2017 年 8 月 31 日，星期四

回归本始：勒索软件时代的蠕虫防御

作者 Edmund Brumaghin

“那些忘记历史的人注定会重蹈覆辙。”— 乔治・桑塔亚那

前篇

2017 年 3 月，Microsoft 针对 Windows 的各种版本发布了安全更新，解决了影响名为 SMBv1 (MS17-010) 的协议的远程代码执行漏洞。此漏洞允许远程攻击者完全破坏受影响的系统，被建议执行安全更新的组织将其评为“严重等级”的漏洞。此外，对于无法直接应用安全更新的环境，Microsoft 发布了消除此漏洞的权变方案指南。同时，思科发布了防护软件以确保我们的客户始终受到保护。

随后，即 2017 年 4 月，一个绰号为“TheShadowBrokers”的团体在互联网上公开发布了几个漏洞利用。这些漏洞利用针对包括一个月前被 MS17-010 解决的各种安全漏洞。一如既往，每当新漏洞利用攻击代码对外发放后，它便成为信息安全产业以及网络犯罪研究两者的焦点。信息安全产业获取信息并通过改善安全将其发挥更大的作用，网络罪犯获取代码并尝试找到方法利用它以达到他们的目的，无论是经济利益、制造破坏等。

勒索软件蠕虫

计算机蠕虫并不是新的概念。蠕虫与其他恶意软件不同，他们会在系统内部以及系统之间自我传播。例如，Conficker 是一种使用 Windows 漏洞传播 (MS08-067) 的计算机蠕虫，可追溯到 2008 年。事实上，几乎十年之后，Conficker 仍然通过在易受攻击的系统之间传播的方式在网络上散播。历史告诉我们，每当针对漏洞对外发布漏洞攻击代码时，那就是“蠕虫化的”的漏洞，将会创建和传播蠕虫。尽管这种现象并不经常发生，但只要出现，蠕虫对全世界便产生巨大影响。在 2017 年，到目前为止便出现两次。然而，蠕虫出现了新变化，那就是它使用计算机蠕虫来传播勒索软件和其他具破坏性的恶意软件。让我们了解 WannaCry 和 Nyetya。

WannaCry

随着时间推移，2017 年 5 月，我们看到了 WannaCry 进入威胁形势的介绍。攻击者将 WannaCry 创建为勒索软件蠕虫，它利用 Windows 内的漏洞进行自身传播并感染不需要显式用户交互的其他系统。WannaCry 利用两个月前 (MS17-010) 已解决的漏洞来来执行此传播。恶意软件一旦感染系统，将会为其安装勒索软件，并且使用他们的系统来向其他系统传播攻击。很快，就像滚雪球一样，越来越多的系统被感染并积极散播恶意软件。WannaCry 所造成的损害是全球性的，全球范围内许多组织要么直接被感染，要么由于恶意软件在其他地方产生的问题而造成间接影响。

Nyetya

时间快进到 2017 年 6 月，出现了更为复杂的攻击，这次攻击同样再次利用了几个月之前发布的安全更新漏洞。由于诸多原因，我们认为这种特定攻击更为复杂。首先，它利用所谓的“供应链攻击”作为危害组织的初始矢量。在供应链攻击中，攻击者利用了组织与供应商之间的信任关系。在这次攻击中，Nyetya 背后的攻击者破坏了乌克兰境内的企业和组织所广泛使用的软件更新服务器。他们利用被攻击的服务器，打着更新软件的幌子，部署带后门版本的软件。部署完带后门的软件后，攻击者便可以将恶意软件直接分发到目标环境中。在这种特殊情况下，恶意软件对系统造成了重大影响，并利用多种方法传遍受危害组织内的整个网络。与 WannaCry 类似，这次攻击导致许多组织面临重大的业务中断，但是本次攻击案例中，破坏主要集中在乌克兰境内。

WANNACRY 与 NYETYA

这两个恶意软件之间有着显著差异。如前文所述，由于许多不同原因，大家认为 Nyetya 更为复杂，以下章节将进行详细介绍。两者之间的复杂性差异之一便是这两个蠕虫的代码本身。WannaCry 具有多个错误（包括扫描功能不全），表明创建 WannaCry 的攻击者与那些创建 Nyetya 的攻击者存在技术水平的差异。这两种蠕虫之间的主要差异表现为恶意软件的交付方式、恶意软件使用的传播方式，以及发布攻击者的任务目标。

交付

两个恶意软件系列所使用的交付机制有显著差异。WannaCry 的交付很简单：找到或建立易受攻击的 SMBv1 服务器，感染它，并导致它扫描互联网并传播。Nyetya 的交付机制明显更先进。Nyetya 蠕虫背后的攻击者能够成功地破坏用于分布某个软件（该软件在特定地理区域内广泛使用）的软件更新的服务器。正如我们的博客文章在此所述，攻击者之所以选择暴露或公布他们在目标地理区域内有此级别的访问权限进入系统，可能是因为他们有更多能在将来使用的类似功能。

传播

Nyetya 使用的传播机制与 WannaCry 所用的功能相似，包括 Nyetya 可用的几种方法，以及入侵证书。Nyetya 不只是简单地依靠 SMBv1 漏洞，还具备利用 PSExec 和 WMI 的能力。此外，当 WannaCry 被设定为蔓延到整个内部和外部网络并包含代码级别问题与导致性能缺陷的扫描功能时，Nyetya 只在感染环境的内部传播。这样做的目的可能是为了将恶意软件的影响范围限制于被攻击的特定区域或组织。

任务目标

这两种恶意软件的怀疑任务目标也不相同。对于 WannaCry，似乎合理地结论为简单拙劣地执行该恶意软件，试图通过大规模部署勒索软件来创造收入。其中包含被称为“killswitch”的指定控制恶意软件传播的单个域名，使得安全研究人员能够轻松地停止此恶意软件的传播，说明该软件程序员的真实复杂程度不高。攻击者后来来自 WannaCry 比特币钱包的比特币行为似乎也进一步支持这一假设。而 Nyetya 的目标任务则表现为造成目标环境中的操作中断。Nyetya 擦除被感染系统的硬盘部分并不提供恢复擦除流程的机制似乎也支持这一假设。

如果采取其他措施，将会是什么结果？

返回到信息安全的本始，这应该是防止或严重限制这两种威胁的影响的有效手段。

修补

对于大多数组织而言，避开 WannaCry 并不困难。只需安装与 MS17-010 相关联的安全更新，就能成功地阻止 WannaCry 感染。关于一些组织仍在大肆使用的旧版系统，这种方法是否可行存在一些争议。WannaCry 针对 MS17-010 漏洞的漏洞利用攻击代码的执行甚至未在大多数的这些系统上正常运行。Microsoft 最终同样针对这些旧版操作系统发布了 MS17-010 更新。

正如安全社区多年以来一直的强调内容，有效的补丁管理是安全控制的关键，组织仅只需要在其环境内执行。我们已经看到很多攻击之所以会成功，就是因为组织未能对其环境进行修补。对于攻击者来说，零日漏洞的可靠漏洞利用通常非常昂贵，但修补公共漏洞却非常便宜。如果攻击者能够找到更便宜的方法来实现其任务目标，他们通常不会使用零日漏洞。作为一个组织，如果环境内的系统所受的大多数攻击是正被利用的零日漏洞，这是个好征兆，表示其他一切执行有效，它意味着攻击者有可能无法找到另一个更便宜的攻击途径破坏防御。

最基本的功能

仅限实现系统功能所需的系统执行他们的预定的角色或功能。Microsoft 建议如果 SMBv1 非必需，可以将其禁用。同样，限制系统和服务的访问权限是安全控制另一个关键。即使系统在使用 SMBv1，也很少需要暴露在互联网等恶意网络环境中。利用基于主机的防火墙，像 Windows 操作系统的内置防火墙甚至内部网段的防火墙都是控制这些服务的访问权限的另一种方式。

最少的权限

限制使用类似 WMI 和 PSExec 的管理工具以及系统管理正在执行系统管理功能的那些系统。监控这些工具在组织的整个网络中的使用，虽然不一定是预防性的安全控制，但可用于快速识别受损系统，并使组织能够启动适当的事件响应流程。

系统和网络监控

计算机蠕虫的传播速度通常非常迅速，使得他们在大多数环境中声响非常大。在这两种情况下，该蠕虫将启动扫描功能，以确定要传播到新的主机。针对环境的服务扫描或通过网络上的单一系统在短时间内连接到多个系统的尝试进行监控，能够较早地识别被破坏的系统，以便在问题未给组织造成更大影响之前将其解决。

网络分段

甚至在不可能安装与 MS17-010 相关联的安全更新的环境中，网络分段也是防止攻击成功，或者限制成功攻击组织的其他环境的可能影响的好方法。在通信路径中创建“阻塞点”是一个很好的方式，它不仅能成功限制危害的影响，还能提供理想的位置部署基于网络的安全控制，成功地防止第一线发生的攻击。如先前所述，最基本的功能的原理会命令分别在这些阻塞点部署访问控制，以限制仅与系统服务其在企业内的角色真正需要的内容进行通信。平面网络虽然易于管理和维护，但在减轻像 WannaCry 或 Nyetya 攻击的影响的方式上几乎没有作用。

流程和政策

当发生意外情况时，组织有既定的政策和流程确保他们作好准备，能恰当和有效地作出反应至关重要。灾难恢复和业务连续性计划使组织能够从意外的系统停机或灾难中迅速恢复。要使这些流程持续保持有效，组织必须做到不但计划到位，而且必须随时对其进行测试和验证，确保它们继续满足组织的需求。您的组织能够足够快速地从系统停机中恢复以满足其业务需求吗？备份策略有发挥作用吗？（比如，单独使用备份能够进行恢复吗？）这些需要随时会发生变化，测试这些流程有助于确保在系统中断或发生灾难之前它们仍然有效。事件响应是另一个流程示例，必须到位并且通过使用狩猎练习、桌面练习和逐步指导进行定期测试。这是真正确保事件响应团队具备在环境内发生严重事件时能够有效反应所需的知识和工具的唯一途径。

结论

WannaCry 和 Nyetya 是导致全球许多组织受到恶意软件严重影响的两个事件示例。这些事件强调了需要从信息安全的角度回到本始，确保组织受到充分的保护，并且针对响应可能在其环境中发生的破坏性事件作好充分的准备。计算机蠕虫几十年来一直存在，并非新鲜事物。制定到位、健全、分层次的深度防御战略将确保组织能够防止广泛的系统停机，并当其环境内部发生系统破坏时进行检测和响应，将这些事件可能产生的影响最小化。

美国国家标准和技术研究所 (NIST) 已发布特别发表刊物 800-53《联邦信息系统和组织的安全与隐私控制》，其中针对推荐最佳实践和如何选择在联网环境中建立良好健全的防御体系结构要实施的安全控制提供了全面的指导。本指南可在此获取。

发布者：EDMUND BRUMAGHIN；发布时间：11:05
标签：防御、NYETYA、勒索软件、WANNACRY、蠕虫