

The Deloitte logo is displayed in white text on a black rectangular background. The word "Deloitte" is in a bold, sans-serif font, with a small green dot at the end of the word.

WEB LOG ANALYSIS

Daikibo Industrials Cyber Breach Investigation

BACKGROUND INFORMATION

A major news publication has revealed sensitive private information about Daikibo Industrials, our client. A production problem has caused its assembly lines to stop, threatening the smooth operation of supply chains relying on Daikibo's products. The client suspects the security of their new status board, Daikibo's telemetry dashboard may have been breached.

Analyst name

Abdiaziz Ibrahim Kar

Tasks Assigned

You will be joining our cyber security team. Your job is to:

1. Determine if the alleged breach could have happened from an attacker on the internet directly (i.e. no access to Daikibo's VPN).
2. Inspect a *web_requests.log* file.

Provided: web_requests.log

1. Determining if the alleged breach could have happened from an attacker on the internet

Analysis:

The first step of the analysis was to check the IP addresses that have had interactions with Daikibo's telemetry dashboard. I observed that all those addresses were class C, private (internal), ruling out direct internet attacks.

Findings:

Attack Origin: Internal only (all IPs were private addresses).

Evidence: No public IPs.

```
C:\> Users > Admin > OneDrive - United States International University (USIU) > Desktop > VirtualInternships > Forge > Data Science > web_activity.log

1
2 192.168.0.50:
3   TIME           METHOD REQUEST                                     STATUS
4   2021-06-25T07:23:00.000Z GET "/" 401 (UNAUTHORIZED)
5   2021-06-25T07:23:00.000Z GET "/login" 200 (SUCCESS)
6   2021-06-25T07:23:00.000Z GET "/login.css" 200 (SUCCESS)
7   2021-06-25T07:23:00.000Z GET "/login.js" 200 (SUCCESS)
8   2021-06-25T07:23:44.000Z POST "/login" 200 (SUCCESS)
9   2021-06-25T07:23:45.000Z GET "/" {authorizedUserId: "5Eckr4DTaLLDaDMGqmM3g"} 200 (SUCCESS) "Eckr": Unknown
10  2021-06-25T07:23:45.000Z GET "/index.css" {authorizedUserId: "5Eckr4DTaLLDaDMGqmM3g"} 200 (SUCCESS) "Eckr": Unknown
11  2021-06-25T07:23:45.000Z GET "/index.js" {authorizedUserId: "5Eckr4DTaLLDaDMGqmM3g"} 200 (SUCCESS) "Eckr": Unknown
12  2021-06-25T07:23:46.000Z GET "/api/factory/status?factory=" {authorizedUserId: "5Eckr4DTaLLDaDMGqmM3g"} 200 (SUCCESS) "Eckr": Unknown
13  2021-06-25T07:24:01.000Z GET "/api/factory/machine/status?factory=meiyo&machine=" {authorizedUserId: "5Eckr4DTaLLDaDMGqmM3g"} 200 (SUCCESS) "meiyo": Unknown
14
15 192.168.0.73:
16   TIME           METHOD REQUEST                                     STATUS
17  2021-06-25T07:47:00.000Z GET "/" 401 (UNAUTHORIZED)
18  2021-06-25T07:47:01.000Z GET "/login" 200 (SUCCESS)
19  2021-06-25T07:47:02.000Z GET "/login.css" 200 (SUCCESS)
20  2021-06-25T07:47:03.000Z GET "/login.js" 200 (SUCCESS)
21  2021-06-25T07:48:01.000Z POST "/login" 200 (SUCCESS)
22  2021-06-25T07:48:02.000Z GET "/" {authorizedUserId: "1FtyZiH0X9c8J3TzIYq4Bs"} 200 (SUCCESS)
23  2021-06-25T07:48:03.000Z GET "/index.css" {authorizedUserId: "1FtyZiH0X9c8J3TzIYq4Bs"} 200 (SUCCESS)
24  2021-06-25T07:48:04.000Z GET "/index.js" {authorizedUserId: "1FtyZiH0X9c8J3TzIYq4Bs"} 200 (SUCCESS)
25  2021-06-25T07:48:04.000Z GET "/api/factory/status?factory=" {authorizedUserId: "1FtyZiH0X9c8J3TzIYq4Bs"} 200 (SUCCESS)
26  2021-06-25T07:48:14.000Z GET "/api/factory/machine/status?factory=meiyo&machine=" {authorizedUserId: "1FtyZiH0X9c8J3TzIYq4Bs"} 200 (SUCCESS)
27  2021-06-25T07:48:17.000Z GET "/api/factory/machine/status?factory=meiyo&machine=LaserWelder" {authorizedUserId: "1FtyZiH0X9c8J3TzIYq4Bs"} 200 (SUCCESS)
28  2021-06-25T07:49:12.000Z GET "/api/factory/machine/status?factory=berlin&machine=" {authorizedUserId: "1FtyZiH0X9c8J3TzIYq4Bs"} 200 (SUCCESS)
29  2021-06-25T07:49:48.000Z GET "/api/factory/machine/status?factory=berlin&machine=LaserCutter" {authorizedUserId: "1FtyZiH0X9c8J3TzIYq4Bs"} 200 (SUCCESS)
30  2021-06-25T07:51:20.000Z GET "/api/factory/machine/status?factory=berlin&machine=MetalPress" {authorizedUserId: "1FtyZiH0X9c8J3TzIYq4Bs"} 200 (SUCCESS)
31  2021-06-25T07:52:15.000Z GET "/api/factory/machine/status?factory=meiyo&machine=" {authorizedUserId: "1FtyZiH0X9c8J3TzIYq4Bs"} 200 (SUCCESS)
32  2021-06-25T07:52:53.000Z GET "/api/factory/machine/status?factory=meiyo&machine=HeavyDutyDrill" {authorizedUserId: "1FtyZiH0X9c8J3TzIYq4Bs"} 200 (SUCCESS)
33
34 192.168.0.38:
35   TIME           METHOD REQUEST                                     STATUS
36  2021-06-25T08:01:00.000Z GET "/" 401 (UNAUTHORIZED)
37  2021-06-25T08:01:00.000Z GET "/login" 200 (SUCCESS)
```

2. web_requests.log file Inspection

Analysis:

To identify user ID and IP address of the attacker, my initial priority was to review at request timestamps for any use of automated tools. The analysis revealed user that sends *GET* request to check status, in *every first 48th second of every hour*, machine-like precision. The user automates what seems to be a brute-force attack on the endpoint `/api/factory/machine/status`. Additionally, there is use of wildcards in some API requests, a clear indication of automated scraping.

Moreover, Legitimate user traffic would typically include requests for static assets like CSS stylesheets and images. The absence of these requests strongly suggests automated tooling. Within the same second, the user makes multiple rapid requests with different parameters, further indicating automation.

```
662 2021-06-25T17:00:48.000Z GET "/api/factory/machine/status?factory=meiyok&machine=*" {authorizedUserId: "mdB7yD2dp1BFZPonTHBQ1Z"} 200 (SUCCESS)
663 2021-06-25T17:00:48.000Z GET "/api/factory/machine/status?factory=seiko&machine=*" {authorizedUserId: "mdB7yD2dp1BFZPonTHBQ1Z"} 200 (SUCCESS)
664 2021-06-25T17:00:48.000Z GET "/api/factory/machine/status?factory=shenzhen&machine=*" {authorizedUserId: "mdB7yD2dp1BFZPonTHBQ1Z"} 200 (SUCCESS)
665 2021-06-25T17:00:48.000Z GET "/api/factory/machine/status?factory=berlin&machine=*" {authorizedUserId: "mdB7yD2dp1BFZPonTHBQ1Z"} 200 (SUCCESS)
666 2021-06-25T18:00:48.000Z GET "/api/factory/machine/status?factory=meiyok&machine=*" {authorizedUserId: "mdB7yD2dp1BFZPonTHBQ1Z"} 200 (SUCCESS)
667 2021-06-25T18:00:48.000Z GET "/api/factory/machine/status?factory=seiko&machine=*" {authorizedUserId: "mdB7yD2dp1BFZPonTHBQ1Z"} 200 (SUCCESS)
668 2021-06-25T18:00:48.000Z GET "/api/factory/machine/status?factory=shenzhen&machine=*" {authorizedUserId: "mdB7yD2dp1BFZPonTHBQ1Z"} 200 (SUCCESS)
669 2021-06-25T18:00:48.000Z GET "/api/factory/machine/status?factory=berlin&machine=*" {authorizedUserId: "mdB7yD2dp1BFZPonTHBQ1Z"} 200 (SUCCESS)
670 2021-06-25T19:00:48.000Z GET "/api/factory/machine/status?factory=meiyok&machine=*" {authorizedUserId: "mdB7yD2dp1BFZPonTHBQ1Z"} 200 (SUCCESS)
671 2021-06-25T19:00:48.000Z GET "/api/factory/machine/status?factory=seiko&machine=*" {authorizedUserId: "mdB7yD2dp1BFZPonTHBQ1Z"} 200 (SUCCESS)
672 2021-06-25T19:00:48.000Z GET "/api/factory/machine/status?factory=shenzhen&machine=*" {authorizedUserId: "mdB7yD2dp1BFZPonTHBQ1Z"} 200 (SUCCESS)
673 2021-06-25T19:00:48.000Z GET "/api/factory/machine/status?factory=berlin&machine=*" {authorizedUserId: "mdB7yD2dp1BFZPonTHBQ1Z"} 200 (SUCCESS)
674 2021-06-25T20:00:48.000Z GET "/api/factory/machine/status?factory=meiyok&machine=*" {authorizedUserId: "mdB7yD2dp1BFZPonTHBQ1Z"} 200 (SUCCESS)
675 2021-06-25T20:00:48.000Z GET "/api/factory/machine/status?factory=shenzhen&machine=*" {authorizedUserId: "mdB7yD2dp1BFZPonTHBQ1Z"} 200 (SUCCESS)
676 2021-06-25T20:00:48.000Z GET "/api/factory/machine/status?factory=berlin&machine=*" {authorizedUserId: "mdB7yD2dp1BFZPonTHBQ1Z"} 200 (SUCCESS)
677 2021-06-25T21:00:48.000Z GET "/api/factory/machine/status?factory=meiyok&machine=*" {authorizedUserId: "mdB7yD2dp1BFZPonTHBQ1Z"} 200 (SUCCESS)
678 2021-06-25T21:00:48.000Z GET "/api/factory/machine/status?factory=seiko&machine=*" {authorizedUserId: "mdB7yD2dp1BFZPonTHBQ1Z"} 200 (SUCCESS)
679 2021-06-25T21:00:48.000Z GET "/api/factory/machine/status?factory=shenzhen&machine=*" {authorizedUserId: "mdB7yD2dp1BFZPonTHBQ1Z"} 200 (SUCCESS)
680 2021-06-25T21:00:48.000Z GET "/api/factory/machine/status?factory=berlin&machine=*" {authorizedUserId: "mdB7yD2dp1BFZPonTHBQ1Z"} 200 (SUCCESS)
681 2021-06-25T22:00:48.000Z GET "/api/factory/machine/status?factory=meiyok&machine=*" {authorizedUserId: "mdB7yD2dp1BFZPonTHBQ1Z"} 200 (SUCCESS)
682 2021-06-25T22:00:48.000Z GET "/api/factory/machine/status?factory=seiko&machine=*" {authorizedUserId: "mdB7yD2dp1BFZPonTHBQ1Z"} 200 (SUCCESS)
683 2021-06-25T22:00:48.000Z GET "/api/factory/machine/status?factory=shenzhen&machine=*" {authorizedUserId: "mdB7yD2dp1BFZPonTHBQ1Z"} 200 (SUCCESS)
684 2021-06-25T22:00:48.000Z GET "/api/factory/machine/status?factory=berlin&machine=*" {authorizedUserId: "mdB7yD2dp1BFZPonTHBQ1Z"} 200 (SUCCESS)
685 2021-06-25T23:00:48.000Z GET "/api/factory/machine/status?factory=meiyok&machine=*" {authorizedUserId: "mdB7yD2dp1BFZPonTHBQ1Z"} 200 (SUCCESS)
686 2021-06-25T23:00:48.000Z GET "/api/factory/machine/status?factory=seiko&machine=*" {authorizedUserId: "mdB7yD2dp1BFZPonTHBQ1Z"} 200 (SUCCESS)
687 2021-06-25T23:00:48.000Z GET "/api/factory/machine/status?factory=shenzhen&machine=*" {authorizedUserId: "mdB7yD2dp1BFZPonTHBQ1Z"} 200 (SUCCESS)
688 2021-06-25T23:00:48.000Z GET "/api/factory/machine/status?factory=berlin&machine=*" {authorizedUserId: "mdB7yD2dp1BFZPonTHBQ1Z"} 200 (SUCCESS)
689 2021-06-26T00:00:48.000Z GET "/api/factory/machine/status?factory=meiyok&machine=*" {authorizedUserId: "mdB7yD2dp1BFZPonTHBQ1Z"} 401 (UNAUTHORIZED)
690 2021-06-26T00:00:48.000Z GET "/api/factory/machine/status?factory=seiko&machine=*" {authorizedUserId: "mdB7yD2dp1BFZPonTHBQ1Z"} 401 (UNAUTHORIZED)
691 2021-06-26T00:00:48.000Z GET "/api/factory/machine/status?factory=shenzhen&machine=*" {authorizedUserId: "mdB7yD2dp1BFZPonTHBQ1Z"} 401 (UNAUTHORIZED)
692 2021-06-26T00:00:48.000Z GET "/api/factory/machine/status?factory=berlin&machine=*" {authorizedUserId: "mdB7yD2dp1BFZPonTHBQ1Z"} 401 (UNAUTHORIZED)
693 2021-06-26T01:00:48.000Z GET "/api/factory/machine/status?factory=meiyok&machine=*" {authorizedUserId: "mdB7yD2dp1BFZPonTHBQ1Z"} 401 (UNAUTHORIZED)
694 2021-06-26T01:00:48.000Z GET "/api/factory/machine/status?factory=seiko&machine=*" {authorizedUserId: "mdB7yD2dp1BFZPonTHBQ1Z"} 401 (UNAUTHORIZED)
695 2021-06-26T01:00:48.000Z GET "/api/factory/machine/status?factory=shenzhen&machine=*" {authorizedUserId: "mdB7yD2dp1BFZPonTHBQ1Z"} 401 (UNAUTHORIZED)
696 2021-06-26T01:00:48.000Z GET "/api/factory/machine/status?factory=berlin&machine=*" {authorizedUserId: "mdB7yD2dp1BFZPonTHBQ1Z"} 401 (UNAUTHORIZED)
697 2021-06-26T01:00:48.000Z GET "/api/factory/machine/status?factory=meiyok&machine=*" {authorizedUserId: "mdB7yD2dp1BFZPonTHBQ1Z"} 401 (UNAUTHORIZED)
```

Finding:

Internal Attacker details: UserID=mdB7yD2dp1BFZPonTHBQ1Z IP: 192.168.0.101

Evidence:

- (i) API calls every first 48th second, of every hour.
- (ii) Wildcard usage factory=*
- (iii) Not loading static assets like stylesheets (css)