AhnLab

安全月刊

2019.11 Vol.84

SMB 漏洞

分析SMB漏洞的编年简史

反复出现的SMB漏洞攻击，究竟是怎么回事?

从2017年的WannaCry勒索软件到Petya勒索软件、Bad Rabbit勒索软件、2018年GandCrab勒索软件变种以及2019年的WannaMine挖矿恶意软件和Clob勒索软件，它们有一个共同的因素。就是“SMB漏洞”。特别是今年在韩国，由于Clop勒索软件，SMB漏洞与AD服务器一起再次成为了热门话题。利用SMB漏洞的恶意代码每次快要忘记的时候就会再次出现，到底什么是SMB漏洞？即使该漏洞是已知的，并且已分发并应于了相关安全补丁，我们为什么仍然由于它而受到折磨？本文对历史上的基于SMB漏洞的攻击做了梳理，并讨论了此漏洞反复出现并造成损害的原因，最后提示了其解决方案。

SMB漏洞全面展开于2017年5月通过WannaCry（或WannaCrytor）勒索软件。当时，WannaCry勒索软件导致瘫痪全球150多个国家/地区的30万个以上系统，正是这SMB漏洞使WannaCry勒索软件具有如此的破坏力。到底SMB是什么？为何具有如此大的破坏力？

SMB是“服务器消息块（Server Message Block）”的简称，是Windows操作系统的协议，旨在在网络上的节点之间共享资源。由网络上的计算机用来传输文件、打印机、端口或其他消息。这使得在不同操作系统之间共享资源变得容易，尤其是当与Linux设备（例如NAS和网络扫描仪）共享文件时，可以使用资源管理器直接对其进行修改，而无需客户端。

由于这种兼容性，SMB协议已经存在了很长时间，但是由于存在多个安全漏洞而被攻击者利用。一个典型的例子是几年前出现的被称为WannaCry（或WannaCryptor）的勒索软件。但是，使用SMB漏洞的恶意软件的年代可以追溯到10年前。

SMB 漏洞（MS08-067）之前奏，Conficker

Conficker于2008年底开始迅速传播，并于2010年在全球感染了650万台计算机，它是一种利用Windows Server服务远程代码执行漏洞的蠕虫（worm）病毒。Conficker主要通过Windows安全漏洞（MS08-067），管理共享文件夹（IPC$，ADMIN$）和可移动磁盘进行传播。如果Conficker感染了具有MS08-067漏洞的系统，则该感染会扩散到网络中的其他系统，并对随机或B类IP频段生成大量流量到远程TCP 445端口，从而消耗组织的网络资源。

但是，当Conficker事件平静下来后，我们很快就忘记了SMB漏洞，并且许多系统没有应用安全补丁的情况下照样使用。

重返并展示其健在的 SMB 漏洞（MS17-010），WannaCry

Conficker蠕虫事件告一段落后，再过五到六年后，利用SMB漏洞（MS17-010）的WannaCry勒索软件席卷全球。WannaCry勒索软件通过SMB远程代码执行漏洞（MS17-010）感染，而不是当时大多数勒索软件使用的电子邮件附件或受感染的网站。

【图1】WannaCry勒索软件的勒索笔记

2017年，席卷全球的WannaCry勒索软件的破坏力是巨大的。当时，Microsoft（MS）认识到事件的严重性，针对已结束服务的Windows XP和Windows Server 2003发布了有关该漏洞的一个紧急安全补丁。
在WannaCry事件中，我们再次意识到安全补丁的重要性。当时，许多公司开始注视补丁管理解决方案，积极检讨引进解决方案或者重新调整现有解决方案的运营状态。由此，大多数的人们已认为SMB漏洞不再对我们造成威胁。

再次出现的 SMB 漏洞（MS17-010），WannaMine

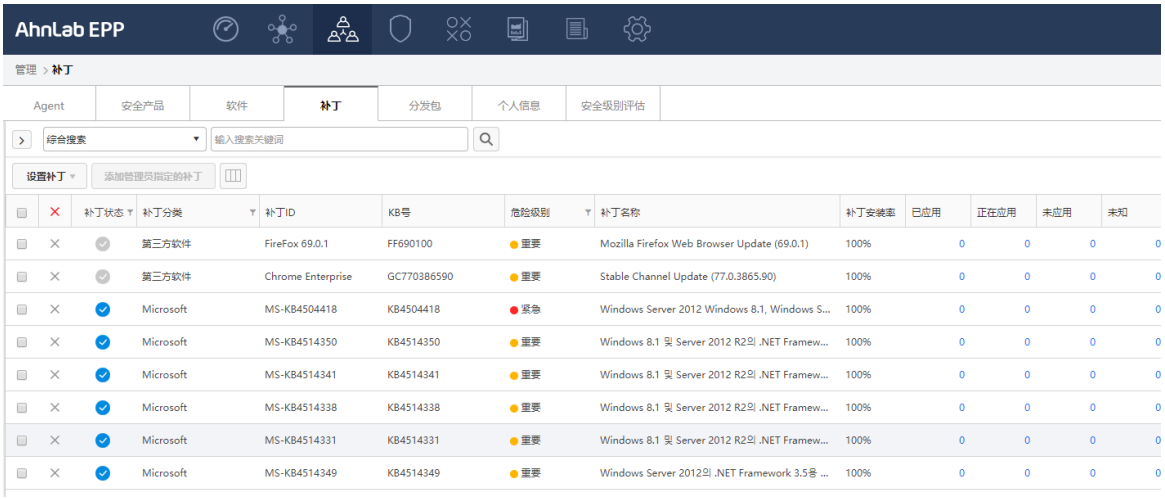
但是，利用相同漏洞的WannaCry等勒索软件沉默了一年之后的2019年，我们不得不再次寻找MS17-010漏洞补丁。这次不是因为勒索软件，而是因为加密货币挖掘恶意软件，它被称为WannaMine。
随着加密货币挖掘恶意软件的增加以及其传播方式变得更加多样化，加密货币挖掘恶意软件（也称为WannaMine）似乎已利用SMB漏洞进行了感染和传播。WanaMine是一种无文件（file-less）的恶意软件，可以挖掘系统中的加密货币并从攻击者的服务器下载另一个恶意文件。此时下载的就是WannaCry勒索软件利用的SMB漏洞攻击工具“EternalBlue”。该挖矿恶意软件被称为WannaMine，因为它利用了与WannaCry相同的漏洞和攻击工具。
WannaMine恶意软件使安全人员紧张的更大原因是，出现了该恶意软件与今年6月发威的Clop勒索软件一起传播的事件。除了SMB漏洞，WannaMine恶意软件还利用WMI和ADMIN$共享文件夹在内部传播感染。

SMB 漏洞如大海里的一根针，如何捕获?

使用SMB协议的一种更安全的方法归根结底是应用安全修补程序，它使在异机种操作系统之间共享资源更加容易。应该具备补丁管理系统，以验证是否已在组织中的所有终端上安装了安全补丁程序，并对未安装补丁的系统采取适当的措施。如果您当前没有补丁管理解决方案或引进不如意，那么使用其他安全产品来建立可以响应的策略也很重要。
AhnLab提供了多种产品来响应SMB漏洞。强烈建议您根据公司的情况和所使用的AhnLab产品，选择最适合您的方法并立即实施。

1. 基于端点保护平台的SMB漏洞响应

AhnLab补丁管理（APM）是基于端点安全平台“AhnLab EPP”的补丁管理解决方案，可轻松掌握公司内部应用MS17-010补丁情况并对其采取措施。如【图2】所示，您可以通过单击“管理 > 补丁”菜单中未应用的补丁数，转到未应用补丁的Agent列表界面，然后发送命令以执行补丁应用。



【图2】AhnLab Patch Management的补丁应用情况

安全汇总补丁可以累积形式提供，其中包括上个月的汇总补丁和本月的安全补丁。因此，对于MS17-010，如果您安装了2017年3月之后发布的安全汇总，则该补丁也将适用。
虽然通过APM可以自动应用最新的安全汇总补丁程序，但是端点安全平台AhnLab EPP的连接规则可以根据每个企业环境中安全人员设置的条件实现更主动和自动化的响应。

2. 通过AhnLab MDS的C＆C流量状态进行检测和响应

高级持续性威胁响应解决方案“AhnLab MDS”通过行为分析信息可以识别并响应未知的SMB漏洞攻击。监控异常流量（Traffic anomaly），以检测尝试使用445端口与特定IP进行通信的行为，并且通过流量镜像还可以检测通过网络的内部传播。

3. 通过V3进行SMB漏洞检测和响应

V3的“网络入侵防御（IPS）”功能可检测并阻止恶意软件，例如通过网络入侵的蠕虫和特洛伊木马。AhnLab不断分析最新威胁并将其添加到V3的IPS检测规则中。安全管理人员可以使用这些更新的IPS检测规则来防止威胁扩散，即使内部有一台受感染的计算机，也可以防止威胁传播到同一网络中的其他计算机。

4. 通过AhnLab EPS保护OT环境（生产设备）

Conficker蠕虫自10年前就没有消失，它的目标是OT（运营技术）环境中的特殊目的系统，例如POS终端和生产设施，而不是普通的计算机。AhnLab的工控系统专用安全解决方案AhnLab EPS可以阻止通过MS08-067漏洞进行攻击的Conficker，不仅阻止Conficker的内部传播，而且还检出主机（宿主）。入站（inbound）和出站（outbound）日志可用于识别攻击主机IP和受感染的节点。 通过入站日志，可以识别当前受感染并向外部攻击的系统，可以识别受到来自同一网络上的受感染系统的攻击的系统。

5. 如果您还没有补丁管理解决方案（PMS）

当然，即使没有单独的补丁管理解决方案或无法使用AhnLab产品，也可以应用SMB漏洞补丁。最基本的方法是，您可以通过计算机上的“ Windows自动更新”功能进行更新，也可以从Microsoft网站下载相关补丁。
如果无法应用与SMB漏洞相关的安全补丁，请通过防火墙设置阻止SMB端口并通过操作系统设置禁用SMB协议。使用RDP（远程桌面协议）时，建议更改IP访问控制并更改默认端口号。

总结

孙子兵法中说道：“最好的胜利就是不战而胜”。还说道：“知己知彼，百战百胜”。与其利用SMB漏洞的攻击者（黑客）进行战斗，不如检查当前的安全补丁应用状态并做好准备，这将使您在数百次的与攻击者的攻防战中不战而胜。尽管大多数人们已知道问题在哪里，也知道如何解决，但是它们仍然会受到黑客的攻击。请大家平时就要做好准备，不要重蹈覆辙！

AhnLab

安全月刊

https:// cn.ahnlab.com

https://global.ahnlab.com

https://www.ahnlab.com

关于AhnLab

Ahnlab的尖端技术和服务不断满足当今世界日新月异的安全需求，
确保我们客户的业务连续性，并致力于为所有客户打造一个安全的计算环境。
我们提供全方位的安全阵容，包括经过证实的适用于桌面和服务器的世界级防病毒产品、
移动安全产品、网上交易安全产品、网络安全设备以及咨询服务。
AhnLab已经牢固地确立了其市场地位，其销售伙伴遍布全球许多国家和地区。

AhnLab

北京市朝阳区望京阜通东大街1号望京SOHO塔2 B座 220502室 | 上海市闵行区万源路2158号18幢泓毅大厦1201室
电话：+86 10 8260 0932（北京） / +86 21 6095 6780（上海） | cn.sales@ahnlab.com