简译版

保护网络免受勒索软件侵害

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	Protecting the Network from Ransomware		
原文作者	Michael Bose	原文发布日期	2018 年 3 月 29 日
作者简介	Michael Bose 是 NAKIVO 的 VMware 管理员，在虚拟化领域拥有 10 年以上的经验。		
原文发布单位	Networkcomputing		
原文出处	https://www.networkcomputing.com/network-security/protecting-network-ransomware/567521910		
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。		

保护网络免受勒索软件侵害

Michael Bose

2018 年 3 月 29 日

请遵循以下安全最佳实践，防止你的企业沦为勒索软件攻击的受害者。

许多网络管理员认为，勒索软件的主要浪潮已经平息，预计勒索软件攻击的数量将稳步减少。因此，他们放松了保护措施，转而执行更重要的任务。

然而，这种疏忽的态度导致一家韩国公司支付了 100 万美元的赎金，可能还有更多的受害者。如果你想避免这些麻烦，请了解如何保护你的网络免受勒索软件的侵害。至少，请确保按照本清单中的描述进行操作；经验表明，忽视基本安全措施常常导致最可怕的后果。

网络隔离。对不同的部门、虚拟机网络和服务器使用单独的子网。子网可以与网关连接以提高安全性。使用正确配置的网关，即使一台机器或一个子网受到感染，攻击者也很难感染网络的其他部分。广播受到子网大小的限制，不会发送到其他网段，从而减轻攻击（如 ARP 欺骗攻击）的影响。（译者注：ARP，Address Resolution Protocol，地址解析协议，是一个位于 TCP/IP 协议栈中的网络层，负责将某个 IP 地址解析成对应的 MAC 地址。ARP 欺骗攻击就是通过伪造 IP 地址和 MAC 地址实现 ARP 欺骗，能够在网络中产生大量的 ARP 通信流量使网络阻塞，攻击者只要持续不断的发出伪造的 ARP 响应包就能更改目标主机 ARP 缓存中的 IP-MAC 条目，造成网络中断或中间人攻击。）

访问限制策略。在可以避免的情况下，不要提供完整的访问权限。尽可能为用户帐户配置适当的非管理员权限。如果你有任何共享资源，请为不需要写入权限的用户和组提供只读访问权限。只允许在工作中有需要的用户访问服务器或网络。禁用未使用的服务。

网关配置。配置网关的 NAT（网络地址转换）、防火墙和访问规则。关闭未使用的端口，特别是外部网络接口上的端口，只允许访问可信 IP 地址和网络。更改标准端口号可能会减少自动扫描的次数。例如，你可以将 SSH（安全壳）协议使用的 TCP 端口 22 更改为任何其他空闲的 TCP 端口号。

使用端口转发从外部网络访问位于内部网络的主机上的服务。可以根据需要更改网关的外部网络接口上的端口号。例如，你可以将 TCP 8082 端口从网关经由 NAT 路由器转发到局

域网中的主机的 TCP 80 端口（HTTP）。

为 VPN 用户单独分配帐户。

MAC/IP 反欺骗保护。IPv4 网络中存在一个基于 ARP 的漏洞，用于 ARP 欺骗攻击（也称为 ARP 中毒）。通过这种类型的攻击（例如中间人攻击），黑客可以拦截通过网络传输的敏感数据，或将你重定向到恶意站点并感染你的系统。

DNS（域名系统）欺骗也有可能发生。为了防止此类攻击，请在网关上为防火墙配置适当的数据包过滤规则。拒绝来自与发送接口不匹配的网络的数据包。使用支持加密的安全协议，如 HSTS、HTTPS、SSL、TLS、SSH 和 IPsec。（译者注：HSTS 全称是 HTTP Strict Transport Security，是国际互联网工程组织[IETE]正在推行的一种新的 web 安全协议。HSTS 的作用是强制客户端[如浏览器]使用 HTTPS 与服务器创建连接。HTTPS 全称是 Hyper Text Transfer Protocol over Secure Socket Layer，安全套接字层超文本传输协议，是以安全为目标的 HTTP 通道，简单讲是 HTTP 的安全版。HTTP 协议[超文本传输协议]被用于在 web 浏览器和网站服务器之间传递信息。HTTP 协议以明文方式发送内容，不提供任何方式的数据加密，如果攻击者截取了 web 浏览器和网站服务器之间的传输报文，就可以直接读懂其中的信息，因此 HTTP 协议不适合传输一些敏感信息，比如信用卡号、密码等。为了解决 HTTP 协议的这一缺陷，需要使用 HTTPS 协议。为了数据传输的安全，HTTPS 在 HTTP 的基础上加入了 SSL 协议，SSL 依靠证书来验证服务器的身份，并为浏览器和服务器之间的通信加密。）

在防火墙上配置 NAT 与代理服务器。在配置了 NAT 和防火墙的网关上配置代理服务器，以便为你的局域网安全地共享互联网连接。阻止已知是恶意的 IP 地址和网络。防止用户连接他们自己的调制解调器设备（例如电话）在你的局域网内访问互联网。

文件名伪造保护。攻击者可以伪造文件名，将恶意可执行文件伪装成无害的文件。常用的方法是使用诸如 picture.jpg.exe 或 music.mp3.exe（用于 Windows 系统）等文件名。你可以配置文件夹选项并取消选中“查看”部分中的“隐藏已知文件类型的扩展名”复选框。你还可以在代理服务器上使用内容过滤器来禁止下载这些文件。

另一种扩展名伪造的方法是从右到左覆盖（RTLO 或 RLO），该方法使用用于改变 Unicode 文件名写入顺序的特殊双向控制字符。例如，伪造的文件名称显示为 exe.monstrapt.pdf 或 axexe.txt，而原始名称是□fdp.yralpm.exe 和 ax□txt.exe。在这些例子中，方框代表 RTLO 字符。请注意文件名并在 Windows 中配置文件夹选项：视图->详细信息或

查看->内容。请注意，垃圾邮件可能包含具有伪造文件名的附件。

反垃圾邮件和反恶意软件过滤器。在邮件服务器上启用和配置过滤器。如果你没有邮件服务器，请为你的电子邮件客户端安装反垃圾邮件过滤器。使用发件人策略框架（SPF）可以帮助你过滤伪造发件人姓名的电子邮件。

杀毒软件。基于特征的杀毒软件可以识别已知的勒索软件。但是，网络犯罪分子在发布恶意软件之前会进行测试，以确保杀毒软件无法检测到其感染。请查找既支持基于行为的检测又支持基于特征的检测的杀毒软件。

高强度口令和证书。使用至少包含八个字符的高强度口令，包括大小写字母、数字以及特殊符号。尽可能使用基于密钥的身份验证，并为 VPN 和 SSH 连接使用证书。

最重要的是，在防御中要主动，不能被动。

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*