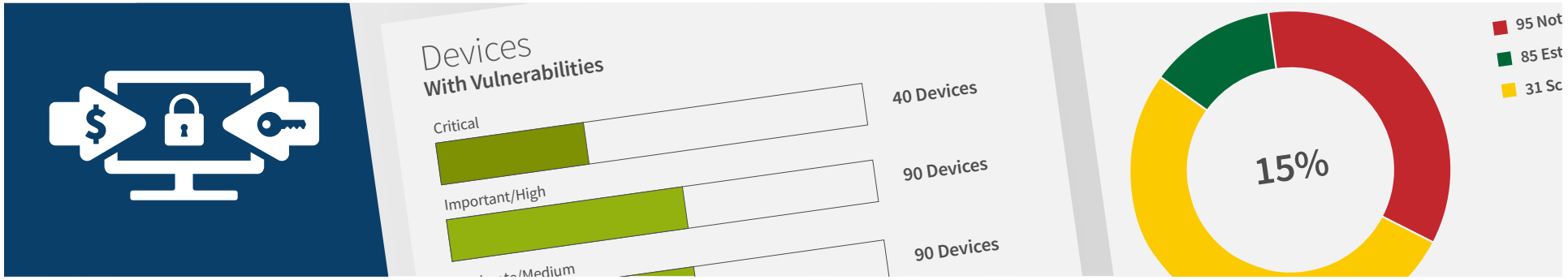
ivanti

防范勒索软件的九大措施



白皮书

目录

简介

“只要交赎款就好了。”某 FBI 官员在 2015 年波士顿网络安全峰会上如是说。[1]不过，此后 FBI 又发表了官方文件提醒人们防范勒索软件，并提供了一系列应对勒索软件的最佳实践。对，新公布的文件还特别指出，“FBI 不建议向勒索者缴纳赎金。”

现在我们知道，大多数勒索软件是通过网络钓鱼或垃圾邮件传播。近期，美国众议院的用户成为勒索软件的受害者，报道称勒索者的目的是欺骗用户打开其雅虎电子邮箱中收到的邮件附件。[2]

加强对终端用户的教育和提高其防范意识的确是一种不错的做法，但重点是要知道，“邪恶的勒索者”非常专业。他们利用多种专业的市场营销和社交工程工具，提高用户打开欺诈邮件和附件的概率。因此，您应假定，即便是受过良好教育且具备防范意识的用户也有可能被骗。事实上，最新的 Verizon 数据泄露报告发现，23% 的网络钓鱼电子邮件收件人会打开邮件，11% 的收件人会点击欺诈附件。[3]可见您也完全有可能这样做。

本 Ivanti 白皮书回顾 FBI 提出的防范建议，并为您介绍实施这些建议应采取的九大措施。

防范措施

“检测并响应”模式对勒索软件的作用不大，因为一旦勒索软件开始运行，一切就都为时已晚。因此，主动防范对于应对此类恶意软件至关重要。FBI 建议您采取以下九条防范措施或方法，我们将在下文中一一为您详细介绍：

1. 为关键操作系统和应用安装补丁
2. 确保杀毒软件更新至最新版本，并已计划定期扫描
3. 管理特权帐户的使用
4. 实施以数据为重点的访问控制
5. 制定、实施并执行软件规则
6. 禁用来自 Microsoft Office 文件的宏指令
7. 实施应用白名单
8. 将用户限定在虚拟化或集装化的环境中
9. 经常备份关键文件

1 为关键操作系统和应用安装补丁

对大多数企业来说，补丁应是防范各类攻击的第一道或第二道防线。这同样适用于勒索软件。

安装补丁
应作为
第一道防线。

切勿成为

已被发现的勒索软件的

受害者

一个月前，Locky 和 Cerber 勒索软件利用 Adobe Flash 的漏洞向受侵害的工作站传播。[4]您可以通过确保操作系统和各客户端系统所需的第三方应用更新至最新版本来防范此类攻击。您还应着重确保及时为 Adobe Flash、Java、Web 浏览器和 Microsoft Office 等应用安装所有最新的关键补丁和更新。此外，您应根据业务需要和政策优先安装补丁和更新，并且在执行这些安装时不应干扰用户或业务运营。

许多企业担心全面、及时且一致的补丁安装和维护过于复杂，或者可能会中断关键的业务应用。但使用最新的补丁管理工具扫描缺失的补丁并为工作站或服务器安装这些补丁非常容易——即便是在最为复杂的环境下也不例外。

Ivanti 在交付完整、灵活的端到端补丁管理解决方案方面拥有丰富的经验。我们的专家可以演示如何有效利用 Ivanti 解决方案使补丁管理自动化——并在尽量不干扰业务或用户的情况下安装关键补丁。

2 确保杀毒软件更新至最新版本，并已计划定期扫描

如果安装补丁是您的第一道防线，那么杀毒软件 (AV) 应紧随其后。安全研究员发现，基于签名的传统杀毒解决方案无法阻止大多数勒索软件的攻击。但您一定不希望自己成为杀毒软件供应商已经识别并标记的恶意软件威胁的受害者。

确保您的病毒定义数据库在所有工作站中始终为最新版本，是有效的杀毒策略最重要的要素。Ivanti 安全管理软件能够让这一流程自动化，为您提供帮助。我们的解决方案能够在任何规模的环境下，根据带宽将最新的病毒定义文件高效快速地传输至您的所有端点。由于我们支持大多数杀毒软件供应商，因此我们的解决方案将很有可能与您的杀毒软件供应商适配。如果您选择使用我们基于卡巴斯基实验室杀毒引擎的杀毒解决方案，我们还将通过单一控制台自动扫描和管理杀毒软件。

3 管理特权帐户的使用

最大程度地减少特权是防范包括勒索软件在内的各类恶意软件的重要战术。比如，近期发现的名为“Petya”的勒索软件攻击需要管理员权限才能运行，如果用户没有授予这些特殊权限，该类软件便无计可施。[5]

取消管理员权限非常容易，但平衡特权访问、用户工作效率和企业安全则不然。因此，您需要特权管理解决方案。

Ivanti 安全团队提倡对特权管理的重视，这也是 Ivanti 收购 AppSense 的原因之一，AppSense 是该领域久经考验的解决方案（及其他优秀工具）的供应商。AppSense 特权管理能够帮助您制定政策，将获授权用户的管理权限限制在其工作所需范围之内。

不过，在防范勒索软件时应注意一点，许多勒索软件攻击会伪装成欺骗用户运行的可执行文件。一旦执行，这些勒索软件会在当下的用户空间内运行，不需要任何管理员权限即可造成破坏。最新版本的 Petya 勒索软件攻击（上述）拥有后备机制，无需管理员权限便可加密文件。

4 实施以数据为重点的访问控制

有效的访问控制解决方案能够帮助您防范勒索软件。不过，如果解决方案主要或仅仅关注用户访问权限的话，其效果可能会不太理想。

访问控制对保护共享驱动器中的文件大有裨益。原因在于，有些用户很可能始终拥有访问和修改各共享驱动器中至少部分文件的合法权限。毕竟，大多数文件是由合法用户创建的文档文件。这意味着，如果勒索软件成功攻击拥有合法访问权限的用户的系统，便能够对所有互联共享驱动器和文件夹中的文件进行加密并将其当做勒索筹码。

最大程度地减少特权是防范特定类型的勒索软件的重要战术。

Ivanti 安全解决方案能够提供不同类型的访问控制，重点控制您想保护的数据，而不是这些用户的权限。Ivanti 软件允许您制定规则，防止（除您规定之外的）任意程序修改关键或敏感文档或文件。比如，仅允许 Microsoft Word 修改 .doc 和 .docx 文件的规则将拒绝已成功安装的勒索软件对此类文件进行的所有加密尝试。

制定类似的规则，保护所有 Microsoft Office、Adobe PDF 以及其他常用和共享的文件类型，是有效防范大多数勒索软件攻击的最好措施。制定此类规则后，即便勒索软件成功侵入用户系统，也无法加密受保护的文件。用户将保有对这些文件的访问权限，并能够在尽可能不中断工作，且无需恢复到很可能已经过时的旧备份版本的情况下继续工作。

（注意，有些勒索软件会试图伪装成合法软件，并将自己添加到随系统启动的软件行列中。Ivanti 解决方案能够防止此类程序进行该操作。）

相较于传统的访问控制，Ivanti 专注于数据保护的方法能够更加有效地防范勒索软件。它主要基于对勒索软件行为的理解，不需要制定和管理针对用户（且不断变化）的规则。因此，它比基于用户权限管理的访问控制解决方案更易于实施和维护。

勒索软件利用 MICROSOFT OFFICE 宏指令攻击用户。通过 IVANTI 安全套件禁用宏指令。

5 制定、实施并执行软件规则

Ivanti 软件还可以让用户轻松制定、实施和执行管理其他软件行为的规则。此类规则可以限制指定系统执行、创建、修改或读取任意文件或者特定文件夹中的文件的能力，这些文件夹包括浏览器及其他程序使用的临时文件夹。这些规则既可以全局通用，也可以局限于特定的用户或群组。

但是，在实施这些规则之前，必须要充分考量这些规则可能导致的用户体验下降问题。例如，在安装新软件或更新软件时，合法用户有时需要直接从浏览器中解压缩或执行文件。用户还可能需要依靠创建或调用宏指令进行工作。软件限制规则可能会阻碍这些合法操作。

6 禁用来自 Microsoft Office 文件的宏指令

禁用来自 Office 文件的宏指令可以阻止包括勒索软件在内的多种恶意软件。Locky 便是其中之一，它是一款相对较新的加密勒索软件，主要通过带附件的垃圾邮件传播。它诱骗用户启用 Word 文档中的宏指令，将恶意软件下载到设备中。

Ivanti 安全套件允许 IT 管理员制定政策来禁用宏指令。向无需使用宏指令的员工部署这一政策能够有效阻止此类勒索软件运行。

其他考量

FBI 还提出了其他旨在加强系统环境保护的建议。这些建议能够帮助您防范多种类型的恶意软件及其他攻击，如使用得当，还能防范勒索软件。

7 实施应用白名单

该解决方案能够有效消除所有勒索软件运行的可能性，因为所有勒索软件均不受信。它能够确保只有受到信任的已知应用可以在任何端点上运行。成功实施白名单的最大挑战在于创建可信应用的初始清单，并确保该清单准确、完整和未过时。

包括 AppSense 应用管理在内的 Ivanti 解决方案能够为制定全面、灵活、有效、简明的白名单提供多种选择。Ivanti 让创建和维护白名单变得轻而易举。比如，Ivanti 解决方案会自动“发现”所有在“干净”的系统中运行的应用，并根据自有的应用信誉数据库验证应用的可靠性。根据所有者（如授权管理员）和供应商（如 Microsoft、Oracle）添加受信任的应用的规则，能够进一步减少创建可信应用清单所需的配置数量。

8 将用户限定在虚拟化或集装化的环境中

在大多数情况下，勒索软件通过电子邮件附件传播。将用户限定在虚拟化或集装化的环境中，能够确保获得用户系统访问权限的任何勒索软件不会危害用户的主要工作环境。

Ivanti ONE 合作伙伴 Bufferzone 提供能与 Ivanti 安全解决方案集成的一流威胁隔离解决方案。如需进一步了解 Bufferzone，请访问
http://www.Ivanti.com.cn/partners/landesk-one/bufferzone/。

9 经常备份关键文件

FBI 文件建议通过及时和经常备份关键文件维持业务的连续性。如操作得当，在您遭受勒索软件攻击时，备份将帮助您化险为夷。不过，如果您实施了本电子书中介绍的防范建议，尤其是由 Ivanti 提供的访问控制功能，您将无需单纯依靠备份对抗勒索软件。

第一时间阻止
勒索软件运行

为您的
应用动态
更新白名单

ivanti

勒索软件犯罪案件日益增多。我们要积极防范，有力回击！

借助 Ivanti 解决方案，您将能够管理和保护所有端点，防范新旧威胁，将保护级别提升到全新的水平。

如需预约
IVANTI 安全解决方案演示，
请致电我们的团队，电话：(800) 982-2130

参考资料

1. http://www.businessinsider.com/fbi-recommends-paying-ransom-for-infected-computer-2015-10

2. http://www.computerworld.com/article/3068623/security/ransomware-attacks-on-house-of-representatives-gets-yahoo-mail-blocked.html

3. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

4. https://threatpost.com/latest-flash-zero-day-being-used-to-push-ransomware/117248/

5. https://blog.malwarebytes.org/threat-analysis/2016/04/petya-ransomware/.