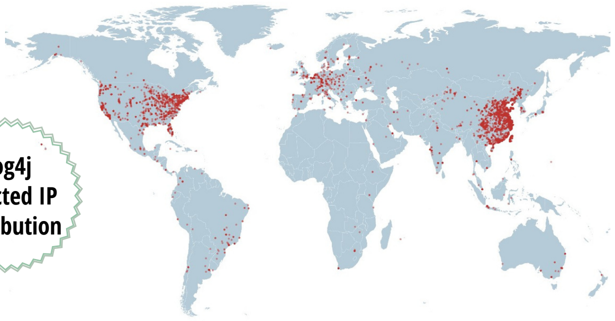
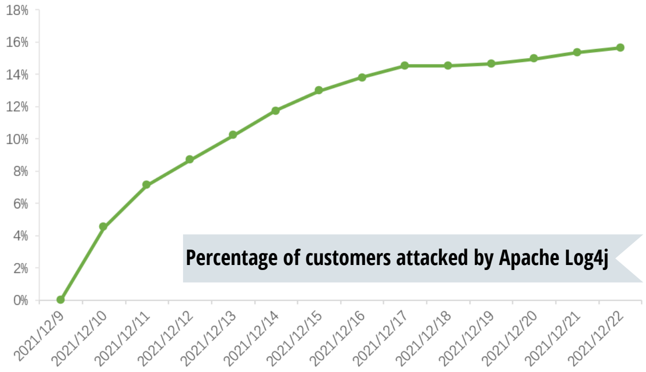
NSFOCUS

*Security Made Smart and Simple*



Log4j affected IP distribution

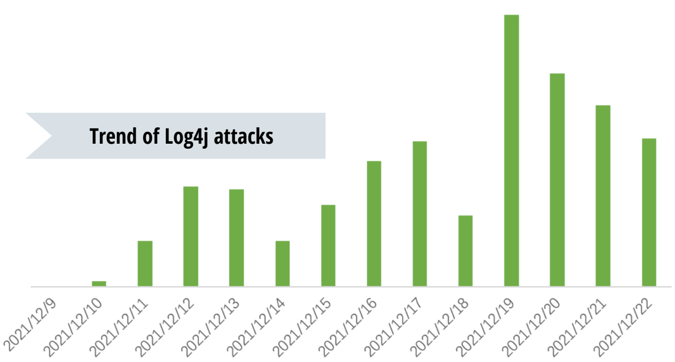
Based on the monitoring of global service assets by the NSFOCUS Threat Intelligence Center, IPs affected by Apache Log4j (hereinafter called "Log4j" ) vulnerabilities are basically all over the world. Among them, China, the United States, and Europe are the regions with the largest number of affected IPs. Since Log4j is a widely used component instead of a software targeting a specific country or region, the distribution of vulnerability impacts is basically related to the degree of local Internet development.



Percentage of customers attacked by Apache Log4j

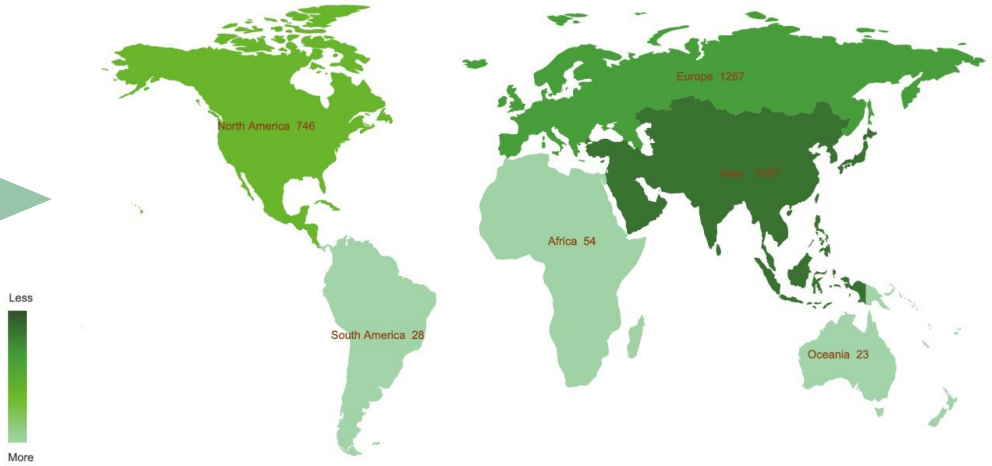
In the customer environments monitored by NSFOCUS, nearly 16% of customer environments have been detected with Log4j vulnerability attacks. The number of attacked customers increased rapidly one week after the vulnerability was released, and stabilized after the second week.

The number of attacks using Log4j vulnerabilities increased rapidly after the vulnerability was released, and reached a peak on the 10th day afterwards. However, with the decline in the popularity of attacks, and the defense's security measures, the number of attacks has remained relatively stable and has declined slightly since then.

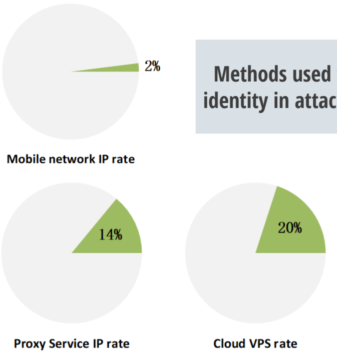


Trend of Log4j attacks

Within one week after the vulnerability was released, NSFOCUS has monitored more than 3700 global IPs using Log4j vulnerabilities for attacks. Among them, the top three regions in terms of IP amounts are Asia, North America and Europe. Through our threat intelligence cloud center, NSFOCUS updates real-time threat intelligence every day, helping NSFOCUS global customers to monitor and block attacks from these IPs.



In addition to concealed attacks using public hidden resources, attackers also used a large number of IPs with a history of malicious attacks, including botnets.



Mobile network IP rate

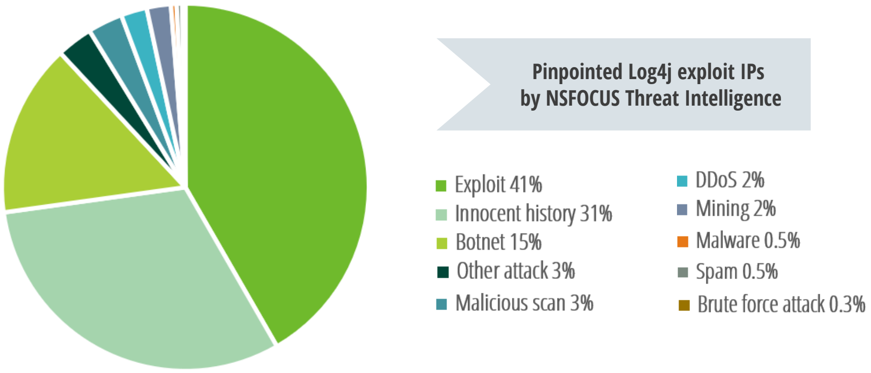
Proxy Service IP rate

Cloud VPS rate

Methods used to hide identity in attack source

In the attack source data monitored by NSFOCUS, we found that some attackers used public resource nodes to launch attacks to hide their true identities.

Among them, the proportion of hidden resources used to initiate attacks such as mobile networks, proxy services, and public cloud hosts were 2%, 14%, and 20% respectively.



Pinpointed Log4j exploit IPs by NSFOCUS Threat Intelligence

Among the 3700+ attack source IPs monitored, 69% have a recent history of network attacks in NSFOCUS threat intelligence, and 41% of them have a history of network attacks using other vulnerabilities. Based on our cloud-based and on-premise hybrid security solution, NSFOCUS helps customers defend a large number of Apache Log4j attacks.