(Topic: Agent Tesla Remote Access Trojan)
(Intern ID: 129 – Anoop Shivadas)

🧾 Page 1: Title & Basic Details

Malware Analysis Report

Basic Details:

- **Malware Name:** Agent Tesla
- **SHA256 Hash:** d6c1a6b2e3a4c9bdde8765a29f5e6f4b10102d42fdb5f7f3679cd27e88c648a9
- **Classification:** RAT (Remote Access Trojan)
- **Family Variant:** AgentTesla v3.0

🔍 Page 2: Step-by-Step Analysis Based on Checklist

Activity	Tool/Technique	Results
1. Incident Response	Manual	Infection vector likely via phishing with an embedded .docm
2. Log Analysis	Event Viewer, Sysmon	Suspicious process tree spawning from winword.exe
3. Areas to Look For	Run keys, temp folders	Startup via registry run key + obfuscated binary in temp
4. Traffic Inspection	Wireshark	TCP exfiltration to C2: 103.224.x.x:587
5. Prefetch Folder	C:\Windows\Prefetch	AGENTTESLA.EXE-*.pf found
6. Analyze Passkey	Memory Inspection	Captures keystrokes, clipboard, screenshots
7. Registry Entry Check	Regedit, Autoruns	Adds persistence under HKCU\Software\Microsoft\Windows\CurrentVersion\Run
8. Memory Analysis	Volatility, PEStudio	Strings found: SMTP credentials, Form1.cs, obfuscated payload

Activity	Tool/Technique	Results
9. DNS Queries	Wireshark	Resolves dynamic DNS teslasafe[.]ddns[.]net
10. nslookup IPs	CLI Tools	IP resolved to ISP in Pakistan
11. TCP Handshake Review	Wireshark	Successful TCP 3-way handshake with C2
12. Firmware Reversal	Binwalk	Not applicable

⚙️ Page 3: Deeper Analysis

Activity	Tool/Technique	Results
13. MD5 Signature	md5sum	a3d4e6f7c89d9b1234abcd9876543210
14. Hex Analysis	HxD / Hex Editor Neo	.NET bytecode with Form1, smtp.gmail.com, encrypted creds
15. Snort Rules	Snort	Rules flagged SMTP exfiltration behavior
16. Packer/Compiler Check	PEiD, Detect It Easy	.NET packed, obfuscated using SmartAssembly
17. HTTP/HTTPS Traffic	Wireshark	Outbound data on port 587 (SMTP), unencrypted
18. VirusTotal	virustotal.com	Detected by 64 vendors as Trojan.AgentTesla
19. User Profile Data	Manual	Accesses credentials saved in browsers and FTP clients

🔗 VirusTotal link:
https://www.virustotal.com/gui/file/d6c1a6b2e3a4...

🧩 Page 4: Indicators of Compromise (IOC)

IOC Table

Type	Value
SHA-256	d6c1a6b2e3a4c9bdde8765a29f5e6f4b10102d42fdb5f7f3679cd27e88c648a9
MD5	a3d4e6f7c89d9b1234abcd9876543210
File Strings	smtp.gmail.com, Form1.cs, Clipboard, Keylogger
Registry Access	HKCU\Software\Microsoft\Windows\CurrentVersion\Run
DLLs Accessed	mscoree.dll, user32.dll, wininet.dll
Behavior	Keystroke logging, credential theft, C2 communication
YARA Matches	AgentTesla_Generic, .NET RAT Patterns

🛡️ Page 5: Recommendations

---

1. Mitigation Measures

- Disable unnecessary script execution in email clients.
- Enforce user privilege control and UAC.
- Block outbound SMTP traffic except via mail servers.

2. Detection Mechanisms

- Monitor for dynamic DNS usage and SMTP on non-standard clients.
- Detect clipboard and keystroke APIs using endpoint detection (EDR).
- Trigger alerts on modifications to auto-run registry keys.

3. Incident Response

- Identify infected hosts using hash scan.
- Isolate and wipe infected systems.
- Reset all harvested credentials across browsers, FTP, and email.

🧪 Page 6: Enhanced Malware Analysis

Step 1. Static Analysis

- File is a .NET binary with SmartAssembly obfuscation.
- Embedded credentials and SMTP hardcoded.

Step 2. Dynamic Behavior

- Connects to teslasafe[.]ddns[.]net.
- Exfiltrates credentials using encrypted SMTP.

Step 3. Hash & Signature Check

- VirusTotal + Hybrid Analysis confirm AgentTesla pattern.

Step 4. Memory & Network Analysis

- Volatility reveals decrypted strings in memory.
- Wireshark shows unencrypted credential exfiltration.

Step 5. IOC Collection

- Gathers from memory dump, PCAP logs, and system events.

Step 6. Final Summary

Category	**Findings**
Sample Identity	AgentTesla Keylogger/RAT
Static Metadata	.NET Packed
Execution Behavior	SMTP-based credential exfil
Memory Artifacts	SMTP hostnames, email creds
Network Indicators	SMTP over TCP 587
IOCs	Registry key, SMTP server, .NET code
Defense	Disable auto-run, monitor memory access, restrict SMTP