加强物联网设备安全刻不容缓

2016 年 10 月，攻击者针对 Dyn 托管的 DNS 基础设施发起成功的分布式拒绝服务 (DDoS) 攻击，《McAfee Labs 威胁报告：2017 年 4 月》这一报告对此主题进行了深入分析。

此攻击使用的是 DNS 协议，因此安全技术很难区分合法通信量与恶意通信量。攻击和合法通信量来自全球数百万 IP 地址，导致问题更加错综复杂。

此类 DDoS 攻击的涌现，应归咎于不安全的物联网 (IoT) 基础设施。Dyn 攻击时所使用的 Mirai 恶意软件利用了各种不安全的物联网设备，比如视频记录器、打印机、监控摄像头、致冷器、自动调温器等。一旦一个物联网设备受到感染，恶意软件就会将病毒传播到其他物联网设备，形成“僵尸网络”，然后使用其聚集的处理能力执行 DDoS 攻击。

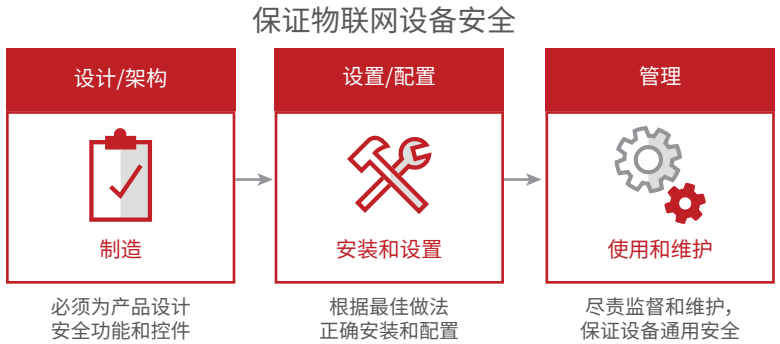
据 Dyn 安全团队称，在攻击高峰期间，Mirai 僵尸网络涉及数千万台恶意物联网设备。

断定网络设备是受到感染还是处于感染阶段并非易事，感染阶段可能包括代码爆发的初始阶段，也可能包括扩散或控制服务器通信到扩充僵尸网络以发起 DDoS 精心设计的攻击。不过，安全团队已提出建议，您可按照建议来确保物联网设备的安全，保护受信任的网络。

如何保证物联网设备安全

攻击者会沿袭最省力的途径来控制物联网设备。通常是破解安全性较弱的凭据。但他们也能应付安全性很强的凭据和其他安全控制。我们发现许多攻击向量均可用于实现此攻击模式。

McAfee 建议阻止已知利用，并且将来有望按不同攻击者解决问题。执行以下三个步骤，从生产到报废，在各个阶段为物联网设备提供保护：



1. 在设计物联网设备时考虑安全性。

物联网制造商必须在确定产品的体系结构、接口和设计时要考虑到安全性。创建和测试基本安全概念和功能，比如数据和代码划分、受信任方之间的通信、正在使用的数据和闲置数据的保护以及用户身份验证。以后的产品将更强大、能够存储更多数据以及具有更多功能。这意味着，产品应具有安全更新、功能锁定、内部版本号验证、软件审查以及遵循行业最佳做法的默认配置等功能。一切始于制造商的坚持；要想日后坚不可摧，必须一开始就奠定坚实的基础。必须将硬件、固件、操作系统和软件设计为能够适应恶意环境的产品。物联网设备买方应在审查潜在交易时考虑到这一点。制造商在设计和架构物联网设备时考虑到安全性了吗？

2. 安全设置和配置。

大多数物联网设备在安装后都需要进行一些设置。设备身份和身份验证是此两步流程中的重要设置部分。坚持最佳安全做法的默认配置很重要，应使用户易于理解。规则不应允许使用默认密码，需要修补和更新才能签名，对数据加密以及仅保证网络连接安全。对于企业，限制网络访问，及时修补漏洞以及仅允许批准的软件运行，才对保证物联网设备安全有帮助。对于能够运行安全软件（比如防恶意软件）的小工具，入侵防护系统和本地防火墙可提升设备的防御姿态。此外，还应配置检测和遥测功能，以便检测系统何时遭受攻击，或者系统采用组织未指定的方式工作。必须为隐私、数据保留、远程访问、关键安全措施和吊销过程制订策略。

3. 应用适当的管理。

对于消费者所有的设备，他们必须自行保留如何管理设备的最终决定权。虽然制造商和在线服务提供商在设置过程中发挥着重要作用，但所有者必须保留设备用途控制权。设置与管理不同。例如，在安装家用摄像机过程中，为了获取最新补丁，甚至为了设置云存储，需要联系制造商。但消费者不希望由制造商来控制家用摄像机。他们不能在买方未授权的情况下操作设备。所有者必须保留打开或关闭其产品的权力，以及选择允许联系哪种在线服务的权力。此功能要求使用正确的用户身份和身份验证。允许共有的默认密码是不良做法，因为任何人都可以用管理员身份接管设备。想象一下这种情况：Microsoft Windows 的每个系统都附带有默认登录密码。那将会是一个安全梦魇，因为许多用户从不更改密码，攻击者可以用户身份登录。

首先，物联网系统必须能够验证其所有者的身份。此外，还必须扩展管理功能，让所有者能够设置限制、数据策略和隐私参数，使所有者的约束力超过任何潜在第三方供应商的约束力。应该在有签名安全更新可用时自动安装这些更新。了解设备的所有者应该能够为入站和出站连接、数据类型、端口和安全设置配置限制。可以推送到受信任系统或在本地查看的日志应捕获错误，以及意外活动和异常活动。对于某些设备而言，通过电子邮件或文本形式发送远程警告通知的系统是特别受欢迎的功能。最后，需要提供重置功能，以防遭受不可恢复的损坏或转让所有权。

保护物联网设备安全的可操作性策略和程序

- **研究物联网设备的安全跟踪记录。**购买物联网设备前，了解设备本身或设备供应商是否存在问题。通过互联网简单搜索即可了解。搜索查看联邦贸易委员会官网，了解之前实施的强制措施。通过简单的搜索即可发现，有一些企业不重视安全问题，也有一些非常重视。
- **及时更新所有物联网设备软件。**这是既简单又最有效的做法，通常能够消除漏洞，尤其是那些近期发现且备受关注的漏洞。请执行修补程序，并验证补丁是否已成功应用。

- **对于无法修补的物联网设备，需要降低风险。**您可以利用应用程序白名单实现此目的，白名单可以锁定系统并防止未经批准的程序执行。
- **使用防火墙或入侵检测系统将这些物联网设备与网络中的其他部分隔离。**禁用这些系统上的不必要服务或端口以减少可能的感染入口点的暴露。Mirai 会利用未使用的端口。
- **更改默认密码，并设置不易破解的密码。**默认和安全性不强的密码是物联网设备的两大安全隐患。养成良好的密码设置习惯，如使用长短语、特殊字符、混合大小写和数据。密码必须具有很强的安全性，不易被破解。
- **充分利用物联网安全设置。**一些物联网设备会提供高级配置，应该充分加以利用。特定物联网产品可能会提供分离网络，类似于主网络连接旁的来宾 Wi-Fi 网络。这只是其中一种功能，其他产品可能会提供更多功能。
- **使用安全的 Wi-Fi 网络连接物联网设备。**创建安全性很强的密码，并使用最新的安全协议，如 WPA2。
- **限制物联网设备的物理访问。**直接篡改设备也可能导致物联网设备被入侵。
- **禁用通用即插即用 (UPnP) 服务支持。**很多物联网设备支持 UPnP，这会让设备暴露在互联网中的位置，易受到恶意软件的感染。如果可以，禁用此功能。
- **定期重新启动物联网设备。**恶意软件通常存储在易失性存储器中，关闭再重启设备即可将其删除。

McAfee 如何保护系统和网络免受物联网设备攻击

除了前述可操作的物联网设备最佳做法以外，McAfee产品也可以帮助减轻物联网设备中的恶意软件感染风险，阻止僵尸网络的恶意活动。以下 McAfee 产品配置可帮助保证物联网设备安全，保护系统和网络免受物联网设备攻击：

McAfee VirusScan® Enterprise 8.8 或 McAfee Endpoint Security 10

- 保证 DAT 文件处于最新状态。
- 确保 **McAfee Global Threat Intelligence** (McAfee GTI) 已启用；McAfee GTI 可识别 6 亿多个唯一的恶意软件特征码。
- 建立访问保护规则以阻止恶意软件安装和负载：
  - 请参阅访问保护规则知识库文章：**KB81095** 和 **KB54812**。
  - 请参阅 McAfee VirusScan 8.8 Enterprise 的最佳配置实践：**PD22940**。
  - 请参阅 McAfee Endpoint Security 的最佳配置实践：**KB86704**。

McAfee Host Intrusion Prevention

- McAfee Host Intrusion Prevention 可用于防范恶意软件扩散。利用自定义 IPS 签名，您可以创建规则来阻止恶意软件执行的文件操作（创建、写入、执行和读取等）。

- 启用 McAfee Host Intrusion Prevention 特征码 3894：Access Protection—Prevent svchost.exe executing non-Windows executables（访问保护可阻止 svchost.exe 执行非 Windows 可执行文件）。
- 启用 McAfee Host Intrusion Prevention 签名 6010 和 6011 可立即拦截植入恶意代码。
- 利用以下两条子规则实现此目的：
  - 1）利用“Files”引擎和包含以下条件的子规则来创建自定义 IPS 签名：
    - Name: <插入名称>
    - Rule type: Files
    - 操作: Create, Execute, Read, Write
    - Parameters: Include - Files - <恶意软件路径/文件名>
      - 文件名必须包含路径。如果您想使用通配符表示路径，文件名开头请使用 “**\”或 “?:\”；如果您想使用通配符表示驱动器号，请使用“**\文件名.exe”或“?:\文件名.exe”。
      - 您不能使用包含“Files”参数的 MD5 哈希，则只能使用路径/文件名。
      - 您还可使用驱动器类型将路径限定为特定驱动器（例如，硬盘驱动器、CD、USB、网络和软盘）。
    - Executables: 可留空，除非您想将签名限定为执行文件操作的特定进程（例如，explorer.exe 和 cmd.exe 等）。
  - 2）利用“Program”引擎和包含以下条件的子规则来创建自定义 IPS 签名：
    - Name: <插入名称>
    - Rule type: Program
    - Operations: Run target executable
    - Parameters: <保留为空>
    - Executables: 可留空，除非您想将签名作为源可执行文件限定为特定进程（例如，您想阻止 explorer.exe 运行 Target Executable（如 notepad.exe））。
    - Target Executables: 定义要阻止执行的可执行文件属性（例如，如果您想阻止 notepad.exe 运行，可指定可执行文件的路径/文件名）。可通过一种或多种标准（如文件说明、文件名、指纹和签名者）来定义可执行文件。

McAfee SiteAdvisor® Enterprise 或 McAfee Web Protection

- 借助网站信誉来阻止用户使用分发恶意软件的站点或向用户发出警告。

McAfee Threat Intelligence Exchange 和 McAfee Advanced Threat Defense

- McAfee Threat Intelligence Exchange 策略配置：
  - 从观察模式开始：由于终端通过可疑进程发现，所以使用系统标记来应用 McAfee Threat Intelligence Exchange 实施策略。

- 清理：Known Malicious（已知恶意）。
- 拦截：Most Likely Malicious（很可能为恶意）的文件，拦截 Unknown（未知）文件可能会提供更好的防护，但也可能会增加初始管理工作负载。
- 对于 Unknown（未知）信誉级别和更低级别，Submit files to McAfee Advanced Threat Defense（将文件提交给 McAfee Advanced Threat Defense）。
- McAfee Threat Intelligence Exchange Server 策略：对于 McAfee Threat Intelligence Exchange 未识别的文件，接受 McAfee Advanced Threat Defense 提供的文件信誉。

- McAfee Threat Intelligence Exchange 人工干预：
  - 文件信誉强制实施（取决于操作模式）。Most likely malicious（很可能为恶意）：清理/删除。
  - Might be malicious（可能为恶意）：拦截。
- 企业（组织）提供的文件信誉优先于 McAfee GTI。
  - 您可以选择阻止某个不需要的进程，比如不支持或有漏洞的应用程序。
  - 将文件标记为 Might be Malicious（可能为恶意）。
- 或选择"测试"某个不需要的进程：
  - 将文件标记为 Might be Trusted（可能为被信任的文件）。

McAfee Advanced Threat Defense

- 检测功能：
  - 基于签名的检测：McAfee GTI 包含 6 亿多个特征码。
  - 基于信誉的检测：McAfee GTI。
  - 实时静态分析和模拟：用于无特征码的检测。
  - 自定义 YARA 规则。
  - 全静态代码分析：对文件代码实施逆向工程，以评估属性和功能集，并访问但不执行全分析源代码。
  - 动态沙盒分析。
- 创建其中可能会运行恶意软件的分析器配置文件：
  - 通用操作系统：Windows 7、Windows 8、Windows 10。
  - 安装 Windows 应用程序（Word 和 Excel）并启用宏。
- 将分析器配置文件接入互联网：
  - 很多样本运行 Microsoft 文档中的脚本，这个脚本进行出站连接并激活恶意软件。为分析器配置文件提供互联网连接可提高检测率。

McAfee Network Security Platform

- McAfee Network Security Platform 的默认策略中包含签名，用以检测可用来传输恶意软件相关文件的 TOR 网络。

- 与 McAfee Advanced Threat Defense 集成，可以防御各种攻击的新变体：
  - 在“高级恶意软件策略”中配置与 McAfee Advanced Threat Defense 集成。
  - 配置 McAfee Network Security Platform，以便将 .exe 文件、Microsoft Office 文档、Java 存档和 PDF 文件发送至 McAfee Advanced Threat Protection 以进行检测。
  - 验证 McAfee Advanced Threat Protection 配置是否在传感器级别应用。
- 更新回拨检测策略（以抗击僵尸网络）。

McAfee Web Gateway

- 启用 Web McAfee Gateway Anti-Malware 防恶意软件检测功能。
- 启用 McAfee GTI 的 URL 和文件信誉功能。
- 与 McAfee Advanced Threat Defense 集成以实现沙盒和零日检测。

VirusTotal Convicter：自动干预

- Convicter 是一种 Python 脚本，可由 McAfee® ePolicy Orchestrator® (McAfee ePO™) 自动响应系统触发，从而交叉引用由 VirusTotal 提供给 McAfee Threat Intelligence Exchange 的威胁事件文件。
- 可更改此脚本以参照其他 McAfee Threat Intelligence Exchange，例如 GetSusp。
- 如果达到了信任社区的阈值，此脚本会自动设置企业信誉。建议的确认阈值：30% 的供应商以及两家主要供应商必须认同此阈值。
- 过滤器：“Target file name does not contain（目标文件名不包含）：McAfeeTestSample.exe。”
- 这是一款社区支持的免费工具（McAfee 不支持）。

McAfee Endpoint Threat Defense and Response

- McAfee Endpoint Threat Defense and Response 可发现高级威胁并作出响应。该工具用于防御由 McAfee GTI、Dell SecureWorks 或 ThreatConnect 提供的威胁源时，可搜索到新威胁，并在这些威胁找到机会扩散之前将其扼杀。
- 自定义收集器可让您构建专用的工具来查找和识别与恶意软件危害相关的迹象。
- 满足特定条件时，用户可创建触发和反应来定义操作。例如，发现哈希或文件名时，可自动运行“删除”操作。

延伸阅读

白皮书: **More Confidence, Safety, and Security in the Digital World** (增强在数字世界的信心，提高安全和保障)

Best Practices for how to use Host IPS rules for a malware outbreak (使用 McAfee Host Intrusion Prevention 规则来应对恶意软件爆发的最佳实践)：**KB84507**

SIEM Orchestration. How McAfee Enterprise Security Manager can drive action, automate remediation, and increase situational awareness (SIEM 编制。McAfee Enterprise Security Manager 可如何推动客户活动，自动进行补救，并提高客户的态势感知能力)：**PD24830**

白皮书: **Secure Beyond the Signature** (超越特征码的安全防护)

FAQs for McAfee Network Security Platform. Advanced Malware Detection McAfee Network Security Platform 常见问题解答)：高级恶意软件检测: **KB75269**

McAfee Web Gateway 产品手册。Web 过滤: **PD26339**

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