Threat of the Month: SMB 与蠕虫的卷土重来

SMB 是什么？

SMB 是一种网络协议，可以帮助计算机之间进行交互，例如共享文件、执行网络打印或连接各种设备。由于 Microsoft 从上世纪 90 年代初开始采用、实施和投资发展 SMB，SMB 曾经是通过网络共享文件的最常用的协议之一。在 Windows 上设置和使用 SMB 非常简单，只需要很少的配置，并且可以用于各种目的。这是一种无缝体验： 您可以访问远程计算机上的文件，就好像这些文件位于本地计算机上一样。计算机之间甚至不需要通过服务器来通信，就可以直接连接。

您为何要关注此种威胁？

SMB 提供的便利性也有不利的一面。作为用于计算机间通信的协议，自然而然，它成为了寻求遍历网络的攻击者的目标。它自然也是恶意攻击者的攻击目标，这些恶意攻击者制作蠕虫以在网络中传播，从一台计算机复制到另一台计算机，随时随地传播恶意负载。

哪些威胁以 SMB 为目标？

2017 年 SMB 爆出了一个重大漏洞，名为 EternalBlue。该漏洞可以帮助攻击者在易受攻击的计算机上安装恶意软件。此后不久，WannaCry 威胁进入威胁格局，利用 EternalBlue 进行传播。一个月后，Nyetya 威胁随之而来。许多其他威胁虽然没有利用 EternalBlue，但也利用了 SMB 来破坏计算机，包括 SamSam、Bad Rabbit 和 Olympic Destroyer。

为什么需要重视此类攻击？

SMB 是在本地网络中建立计算机间网络的便捷选择。然而，这种易用性也伴随着风险。利用 SMB 连接到共享时几乎无身份验证，并且连接未利用加密。虽然更高版本的 SMB 提高了安全性，但由于向后兼容性，旧版本在被发现不安全后仍继续使用了很长时间。鉴于该协议可以连接计算机，它自然成了黑客和蠕虫的攻击目标。

延伸阅读

https://blog.talosintelligence.com/2017/05/wannacry.html

https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html

https://blog.talosintelligence.com/2018/01/samsam-evolution-continues-netting-over.html

https://blog.talosintelligence.com/2017/10/bad-rabbit.html

https://blog.talosintelligence.com/2018/02/olympic-destroyer.html

CXX-XXXXXX-00　01/19

我该怎么做？

最简单的办法是停止使用 SMB，因为目前几乎没有什么理由要继续使用它。不要通过 SMB 连接计算机来共享文件，请改用专用的文件服务器或基于云的产品。将网络打印机配置为使用其他协议。如果在您的环境中无法关闭 SMB，请至少确保禁用 SMB1。阻止网络边界的 TCP 端口 445 和 139，以确保 SMB 通信仅限于内部网络。除此之外，所有终端都应无法通过 SMB 相互通信。

思科如何为您提供保护？

下一代防火墙/下一代入侵防御系统	检测并阻止与 SMB 攻击相关联的恶意流量。
面向终端的高级恶意软件防护 (AMP)	持续监控和追溯安全功能可以阻止利用 SMB 的威胁。
思科 Stealthwatch®	可以检测与 SMB 共享的连接，对此活动进行关联分析，从而向管理员发出警报。
Threat Grid	可以帮助识别恶意文件行为，并自动通知所有思科安全产品。