FIREEYE™

解决方案简述

智能服务器防御

使用网络和终端威胁防护来抵御高级攻击

亮点

- 现代攻击以难以检测的方法针对服务器
- FireEye 解决了从网络到服务器的威胁
- FireEye 的高级威胁情报使我们的解决方案能够检测到其他解决方案遗漏的攻击

概要

普通员工在移动设备不断与数据中心和云中的服务器进行交互的环境中工作，并共享各种敏感数据，因为业务通常是在办公室外进行而不是在室内进行的。这会给组织的核心业务留下开放的攻击路径：存储在服务器上的数据、客户信息和知识产权。

服务器通常运行面向 web 的应用程序，这些应用程序从网络和在管理组织内部提供直接攻击面。威胁实施者通过由外而内的攻击直接攻击服务器，该攻击会扫描服务器并确定正在运行的操作系统、网络服务和应用程序。他们可以使用此信息来识别漏洞或入侵进行危害。

安全行业提供很多保护客户端的终端和网络本身的解决方案，但是服务器（Linux 和 Windows）具有与客户端终端不同的攻击面、漏洞和模式。攻击者隐藏在服务器上；发现攻击者的平均时间为 78 天；让攻击者有时间执行侦察、升级特权、窃取组织最敏感的数据并掩盖其踪迹。

攻击者如何接近服务器

对服务器的攻击通常与对客户端终端的攻击截然不同。攻击者的目的是驻留在系统上并收集网络侦察数据、个人可识别信息或金融交易信息。攻击者隐藏的时间越长，获得的价值越多。基本攻击（如恶意软件或 “蠕虫”病毒）很容易被击败，现代攻击者使用 web shells 作为远程访问木马；网络服务器上安装的几行简单代码，用于提供后门访问或访问服务器文件系统。

这几行代码看起来与在服务器上现有的代码类似，除非 web shells 处于活动状态，否则检测起来并不容易。通过使用 web shells，攻击者可以修改 网络服务器，将搜索引擎请求重新定向到受损的网页。或者向搜索引擎呈现与用户看到的内容不同的内容。定位 web shells 通常需要更改 crawler bot 的用户代理。

当今客户如何检测服务器攻击

检测 web shells 攻击的自动化工具仅提供有限的检测手段。管理员被迫使用指示器来查找 web shells 攻击：

- 网络服务器使用率异常高（由于攻击者大量下载和上传）
- 时间戳异常的文件（例如，比上次修改日期更新）
- 服务器上的未知文件
- 具有可疑引用的文件，如 cmd.exe 或 evals
- 网络服务器日志中的未知连接

分析网络服务器日志可以确定 web shells 的位置，但该过程非常耗时，因为必须检查每个可疑的日志。并且，在此过程中，攻击仍在继续。

传统的安全工具对现代服务器攻击无效。防火墙和入侵检测系统通常依赖于签名，而 web shells 可以轻松绕过签名。安全的网络网关和其他产品可能会查看内容，但 web shells 可以很容易骗过这些扫描仪，因为它们是合法的代码。组织需要的解决方案能够完全模拟系统、与代码交互、寻找指示器，然后才能确定代码是否是恶意的。

FireEye 解决方案

FireEye 网络威胁防护和终端威胁防护中的新功能检测 web shells 流量，确定服务器是否已被感染，并启用调查对攻击作出响应。

网络威胁防护

对于组织的网络流量，客户可以使用网络威胁防护解决方案中的 FireEye SmartVision 引擎，来检测客户端与通过 SMB 进行通信的网络设备之间的恶意流量移动。使用网络威胁防护 8.3，FireEye 可以检测 web shells 流量，确定 web shells 正在执行的操作、活动时间以及正在使用的设备。事故响应者可以使用此信息来确定攻击是否正在进行以及如何开始调查。

终端威胁防护

FireEye 终端威胁防护使用四个专用引擎来帮助保护、检测和响应使用 Microsoft Windows 和 Windows 服务器对客户端的攻击。对于 Linux 服务器，终端威胁防护 4.8 为事故响应者提供实时检测和调查功能。

通过这两个更新的解决方案，调查人员可以使用终端威胁防护来确定 web shells 是否被用作涉及服务器的攻击的一部分，并识别受影响的服务器。然后，调查人员可以使用终端威胁防护对这些服务器执行深入调查，确定哪些网页或应用程序已被 web shells 破坏。继而，他们可以隔离这些网页或应用程序，修复环境并恢复正常操作。一旦确定攻击的发生方式，安全团队就可以通过解决漏洞或修补受感染的系统阻止进一步感染。类似的主动修复可以作为预防措施应用于未受感染的系统。

更好地协同工作

通过这种组合解决方案，FireEye 将检测和解决攻击的时间从数周缩短至数小时。处理受感染的文件或应用程序的时间从几天减少到几分钟。FireEye 为客户提供深度数据中心攻击的端到端检测和调查生命周期，这是其他供应商无法比拟的。

若要了解更多关于 FireEye 的信息，请访问：**www.FireEye.com**

FireEye, Inc.
26/F Times Square, 93 Middle Huaihai,
HuangpuShanghai, China
China@FireEye.com

关于 FireEye, Inc.

FireEye 是一家情报主导型安全企业。FireEye 为客户提供无缝式、可扩展的讯息安全解决方案，提供一个将创新型安全技术、国家级威胁情报以及闻名于世的 Mandiant® 咨询集成于一体的平台。通过这种方式，FireEye 为殚精竭虑防备、阻止和应对网络攻击的组织，消除了网络安全的复杂性和负担。

NS-EXT-SB-US-EN-000210-01