OWASP 中国
The Open Web Application Security Project

反勒索软件指南

Christopher M. Frenz & Christian Diaz 著
肖文棣 译

关于 OWASP

Open Web Application Security Project (OWASP) 是一个 501c3 非盈利性教育慈善机构, 致力于使组织机构能够设计、开发、获取、运营和维护安全的软件。所有 OWASP 的工具、文档、论坛和区域分会都是免费的，并对任何有兴趣提高应用程序安全性的人士开放。我们的网站是：www.owasp.org 。

OWASP 是一个新型组织。我们没有商业压力，使得我们能够提供无偏见、实用、低成本的应用安全信息。

OWASP 不隶属于任何技术公司。和许多开源软件项目一样，OWASP 以一种协作、开放的方式制作了许多不同种类的材料。OWASP 基金会是确保项目长期成功的非营利性组织。

关于 OWASP 中国

OWASP 中国是 OWASP 安全组织在中国区域的分部，是全球 262 个区域分部之一。OWASP 中国成立于 2008 年，在过去 11 年的发展历程中，OWASP 中国已在国内形成了超过 20 个子区域（包括：北京、上海、广东、广西、浙江、江苏、陕西、山西、四川、吉林、辽宁、黑龙江等区域），并吸引了超过 6000 名行业专家成为 OWASP 中国区会员、3 家国内企业成为 OWASP 中国企业会员单位、3 家高等院校成为 OWASP 中国学术支持单位。

中文版说明

本文档基于《OWASP Anti-Ransomware Guide》V2.0 译制完成，对于翻译中存在的错误敬请指正。

如有任何意见或建议，可联系我们。邮箱：project@owasp.org.cn

肖文棣 [译]

OWASP 中国广东分会负责人，现任晨星资讯（深圳）有限公司安全架构师，拥有 17 年的 IT 专业领域经验，在多个安全领域有丰富的经验。曾应邀在多个平台，如 OWASP 峰会、安全加、漏洞盒子等，做 OWASP 项目相关的分享，并参与和领导多个 OWASP 中国项目。

目录

一、概述

打开任何报纸或新闻网站，“医院勒索赎金”正成为一个越来越普遍的标题。虽然医院和其他组织通常都有停机程序，让他们可以重新回到纸面上处理停电和其他灾难，但是由于有人点击了恶意链接或打开了一个可疑的电子邮件附件，就导致整个组织的IT基础架构全部停止运行，这仍然是一个噩梦。此外，许多组织都有大量的遗留系统，而这些系统使安全成为一项挑战，并且在非常基本的安全规定之外，这些组织往往也没有一种高度重视信息安全的企业文化。这使得许多组织在如何处理勒索软件攻击上举步维艰。以下内容旨在作为一个全面的纵深防御检查表和指南，防止勒索软件在您的组织中站稳脚跟，并确保有适当的程序来处理您的环境中的实际勒索软件的爆发。鉴于Windows系统作为勒索软件目标的普遍性，本《指南》面向Windows环境，但其设计与产品无关。请注意，清单的设计是全面的，因此并非所有控制措施都适用于所有环境。

二、边界保护

这是你的第一道防线，因为在威胁进入你的任何系统或员工之前阻止它总是很理想的。

1、防火墙

虽然对于大多数组织来说，外围防火墙可能已经就位，但重要的是要验证你的防火墙是否配置为出口过滤和入口过滤。入口过滤控制允许哪些通信进入组织的网络，而出口过滤控制允许哪些通信离开组织的网络。出入口访问控制都应该基于最小权限原则。应阻止不需要访问外部信息源和系统的系统与外部实体通信。一个无法访问任何外部实体的系统比一个连接互联网的系统更不可能成为恶意软件的入口。此外，如果发生勒索软件感染，如果适当的出口过滤到位，它将无法回调它预置的地址。另外还应为防火墙打开日志记录，因为记录到已知恶意IP地址的重复访问尝试可以作为问题的指示器。组织可能还想考虑在其防火墙中阻止勒索软件跟踪程序域阻止列表中包含的域 - https://ransomwaretracker.abuse.ch/downloads/RW_DOMBL.txt

2、代理服务器/Web 过滤器

如上所述，在可行的情况下，完全切断系统与互联网的连接是一个很好的防御措施，但现实情况是，在所有系统上完全阻断互联网是不可行的，并且会阻碍业务运营。应将连接到Internet的系统配置为通过允许过滤Web内容的代理服务器，并使用防火墙规则来确保代理Web访问是http和https连接的唯一出口方式。尽管对Web访问采用白名单方式最为理想，但组织至少应使用其过滤设备来阻止其对已知恶意网站、垃圾邮件/钓鱼网站、代理规避网站、色情网站和所有其他被认为对正常业务运营不必要的网站的访问。在可行的情况下，还建议屏蔽供应商尚未分类的任何网站，因为与新的有效商业网站相比，此类网站更可能是恶意的。虽然它在许多组织中可能在政治上不受欢迎，但强烈建议在这

一级别阻止访问个人电子邮件、文件共享网站、社交媒体、即时消息和广告网络。文件共享网站、社交媒体等的特殊豁免可根据需要添加。还应禁止将可执行文件（例如.exe、.scr等）下载到端点。许多代理服务器/Web过滤设备还能够使用AV引擎扫描传入的Web内容。如果支持这一点，建议将其打开，并在可行的情况下，使用不同于内部使用的AV引擎，以增加发现相对新的威胁的可能性。应定期更新Web筛选器，以确保恶意网站和其他网站的分类始终是最新的。

除了上述块之外，建议完全阻止来自Spamhaus（https://www.Spamhaus.org/statistics/tlds/）和BlueCoat（http://www.tripwire.com/state-of-security/security-data-protection/cyber-security/most-suspicious-tlds-revealed-by-blue-coat-systems）的到以下顶级域的Web流量。建议这些TLD上托管的大多数站点在性质上是可疑的：

顶级域名		
.accountant	.gq	.stream
.biz	.kim	.tk
.click	.link	.top
.country	.party	.trade
.cricket	.review	.win
.download	.review	.work
.gdn	.science	.zip

组织可能还希望考虑在其Web筛选设备中阻止勒索软件追踪器URL阻止列表中包含的URL-https://ransomwaretracker.abuse.ch/downloads/RW-URLBL.txt

3、SPAM 过滤器

作为外围防御，我们讨论垃圾邮件过滤器，这些过滤器在邮件到达公司邮件服务器之前过滤邮件，或者如果您使用的是托管邮件，请确保由托管提供商提供的垃圾邮件过滤器已打开。最好在边界屏蔽已知的垃圾邮件、包含恶意链接的邮件和包含恶意附件的邮件，以便让其他内部防御层处理它。还建议阻止任何包含.exe或.vbs文件等可执行附件的邮件。对于没有任何国际业务的机构，最好屏蔽来自公司所在区域以外地区的所有电子邮件，并将任何必要的例外情况列入白名单。与Web过滤软件一样，垃圾邮件过滤器应始终保持最新，以确保它们具有最新的阻止列表，并且其AV引擎具有用于分析附件的最新签名。在可行的情况下，垃圾邮件过滤器中使用的AV引擎应与访问电子邮件的端点上使用的AV引擎不同。

4、VPN/远程访问

SamSam勒索软件通常被报告为通过尝试使用安全性差的面向公众的RDP服务远程连接到组织内部进行传播。建议各组织将远程访问限制为只访问必需的帐户，并制定帐户锁定策略，以帮助防止访问凭据的暴力破解。远程访问还应在可行的情况下使用双因素身份验证，以减轻丢失或被盗的访问凭据可能造成的损害。

5、沙盒

许多外围设备，如下一代防火墙（NGFWs）和垃圾邮件过滤器，现在能够与恶意软件沙盒集成，当用户试图访问它们时，这些沙盒将允许在受监控的虚拟机上执行未知文件和url。这是发现新的恶意软件变体的一个很好的方法，而基于签名的防御可能不会被认为这些变体是恶意的。

三、网络防御

可部署在局域网上的防御措施，以帮助检测和减轻恶意软件的爆发。

.

1、DNS 沉洞

虽然与恶意站点的连接在理想情况下在外围被阻止，但是可以通过创建DNS 沉洞来添加一层额外的防御，当DNS请求进入某个沉洞中的某个域时，该沉洞将通过发出错误信息来阻止与某些域的连接。与周界防御一样，防止任何系统或人员访问恶意内容总是比在下载到端点或由端点访问时减轻恶意内容要好得多。理想情况下，您的沉洞域列表将来自不同的来源，而不是用于您的网络过滤器，以确保更全面的恶意域的覆盖范围。有关在Windows DNS服务器上创建DNS沉洞的教程，请访问：

https://cyber-defence.sans.org/blog/2010/08/31/Windows-DNS-server-blackhole-blacklist

2、网络分段

通过VLAN和控制VLAN之间流量的ACL进行网络分段将无法防止勒索软件攻击访问您的系统，但如果恶意软件感染能够在您的组织内站稳脚跟，这将是非常宝贵的。网络分段有助于确保恶意软件感染或其他安全问题仅与受感染端点所在的网段隔离，并且不会在整个组织中传播。对于维护不再能够接收安全更新的遗留系统的组织来说，这一点尤为重要。只要可行，就应尽可能细化网络分段，以确保仅允许在网络上进行必要的通信，并且默认情况下阻止所有其他通信。对网络安全采取零信任的方法将极大地减少在您的环境中发生横向移动的可能性，从而大大减少恶意软件和其他威胁的传播。

3、虚拟机分段

正如上面讨论的网络分段是确保恶意软件感染可以传播到的系统数量最小化的关键，记住许多虚拟机通信是在服务器的后平面上进行的，而不是像交换机那样横穿标准网络设备，这一点很重要。对于高度虚拟化的环境，建议部署虚拟机分段技术，如VMware的NSX或Microsoft的HNV，以确保虚拟机通信可以通过与物理系统等效的网络安全机制进行控制。与物理网络分段一样，对网络安全采取零信任的方法，即只允许必要的通信，这是应该争取的理想做法。

4、网络入侵检测系统 (NIDS)

拥有NIDS可能不是防止恶意软件访问您的系统的一个非常有效的方法，因为大多数NIDS都更倾向于检测攻击企图而不是恶意软件，但是当恶意软件与恶意IP地址，如僵尸网络的指挥控制中心和勒索软件工具的密钥生成站点，进行尝试通信时，NIDS系统可以警告潜在的风险爆发。IT和安全工作人员越早收到恶意软件爆发的警报，成功控制事件的可能性就越大，这是一种可以利用的检测手段。根据部署情况，NIDS系统还可以帮助确定组织内试图感染其他系统的系统。

四、终端保护

桌面PC和其他用户界面系统上的保护。

1、完全修补和更新

勒索软件和其他恶意软件通常使用各种漏洞攻击来在系统上站稳脚跟，确保操作系统和系统上的所有应用程序都得到了完全修补和更新，这将是最大限度地减少端点被成功利用的方式。针对勒索软件，保持您的电子邮件客户端，浏览器，和Flash完全更新是至关重要的。组织应该有健全的程序来确保正确的补丁管理和软件的日常补丁。

2、不安装不必要的应用程序和服务

如果系统上不存在应用程序，则无法利用该应用程序，因此确保端点配置也遵循最小权限原则是减少端点攻击面的有效方法。特别建议不要在不需要Java和Flash的计算机上运行Java和Flash。

3、无管理权限

管理权限应仅用于管理任务，并且不应使用具有管理权限的帐户执行正常的计算机操作。这将阻止许多类型的恶意软件获得立足点，因为他们的用户帐户可能根本没有“安装”恶意软件的适当权限。

4、防病毒软件(AV)

应在所有端点上运行防病毒软件，并将其配置为在访问时扫描文件和其他资源。防病毒软件应保持最新，并应配置警报以通知IT人员任何可能的感染。重要的是要记住，AV在很大程度上是基于签名的，因此，只能有效地检测已知的威胁。AV可能无法提供任何针对新病毒或新恶意软件变体的保护。理想情况下，这些病毒是来自一个不同的供应商，而不是一个用于扫描周边防御级别的病毒。

5、下一代防病毒软件

下一代反病毒解决方案，具有签名较少的性质，因此有可能检测零日攻击和新的恶意软件变体。下一代AV使用行为检测、机器学习和基于云的文件执行等方法来尝试识别攻击企图和恶意软件。一些下一代AV软件包在PCI-DSS下被认证为AV替代品，但并非所有都是。在许多情况下，它们可以作为对传统AV的潜在补充。

6、基于主机的入侵检测/防御系统 (HIDS/HIPS)

这些系统可以是独立的，也可以集成到AV供应商提供的端点保护解决方案中。它们用于检测关键系统文件的可疑更改、潜在的缓冲区溢出以及端点上的其他潜在可疑活动。它们可能有助于对可能爆发的疫情提供早期洞察，有些则在缓解某些攻击企图方面能力有限。

7、Web 过滤器

许多端点防护软件包提供了一种过滤恶意Web内容的附加方法，而且最好也打开这些过滤器，特别是在遵循对内部系统和外围环境使用不同供应商的推荐做法时。这将增加恶意Web内容在系统或用户能够访问之前被阻止的可能性。

8、SPAM 过滤

与Web过滤一样，垃圾邮件过滤也可以在端点级别进行，在端点上设置不同的过滤解决方案有助于增加检测到绕过外围防御的垃圾邮件和恶意电子邮件的可能性。这一点至关重要，因为像Locky这样的勒索软件变体通常通过恶意电子邮件附件传播。

9、禁止对宏的支持

宏和其他可执行内容可以嵌入到office应用程序和PDF文件中使用的文档中。很可能您组织中的大多数用户没有合法的此类功能需求，默认情况下应关闭对此类功能的支持。

10、软件限制策略/应用程序锁

可以将GPO策略设置为将某些正在运行的应用程序列入黑名单，并将某些正在运行的应用程序列入黑名单，例如用户配置文件的AppData文件夹，该文件夹是常见的恶意软件目标。组织可以制定自己的策略或使用第三层等组织提供的反勒索软件策略。作为GPO黑名单的替代方案，免费的CryptoPrevent实用程序还可以用于将软件限制策略部署到端点。这样的政策是对

AV软件的一种有效补充，因为它们不是基于签名的，并且可能会阻止事件新的恶意软件变种成功运行。只需确保测试任何此类策略，以确保它们不会干扰在您的环境中使用的任何合法应用程序。一个比黑名单更好的方法是应用程序白名单方法，但这是一个更具

挑战性和耗时的项目，以确保在只允许运行白名单应用程序的情况下不会损坏任何关键应用程序。

11、Hosts 文件

在DNS之前检查Hosts文件以解析IP地址，并且可以使用类似于DNS沉洞的方式来防止恶意域被正确解析。除了其他Web过滤机制外，这还可以为潜在连接到恶意站点的用户或系统提供另一层防御。

12、禁用 USB 访问

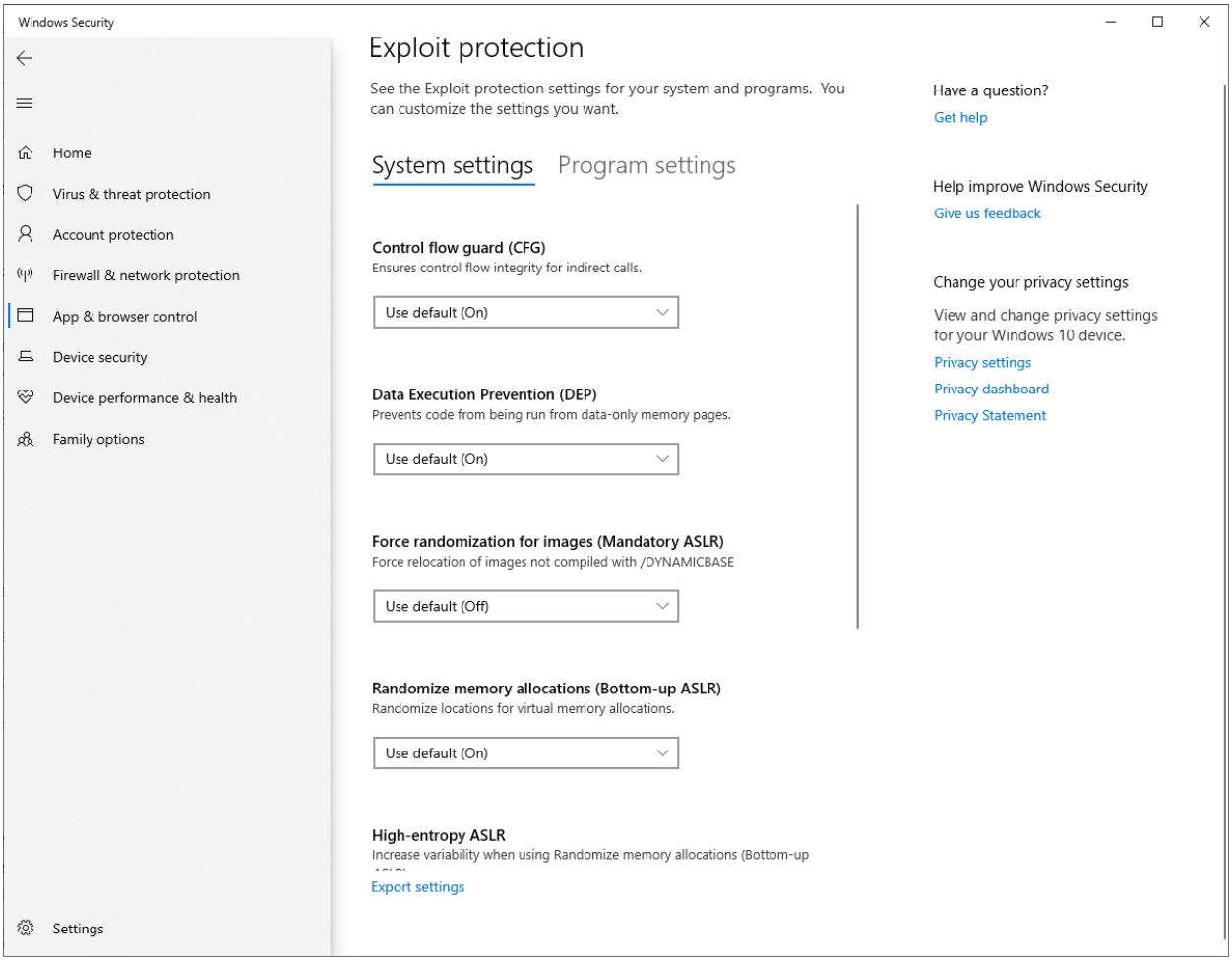
虽然不像基于Web和电子邮件的传输载体那样常见，但已经有了通过USB驱动器传播的CryptoLocker勒索软件的变体。在可行的情况下，应阻止USB驱动器访问。

13、虚拟桌面基础架构

如果组织的端点是虚拟化的，则恶意软件防御的另一个选项是确保所有VDI桌面都是非持久性的，并且系统在每次会话后都恢复到预定义的状态。这将确保在用户会话结束后消除感染VDI桌面的任何恶意软件，并且系统恢复将使桌面恢复到“类似新”的感染前状态。

14、Exploit Protection

微软以前以EMET的形式提供了Exploit Protection功能，但在Windows安全中心的App&browser控制部分将这些功能集成到了Windows 10中。虽然组织可能希望首先进行测试，以确保运行这些保护时不存在与应用程序兼容性相关的问题，但理想情况下应该启用这些保护。对于那些寻求额外Exploit Protection的用户，许多端点安全产品现在也具有Exploit Protection功能。



15、本地管理员密码解决方案

虽然作者不知道使用pass-the-hash技术传播到其他系统的任何已知勒索软件变体，但这是许多windows环境中常见的可利用漏洞，因为每台计算机的本地管理密码在所有系统中都很常见。LAPS将系统的本地管理密码随机化，并将密码存储在活动目录中。它还允许设置访问控制，以控制谁可以查找这些广告存储的本地管理密码。因此，LAPS使得攻击者和潜在的蠕虫类恶意软件更难在被破坏的组织中横向移动。有关LAPS的更多信息，请访问-https://www.microsoft.com/en-us/download/details.aspx?id=46899

16、应用程序沙箱

应用程序沙箱是一种隔离应用程序的方法，这样它们只能访问一组严格控制的资源，如内存和磁盘空间。通常，沙盒应用程序被阻止永久提交对磁盘的任何更改。因此，沙箱应用程序（如web浏览器及其各自的插件）可以帮助防止某些形式的勒索软件影响您的系统，因为沙箱有可能阻止勒索软件访问硬盘或网络共享上的文件。

17、禁用 SMBv1

许多勒索软件变体（包括WannaCry）利用SMBv1协议中的漏洞进行攻击。现代版本的windows能够使用较新的SMBv2和/或SMBv3协议，在许多情况下，可以在您的环境中安全地禁用SMBv1。如果在SMBv1协议中发现其他安全漏洞并将其禁用，则可以提供针对未来勒索软件攻击的主动安全防御。Microsoft在

https://blogs.technet.Microsoft.com/staysafe/2017/05/17/disable-smb-v1-in-managed-environments-with-ad-group-policy/上提供了禁用SMBv1的指南。请确保在应用域范围之前对此进行彻底测试，因为旧版本的Windows和其他旧设备可能需要SMBv1才能正常工作。

18、受控文件夹访问

Windows 10中引入的一项新功能将阻止未经授权的应用程序对受保护文件夹的内容进行任何更改。

https://blogs.windows.com/windowsexperience/2017/06/28/announcing-windows-10-insider-preview-build-16232-pc-build-15228-mobile

19、重命名 vssadmin.exe

卷影副本通常在Windows中用于创建以前版本文件的快照，vssadmin.exe是用于管理这些卷影副本的实用程序。许多勒索软件变体也使用相同的实用程序删除所有卷影副本，并使恢复文件更加困难。有关重命名vssadmin的教程，请访问 https://www.bleepingcomputer.com/news/security/why-everyone-should-disable-vssadmin-exe-now/.

20、PayBreak

一个有趣的研究项目，通过记录勒索软件用来加密每个文件的加密密钥，有可能逆转勒索软件攻击的影响。有关研究开发的技术和工具可在下面链接找到 https://eugenekolo.com/static/paybreak.pdf.

五、NAS 服务器

大多数组织都拥有托管在某种形式的NAS设备上的共享驱动器，这些设备可能具有受勒索软件影响的共享。下面列出的保护机制是对终端保护下描述的所有保护机制（如完全修补、AV等）的补充。

1、文件权限

信息安全的一个共同原则是最小权限原则，即个人只能获得其工作所需的信息，而不能再获得更多信息。不幸的是，在网络共享驱动器方面，随着时间的推移，许多组织在授权蔓延的情况并不少见。当员工被调到一个新的部门或以其他方式改变组织中的角色时，并不总是能得到适当的通知。这通常会导致为新角色添加权限，但不再需要保留旧角色的权限。虽然删除不必要的访问权限通常是一种良好的安全做法，但考虑到勒索软件攻击的激增，现在是组织审核所有文件共享上的访问权限并确保实施最低权限的非常恰当的时间。如果用户一开始没有访问文件的权限，恶意软件感染对文件进行加密将非常困难。因

此，虽然此控件可能无助于防止勒索软件攻击，但它可以在很大程度上减轻对组织中数据的影响

2、卷影副本

虽然一些较新的勒索软件变体具有某种能力，可以防止数据从卷影副本恢复，但在许多情况下，使用数据的时间点快照可以提供一种快速恢复数据的方法。Windows支持拍摄存储数据的时间点快照，并支持回滚到文件的以前时间点版本。

3、虚拟机快照

服务器基础设施的虚拟化非常常见，通过定期拍摄虚拟机快照（允许您将虚拟机状态回滚到以前的时间点）也可以防止勒索软件。这可以在勒索软件攻击命中时提供备用恢复选项。

4、数据清单

拥有一个数据清单，它可以列出每个共享中存在的数据类型，这非常有益，因为它可以帮助您划分恢复和补救的优先级。此外，威胁dox受害者的恶意软件也在出现。清楚地知道哪些数据被加密或受到恶意软件的其他影响，将有助于组织更好地评估Doxing的威胁。

六、SIEM 和日志管理

防火墙、服务器、IDS设备、Web过滤器、端点等都会生成日志数据，这些数据可能提供恶意软件爆发的线索。拥有一个SIEM解决方案监视和处理这些日志可能有助于提供可能的恶意软件爆发的早期指示，因此可能有助于提高响应时间。如果以后需要进行根本原因分析，集中收集这些数据也可能有助于对其进行分析。

七、备份

如果发生攻击，从勒索软件攻击中恢复需要有适当的备份和恢复计划。

1、备份和恢复计划

组织应该为每个资产定义一个明确的恢复点和恢复时间目标，这将有助于他们为其特定环境确定适当的备份技术和过程。应制定明确的政策和程序，以描述备份计划、数据应如何备份或恢复、谁负责备份和恢复等。在这方面对员工进行交叉培训也是值得的。

2、存储快照

在大多数大型环境中，服务器存储通常位于SAN上，大多数现代SAN设备允许您保留存储卷的一个或多个快照。应配置存储快照，以便在必要时可以将卷回滚到爆发前快照的先前状态。快照的频率应根据组织预定的恢复点和恢复时间目标来确定。

3、脱机备份

虽然SAN或数据中心之间的实时复制等技术对于业务连续性非常有用，但它们在从勒索软件攻击中恢复时用处不大，因为加密版本的文件也将快速复制到其他位置。为了在勒索软件事件后成功地从备份中还原数据，备份应以Pull Only方式进行并脱机存储，以确保备份数据不会加密和不可恢复。虽然没有许多新的基于磁盘的备份系统那么性感，但磁带仍然可以作为理想的备份介质，用于存储环境中数据的多个历史时间点快照。备份频率应根据组织预先确定的恢复点和恢复时间目标来确定。

4、备份和恢复测试

灾难恢复计划经常被搁置，直到灾难真正发生，这可能是一个大错误。备份和恢复应按常规计划进行成功测试，以确保所有系统正常工作，并确保工作人员具有足够的知识来实际操作系统。您不想等到勒索软件攻击或其他灾难发生后才发现关键服务器没有正确备份。如果灾难真的发生，例行测试也会缩短恢复时间。

八、安全意识培训

尽管有许多保护机制，但现实情况是，恶意电子邮件或恶意链接，以通过并发现自己呈现给用户。在这种情况下，尽管AV、软件限制策略和其他端点防御措施仍然可以保护您，但最好的防御措施是受过良好教育的用户，能够识别可疑电子邮件并及时将其报告给IT部门进行调查。这种可疑的通信越早被报告，它们就越快可以被封锁在周边地区，联系AV公司以创建签名，并部署其他防御措施以帮助阻止威胁在整个组织中的扩散。

九、物联网恶意软件

像Mirai和Brickerbot这样的物联网恶意软件说明了物联网设备与任何其他支持网络的计算设备一样可能受到危害。以下控件不是物联网安全控件的综合列表，而是最有可能帮助预防、缓解和补救勒索软件攻击的安全控件列表。本节仅介绍适用于物联网设备本身的控件。网络控制等，如网络分割，对物联网的正确安全至关重要，但在其他章节中也有介绍。

1、不使用默认凭据

迄今为止，物联网设备最常见的危害因素是使用默认凭据，例如在Mirai的案例中，62个用户名和密码对的列表用于危害数十万个设备。简单地说，改变你的物联网设备的默认密码将有助于防止当前许多针对物联网设备的恶意软件变体。

2、账户锁定

考虑到使用密码猜测攻击的物联网恶意软件的普遍性，尽可能配置帐户锁定策略可以帮助阻止许多物联网恶意软件变体。尝试3次或3次以上失败后，应限制访问。

3、固件的备用副本

如果一个设备被感染，拥有设备固件的备用副本或将设备重置为类似新状态的方法对于将设备恢复到功能状态至关重要。

4、备份配置

与上述控件相关，备份所有自定义配置和设置对于快速将设备恢复到功能状态至关重要。

5、受限管理界面

管理接口应尽可能与任何面向Internet的接口分离，并将管理接口放置在一个独立的网段上。在可行的情况下，管理员访问权限应限制在管理界面上。

6、更新机制

所有物联网设备应配置为定期接收更新，并确保设备始终运行可用的最新固件版本。

十、漏洞管理

所有组织都应实施一个全面的漏洞管理计划，该计划旨在识别所有未完全修补且不符合组织定义的安全策略的信息系统（端点、服务器、物联网等）。该计划应包括在有限时间内执行纠正措施的规定，目的是随着时间的推移减少组织的攻击面。脆弱性管理计划应包括持续监测的规定，以便在出现脆弱性时能够识别和缓解。

十一、威胁获取

1、威胁情报

订阅一个或多个威胁情报可能有助于您及时访问IOC和其他信息，以防当前正在进行的攻击，并且您的防御可能还没有更新的签名集或阻止列表来阻止这些攻击。威胁情报还提供了一种很好的方法，可以在威胁出现时主动阻止和/或搜索威胁，从而采取更主动的姿态来保护组织的安全。

2、IOC

在确定系统是否暴露于恶意软件或受到恶意软件的影响时，折衷指标可能很有用。有关各种勒索软件变体的危害指标的详细信息，请访问：

https://www.cyber.nj.gov/threat-profiles/ransomware#LIST-OF-KNOWN-RANSOMWARE

3、EDR

许多端点保护包现在都包括EDR功能，它允许详细查看组织内所有端点上运行的所有进程。EDR功能提供了一种基于可疑行为、IOC和环境知识进行威胁搜索的好方法。如果以后需要事故响应，EDR功能还可以帮助取证工作。

十二、事件响应

尽管希望上述所有防御措施都能将事件降至最低，但组织需要做好准备，以应对这样一个现实：无论控制措施如何到位，勒索软件事件总是有可能发生的。

1、事件响应计划

一个组织能做的最糟糕的事情之一就是等到一个事件发生后才开始考虑如何处理它。组织应该有一个明确的计划，定义他们将如何应对一个事件，以及谁将负责在检测、遏

制、根除和恢复阶段采取什么行动。同样重要的是，所有工作人员都了解该计划，并接受适当和有效的应对培训。对于没有任何事故响应计划的组织，一个好的开始资源是：https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

2、事件模拟

当事件发生时，减轻损害的最佳方法是检测并控制事故尽快。最好的方法是定期测试事件响应计划，以查看组织内的人员如何响应模拟事件。虽然有许多模拟事件可以执行，但一些建议的启动事件将包括针对员工的网络钓鱼活动和模拟恶意软件爆发，可以安全地使用EICAR测试字符串。有关进行模拟恶意软件爆发的指南，请访问：http://www.aehis.org/download/17368/

3、数据恢复

如果灾难来临，最好能够从意外备份中恢复数据和应用程序，而不是通过解密，因为这将更好地帮助确保系统的清洁，但这可能不总是可能的。如果你发现自己是勒索软件的牺牲品，并且没有备份就被卡住了，你可以去nomoreransom.org（https://www.nomoreransom.org/en/index.html）网站看看，该网站提供了基于上传样本文件的勒索软件方差检测，并且还托管了任何变体的解密密钥。另一个著名的勒索软件解密网站isID勒索软件（https://id ransomware.malwarehunterteam.com/）。

4、保险

越来越多的公司正通过采取保险措施防止数据泄露，将部分网络风险转移给保险公司。一些保险公司现在在政策范围内提供特别处理勒索软件攻击的政策或规定。目标明确的行业中的公司可能会考虑制定涵盖此类攻击的政策或确定其现有政策是否涵盖勒索软件攻击。

致谢

感谢Adrian Sanabria 提供人们对 PayBreak的认识。