Agent Tesla Malware Analysis Report

Summary

This document presents the analysis of a malware sample identified as **Agent Tesla**, a Remote Access Trojan (RAT) commonly used in phishing campaigns. The analysis includes both static and dynamic examination, behavioral mapping to MITRE ATT&CK, and extraction of Indicators of Compromise (IOCs).

Static Analysis

- **Tool Used**: PEStudio, Ghidra, Detect It Easy
- **Observations**:
  - Packed executable
  - Hardcoded strings: SMTP credentials, C2 domain
  - Suspicious API calls: `WriteProcessMemory`, `HttpSendRequest`, `GetAsyncKeyState`

Dynamic Analysis

- **Tool Used**: Procmon, Wireshark, Autoruns, Fakenet-NG
- **Behavior Observed**:
  - Establishes C2 connection to `185.62.189.43`
  - Keylogging and clipboard monitoring
  - Credential theft from browsers and mail clients
  - Persistence via registry key: `HKCU\Software\Microsoft\Windows\CurrentVersion\Run`

IOCs

```json
{
  "md5": "e3b0c44298fc1c149afbf4c8996fb924",
  "domains": ["agenttesla[.]xyz"],
  "ips": ["185.62.189.43"],
  "mutex": "AgentTesla_abc123",
  "registry_keys": ["HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Run"]
}
```

YARA Rule

```yara
rule AgentTesla_Generic
{
    meta:
        description = "Detects Agent Tesla variant"
        author = "@elebekenny"
    strings:
        $s1 = "smtp.gmail.com"
        $s2 = "user=admin&pass="
    condition:
```

```
    uint16(0) == 0x5A4D and all of ($s*)
}
```

MITRE ATT&CK Mapping

Tactic	Technique	ID
Initial Access	Phishing via Attachment	T1566
Execution	Malicious Script	T1059
Credential Access	Credential Dumping	T1555
Persistence	Registry Run Key	T1547
Exfiltration	Exfiltration Over C2 Channel	T1041

Conclusion

This malware demonstrates classic RAT behaviors with data exfiltration, credential theft, and persistence capabilities. Proper email filtering, behavior-based detection, and network monitoring are recommended to defend against such threats.

Author: [@elebekenny](https://github.com/elebekenny)