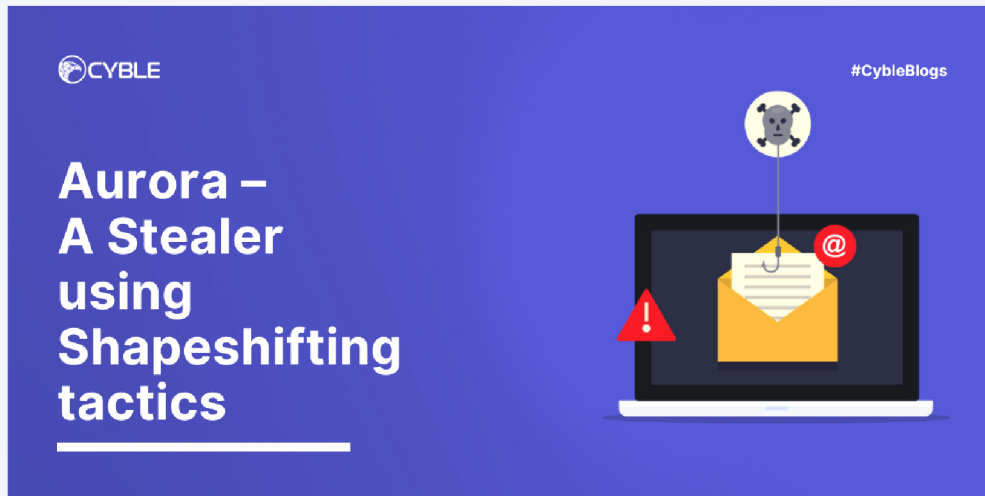


Home » Blog » Aurora – A Stealer Using Shapeshifting Tactics



INFOSTEALER

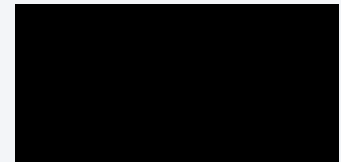
January 18, 2023

Aurora – A Stealer Using Shapeshifting Tactics

CRIL Analyzes Aurora, An Information Stealer Using Shapeshifting Tactics To Imitate Popular Applications

Threat Actors Leveraging Popular Applications To Trick Victims

Threat Actors (TAs) are increasingly using phishing sites to trick victims into downloading malware such as Information stealer, Remote Access Trojan, and other malicious software. Links to these phishing pages are often distributed via email, online ads, and other channels. Cyble



Votre vie privée nous importe

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

Research and Intelligence Labs (CRIL) has also been regularly monitoring various phishing campaigns and discussing them. Aurora Stealer is the latest example of this that we have encountered. We have observed it using phishing sites to imitate popular applications to infect the maximum possible number of victims.

Shapeshifting Behavior

Cyble Research and Intelligence Labs (CRIL) initially identified a phishing site, “[hxxps://messenger-download\[.\]top](https://messenger-download[.]top)”, that was impersonating a legitimate chat application website on January 16th, 2023.

The next day, January 17th, 2023, the same phishing site was found to be mimicking a legitimate TeamViewer website, showing that the threat actors behind this campaign are actively changing and customizing their phishing websites to target multiple popular applications.

The initial infection occurs when the user clicks on the “Download” button on the phishing website, which then downloads **malware** named “messenger.exe” and “teamviewer.exe” from the following URLs:

- [hxxps://download\[.\]balint\[.\]info\[.\]hu/messenger\[.\]exe](https://download[.]balint[.]info[.]hu/messenger[.]exe)
- [hxxps://kodem\[.\]hemsida\[.\]eu/downloads/teamviewer\[.\]exe](https://kodem[.]hemsida[.]eu/downloads/teamviewer[.]exe)

The image below shows the phishing site downloading Aurora stealer with the file name “teamviewer.exe”.

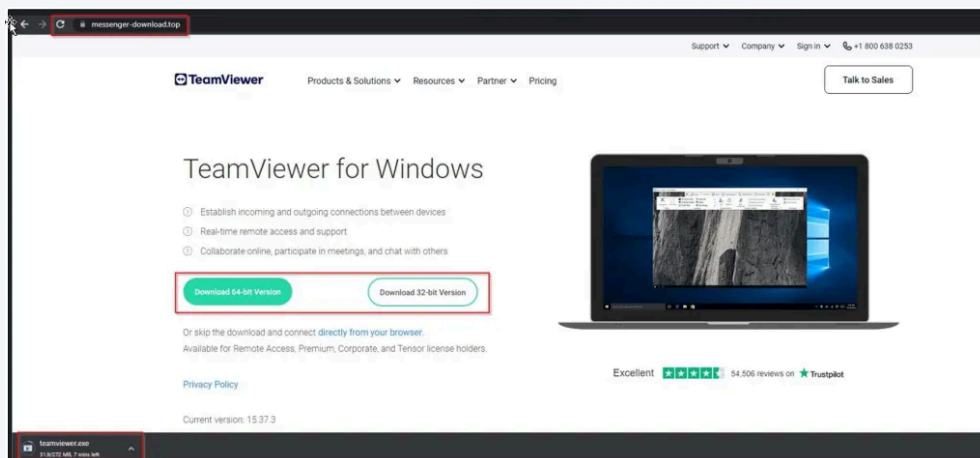
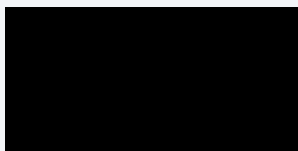


Figure 1 – Messenger phishing page downloading Aurora stealer as teamviewer.exe

The “messenger.exe” and “teamviewer.exe” files that have been downloaded are Aurora Stealer samples, which have been padded with extra zeroes at the end to reach 260MB. TAs use this method to evade detection by antivirus software, as the download process.



Aurora is a type of malware that aims to steal personal information; it targets crypto wallets, browser extensions, Telegram, and specific user directories.

After gathering all the necessary information, it saves the data in JSON format and converts it into Base64 encoding format before sending it to the C&C server.

We have analyzed and explained the detailed behavior of Aurora in the

Technical Analysis

 **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

We have taken the below sample hash for our analysis: (SHA256),
fd17b39833ee0fae6cc8549dfa602adff3cf002cd0a0ef8fa63876ec50a74552, which is a 32-bit Golang executable file. The unique build ID of the Go compiled binary is shown below.

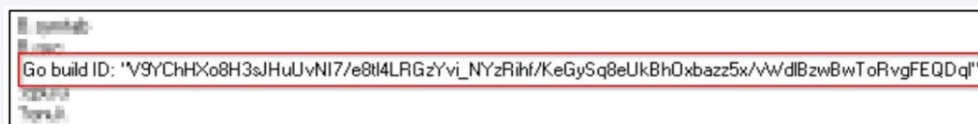


Figure 2 – Go build ID

Upon executing the malware file, it attempts to identify if the file is running in a WINE environment by checking the `wine_get_version()` function via the `GetProcAddress()` API. Then, the malware file uses Windows Management Instrumentation (WMI) commands to gather system information, including the operating system's name, the graphics card's name, and the processor's name.

- **wmic os get Caption**
 - Returns the caption or name of the operating system
- **wmic path win32_VideoController get name**
 - Returns the name of the video controller or graphics card on the computer
- **wmic cpu get name**
 - Returns the name of the processor

After gathering the system details, the malware proceeds to collect additional information about the system, such as the username, Hardware Identification (HWID), Random-Access Memory (RAM) size, screen resolution, and IP address, as shown below.

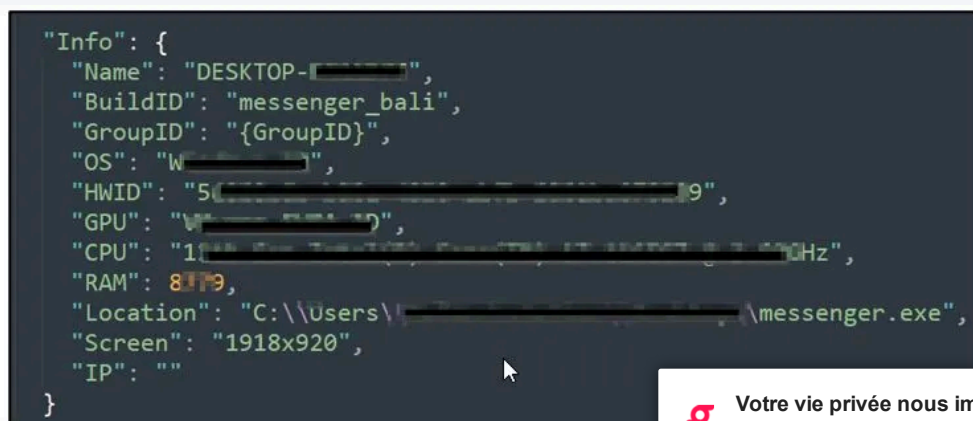


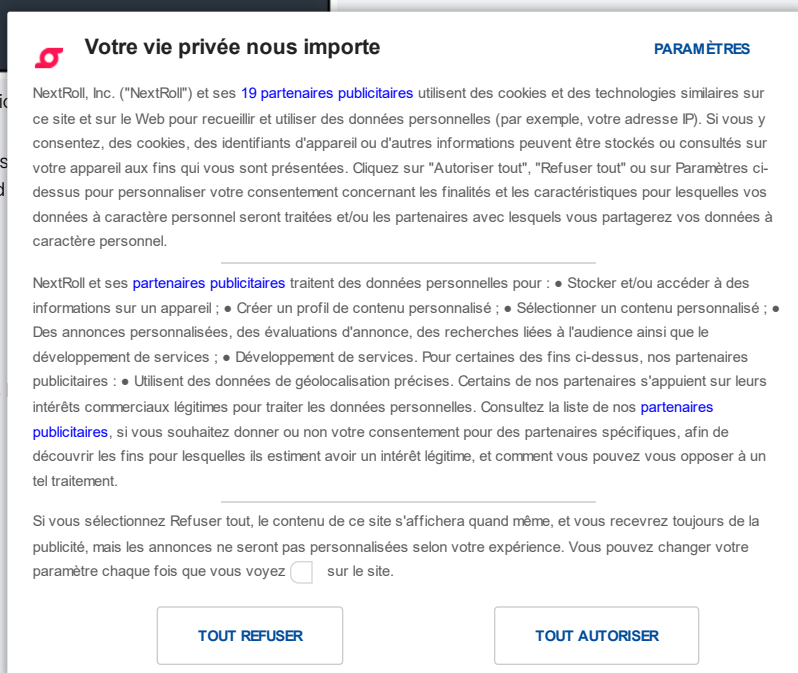
Figure 3 – Collected system information

After collecting system information, the malware queries the directories on the victim's machine and searches for specific browser-related files stored in the following locations:

- Cookies
- History
- Login Data
- Web Data

Then, the stealer begins to extract information related to crypto wallets specific directories. The stealer targets the following crypto wallets:

- "\\AppData\\Roaming\\Armory"
- "\\AppData\\Roaming\\bytecoin"
- "\\AppData\\Roaming\\Exodus"
- "\\AppData\\Roaming\\Ethereum\\keystore"
- "\\AppData\\Roaming\\Electrum\\wallets"
- "\\AppData\\Roaming\\com.liberty.jaxx\\IndexedDB"
- "\\AppData\\Roaming\\Guarda\\Local Storage\\leveldb"
- "\\AppData\\Roaming\\Atomic\\Local Storage\\leveldb"



- “\\AppData\\Roaming\\Zcash\\User Data\\Local State”

In addition to accessing crypto wallets through specific directories, Aurora stealer also steals data from crypto wallet browser extensions. These extensions are hard-coded into the stealer binary, and over 100 extensions have been targeted. Some of the targeted extensions are shown in the image below.

Figure 4 – Targeted Crypto wallets with the ex

The malware continues its data collection by searching for FTP client so Steam applications in the victim's machine and steals important inform data files. The malware also grabs specific files from directories like the screenshots of the victim's system.

Finally, the Aurora stealer processes the stolen information by convertin GZIP archive of it, and encoding the GZIP archive in Base64 format for e; illustrates the structure of the JSON content that is used by the malware

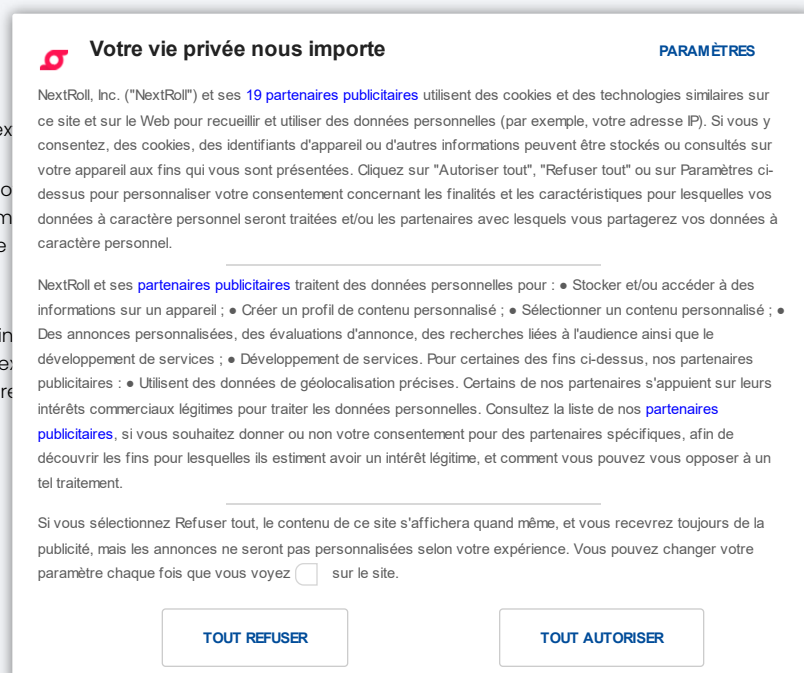




Figure 5 – JSON format to store stolen c

The table below describes the keys of the JSON content.

Type	Type of the stolen data (Browser, Screenshots, etc.)
Info { Name BuildID GroupID OS HWID GPU CPU RAM Location Screen IP }	Victims' device name Build name used for identification Operating system version Victims' machine information Processor information RAM size machine screen resolution Victims' system IP
Browser	Browser name (Chrome, brave, edge, etc.)
Cache	Encoded in base64 content of the stolen files
Type_Grab	Target file info (Cookie, Password, etc.)
FileP	Target browser file (Cookies, Login Data, etc.)

Command & Control

Aurora Stealer communicates with the below C&C server IP (port 8081)



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

- 45[.]15[.]156[.]210:8081

The below figure shows the network communication of the malware's data exfiltration.

Figure 6 – Exfiltrated data

Conclusion

Information stealers are a form of malware that pose a significant threat to corporate networks by allowing unauthorized access. TAs employ various methods to deliver malware to their victims. In this case, we have observed that they are using phishing websites that mimic legitimate messenger sites to deliver Aurora Stealer.

Recently, we have seen a rise in the number of malware samples padded with unnecessary data to increase their size in order to evade detection. This technique was also observed in other stealers, such as [RedLine](#), [Vidar](#), and [RecordBreaker](#).

Cyble Research and Intelligence Labs (CRIL) will continue monitoring the campaigns in the wild and update blogs with actionable intelligence to help defend against attacks.

Our Recommendations

- The initial infection may happen via phishing websites, so enterprises should detect phishing websites.
- Avoid downloading pirated software from Warez/Torrent websites. Websites such as YouTube, Torrent sites, etc., contain such malware.
- Use strong passwords and enforce multi-factor authentication with all accounts.
- Turn on the automatic software update feature on your computer and mobile devices.
- Use a reputed antivirus and internet security software package on all devices, including PC, laptop, and mobile.
- Refrain from opening untrusted links and email attachments with unknown sources.
- Educate employees on protecting themselves from threats like phishing.
- Block URLs that could be used to spread the malware, e.g., Torrent sites.
- Monitor the beacon on the network level to block data exfiltration.

MITRE ATT&CK® Techniques



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](#)

Tactic	Technique ID	Technique Name
Execution	Ti204 Ti059 Ti047	User Execution Command and Scripting Interpreter Windows Management Instrumentation
Defense Evasion	Ti027 Ti497	Obfuscated Files or Information Virtualization/Sandbox Evasion
Credential Access	Ti003 Ti056 Ti552	OS Credential Dumping Input Capture Credentials in Registry
Discovery	Ti082 Ti518 Ti083 Ti087	System Information Discovery Security Software Discovery File and Directory Discovery Account Discovery
Collection	Ti005	Data from Local System
Command and Control	Ti071 Ti095	Application Layer Protocol Non-Application Layer Protocol

Indicators of Compromise (IOCs)

Indicators	Indicator Type	Description
b810b7d416251367ef790bc9a8a9830a69760ba5c1b83055e9a0647270629d9c	Sha256	messenger.exe
fd17b39833ee0fae6cc8549dfa602adff3cf002cd0a0ef8fa63876ec50a74552	Sha256	messenger.exe removed zero padding
44b64cb2be0a5e9fd51528f00a308df7lead226c7cf733ed2568ada07c9044a8	Sha256	teamviewer.exe
c7f43e2afe62a622f77f888f56712a41aec56d5a765a95585f69e870359119c9	Sha256	teamviewer.exe removed zero padding
hxps[://messenger-download[.]top	Domain	Phishing site
hxps[://download[.]balint[.]info[.]hu/messenger[.]exe		
hxps[://kodfem[.]hemsida[.]eu/downloads/teamviewer[.]exe		
45[.]15[.]156[.]210:8081		

Share the Post:



Previous

Next



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

Related Posts

Cyble Sensors Detect New Attacks on LightSpeed, GutenKit WordPress Plugins

October 31, 2024

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

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

Privacy Policy

- AmlBreached
- Cyble Vision
- Cyble Trust Portal

Schedule a Personalized Demo to Uncover Threats That No One Else Can




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