## 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 <u>blog</u> about Qakbot malware that leverages a calculator to perform DLL Sideloading.

Similarly, we came across a <u>Twitter post</u> 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.

1	SECURITY WARNING Macros have been disabled.	Enable Content		×
Г				
	PPERMIT: ACTUR	*		
	Modulo Testimone Unive	ersitario		
	Caricamento modulo questa oper	azione potrebbe ricł	niedere alcuni secondi.	
	Seleziona il tasto "Abilita" siuat	to nella barra gialla p	per scaricare l'ultima versione del modulo.	

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.

Macros	? ×	]
Macro name: AutoOpen	<u>R</u> un	Figure 2 –
h Process	Step Into	
s sc	<u>E</u> dit	
ShowContent	<u>C</u> reate	

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.



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.

<pre>d = GetWP() For 1 = 0 To UBound(d)</pre>									
Expression	Value	Туре	Context						
66 🖃 d		Ching(0 to 451)	ThisDocument.GetParagraph						
- d(0)	******	String	ThisDocument.GetParagraph						
- d(1)	"AAgdQiOADsEkN2ISAQgL8XRjBAAnEBuBBAA2IK6AEgTw3YjJBABHU1FNIEAAcSE4GEAAYnwoDQAEDVJNIEADAu7	String	ThisDocument.GetParagraph						
- d(2)	*AMQqhuYjIBAAydN6AMA6QUZjIBAAnEBuBBwACG5INIEAAIH8oDwAADfINIEAAcSE4GEADsVgL2ISAAwcJgOADkJ0	String	ThisDocument.GetParagraph						
- d(3)	"NvIToQCdJy0///PmojHJ01IT/rXjIBDJ0ITbPDOkwXiIN8Wd5FQEPISZkoZbPDAAAQhE+g0FiEgHAwV4uhd/9//+3DSxvISovY	String	ThisDocument.GetParagraph						
- d(4)	*kQVihBJEITgQCTJyE4/jElkw0iMhBJEtTQQCVLiECkw0ihCxDi0//nf6oDAAAEAgGAIS6iEAAAgCBfMSWUHwFiEAGEGzf	String	ThisDocument.GetParagraph						
- d(5)	BfMSWUHwFiEAG4FMFsISow+glhAJMISQQCVJiEGkQUiMBCJMITg/PSgQCTLyEGkQ0iMBBJUtISlQCTLiEKEPIS//v9Ch0/	String	ThisDocument.GetParagraph						
d(6)	"LiEKEPIS//v8Gh0AAAQAAaQgAoLSAAAAhE8xIZRdAXISAYgWhXwilhC7DiECkwUiBBJUIISYQCRJyElkwUiMB+/IBCJM	String	ThisDocument.GetParagraph						

Figure 5 – StrReverse and Base64Decode Operations to get DLL

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

Home Share View			File	File Home Share View			
	~ O	← →	✓ ↑ ≪ AppData → Local → Microsoft → OneDrive		5 V		
Name	Size	Туре		Name	Size	Туре	
cache-XJDNSJWPFHD.tmp	422 KB	TMP File		22.055.0412.0004		Ch. Coldan	
SquirrelSetup.log	1 KB	Text Document		22.065.0412.0004		File folder	
ThirdPartyNotice.txt	448 KB	Text Document		Logolmages		File folder	
n Teams.exe	1,21,048 KB	Application		logs		File folder	
ucrtbase.dll	999 KB	Application extension		setup		File folder	
we context snanshot hin	168 KB	RIN File		🔄 iphlpapi.dll	422 KB	Application exten	
a la	100 KD			ConeDrive.exe	2,390 KB	Application	

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.

UI reans exe 1420 Mi Closenie		C.AVEIDOWS (System32)	WEIRING W	30000233					
Teams.exe 1420 CreateFile		C:\Users\P	C:\Users\#\AppData\Local\Microsoft\Teams\current\dbghelp.dl NAME.NOT.FOUND						
Teams.exe	1420	m CreateFile	C:\Users\******	m\AppData\Loc	SUCCESS				
Teams.exe	1420	Query Basic Informatio	nFile C:\Users\	C:\Users\\AppData\Local\Microsoft\Teams\current\phipapi.dll SUCCESS					
Teams.exe	1420	The CloseFile	C:\Users\Ina succession	III\AppData\Loc	SUCCESS				
Teams.exe	1420	In CreateFile	C:\Users\Ife an an and	III\AppData\Loc	al/Microsoft/Teams/current/DWrite.dll	NAME NOT FOUND			
Teams.exe	1420	In CreateFile	C:\Users\Multilline energy	AppData\Loc	al/Microsoft/Teams/current/iphlpapi.dll	SUCCESS			
Teams.exe	1420	an CreateFileMapping	C:\Users\!	AppData\Loc	al/Microsoft/Teams/current/iphlpapi.dll	FILE LOCKED WITH ONLY READERS			
Teams.exe	1420	RegOpenKey	HKLM\System\CurrentC	Control Set \Contro	/\CI	REPARSE			
Teams.exe	1420	RegOpenKey	HKLM\System\CurrentC	Control Set \Contro	/\CI	SUCCESS			
Teams.exe	1420	RegQueryValue	HKLM\System\CurrentC	Control Set \Contro	I\CI\Disable26178932	NAME NOT FOUND			
Teams.exe	1420	RegClose Key	HKLM\System\CurrentC	Control Set \Contro	NCI Procmon	SUCCESS			
Teams.exe	1420	RegOpenKey	HKLM\System\CurrentC	ControlSet \Contro	4\CI	REPARSE			
Teams.exe	1420	RegOpenKey	HKLM\System\CurrentC	Control Set \Contro	4/CI	SUCCESS			
Teams.exe	1420	RegQueryValue	HKLM\System\CurrentC	and Set Contro	I\CI\Disable26178932	NAME NOT FOUND			
Teams.exe	1420	RegClose Key	HKLM\System\CurrentC	HKLM\System\CurrentControlSet\Control\Cl SUCCESS					
Teams.exe	1420	m CreateFileMapping	C:\Users\	C:\Users\\\AppData\Local\Microsoft\Teams\current\iphipapi.dl SUCCESS					
Teams.exe	1420	C <sup>S</sup> Load Image	C:\Users\	C:\Users\\AppData\Local\Microsoft\Teams\current\phipapi.dl SUCCESS					
Teams.exe 1420 CloseFile			C:\Users\land	AppData\Loc	al \Microsoft \Teams \current \iphlpapi.dl	SUCCESS			
	_								
A LET TANK AND	_	200	60.25 M	DECKTO	AF				
run leams.exe	-	366	00.35 MB	DESKIONS	Microsoft leams				
🚺 Teams.exe		60	Eind Handles or DLLs						
Teams.exe		4248	E This families of Dees		ProcExp				
Teams eve		024	-						
ieonis.exe		524	Filter: Microsoft\Teams\curren	nt\phlpapi.dll					
Teams.exe	- 1	360							
🚺 Teams.exe		6888	Process	Type	Name				
Teams.exe 3424		3424	Teams and (60)	DU	Collinson in the International and	an Mission Al Teams In grant linking of			
- Iconsider		Teams.exe (60)	DLL	C: Users ( AppData Local Wicrosoft Teams (current yphipapi.dl					
			Teams.exe (360)	DLL	C: Users V AppData Local Microsoft (Teams \current \phlpapi.dl				
			Teams.exe (388)	DLL	C: \Users\\AppData\Local\Microsoft\Teams\current\phlpapi.dl				
			Teams.exe (924)	DLL	C:\Users\\ \AppData\Local\Microsoft\Teams\current\phlpapi.dl				
			Teams.exe (3424)	DLL	C: Users \ AppData \Local Microsoft \Teams \current \phipapi.				
			Teams, exe (4248)	DU	C:\Users\	cal/Microsoft/Teams/current/iphlpapi.dl			
Usage: 6.02% Physical memory: 2.94 GB (34			Teams ave (6999)	Dil	Cillierell				
			reams.exe (0000)	DLL	C: Users y manual and AppUata Lo	carymolosorcyreams (current ypnipap).di			

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.* 



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.

No.	Source	Destination	Protocol	Length Hos	t Info
F	10 200 100 5.11 200	52.84.6.32	TCP	66	1376 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
	11 52.84.6.32	100.000.000.000	TCP	68	80 + 1376 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
	12 1010 - 1010 - 1010	52.84.6.32	TCP	54	1376 → 80 [ACK] Seg=1 Ack=1 Win=65535 Len=0
	13 group part a rate play	52.84.6.32	HTTP	296 d25	iq5m2a8wmm4.cloudfront.net GET /communications HTTP/1.1
	14 52.84.6.32	1007-010-001-008	TCP	68	80 + 1376 [ACK] Seq=1 Ack=243 Win=64240 Len=0
-	15 52.84.6.32	182.018.02.000	HTTP	1358	HTTP/1.1 502 Bad Gateway (text/html)
	16 pres. 1889. 8.00. albei	10.00.4238	TCP	54	1376 + 80 [ACK] Seq=243 Ack=1305 Win=65535 Len=0
	17 1 1 1 1 1 1 1 1 1 1	10.00.0.0	TCP	54	Wireshark - Follow TCP Stream (tcp.stream eq.1) - Ethernet1
	18	100 Hold 100 100	TCP	54	
> Er > II > Ti > Ti > Ti	thernet II, Src: VMware, tternet Ir, Src: VMware, tternet Protocol Version amassission Control Proto (BET /communications HT User-Agent Nosilla/S. Host: d2xiq5m2a8wmm4.c Connection: Keep-Alive Cache-Control: no-cach \r\n [Full request URI: [HTTP request URI: [HTTP request 1/1] [Response in frame: 15	ed:5b:d8 (00:00:29:en 14, Src: icol, Src Port: 1376 col TP/1.1\r\n 0 (Windows NT 10.0; i cloudfront.net\r\n kr\n p://d2xiq5m2a8wm4.c i]	d:5b:d8), Dst: Dst Port Min64; x64	Dst: VMwar 52.84.6.3 :: 80, Seq: ) AppleWeb <u>net/commun</u>	e_ce:c5:38 Connection: Keep-Alive Cache-Control: no-cache HTTP/1.1 502 Bad Gateway Content-Type: text/html Content-tength: 951 Connection: keep-alive Server: CloudFront Date: Mon, 25 Jul 2022 14:28:56 GMT X-Cache: Error from CloudFront Via: 1.1 b90e5scddda40ec72211a632a9693b8.cloudfront.net (CloudFront) X-Amz-Cf-Pop: MAA51-C2 X-Amz-Cf-Id: wwnWCx02o8DwEGt9118vp4VhRruuWo410-HYH3_SaeAwbiKJuW60NA==

#### 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	<u>T1204</u>	User Execution

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