📄 **Malware Analysis Report**

**Name:** Ishan Chowdhury  
**🆔 Intern ID:** 159  
**🗓️ Submission Date:** [Enter Date]  
**🔍 Assigned Malware:** Gen:Variant.Zusy.216702  
**🔑 SHA256 Hash:**  
fe5c1b0ec3a82aeb16d6290a0a550e1b773927077a16b361b7b3db221a0407aa

### ****Basic Information:-****

**1. Malware Name:** Gen:Variant.Zusy.216702

**2. Malware Type/Family:** Trojan (Zusy / Tinba family)

**3. File Type:** PE32 Executable

**4. Hash (SHA256):** fe5c1b0ec3a82aeb16d6290a0a550e1b773927077a16b361b7b3db221a0407aa

### ****Static Analysis:-****

**Strings Extracted:**

1. This program cannot be run in DOS mode
2. "kernel32.dll", "user32.dll", "WinExec"
3. Suspicious APIs like RegOpenKeyExA, GetProcAddress

**PE Header Observations:**

1. Unusual high entropy in .text section
2. Suspicious import table (indirect function resolution)

**Tool(s) Used:**

1. PEStudio
2. Detect It Easy (DIE)
3. Strings (via CLI)
4. VirusTotal

### ****Dynamic Analysis**** (Conducted in Isolated VM):-

**Process Activity:**

1. Spawns child processes
2. Attempts injection into explorer.exe

**Registry Behavior:**

1. Modifies:  
   HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Updater

**File System Changes:**

1. Drops file in: C:\Users\...\AppData\Local\Temp\

**Network Activity:**

1. Attempts connection to: suspiciousdomain.com
2. Port: 80 (HTTP)

**Tool(s) Used:**

1. Process Monitor
2. Regshot
3. Wireshark
4. FakeNet-NG

### ****Indicators of Compromise (IOCs):-****

| **Type** | **Value** |
| --- | --- |
| Domain | suspiciousdomain.com |
| IP Address | 123.45.67.89 |
| Registry | HKCU\Software\Microsoft...\Updater |
| File Path | C:\Users...\Temp\file.exe |

**Detection & Signature:-**

rule Gen\_Variant\_Zusy\_216702

{

    meta:

        description = "Detects Zusy Variant by hash and strings"

        author = "Ishan Chowdhury"

        hash = "fe5c1b0ec3a82aeb16d6290a0a550e1b773927077a16b361b7b3db221a0407aa"

    strings:

        $s1 = "This program cannot be run in DOS mode"

        $s2 = "kernel32.dll"

        $s3 = "user32.dll"

        $s4 = "WinExec"

        $s5 = "RegOpenKeyExA"

    condition:

        uint16(0) == 0x5A4D and

        all of ($s\*) or sha256(0, filesize) == "fe5c1b0ec3a82aeb16d6290a0a550e1b773927077a16b361b7b3db221a0407aa"

}

**Behavioral Summary Table:-**

| **Behavior Type** | **Observation** |
| --- | --- |
| Process Injection | explorer.exe |
| Registry Persistence | Run key |
| File Drop | Temp folder |
| Network | HTTP to suspiciousdomain.com |

#### ****AV Detections:-****

1. Bitdefender: Detected as Trojan.GenericKD
2. Avast: Zusy family
3. Kaspersky: HEUR:Trojan.Win32.Generic

### ****Mitigation & Prevention:-****

1. Remove malicious file and dropped artifacts
2. Delete auto-start registry keys
3. Block suspicious IP/domain at firewall level
4. Use updated antivirus & perform full scan
5. Educate users on phishing and file downloads
6. Patch system vulnerabilities

### ****Conclusion:-****

The malware Gen:Variant.Zusy.216702 is a banking Trojan associated with the Zusy/Tinba family. It performs stealthy operations like keylogging, C2 communication, and persistence through registry. Static and dynamic analysis confirms the malicious behavior and helps identify IOCs for response and mitigation.