



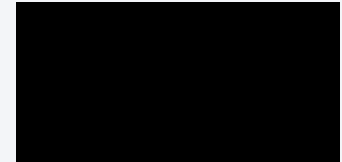
TRENDING TARGETED INDUSTRIES → IT & ITES | Government & LEA | Technology | Healthcare | BFSI **TARGETED COUNTRIES** → United States | Russian Federation | China

[Home](#) » [Blog](#) » Prynt Stealer Spotted In the Wild



CYBER NEWS, DATA BREACH, INFOSTEALER, OSINT, VULNERABILITY

April 21, 2022




Prynt Stealer Spotted In the Wild

The Stealer Is New On The Cybercrime Forum Financial Data Using A Clipper And Keylogger

A New Info Stealer Performing Clipper And Keylogger Activities

Cyble research labs discovered a new Infostealer named Prynt Stealer. It was spotted on cybercrime forums and comes with various capabilities. Along with stealing the victims data, this stealer

 **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](#)

can also perform financial thefts using a clipper and keylogging operations. Additionally, it can target 30+ Chromium-based browsers, 5+ Firefox-based browsers, and a range of VPN, FTP, Messaging, and Gaming apps. Furthermore, a builder may customize the functionality of this stealer.

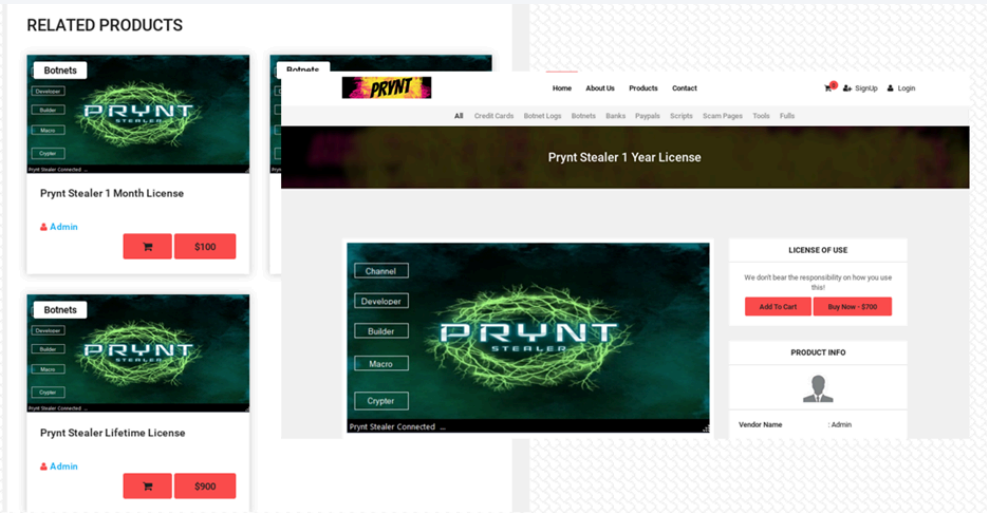


Figure 1: Post on cybercrime marketplace

The developer of the stealer recently claimed the recent versions of the stealer to be FUD (Fully Undetectable), as shown in Figure 2. We could also spot a few stealer logs available for free on the Telegram channel.

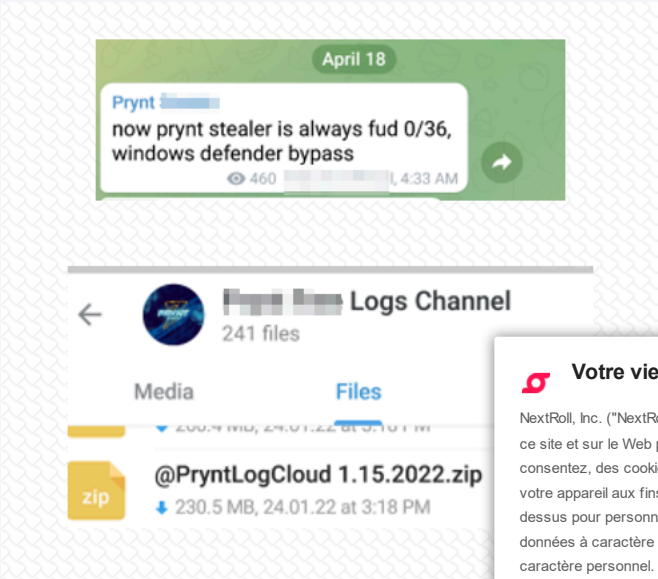


Figure 2: Details from Telegram

The embedded binary contains hardcoded strings which are encrypted with an encryption algorithm. Prynt Stealer is a .Net-based malware. Figure 3 shows the



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

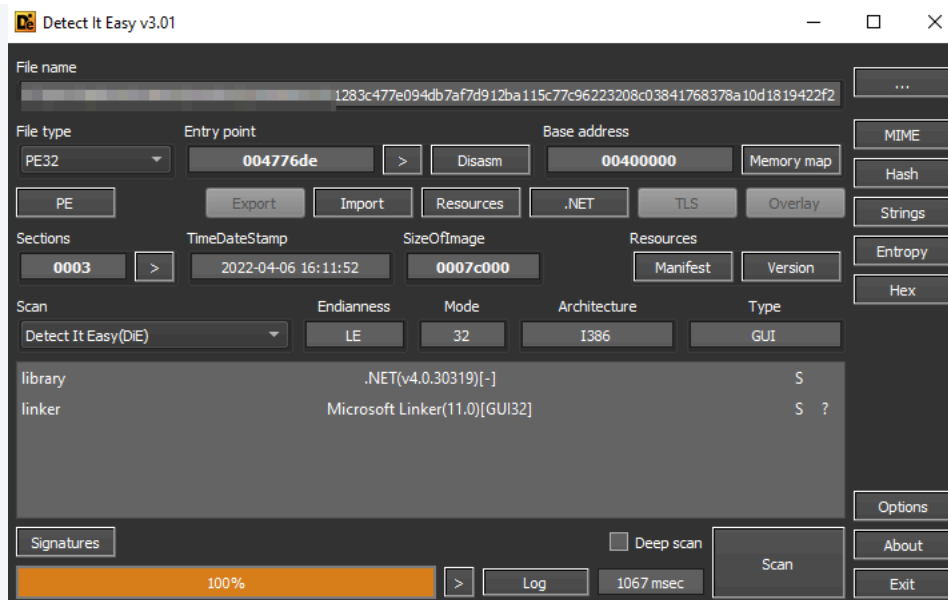


Figure 3: File details


Technical Analysis

The sample (**SHA 256**: 1283c477e094db7af7d912ba115c77c96223208c03841768378a10d1819422f2) has an obfuscated binary stored as a string, as shown in Figure 4.



Figure 4: Obfuscated binary

The binary is encoded using the rot13 cipher. ROT13 (rotate by 13 places) positions from the current letter. The rot13 algorithm is applied on a Base64 encoded string. The malware rather than dropping the payload executes it directly in the `AppDomain.CurrentDomain.Load()` method.



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

Page 3 of 18

Figure 5: Binary decoding process

The malware uses *ServicePointManager* class to establish an encrypted channel to interact with the server. There are a few hardcoded strings encrypted using the AES256 algorithm. All these strings are decrypted by calling *Settings.aes256.Decrypt()* method is assigned back to the same variables, as shown in the Figure below.

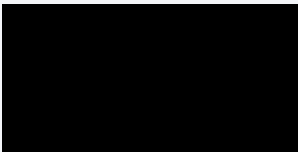



Figure 6: Decrypts hardcoded strings

After this, the malware creates a hidden directory in the AppData folder, and stores the MD5 hash value. The Figure below shows the part of code in malware for



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 7: Creates a hidden directory

Then a subfolder is created inside the parent directory created above and is named using the format "username@computername_culture." Malware will also create other folders inside this folder, such as Browsers, Grabber, etc. These folders will be used for saving the stolen data from respective sources.

The malware then identifies all the logical drives present in the victim's system using the DriveInfo() class and checks for the presence of removable devices. Next, the malware adds the drive's name and path to its target list for stealing data. After identifying the drive details, the malware steals the files from the targeted directories, as shown in Figure 8. The malware uses a multithreading approach for stealing the files fast from the victims' machines. Prynt Stealer only steals the files whose size is less than 5120 bytes and should have the following extensions:

Document: pdf, rtf, doc, docx, xls, xlsx, ppt, pptx, indd, txt, json.

Database: db, db3, db4, kdb, kdbx, sql, sqlite, mdf, mdb, dsk, dbf, wallet, ini.

Source Code: c, cs, cpp, asm, sh, py, pyw, html, css, php, go, js, rb, pl, swift, java, kt, kts, ino.

Image: jpg, jpeg, png, bmp, psd, svg, ai.

Figure 8: Steal files

Browsers

After stealing files from the victim's system, Prynt Stealer steals data from

Targeted browsers include:

- Chromium-based browsers
- MS Edge
- Firefox-based browsers

Chromium-based browsers:



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

It first creates a folder named "Browsers" and then checks for the Browsers directories (refer to the **Figure** below) in the "AppData" folder using *Directory.Exists()* method. If it returns true, the malware starts stealing data from the respective location. The stealer can target nearly all chromium-based browsers, as can be seen in the Figure below. The Chromium browsers use multiple .sqlite files for storing users' data.

Figure 9: Targeted chromium-based browsers

It steals the master key from the "Local Sate" file, which is used for decrypting the sensitive information stored in the browsers.

The malware steals Credit Cards, Passwords, Cookies, Autofill, History, Downloads, and Bookmarks data from browsers, and saves the stolen data in respective text files created under the "Browsers" directory.

Files targeted by malware for stealing data:

- Web Data (for Autofill data)
- Login Data (for Login Credentials)
- History (for search history)
- Cookies (for browser Cookies)

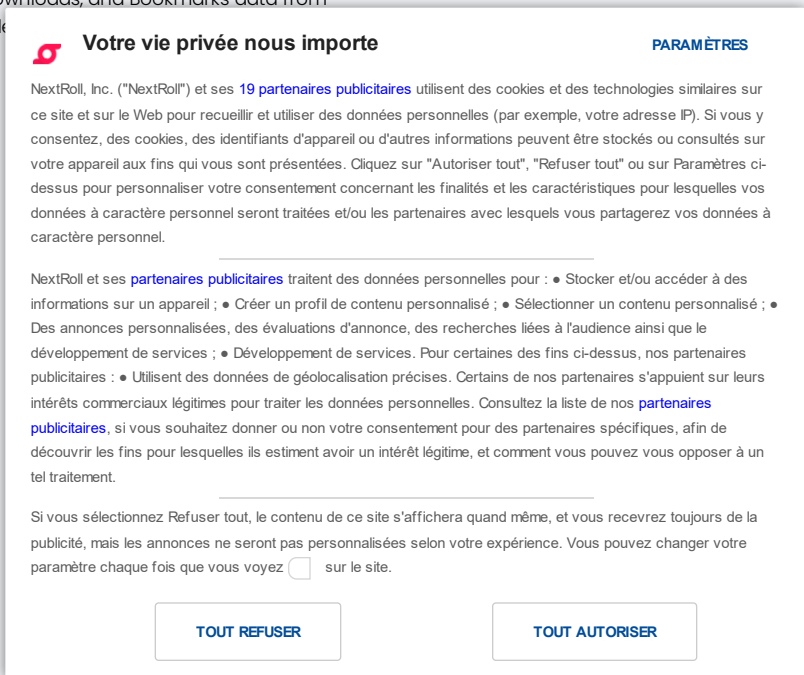


Figure 10: Steals data from chromium-based browsers

While stealing the data from browsers, the malware also checks if keywords belonging to services such as Banking, Cryptocurrency, and Porn are present in the browser data using *ScanData()* method. The Figure below shows the services for which malware runs string search operations.

Figure 11: Checks for specific services

MS Edge Browsers:

The malware first checks for the directory “\AppData\Local\Microsoft\” to identify if an edge browser is installed on the victim’s system. After this, it checks the “Login Data” file. If so, then it steals the data. The data to be seen in the Figure below. Finally, the *ScanData()* method is used again to check for browser

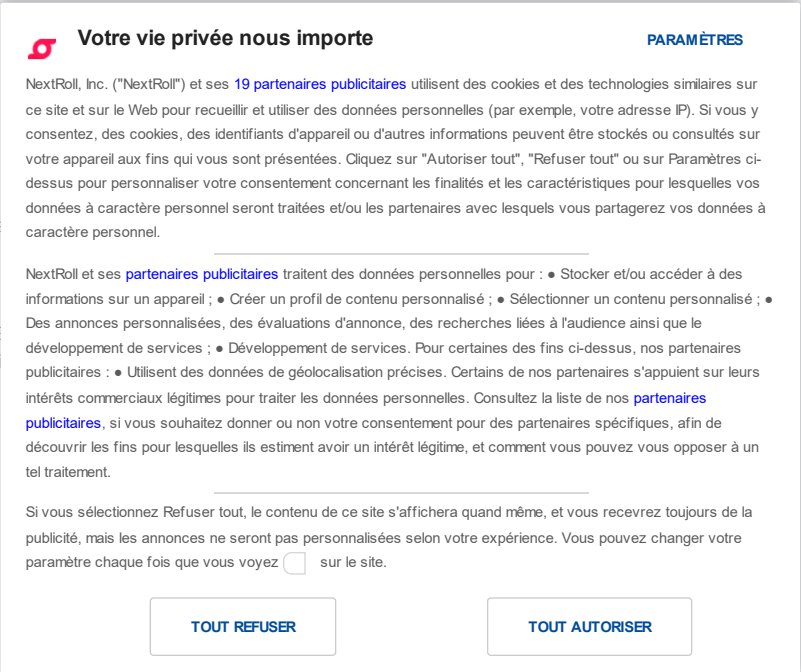


Figure 12: Steals data from MS Edge browser

Firefox-based browsers:

Prynt stealer targets eight Firefox-based browsers which can be seen in Figure 13.

Figure 13: Targeted Firefox-based browsers

The malware only proceeds to steal data if the Profile folder is present under the "AppData\Browser_name" directory. Firefox Browser uses this folder for saving user data. The malware copies the "logins.json" file from the "Profile" folder to the initially created folder for saving stolen data. The "Logins.json" file is used for storing the Firefox login credentials. Following files are targeted by malware for stealing data, present under the "Profile" folder:

- Places.sqlite (for Bookmarks and History)
- cookies.sqlite (for browser cookies)
- logins.json (for Login Credentials)

Figure 14: Steals data from Firefox-based br

Messaging Applications

After stealing data from browsers, the malware targets the following me

- Discord



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









- Pidgin
- Telegram

The malware first creates a folder names Messenger which will be used for saving data from these applications.

Discord:

After this, the malware checks for Discord tokens. It first searches for the following directories:

- *Discord\\Local Storage\\leveldb*
- *discordptb\\Local Storage\\leveldb*
- *Discord Canary\\leveldb*


It only proceeds if the above directory exists. If directories are present, malware checks for files ending with .ldb or .log and extracts Discord tokens from them using regular expression. Then it creates a folder named "Discord" and will write the stolen tokens to "Tokens.txt."

Figure 15: Steals Discord tokens

Pidgin:

Pidgin is a chat program that lets you log in to accounts on multiple chat networks. It is compatible with the following chat networks: Jabber/XMPP, Bonjour, Gad, Gaim, Google Talk, Messenger, Lotus Sametime, SILC, SIMPLE, and Zephyr.

The malware first identifies if ".purple\\accounts.xml" is present in the AppData directory. If it is, it searches for Pidgin login credentials. It steals the Login credentials and Protocol details and saves them in an accounts.txt file for exfiltration.



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 16: Steals data from Pidgin

Telegram:

The malware calls `Process.GetProcessByName()` method for getting the running process name and path in the victims' machine. The malware then checks if the Telegram string is present in the retrieved path. Finally, it gets the Telegram directory and steals data from there if it is present—the malware targets “tdata” folder for stealing telegram sessions.

Figure 17: Steals telegram sessions

Gaming Applications

Prynt Stealer targets the following gaming applications:

- Steam
- Minecraft
- Uplay

Steam:

The malware identifies the Steam installation path by checking the registry key value at “HKEY_LOCAL_MACHINE\Software\Valve\Steam.” After this action, it enumerates the subkey present under “HKEY_LOCAL_MACHINE\Software\Valve\Steam\Apps” to get details of the application, as can be seen in the Figure below. The malware also targets the steam’s SSFN file, known as the authorization file, and copies it for exfiltration.

Figure 18: Steals data from steam

Uplay:

The malware looks for “Ubisoft Game Launcher” in the AppData folder, and steals all the files in it for exfiltration.

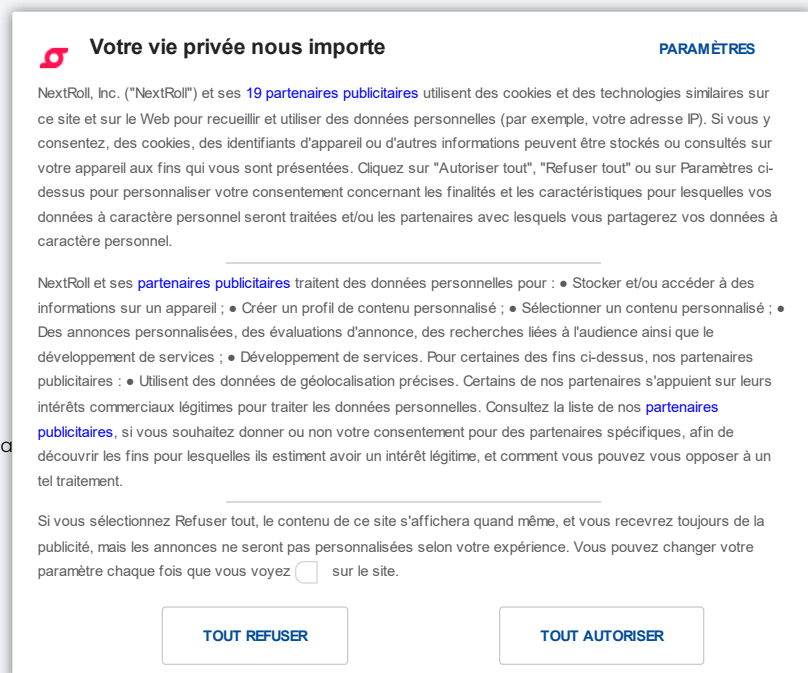


Figure 19: Steals data from Uplay

Minecraft:

For Minecraft, the stealer checks if the ".minecraft" folder is present under the AppData directory. If it is present, it creates a folder named "Minecraft" under the "Gaming" folder to save the stolen data.

This stealer copies "launcher_profiles.json", "servers.dat" and screenshots to "Minecraft " folder for exfiltration. It also extracts mods and version details and saves them to respective text files created in "Minecraft" folder.

Figure 20: Steals data from Minecraft


Crypto Wallets

The malware targets the following crypto wallets:

Zcash, Armory, Bytecoin, Jaxx, Ethereum, AtomicWallet, Guarda, and Coinomi

It creates a folder named "Wallets" and then enumerates a list of hardcoded crypto wallet used by the victim.

Stealer queries registry for identifying the location of Blockchains such as shown in Figure below. It obtains the path from registry data "strDataDir" under "HKEY_CURRENT_USER\Software\Blockchain_name\ Blockchain_name-Config"



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 21: Steals data from Crypto wallets

FTP Applications

Prynt stealer targets FileZilla, a free and open-source, cross-platform FTP application. It steals the data from "sitemanager.xml" and "recentervers.xml" and stores the data in the "Hosts.txt" file under the "FileZilla" folder for exfiltration.

Figure 22: Steals data from FileZilla

VPN

Prynt Stealer targets the following VPN applications:

- OpenVPN
- ProtonVPN
- NordVPN

It copies the configuration file of ProtonVPN, OpenVPN and steals the user's configuration file.

Figure 23: Steals data from VPN's configuration files

Directory tree

After this action, the malware creates a folder named "Directories" and writes the directory structure to text files, as shown in the Figure below. The files include the one targeted initially for copying data.

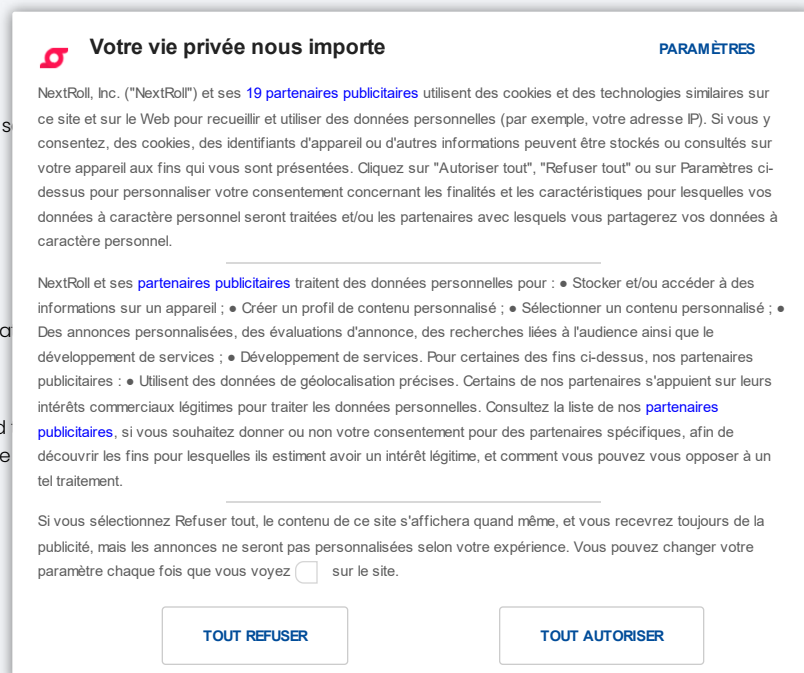


Figure 24: Obtains the directory tree

System Information

It creates a folder named "System" in which it will store the solen information regarding running processes, network details, and victim's system screenshot, etc.

Process Details:

Prynt stealer uses `Process.GetProcesses()` method to identify all the run system and write them to the "Process.txt" file in the format:

- Process name
- Process ID
- Executable path

After this action, it gets the active windows using the `process.MainWindow` into the "Windows.txt" file in the format:

- Process name
- Process ID
- Executable path

 **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 25: Extract details of current processes

Screenshot:

Now it takes a screenshot of the victim's system and saves it as a "Desktop.jpg" file:

Figure 26: Takes Screenshot

Network Information:

The stealer also extracts the network credentials using the command "*chcp 65001 && netsh wlan show profile*" and saves them into the "Savednetworks.txt" file. After this, using the command "*/C chcp 65001 && netsh wlan show networks mode=bssid*" it obtains the list of available networks and saves them into the "ScanningNetworks.txt" file.

Figure 27: Steals save network credentials and identify the

Windows Product Key:

It steals the windows product key from the "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion, the "ProductKey.txt 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 28: Steal Windows product key

Data exfiltration:

The malware creates a list and adds the overview of stolen data to it, as shown in the Figure below. Then it sends a chat message using the Telegram bot.

For identifying the public IP, it sends a request to `hxxp[:]//icanhazip[.]com`

For identifying the geolocation, it sends a request to `hxxps[:]//api.mylnikov.org/geolocation/wifi?v=1.1&bssid=`

Figure 29: Creates an overview of stolen

The malware compresses the folder where the stolen data is saved and Furthermore, it uses a secure network connection for exfiltrating the sto



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 30: Decrypted network traffic


Other Capabilities

Our analysis found that specific modules in the sample are not executed by the malware, including the Anti-analysis, Keylogger, and Clipper. Threat Actors (TAs) also provide a builder for this stealer, which can be customized to control these functionalities. Taking the case of anti-analysis, it's working on the hardcoded string present in malware. The Figure below shows the method responsible for executing anti-analysis functionalities. Similarly, other processes also depend on these hard-coded strings.

Figure 31: Anti-analysis

Clipper:

The Figure below shows the list in which TAs can store their crypto address populated, highlighting the fact that TA might not have opted for this functionality.



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 32: Clipper

Keylogger:

This stealer enables the keylogging feature only if the hardcoded specific applications are running in the system. The stolen data will be saved in "logs\keylogger" folder.

Share the Post:



[Previous](#)
[Fake MetaMask App Steals Cryptocurrency](#)

[Next](#)

Related

Figure 33: Keylogger module

Conclusion


Prynt Stealer is a recent Infostealer strain. It has a ton of capabilities. The stealers in the cybercrime marketplaces, TAs do adopt new toolkits which Tactics, Techniques, and Procedures. These types of malware provide a corporate networks, as breaking into a network is not everyone's cup of

Our Recommendations:

- Avoid downloading pirated software from warez/torrent websites, such as YouTube, torrent sites, etc., mainly contains such malware
- Use strong passwords and enforce multi-factor authentication when
- Turn on the automatic software update feature on your computer devices.

Cyble Sensors Detect New Attacks on LightSpeed Cyber-Security Software Package
including Eternit WordPress Plugins

October 31, 2024



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

- Refrain from opening untrusted links and email attachments without first verifying their authenticity.
- Educate employees in terms of protecting themselves from threats like phishing's/untrusted URLs.
- Block URLs that could be used 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) Solution on the employees' systems.

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



Indicators of Compromise (IoCs):

Indicators	Indicator type	Description
ab913c26832cd6e038625e30ebd38ec2 719873f61eeb769493ac17d61603a6023a3db6dd 1283c477e094db7af7d912ball5c77c96223208c03841768378a10dl819422f2	MD5 SHA1 SHA256	Malicious binary
0b75113f8a78dcc1dea18d0e9aabc10a 269e61eed692911c3a886a108374e2a6d155c8dl 808385d902d8472046e5899237e965d8087da09d623l49ba38b38l465		
661842995f7fdd2e61667dbc2f019ff3 1a638a81b9135340bc7dlf5e7eae5f3f06667a42 4569670aca0cc480903b07c7026544e7el5b3f293e7cl533273c90l53c4		



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