防范 WannaCry 和 Petya

2017 年 5 月，出现了一种基于 WannaCry 恶意软件系列的大规模网络攻击。WannaCry 利用了 Microsoft Windows 某些版本中的漏洞。据估计，在攻击高峰期，全球有 150 个国家/地区的 30 多万台计算机受到感染，攻击者要求每台计算机都支付赎金。

最初的攻击途径不得而知，但攻击性蠕虫助长了恶意软件的传播。Microsoft 在 3 月份发布了一个关键修补程序，用于删除受支持的 Windows 版本中的内在漏洞，但许多组织尚未有效应用此修补程序。

运行不受支持的 Windows（Windows XP，Windows Server 2003）版本的计算机无法获取有效的修补程序。在受到 WannaCry 攻击后，Microsoft 针对 Windows XP 和 Windows Server 2003 发布了特殊的安全修补程序。

大约六周后，另一次网络攻击也利用了同一个漏洞。Petya 没有造成像 WannaCry 那么大的影响，但这两次攻击都暴露了在关键领域继续使用旧版本或不受支持版本的操作系统的巨大风险，以及一些组织不遵循有效修补更新过程所面临的风险。《McAfee Labs 威胁报告：2017 年 9 月》中详细分析了这两次攻击。

防御 WannaCry 和 Petya 的策略和步骤

- **备份文件：**防范勒索软件最为有效的步骤是定期备份数据文件并检查网络还原程序。
- **培训网络用户：**与其他恶意软件相似，勒索软件通常通过使用电子邮件附件、下载或跨脚本 Web 浏览的钓鱼攻击感染系统。
- **监控和检查网络流量：**该步骤将帮助确定与勒索软件行为相关的异常流量。
- **使用威胁情报数据源：**该做法有助于更快地检测威胁。
- **限制代码执行：**勒索软件通常设计成在广为人知的操作系统文件夹下运行。如果由于访问控制而导致勒索软件无法访问这些文件夹，则可阻止恶意数据加密。
- **限制管理和系统访问：**一些类型的勒索软件设计成使用默认的帐户来执行其操作。对于这种类型的勒索软件，重命名默认用户帐户和禁用所有不必要的有权限和无权限帐户可加强保护。
- **删除本地管理权限：**根据管理权限阻止勒索软件在本地系统上运行，并阻止其传播。删除本地管理权限也可阻止对于勒索软件作为加密目标的任何关键系统资源和文件的访问。
- **其他权限相关的做法：**考虑限制用户写入能力、阻止从用户目录执行、将应用程序列入白名单以及限制对于网络存储或共享的访问。一些勒索软件需要特定文件路径的写入访问权限方可安装或执行。限制对于少数目录的写入权限（例如“我的文档”和“我的下载”）可阻止一些勒索软件变体。也可通过从这些目录中删除执行权限来阻止勒索软件可执行文件。许多组织使用有限的应用程序集来开展业务。通过对应用程序保持纯白名单策略，可阻止含有勒索软件的未列入白名单的应用程序执行。另一个与权限相关的做法是在诸如网络文件夹的共享资源上要求登录。
- **维护和更新软件：**防范勒索软件的另一个重要基本规则是维护和更新软件，尤其是操作系统补丁，以及安全和防恶意软件的软件。

特别重要的是减少受攻击面，尤其是钓鱼攻击的受攻击面，这种攻击是勒索软件最常用的技术之一。对于电子邮件，请考虑以下办法：

- **筛选电子邮件内容：**确保电子邮件通信安全是一个关键步骤。如果网络用户收到的可能包含潜在恶意和不安全内容的垃圾邮件减少，成功攻击的可能性也将降低。
- **阻止附件：**附件检查是减小攻击面的重要步骤。勒索软件通常以可执行附件的形式提供。可以颁布政策，规定某些文件扩展名不能通过电子邮件发送。可通过沙盒解决方案分析这些附件，并由电子邮件安全工具将这些附件删除掉。

McAfee 产品如何防御 WannaCry

McAfee Network Security Platform (NSP)

McAfee NSP 响应迅速，可以防止网络中的资产遭到利用，并提供妥善保护。McAfee NSP 团队致力于为关键事务开发和部署用户定义的签名 (UDS)。在 WannaCry 攻击的 24 小时内，McAfee 为客户开发并上传了多个 UDS，供他们部署在自己的网络传感器上。在这种情况下，UDS 明确针对的是利用工具，如 EternalBlue、Eternal Romance SMB Remote Code Execution 和 DoublePulsar。同时，McAfee 还发布了可能会被添加到黑名单中的相关危害指标，用于阻止与原始木马病毒相关的潜在威胁。

单击此处阅读有关 NSP 签名的更多信息。

McAfee Host Intrusion Prevention (HIPS)

具有 NIPS 签名 6095 的 McAfee HIPS 8.0 可防御 WannaCry 的所有四种已知变体。有关这些配置的最新信息，请参阅 KB89335。

自定义签名 #1：WannaCry 注册表阻止规则

使用标准子规则
规则类型 = 注册表
操作 = 创建、修改、更改权限参数，包括注册表项
注册表项 = \REGISTRY\MACHINE\SOFTWARE\WanaCrypt0r
可执行文件 = *

自定义签名 #2：WannaCry 文件/文件夹阻止规则

使用标准子规则
规则类型 = 文件
操作 = 创建、写入、重命名、更改只读/隐藏属性，参数包括文件
文件 = *.wnry
可执行文件 = *

McAfee Endpoint Protection (ENS) 和 McAfee VirusScan Enterprise (VSE) 自适应威胁防护配置

McAfee Endpoint Security 10.5 — 自适应威胁防护

具有自适应威胁防护 Real Protect 和动态应用程序遏制可以 (DAC) 功能的 McAfee Endpoint Security 10.5 可针对 WannaCry 的已知或未知攻击提供保护。

- 在自适应威胁防护—选项策略中配置以下设置：
  - 规则分配 = 安全性。(默认设置为“平衡”。)
- 在自适应威胁防护—动态应用程序遏制策略中配置以下规则：
  - 动态应用程序遏制—遏制规则

请参阅 KB87843：ENS 动态应用程序遏制规则列表和最佳做法，并根据所述将推荐的 DAC 规则设置为“阻止”。

McAfee Endpoint Security 10.1、10.2 和 10.5 — 威胁防护

具有 AMCore 内容版本 2978 或更高版本的 McAfee Endpoint Security 10.x 威胁防护可针对 WannaCry 的所有四种当前已知变体提供保护。

McAfee VirusScan Enterprise 8.8

具有 DAT 内容版本 8527 或更高版本的 McAfee VirusScan Enterprise 8.8 可针对 WannaCry 的所有四种当前已知变体提供保护。

McAfee Endpoint Security (ENS) 保护和 McAfee VirusScan Enterprise (VSE) 访问保护主动措施

McAfee ENS 和 McAfee VSE 访问保护规则将阻止创建 .wnry 文件。该规则停止加密例程，创建包含 .wncryt、.wncry 或 .wcry 扩展名的加密文件。对 .wnry 文件实施阻止策略后，不必再对其他加密文件类型实施阻止策略。

阅读有关 McAfee VSE 访问保护规则配置的更多信息。

配置终端安全系统以防止 WannaCry（包括未来未知变体）加密文件。

不使用 McAfee ENS 自适应威胁防护安全的客户，可能无法收到防御尚未发布的变体的 McAfee 自定义内容。我们推荐使用最小的刷新间隔来配置存储库更新任务，以确保在 McAfee 发布新内容后及时应用。

可以使用 McAfee VSE/ENS 访问保护规则或 McAfee HIPS 自定义规则配置针对加密例程的其他防御措施。有关这些配置的最新信息，请参阅 KB89335。

McAfee VSE 和 McAfee ENS 访问保护规则，以及 McAfee HIPS 客户签名将阻止创建 .wnry 文件。

该规则阻止加密例程，创建包含 .wncryt、.wncry 或 .wcry 扩展名的加密文件。

通过对 .wnry 文件实施阻止策略后，不必再对其他加密文件类型实施阻止策略。

有关这些配置的最新信息，请参阅 KB89335（McAfee 注册客户可访问）。

McAfee Advanced Threat Defense (ATD)

McAfee ATD 机器学习可在“中等严重性”分析中识别示例。

McAfee ATD 已经观察到以下内容：

行为分类：

- 模糊文件
- 传播
- 通过外壳代码利用
- 网络传播

动态分析：

- 触发勒索软件行为
- 加密文件
- 创建并执行可疑脚本内容
- 如木马宏植入程序等行为

从出现 WannaCry 攻击到目前为止，McAfee ATD 已经观察到 22 个进程操作，包括 5 个运行时 DLL、58 个文件操作、注册表修改、文件创建 (dll.exe)、DLL 注入和 34 个网络操作。

McAfee Web Gateway (MWG)

McAfee Web Gateway (MWG) 是 Web 代理的产品系列（设备、云和混合），可通过 Web (HTTP/HTTPS) 使用多个实时扫描引擎针对所提供的 WannaCry 变体提供及时防护。

当通过代理处理 Web 流量时，可通过 McAfee Global Threat Intelligence (GTI) 信誉和防恶意软件扫描阻止已知变体。

MWG 中的 Gateway Anti-Malware (GAM) Engine 通过本身对文件、HTML 和 JavaScript 进行的行为仿真过程，有效防范使用签名尚未识别的变体（“零日”威胁）。仿真程序通过机器学习模型定期馈送情报。在处理流量时，GAM 与 GTI 信誉和防恶意软件扫描一起运行。

同时运行 MWG 和 ATD 可进一步进行检查，并实现有效的防护和检测方法。

McAfee Threat Intelligence Exchange (TIE)

McAfee Threat Intelligence Exchange (TIE) 可进一步增强客户的安全状态。凭借结合 ENS、VSE、MWG 和 NSP 的信誉判定能力，TIE 可使用任何集成的媒介快速共享与 WannaCry 相关的信誉信息。通过提供使用 GTI 进行全球信誉查询的能力，TIE 还可使集成产品在执行勒索软件负载之前立即做出决定，从而利用 TIE 数据库中缓存的信誉。

作为一种终端保护，可从任何相关变体中进行检测并将信誉分数更新到 TIE，这种全面的方法通过将此信息传播到与 TIE 集成的所有终端来延长保护期限。威胁情报的这种双向共享可使用 MWG 和 NSP 功能进行重复。因此，当潜在威胁企图渗入网络或 Web 时，MWG 和 NSP 将提供保护和检测，并与 TIE 共享此信息以保护终端 — 及时保护企业，不再需要针对环境中的潜在“第一感染源”进一步执行识别的变体。

McAfee 产品如何防御 Petya

McAfee 通过使用 McAfee Advanced Threat Defense 中可用的 Real Protect Cloud 和动态神经网络 (DNN) 分析技术进行高级恶意软件行为分析的形式，提供针对最初的 Petya 攻击的保护。

ATD 4.0 推出了一种利用半监督学习来使用多层，反向传播神经网络 (DNN) 的全新检测功能。DNN 查看恶意软件执行的某些功能以得出肯定或否定的判决，从而确定代码是否是恶意的。

无论是在独立模式下还是连接到 McAfee 终端或网络传感器，ATD 都会将威胁情报与沙盒行为分析和高级机器学习进行相结合，以提供高度适应的零日保护。Real Protect 是 Dynamic Endpoint 解决方案的一部分，而且还可以在不需要签名的情况下使用机器学习和链接分析防御恶意软件，并为 Dynamic Endpoint 和其他 McAfee 生态系统提供丰富的情报。Real Protect 结合动态应用程序遏制可针对 Petya 尽早提供保护。

McAfee 的多种产品可提供额外的保护，以遏制攻击或防止进一步执行。

McAfee Endpoint Security

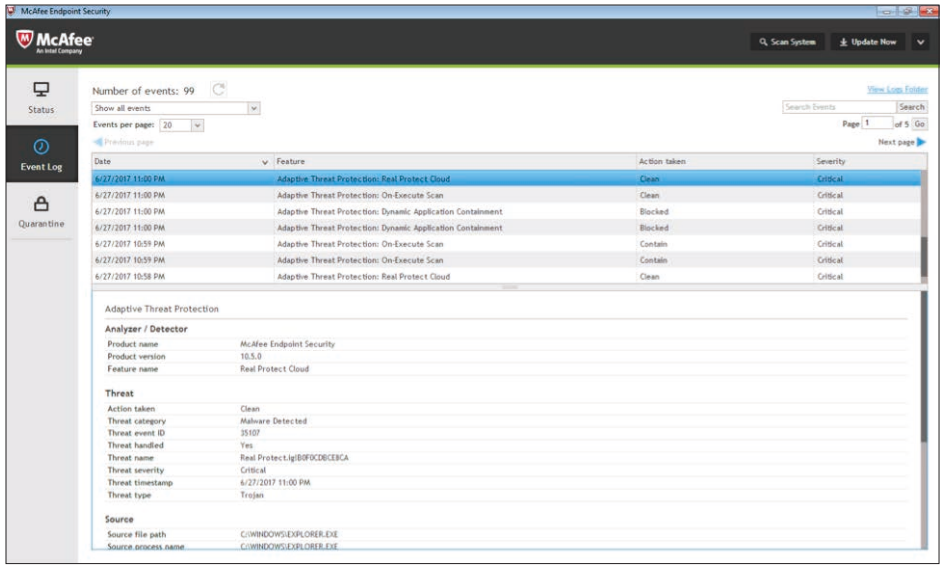
威胁预防

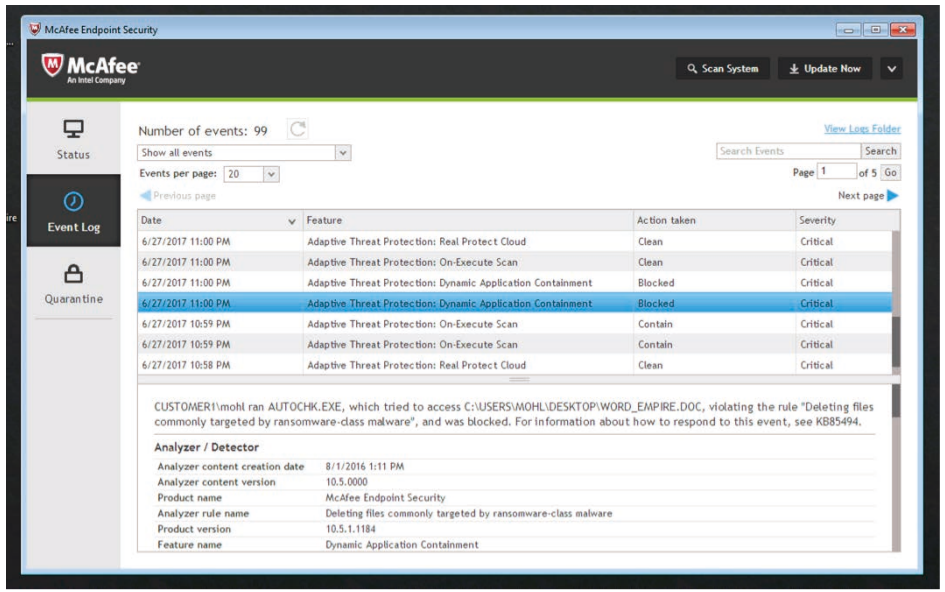
- 具有 McAfee Global Threat Intelligence 和按访问级别策略（敏感度级别设置为“低”）的 McAfee Endpoint Security 可防御已知的示例和变体。
- 请参阅 KB74983 了解推荐的 McAfee GTI 文件信誉设置的更多信息；请参阅 KB53735 了解更多信息。
- 具有 GTI 的 McAfee Threat Intelligence Exchange 可防御已知的示例和变体。

使用 McAfee ENS 10 的系统可同时使用签名和威胁情报防御已知的示例和变体。

自适应威胁防护

- 自适应威胁防护 (ATP) 具有在“平衡模式”(“自适应威胁防护\选项\规则设置”中的默认值) 下配置的规则分配，可防御 Petya 勒索软件的已知和未知变体。
- ATP 模块利用多层高级防护和遏制来防御这种未知的威胁：
  - ATP Real Protect Static 使用客户端预执行行为分析，在未知的恶意威胁启动之前对其进行监控。
  - ATP Real Protect Cloud 使用云辅助机器学习来识别和清除威胁，如右上所述。
- ATP 动态应用程序遏制 (DAC) 成功遏制威胁并防止发生任何潜在的损害 (DAC 事件如右下所述)。





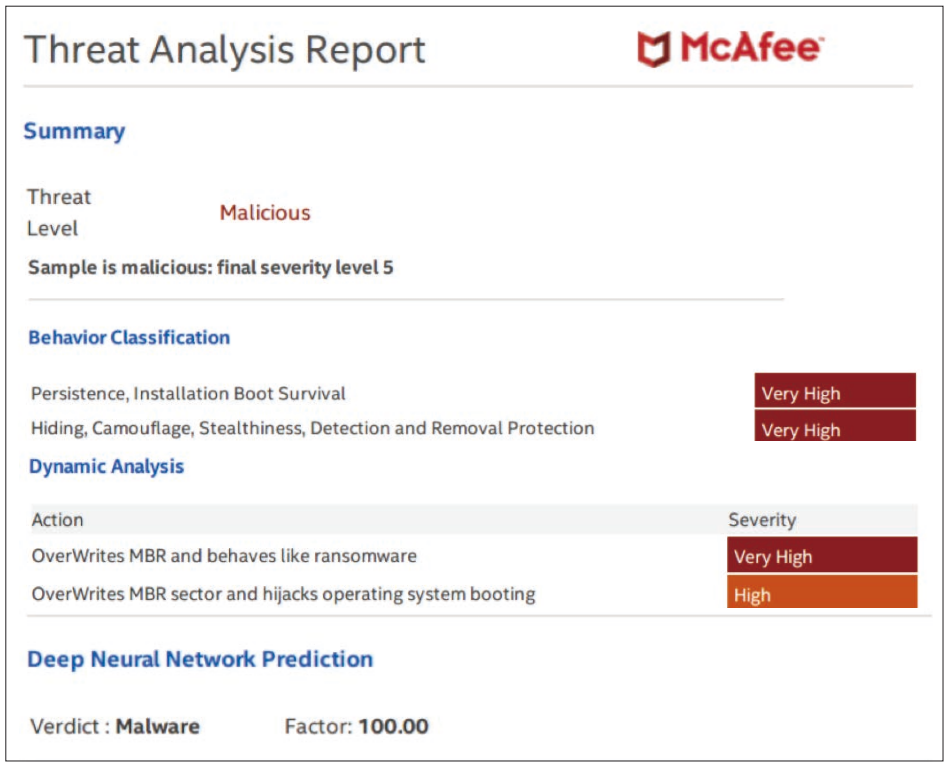
McAfee Advanced Threat Defense

- 具有深层神经网络和动态沙盒的 McAfee Advanced Threat Defense 4.0 可识别威胁，并主动更新网络防御生态系统。（见下文。）

McAfee Enterprise Security Manager

McAfee Enterprise Security Manager (ESM) 是一种安全信息和事件管理解决方案，提供切实可行的情报和集成，以便对威胁进行优先级划分、执行调查并作出响应。适用于 McAfee ESM 的 Suspicious Activity Content Pack 和 Exploit Content Pack 已经使用 WannaCry 特定的规则、警报和监视列表进行更新，因此您可以找到并识别可能的感染。此外，这些更新也将有助于防御 Petya。可在 McAfee ESM 控制台中免费下载这两个包。McAfee ESM 中的默认关联规则还可以提醒用户提高水平 SMB 扫描的级别。

与 WannaCry 类似，Petya 攻击为安全运营中心分析师带来了一个学习机会。了解和自动化这些最佳做法将有助于安全从业人员处理下一次快速攻击。



McAfee Web Gateway

McAfee Web Gateway (MWG) 是 Web 代理的产品系列(设备、云和混合),可通过 Web (HTTP/HTTPS) 使用多个实时扫描引擎针对所提交的 Petya 变体提供及时防护。当通过代理处理 Web 流量时,可通过 GTI 信誉和防恶意软件扫描阻止已知变体。

MWG 中的 Gateway Anti-Malware Engine 通过 GAM 对文件、HTML 和 JavaScript 进行的行为仿真过程,有效防范使用签名尚未识别的“零日”变体。仿真程序通过机器学习模型定期馈送情报。在处理流量时,GAM 与 GTI 信誉和防恶意软件扫描一起运行。

同时运行 MWG 和 ATD 可进一步进行检查,并实现有效的防护和检测方法。

McAfee 产品使用 DAT 文件

McAfee 发布了 Extra.DAT,以包含 Petya 的涉及范围。并且,McAfee 还发布了紧急 DAT,以包含此威胁的涉及范围。随后发布的 DAT 将会包含相关的涉及范围。可通过知识中心文章 KB89540 获取最新的 DAT 文件。

延伸阅读

可在知识中心文章 KB89335、KB87843、KB74983、KB53735 和 KB89540 中找到经常更新的技术详细信息。

北京市东城区北三环东路 36 号
北京环球贸易中心 D 座 18 层,100013
电话:8610 8572 2000
www.mcafee.com/cn

McAfee 和 McAfee 徽标是 McAfee, LLC 或其分支机构在美国和/或其他国家/地区的注册商标或商标。其他商标和品牌可能是其各自所有者的财产。Copyright © 2017 McAfee, LLC. 3530_0917
2017 年 9 月