2024

SECURITY REPORT

Outbound connections to multiple suspicious IPs (Open Wire Lab)

github.com/Abdibimantara abdibimantara.github.io abdibimantara91@gmail.com

Daftar Isi

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 mengekploitasi 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 tersebu melakukan outbound connection ke dua IP public yang setelah dilakukan penelusuran koneksi keara dua ip tersebut masuk dalam unautorized connection.

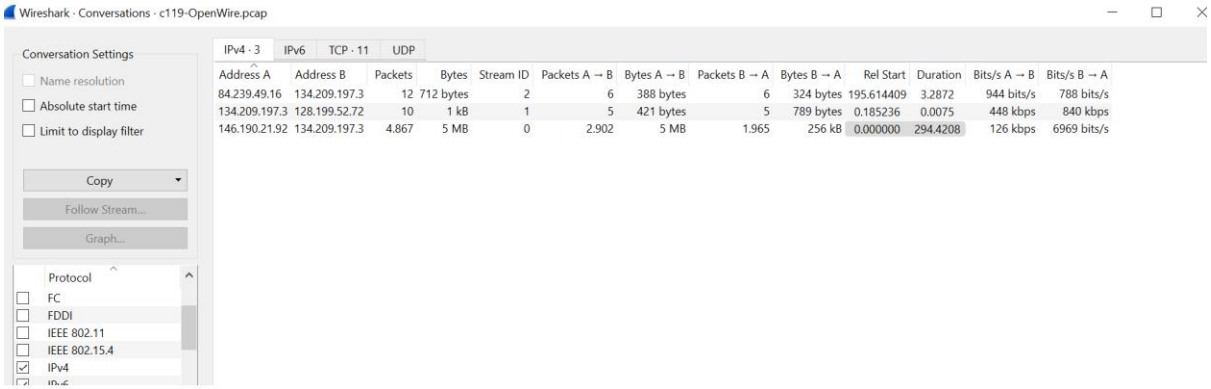
Lab Environment

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 Susppicious 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.

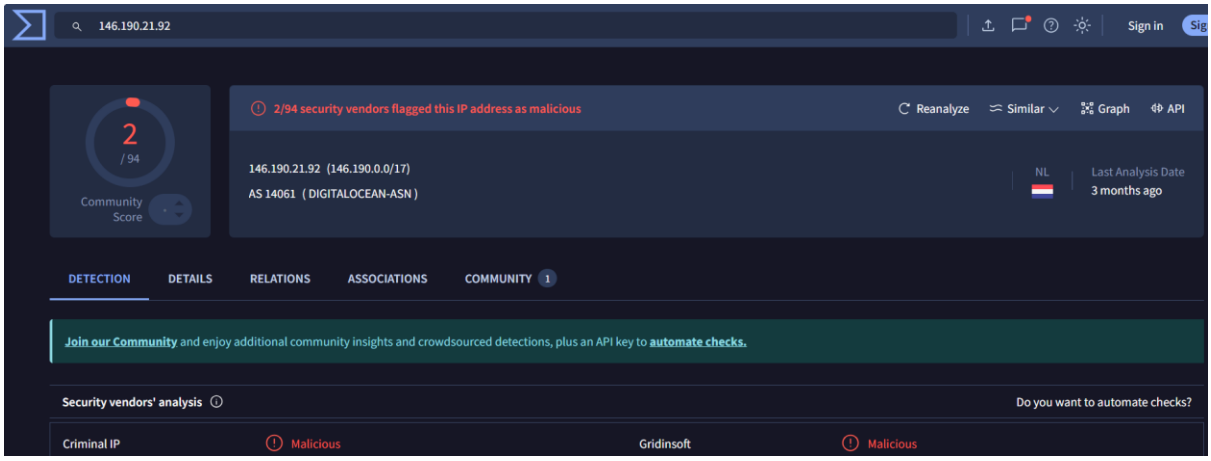
Proses Analisa dari tim L2 SOC dimulai dengan melakukan penelusuran melalui data network traffic menggunakan bantuan tools wireshark. Dimana dari hasil penelusuran tersebut, didapatkan bahwa aktivitas tersebut diketahui dimulai pada jam 13:38:27 UTC.



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

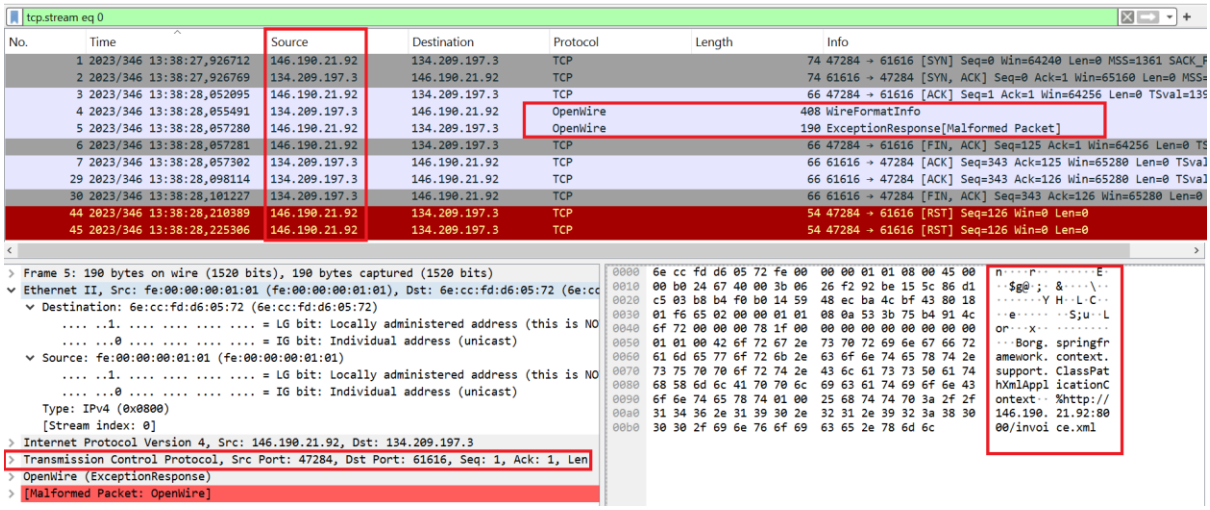
Berdasarkan penelusuran awal tim L2 SOC menggunakan data statistic IPv4, diketahui bahwa terdapat adanya indikasi packets terbanyak berasal dari IP 146.190.21.92 (Eksternal) 4867 packet ssebesar 5MB menuju ip 134.209.197.3 (IP Public Server), dimana dari hasil temuan tersebut patut untuk dicurigai.



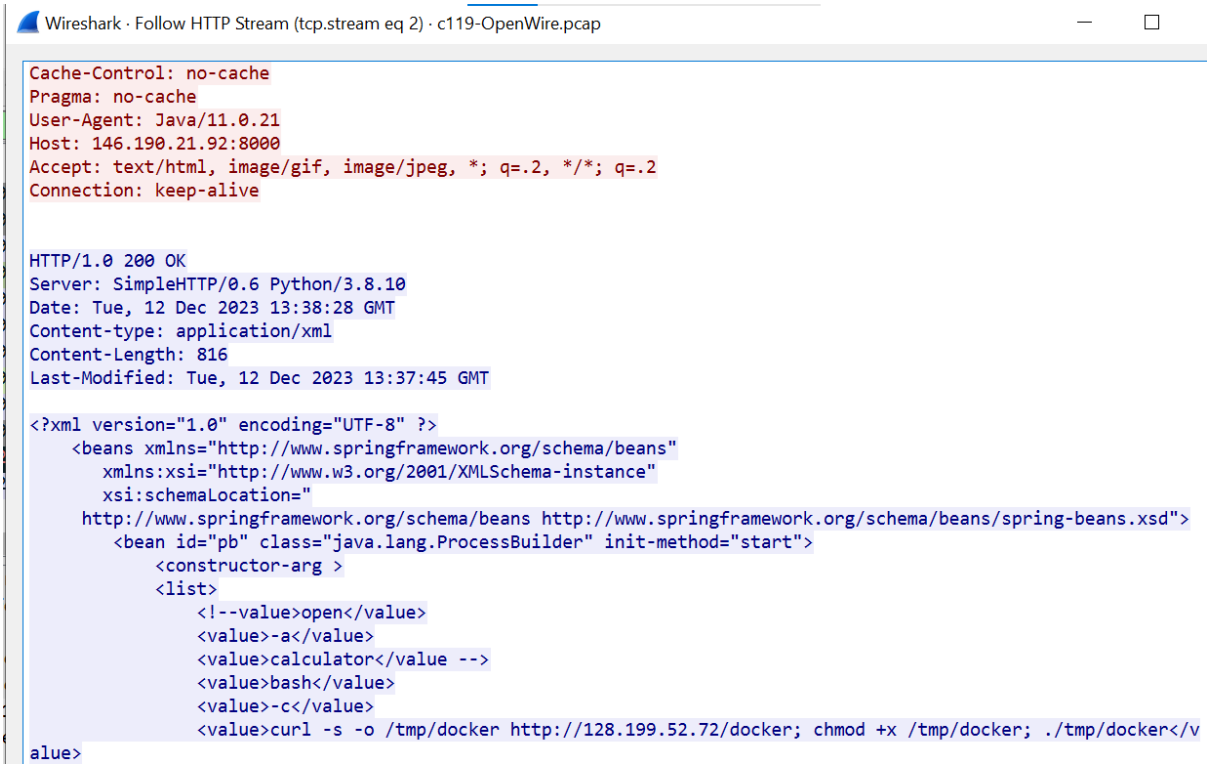
Validasi pertama dilakukan dengan melakukan pengecekkan reputasi IP trersebut menggunakan bantuan tools Virustotals. Hasil dari penelusuran tersebut,

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

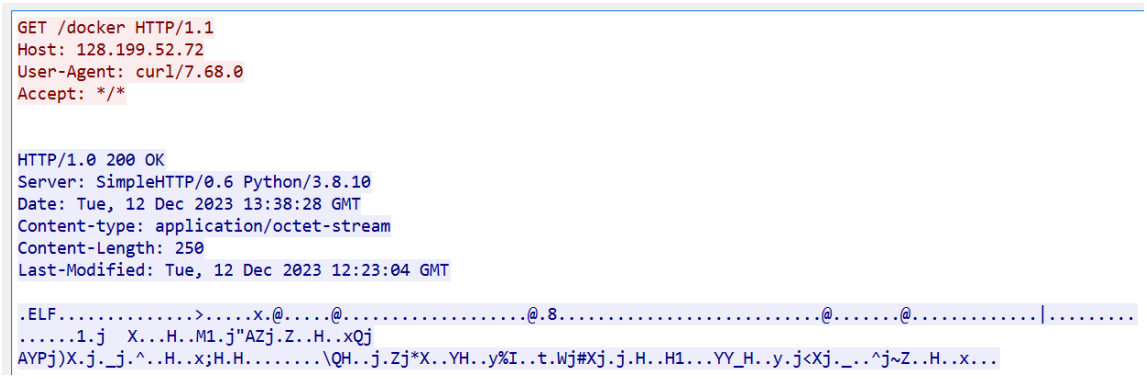
Penelusuran dilanjutkan dengan mencari tahu, dimana Fase initial access dari Suspicious IP tersebut berasal. Sehingga dari temuan tersebut akan dijadikan evaluasi oleh tim Security untuk mencegah adanya potensi incident yang berulang. Penelusuran kembali berfokus pada data network traffic yang didapatkan 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.



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.



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.



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 berahasil 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 scaning 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