安全

Office 365 网络钓鱼

Ben Nahorney
2019 年 5 月 29 日 - 0 条评论

老实说：管理邮件令人痛苦。路由问题、磁盘配额、退信、用户可以发送但无法接收邮件的情况、可以接收但无法发送的情况，或者竭尽全力也无法发送或接收的情况，不胜枚举。

因此，无怪乎 Office 365 等邮件托管服务大行其道。此类基于云的邮件服务可以消除邮件配置带来的许多麻烦。它们甚至包括基本的安全功能，旨在帮助用户防御最新威胁。

此外，它们还提供简化用户体验的选项。用户可以直接访问 Office 365 网页，输入公司凭证，不受所在位置限制直接登录到自己的邮箱账户。

考虑到以上所有因素，再加上云邮件解决方案通常还能降低成本，它无疑是理想的解决方案。因此，Office 365 等服务的使用量增长迅猛。

已经引起攻击者注意

当然，这种服务的风行也导致其受到恶意攻击。攻击者正在策划并发起针对 Office 365 用户的网络钓鱼活动。攻击者试图窃取用户的登录凭证以达到接管账户的目的。如果得逞，攻击者通常可以登录受感染的账户，并执行各种恶意活动:

- 在内部网络中散播恶意软件、垃圾邮件和网络钓鱼邮件。
- 实施定制攻击，例如鱼叉式网络钓鱼和企业邮件入侵。
- 针对用户的合作伙伴和客户发起攻击。

乍一看，这和基于邮件的外部攻击似乎并无很大区别。但其实这二者之间存在一个重要的不同之处：现在攻击者是从合法账户发送恶意邮件。在收件人看来，发件人甚至往往是他们认识的人，由此获得的信任是未知邮件来源不一定能给予的。让情况变得更加复杂的是，攻击者通常会利用 “会话劫持”，即通过回复已经位于受感染收件箱中的邮件来投放负载。

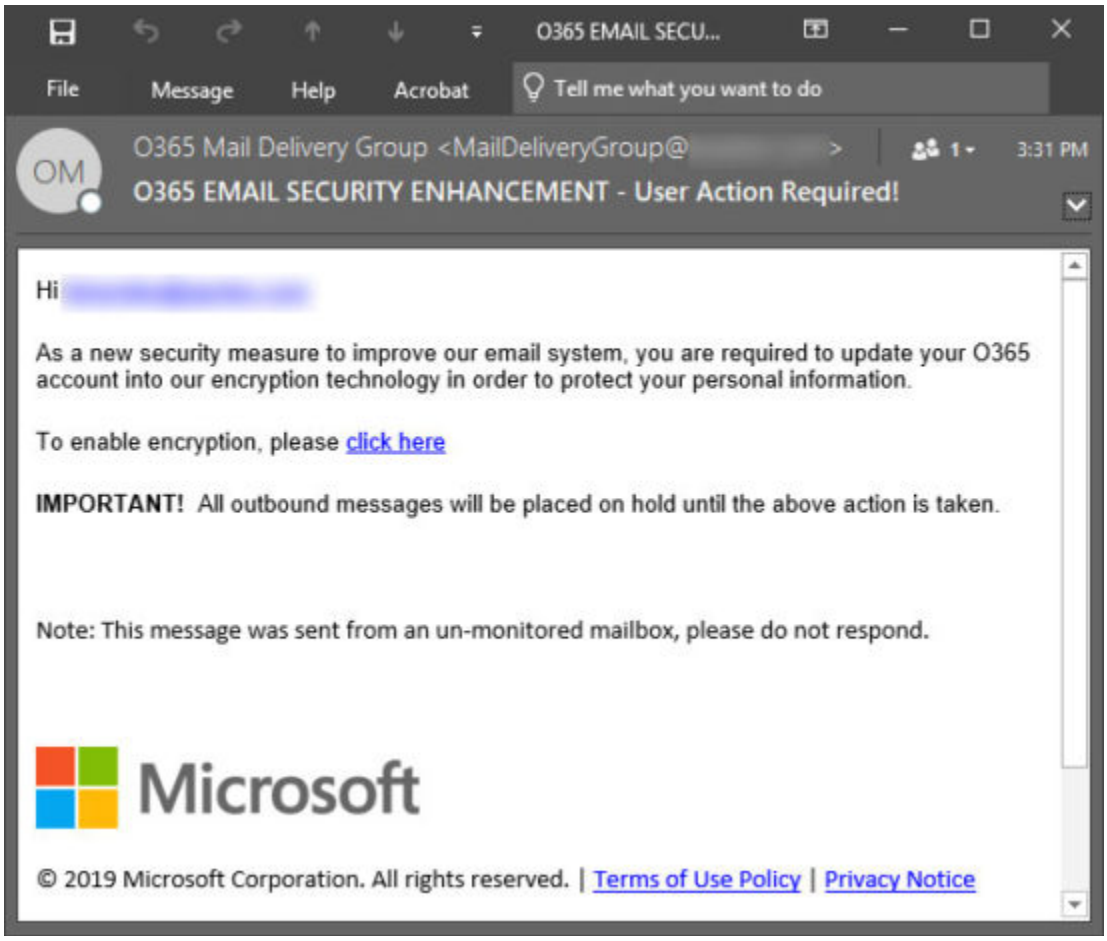


图 1 - Office 365 网络钓鱼邮件示例。

侦察攻击

但是，除了发送邮件之外，攻击者还能执行许多其他活动。一旦攻击者有权访问合法邮箱，他们还可以执行以下操作：

- 获取公司的全局邮件地址列表。
- 扫描邮箱，查找其他凭证、个人信息或公司信息。
- 试图获取对公司资源的进一步访问权限。

这些活动可能会被忽视，因为攻击者只是在使用授权凭证登录时收集信息。这为攻击者提供了侦察的时间：这是观察并计划其他攻击的机会。此类攻击也不会像针对网页邮件客户端的暴力攻击一样引发安全警报。在暴力攻击中，攻击者会不断猜测不同密码，直至登录账户或被发现。

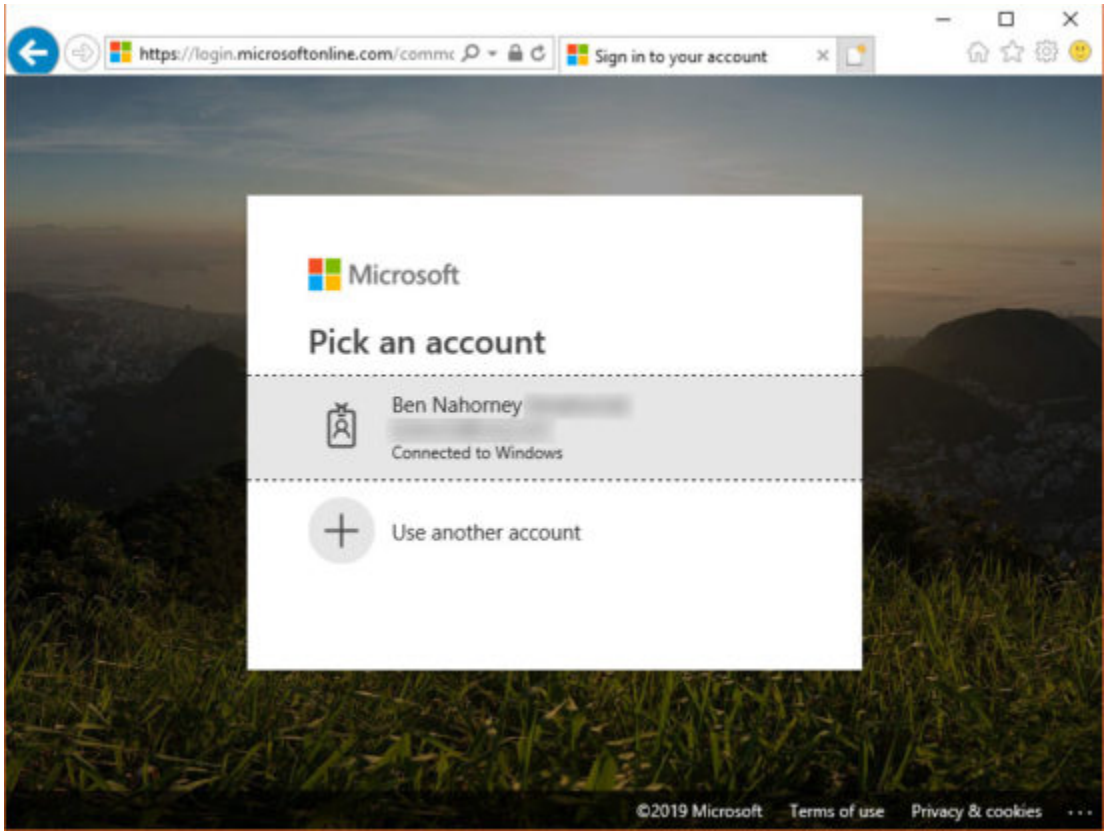
攻击链

攻击者用于获取 Office 365 账户访问权限的方法相当简单。网络钓鱼攻击活动通常采用来自 Microsoft 的邮件的形式。邮件中包含登录要求，声称用户需要重置密码、最近未登录，或账户出现需要他们注意的问题。邮件中还包含一个 URL，诱使读者点击它修复问题。

事件链通常如下所示:

1. 攻击者发送似乎来自 Microsoft 或其他可信来源的网络钓鱼邮件。
2. 用户点击邮件中的链接，被转到模仿 Office 365 登录页面的页面。
3. 用户输入登录凭证，被攻击者获取。
4. 假冒页面不会执行任何活动，只是表示登录不正确，或将用户重定向至真实的 Office 365 登录页面。

哪怕经历了这一系列事件，用户仍然不明白其凭证已被盗。



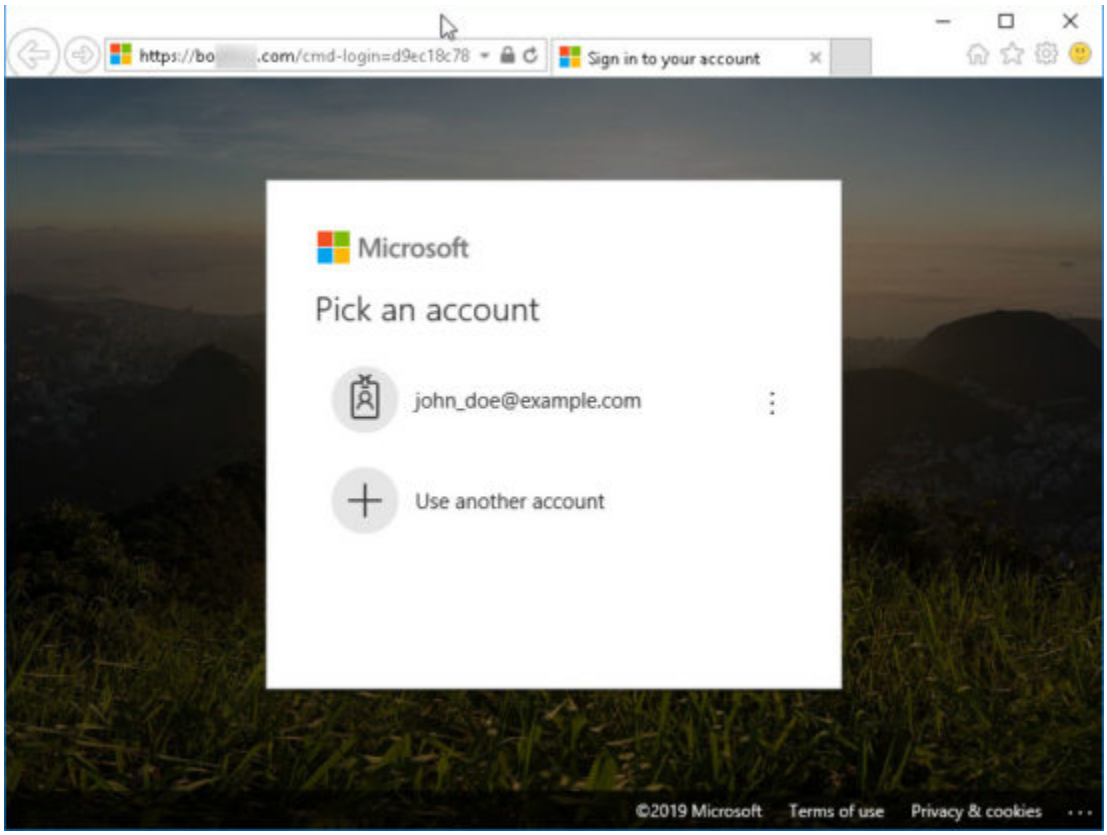


图 2 - Office 365 登录页与网络钓鱼登录页。您能看出区别吗？

攻击频率

这些攻击的成功率如何？虽然除了攻击者之外，其他任何人都不可能会有被盗凭证数量或总成功率的数据，但我们可以通过分析网络钓鱼邮件得出一些结论。

Agari Data Inc. 是一家围绕网络钓鱼攻击活动监控各种数据点的公司。事实上，在其季度邮件欺诈和身份欺骗趋势报告中，他们通常会分析品牌假冒趋势，并为我们提供一些新的数据。

过去几个季度，假冒 Microsoft 的网络钓鱼邮件数量呈稳定增长态势。尽管 Microsoft 长期以来一直是被假冒最多的品牌，但现在它已占到上个季度所有品牌假冒邮件的一半以上。

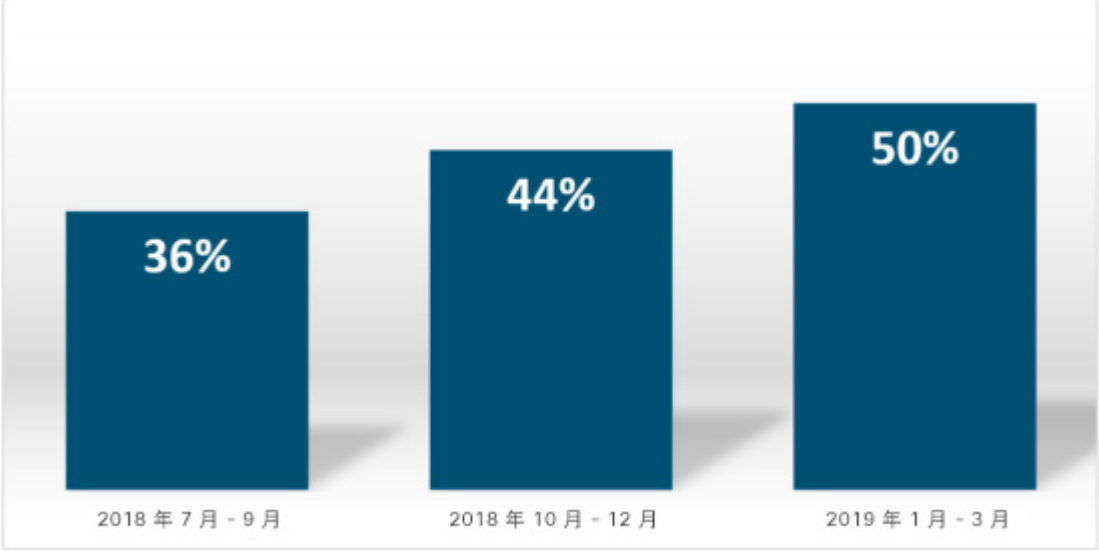


图 3 - 伪装成 “Microsoft” 的品牌假冒网络钓鱼邮件

云邮件安全的功效

值得称道的是，Microsoft 已将多项安全技术加到 Office 365 产品中。但是，考虑到此类网络钓鱼攻击是在其网络外发生，可以在云端采取的防御措施极其有限。如果攻击者获取并使用有效凭证，如何才能根据登录尝试辨别差异？

幸运的是，您可以采取以下措施来进一步保护您的邮件:

- **使用多因素身份验证。**如果登录尝试需要辅助授权后才允许用户访问收件箱，则会阻止许多攻击者，即便使用钓到的凭证也是如此。
- **部署高级反钓鱼技术。**一些机器学习技术可以将本地身份和关系建模与行为分析配合使用，发现基于欺骗的威胁。
- **定期进行网络钓鱼练习。**在整个组织中定期进行强制性的网络钓鱼练习有助于培训员工识别网络钓鱼邮件，使其不会点击恶意 URL 或在恶意网站中输入凭证。例如，Duo 提供一种免费的网络钓鱼模拟工具，名为 Duo Insight。

未来趋势

Office 365 等云邮件服务不会改变方向。鉴于其具备的诸多优势，这些服务也没有理由这样做。事实上，考虑到当前的威胁形势，利用其他安全解决方案往往很有必要。

根据 ESG 代表思科进行的一项近期研究，超过 80% 的受访者称，他们的组织正在使用 SaaS 邮件服务。但是，43% 的受访者仍然发现，在迁移后，他们需要辅助安全技术才能加固邮件防御。

最终，IT 团队仍然需要制定策略、获得可视性与可控性、利用沙盒和外部拦截功能。云邮件解决方案提供了许多优势，但要完全兑现承诺，仍然需要 IT 部门发挥作用，尽可能确保解决方案的安全。

*有意阅读更多有关邮件安全的内容？我们的网络安全报告系列刚刚发布了最新报告：“**邮件：谨慎点击 - 如何防范网络钓鱼、欺诈和其他诈骗**”。下载该报告，深入了解有关邮件诈骗以及如何发现邮件诈骗的详细信息。*

喜欢这篇博客吗？请订阅每月热点威胁博客系列，并在下一篇博客发布时收到提醒。

标签:

- 思科邮件安全
- 邮件安全
- Office 365
- 网络钓鱼
- 每月热点威胁