On January 30, 2022 we received an email notification from AWS China Support about a suspected crypto-mining activity in our AWS account.

Immediately upon receiving the notification from AWS, we began to conduct an investigation of the incident regarding instance ID: **i-04604015cd7bdbfe2** in account ID: **373191821071 –** for possible abuse of our account for crypto-mining activity.

We detail below our findings per our available forensic data – and have also requested additional data from AWS to allow for additional conclusive analysis.

We have also, in parallel, defined further protective, monitoring and logging capabilities to allow us faster response for such incidents.

Investigation process:

【What specific investigations were taken?】

***Investigations conducted:***

Mobileye received the notification from Amazon on Sunday Jan 30th [04:26 IL time]

A joint Mobileye and Amazon Incident Response team was convened [~09:00 IL time] and a thorough investigation was launched.

1. Investigation of the identified instance -

We have identified the suspected instance i-04604015cd7bdbfe2 in our AWS CloudTrail logs.

we see the instance was up for ~6 hours, from 04:57:23 to 11:05:00 [UTC] on Jan 29th – after which it was terminated.



As the instance was terminated, prior to the alert, we are unable to investigate the actual file-system of the instance – for signs of intrusion and abuse.

**Note:** The instance involved in this alert, is designated as an 'ephemeral' workstation and is created upon request.

These workstations are provided to a 3rd party supplier, whose staff performs data analysis work on these workstations only.

Access to these instances is performed from the 3rd party supplier machines. We strongly authenticate user access through use of MFA and a unique password per instance, complex and randomly generated.

As we specifically designed these workstation instances to be short lived (to avoid data persistency and possible abuse), these instances are terminated upon end of use, or at the end of working hours in China; and in any case no later than after 12 hours.

\*\* Should a more precise time stamp of suspected actions be available- we may be able to correlate for better identification.

1. Investigation of instance connectivity -

For protection of our own data , this instance type is using a network Security Group which does NOT allow outbound traffic to go to the Internet.

It is only permitting outbound traffic to predefined IP addresses which are part of our business operation. As such, no traffic to Bitcoin mining destinations would be possible.



\*\* Should further details in regards to the traffic involved with the notification and alert be available, we may be able to correlate for better identification.

1. Investigation of monitoring – GuardDuty alerts

We are using AWS GuardDuty in this account for identification and alerting of anomalous actions, including Bitcoin-mining actions.

Our monitoring shows no indication or alert about Crypto-Mining activity for the recent period. Should an alert have been generated, our SOC (Security Operations Center)  would have initiated immediate response.



[The only alert GuardDuty had was about port scanning from the internet of a **different** instance ID]

We opened a support case (Case ID 1649765304) in AWS to understand why GuardDuty didn't alert about crypto-mining; and asked for further information.

              \*\* Should further details of the identification of suspicious activity be available, we shall be able to investigate with AWS.

1. Investigation of additional signs of anomalous activity -

We have also investigated the CPU usage of the specific instance.

This showed no evidence of crypto-mining activity either – which should be CPU intensive, as the CPU utilization never went beyond 25.1% during the lifetime of the instance:



***Findings:***

【What is the current survey result?】

Our available forensic data shows no positive indication of actual Bitcoin-mining activity in the instance.

To be able further investigate, we would appreciate any specific time-stamp details or traffic patterns that would allow us to correlate and analyze

***Disposal measures and follow-up reinforcement and rectification plan:***

[What rectification measures have been taken after the incident, and what plans are there in the future to ensure that this problem does not occur again]

We have added further prevention of uploading of files to these workstation instances – to prevent possibility of intrusion and abuse .

We are adding backup through snapshots of instances before termination, to allow investigation and analysis of file systems, if reoccurring.

In addition, we are adding further logging and monitoring capabilities to immediately identify such related alerts.