Team Viewer Integrations

Remote File Copy via TeamViewer

Identifies an executable or script file remotely downloaded via a TeamViewer transfer session.

Rule type: eql

Rule indices:

- winlogbeat-*
- logs-endpoint.events.*
- logs-windows.*

Severity: medium

Risk score: 47

Runs every: 5m

Searches indices from: now-9m (Date Math format, see also Additional look-back time)

Maximum alerts per execution: 100

References:

- https://blog.menasec.net/2019/11/hunting-for-suspicious-use-of.html

Tags:

- Elastic
- Host
- Windows
- Threat Detection
- Command and Control

Version: 5

Rule authors:

- Elastic

Rule license: Elastic License v2

Rule query

file where event.type == "creation" and process.name : "TeamViewer.exe" and

file.extension : ("exe", "dll", "scr", "com", "bat", "ps1", "vbs", "vbe", "js", "wsh", "hta")

Framework: MITRE ATT&CKTM

- Tactic:
    - Name: Command and Control
    - ID: TA0011
    - Reference URL: https://attack.mitre.org/tactics/TA0011/
- Technique:
    - Name: Ingress Tool Transfer
    - ID: T1105
    - Reference URL: https://attack.mitre.org/techniques/T1105/
- Technique:
    - Name: Remote Access Software
    - ID: T1219
    - Reference URL: https://attack.mitre.org/techniques/T1219/

Source: https://www.elastic.co/guide/en/security/master/prebuilt-rule-0-14-2-remote-file-copy-via-teamviewer.html

TeamViewer Integration Procedure

1. Install the Elastic Stack (Elasticsearch, Kibana, and Logstash) on your Ubuntu machine by following the instructions provided on the Elastic website.

Graphical user interface, text, applicationDescription automatically generated

2. Once you have installed and configured the Elastic Stack, navigate to the Logstash directory and create a new configuration file for the TeamViewer logs by running the command:

Copy and paste the following Logstash configuration into the file:

TextDescription automatically generated

3. Save and close the file.
4. Start Logstash by running the command:

```sql
sudo service logstash start
```

5. Ensure that Logstash is properly reading and processing the TeamViewer logs by checking the Logstash logs in the /var/log/logstash/ directory.
6. Navigate to the Kibana web interface by opening a web browser and entering the URL: http://localhost:5601/.
7. In Kibana, click on the "Discover" tab to view your logs.
8. Click on the "Create index pattern" button and enter the name of the TeamViewer index pattern (e.g. teamviewer-*).
9. Select the time range for the logs you want to view, and click on the "Create index pattern" button.
10. You should now see a list of logs from your TeamViewer deployment. You can filter the logs based on various criteria like severity, source, or date.
11. You can also create custom dashboards or visualizations to monitor specific aspects of your TeamViewer deployment, such as usage patterns or connection quality.
12. If you encounter any issues with your TeamViewer deployment, you can use the logs to identify the root cause and take corrective action.

Source: ChatGPT

1. Elastic official documentation: https://www.elastic.co/guide/index.html

2. Logstash input plugin documentation:
   https://www.elastic.co/guide/en/logstash/current/plugins-inputs-file.html

3. Logstash output plugin documentation:
   https://www.elastic.co/guide/en/logstash/current/plugins-outputs-elasticsearch.html

4. Kibana official documentation: https://www.elastic.co/guide/en/kibana/current/index.html

---

Revision #2
Created 23 April 2024 14:49:57
Updated 19 June 2024 06:54:01