没有太大的发展。”布莱姆勒说。

企业可以做些什么？

为了提高电子邮件的安全性，沃仑斯特罗姆建议企业将安全和数据最小化作为默认设置，“员工在每次通信时不必加入某些信息，”他说。此外，实施禁止通过电子邮件发送有价值的数据（财务信息、商业情报）的企业范围策略也有助于建立安全性。

“令我惊讶的是，即使在今天，大量的管理员帐户仍然没有采取双因子身份验证。”纳德卡尔尼说，“如果你有系统管理员权限，而且该系统被入侵，那么麻烦就大了。”

她还建议企业采用安全钥匙。“这会带来很大的不同，”她解释说，并指出即使是多因子身份验证码也可能会被盗用。“引入物理安全因素，安全性会大大增强。”

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，安天依托下一代威胁检测引擎、主动防御内核等自主先进技术、“赛博超脑”支撑平台和专家团队，为用户提供端点防护、流量监测、快速处置、深度分析等产品，以及安全管理、威胁情报、态势感知和靶场演练等解决方案。

安天为国家主管部门、军队、保密、部委行业等高安全需求部门，提供高级威胁和新兴威胁解决方案和能力体系，产品与服务保障了“载人航天”、“探月工程”、“空间站对接”、“大飞机首飞”等重大国防军工任务。安天也是全球重要的基础安全供应链上的核心节点，全球近百家著名安全厂商、IT 厂商选择安天作为检测能力合作伙伴，安天的检测引擎为全球近十万台网络设备和网络安全设备、超过十亿部智能设备提供安全防护。其中移动检测引擎是全球首个获得 AV-TEST 年度奖项的中国产品。

安天技术实力得到行业管理机构、客户和伙伴的认可，安天已连续五届蝉联国家级安全应急支撑单位资质，亦是中国国家信息安全漏洞库六家首批一级支撑单位之一。安天是中国应急响应体系中重要的企业节点，在红色代码、口令蠕虫、心脏出血、破壳、魔窟等重大安全威胁和病毒疫情方面，提供了先发预警和全面应急支撑。安天针对震网、毒曲、火焰、沙虫、方程式、白象等 APT 组织或 APT 行动，进行了深度的解析，对捍卫国家主权、安全和发展利益形成了有利的支撑。

在 2016 年 4 月 19 日由习近平总书记召开的网络安全和信息化工作座谈会上，安天创始人、首席技术架构师作为网络安全领域的发言代表，向习总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了位于哈尔滨科技创新城的安天公司，对安天负责人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问： *http://www.antiy.com（中文）*

http://www.antiy.net（英文）

安天企业安全公司更多信息请访问： *http://www.antiy.cn*

安天移动安全公司（AVL TEAM）更多信息请访问： *http://www.avlsec.com*