- **The complete time range of the incident: starting with the initial event (the spear phishing email) and ending with the final event (the last attempted but unsuccessful C2 communication).**

Initial event: [2017-12-29 20:58:29 GMT] Spear phishing emails are sent
Final event: [2018-01-08 16:40:49.938 GMT] Last attempted C2 communication (unsuccessful)

- **The timestamp at which the spear phishing email was sent and the recipients of the email.**

[2017-12-29 20:58:29 GMT] S.P. email sent to p.brand@at-usa.co
^siem_event_id: email:1:7383

[2017-12-29 20:58:29 GMT] S.P. email sent to m.land@at-usa.co
^siem_event_id: email:1:7430

[2017-12-29 20:58:30 GMT] S.P. email sent to d.walker@at-usa.co
^siem_event_id: email:1:7313

[2017-12-29 20:58:31 GMT] S.P. email sent to s.adams@at-usa.co
^siem_event_id: email:1:7255

- **The time range during which any AT-USA devices were exposed to the threat associated with ciso,guide (the EK landing page.)**

[2017-12-29 23:16:10.787 - 23:37:03.788 GMT] 10.5.10.127 is exposed to the threat
[2017-12-29 22:50:07.951 - 23:10:11.405 GMT] 10.5.10.130 is exposed to the threat
[2017-12-29 21:40:33.974 - 21:55:53.103 GMT] 10.5.10.128 is exposed to the threat
[2017-12-29 21:24:23.931 - 21:47:16.489 GMT] 10.5.10.129 is exposed to the threat

- **The time range during which malware payloads were delivered onto AT-USA devices by the EK. List the filenames of each payload.**

[2017-12-29 23:14:33.073 GMT] First payload ‘bilo400.exe’ is dropped on host Daniel-PC.

- **The time range during which any AT-USA device was actively infected with malware. This should be determined by the earliest and latest timestamps for the following specific events:**
    - **Execution events:**

        - **Timestamps of the first execution of the malware binary.**
          [2017-12-29 23:14:33.073 GMT] Process creation of the malicious 'bilo400.exe' malware file on Daniel-PC begins
        - **Timestamp of the last execution of the malware binary.**
          [2017-12-29 23:15:03.190 GMT] Last execution of malware binary
    - **Command and Control (C2) activity:**
        - **Timestamp of the initial connection with the malware's C2 server.**
          Initial connection with C2 server: [2017-12-29 23:16:34 GMT]
        - **Timestamp of the most recent successful connection established with the malware's C2 server.**
          Most recent successful connection with C2 server: [2018-01-02 05:39:55 GMT]
        - **Timestamp of the last attempted (but unsuccessful) connection established with the malware's C2 server.**
          Last attempted (but unsuccessful) connection with C2 server: [2018-01-08 16:40:49.938 GMT]