Malware Analysis

Proof of Concept (PoC) Document: Gen:Variant.Razy.107792

Name: Akkshat Shah

Intern id:261

---

1. Introduction

This document provides a simplified but detailed Proof of Concept (PoC) on the detection of a malware variant identified as **Gen:Variant.Razy.107792**. This detection was observed in a VirusTotal scan where the file was flagged by Emsisoft and eScan antivirus engines. The aim of this PoC is to understand:

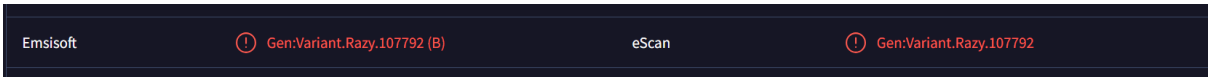
- What is this malware?
- Why it might have been flagged
- Whether it is dangerous
- How to analyze and handle it safely

---

2. Overview of the Detection

Detection Name: Gen:Variant.Razy.107792
Detected By: Emsisoft (B), eScan

Proof of Concept taken from VirusTotal websit



This means that **only 2 antivirus engines** flagged this file as malicious, out of the 70+ typically used by VirusTotal. Such low detection count may indicate:

- A false positive
- A new or low-risk variant
- A potentially unwanted application (PUA)

---

3. What is Razy Malware?

Razy is a family of malware known for:

- Injecting ads into websites
- Hijacking cryptocurrency-related traffic (like wallets or trading sites)
- Modifying browser settings or extensions
- Spreading via cracked software, torrents, or fake updates

Variant:107792 refers to a specific signature used by Emsisoft and eScan to detect this particular sample. It does **not** necessarily mean it's highly dangerous—it might be based on heuristics or patterns similar to known Razy samples.

---

4. Possible Causes of the Detection

There are a few scenarios why this detection could occur:

Scenario	Explanation
False Positive	If only 1–2 AVs detect it and others don't, the file might be safe but misflagged
Modified Software	If the file is from unofficial sources (e.g. cracked software), it might have been altered
Obfuscated Code	Some programs use code packing/obfuscation which triggers antivirus alarms even if they are harmless

---

5. Safe Analysis Methods

To analyze a suspicious file safely, you can:

A. Use a Virtual Machine (VM):
Install Windows or Linux in a VM using VirtualBox or VMware. Run the file inside the VM to observe its behavior without risking your real system.

B. Upload to Online Sandboxes:
Platforms like **Any.Run**, **Hybrid Analysis**, or **Joe Sandbox** simulate execution and show file behavior in detail.

C. Use Strings & PE Tools:
Using tools like `strings`, `PEStudio`, or `Detect It Easy` can help peek into the internals of the file without running it.

D. Monitor with Process Monitor:
Sysinternals tools like `procmon.exe` and `Process Explorer` help track suspicious behavior like network connections or registry changes.

---

6. Remediation and Recommendations

If you suspect a file is infected:

- **Delete or quarantine** the file if not needed
- **Scan with multiple AVs** (e.g., Malwarebytes, Bitdefender)
- **Update OS and AV software** to avoid vulnerabilities
- **Avoid cracked software or suspicious email links**
- **Use browser extensions carefully** — many Razy variants come through shady browser plugins

---

7. Conclusion

The detection of `Gen:Variant.Razy.107792` by only two antivirus vendors suggests caution but not panic. It could be a false positive or a low-risk malware variant. The file should be examined in a sandboxed or isolated environment if necessary.

Following proper analysis steps and understanding the behavior is key to accurate judgment. Malware analysis should always be done carefully to avoid system compromise.