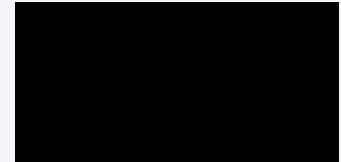


Home » Blog » Targeted Attacks being carried out via DLL SideLoading



CYBERCRIME, EXPLOIT, MALWARE

July 27, 2022



Targeted Attacks being carried out via DLL SideLoading

Cyble Analyzes How Threat Actors Are Leveraging Microsoft Applications And DLL Sideloads To Deliver

Threat Actors Leveraging Microsoft Applications And Cobalt-Strike Beacons

DLL (Dynamic-Link Library) sideloading is a technique used by Threat Actors to load malicious DLL files that spoof legitimate ones. Recently, Cyble Research Lab

 **Votre vie privée nous importe** [PARAMÈTRES](#)

NextRoll, Inc. ("NextRoll") et ses [19 partenaires publicitaires](#) utilisent des cookies et des technologies similaires sur ce site et sur le Web pour recueillir et utiliser des données personnelles (par exemple, votre adresse IP). Si vous y consentez, des cookies, des identifiants d'appareil ou d'autres informations peuvent être stockés ou consultés sur votre appareil aux fins qui vous sont présentées. Cliquez sur "Autoriser tout", "Refuser tout" ou sur Paramètres ci-dessus pour personnaliser votre consentement concernant les finalités et les caractéristiques pour lesquelles vos données à caractère personnel seront traitées et/ou les partenaires avec lesquels vous partagerez vos données à caractère personnel.

NextRoll et ses [partenaires publicitaires](#) traitent des données personnelles pour :
• Stocker et/ou accéder à des informations sur un appareil ;
• Créer un profil de contenu personnalisé ;
• Sélectionner un contenu personnalisé ;
• Des annonces personnalisées, des évaluations d'annonce, des recherches liées à l'audience ainsi que le développement de services ;
• Développement de services. Pour certaines des fins ci-dessus, nos partenaires publicitaires :
• Utilisent des données de géolocalisation précises. Certains de nos partenaires s'appuient sur leurs intérêts commerciaux légitimes pour traiter les données personnelles. Consultez la liste de nos [partenaires publicitaires](#), si vous souhaitez donner ou non votre consentement pour des partenaires spécifiques, afin de découvrir les fins pour lesquelles ils estiment avoir un intérêt légitime, et comment vous pouvez vous opposer à un tel traitement.

Si vous sélectionnez Refuser tout, le contenu de ce site s'affichera quand même, et vous recevrez toujours de la publicité, mais les annonces ne seront pas personnalisées selon votre expérience. Vous pouvez changer votre paramètre chaque fois que vous voyez ☐ sur le site.

[TOUT REFUSER](#)

[TOUT AUTORISER](#)

published a [blog](#) about Qakbot malware that leverages a calculator to perform DLL Sideload.

Similarly, we came across a [Twitter post](#) wherein researchers mentioned a document file that performs DLL Sideload 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.

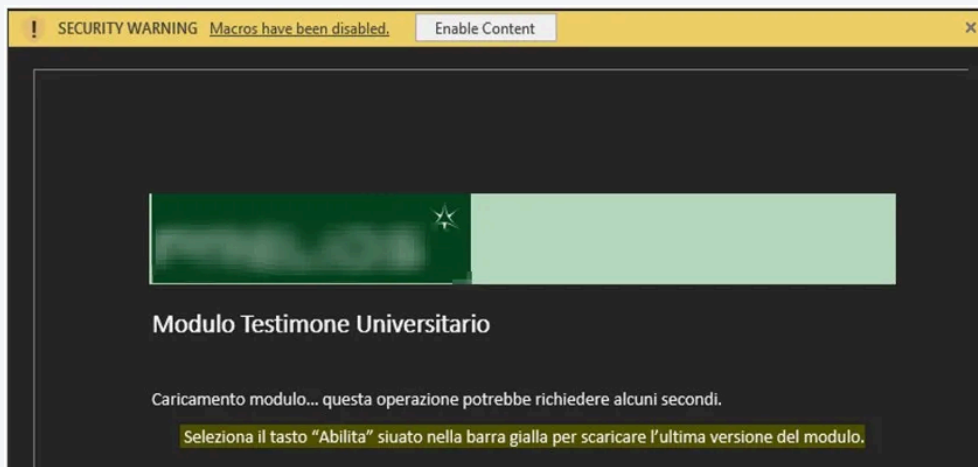


Figure 1 – Document with Macro Content

Technical Analysis

When opening the malicious document, it shows a security warning stating that macros are disabled. The [malware](#) then requests the user to enable the content. Once the user enables the content, the document runs the macro code automatically in the background using

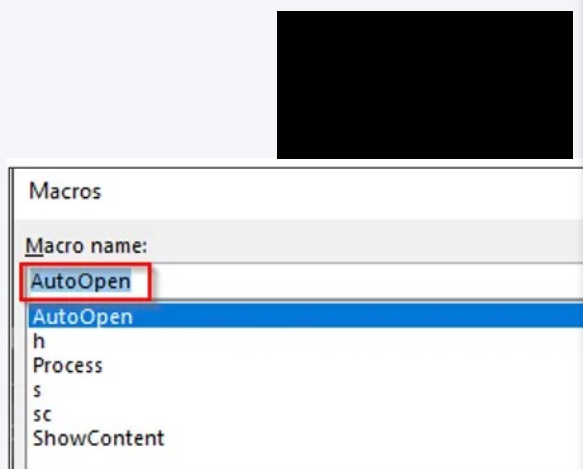
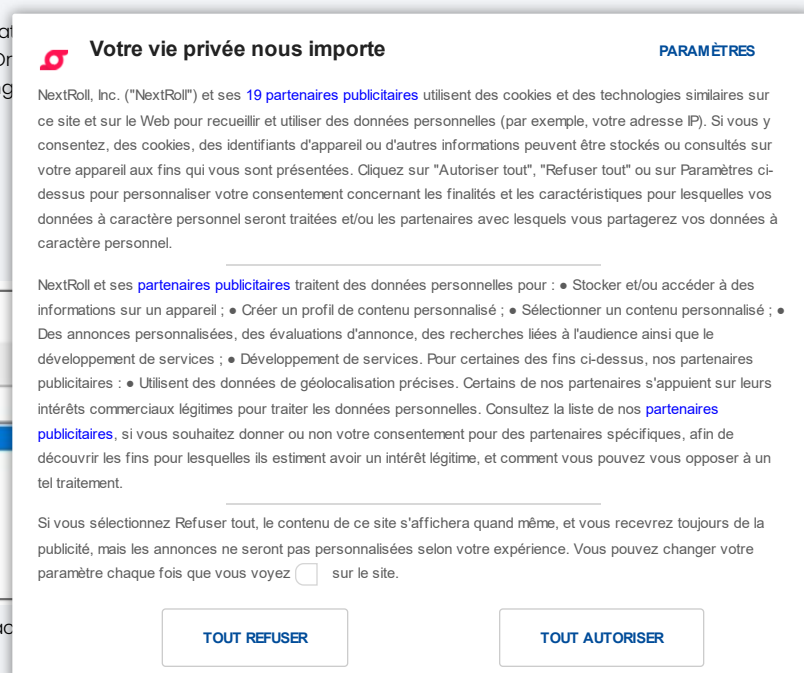


Figure 2 – AutoOpen() function in Macro



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("TE9DQXxUFBEQVRB")) & Base64Decode("XEIpY3Jvc29mdFxBmVEcm12ZVxPbmVEcm12ZS5leGU=")  
    strfe = Dir(strnf)  
  
    If Not strfe = "" Then  
        proc = Base64Decode("XEIpY3Jvc29mdFxBmVEcm12ZQ==")  
        EnableContent (proc)  
    End If  
  
    \Microsoft OneDrive\OneDrive.exe  
    strnf = Environ(Base64Decode("TE9DQXxUFBEQVRB")) & Base64Decode("XEIpY3Jvc29mdCBPbmVEcm12ZVxPbmVEcm12ZS5leGU=")  
    strfe = Dir(strnf)  
  
    If Not strfe = "" Then  
        proc = Base64Decode("XEIpY3Jvc29mdCBPbmVEcm12ZQ==")  
        EnableContent (proc)  
    End If  
  
    \Microsoft\Teams\current\teams.exe  
    strnf = Environ(Base64Decode("TE9DQXxUFBEQVRB")) & Base64Decode("XEIpY3Jvc29mdFkUZWZfc1xjdXJyZW50XHRlYWIzLmV4ZQ==")  
    strfe = Dir(strnf)  
    \Microsoft\Teams\current  
    If Not strfe = "" Then  
        proc = Base64Decode("XEIpY3Jvc29mdFkUZWZfc1xjdXJyZW50")  
        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.

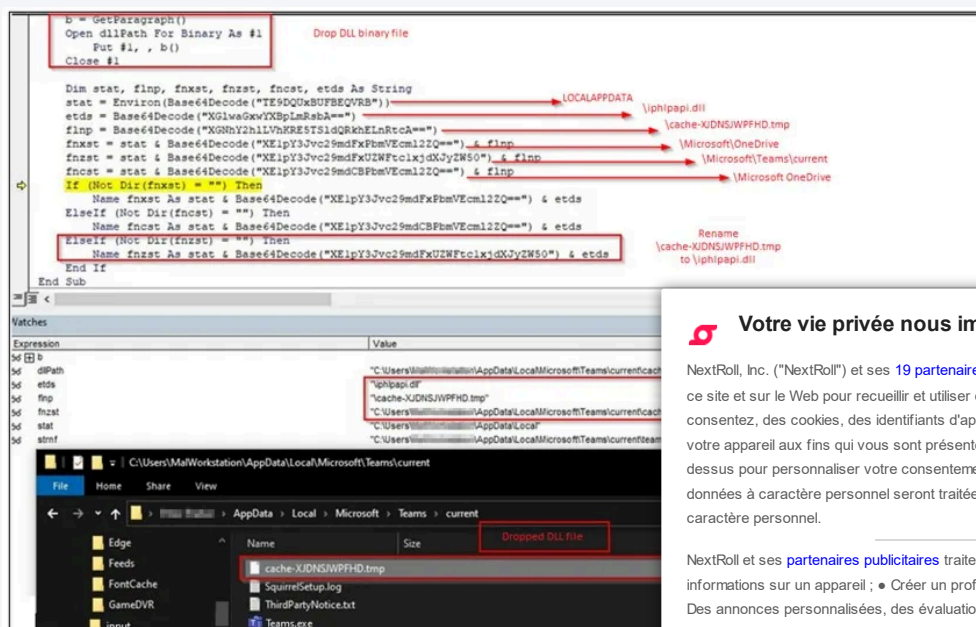


Figure 4 – Drops DLL File

The document file contains an embedded DLL file in reversed Base64 and calls the *GetParagraph()* function, which gets the Base64 encoded string and *Base64Decode* operations to drop the malicious DLL file in the local applications are present.

 **Votre vie privée nous importe** [PARAMÈTRES](#)

NextRoll, Inc. ("NextRoll") et ses [19 partenaires publicitaires](#) utilisent des cookies et des technologies similaires sur ce site et sur le Web pour recueillir et utiliser des données personnelles (par exemple, votre adresse IP). Si vous y consentez, des cookies, des identifiants d'appareil ou d'autres informations peuvent être stockés ou consultés sur votre appareil aux fins qui vous sont présentées. Cliquez sur "Autoriser tout", "Refuser tout" ou sur Paramètres ci-dessus pour personnaliser votre consentement concernant les finalités et les caractéristiques pour lesquelles vos données à caractère personnel seront traitées et/ou les partenaires avec lesquels vous partagerez vos données à caractère personnel.

NextRoll et ses [partenaires publicitaires](#) traitent des données personnelles pour :

- Stocker et/ou accéder à des informations sur un appareil ;
- Créer un profil de contenu personnalisé ;
- Sélectionner un contenu personnalisé ;
- Des annonces personnalisées, des évaluations d'annonce, des recherches liées à l'audience ainsi que le développement de services ;
- Développement de services. Pour certaines des fins ci-dessus, nos partenaires publicitaires :
 - Utilisent des données de géolocalisation précises. Certains de nos partenaires s'appuient sur leurs intérêts commerciaux légitimes pour traiter les données personnelles. Consultez la liste de nos [partenaires publicitaires](#), si vous souhaitez donner ou non votre consentement pour des partenaires spécifiques, afin de découvrir les fins pour lesquelles ils estiment avoir un intérêt légitime, et comment vous pouvez vous opposer à un tel traitement.

Si vous sélectionnez Refuser tout, le contenu de ce site s'affichera quand même, et vous recevrez toujours de la publicité, mais les annonces ne seront pas personnalisées selon votre expérience. Vous pouvez changer votre paramètre chaque fois que vous voyez ☐ sur le site.

TOUT REFUSER

TOUT AUTORISER

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.

Payload Analysis

The below figure shows the code of sideloaded DLL malware, which creates a process "MSTeams.Synchronization.Primitive.2.0" to avoid running another instance of Teams. The malware then communicates to the C&C server using the below URL: `d2xiq5m2a8wmm4.cloudfront.net/communications`.

Figure 7 – DLL Sideloaded in Microsoft Teams



Votre vie privée nous importe

[PARAMÈTRES](#)

NextRoll, Inc. ("NextRoll") et ses [19 partenaires publicitaires](#) utilisent des cookies et des technologies similaires sur ce site et sur le Web pour recueillir et utiliser des données personnelles (par exemple, votre adresse IP). Si vous y consentez, des cookies, des identifiants d'appareil ou d'autres informations peuvent être stockés ou consultés sur votre appareil aux fins qui vous sont présentées. Cliquez sur "Autoriser tout", "Refuser tout" ou sur Paramètres ci-dessus pour personnaliser votre consentement concernant les finalités et les caractéristiques pour lesquelles vos données à caractère personnel seront traitées et/ou les partenaires avec lesquels vous partagerez vos données à caractère personnel.

NextRoll et ses [partenaires publicitaires](#) traitent des données personnelles pour : • Stocker et/ou accéder à des informations sur un appareil ; • Créer un profil de contenu personnalisé ; • Sélectionner un contenu personnalisé ; • Des annonces personnalisées, des évaluations d'annonce, des recherches liées à l'audience ainsi que le développement de services ; • Développement de services. Pour certaines des fins ci-dessus, nos partenaires publicitaires : • Utilisent des données de géolocalisation précises. Certains de nos partenaires s'appuient sur leurs intérêts commerciaux légitimes pour traiter les données personnelles. Consultez la liste de nos [partenaires publicitaires](#), si vous souhaitez donner ou non votre consentement pour des partenaires spécifiques, afin de découvrir les fins pour lesquelles ils estiment avoir un intérêt légitime, et comment vous pouvez vous opposer à un tel traitement.

Si vous sélectionnez Refuser tout, le contenu de ce site s'affichera quand même, et vous recevrez toujours de la publicité, mais les annonces ne seront pas personnalisées selon votre expérience. Vous pouvez changer votre paramètre chaque fois que vous voyez ☐ sur le site.

TOUT REFUSER

TOUT AUTORISER

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 data exfiltration, lateral movement, etc.

Conclusion


TAs are adopting various sophisticated techniques to deploy malware. In this article, we saw how TAs are using Microsoft apps such as Teams and OneDrive to sideload and deploy the Cobalt Strike Beacon.

Cyble Research Labs continuously monitors all new and existing malware and keeps you informed.

Our Recommendations

We have listed some essential cybersecurity best practices that create a barrier for 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 all devices including PC, laptop, and mobile.
- Refrain from opening untrusted links, email attachments, or unknown files, always verifying their authenticity.



Votre vie privée nous importe

[PARAMÈTRES](#)

NextRoll, Inc. ("NextRoll") et ses [19 partenaires publicitaires](#) utilisent des cookies et des technologies similaires sur ce site et sur le Web pour recueillir et utiliser des données personnelles (par exemple, votre adresse IP). Si vous y consentez, des cookies, des identifiants d'appareil ou d'autres informations peuvent être stockés ou consultés sur votre appareil aux fins qui vous sont présentées. Cliquez sur "Autoriser tout", "Refuser tout" ou sur Paramètres ci-dessus pour personnaliser votre consentement concernant les finalités et les caractéristiques pour lesquelles vos données à caractère personnel seront traitées et/ou les partenaires avec lesquels vous partagerez vos données à caractère personnel.

NextRoll et ses [partenaires publicitaires](#) traitent des données personnelles pour : • Stocker et/ou accéder à des informations sur un appareil ; • Créer un profil de contenu personnalisé ; • Sélectionner un contenu personnalisé ; • Des annonces personnalisées, des évaluations d'annonce, des recherches liées à l'audience ainsi que le développement de services ; • Développement de services. Pour certaines des fins ci-dessus, nos partenaires publicitaires : • Utilisent des données de géolocalisation précises. Certains de nos partenaires s'appuient sur leurs intérêts commerciaux légitimes pour traiter les données personnelles. Consultez la liste de nos [partenaires publicitaires](#), si vous souhaitez donner ou non votre consentement pour des partenaires spécifiques, afin de découvrir les fins pour lesquelles ils estiment avoir un intérêt légitime, et comment vous pouvez vous opposer à un tel traitement.

Si vous sélectionnez Refuser tout, le contenu de ce site s'affichera quand même, et vous recevrez toujours de la publicité, mais les annonces ne seront pas personnalisées selon votre expérience. Vous pouvez changer votre paramètre chaque fois que vous voyez ☐ sur le site.

TOUT REFUSER

TOUT AUTORISER

- 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
hxtps://laureati-prelios.azureedge[.]net/forms/Modulo_Testimone_Universitario_v3.doc	URL	Download URL



Share the Post:



Previous
Global Hacktivism On The Rise

Related



Votre vie privée nous importe

PARAMÈTRES

NextRoll, Inc. ("NextRoll") et ses [19 partenaires publicitaires](#) utilisent des cookies et des technologies similaires sur ce site et sur le Web pour recueillir et utiliser des données personnelles (par exemple, votre adresse IP). Si vous y consentez, des cookies, des identifiants d'appareil ou d'autres informations peuvent être stockés ou consultés sur votre appareil aux fins qui vous sont présentées. Cliquez sur "Autoriser tout", "Refuser tout" ou sur Paramètres ci-dessus pour personnaliser votre consentement concernant les finalités et les caractéristiques pour lesquelles vos données à caractère personnel seront traitées et/ou les partenaires avec lesquels vous partagerez vos données à caractère personnel.

NextRoll et ses [partenaires publicitaires](#) traitent des données personnelles pour : • Stocker et/ou accéder à des informations sur un appareil ; • Créer un profil de contenu personnalisé ; • Sélectionner un contenu personnalisé ; • Des annonces personnalisées, des évaluations d'annonce, des recherches liées à l'audience ainsi que le développement de services ; • Développement de services. Pour certaines des fins ci-dessus, nos partenaires publicitaires : • Utilisent des données de géolocalisation précises. Certains de nos partenaires s'appuient sur leurs intérêts commerciaux légitimes pour traiter les données personnelles. Consultez la liste de nos [partenaires publicitaires](#), si vous souhaitez donner ou non votre consentement pour des partenaires spécifiques, afin de découvrir les fins pour lesquelles ils estiment avoir un intérêt légitime, et comment vous pouvez vous opposer à un tel traitement.

Si vous sélectionnez Refuser tout, le contenu de ce site s'affichera quand même, et vous recevrez toujours de la publicité, mais les annonces ne seront pas personnalisées selon votre expérience. Vous pouvez changer votre paramètre chaque fois que vous voyez ☐ sur le site.

TOUT REFUSER

TOUT AUTORISER

The Cybersecurity and Infrastructure Security Agency (CISA) Reports Urgent Security Updates for Apple Products

Strela Stealer targets Central and Southwestern Europe through Stealthy Execution via WebDAV

October 30, 2024

Quick Links

- Home
- About Us
- Blog
- Cyble Partner Network (CPN)
- Press
- Responsible Disclosure
- Knowledge Hub
- Sitemap

Products

- AmlBreached
- Cyble Vision
- Cyble Hawk
- Cyble Odin
- The Cyber Express

Solutions

- Attack Surface Management
- Brand Intelligence
- Threat Intelligence Platform
- Dark Web Monitoring
- Takedown and Disruption
- Vulnerability Management

Privacy Policy

- AmlBreached
- Cyble Vision
- Cyble Trust Portal

Schedule a Personalized Demo to Uncover Threats That No One Tells You

Book a Demo




Votre vie privée nous importe

PARAMÈTRES

NextRoll, Inc. ("NextRoll") et ses 19 partenaires publicitaires utilisent des cookies et des technologies similaires sur ce site et sur le Web pour recueillir et utiliser des données personnelles (par exemple, votre adresse IP). Si vous y consentez, des cookies, des identifiants d'appareil ou d'autres informations peuvent être stockés ou consultés sur votre appareil aux fins qui vous sont présentées. Cliquez sur "Autoriser tout", "Refuser tout" ou sur Paramètres ci-dessus pour personnaliser votre consentement concernant les finalités et les caractéristiques pour lesquelles vos données à caractère personnel seront traitées et/ou les partenaires avec lesquels vous partagerez vos données à caractère personnel.

NextRoll et ses partenaires publicitaires traitent des données personnelles pour : • Stocker et/ou accéder à des informations sur un appareil ; • Créer un profil de contenu personnalisé ; • Sélectionner un contenu personnalisé ; • Des annonces personnalisées, des évaluations d'annonce, des recherches liées à l'audience ainsi que le développement de services ; • Développement de services. Pour certaines des fins ci-dessus, nos partenaires publicitaires : • Utilisent des données de géolocalisation précises. Certains de nos partenaires s'appuient sur leurs intérêts commerciaux légitimes pour traiter les données personnelles. Consultez la liste de nos partenaires publicitaires, si vous souhaitez donner ou non votre consentement pour des partenaires spécifiques, afin de découvrir les fins pour lesquelles ils estiment avoir un intérêt légitime, et comment vous pouvez vous opposer à un tel traitement.

Si vous sélectionnez Refuser tout, le contenu de ce site s'affichera quand même, et vous recevrez toujours de la publicité, mais les annonces ne seront pas personnalisées selon votre expérience. Vous pouvez changer votre paramètre chaque fois que vous voyez  sur le site.

TOUT REFUSER

TOUT AUTORISER