



中小型企业 面临重大威胁

前言

新闻头条往往关注的是大型企业遭遇网络攻击的事件，但中小型企业 (SMB) 的情况同样不容忽视，他们越来越多地面对与大型企业相同的网络安全风险。当今的许多漏洞利用攻击并不会区别对待中小型企业，因为攻击者关心的只是如何牟利。只要能牟利，他们才不会在意所攻击企业的规模大小。犯罪分子利用各种手法攻击职场人士及其高度依赖的设备，甚至包括应用广泛的智能互联设备。互联网服务提供商有着帮助中小型企业自我防御的独到优势。

这份内容精简的白皮书将探讨给中小型企业造成风险的一些最常见的威胁，以及这些威胁的影响。

由全美小型企业联盟发布的《科技与小型企业调查》报告揭示了一些耐人寻味的统计数据：



当今基于 Web 的威胁可大致划分成两个主要类别：**恶意软件和网络钓鱼**。而**僵尸网络**则是一类需要特别关注的恶意软件。

恶意软件会在用户不知情的情况下安装到设备上。遭遇入侵的网站可利用设备上的软件缺陷加载恶意软件。此外，用户还有可能被诱骗到某恶意网站上并点击下载恶意文件。部分恶意软件可能首先在一台设备上激活，随后自行在网络中传播。有多种不同的恶意软件将企业作为攻击对象：

加密货币挖矿软件会在未经受害者同意的情况下利用设备的处理能力挖矿。这些攻击会入侵 SMB 资源，而且很难检测，因为它们不同于勒索软件，不会向设备所有者索要赎金。

专用恶意软件会加载到销售点设备上，捕捉付款卡数据，并将其上传给恶意攻击者，从而给企业主造成风险。

高级持久威胁 (APT) 会获得网络访问权限，从而搜集并提取高价值数据。APT 经过专门设计，具有极高的隐匿性，因此可以保持较长的有效时间。SMB 丢失的不只有宝贵的数据，更重要的是，可能会失去客户的信任。如果个人数据被暴露，他们也有可能要受到监管处罚。

勒索软件会通过加密设备或服务器上的一切数据，导致文件无法访问。攻击者要求受害者支付高额赎金来换取解密密钥，而且有时在拿到钱后根本不会提供密钥。即便在最好的情况下，中小型企业也要损失一笔高额赎金。在最糟糕的情况下，他们不但损失了赎金，还会**同时**失去对于业务至关重要的数据。

恶意软件通过几种方式搜集高价值数据。**间谍软件**会寻找登录凭据和财务数据这类高价值数据，并将报告发送给犯罪分子。**数据渗漏**恶意软件专门用于在计算机中查找、识别和提取高价值数据。**按键记录器**记录按键操作，经过训练后可让犯罪分子访问金融账号、社交媒体登录凭据以及其他高价值信息。**银行木马**监控用户行为，从而了解登录凭据和/或冒充银行网站来窃取钱财。

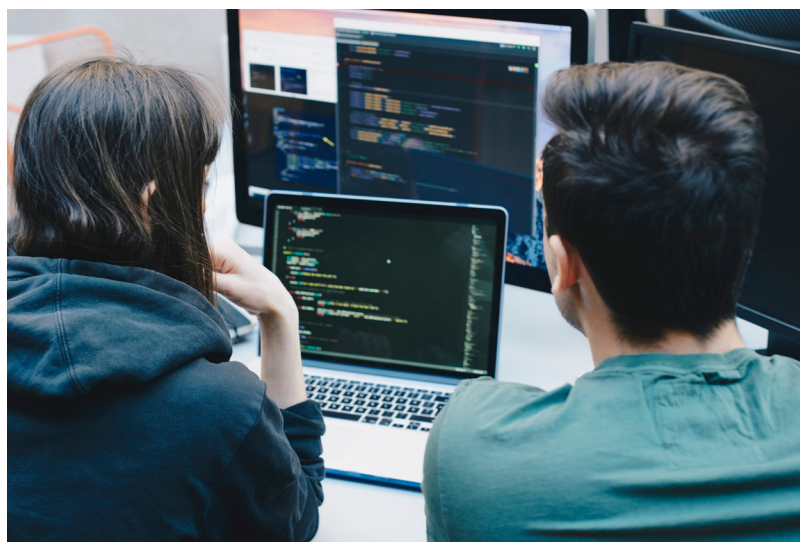
僵尸网络是由符合两个特征的受感染设备组成的网络：感染相同恶意软件；由相同犯罪分子或犯罪集团通过一个集中渠道（称为命令与控制 [C2] 服务器）控制。僵尸网络往往可供租用——大多数都能执行许多不同的功能，比如上述恶意软件的功能，从而谋取不义之财。

网络钓鱼使用以社会工程为主的欺骗手段，诱使受害者透露攻击者可变的信息。过去，网络钓鱼攻击会诱骗用户点击骚扰垃圾邮件中的链接，并透露敏感信息。当今的网络钓鱼攻击开发者采用比以往更加多元的攻击手法，除了垃圾邮件之外，还会在社交媒体帖子或评论以及文字消息、短信、Skype 消息、Messenger 消息或其他服务中整合网络钓鱼 URL。

移动设备是当今网络钓鱼攻击的主要目标，这类设备的屏幕较小，而且用户会一心多用，因此常常会漏掉表明恶意链接的细微线索。更加棘手的是，网络钓鱼者如今会使用来自不同字符集但外观相似的字符，以冒充合法域名。

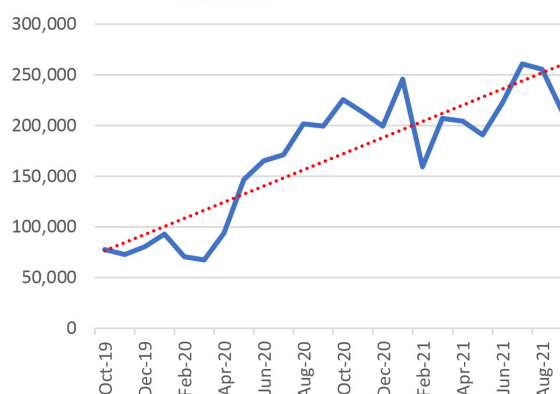
下面这些是使用这类手法的字符串的真实例子：

7elęven.com	rolex.com
Adîdas.com	singaporeair.com
adidâs.com	thaiairways.com
philippineairlines.com	



网络钓鱼近期呈现增长趋势。反网络钓鱼工作组发布的 2021 年第三季度《网络钓鱼活动趋势报告》中透露：“第三季度，我们看到了网络钓鱼攻击月度数量的新纪录；自 2019 年的年底以来，攻击数量翻了一番。”下方图表摘自那份报告，直观地呈现了这种趋势。这是因为与利用软件缺陷相比，哄骗用户采取超出其预期的行动要容易得多。

网络钓鱼攻击，
2019 年第四季度至 2021 年第三季度



由 Akamai 运营商和企业级安全研究团队搜集的数据还表明，网络钓鱼所用域名的使用寿命正在缩短，在 2019 年 3 月，此项指标的中位数已下降到大约 1.5 小时。这对于保护机制有着直接的影响：防御措施必须与攻击同样敏捷。

结论

本文并非网络威胁的详尽列表。攻击者不断评估其漏洞利用手法的可行性，并发挥“创意”来尽可能提高其回报，其攻击的形式与运作方式都在发生变化。还有其他一些恶意软件以滋扰受害者为主，旨在显示用户不需要的广告或内容。

中小型企业需要采用适合其独特需求和约束的解决方案，从而抵御基于 Web 的威胁。Akamai 提供了专为中小型企业打造的 Secure Internet Access。它们可保护中小型企业免受本白皮书所述攻击类型的侵扰，同时不会造成管理负担。工作场所中的每台设备和每个人（包括访客在内）都会自动获得保护。企业管理者可以通过方便易用的图形化门户，即时查看其网络内发生的情况，以及已被阻止的威胁。

Akamai Secure Internet Access 服务专门用于帮助 ISP：

- 为中小型企业提供企业级安全防御解决方案，并借此创收
- 除了服务速度和可靠性之外，还能凭借安全性树立其 SMB 服务的独特优势
- 通过 Secure Internet Access 服务的云端版本，尽可能减少部署障碍、降低成本并简化服务交付

这些服务完全支持品牌定制，可打造与品牌形象契合的外观和使用体验，其功能集和威胁情报也可按照当地市场需求量身定制。

任何用户，任何设备，任何时间，Akamai 为您倾力打造全方位安全防护。
立即联系 Akamai，了解详情。



Akamai 支持并保护网络生活。全球各大优秀公司纷纷选择 Akamai 来打造并提供安全的数字化体验，为数十亿人每天的生活、工作和娱乐提供助力。我们横跨云端和边缘的计算平台在全球广泛分布，不仅能让客户轻松开发和运行应用程序，而且还能让体验更贴近用户，帮助用户远离威胁。如需详细了解 Akamai 的安全、计算及交付解决方案，请访问 akamai.com 和 akamai.com/blog，或者扫描下方二维码，关注我们的微信公众号。发布时间：2022 年 6 月。



扫码关注，获取最新CDN前沿资讯