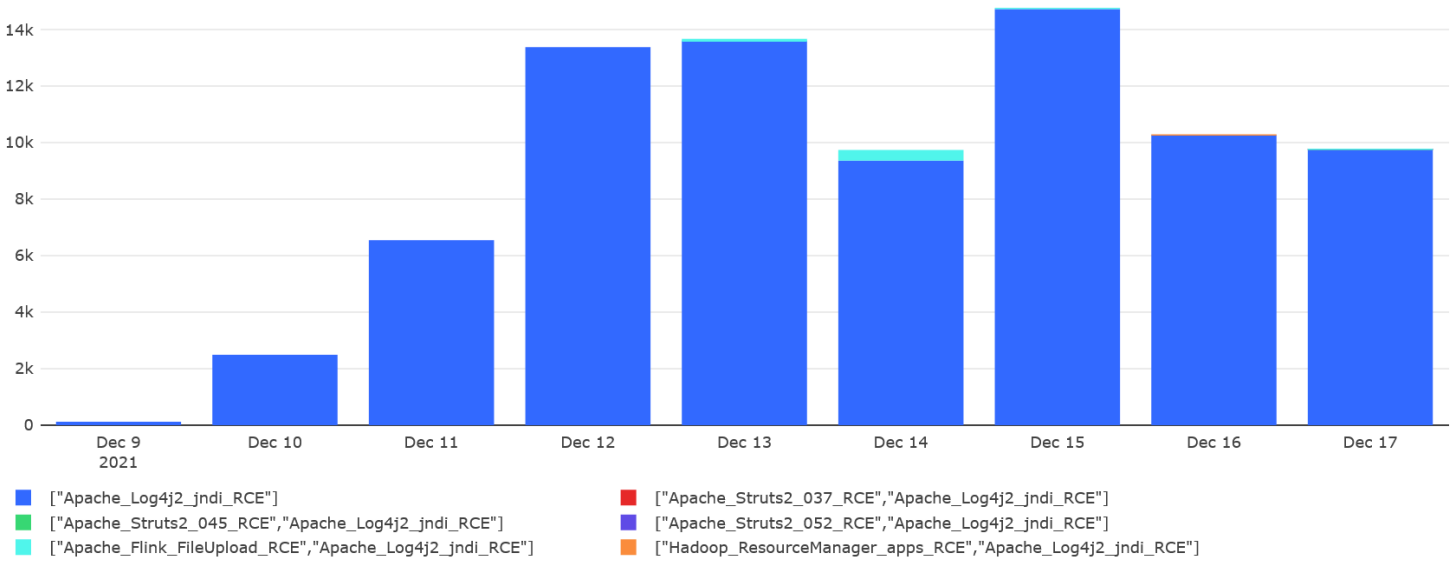
Log4j

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

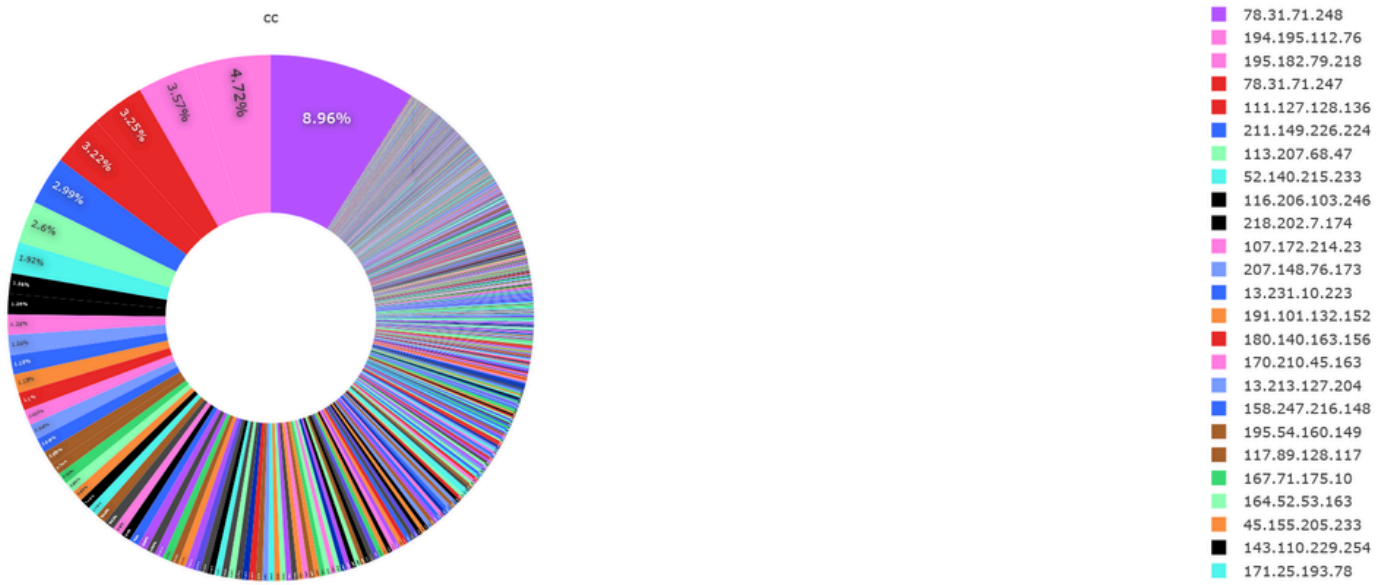
Rugang Chen
Dec 21, 2021 • 3 min read

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, here and here. And looks like more malware are jumping on the bandwagon, as of December 17, we have captured a total of 72,242 attacks launched by 2042 attack source IPs (250 in China and 1,792 abroad), with the source IPs involved in 54 countries, and 132 attack source IPs were found to have exploited the vulnerability to propagate 617 known malware md5s belonging to 30 malware families.



The graph above shows the curve of the number of exploit attacks over time, which shows that the number of attack sessions rose rapidly in the next few days after the

vulnerability was exposed. On December 18, the day with the highest number of attack sessions so fare, there were over 28,000 attack sessions in one day. starting on December 13, there were also combined attacks of this vulnerability with other vulnerabilities (Apache Flink, Hadoop, Apache Struts2 vulnerability, etc.).



The figure above shows the main attack source IPs, so far the No.1 is **78.31.71.248**(PDNS points to srv62134.dus4.dedicated.server-hosting.expert), accounting for about 9% of the overall IP attacks, and the other main attack source IPs are shown in the legend on the right.

In terms of spreading malware, we reported the first botnet(Muhstik) taking advantage of this at exactly 8:00 on December 11, the number of malware spreading increasing significantly over time after that.

IPS	SESSIONS WITH MALWARE	MD5S	MALWARE FAMILIES
170.210.45.163	4,753	28	6
167.71.175.10	4,678	15	4
164.52.53.163	3,926	30	6
46.105.95.220	3,710	30	6
1.116.59.211	2,824	31	6
89.249.63.3	2,195	31	6
86.109.208.194	2,121	29	6

IPS	SESSIONS WITH MALWARE	MD5S	MALWARE FAMILIES
178.176.202.121	2,081	29	6
175.6.210.66	2,025	30	7
191.232.38.25	1,776	23	6

The table above lists the 10 IPs that spread the most malware, as well as the number of malware md5s and the number of malware families spread by each IPs.

When we break down the 1083 executable samples and Java bytecode according to their ssdeep values., we get a total of 107 groups of samples (mainly Java bytecode

files), within which, 30 groups (correspondingly 617 malware md5s) can be identified as specific malware families, the rest of them are currently unknown.

In terms of malware download servers, 34.221.40.237 is the most frequent download server, with nearly half of the malware coming from this download server. This is an AWS cloud server IP located in the U.S. Other common download servers are shown in the legend on the right side of the image above, and the table below lists the 10 download servers used by the attackers.

DOWNLOAD SERVERS	ATTACKERS	MALWARE MD5S	MALWARE FAMILIES	SESSIONS
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
137.184.174.180	66	1	1	1,097
68.183.165.105	66	5	1	6,334

DOWNLOAD SERVERS	ATTACKERS	MALWARE MD5S	MALWARE FAMILIES	SESSIONS
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

Among the attack source IPs that can be traced, most of attackers come from Alpha Strike Labs (a German network security company). In addition to security vendors and research institutions, there are also a large number of attacks from Tor exit nodes.

Contact us

Readers are always welcomed to reach us on twitter or email us to netlab at 360 dot cn.

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

Log4j

从蜜罐视角看Apache Log4j2漏洞攻击趋势

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

See all 3 posts →

DTA

用DTA照亮DNS威胁分析之路 (1)

--- “历史重现”小功能 概述 2021年10月，《七年一剑，360 DNS威胁分析平台》宣告了360 DNS威胁分析平台(简称DTA)的诞生。在文章开头，Netlab阐述了设计DTA的核心理念： 让情报发挥应有价值 让威胁分析真正有效 理念是简洁的，也是抽象的。18个字背后，对应着Neltab 7年的安全研究经验；而7年的沉淀，又在2年时间的打磨里，变成了DTA众多的功能...

· Dec 27, 2021 · 9 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...

· Dec 21, 2021 · 6 min read