Log4Shell: No Mass Abuse, But No Respite, What Happened?

news.sophos.com/en-us/2022/01/24/log4shell-no-mass-abuse-but-no-respite-what-happened/

Chester Wisniewski January 24, 2022

Sometimes, when a software crisis doesn't cause the kind of devastation everyone expects, it is because there may not have been a crisis in the first place. That is not the case with the Log4Shell vulnerability found in the widely used Apache Log4J software in early December 2021. Even though the world hasn't seen the feared mass exploitation of the vulnerability, the Log4Shell bug, buried deep in many digital applications and products, will likely be a target for exploitation for years to come.

Sophos believes that the immediate threat of attackers mass exploiting Log4Shell was averted because the severity of the bug united the digital and security communities and galvanised people into action. This was seen back in 2000 with the Y2K bug and it seems to have made a significant difference here.

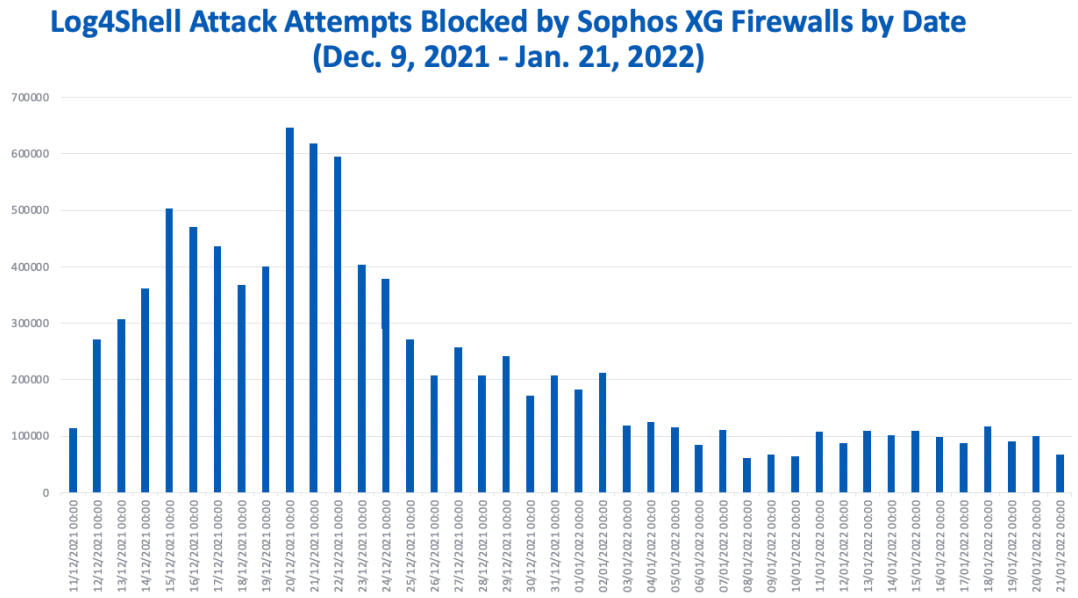
As soon as details of the Log4Shell bug became clear, the world's biggest and most important cloud services, software packages and enterprises took action to steer away from the iceberg, supported by shared threat intelligence and practical guidance from the security community.

Like others across the security industry, Sophos has continued to track and monitor the threat. It is worth taking stock of how things have unfolded since Dec. 9, 2021; what we know now and what we anticipate for the future.

Scanning the Scanners

Sophos telemetry on scans for exposed instances of Log4J reveals a typical pattern for a newly reported vulnerability. In the first few days, the volume of scans was moderate, reflecting the early development of Proof-of-Concept exploits and preliminary online scanning for exploitable systems.

Within a week, there was a significant increase in scan detections, with numbers peaking between Dec. 20 and Dec. 23, 2021.



SOPHOSlabs Source: Total IPS alerts for Log4Shell attack attempts on Sophos XG Firewalls, from Sophos customers sharing telemetry data. Out of 67.7K devices sharing data, 13K (19%) were subject to scanning attacks

These numbers will undoubtably include successful but not yet identified exploitations, opportunistic cryptominers, nation-state supported threat actors and other cybercriminals looking to find and breach targets. However, it is also worth noting that during these days in late December, many security companies were still open for business before the holidays and were actively monitoring the landscape.

In other words, the numbers simply confirm that a great many people, with good or bad intentions, were trying to gauge how vulnerable others were to the threat by looking for the number of potentially exposed systems.

Another factor to consider when evaluating the scanning numbers is that a Log4Shell type of flaw is exploited differently based on which application the Log4J code is in and how it has been integrated with that application. This results in a high volume of redundant scans trying different ways to exploit different applications.

From late December through January 2022, however, the curve of attack attempts flattened out and declined. This doesn't mean the threat level declined too: by this time, an ever-greater percentage of detections were likely real attacks, with fewer coming from researchers

monitoring the latest patching status.

Limited Mass Exploitation

The overall number of successful attacks to date remains lower than expected. Evidence for this can be found on the frontline. The Sophos Managed Threat Response Team (MTR) notes that while the team has detected many scans and attempts to trigger the Log4Shell exploit, by early January 2022 only a handful of MTR customers faced attempted intrusions where Log4j was determined to be the initial entry point. The majority of these were cryptominers.

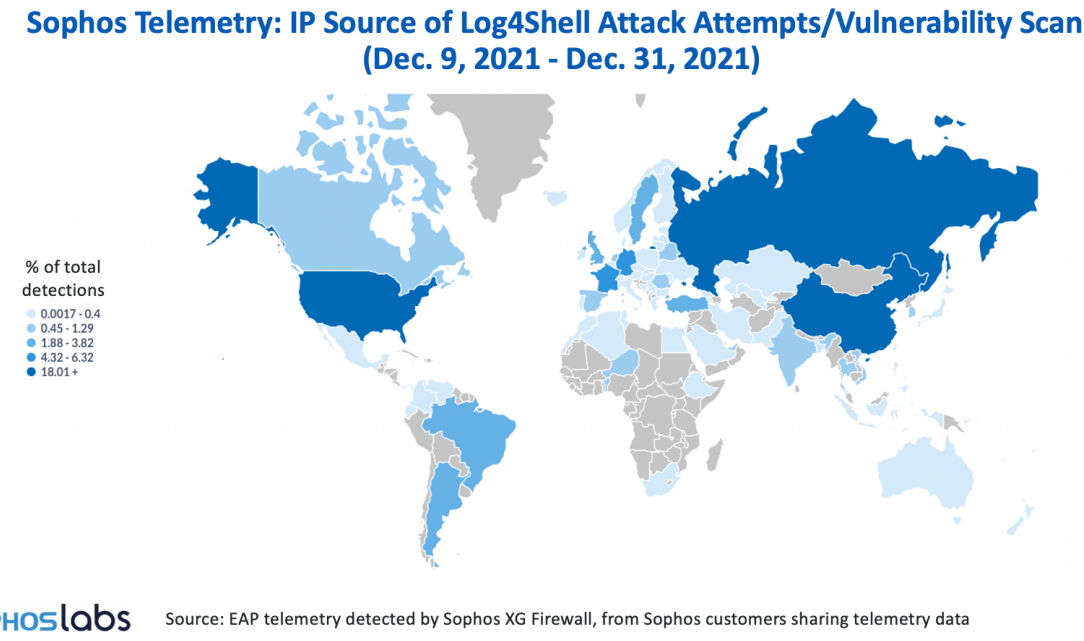
Another possible reason for the limited mass exploitation could be the need to customize the attack to each application that includes the vulnerable Apache Log4J code.

At one end of the scale are the incredibly widely used applications that are exposed to the internet and which need to be manually updated, one by one. These are being exploited at scale in an automated fashion. An example of such an application is VMware Horizon. The first intrusion seen by Sophos MTR that leveraged Log4Shell involved VMware Horizon.

At the other end of the scale are many other, more obscure applications involving Apache Log4J that will take time to be discovered and exploited by attackers. These attacks will proceed at a human pace and won't result in giant spikes of activity, although they will still present a significant risk to organizations that remain vulnerable.

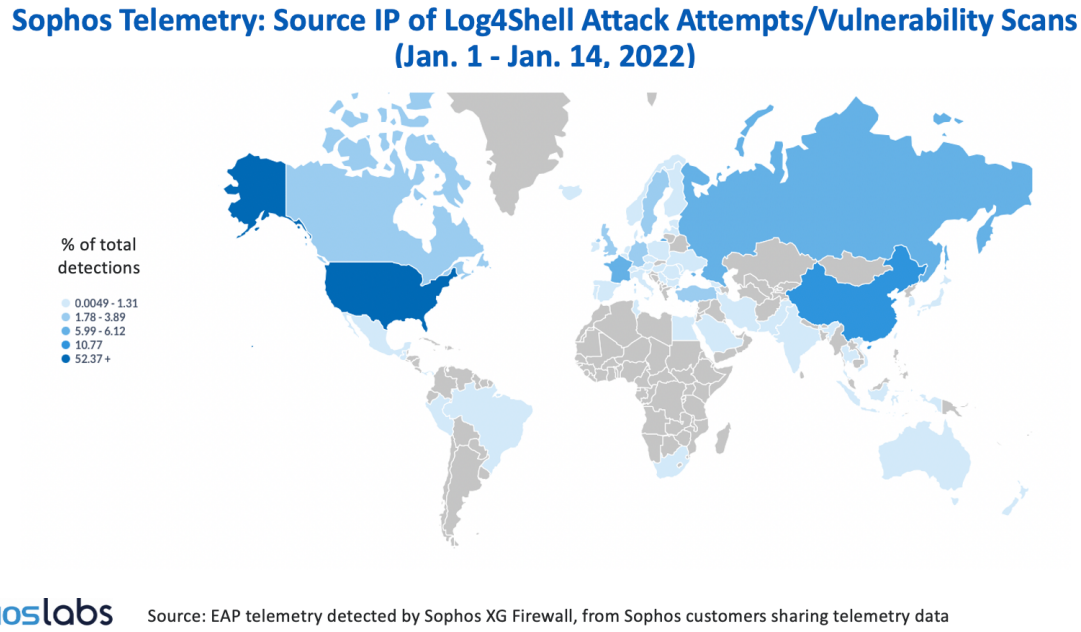
The Geography of Attack Attempts: Then and Now

Sophos geolocation telemetry from when the bug was reported on Dec. 9, 2021, to the end of the year, and for the first two weeks of January 2022 shows some interesting variations in the sources of attack attempts and scans.



Looking at the map for December, it is worth noting that the top countries, including the U.S., Russia, and China, as well as countries in Western Europe and Latin America, generally have large populations and a significant, skilled cybersecurity workforce. Many also have well established digital infrastructure and are popular internet hosting hubs. For example, the heavy weighting of the U.S. and Germany in the geolocation IP source data likely reflects the large data centres that are based there and operated by Amazon, Microsoft, and Google, among others.

This picture changes dramatically in early 2022, as detections of mass scanning give way to indicators of more detailed probing and exploitation.

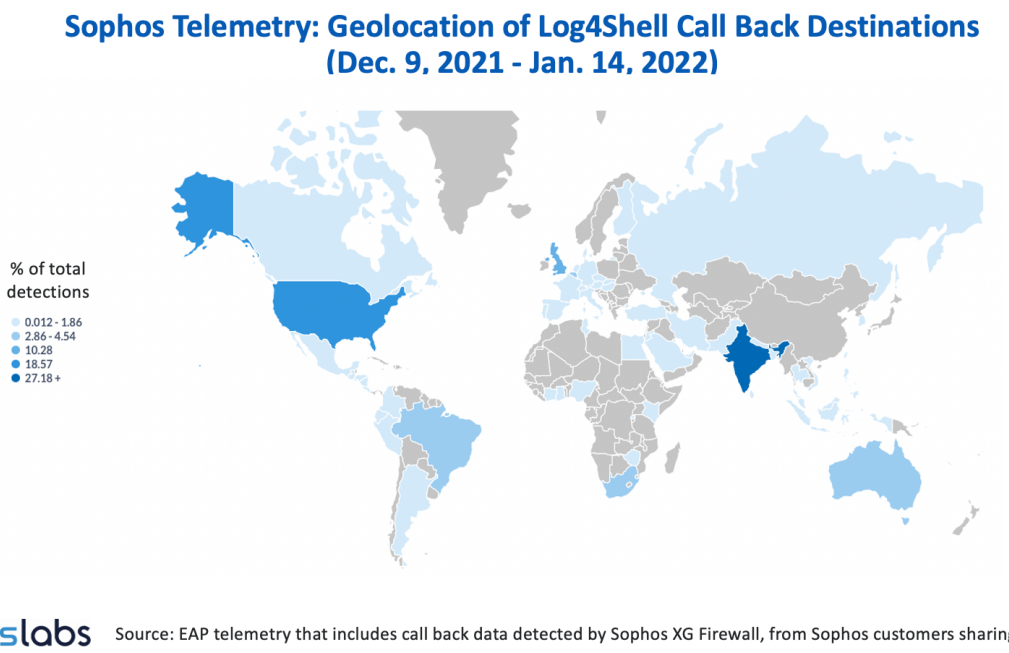


The most noticeable difference between the two maps is how the early dominance of Russia and China appears to have diminished by January. Sophos intelligence suggests that this reflects an apparent decline in the number of attack attempts by a small number of highly aggressive cryptominers based in these regions.

It's important to note that there may not be a relationship between the source IPs that are scanning or exploiting the vulnerability, and the actual location of those who are generating the traffic. A better view might be the destination of the call backs.

The Geography of Call Back Destinations

Like the source IP data, Sophos has captured call back destinations relating to Log4Shell for the end of 2021 and the beginning of 2022. There are fewer variations over time, but the overall picture is very different to that of the IP source location.



The data shows the top destinations worldwide that vulnerable (unpatched) devices are reaching out to in order to retrieve a Java payload or to dump information extracted from the machine, such as AWS security keys or other variables.

While the U.S. remains a top contender, this view brings India into the number one position and highlights Turkey, Brazil and even Australia. It is difficult to speculate as to why these regions are top destinations for call backs. One reason might be that these countries have many active participants in bug bounty programs, hoping to earn money by being the first to alert organizations that they are exposed.

The Threat Remains

Just because we've steered round the immediate iceberg, that doesn't mean we're clear of the risk.

As others have pointed out, some of the initial attack scans may have resulted in attackers securing access to a vulnerable target, but not actually abusing that access to deliver malware, for instance – so the successful breach remains undetected.

In the past Sophos has observed countries such as Iran and North Korea pounce on VPN vulnerabilities to gain access to targets' networks and install backdoors before the targets have had a chance to deploy the patches, and then waiting months before using that access in an attack.

In another example, attackers targeted vulnerable Exchange servers in the immediate aftermath of the first ProxyLogon patches, leaving behind web shells as backdoors for later attacks. Patching your Exchange server wasn't enough, you also had to remove any backdoors that were dropped.

There’s more. Over time, internet facing applications vulnerable to a Log4Shell exploit are likely to be identified patched or removed. However, unknown internally vulnerable systems may never be known or discovered, and these will remain a security risk. Sophos telemetry shows that the number of vulnerable Java Archive files (JAR) on Sophos protected endpoints hasn’t changed. These could become a favorite tool for malicious lateral movement down the road.

Conclusion

Sophos believes that attempted exploitation of the Log4Shell vulnerability will likely continue for years and will become a favourite target for penetration testers and nation-state supported threat actors alike. The urgency of identifying where it is used in applications and updating the software with the patch remains as critical as ever.