



houliuyang

honeypot

## Spring4Shell在野漏洞传播分析

背景介绍 2022年3月31号，Spring针对Spring4Shell漏洞(CVE-2022-22965)事件发布了安全公告[1]，并提供了漏洞修复程序，此次漏洞事件在安全社区引起广泛关注。360网络安全研究院高级威胁狩猎蜜罐系统[2]通过被动监测方式看到了该漏洞在野传播过程，我们也看到了Mirai僵尸网络入场，相关在野漏洞攻击威胁情报已通过自动化形式输出。Spring4Shell 在野传播 360网络安全研究院高级威胁狩猎蜜罐系统持续监测到 Spring4Shell漏洞(CVE-2022-22965)扫描和漏洞利用行为，部分源IP地理位置分布如下：以下是Top 10 国家/地区统计列表 United States 92 The Netherlands 49 Germany 30 China 21 France 6 Luxembourg 6 Sweden 6 Switzerland 5 Ukraine



· Apr 1, 2022 · 18 min read

honeypot

## What Our Honeypot Sees Just One Day After The Spring4Shell Advisory

Background On March 31, 2022, Spring issued a security advisory[1] for the Spring4Shell vulnerability (CVE-2022-22965), this vulnerability has caused widespread concern in the security community. When we looked back at our data, our threat hunting honeypot System[2] had already captured activities related

to this exact vulnerability. After March



· Apr 1, 2022 · 17 min read

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	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

en

## Mirai\_ptea Botnet is Exploiting Undisclosed KGUARD DVR Vulnerability

Overview On 2021-06-22 we detected a sample of a mirai variant that we named mirai\_ptea propagating through a new vulnerability targeting KGUARD DVR. Coincidentally, a day later, on June 23, we received an inquiry from the security community asking if we had seen a new DDoS botnet, cross-referencing some



· Jul 1, 2021 · 11 min read

nday

## Mirai\_ptea Botnet利用KGUARD DVR未公开漏洞报告

2021-06-22我们检测到一个我们命名为mirai\_ptea的mirai变种样本通过未知漏洞传播。经过分析，该漏洞为KGUARD DVR未公开的漏洞。从我们的分析看该漏洞存在于2016年的固件版本中。我们能找到的2017年之后的固件厂家均已经修复该漏洞



· Jul 1, 2021 · 12 min read

CVE-2021-26855

## Microsoft Exchange Vulnerability (CVE-2021-26855) Scan Analysis

Background On March 2, 2021, Microsoft disclosed a remote code execution vulnerability in Microsoft Exchange server[1]。 We customized our Anglerfish honeypot to simulate and deploy Microsoft Exchange honeypot plug-in on March 3, and soon we started to see a large amount of related data, so far, we have already



· Mar 25, 2021 · 12 min read

CVE-2021-26855

## Microsoft Exchange 漏洞 (CVE-2021-26855) 在野扫描分析报告

背景介绍 2021年3月2号，微软披露了Microsoft Exchange服务器的远程代码执行漏洞[1]。2021年3月3号开始，360网络安全研究院Anglerfish蜜罐开始模拟和部署Microsoft Exchange蜜罐插件，很快我们搜集到大量的漏洞检测数据，目前我们已经检测到攻击者植入Webshell，获取邮箱信息，甚至进行XMRig恶意挖矿(<http://178.62.226.184/run.ps1>)的网络攻击行为。根据挖矿文件路径名特征，我们将该Miner命名为Tripleone。2021年3月6号开始，ProjectDiscovery和微软CSS-Exchange项目相继披露了漏洞检测脚本[2][3]。Microsoft Exchange服务器的远程代码执行漏洞利用步骤复杂，一般从PoC公布到黑色产业攻击者利用需要一定的时间，我们看到这个攻击现象已经开始了。CVE-2021-26855 植入Webshell POST /ecp/j2r3.js  
HTTP/1.1 Host: {target} Connection: keep-alive



· Mar 25, 2021 · 13 min read

