Analyst: Nelson Pinder

Date: 26/05/25

Introduction

This report presents the static analysis of two malware samples, focusing on their artifacts and characteristics without execution. The objective is to identify malicious indicators and assess their potential threats.

**Observed Artifacts and Characteristics:**

Malware Sample 1

**File Type & Signature:**

- HxD confirms the file is an .exe (Figure 1).

- Cmderfile command verifies executable signatures (Figure 2).

**Hash found using HashCalc:** ea0a5854aa6e91ebe816d256f34f820697a92d86b4f81e8855c84daeed40b9d4(Figure 3).

**VirusTotal Findings:**

- Popular threat label: Trojan.Autoit/Nymeria (Figure 5).

- Threat categories: Trojan, ransomware, banker.

- Family labels: Autoit, Nymeria, Lokmwiz.

**- Notable indicators (Figure 4):**

- Checks USB bus – May indicate attempts to spread via removable drives.

- UPX packing – Suggests obfuscation techniques to evade detection.

- Checks user input – Could be used for keylogging or monitoring user activity.

- Long sleep periods – Often used to delay execution and evade sandbox analysis.

- Executes dropped file – Indicates potential payload deployment.

- Persistence mechanisms – Suggests the malware attempts to remain active after reboot.

- Direct CPU clock access – Can be used for anti-debugging techniques.

- Runtime modules – May indicate modular malware with additional payloads.

- Detects debugging environment – Likely an anti-analysis feature.

- Suspicious Strings: Xorsearch reveals encoded data, suggesting obfuscation (Figure 6).

**Malware Sample 2 (UPX Packed)**

**Packing Technique:**

- Exeinfo confirms UPX packing (Figure 7).

- Lamer Info provides an unpacking command (Figure 7).

- Unpacking Process: Successfully unpacked using the provided command (Figure 8).

- Suspicious Strings & Signatures:

- Pestudio flags UPX-related signatures (upx0, upx1, VirtualProtect), indicating anti-analysis techniques (Figures 9 & 10).

- VirusTotal Findings:

- Popular threat label: Trojan.Renos/SpySheriff (Figure 12).

- Threat categories: Trojan, downloader, adware.

- Family labels: Renos, SpySheriff, Zlob.

**Notable indicators (Figure 11):**

- UPX packing – Suggests obfuscation to evade detection.

- Long sleep periods – Likely used to bypass sandbox analysis.

- Persistence mechanisms – Indicates attempts to maintain presence on the system.

- Direct CPU clock access – Can be used for anti-debugging techniques.

- Runtime modules – Suggests modular malware behavior.

- Exploit CVE-2014-3931 – Indicates the malware may leverage a known vulnerability for execution.

Analysis Methods

The following static analysis techniques were utilized:

1. File Signature Analysis: Confirmed file types using hex editors and command-line tools.

2. String Inspection: Extracted encoded and suspicious strings for deeper insight.

3. Hash Analysis: Malware samples were compared against VirusTotal for known detections.

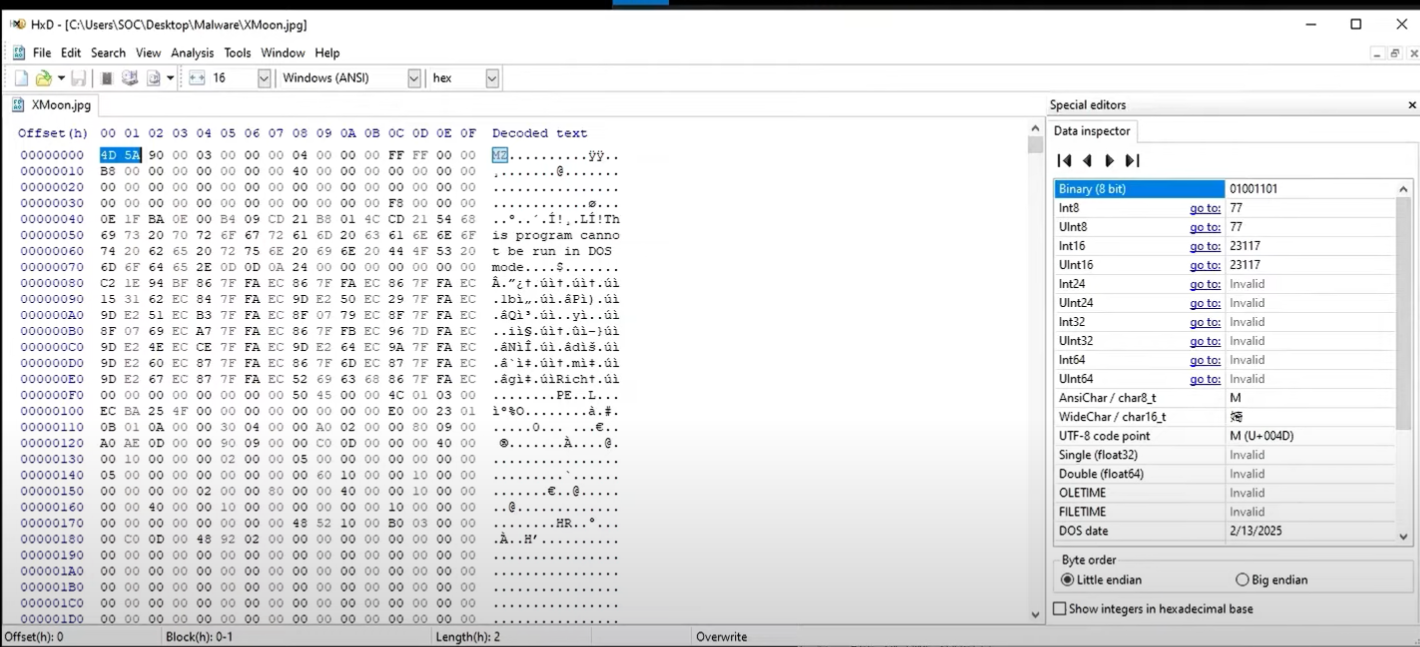
4. Packing Identification & Unpacking: UPX packing detected and manually unpacked for further examination.

Conclusion

Both malware samples exhibit multiple malicious characteristics, including packing techniques, obfuscation, persistence mechanisms, and system reconnaissance methods. Malware Sample 1 aligns with trojan and ransomware behaviours, while Malware Sample 2 leverages UPX packing and exploits known vulnerabilities to evade detection. Additional dynamic analysis is recommended to fully assess execution behaviour, network activity, and payload deployment.

**Appendix:**

**Malware sample 1.**

Figure 1. using HxD to see signs that it is an .exe

Cmder-

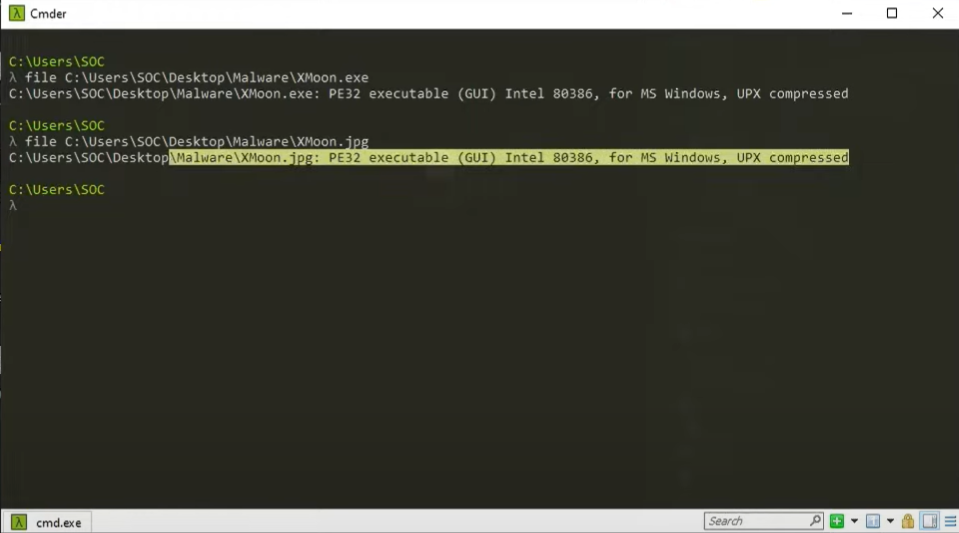


Figure 2. file command on Cmder reveals the file signatures show it as executable (.exe)

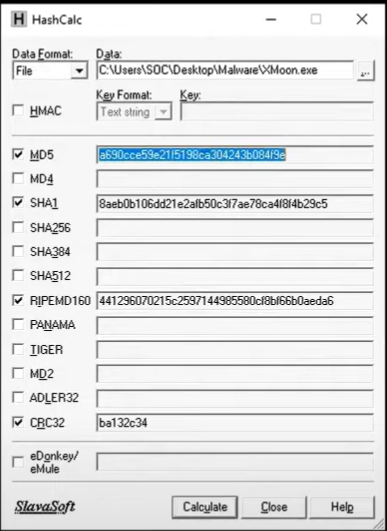


Figure 3. HashCalc to calculate the hash of the file.

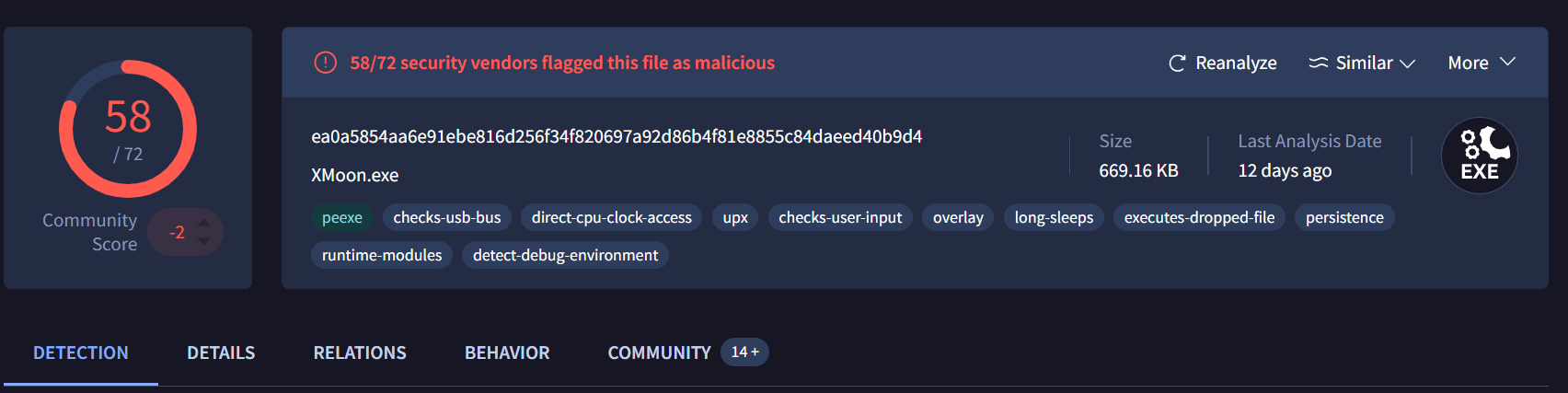


Figure 4. Virus Total search on the hash (ea0a…)

Fig. 4 has the tags peexe, checks-usb-bus, upx, checks-user-input, long sleeps, executes-dropped-file, persistence, direct-cpu-clock-access, runtime-modules, detect-debug-environment.

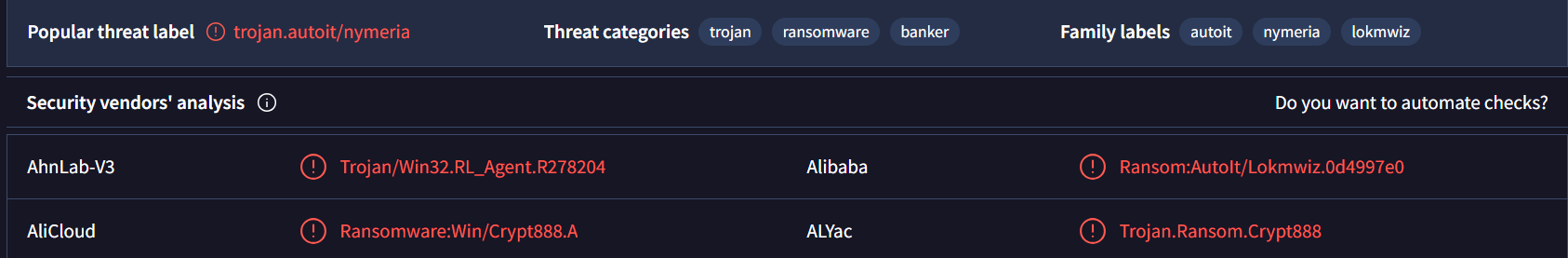


Figure 5. Vendor analysis and VirusTotal’s header on the hash (ea0a…)

Fig. 5 has popular threat label as trojan. autoit/Nymeria. Threat categories – trojan, ransomware, banker. Family labels- autoit, Nymeria, lokmwiz

A computer screen with white text

AI-generated content may be incorrect.

Figure 6. Xorsearch command on Cmder also reveals suspicious output when using keywords.

Malware Sample 2- UPX packed malware

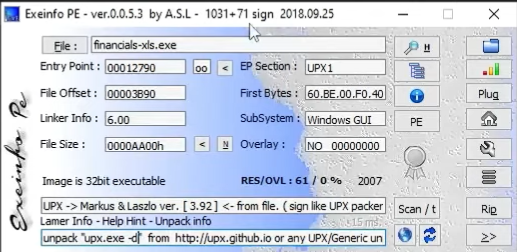


Figure 7. Exeinfo shows that the Upx packing technique is used and Lamer info tells us how to unpack by using the following command

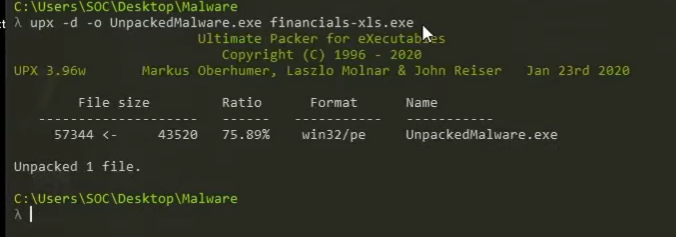
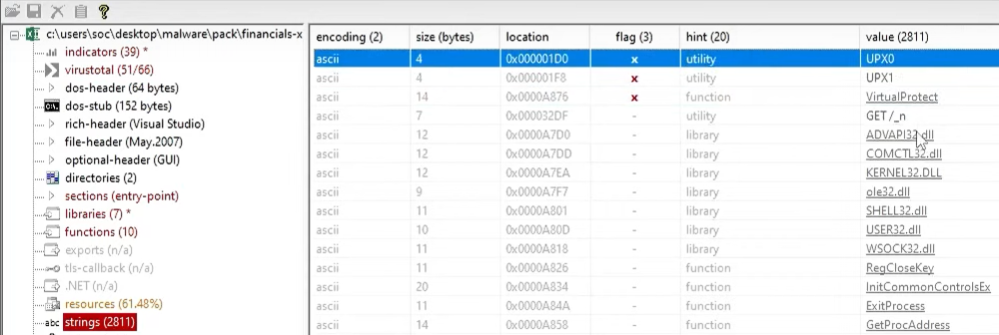


Figure 8. Unpacking the UPX malware using the Lamar info command

A screenshot of a computer

AI-generated content may be incorrect. Figure 9. pestudio shows a suspicious upx signature indicating packing Figure 10. Pestudio allows us to analyse suspicious/flagged strings and see “upx0”, “upx1”, “VirtualProtect”.

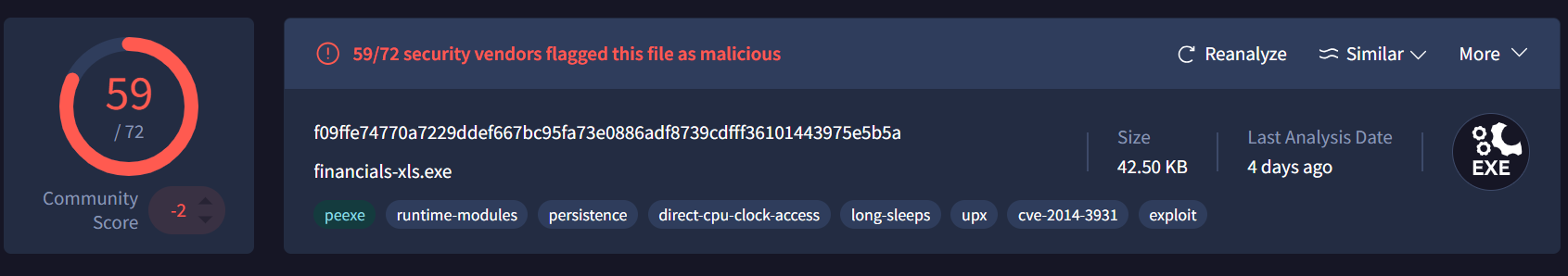


Figure 11. Virus Total search on the hash (f09f…)

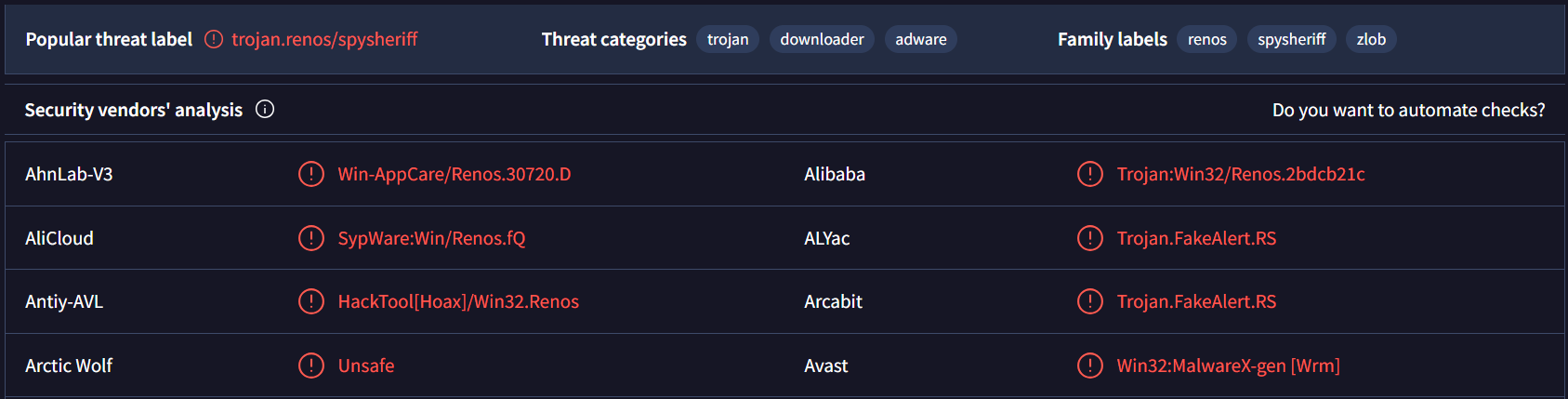
Fig. 11 has the tags peexe, upx, long sleeps, persistence, direct-cpu-clock-access, runtime-modules, exploit, cve-2014-3931.

Figure 12. Vendor analysis and VirusTotal’s header on hash (f09f…)

Fig. 12 has popular threat label as trojan.renos/spysheriff. Threat categories – trojan, downloader, adware. Family labels- renos, spysherif, zlob