Web浏览器扩展程序安全：缓解浏览器插件威胁

大多数Web浏览器用户都期望浏览器扩展程序、插件和浏览器帮助者对象（BHO）能提供一些便利。

不幸的是，这些附加产品通过将组件添加到浏览器的默认功能来提高生产力的同时，也成为恶意攻击者的首要攻击目标。因为企业在修补和更新插件和扩展程序方面的能力普遍较差，所以浏览器就成为了终端最脆弱的攻击目标。对于终端环境来说，大多数企业的补丁周期是2~3个月，这个周期很长以至于企业不能及时地跟上利用浏览器扩展程序和插件漏洞的攻击组件。

在本文中，我们将探讨Web浏览器扩展程序在普及程度和功能完善两方面的发展，以及它对固有环境的威胁和如何缓解这种状况。

虽然很多热门的附加组件是由知名供应商所开发，但是任何人都可以写一段代码让这些组件成为传递恶意的潜在工具。过去，恶意浏览器扩展程序通过在网站插入虚假广告或挟持搜索查询，来进行点击欺诈。例如，安全研究员Zoltan Balazs开发了一个可以修改网页，下载并执行文件，挟持账户和绕过双因素身份认证的浏览器扩展程序。感染了这个扩展程序的浏览器会被控制，就像一个僵尸客户端：这个扩展程序接收指令并且将信息发送给攻击者。因为依据浏览器发起的HTTP通信数据看起来是正常的，那么对于本地或网络防火墙来说，很难发现并阻止这个恶意软件。

浏览器旨在为用户提供一些扩展程序权限控制，但是通常会因为粗粒度访问控制而被攻击，另外，用户总是对各种附加产品授予权限，危险意识不足。永远不要只是因为一个附加产品托管在官方扩展程序库中，就想当然认为它是安全的。尽管大多数附加产品在推出之前都要经过审查，但是违反浏览器开发者程序政策的恶意扩展程序并不少见。比如，提交给苹果扩展程序库的苹果Safari扩展程序其实托管在一个外部位置，而Mozilla Firefox允许来自第三方网站扩展程序的安装。

当审查要安装在企业的扩展程序时，始终牢记扩展程序可以访问的资源类型和数据发送的目标位置。尽管谷歌为Chrome浏览器扩展程序设定了风险等级，而且谷歌最近刚刚宣布将收紧限制，使基于Windows的扩展程序只能通过Chrome Web商店来添加，但是管理员还是应该完成他们自己的评估。对待任意扩展程序都应该高度谨慎，做到以下要求：

与本地文件交互

与Windows注册表交互

与cookies交互

访问任意浏览器选项卡或窗口

执行用户的shell指令

沙盒插件应该总是优于非沙盒插件，因为后者是在用户的特权级别下运行，可能访问到如系统文件或网络资源。在企业中，任意需要高特权访问的扩展程序或插件如果想要被允许，其只能是一个大的业务案件而且风险评估认为其是绝对必要的。

浏览器应该始终开启自动更新选项，但是要知道并不是所有插件都会自动更新。例如，Chrome会自动更新Adobe Flash插件，但是大部分其他扩展程序需要通过运行相关产品的安装程序进行更新。建议禁止运行已经过时的插件，这样有助于确保企业的修复策略，包括浏览器扩展程序和插件。企业可能考虑实施审计工具，如Secunia CSI 7.0或Qualys BrowserCheck，这些可以扫描常见的浏览器插件，并确定它们是否需要更新。

同时，很多浏览器厂商都试图提高附加产品的安全性。Chrome浏览器不再允许静默扩展程序安装，这和IE浏览器的Protected Mode、Firefox的扩展程序控制类似，这些都不允许静默扩展程序安装。在活动目录（Active Directory）环境中，组策略（Group Policy）提供一套全面的设置来管理Windows IE8，包括启用或禁用ActiveX空间和限制扩展程序安装或运行的能力。FirefoxADM也可以产生安全组策略对象（GPO）来管理安装设置。尽管Chrome浏览器有安装模版，还是要手动创建GPO来部署一个Windows域。

为了成功的降低扩展程序风险，推荐将所有的插件列入黑名单，然后选择性地添加一些必要的插件进入白名单。需要降低风险状况的企业应该也要考虑清除最广泛受到攻击的插件，将其从所有计算机上完全卸载，除非业务应用程序对其有迫切需求。Java作为最广泛的插件目标对象，应该被考虑到。第二最常见被利用的目标应用程序是Adobe Reader. 企业可能考

分层安全策略为什么不是万能的

为了应对日益复杂的恶意行为和恶意软件，分层安全策略在不久之前变得相当受欢迎，而且现在已经深入人心，成为整个行业保护企业网络最好的实践方式。从直观的角度来看，它似乎在网络内部署了多台安全设备，每一台都有其自身的防御载体，提供一种具有重复性、在几个不同层次上都有意义的网络防御。

比如，如果一个组织部署了一个防火墙、入侵防御系统(IPS)和端点保护(EPP)系统，组织会认为这些产品可以通过其不同的功能组合提供更强大的保护：在网络外部，防火墙会检查恶意 URL、IP 地址和其他类似可以在访问控制列表中容易验证的指标传入的数据包。数据包如果通过防火墙，IPS 系统会检查数据包的内容和头信息，如果任意数据包内容被视为符合 IPS 签名列表的恶意内容，这个数据包就会被丢弃或阻止。最后，在网络中 EPP 系统驻扎在每个终端设备上，作为防御恶意代码的最后一道防御线，对抗可能通过防火墙和 IPS 的恶意代码。

给定的数据包通过网络的每一个节点时，都需要接受为了保护网络而日益侵入性的检查。安全管理员都感到欣慰，觉得只有最复杂的恶意编码可以成功渗透安全设备的几层防御。然而，NSS 实验室的独立安全测试人员发布的一份报告质疑部署分层安全方法会增强企业网络安全。

在报告中关于入侵侦测故障的部分，NSS 实验室决定测试 37 种不同的安全设备，包括来自 24 家安全厂商提供的解决 1711 种已知漏洞的防火墙、下一代防火墙(NGFW)、IPS 和 EPP 设备。所选择的攻击已知感染过超过 200 多种软件供应商，包括来自微软、苹果和思科的产品。NSS 实验室为了确定对于检测漏洞的最佳配对，测试了各种设备的不同组合。对于分层安全策略的潜在故障，结果提供了一个有趣的答案。

测试的 606 种不同组合中，只有 19 种成功阻止了所有入侵企图，值得注意的是，没有一种单独进行测试的设备能够阻止所有的恶意企图。至于哪些产品一起工作是最佳搭配，NSS 实验室发现 NGFW 和 IPS 的组合比任意 EPP 系统组合都能更有效地阻止已知的攻击。例如，任意 NGFW-IPS 组合平均故障率约为 0.8%，而任意 EPP 组合平均故障率是惊人的 26%. 单单这些结果表明，如果不将一些内嵌的安全设备搭配起来，仅仅只是部署端点防护是不够安全的方法。

那么，组织应该采取或计划采取怎样的分层安全方法来应对这个报告？首先，企业应该重视报告的具体内容。例如，应当注意到，没有任何安全装置可以仅仅凭借自身来检测到所有直接的微软相关攻击。以微软为中心的组织决定部署安全设备组合时，应该认识到这个事实。

该报告提供了大量关于各种设备组合的性能详情，我建议至少通读整个报告，然后采用其中关于您的组织所使用的产品或供应商的性能内容。苹果对苹果产品的比较可能并不太合适，但是数据可能会凸显你的产品表现不佳的状况以及怎样将产品和其他技术结合起来可以提高你的分层安全。例如，一个特别的组合：Sourcefire 3D8250 IPS 和 Stonesoft 1301 NGFWs，在我心目中脱颖而出，因为它在测试过程中的阻拦表现非常好。尽管如此，某些产品可能适合一个组织，但不一定会适合另一个组织。

为此，每一个组织考虑或部署分层安全方式时，最好考虑到自身的威胁状况和安全要求，然后按照 NSS 实验室的方法自行进行测试。这将为每个组织提供特定的结果组合，并能产生一个更清晰的画面，告诉组织哪些产品可以提供最佳的性能。

最后，部署分层安全策略时如果不考虑到设备组合，其实很有可能导致灾难性的后果。虽然会有故障可能性，但是对于攻击者带来的许多问题，分层网络安全仍旧可以像当前任意方法一样提供极有说服力的解决方法。为了确保使用分层安全策略可以带来更好的效果，在部署设备之前，安全管理员应该深入研究不同厂商的设备组合，上述 NSS 实验室报告就是这个过程一个明智的开始。

(jiangxun)

虑到使用替代品，如使用集成在 Firefox 浏览器的 Mozilla PDF 阅读器来替代 Adobe 版本。

浏览器扩展程序的风险是非常现实的。企业和终端用户都需要非常认真地对待这些威胁。安装意识培训应该强调扩展程序可以潜在地访问浏览器中的一切，所有数据、密码和浏览的网站。还应该注意的是，用户永远不应该安装未知扩展程序，允许任意失控插件的安装可能会提高网络的整体攻击面，并让用户和网络对于感染和数据丢失无防备。

(TechTarget)

Web浏览器扩展程序安全:缓解浏览器插件威胁

作者： TechTarget
作者单位：
刊名： 计算机与网络
英文刊名： Computer & Network
年，卷(期)： 2013,39(23)