# OSKI Cyber Defender Lab: Stealc Malware Analysis

## Incident Overview

An accountant received a suspicious email titled "Urgent New Order" containing a malicious PPT attachment. The SIEM alerted on malicious file download activity. Analysis revealed Stealc malware payload.

MD5 Hash: 12c1842c3ccafe7408c23ebf292ee3d9

Tools:

VirusTotal

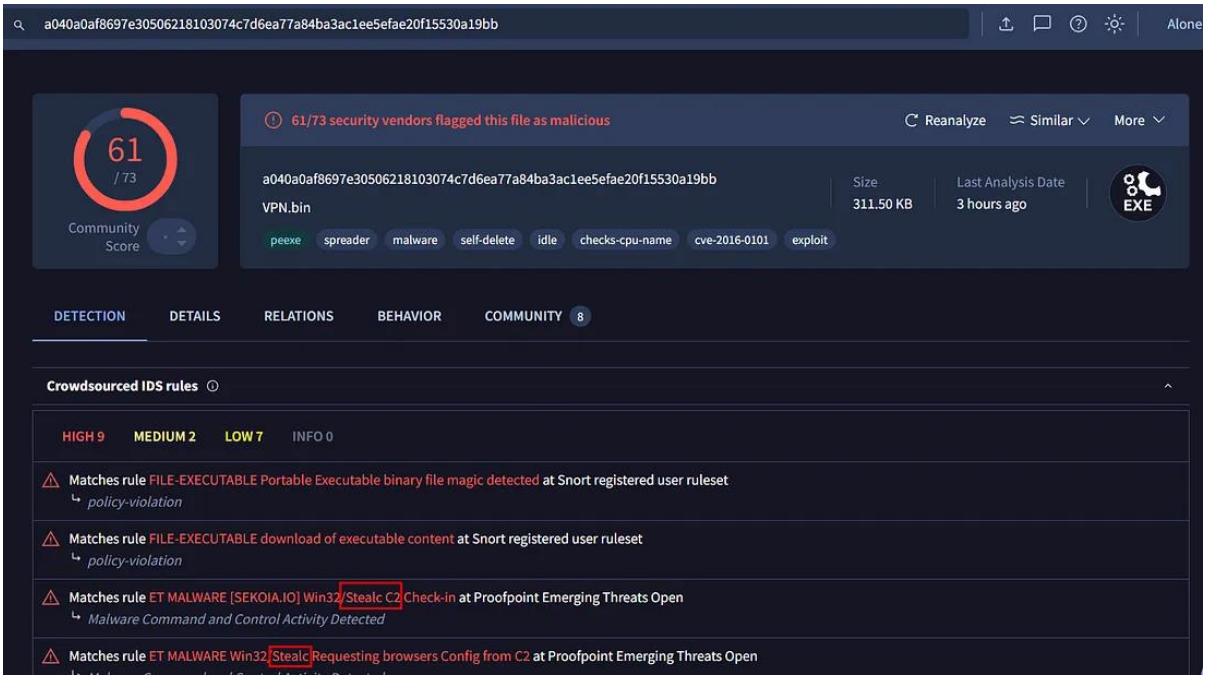
Any.Run

# Analysis Findings

**Q1**: To better categorize and comprehend the behavior and intent of this potential malware, it's essential to identify its family. What is the malware family name for the malicious executable found within the PPT?

### A1: Malware Family Identification

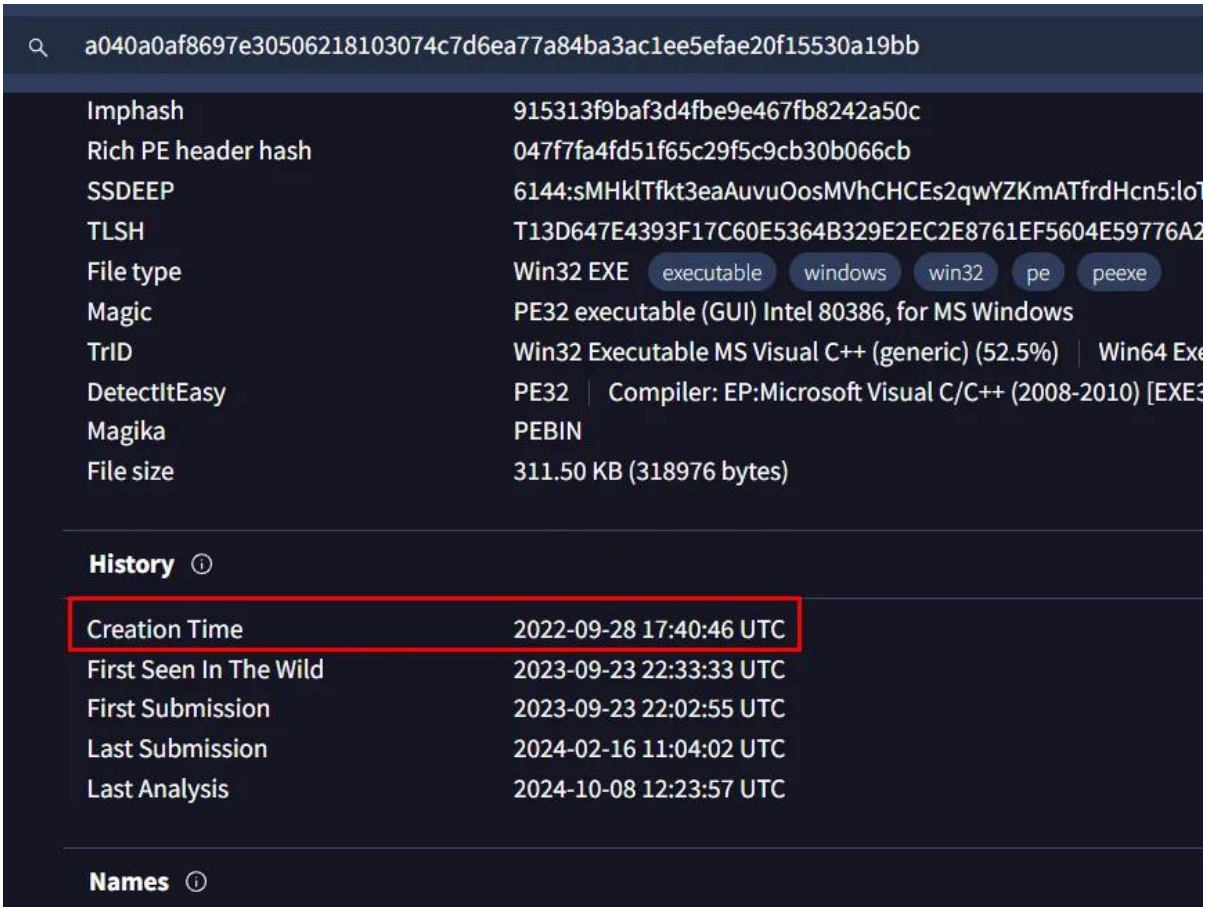
- **Malware Family**: Stealc
- **Characteristics**: Uses legitimate DLLs to exfiltrate files, credentials, and cryptocurrency wallets



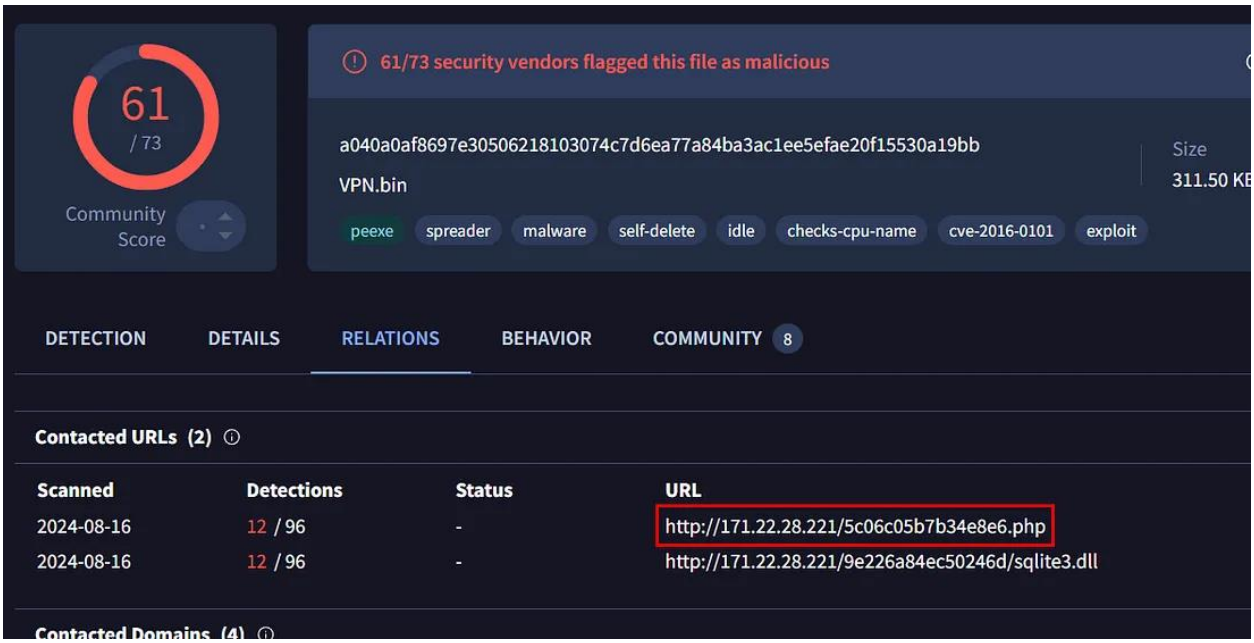

**Q2:** Determining the creation time of the malware can provide insights into its origin. When was the malware creation time?

## A2: Malware Creation Time

- **Creation Time**:2022-09-28 17:40:46 UTC




**Q3:** Identifying the command and control (C2C) server that the malware communicates with can help trace back to the attacker. Which C2C server does the malware in the PPT file communicate with?

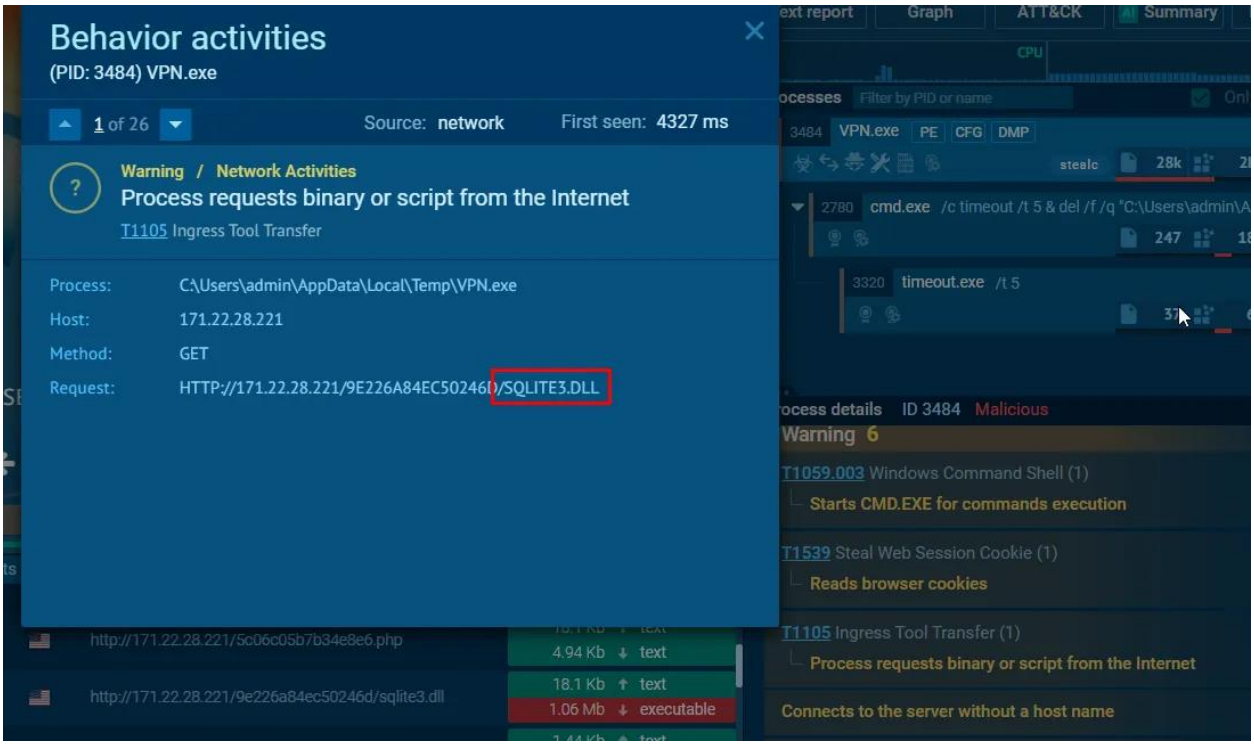



### A3: Command & Control Server

- **C2 Server**: http://171.22.28.221/5c06c05b7b34e8e6.php

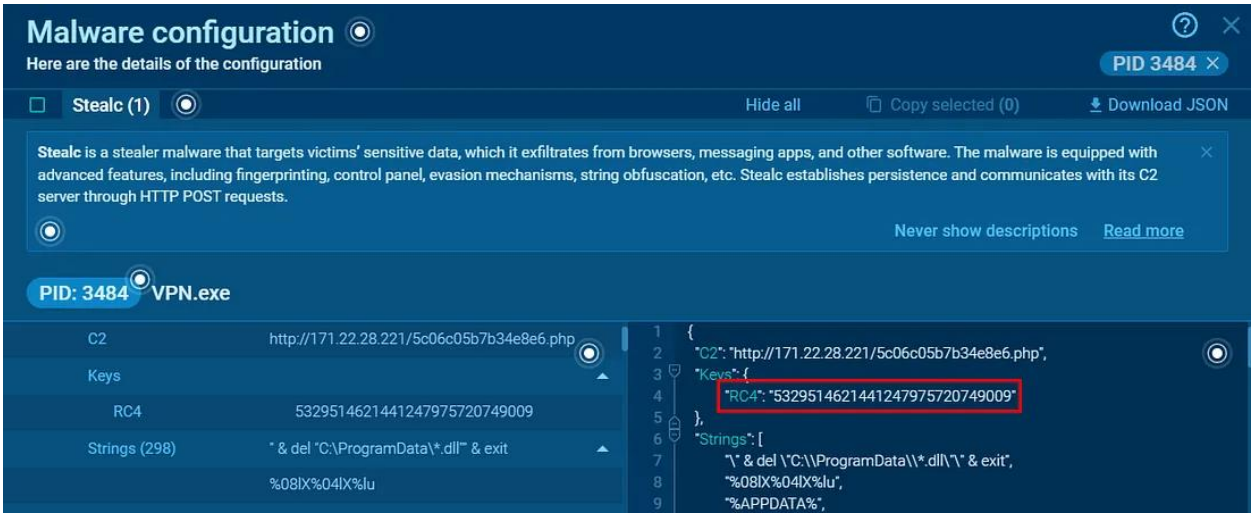
- **Note**: Identified as the endpoint receiving exfiltrated data (not hosting DLLs)

**Q4:** Identifying the initial actions of the malware post-infection can provide insights into its primary objectives. What is the first library that malware requests post-infection?



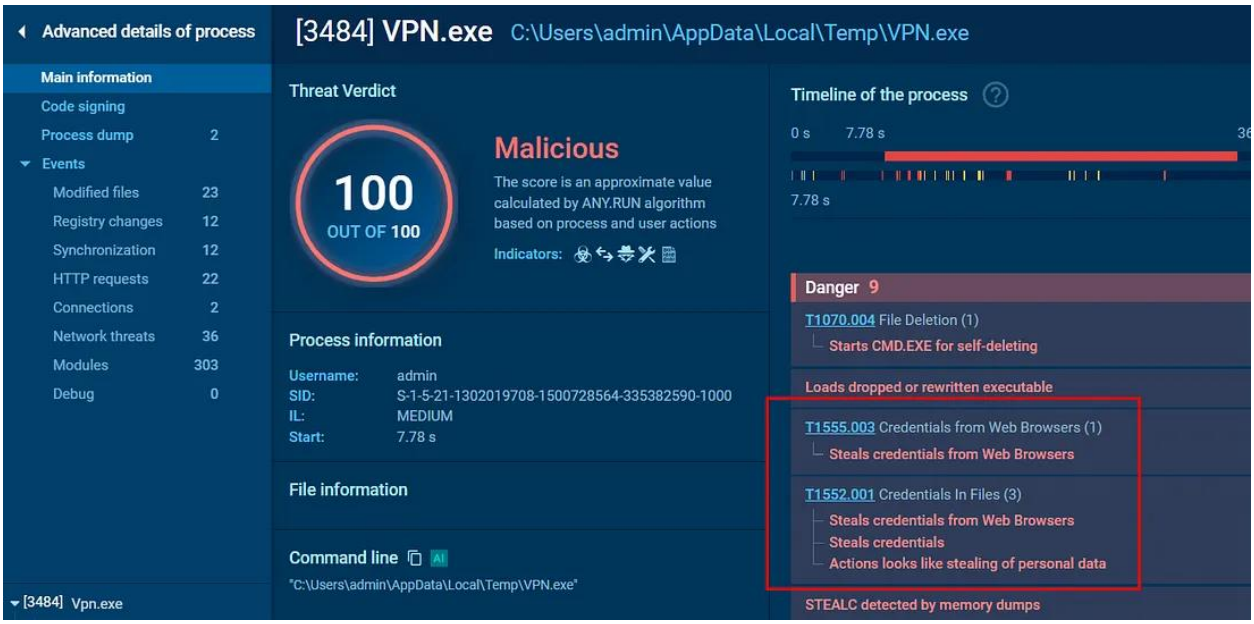

**Q5**: Upon examining the malware, it appears to utilize the RC4 key for decrypting a base64 string. What is the specific RC4 key used by this malware?

## A5: RC4 Decryption Key


- **Purpose**: Used to decrypt base64-encoded strings

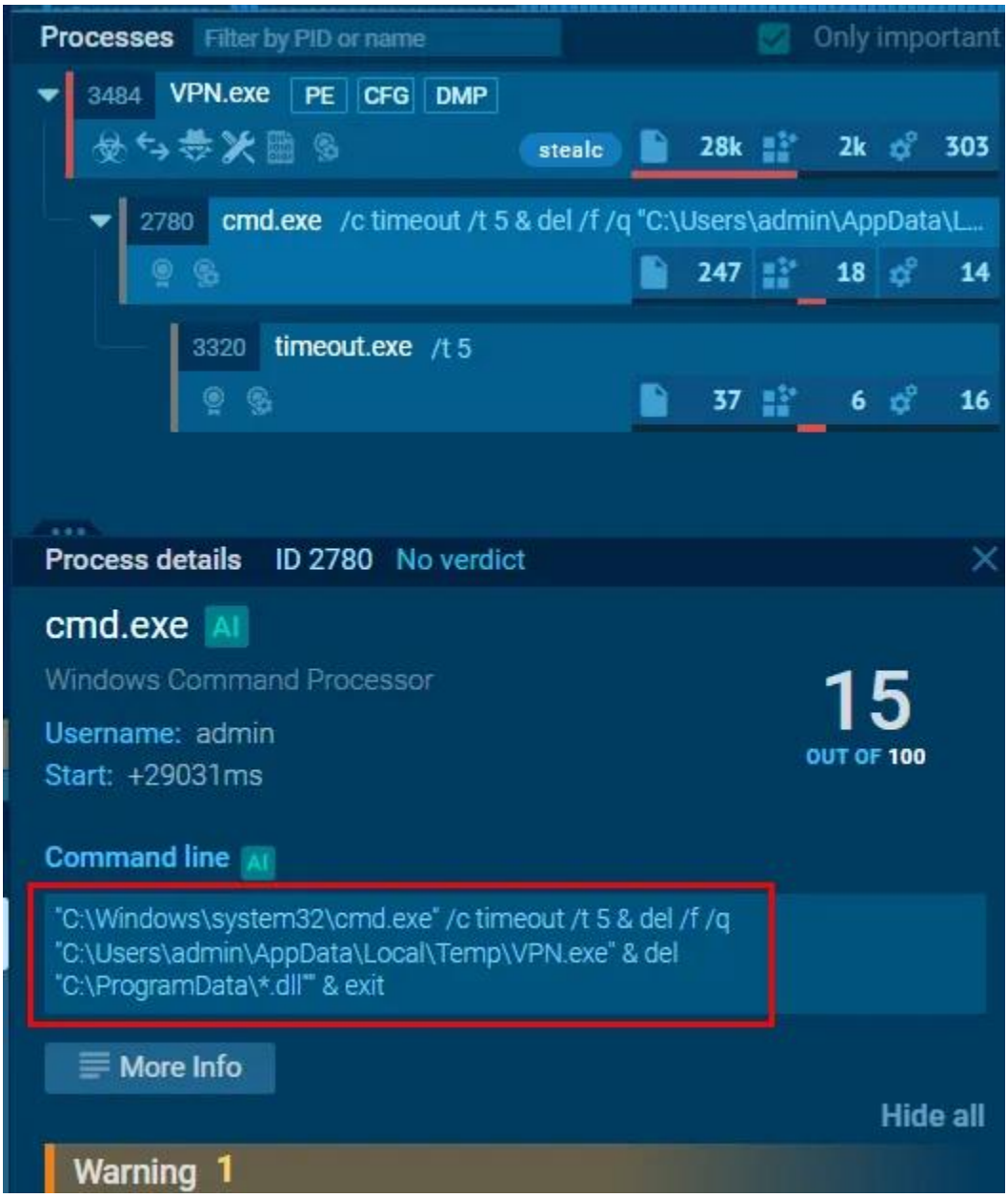
**Q6:** Identifying an adversary's techniques can aid in understanding their methods and devising countermeasures. Which MITRE ATT&CK technique are they employing to steal a user's password?




## A6: MITRE ATT&CK Technique

- **Technique**: T1555 - Credentials from Password Stores
- **Evidence**:
    - Exfiltrates browser artifacts containing passwords
    - Base64-encoded POST requests to C2

Q7: Malwares may delete files left behind by the actions of their intrusion activity. Which directory or path does malware target for deletion?


Processes
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\L...
247 18 14
3320 timeout.exe /t 5
37 6 16
Process details ID 2780 No verdict
cmd.exe AI
Windows Command Processor
Username: admin
Start: +29031ms
15
OUT OF 100
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
More Info
Hide all
Warning 1

**Q8:** Understanding the malware's behavior post-data exfiltration can give insights into its evasion techniques. After successfully exfiltrating the user's data, how many seconds does it take for the malware to self-delete?

### A8: Self-Deletion Timing

- **Delay**: 5 seconds post-exfiltration
- **Evasion**: Rapid self-deletion to hinder forensic analysis

## Recommended Mitigations

1. Block C2 server at network perimeter
2. Scan for `%ProgramData%` anomalies
3. Reset all credentials from affected systems
4. Implement email attachment filtering for Office files