Cisco WSA勒索软件检测功能和AMP集成验证

目录

问题

我们询问思科安全网络设备(WSA)是否为Triple X勒索软件提供特定签名或检测功能。此问题还包括请求澄清如何验证高级恶意软件防护(AMP)与思科Talos威胁情报之间的集成在WSA平台上是否正常运行。

环境

- 思科安全Web设备(WSA)
- 高级恶意软件防护(AMP)集成
- 思科Talos威胁情报集成
- Web信誉和URL过滤(WBRS)
- 防恶意软件扫描引擎(Webroot、McAfee、Sophos)
- 应用可视性与可控性 (AVC)

分辨率

思科安全Web设备不依赖于一个专门命名为Triple X Ransomware的专用签名。相反，WSA采用综合的多层安全架构，利用各种检测技术来识别和阻止勒索软件威胁，包括Triple X勒索软件变体。

WSA检测方法

WSA平台使用以下检测技术保护勒索软件：

- 模式匹配算法
- 启发式分析
- 仿真技术
- 与思科Talos威胁情报集成的高级恶意软件防护(AMP)
- Web信誉和URL过滤(WBRS)
- 多个防恶意软件扫描引擎，包括Webroot、McAfee和Sophos
- 应用可视性与可控性 (AVC)

这些检测功能会随着每隔几分钟部署的新规则不断更新，以确保防御新兴威胁。

验证AMP和Talos集成

要确认高级恶意软件防护(AMP)与思科Talos威胁情报之间的集成在WSA上正常工作，管理员可以查看以下日志：

步骤 1：查看WSA访问日志

检查WSA设备上的访问日志，以验证AMP判定是否正在应用于下载的文件和Web请求。

步骤 2：检查AMP日志

查看AMP日志，确认恶意软件分析结果和正在处理的威胁情报数据。

步骤 3：验证WBRS得分

确保Web信誉(WBRS)分数已填充且与日志中的Web请求相关联。

如果AMP判定结果和WBRS得分在日志中填充和实施，这表示AMP和Talos集成工作正常，并提供基于威胁情报的实时决策。

原因

这是有关WSA勒索软件检测功能的信息请求，而不是需要故障排除的技术问题。此调查源于需要了解WSA如何防御特定勒索软件变体并验证威胁情报集成是否正常运行。

相关内容

- Cisco Secure Web Appliance的功能和优势
- 思科Talos威胁情报服务
- 思科安全Web设备数据表
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。