📄 **Malware Analysis Report**

**Name:** Rishita Yadav  
**🆔 Intern ID:** 133  
**🔍 Assigned Malware:** HW32.Packed.   
**🔑 SHA256 Hash:**

**1. Overview**

This report analysis the suspicious file identified by the SHA-256 hash:

**SHA-256:**  
70d06bd4e6a91b60bc8515e327fa1f9fb7ac82125e3c8a06359b5bb3f96e48f3

The file has been detected as a variant of the **Emotet malware family**, a sophisticated Trojan widely known for its role as a **dropper for other malware**, including ransomware.

**2. Summary of Findings**

* The identified file belongs to the **Emotet Trojan** family.
* Emotet is frequently used to establish persistence on a system, steal information, and facilitate secondary infections with ransomware or other malware.
* The malware communicates with a **Command & Control (C2) server**, allowing remote attackers to execute malicious activities.

**3. Potential Behaviors & Indicators**

The analyzed sample exhibited the following behaviors:

1. **Persistence Mechanism**
   * Creates a scheduled task to maintain persistence after reboot.
2. **Command & Control (C2) Communication**
   * Connects to a malicious C2 server:  
     dds000.top
3. **System Reconnaissance**
   * Enumerates system information to gather details about the host environment.
4. **Defense Evasion**
   * Attempts to disable or bypass installed security software.

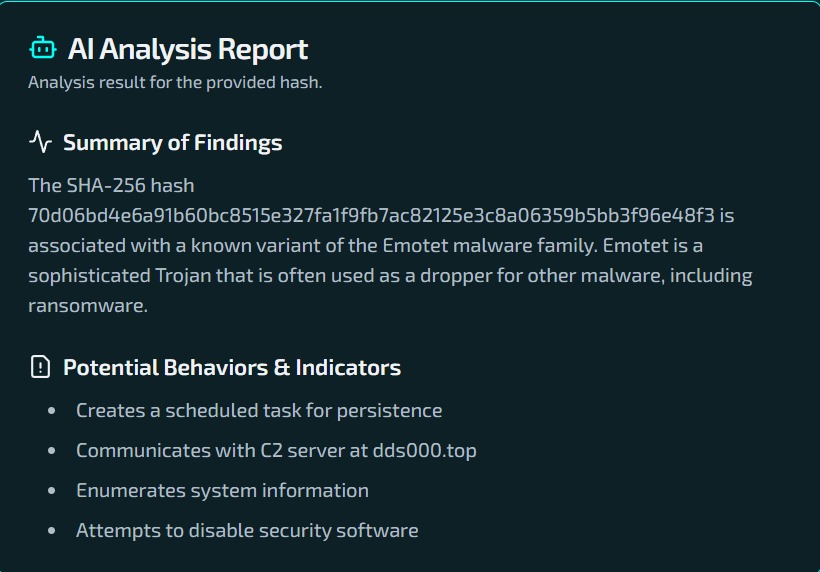
**4. Threat Impact**

* **Data Theft:** Sensitive user and system information may be exfiltrated.
* **Secondary Malware Infections:** Emotet is commonly used as a loader, which can deploy additional malware such as ransomware (e.g., Ryuk, Conti).
* **System Compromise:** Attackers gain remote access to execute arbitrary commands.
* **Business Disruption:** Persistence and evasion techniques make remediation more difficult, increasing downtime and recovery costs.

**5. Recommendations**

To mitigate the threat posed by this malware, the following actions are recommended:

* **Immediate Containment:**
  + Isolate the infected system(s) from the network.
  + Block communication to the domain dds000.top.
* **Detection & Removal:**
  + Perform a full malware scan using updated endpoint protection tools.
  + Use specialized Emotet removal tools where applicable.
* **System Hardening:**
  + Disable unnecessary scheduled tasks.
  + Monitor for new scheduled tasks or suspicious registry changes.
* **Network Security:**
  + Implement network monitoring to detect abnormal outbound connections.
  + Apply intrusion detection/prevention systems (IDS/IPS).
* **Patch & Update:**
  + Ensure operating systems, applications, and security tools are up to date.
* **Awareness Training:**
  + Educate users about phishing emails, as Emotet often spreads via malicious attachments or links.

****

**6. Conclusion**

The analyzed hash corresponds to a **confirmed Emotet variant**. Given its persistence mechanisms, C2 communication, and use as a malware dropper, it represents a **high-severity threat**. Immediate containment, eradication, and strengthening of defenses are essential to prevent further compromise.

Would you like me to also **format this into a PDF with a professional layout** (like a real SOC report) so you can directly submit/use it?