Rugang Chen

公有云威胁情报

公有云网络安全威胁情报（202202）

1. 概述 * 17个云上重点资产有漏洞攻击行为，包括某民主党派市级委员会、某县级中医院等云上重点单位。 * 随着俄乌冲突全面升级，我们发现有攻击者利用Docker Remote API未授权访问漏洞，对俄罗斯境内服务器发起拒绝服务(DoS)网络攻击。 * Apache APISIX本月爆出远程代码执行漏洞(CVE-2022-24112)，攻击者通过两种攻击方式可远程执行恶意代码。 本文主要通过360网络安全研究院 Anglerfish蜜罐视角，分析云上热门漏洞攻击细节，以及云上重要资产在公网上发起攻击的情况。 2. 云上资产对外扫描攻击 2月份我们共发现17个命中蜜罐节点的重要单位的云上资产，下表为其中一部分案例，如果需要更多相关资料，请根据文末的联系方式与我们联系。 IP地址 云服务商 单位名称 所属行业 IP所在省份 漏洞利用 扫描协议 39.105.204.* 阿里云 中国**** 市委员会 政府机关 北京 Redis RCE Redis

Mar 11, 2022 · 9 min read

公有云威胁情报

公有云网络安全威胁情报（202201）

1. 概述 2022年的第一个月份，虽然没有爆发新的热门漏洞，且随着越来越多设备的Apache Log4j2漏洞被修复，12月开始的Apache Log4j2漏洞爆发也进入尾声，相关攻击源数量明显减少。但是，Docker Remote API未授权访问漏洞、美国飞塔（Fortinet）FortiOS未授权任意文件读取漏洞等旧漏洞的云服务器攻击源IP数量突

然较12月大幅度增加。在第2部分，我们分析了这两个漏洞的攻击趋势和攻击方法。政府和企事业单位的云上资产方面，1月份共发现26个云上资产对外扫描攻击，其中某航天研究单位、某县级人民医院（都架设在阿里云上）等单位使用的云服务器IP在公网上发起攻击，值得关注。本文主要通过360网络安全研究院 Anglerfish蜜罐视角，分析云上热门漏洞攻击细节，以及云上重要资产在公网上发起攻击的情况。 2. 云上热门漏洞攻击威胁 本月没有爆发的新漏洞攻击，但值得注意的是，本月有一些旧漏洞的攻击源IP数量较12月出现了大幅增加。增长最多的是Docker Remote API未授权访问漏洞和美国飞塔（Fortinet）FortiOS未授权任意文件

· Feb 21, 2022 · 11 min read

公有云威胁情报

公有云网络安全威胁情报（202112）

1. 概述 云服务具备部署方便、资源灵活弹性、按需付费等优势，各类企业、政府、事业单位、高校和研究机构近年来都参与到了“上云”的潮流中。然而，随着越来越多各行各业的敏感数据“上云”，云安全问题的重要性和紧迫性也越发突出。近年来，全球云服务器被DDoS攻击、入侵、网站页面恶意修改、敏感数据泄露、加密勒索、恶意挖矿等安全事件频发，特别是提供公网服务的云主机，时时刻刻面临着漏洞攻击、暴力破解、Bot流量等云上网络威胁，这要求无论是云服务商还是云上用户都需要时刻做好威胁检测和处置的准备。 云安全的关键是“知己知彼”。“知己”就是做好云上资产、组件、数据和漏洞的管理，包括对云上数据按照敏感程度分类管控、对云上资产和组件做好清点和监控，及时全面修复漏洞，保证云产品安全配置正确等。而“知彼”就是及时发现和阻断各类外部网络威胁。传统的以硬件为载体的各类安全产品难以部署于云端资产，无法适应公有云轻量、虚拟化、灵活取用的特点。而威胁情报结合云原生防火墙，不需要复杂的部署和配置，就可实现云上资产对公网威胁的全面防护和管控。 根据360 Anglerfish蜜罐系统捕获的威胁情报数据，本文从近期云

· Jan 19, 2022 · 14 min read

Log4j

Day 10: where we are with log4j from honeypot’s perspective

Our team spent great deal of effort on simulating different protocols, applications and vulnerabilities with our honeypot (Anglerfish and Apacket) system. When big event happens, we are always curious what we see from the honeypot side. Since log4j came to light 10 days ago, we have published two related blogs,

· Dec 21, 2021 · 3 min read

Log4j

从蜜罐视角看Apache Log4j2漏洞攻击趋势

1 概述 Apache Log4j2是一个Java的日志库，可用于控制日志信息的级别和日志生成过程。最近，Apache Log4j2被曝出JNDI注入漏洞（CVE-2021-44228），攻击者仅需要向目标服务器发送特定JNDI链接就可以触发漏洞并在目标机器上执行任意代码，影响面和破坏力极大。受影响用户需及时升级到安全版本。 360网络安全

研究院 Anglerfish蜜罐系统在搜集网络攻击威胁情报领域具有国际领先的技术优势。从2017年WannaCry勒索病毒爆发至今，我们通过对网络攻击常见套路的分析和总结，模拟了大量应用协议和漏洞特征。该系统已经具备及时发现并响应大网威胁的能力，在第一时间内发现了多起大规模网络攻击事件。 北京时间2021年12月10日凌晨0:20，距离漏洞公开不足一天，该系统就首次捕获到了Apache Log4j2漏洞相关攻击。截至12月17日，该系统共捕获2042个攻击源IP（其中中国250个，国外1792个）发起的利用Apache Log4j2漏洞的攻击72242次，攻击源IP涉及54个国家，发现132个攻击源IP利用该漏洞传播了属于30个恶意软件家

· Dec 21, 2021 · 6 min read

公有云威胁情报

公有云网络安全威胁情报（202111）：云上多个资源对外发起攻击

1 概述 2021年11月，360网络安全研究院 Anglerfish蜜罐（以下简称“蜜罐系统”）共监测到全球53745个云服务器发起的网络会话9016万次，与10月份的数据相比略有下降，IP数量下降7.7%，会话数量下降2.1%。本月我们发现了涉及政府、事业单位、新闻媒体等多个行业的单位的8个云服务器IP地址在互联网上发起扫描和攻击。 2 云服务器攻击总体情况 11月22日~24日的突增主要是由以下两个IP地址造成的：一个是腾讯云119.45.229.133，在11月22~24日每天向蜜罐系统发送了数十万个敏感文件嗅探数据包以及上千个微软OMI漏洞探测数据包。另一个是位于荷兰的DigitalOcean云服务器188.166.54.243，该服务器在11月24日一天内向蜜罐系统发送了18万个Telnet暴力破解数据包。 按云服务商维度来看，与上月相比，来自腾讯云和DigitalOcean的攻击会话数量明显增多。特别是腾讯云的攻击会话数量从上月的10万左右增加到了本月超过100万。 10月份腾讯云攻击会话前三的IP地址和会话数分别为：43.128.26.129（21,128）

· Dec 9, 2021 · 14 min read

公有云威胁情报

公有云网络安全威胁情报（202110）：趋势及典型案例分析

1 概述 云计算服务价格低廉，部署快捷方便，但存在安全风险。黑客可以用虚假信息购买，或入侵他人机器获得云资源，用这些资源窃取、勒索原有用户的数据，或用于发起DDoS攻击、发送垃圾和钓鱼邮件、虚拟货币挖矿、刷单、违法代理和传播僵尸网络木马等其他恶意行为。 360网络安全研究院 Anglerfish蜜罐（以下简称“蜜罐系统”）通过模拟仿真技术伪装成针对互联网、物联网以及工业互联网的指纹特征、应用协议、应用程序和漏洞，捕获并分析网络扫描和网络攻击行为。在2021年10月，我们共监测到来自全球58253个云服务器IP共计9213万次的网络扫描和攻击，其中发现云上网站“某市供排水总公司”持续地对外发起网络攻击行为。 2 云服务器攻击总体情况 由于IPv4地址和网络端口数量是有限的，黑客通过购买或入侵获取云服务器资源后，会扫描互联网IP地址，确定攻击目标。公网上的蜜罐系统模拟成相关设备和应用程序后，就有可能被黑客攻击。因此，蜜罐系统可以用于监测互联网上包括利用云服务器发起攻击在内的各类网络攻击行为。 我们的数据来源除了蜜罐系统搜集到的网络五元组、网络数据包和恶意软件样本信息外，还包括一

· Nov 25, 2021 · 10 min read