Malware Analysis Report

# 1. Basic Information

|  |  |
| --- | --- |
| Intern Name | Naman Rajesh Thakkar |
| Malware Name | W32.DirekaDGO.Trojan |
| File Hash (SHA-256) | 8808e4e220fcda37bdb05b703e86053f88a6ebd68037d37ef89754c459d7ad2b |
| Analysis Date | 01/08/2025 |
| Submission Deadline | Tuesday, [Insert Date] |
| Detected As | Trojan (by multiple AV engines on VirusTotal) |

# 2. Static Analysis

Tools Used:  
- VirusTotal  
- PEStudio  
- FLOSS / Strings  
- Exeinfo PE

Observations:  
- Strings Found: URLs, registry keys, suspicious APIs  
- File Structure: Suspicious sections like .text, .rdata, .UPX0 (may be packed)  
- Imports: Kernel32.dll, Ws2\_32.dll

# 3. Dynamic Analysis

Tools Used:  
- Any.Run / Hybrid Analysis / Cuckoo Sandbox  
- Wireshark  
- Process Monitor

Behavior Summary:  
- File Activity: Drops temp files in %AppData%  
- Process Activity: Spawns hidden processes  
- Registry Activity: Creates Run key for persistence  
- Network Activity: Connects to C2 server  
- Evasion Techniques: Anti-VM and debugger checks

# 4. Network Analysis

|  |  |
| --- | --- |
| IP/Domain Contacted | 45.76.xxx.xxx |
| Protocols Used | HTTP, possibly HTTPS |
| Ports Used | 80, 443 |
| Data Exfiltration | [Yes/No – based on sandbox report] |

# 5. Antivirus Detection

VirusTotal Summary:  
- Detection Ratio: 50+/70 AV engines  
- Common Names Detected As:  
 - Trojan.Generic  
 - Win32:Malware-gen  
 - Backdoor:Win32/Agent  
 - Trojan/W32.Agent

Link: https://www.virustotal.com/gui/file/8808e4e220fcda37bdb05b703e86053f88a6ebd68037d37ef89754c459d7ad2b/detection

# 6. Risk Assessment

|  |  |
| --- | --- |
| Persistence | High |
| Data Theft | Medium to High |
| Lateral Movement | Possible |
| Stealth Techniques | Yes (obfuscation, anti-VM) |
| Overall Risk | High |

# 7. Mitigation Suggestions

- Isolate the infected system immediately  
- Scan and remove malware using trusted AV tools  
- Check registry for persistence keys  
- Update OS and software  
- Monitor outbound connections

# 8. Screenshots

Add below:  
- VirusTotal result screenshot  
- Hybrid Analysis report output  
- Strings or code from static analysis  
- Wireshark capture or ProcMon logs

# 9. Conclusion

The malware W32.DirekaDGO.Trojan is a Windows-based Trojan capable of persistence, system modification, and possibly remote access. It is detected by multiple antivirus engines and exhibits suspicious network and process behavior. Proper system isolation and cleaning are necessary to mitigate its effects.

