📄 **Malware Analysis Report**

**NAME** : Nikita Shukla

**Intern ID** : 134

**Assigned Malware** : Gen:Heur.PonyStealer.2

**SHA256 Hash:** 882a04265361d588801b3514a604182ce9b8271dd500728fa2897524a2f05a7e

**1. Overview**

This report documents the analysis of a malicious Windows executable suspected to be a **Remote Access Trojan (RAT) / Stealer**. Based on behavioral and static analysis, the sample shows strong similarities to known malware families such as **AgentTesla, RedLine Stealer, and NanoCore**.

The malware is designed to **steal sensitive data**, maintain persistence, and communicate with a remote **Command & Control (C2) server** for data exfiltration.

* **Risk Level:** High
* **Category:** Remote Access Trojan (RAT) / Stealer
* **Platform:** Windows

## **2. Basic Information**

| **Field** | **Value** |
| --- | --- |
| **File Hash (SHA-256)** | 882a04265361d588801b3514a604182ce9b8271dd500728fa2897524a2f05a7e |
| **Type** | Windows Executable (.exe) |
| **First Seen** | Publicly known on threat intel platforms |
| **Aliases** | AgentTesla, RedLine Stealer, NanoCore |

**3. Static Analysis**

**Key Observations:**

* Obfuscated strings and packed sections
* Anti-analysis features (anti-VM, anti-debugging)
* Embedded encrypted configuration (consistent with AgentTesla-like malware)
* Use of Win32 API calls: CreateProcessA, WriteFile, InternetOpen

**4. Dynamic Behavior (Sandbox Results)**

**Network Communication**

* Connects to **remote C2** over **HTTP/SMTP**
* May use ports **587/25**
* Sends stolen data via **SMTP or HTTP POST requests**

**Data Exfiltration**

* Captures **keystrokes, clipboard content, and browser credentials**

### **Persistence**

* Modifies registry keys for persistence:

HKCU\Software\Microsoft\Windows\CurrentVersion\Run

**Dropped Files**

* May drop **DLLs or additional payloads**

**Targeted Software**

* **Browsers:** Chrome, Firefox
* **Email clients:** Outlook
* **FTP clients**

**Processes Spawned**

* cmd.exe, powershell.exe for **lateral movement** and further payload execution

## **5. Network Indicators (IOCs)**

| **IOC Type** | **Value** | **Notes** |
| --- | --- | --- |
| **C2 URL** | http://maliciousdomain.com/send.php (example) | C2 endpoint |
| **SMTP** | Sends stolen data via email | Alternative exfiltration |
| **IP Address** | 145.239.11.32 | Example C2 IP |

**6. Techniques Used (MITRE ATT&CK Mapping)**

| **Technique ID** | **Description** |
| --- | --- |
| **T1059.003** | Windows Command Shell execution |
| **T1056.001** | Keylogging |
| **T1113** | Screen Capture |
| **T1005** | Data from Local System |
| **T1115** | Clipboard Data |
| **T1071.001** | Exfiltration over HTTP/S |

**7. Impact Assessment**

* **Credential Theft** – Browser and email passwords compromised
* **Keylogging** – Captures sensitive keystrokes (logins, banking info)
* **Persistence** – Survives reboots via registry modifications
* **System Compromise** – Potential lateral movement through PowerShell
* **High Data Exfiltration Risk** – Confidential information sent to remote C2

**8. Mitigation & Recommendations**

🛠️ **Immediate Response**

1. **Isolate infected endpoints** from the network
2. **Block IOCs** (C2 domain, IPs, SMTP channels) on firewall and DNS
3. **Reset all compromised credentials** (especially browser, email, and FTP logins)

🔐 **Preventive Measures**

* Deploy **Endpoint Detection & Response (EDR)** with behavior-based detection
* Enforce **2FA/MFA** for critical accounts
* Disable **macros and unnecessary scripting** (PowerShell restrictions)
* Regular **patching and updates**
* User training to avoid malicious attachments and phishing campaigns

**9. Conclusion**

The analyzed sample is a **high-risk Windows RAT/Stealer**, functioning similarly to **AgentTesla/RedLine/NanoCore**. It exfiltrates sensitive data through HTTP and SMTP, achieves persistence via registry keys, and can escalate further through dropped payloads and spawned processes.