



Home » Blog » Onyx Ransomware Renames its Leak Site To "VSOP"



CYBERATTACK, CYBERCRIME, RANSOMWARE

August 10, 2022



# Onyx Ransomware Renames its Leak Site To "VSOP"

Cyble Shares Its Insights Into The Recent Act of Onyx Ransomware Group And Its New Leak Site No Longer Active

## Insights into Onyx Ransomware's recent Operations

Onyx ransomware was initially identified by researchers in mid-April 2022 using a double extortion technique to target its victims where it exfiltrates the victim's data. If the victim cannot pay the ransom, then Threat Actors (TA) leak the victim's data.

**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

has a total of 13 victims from 6 different countries to date. The United States remains the most targeted country, with over 60% of the total victims.

According to researchers, Onyx ransomware is based on Chaos ransomware. Onyx encrypts files smaller than 2MB and overwrites files larger than 2MB, rendering them unrecoverable. The figure below shows the highlights of the activities of Onyx ransomware.

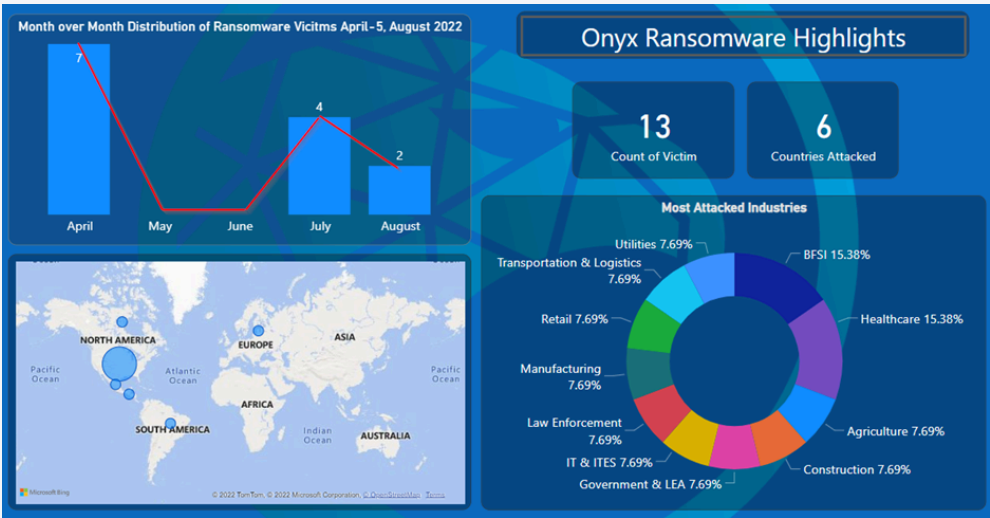


Figure 1 – Onyx ransomware highlights

Onyx is a .NET-based ransomware. This ransomware, upon successful execution, encrypts the files with the “.ampkcz” extension and drops a ransom note named “readme.txt.”

This note contains instructions given by the TA to recover encrypted files and details of the communication medium. The figure below shows the TA’s message to the victim.

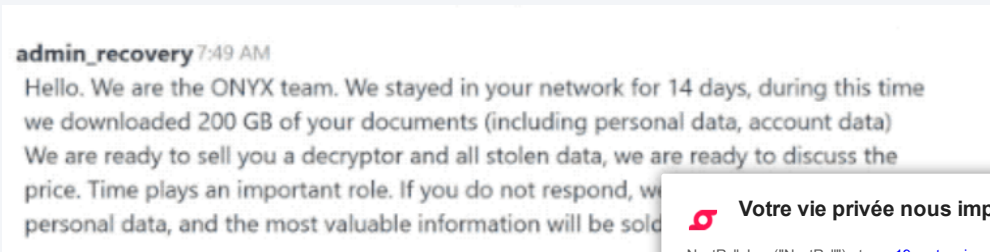
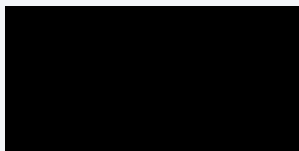


Figure 2 – TA’s message to a victim

## Recent Activities

By the end of April 2022, the Onyx ransomware group had posted details of the Conti ransomware leak site on 4 April 2022. It is possible that the same day we heeded the sequence of events, the victim was first posted by Conti ransomware.

Conti Ransomware was expected to shut down its operations at that time, so we thought that Conti’s affiliates/members might be behind Onyx ransomware or might be involved in this attack.



**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

After announcing 7 victims in April, the Onyx group went silent for nearly two months on their leak site and restarted their operations by July end. The figure below shows the common victim details posted by Onyx and Conti ransomware.

Date	Victim	Ransomware Gang	Target Industry	Country	Website	Conti's Post Details
Apr 2, 2022	Plumbing	Conti	Utilities	United States	plumbinginc.com	




Figure 3 – Common Victim details shared by Onyx and Conti groups

During our Ransomware research and monitoring activities, we found that the ONYX ransomware had renamed its leak site from "ONYX NEWS" to "VSOP NEWS." The group has not launched a new site but updated the existing site with new names. The figure below compares the old and new ONYX ransomware leak sites.

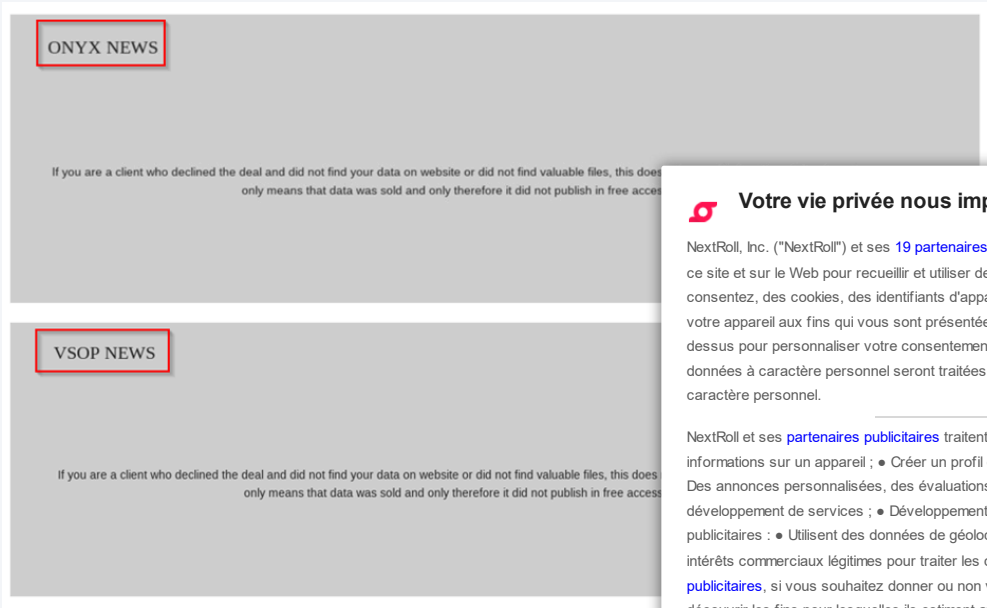


Figure 4 – Renaming Leak site

## Technical Analysis

(Sample SHA256: a7f09cfde433f3d47fc96502bf2b623ae5e7626da85d)



**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

Onyx ransomware uses AES and RSA encryption algorithms to encrypt the victim’s files. The ransomware targets the following directories for encryption:

- Desktop
- Links
- Contacts
- Documents
- Downloads
- Pictures
- Music
- OneDrive
- Saved Games
- Favorites
- Searches
- Videos


Onyx ransomware encrypts files that have the following extensions:

.txt, .jar, .dat, .contact, .settings, .doc, .docx, .xls, .xlsx, .ppt, .pptx, .odt, .jpg, .mka, .mhtml, .oqy, .png, .csv, .py, .sql, .mdb, .php, .asp, .aspx, .html, .htm, .xml, .psd, .pdf, .xla, .cub, .dae, .indd, .cs, .mp3, .mp4, .dwg, .zip, .rar, .mov, .rtf, .bmp, .mkv, .avi, .apk, .url, .dib, .dic, .dif, .divx, .iso, .7zip, .ace, .arj, .bz2, .cab, .gzip, .lzh, .tar, .jpeg, .xz, .mpeg, .torrent, .mpg, .core, .pdb, .ico, .pas, .db, .wmv, .swf, .cer, .bak, .backup, .accdb, .bay, .p7c, .exif, .vss, .raw, .m4a, .wma, .flv, .sie, .sum, .ibank, .wallet, .css, .js, .rb, .crt, .xls, .xlb, .7z, .cpp, .java, .jpe, .ini, .blob, .wps, .docm, .wav, .3gp, .webm, .m4v, .amv, .m4p, .svg, .ods, .bk, .vdi, .vmdk, .onepkg, .accde, .jsp, .json, .gif, .log, .gz, .config, .vb, .mlv, .sln, .pst, .obj, .xlam, .djvu, .inc, .cvs, .dbf, .tbi, .wpd, .dot, .dotx, .xltx, .pptm, .potx, .potm, .pot, .xlw, .xps, .xsd, .xsf, .xsl, .kmz, .accdr, .stm, .accdt, .ppam, .pps, .ppsm, .lcd, .3ds, .3fr, .3g2, .accda, .accdc, .accdw, .adp, .ai, .ai3, .ai4, .ai5, .ai6, .ai7, .ai8, .arw, .ascx, .asm, .asmx, .avs, .bin, .cfm, .dbx, .dcm, .dcr, .pict, .rgbe, .dwt, .f4v, .exr, .kwm, .max, .mda, .mde, .mdf, .mdw, .mht, .mpv, .msg, .myi, .nef, .odc, .geo, .swift, .odm, .odp, .oft, .orf, .pfx, .pl2, .pl, .pls, .safe, .tab, .vbs, .xlk, .xlm, .xlt, .xltm, .svgz, .slk, .tar.gz, .dmg, .ps, .psb, .tif, .rss, .key, .vob, .epsp, .dc3, .iff, .onepkg, .onetoc2, .opt, .p7b, .pam, .r3d, .dsn, .dmp, .qbw, .imr, .nd, .chw, .spi, .ep, .tlg, .qbb, .msi, .eml, .thmx, .obi, .chm, .pub, .md5, .spf, .spk, .idx, .scc, .jdk, .cnt, .tum, .dsm, .reg, .cfg, .ldf, .bat, .dxf, .SLDDRW, .SLDPRT, .SLDASM, .mil, .dlf, .c4, .pdx

If the size of files with the extensions mentioned above is larger than 2MB, the ransomware destroys the files by overwriting them with random data, making them forever inaccessible.

Figure 5 – Overwriting files larger than 2MB

The ransomware has hardcoded strings such as Ransom note, an extension, and the file name of Ransom Note. The ransomware appends the “.” to the end of the file name, encrypts the files, and drops a ransom note named “readme.txt.” The figure shows the following strings:



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 6 – Hardcoded Strings

This ransomware also deletes the volume shadow copies and backup catalogs to prevent the recovery of the victim’s data. Additionally, it modifies the registry’s RunOnce key and creates a shortcut file to establish persistence. It also tries to spread by checking the mounted drives on the victim’s system, as shown in the figure below.

Figure 7 – Targeting Mounted Drives

Conclusion

Cyble Research Labs actively monitors emerging ransomware threats. C and renamed it after two months of inactivity.

It is possible that ransomware groups might be trying to restart their ma researchers discovered that due to a flaw, the ransomware was destroy encryption, which might lead to a loss in the ransom earned.

A fresh sample of Onyx ransomware hasn’t been spotted in the wild unt the above assumptions, that TAs might also upgrade the ransomware e

Our Recommendations



**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



With Threat Actors and their TTPs increasing in sophistication, the industry is still searching for the proverbial silver bullet to counter this cyber threat. However, there are a few cybersecurity measures that we strongly recommend to organizations to reduce the likelihood of a successful attack:

- Victim organizations should perform incident response activities to minimize the losses and mitigate the exploited vulnerabilities.
- Deploy reputed anti-virus and internet security software package on your company-managed devices, including PCs, laptops, and mobile devices.
- Define and implement a backup process and secure those backup copies by keeping them offline or on a separate network.
- Enforce password change policies for the network and critical business applications or consider implementing multi-factor authentication for all remote network access points.
- Reduce the attack surface by ensuring that sensitive ports are not exposed to the Internet.
- Conduct cybersecurity awareness programs for employees and contractors.
- Implement a risk-based vulnerability management process for IT infrastructure to identify and prioritize critical vulnerabilities and security misconfigurations for remediation.
- Instruct users to avoid opening untrusted links and email attachments without verifying their authenticity.
- Turn on the automatic software update features on computers, mobiles, and other connected devices wherever possible and pragmatic.

MITRE ATT&CK® Techniques

Tactic	Technique ID	Technique Name
Execution	T1106	Native API
Persistence	T1547.001	Boot or Logon AutoStart Execution: Registry Run Keys / Startup Folder
Discovery	T1082 T1083	System Information Discovery File and Directory Discovery
Impact	T1486	Data Encrypted for Impact

Indicators of Compromise

Indicators	Indicator type	Description
cf6ff9e0403b8d89e42ae54701026c1f a4f5cbl1b9340f80a89022131fb525b888aa8bc6 a7f09cfde433f3d47fc96502bf2b623ae5e7626da85d0a0130dcd19d1679		

Share the Post:



Previous  
Bitter APT Group Using “Dracarys” Android Spyware

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

October 30, 2024

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 Else Can

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

Made with



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