黄安欣

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