

简译版

减轻供应链威胁

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	Tackling Supply Chain Threats		
原文作者	Ang Cui	原文发布日期	2018 年 10 月 24 日
作者简介	Ang Cui 是 Red Balloon Security 公司的创始人兼首席执行官。 https://www.darkreading.com/author-bio.asp?author_id=4941		
原文发布单位	Dark Reading		
原文出处	https://www.darkreading.com/iot/tackling-supply-chain-threats/a/d-id/1333102		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
免责声明	<ul style="list-style-type: none"> 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。 		

减轻供应链威胁

Ang Cui

2018 年 10 月 24 日

源自供应商的恶意软件是一种经常被忽视的威胁，这一点必须要改变。

如今，推动企业发展的各种技术产品，通常是通过高度多样化和复杂化的国际供应链生产的。无论是标准网络设备，还是人机界面或远程终端设备等更专业的设备，通常都是通过代工生产商（OEM）、芯片制造商、零件供应商、软件/硬件设计人员和外包生产工厂等密切合作、共同完成的。这使得设备安全性的审查变得更加困难，并且为恶意行为者提供了篡改设备硬件或软件的机会。

最近，特别是在《2019 财年国防授权法》（该法案禁止美国政府机关和承包商使用某些外国公司制造的电信设备）签署后，供应链风险受到了更多的关注。其他一些事件，如“幽灵”（Spectre）和“熔断”（Meltdown）计算机芯片漏洞，以及英特尔芯片组平台中隐藏的管理引擎漏洞，也凸显了关键技术产品中的漏洞给产业链下游的各个公司带来的连带风险。

固件威胁

在供应链威胁中，最严重的是基于固件的恶意软件。固件级威胁极难对抗，这是因为安全公司和企业最终用户通常缺乏对其代码的可见性，因此无法准确了解这些设备上运行的是什么。

几乎所有嵌入式设备都使用专有的操作系统，这些系统不接受用户访问和输入。在 Windows 和 macOS 设备中，用户可以直接管理和查看所有正在运行的进程；但是嵌入式设备与它们不同——制造商完全控制着这些设备和系统。在大多数情况下，最终用户无法自行管理和/或修复这些设备。如果不致电制造商请求服务，他们甚至无法安装安全补丁。

更麻烦的是，每台嵌入式设备的操作系统/固件通常是唯一的。与其他类型的设备（例如台式机、服务器和其他网络设备）相比，这些设备缺乏统一性和标准化。

这些威胁最有可能存在于固件的签名代码中，因此看起来就像是来自合法的供应链。植入程序、后门、远程网络通道、硬编码口令、调试模式等都有可能潜伏在看似合法的代码中。固件的无线更新也是一种风险，因为这种更新可能会被供应商恶意使用（或者只是执行不当），

容易受到感染。

持续性植入程序探测器

美国国土安全部科学技术局 (DHS S & T) 正在与私营企业合作新的项目, 旨在分析固件级设备并检测可能被恶意行为者利用的隐藏威胁。

DHS S & T 资助的一项技术是“持续性植入程序探测器”(Persistent Implant Finder ,PIF)。PIF 是一款私人开发工具, 能够自动解压和分析设备固件, 以发现恶意植入程序和漏洞。PIF 采用模块化设计, 可与多个固件分析器(包括设备系列专用分析器和通用分析器) 配合使用。这些固件分析器可以搜索各种隐藏的植入程序, 包括口令后门、活跃恶意软件 rootkit 和网络服务后门。PIF 工具能够与业界的网络漏洞扫描产品和服务兼容。

通过使用 PIF 恶意软件测试平台, 我们已经发现了多个可疑设备, 包括一款 PoS 设备和一款智能手表。在这些案例中, 可疑软件在出厂时就已经安装了, 这些可疑的恶意软件能够进行固件更新, 并将用户数据发送给未知方。

在 PoS 设备案例中, 预安装的应用主动连接到 Adups.com 域, 而该域先前已被发现泄露 Android 手机短信等敏感数据。PIF 在这个 PoS 设备中检测到的功能, 类似于 Kryptowire 公司在 2016 年报告 (该报告分析了 Adups 科技有限公司制造的, 用于低价 Android 手机的固件) 中提到的功能。这个预安装的 PoS 应用具有完全的 root 权限, 能够从设备中收集大量的用户数据, 并通过加密通道发送给外部服务器。

减轻供应链威胁

除非能够通过 PIF 等自动化工具或渗透测试解压和分析设备的固件, 否则各公司难以对抗源自供应商的恶意软件。这些公司应该考虑对他们依赖的技术进行深入的安全分析。

最重要的是, 各公司应该从信誉良好的制造商购买技术。这意味着公司应该避免通过经销商和其他第三方代理商或网站购买设备——这是因为如果使用这些渠道, 公司将更难确定设备的真实性、可靠性和安全性。需要更高安全级别的公司可能需要采取更进一步的措施, 只从总务管理局 (General Services Administration) 批准的供应商那里购买设备。

此外, 实施纵深防御方法十分重要。这些方法包括网络分段、员工访问控制、强口令策略、减少或消除远程访问、强加密, 以及通过物理隔离分割敏感网络。此外, 对第三方承包

商进行审计也很重要。

结论

源自供应商的恶意软件是一种经常被忽视的威胁。随着供应链的多元化以及国家支持的网络间谍活动的增多，公司必须了解他们面临的此类风险。

除非公司能够分析固件，否则他们很难防御固件级威胁。此外，公司还应使用分层的安全策略来降低整体风险。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进能力导向，依托下一代威胁检测引擎等先进技术和工程能力积累，研发了智甲、镇关、探海、捕风、追影、拓痕等系列产品，为客户构建端点防护、边界防护、流量监测、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报有机结合，推动客户整体安全能力建设的叠加演进。安天为网信主管部门、军队、保密、部委行业和关键信息基础设施等高安全需求客户，提供整体安全解决方案，产品与服务为载人航天、探月工程、空间站对接、大飞机首飞、主力舰护航、南极科考等提供了安全保障。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全厂商、IT 厂商选择安天作为检测能力合作伙伴，安天的威胁检测引擎为全球超过三十万台网络设备和网络安全设备、超过十四亿部智能终端设备提供了安全检测能力。

安天技术实力得到行业管理机构、客户和伙伴的认可，已连续五届蝉联国家级安全应急服务支撑单位。安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，为捍卫国家主权、安全和发展利益提供了有力支撑。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域的发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问：

<http://www.antiy.com> (中文)

<http://www.antiy.net> (英文)

安天企业安全公司更多信息请访问：

<http://www.antiy.cn>

安天移动安全公司 (AVL TEAM) 更多信息请访问：<http://www.avlsec.com>