Endpoint Forensics Incident Report: Sysinternals

Case Title: Sysinternals Endpoint Compromise
Date of Report: 02/10/2026
Reported By: CyberDefenders (CTF Scenario)
Analyst: Nizar Aderbaz
Severity: High

---

1. Executive Summary

This report documents the process of investigating **a simulated endpoint security incident** in a **Windows machine** that has been compromised by the **Rozena malware**. The goal of the investigation was to **detect the activities of the attacker**, **persistence tools**, and **command-and-control (C2) infrastructure**.

The analysis was conducted through **endpoint forensic artifacts**, **MFT records**, and **system configuration files**. From the evidence, it is clear that **the malware** was deployed through **social engineering**, where it was disguised as **a legitimate administrative tool** named **sysinternals.exe**.

Once executed, **the malware** established **persistence** by creating an **automatic system service** named **VMwareIOHelperService**. The investigation successfully identified the attacker's infrastructure by examining the hosts file, which revealed a static mapping of the domain **www.malware430.com** to the IP address **192.168.15.10.**

This analysis proved successful in identifying **the tools**, **techniques**, and **infrastructure** used by **the attacker**, providing a comprehensive view of the **attack lifecycle**.

2. Incident Timeline

Timestamp	Event
T0	User downloaded a malicious executable masquerading as a legitimate utility.
T1	**sysinternals.exe** was executed from the **Public\Downloads** directory.
T2	The initial process spawned **cmd.exe** to initiate the next stage of infection.
T3	**vmtoolsIO.exe** was dropped and executed as the second-stage payload.
T4	**VMwareIOHelperService** was installed and set to **"Automatic"** for persistence.
T5	Communication established with the **external C2** IP **192.168.15.10**

3. Indicators of Compromise (IOCs)

IP Addresses

IP Address	Purpose	Notes
192.168.15.10	Command & Control (C2)	Identified via static entry in the system hosts file

Domains

Domain	Purpose	Context
www.malware430.com	C2 Communication	Linked to the malicious IP in the hosts file

Malicious Files

File Name	Type	Context
sysinternals.exe	**Executable (Trojan)**	**First stage payload used for initial access and execution**
vmtoolsIO.exe	**Executable**	**Second stage payload dropped by the initial process**

4. Attack Techniques (MITRE ATT&CK Mapping)

- **Initial Access (TA0001):** User execution of a malicious file **(T1204.002)**.
- **Execution (TA0002):** Command and Scripting Interpreter: Windows Command Shell **(T1059.003)**.
- **Persistence (TA0003):** Create or Modify System Process: Windows Service **(T1543.003)**.
- **Defense Evasion (TA0005):** Masquerading as a legitimate tool **(T1036.005)**.
- **Command and Control (TA0011):** DNS infrastructure bypass via Hosts File modification **(T1562.006)**.

5. Recommendations

- **Endpoint Hardening:** Block the execution of unsigned binaries named **sysinternals.exe**
- **Monitoring & Detection:** Implement alerts for unauthorized modifications to **C:\Windows\System32\drivers\etc\hosts**.
- **Persistence Detection:** Audit services for the existence of **VMwareIOHelperService** or any unknown services set to **start automatically**.
- **User Awareness:** Educate staff **to download administrative tools only from verified official sources**

6. Conclusion

The investigation verified that the **Rozena malware** successfully compromised the endpoint **by masquerading as a trusted utility**. It maintained **presence** through the creation of a **persistent system service** and **ensured reliable C2 communication by manually altering the host's DNS configuration via the hosts file**. This case highlights the effectiveness of **simple masquerading** and **service creation** in bypassing standard security assumptions.