Log4j

从蜜罐视角看Apache Log4j2漏洞攻击趋势

Rugang Chen
Dec 21, 2021 • 6 min read

1 概述

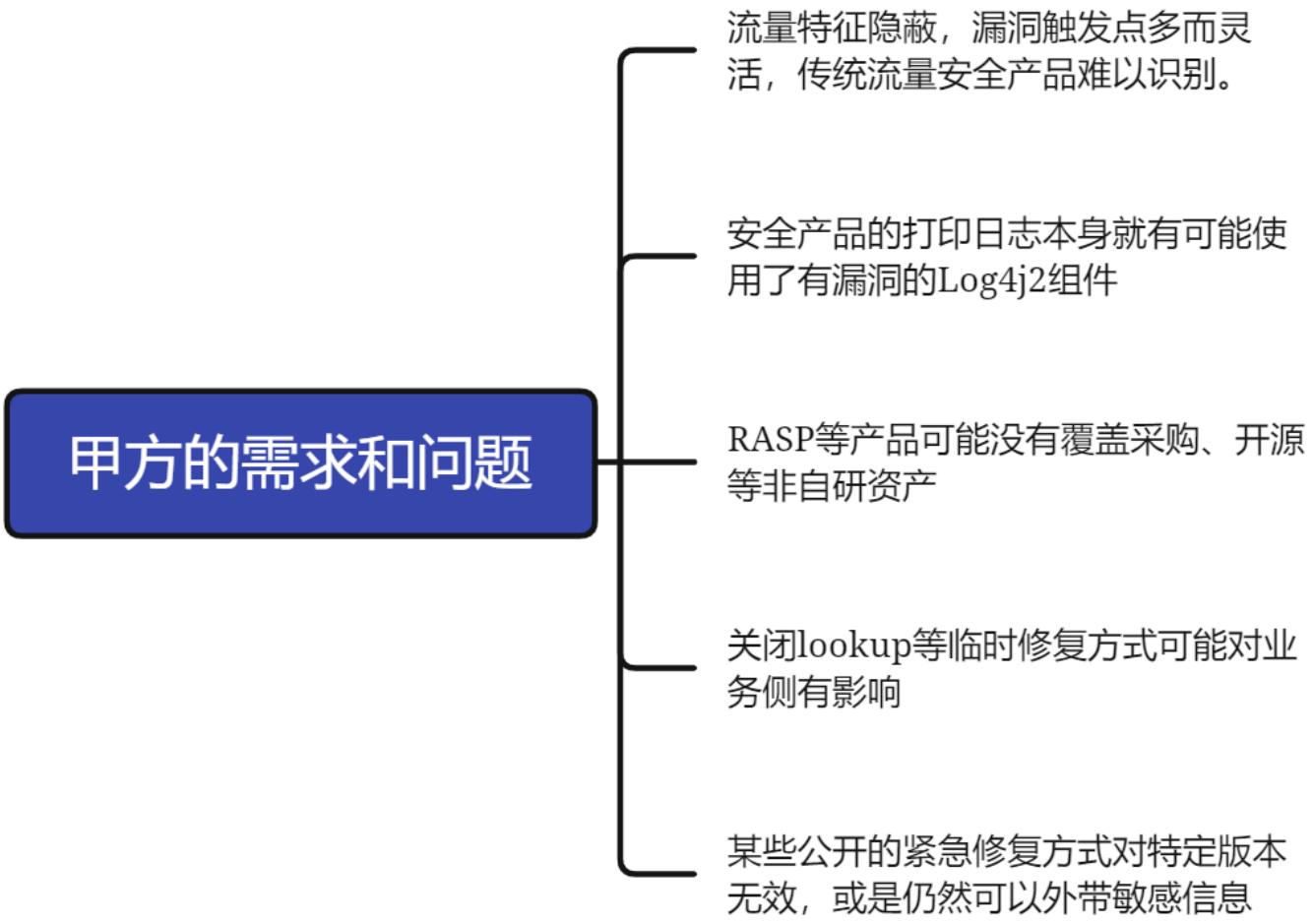
Apache Log4j2是一个Java的日志库，可用于控制日志信息的级别和日志生成过程。最近，Apache Log4j2被曝出JNDI注入漏洞（CVE-2021-44228），攻击者仅需要向目标服务器发送特定JNDI链接就可以触发漏洞并在目标机器上执行任意代码，影响面和破坏力极大。受影响用户需及时升级到安全版本。

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个恶意软件家族的617个已知恶意软件md5。

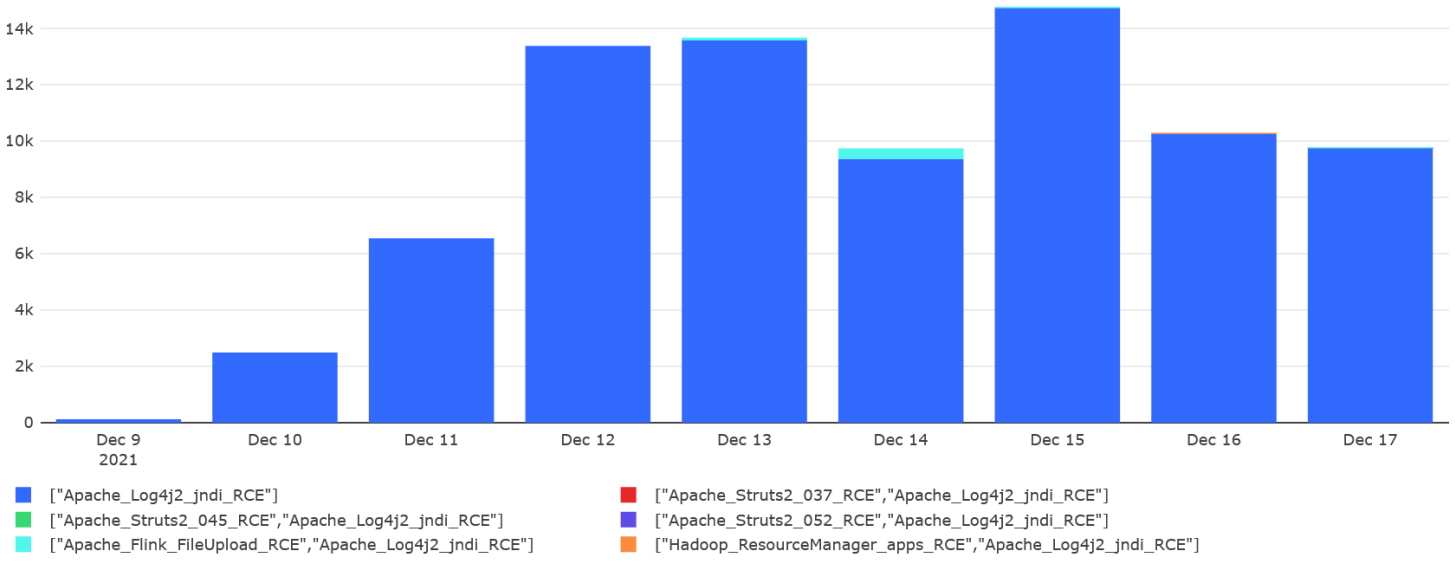
2 甲方的相关需求

对于受影响的甲方而言，在采用安全产品进行防御，以及对相关组件的紧急修复也存在着一些“坑”，比如下面这些：

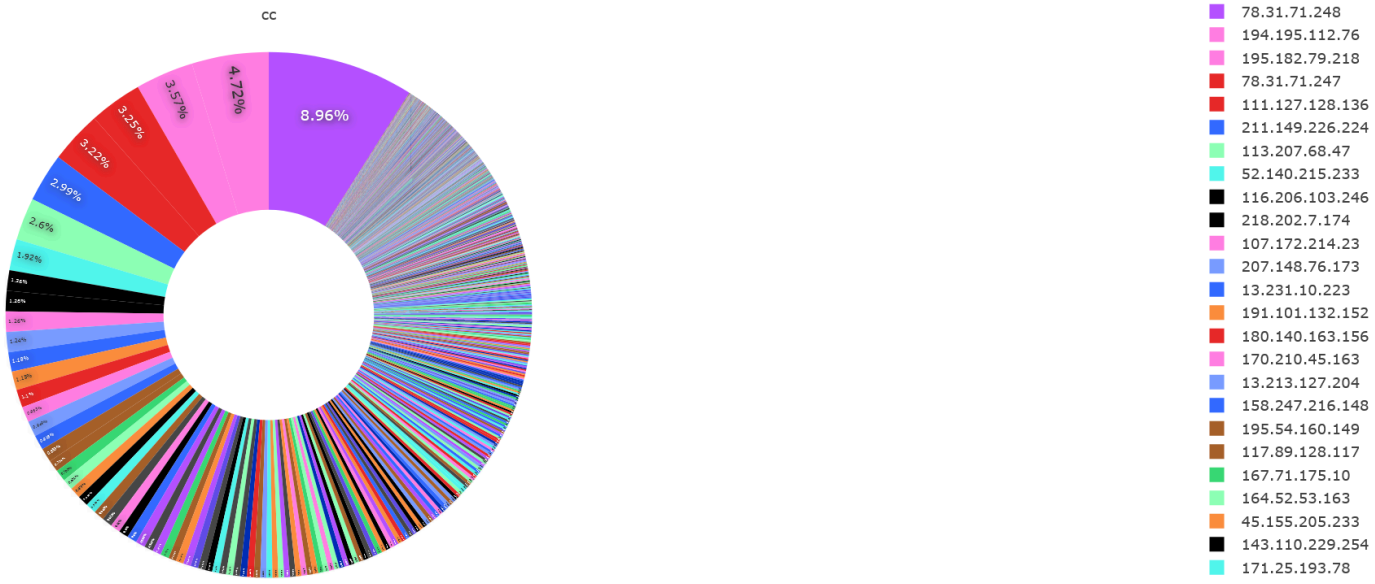


对于传统安全产品和紧急修复措施存在的种种问题，威胁情报是一个非常好的补充。甲方可根据威胁情报，针对性地阻断漏洞攻击源IP和下载服务器链接，为资产打上“预防针”。

3 威胁情报的视角



上图是漏洞攻击数量随时间变化的曲线，可以看出漏洞曝光后，攻击会话的数量在接下来的几天内快速上升。在攻击会话数最多的12月18日，一天内有超过28000次的攻击会话。12月13日开始，还出现了该漏洞与其他漏洞（Apache Flink、Hadoop、Apache Struts2漏洞等）的组合攻击。



上图是主要的攻击源IP，可以看出发起漏洞攻击最多的源IP地址为**78.31.71.248**，占总体IP攻击数的约9%，其它主要的攻击源IP见右边图例。

在传播恶意软件方面，我们最早在12月11日8点整率先捕获到了Muhstik僵尸网络样本，随着时间推移，恶意软件传播的数量明显增加。

攻击源IP
170.210.45.163
167.71.175.10
164.52.53.163
46.105.95.220
1.116.59.211
89.249.63.3
86.109.208.194
178.176.202.121
175.6.210.66
191.232.38.25
上表列出了利用Apache Log4j2漏洞传播恶意软件最多的10个IP，以及这些IP传播恶意软件md5的数量

我们按照ssdeep值对捕获的1083个可执行文件和Java 字节码类型的样本进行聚类分析，共得到107类样本，主要为Java字节码文件，其中的30类617个恶意软件md5我们可以识别出属于特定的恶意软件家族，剩下的目前还未知。

从恶意软件的下载服务器来看，**34.221.40.237**是出现次数最多的下载服务器，有接近一半的恶意软件都来自这个下载服务器。这是一个位于美国的AWS云服务器IP，其它常见的下载服务器见上图右边的图例，下表列出了攻击者使用的10个下载服务器。

域名/IP	攻击源IP数量	恶意软件数量	恶意软件家族	传播会话次数
34.221.40.237	102	8	2	50,358
159.89.182.117	102	1	1	1,850
18.228.7.109	75	15	1	2,947
31.220.58.29	73	6	2	467

域名/IP	攻击源IP数量	恶意软件数量	恶意软件家族	传播会话次数
137.184.174.180	66	1	1	1,097
68.183.165.105	66	5	1	6,334
210.141.105.67	51	1	1	183
45.130.229.168	15	1	1	34
103.13.230.149	14	6	1	156
54.210.230.186	14	1	1	19
45.80.181.55	6	6	1	54

在可以溯源的攻击源IP中，大多数攻击来自于Alpha Strike Labs（一家德国网络安全企业）的漏洞扫描测绘。除了安全厂商和研究机构外，还有大量来自Tor出口节点的攻击。

4 把威胁情报用于攻击防护

威胁情报可以帮助相关单位了解公网上正在发生的漏洞攻击的趋势和攻击者的来源，帮助用户及时把还未发生的网络攻击事件扼杀在摇篮中，具有使用方法简单，数据内容丰富，准确性高，并且不会对业务产生影响等优势。

此次Apache Log4j2 RCE漏洞攻击对网络安全产品是一次大考，面对未知漏洞攻击，表现不尽人意。

360 Anglerfish蜜罐系统通过多样的协议、应用和漏洞模拟和部署在全球范围的公网节点，及时、快速发现和捕获网络攻击威胁相关信息，并支持自动化输出漏洞利用，扫描协议、组织溯源和恶意样本四个维度的威胁情报。

— 360 Netlab Blog - Network Security Research Lab at 360 —

Log4j

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

已有10个家族的恶意样本利用Log4j2漏洞传播

威胁快讯：Log4j漏洞已经被用来组建botnet，针对Linux设备

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,

honeypot

Ten families of malicious samples are spreading using the Log4j2 vulnerability Now

Background On December 11, 2021, at 8:00 pm, we published a blog disclosing Mirai and Muhstik botnet samples propagating through Log4j2 RCE vulnerability[1]。Over the past 2 days, we have captured samples from other families, and now the list of families has exceeded 10. It looks like the

See all 3 posts →

· Dec 21, 2021 · 3 min read

· Dec 13, 2021 · 17 min read