

应对供应链安全问题

简译版

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 security head-on		
原文作者	约尔格·博尔切特博士 (Dr. Joerg Borchert)	原文发布日期	2022 年 2 月 17 日
作者简介	约尔格·博尔切特博士是 Trusted Computing Group 的总裁兼董事长。		
原文发布单位	Security Intelligence		
原文出处	https://www.helpnetsecurity.com/2022/02/17/supply-chain-threats/		
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		
摘要	供应链攻击不断增加,在过去的几个月中就发生了多起案例。全球供应链中的企业必须采用能够检测恶意软件和确定供应链完整性的工具和技术。越早发现威胁,威胁对供应链其他部分造成的损害就越小。全球供应链非常复杂,没有一家公司可以进行端到端的控制,每个参与者都需要尽自己的一份力量。在如此多的风险下,供应链的各个环节都应采取“安全第一”的方法。		
免责声明	本译文不得用于任何商业目的,基于上述问题产生的法律责任,译者与安天集团一律不予承担。		

应对供应链安全问题

约尔格·博尔切特博士

2022 年 2 月 17 日

针对供应链的威胁不断增加，这些威胁的规模、成本和复杂程度都达到了前所未有的水平，任何组织都很难防范。供应链威胁影响着全球广泛的行业和组织，包括军队、金融服务、消费电子、教育和医疗等等。确保供应链的安全并非易事，没有任何实体能够进行端到端的控制。此外，供应链涉及大量的阶段、组织和公司，难免会出现安全薄弱环节，而黑客正是利用了这些薄弱环节。

为了应对供应链安全问题，所有利益相关者都必须将安全问题放在首位，齐心协力加强保护措施并确保完整性。为了实现这一点，我们需要推出供应链行业标准，以定义、实施和维护供应链安全措施。

薄弱环节

任何一个安全措施不足的公司、阶段或流程，都会导致整个供应链更容易受到黑客攻击。尤其是跨多个国家的全球供应链，其规模和价值更加庞大，面临的风险也更大。如今的网络攻击更加复杂，很多黑客能够隐藏更长的时间，其恶意软件可以在不被发现的情况下广泛传播，造成重大的损害。对于黑客来说，供应链攻击已成为一种“从单一入口点攻击多个组织”的有效方式。一旦他们发现并利用供应链某个阶段的漏洞，就会影响从该点开始购买硬件或软件的每个组织。

恶意/假冒软件或硬件极其难以识别，许多最终用户甚至没有想过从第三方供应商处购买产品可能会带来风险。许多用户认为，只有供应商是合法的，其产品就是可靠和可信的。不幸的是，情况并非如此。欧盟网络安全局（ENISA）最近的一份报告发现，在针对供应商客户的攻击中，大约 62% 利用了客户对供应商的信任。因此，企业必须验证第三方代码和软件的安全性，以确保它们没有被篡改或操纵。

更糟糕的是，供应链中实施的许多安全方法是主观的，依赖于人工干预，例如目视检查，包括检查标签的位置，标签的颜色、大小或形状是否正确，以及验证序列号的真实性等。实施这些检查非常耗时且成本高昂。但是，许多组织不具备实施更复杂、更有效方法的知识

工具。

更高的安全标准

能够确保供应链完整性的行业标准，是防范攻击的最佳方法之一。如果所有组织都遵循这些开源技术和标准，就能够减少攻击者可以利用的漏洞。

今年，由多个领先技术成员领导，由 Trusted Computing Group 发布的《固件完整性测量（FIM）规范》就是一个很好的例子。在此之前，没有标准方法来确定网络中多个端点的安全状态。FIM 规范提供了官方权威指南和安全基线。企业可以根据该规范，在制造阶段确定设备的完整性，并在产品的整个生命周期中进行安全结果对比。这意味着在供应链的任何阶段，用户或制造商都可以确定设备的完整性。大型供应链涉及的阶段、组织和流程非常之多，因此跟踪设备的安全状态非常困难。对这些供应链来说，该规范尤其重要。

FIM 规范可以验证每个端点的完整性，以证明设备是可信任的。为此，必须在任何黑客有机会篡改供应链中的设备之前进行基线测量，这称为“参考完整性测量”（RIM）。RIM 通常在设备发货之前进行。一旦设备到达最终客户，客户就可以测量 FIM 并将其与 RIM 进行比较，以确认设备在供应链中的任何阶段都没有受到损害。

黑客安装的恶意软件在供应链中传播时极难检测。FIM 规范可以帮助解决这个问题，自始至终验证设备和网络的完整性。因此，FIM 和 RIM 的广泛采用能够提高设备的安全性。

改善供应链安全

供应链攻击不断增加，在过去的几个月中就发生了多起案例。全球供应链中的企业必须采用能够检测恶意软件和确定供应链完整性的工具和技术。越早发现威胁，威胁对供应链其他部分造成的损害就越小。全球供应链非常复杂，没有一家公司可以进行端到端的控制，每个参与者都需要尽自己的一份力量。在如此多的风险下，供应链的各个环节都应采取“安全第一”的方法。

安天简介

安天致力于全面提升客户的网络安全防御能力，有效应对安全威胁。通过 20 余年自主研发积累，安天形成了威胁检测引擎、高级威胁对抗、大规模威胁自动化分析等方面的技术领先优势，打造了面向服务器、云、虚拟化、容器和传统办公节点等提供全防御能力覆盖的智甲安全产品家族，满足客户对于包括终端杀毒、终端防护 (EPP)、终端检测与响应 (EDR)、云工作安全防护 (CWPP) 等系统安全层面需求；整合强化包括 ATID 威胁情报门户、追影沙箱和捕风蜜罐等产品在内的威胁情报板块产品，有效提升客户情报赋能和自主情报生产能力；基于流量产品探海有效应对客户对于网络威胁检测与响应 (NDR) 和网络流量分析 (NTA) 的安全需求，相关产品可以实现交叉联动，统一管理，形成面向从勒索软件到高级威胁 (APT) 的纵深安全防线。同时打造威胁对抗、威胁猎杀、威胁巡检服务三款主打安全服务，辅以平台支撑、快速到达的轻量级垂直响应服务，以运营模式有效支撑应对综合威胁对抗能力升级。

安天为网信主管部门、军队、部委、保密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，已连续七届蝉联国家级网络安全应急支撑单位。安天参与了 2005 年后历次国家重大政治社会活动的安保工作，获得杰出贡献奖、安保先进集体等荣誉称号；自 2015 年来，安天的产品与服务为包括载人航天、探月工程、空间站对接等历次重大航天飞行任务，以及大飞机首飞、主力舰护航、南极科考等重大任务提供安全保障支撑。

目前，安天的威胁检测引擎为全球超过一百万台网络设备和网络安全设备、超过三十亿部智能终端设备提供了安全检测能力，已经成为“国民级”引擎。

安天已发展成为以哈尔滨为总部基地，建有六地研发中心、两个控股子公司，参与一个国家工程实验室建设，拥有两个省级工程中心和重点实验室、一个博士后创新创业基地和多个高校联合实验室的集团化创新企业，同时在地多设有办事处和应急响应站，为客户提供全面的安全服务与技术支持。

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>