思科Stealthwatch让WannaCry无计可施！

原创 2017-05-18 思科联天下 思科联天下

博客作者： Hanna Jabbour

5 月 12 日星期五，互联网上爆发了一个极度危险的全新恶意软件威胁，让全球众多的计算机用户为其胆战心惊。**穷其源头，这一名为 “WannaCry” 的恶意软件原本是掌握在政府机构手中的一个秘密武器，后于一年前被未知攻击者窃取并泄露。**

思科行业领先的 Talos 威胁情报团队凭借一双火眼金睛，从众多威胁中发现了这一恶意软件，并确认了其威胁性。WannaCry 的初始版本通过一个恶意软件载荷在被感染的计算机上安装勒索软件。它会扫描 TCP 445 端口，以利用部分未打补丁的 Windows 计算机上存在的漏洞。与蠕虫病毒类似，WannaCry 能够在网络中传播，导致大规模感染。

本篇内容介绍了客户可以**如何利用思科安全解决方案来保护其网络和计算机**，以免受此恶意软件及其在未来数天、数周乃至数月可能生成的新变种的攻击。

感染检测

WannaCry 恶意软件的初始版本利用 Server Message Block（SMB）协议来感染网络上运行 Microsoft Windows 操作系统的计算机，并进行传播。**借助 Cisco Stealthwatch，网络操作员可以监控网络内的 SMB 活动。**

- **Cisco Stealthwatch 具有内建的报告功能**，可以专门跟踪和报告内部主机计算机与互联网上主机之间的 SMB 流量，此类流量是表明系统感染 WannaCry 的一个重要迹象。
- WannaCry 恶意软件还使用 SMB 流量进行内部传播。**Stealthwatch 会检测到相同子网内主机使用的 SMB 流量**，并将其判定为可疑活动。
- **Stealthwatch 会针对可疑 SMB 活动发出多个提醒。**它尤其会关注针对大量不同主机发起的激增的 SMB 流量和 SMB 联接。这一信息可帮助确定主机是否被 WannaCry 感染。
- **Stealthwatch 还能够检测并报告到 Tor 网络、Bogon IP 地址和已知命令与控制主机的联接。**
  - 借助持续更新的威胁情报源，**Stealthwatch 也能够检测到主机与 Tor 网络和 Bogon IP 地址的通信。**这使得安全人员能够发现任意联接到互联网上可疑主机的内部 IP。

传播检测

WannaCry 恶意软件的初始版本会在网络内部横向传播（从主机到主机），以试图感染尽可能多的主机。在恶意软件触发其勒索软件载荷前，这一传播机制就已经开始。**Stealthwatch 能够检测到横向移动事件，尤其是相同子网内系统间的此类移动。**

- 任意侦察和扫描活动，尤其是相同子网内的系统间的此类活动，都会被 Stealthwatch跟踪到。
- Stealthwatch 蠕虫传播检测报告功能可以跟踪并关联成功联接到外部命令与控制主机的扫描活动。WannaCry 与其他蠕虫病毒均有着类似的一致活动。

关联

思科 Stealthwatch 将关联在特定主机计算机上观察到的不同活动，并根据每次观察所得的数字评分将该 IP 判定为可疑。之后 Stealthwatch 会针对每个主机 IP 地址，基于一个指数累积这些评分，然后发出名为 “威胁指数”（Concern Index）的提醒。威胁指数数值越高，表明主机参与恶意活动的可能性越大。

确定范围和规避威胁

通过使用思科 Stealthwatch Management Center 和仪表板，您可以轻松建立一份简单的报告，列出所有存在可疑活动和可能被感染的系统。借助集成的思科身份服务引擎（ISE），之后您可以隔离可疑计算机，避免 WannaCry 进一步传播，直至威胁被修复。

阻止 WannaCry 传播

WannaCry 在互联网上大肆扩散，我们预计在未来几年还将会看到更多变种。**利用 Stealthwatch 无处不在的渗透力和高级分析功能，您将可以尽早检测到 WannaCry 活动，阻止其在您的环境中进行传播。**

思科 Stealthwatch 介绍

思科 Stealthwatch 可提供行业领先的网络可视性和安全情报，帮助提高威胁检测、事件响应和调查分析的速度和精确度。该系统能够利用 Netflow 和现有基础设施中的其他态势感知数据，以快捷高效的方式将整个网络转化为一个传感器网。它通过基于行为的自动化学习和关联建模分析，能够快速检测各种异常流量和行为，包括零日恶意软件、分布式拒绝服务（DDoS）攻击、内部威胁和高级持久性威胁（APT）、以及网络分段访问违规等。

Stealthwatch 的管理界面十分直观、简洁，它通过单一视图展示流量在网络中的横向移动，同时集成了思科 Talos 的全球信息安全情报，为用户提供一个简单、精致且功能强大的平台，全面增强企业可视化、安全分析、高级威胁感知和事件响应调查的能力。

点击 “阅读原文” ，

利用 Stealthwatch 更快地检测威胁！

阅读原文