ThingPot: an interactive Internet-of-Things honeypot

本文提出并部署了一种名为 ThingPot 的新型物联网蜜罐。蜜罐技术模仿可能被攻击者利用的设备并记录他们的行为以检测和分析使用的攻击向量。

ThingPot 是同类产品中的第一个，因为它不仅关注物联网应用协议本身，还关注整个物联网平台。使用 XMPP 和 REST API 实现概念验证，以模仿飞利浦 Hue 智能照明系统。 ThingPot 已经部署了 1.5 个月，通过捕获的数据，我们发现了五种针对智能设备的攻击和攻击向量。 ThingPot 源代码以开源形式提供。

ThingPot模拟整个 IoT 平台，而不是单个应用层通信协议（例如 Telnet、HTTP、等等。）。蜜罐是通过模拟真实系统或协议来捕获和识别恶意活动的系统。它旨在被攻击，但由于它被放置在受控环境中，任何攻击都将被遏制。目前缺少一个模拟物联网平台的综合蜜罐。 ThingPot 填补了这个空白。

提供了 ThingPot 的概念验证 (PoC) 实现，它以开源代码的形式提供，重点关注 Philips Hue（智能灯系统）的 IoT 平台用例。该 ThingPot PoC 用例的两个重要组件是 XMPP 客户端和 REST API。对捕获的数据的分析表明，XMPP 部分只有很少的攻击者活动（甚至是通用扫描或请求）。事实上，没有通过 XMPP 路径对设备的直接请求。这支持了 XMPP 增加了攻击者到达物联网平台和设备的复杂性的说法。对 REST 日志数据的分析表明，物联网平台和设备已被攻击者注意到。特别是，发现了五种主要类型的攻击。一般来说，攻击者都在寻找 Philips Hue、Belkin Wemo、TPlink 等设备。特别是，他们有兴趣获取有关智能设备的信息并接管它们的控制权。通常，攻击者使用 TOR 网络来掩盖他们的真实来源。攻击者似乎更喜欢的方法是首先进行一般扫描以寻找漏洞，然后通过蛮力或模糊测试进行更有针对性和具体的攻击。还发现了专门针对飞利浦 Hue 的攻击。