

## General

The screenshot shows a web interface for a threat object. On the left is a blue sidebar with navigation links: General (selected), Report, Vulnerabilities, Technologies, Exploits, Related Links, Targeted Entities, Related Threats, Tickets, and Incidents. The main content area is titled 'Threat: TOMMYGUN Malware Overview' and has an 'Edit' button in the top right. It is divided into three sections: 'Threat Information', 'Mitigation Status', and 'Change History'. The 'Threat Information' section lists various attributes such as Type, Subtype, Source, Title, Description, Published Date, Last Updated, Owner, Reference Count, Severity, Likelihood, Risk, Risk Rating, Risk Score, Exploit Rating, Proof Of Concept Exploit, Quantity of Proof Of Concept Exploits, Weaponized Exploit, Quantity of Weaponized Exploits, Exploited in the Wild, Quantity of Exploits Exploited in the Wild, Exploitation Consequence, and Zero Day/Early Warning. The 'Mitigation Status' section shows Status as 'New' and Comment as 'N/A'. The 'Change History' section shows results as of 2021-06-01 15:47:04, with a 'Save as CSV' button, a 'Filter by' dropdown set to '- Show all -', and a 'Refresh' button. Below this is a table header with columns: Changed Attribute, Old Value, New Value, Who, and When. A message box below the table states 'No change records found.'

Threat: TOMMYGUN Malware Overview Edit

**General**

Report

Vulnerabilities

Technologies

Exploits

Related Links

Targeted Entities

Related Threats

Tickets

Incidents

**Threat Information**

Type Threat

Subtype N/A

Source FireEye

Title TOMMYGUN Malware Overview

Description TOMMYGUN Malware Overview

Published Date 2020-03-22

Last Updated N/A

Owner N/A

Reference Count N/A

Severity N/A

Likelihood N/A

Risk N/A

Risk Rating N/A

Risk Score N/A

Exploit Rating N/A

Proof Of Concept Exploit N/A

Quantity of Proof Of Concept Exploits N/A

Weaponized Exploit N/A

Quantity of Weaponized Exploits N/A

Exploited in the Wild N/A

Quantity of Exploits Exploited in the Wild N/A

Exploitation Consequence N/A

Zero Day/Early Warning N/A

**Mitigation Status**

Status New

Comment N/A

**Change History**

Results as of 2021-06-01 15:47:04

[Save as CSV](#) Filter by - Show all - [Refresh](#)

Changed Attribute	Old Value	New Value	Who	When
No change records found.				

*The General tab.*

The **General** tab of the **Threat** object pop-up displays the following fields:

- **Type:** Type of report that RiskVision imported.
- **Subtype:** Subtype of report that RiskVision imported.
- **Source:** Threat feed provider.
- **Identifier:** ID assigned by threat intelligence provider.
- **Title:** Descriptive name of the threat intelligence.
- **Description:** Summary of the threat intelligence.
- **Owner:** The person responsible for analyzing or mitigating the threat.
- **Reference Count:** The number of references for the threat report. The higher the number, the greater the threat.
- **Severity:** Severity of the threat. You need to manually select this field. Possible values include:
  1. Informational (score = 1)
  2. Low (score = 2)
  3. Medium (score = 3)
  4. High (score = 4)
  5. Critical (score = 5)
- **Likelihood:** You need to manually select this field. The Likelihood values are ordered as follows:
  1. Unlikely (score = 1)

2. Possible (score = 2)
  3. Likely (score = 3)
  4. Almost Certain (score = 4)
  5. Certain (score = 5)
- **Risk:** The risk posed by the threat. This is a calculated field and cannot be edited. Calculated Risk = (Severity \* Likelihood). Risk values are as follows:
    1. Very Low (1 score)
    2. Low (2 - 5 score)
    3. Medium (6 - 11 score)
    4. High (12 - 19 score)
    5. Very High (20 - 25 score)
  - **Risk Rating:** The rating assigned to the threat by the feed.
  - **Risk Score:** The threat's quantitative risk score as reported by threat intelligent providers.
  - **Exploit Rating:** The rating assigned to the threats exploit by the feed. The higher the rating, the more dangerous the threat is.
  - **Proof of Concept Exploit:** Marked **True** if the threat has an exploit code, **False** if it doesn't.
  - **Quantity of Proof of Concept Exploits:** The number of proof of concept exploits that exist for this threat.
  - **Weaponized Exploit:** Marked **True** if the exploit has been automated, **False** if it hasn't.
  - **Quantity of Weaponized Exploits:** The number of weaponized exploits that exist for this threat.
  - **Exploited in the Wild:** Marked **True** if the threat has been exploited in a real-life setting, **False** if it hasn't.
  - **Quantity of Exploits in the Wild:** The number of exploits that have been exploited in the wild, not the number of times an exploit has been exploited in the wild.
  - **Exploitation Consequence:** The consequences of the threat's exploit.
  - **Zero Day/Early Warning:** Will display whether or not there is an early warning for this threat.
  - **Status:** Potential values are as follows:
    1. New
    2. Acknowledged
    3. Investigating
    4. Ignore
    5. Mitigating
    6. Mitigated