

简译版

2022 年云攻击会继续增加

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	The rising threat of cyber criminals targeting cloud infrastructure in 2022		
原文作者	瑞恩·谢尔德雷克 (Ryan Sheldrake)	原文发布日期	2022 年 1 月 13 日
作者简介	瑞恩·谢尔德雷克是 Lacework 公司 EMEA 地区现场首席技术官。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2022/01/13/threats-2022/		
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	受加密货币使用趋势、地缘政治、疫情等因素的影响，安全威胁一直在不断变化。因此，企业应对其威胁形势有一个清晰的认识，这一点很重要。本文详细分析了 2022 年的严重威胁。		
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。		

2022 年云攻击会继续增加

瑞恩·谢尔德雷克

2022 年 1 月 13 日

在网络安全的世界里，对抗威胁就像玩永无止境的、超先进的多维打地鼠游戏：新的威胁不断出现，而且其来源往往意想不到，防御者根本无法防御。

受加密货币使用趋势、地缘政治、疫情等因素的影响，安全威胁一直在不断变化。因此，企业应对其威胁形势有一个清晰的认识，这一点很重要。在下文中，我们将详细分析 2022 年的严重威胁。

Linux 和云基础设施将继续成为攻击目标

对于攻击者来说，有一个简单的计算方法来决定是否发动攻击。即，哪种攻击方法是：
a) 最简单的；b) 最有可能产生最大的回报。目前，这些问题的答案是基于 Linux 的云基础设施，这类云占整个云基础设施的 80% 以上。疫情期间，云的采用率大幅增加，针对云基础设施的攻击可能会成为一个大问题。

在过去的几个月里，BlackMatter、HelloKitty 和 REvil 等勒索软件组织利用 ELF 加密器，通过 ESXi 服务器攻击 Linux 系统。最近，PYSa 勒索软件组织也开始攻击 Linux 系统。同时，安全专家发现日益复杂的新型 Linux 恶意软件家族不断出现。要想对抗这些威胁，就要先发制人，这一点比以往任何时候都更加重要。

攻击者继续利用初始访问代理和加密劫持技术

虽说窃取信息是一个重要目标，但是许多云攻击纯粹出于经济动机。2022 年，网络犯罪分子会继续使用两种主要的货币化方法：挖矿和初始访问代理（IAB）。

这两种方法有其各自的优缺点。如果攻击者在云环境中未被发现，他们就可以通过加密劫持和挖矿，实时获取利润。在 IAB 方面，攻击者可能需要更长的时间才能获得他们想要的利润。但是，IAB 更能规避风险：攻击者在云环境中待多久都可以。只要挖矿仍然有利可图，加密攻击就会继续存在，执行攻击活动的初始访问代理也会继续存在。

内部人员威胁将会增加

去年，针对企业员工的黑客攻击急剧增加。通常，这些黑客会试图招募员工实施内部攻击。2021 年，科技行业的辞职人数创历史新高，这表明员工的不满情绪很高，员工离职比以往任何时候都更加严重，企业面临的风险不断增加。

黑客将继续攻击软件供应链

供应链攻击不像上述攻击那样频繁，但它们有可能造成更大的损害（2020 年的 SolarWinds 攻击就是一个很好的例子）。成功的供应链攻击能够“一箭多雕”。因此，我们认为 2022 年将会出现更多软件供应链攻击。

没有人可以精准预测即将发生的灾难。但是，通过分析过去的情况，我们可以做好准备来抵御最有可能发生的攻击。从这个意义上说，2022 年会与其他年份一样：网络犯罪分子将试图开发新的攻击手段，而防御者也会部署先进技术，通过最佳威胁分析来阻止他们。希望防御者能够获胜。

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，始终坚持自主先进的能力导向，依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累，研发智甲、探海、镇关、捕风、追影、拓痕等系列产品，为客户构建端点防护、流量监测、边界防护、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的有机结合，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能客户筑起可对抗高级威胁的网络安全防线。

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企业、IT 企业选择安天作为检测能力合作伙伴，目前，安天的威胁检测引擎为全球超过八十万台网络设备和网络安全设备、超过十七亿部智能终端设备提供了安全检测能力。安天的移动检测引擎获得国际知名测试机构颁发的 2013 年度权威评测奖项。

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（如 APT 组织）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，通过深度分析高级网空威胁行为体的作业能力，安天建立了以实战化对抗场景为导向的能力体系。

安天被行业管理机构、客户和伙伴广泛认可，已连续六届蝉联国家级安全应急支撑单位，是中国国家信息安全漏洞库六家首批一级支撑单位之一，亦是国家网络与信息安全信息通报机制技术支撑单位，国家信息安全漏洞共享平台成员单位。

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>