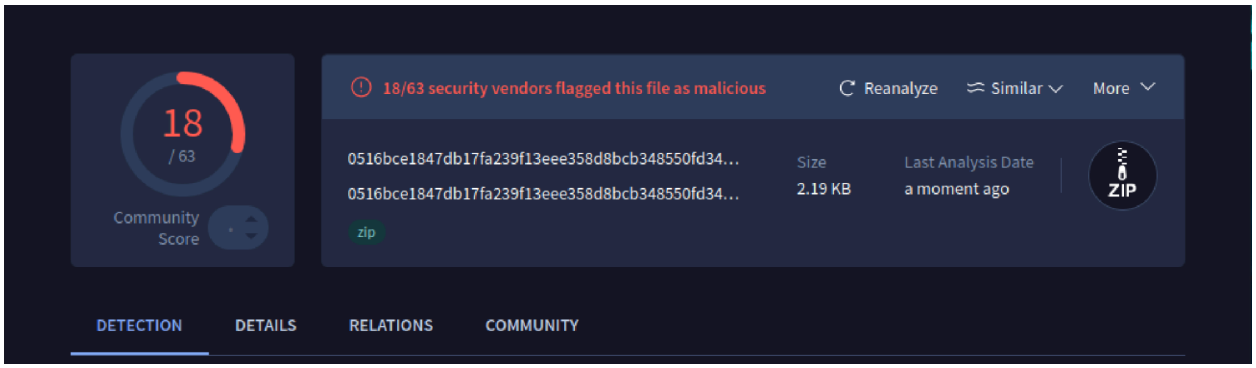
ScreenShots:



Here's a sample report based on the provided screenshots:

Malware Scan Report

File Details

- **Hash**: `0516bce1847db17fa239f13eee358d8b348550fd34...`
- **File Type**: ZIP Archive
- **File Size**: 2.19 KB

Scan Summary

The file was analyzed by 63 security vendors, and **18 of them flagged it as malicious**. The detections primarily identify the file as a form of Trojan, suggesting it is a potentially harmful file that could execute unauthorized actions on a system.

Key Detection Results

Vendor	Detection
Avira	HEUR/Suspar.Gen
CTX	Zip.trojan.generic
Google	Detected
Kaspersky	HEUR:Trojan.Script.Generic
NANO-Antivirus	Trojan.Script.Heuristic-js.iacgm
Sophos	Mal/DrodZp-A
Trellix (HX)	Trojan.GenericKD.75352686
Tencent	Script.Trojan.Generic.Pzfl
VirIT	Trojan.Win32.MSIL_Heur.A

Common Classifications:

- **Trojan-Downloader**: Indicates the file may be used to download additional malicious payloads onto the system.
- **Generic Heuristics**: Many vendors classified the file using heuristic analysis, implying it exhibits behavior similar to known malware.

Risk Level: High

Despite not all vendors detecting the file as malicious, the results from reputable sources like Kaspersky, Google, and Avira suggest it contains harmful components. The small file size also raises concerns, as it could serve as a downloader or dropper.

Recommendations

1. **Do Not Open or Execute the File**:

    - Avoid extracting or running the ZIP file to prevent triggering any harmful actions.
2. **Further Analysis**:
    - Submit the file for dynamic analysis in a controlled sandbox environment to understand its behavior.
3. **Update Security Tools**:
    - Ensure your antivirus and antimalware tools are updated to prevent any infection.
4. **System Monitoring**:
    - If the file has been accessed, monitor your system for unusual behavior or unauthorized connections.
5. **Block and Quarantine**:
    - Blocklist the file on your network and quarantine it to prevent accidental access.

This report suggests a proactive approach to avoid risks associated with potentially malicious files.

Likely Actions of This Malware

1. **Downloading Additional Malicious Payloads**:
    - **Trojan-Downloader** detections (e.g., from Ikarus and others) suggest that the file might be designed to connect to a remote server and download additional malicious files or programs. These payloads could range from ransomware to spyware.
2. **Stealing Sensitive Information**:
    - Some vendors flagged it as **Trojan.Script.Generic** or similar, which suggests it might harvest sensitive data, such as:
        - Login credentials (via keylogging or form grabbing).
        - Payment details.
        - Stored browser data or files on the system.
3. **Remote Command Execution**:
    - As a Trojan, it could allow attackers to execute commands on the infected system, potentially granting them control over the device. This could include installing other malware, modifying files, or creating backdoors for later access.
4. **Exploitation**:
    - Heuristic detections (e.g., from NANO-Antivirus) indicate that the malware may exploit vulnerabilities in the system or applications to escalate privileges or avoid detection.
5. **Spreading to Other Systems**:
    - If part of the ZIP file includes scripts or programs designed for propagation, it could spread across a network or via removable drives, targeting more devices.
6. **Creating Persistence**:
    - Malware of this type often creates persistence by modifying registry keys, adding itself to startup programs, or hiding in system directories to ensure it runs every time the system starts.

7. **Potentially Dropping Ransomware**:
    - While not explicitly detected as ransomware, its ability to download other malicious files means it could install ransomware on the system, encrypting files and demanding payment.

Why It's Dangerous

- **Heuristic Detections**: Several vendors used heuristic analysis, meaning the file exhibits behaviors common to a wide variety of malicious programs, making it difficult to pinpoint its exact functionality.
- **Small File Size**: The small size (2.19 KB) suggests it may be a loader or downloader, designed to evade detection initially and then pull in larger malicious payloads.

How It Works

1. **Infection**:
    - The malware is likely activated when the ZIP file is extracted, or when a file inside it is executed.
2. **Execution**:
    - Once active, it connects to a remote server (command-and-control, or C2) to receive instructions or download additional files.
3. **Harmful Activities**:
    - Depending on its payload, it could:
        - Install additional malware.
        - Steal data or spy on user activities.
        - Cause financial harm through theft or fraud.
        - Turn the infected device into part of a botnet.

Conclusion

The malware in this ZIP file likely acts as a **Trojan-downloader or info-stealer**, with capabilities to extend its malicious actions through other downloaded payloads. It's highly recommended to avoid executing the file and to investigate further in a sandboxed environment if needed.