Malware Analysis

Proof of Concept (PoC) Document: Trojan.Ransom.Locky.AZ

Name: Soham Kadu
Intern ID: *235*

---

1. Introduction

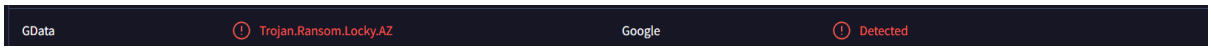
This document provides a simplified yet informative Proof of Concept (PoC) analysis of the malware sample identified as **Trojan.Ransom.Locky.AZ**. The file was analyzed using VirusTotal, where it was flagged by multiple antivirus engines. The purpose of this document is to explore:

- What is Trojan.Ransom.Locky.AZ?
- Why it may have been flagged
- How dangerous it is
- Safe techniques to analyze and detect such threats

---

2. Overview of the Detection

Detection Name: Trojan.Ransom.Locky.AZ
File Hash (SHA-256):
5ed2f09e648dca8f0ca75466b1442f6e599afddc80777e0559fb6881c6cd9ff3
Detected By: Multiple Antivirus Engines on VirusTotal



This malware sample was flagged by a significant number of antivirus engines, indicating a high probability that the file is malicious and dangerous. Locky ransomware is known for encrypting user files and demanding ransom payments in cryptocurrency.

---

3. What is Locky Ransomware?

Locky is a notorious **ransomware family** first seen in 2016 and widely distributed through malicious email attachments and exploit kits. Key characteristics of Locky include:

- Encrypts user documents (e.g., .doc, .jpg, .xlsx) with strong RSA/AES encryption
- Renames files with random extensions like .locky, .zepto, .odin
- Drops a **ransom note** demanding payment in **Bitcoin**
- Deletes shadow copies to prevent recovery
- Uses command-and-control (C2) servers to communicate with attackers

---

4. Possible Causes of the Detection

Scenario	Explanation
Known Ransomware	Most antivirus engines identify Locky due to its well-known encryption behavior
File Encryption	It encrypts data and demands payment, a hallmark of ransomware
Network Behavior	It often contacts remote C2 servers or drops files
Packed/Obfuscated Code	Locky uses obfuscation to avoid detection, increasing false positives in generic tools

---

5. Safe Analysis Methods

A. Use a Virtual Machine (VM)

Run the sample in **VirtualBox** or **VMware** with no network connection. Take VM snapshots before and after to observe changes.

B. Upload to Online Sandboxes

Submit the file to:

- Any.Run
- Hybrid Analysis
- Joe Sandbox

These provide detailed dynamic behavior without risking your local system.

C. Use Strings & PE Tools

Tools like:

- strings
- **PEStudio**
- **Detect It Easy (DIE)**

can help you inspect the binary without running it.

D. Monitor with Process Monitor

Use **Procmon** and **Process Explorer** to track:

- File operations
- Registry modifications

---

6. Remediation and Recommendations

If Locky or any ransomware is suspected:

- **Immediately isolate the machine** from the network
- **Do not pay the ransom** – there's no guarantee of data recovery
- Use ransomware decryption tools if available (from NoMoreRansom.org)
- Keep **backups** of critical data offline
- Avoid clicking on suspicious emails or downloading unknown attachments
- Use reputable antivirus and keep it **up to date**

---

7. Conclusion

The detection of **Trojan.Ransom.Locky.AZ** indicates a high-risk ransomware infection capable of encrypting files and demanding a ransom. It is crucial to handle such samples in a secure environment and follow structured analysis techniques. Prevention and preparation, such as user awareness and regular backups, are key to reducing ransomware impact.

---

8. Proof of Concept from VirusTotal