Endpoint Forensics Incident Report: KrakenKeylogger

Case Title: KrakenKeylogger Endpoint Compromise
Date of Report: 01/18/2026
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 **KrakenKeylogger malware**.
The goal of the investigation was **to detect the activities of the attacker, persistence tools, exfiltration techniques**, as well as **infrastructure.**
The analysis was done through **endpoint forensic artifacts**, **windows logs**, **application database files**, and **configuration files**. From evidence, it is evident that **key logging malware** was deployed through **social engineering**, **file execution**, **persistence for abusing a legitimate program**, and **data exfiltration to a third-party server by the malicious agent**.
This analysis proved successful in identifying the **tools**, **techniques**, and **infrastructure** used by the attacker. **This helped create an idea of the attack.**

---

2. Incident Timeline

Timestamp	Event
T0	User interacted with a malicious ZIP file downloaded to the system
T1	Password-protected ZIP file extracted
T2	Malicious shortcut (.lnk) executed PowerShell command
T3	Second-stage malware downloaded from attacker-controlled domain
T4	Persistence mechanism established via modified application configuration
T5	KrakenKeylogger executed on the system
T6	Data exfiltration initiated using legitimate application
T7	Communication established with external attacker IP

3. Indicators of Compromise (IOCs)

IP Addresses

IP Address	Purpose	Notes
77.232.122.31	Data exfiltration / C2	Identified in application logs

Domains

Domain	Purpose	Context
masherofmasters.cyou	Malware download	Found in Decode PowerShell command

Malicious Files

File Name	Type	Context
template.lnk	**Shortcut**	**Used to execute an obfuscated PowerShell command for malicious payload delivery.**

Crendentials Observed

- **ZIP file password: @1122d**
- **Method of discovery: SQLite database**

---

4. Attack Techniques (MITRE ATT&CK Mapping)

- **Initial Access (TA0001):** User execution of malicious file **(T1204)**
- **Execution (TA0002):** Powershell execution **(T1059.001)**
- **Persistence (TA0003):** Abuse of legitimate application configuration
- **Defense Evasion (TA0005) :** Obfuscated PowerSshell command
- **Exfiltation (TA0010):** Exfiltration over legitimate application channel
- **Command and Control (TA0011) :** External IP communication

---

5. Root Cause Analysis

The compromise was made possible by:

1. Execution of a malicious file by the user.
2. Lack of application behavior monitoring.
3. Abuse of trusted software for persistence.
4. Insufficient detection of abnormal outbound traffic.

---

6. Recommendations

1. Endpoint Hardening

- Restrict execution of unknown or untrusted files.
- Implement application whitelisting.

2. Monitoring & Detection

- Monitor PowerShell execution with enhanced logging.
- Detect abnormal application network usage.

3. Persistence Detection

- Regularly audit configuration files of installed applications.
- Alert on unauthorized configuration changes.

4. User Awareness

- Train users to recognize suspicious archives and shortcuts.
- Limit execution privileges where possible.

5. Incident Response Readiness

- Develop endpoint compromise playbooks.
- Maintain forensic logging retention policies.

---

7. Conclusion

Investigation has verified the **KrakenKeylogger malware** used malicious file execution to infect the endpoint**, persisted on the endpoint by abusing a legitimate application**, and then communicated with the **external hostile** server to **exfiltrate the stolen information.**

This case shows how **usual user behavior** and **legitimate software** may be **exploited to overcome security measures. Greater security control** over the endpoint together with **user education** could greatly **lower the probability of a similar occurrence.**