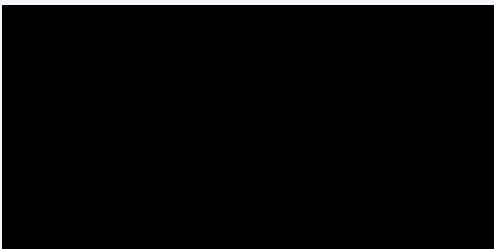


[Home](#) » [Blog](#) » Qakbot Resurfaces with new Playbook

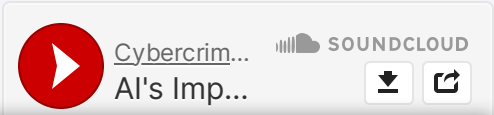


C Y B E R C R I M E , M A L W A R E , P H I S H I N G

July 21, 2022



Qakbot Resurfaces with new Playbook



Read Cyble Research Lab's Analysis of Qakbot That Leverages DLL-SideLoading To In

Threat Actors Leveraging DLL-SideLo

During a routine threat-hunting exercise, Cyble Resear wherein a researcher shared new IoCs related to the

For initial infection, Qakbot uses an email mass spam Actors (TAs) have continuously evolved their infection identified in the wild.

In this campaign, the spam email contains a password ISO file. When mounted, this ISO file shows a .lnk file m opens the .lnk file, the system is infected with Qakbot Qakbot’s infection chain.



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

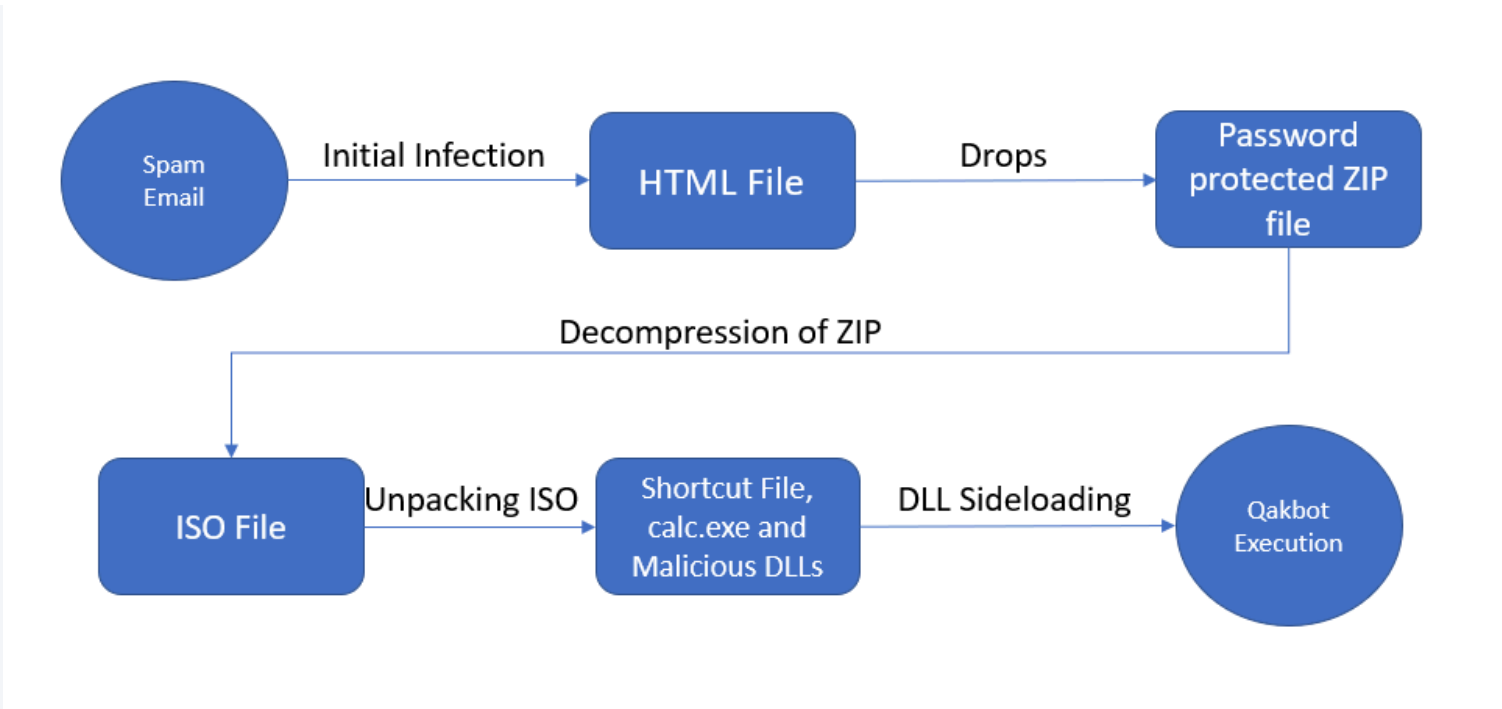


Figure 1 – Qakbot Execution Flow

Technical Analysis

The initial infection of Qakbot starts with a malicious spam campaign that contains various themes to lure the users into opening the attachments.

In this campaign, the spam email contains an HTML file that has base64 encoded images and a password-protected ZIP file, as shown below.

```
document.getElementById("app").style.visibility = "visible";
var text = 'UEsDBBQAAAAAACeh71QAAAAAAAAAAAAAAAAFAAAAMzU5MC9Q5wMEFAABAAgA2KDuVFE4wmIp4
var content_type = 'application/zip';
var target_file_name = 'Report Jul 14 47787.zip';
```

Figure 2 – Embedded ZIP File in HTML File

After opening the HTML file, it will automatically drop the password-protected zip file in the Downloads location. In our sample, the zip file is named “Report Jul 14 47787.zip.” The zip password is mentioned in the HTML, as shown below.

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 REFUSERTOUT AUTORISER

Figure 3 – Contents of Sp

Upon opening the zip file using the password, it extracts another file from the folder containing an ISO image file named “*Report Jul 14 47787.iso*”. The ISO file contains four different files:

- a .lnk file
- a legitimate *calc.exe*
- *WindowsCodecs.dll*
- *7533.dll*.

The figure below shows the details of extracted files.

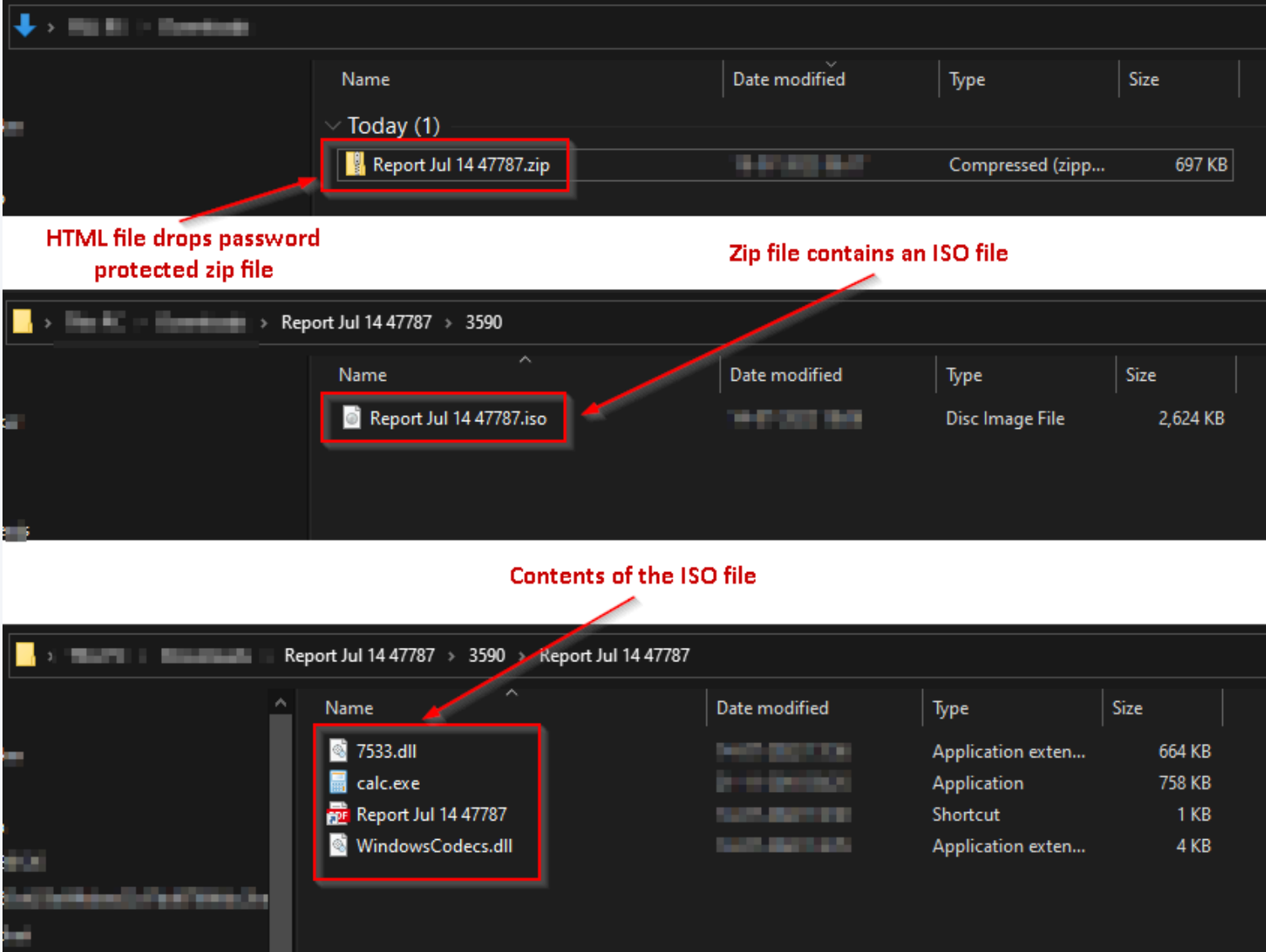


Figure 4 – File Details

If the user executes the ISO file, it mounts the ISO to a drive and shows only the .lnk file to the user. In this case, the .lnk file is named “*Report Jul 14 4778.lnk*” and masquerades as a PDF file.

The property of the .lnk file shows that it executes *calc.exe* present in the ISO file. The figure below shows the .lnk file.



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 – Properties of Shortcut File

DLL Sideloadng:

DLL sideloading is a technique used by TAs to execute malicious code using legitimation applications. In this technique, TAs place legitimate applications and malicious .dll files together in a common directory.

The malicious .dll file name is the same as a legitimate file loaded by the application during execution. The attacker leverages this trick and executes the malicious .dll file.

In this case, the application is *calc.exe*, and the malicious file named *WindowsCodecs.dll* masquerades as a support file for *calc.exe*.

Upon executing the *calc.exe*, it further loads *WindowsCodec.dll* and executes the final Qakbot payload using *regsvr32.exe*. The final payload injects its malicious code into *explorer.exe* and performs all the malicious activities.


Figure 6 – WindowsCodec.dll file Executi

The figure below shows the execution process tree of

Figure 7 – Qakbot Pro

Conclusion

The TAs behind Qakbot are highly active and are con increase their efficacy and impact.



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









Qakbot steals credentials from the victim’s system and uses them for the TA’s financial gain. Apart from the direct financial impact, this can also lead to incidences of fraud, identity theft, and other consequences for any victim of Qakbot malware.

Cyble Research Labs is monitoring the activity of Qakbot and will continue to inform our readers about any updates promptly.

Our Recommendations

- Do not open emails from unknown or irrelevant senders.
- Avoid downloading pirated software from unverified sites.
- Use strong passwords and enforce multi-factor authentication wherever possible.
- Keep updating your passwords after certain intervals.
- Use reputed anti-virus solutions and internet security software packages on your connected devices, including PCs, laptops, and mobile devices.
- Avoid opening untrusted links and email attachments without first verifying their authenticity.
- Block URLs that could use to spread the malware, e.g., Torrent/Warez.
- Monitor the beacon on the network level to block data exfiltration by malware or TAs.
- Enable Data Loss Prevention (DLP) Solutions on employees’ systems.

MITRE ATT&CK® Techniques

Tactic	Technique ID	Technique Name
Initial Access	T1566	Phishing
Execution	T1204	User Execution
Défense Evasion	T1574.002	Hijack Execution Flow: DLL Side-Loading
Défense Evasion	T1055	Process Injection

Indicator Of Compromise (IOCs)

Indicators	Indicator Type
d79ac5762e68b8f19146c78c85b72d5e899c8c030a88ebcc0b3e8482fbfe31e59d095641cb83a65a625a69bbae22d7dd87686dc2be8bd8a1f	MD5
a4a09d3d5905910ad2a207522dceec67c8e7984a0af138aac5427b785e4385cdc6b9b8963197ee022aa311568cd98fee15baf2ee1a2f10ab32a6123	
b6cb21060e11c251ed52d92e83cbcf42b2a3d6a620c050fd03fle16649c6b5bfdc1950899887e7a708b4fc3a91114f78ebfd8dcc2d5149fd9c365	
21930abbbb06588edf0240cc6030214348bf9b838ecb90b8389a0c50b301acc32b44b53e8760c4b4cc8fdcd144651d5ba02195d238950d3b70c	
a8c071f4d69627f581fa15495218bff725beb06d731192ea20bc7eb0c81ae952f2a0bd33092196a35528b12b39052e8dedc74d42c6d96e5e6	

Share this post





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



Previous

AMEXTROLL Android Banking Trojan Spotted In The Wild

Next

Luca Stealer Source Code Leaked On A Cybercrime Forum

Related Posts

IT Vulnerability Report: Fortinet, SonicWall, Grafana Exposures Top 1 Million

November 1, 2024

Cyble Sensors Detect New Attacks on LightSpeed, GutenKit WordPress Plugins

October 31, 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 Today

© 2024. Cyble Inc. (#1 Threat Intelligence Platform Company). All Rights Reserved




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