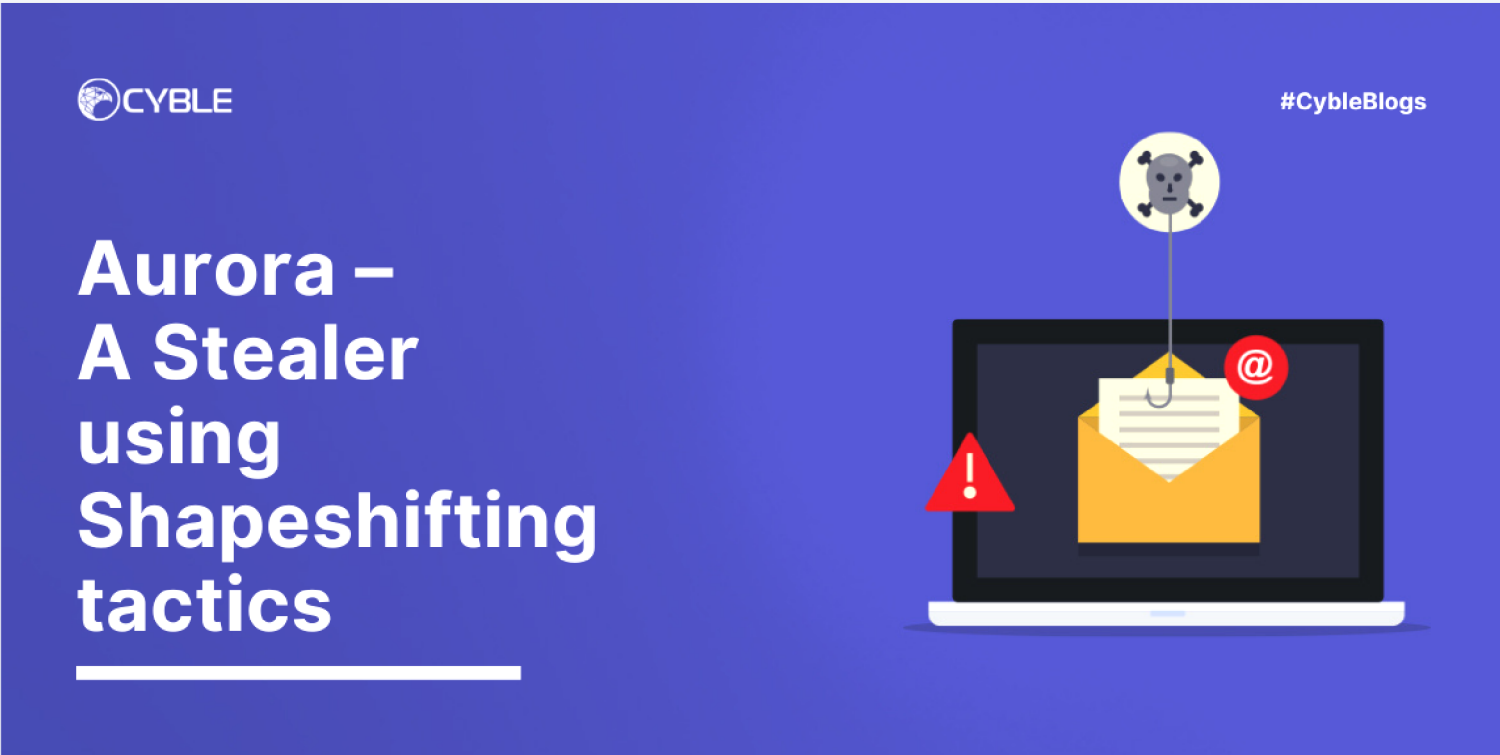
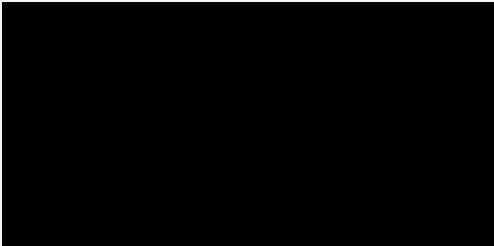


Home » Blog » Aurora – A Stealer Using Shapeshifting Tactics



I N F O S T E A L E R

January 18, 2023



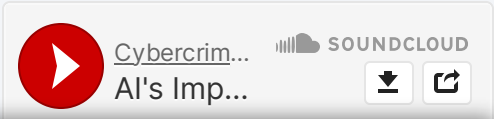
# Aurora – A Stealer Using Shapeshifting Tactics

## CRIL Analyzes Aurora, An Information Pages Imitating Popular Applications

## Threat Actors Leveraging Popular Applications

Threat Actors (TAs) are increasingly using phishing sites to steal information or downloading malware such as Information Stealers (RATs), and other malware. The links to these phishing sites are often found in online ads, and other channels. Cyble Research and Analysis is regularly monitoring various phishing campaigns and has recently found the latest example of this that we have encountered. We will analyze how it imitates popular applications to infect the maximum number of users.

## Shapeshifting Behavior





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

Cyble Research and Intelligence Labs (CRIL) initially identified a phishing site, “hxxps[:]//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
- hxxps[:]//kodfem[.]hemsida[.]eu/downloads/teamviewer[.]exe

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

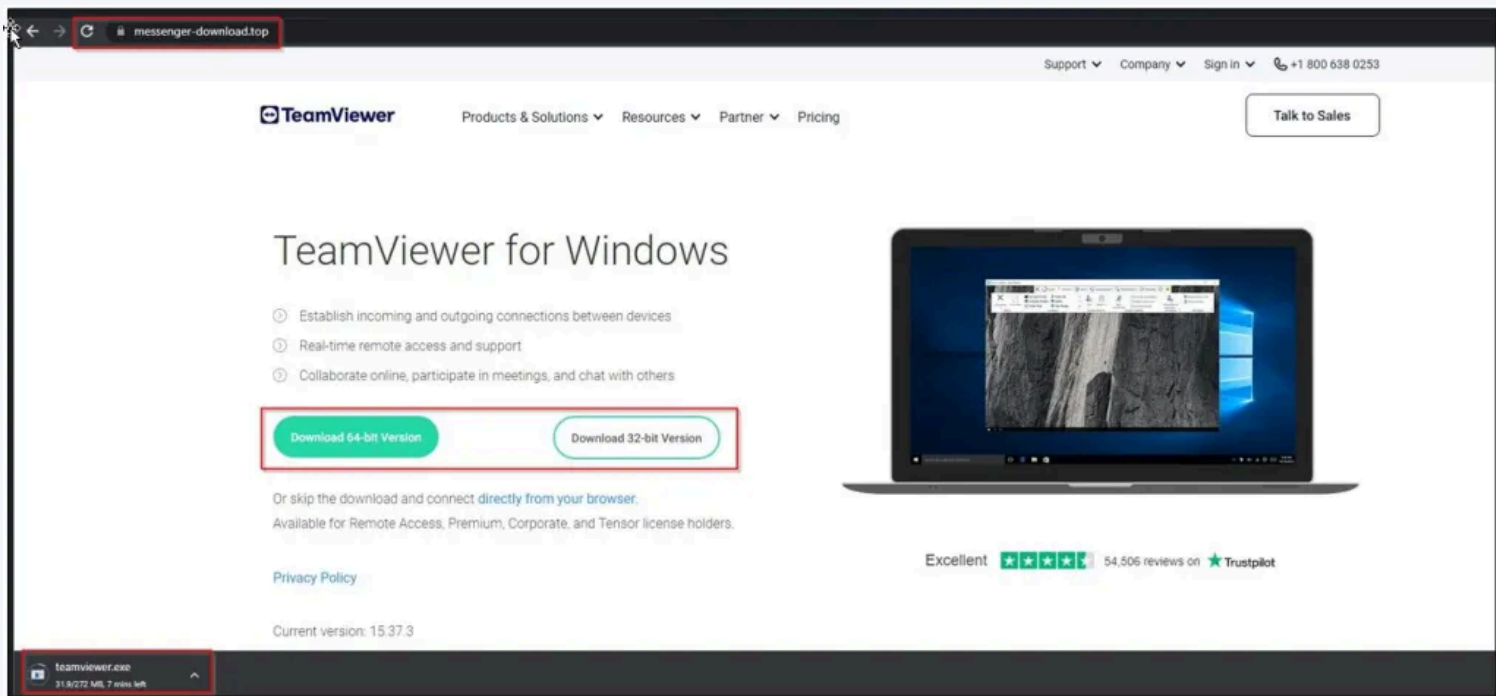


Figure 1 – Messenger phishing page downloading Aurora stealer as teamviewer.exe

The “messenger.exe” and “teamviewer.exe” files that have been downloaded are actually malicious Aurora Stealer samples, which have been padded with extra zeroes at the end to increase their size to around 260MB. TAs use this method to evade detection by antivirus software, as larger files can be harder for AV to process.



Aurora is a type of malware that aims to steal personal data from web browsers, crypto wallets, browser extensions, Telegram, and other applications.

After gathering all the necessary information, it saves it to a file, compresses it using GZIP, and converts it into Base64 encoding format to be sent to the Command-and-Control (C&C) server.

We have analyzed and explained the detailed behavior of the malware in the next section.

## Technical Analysis

We have taken the below sample hash for our analysis: `fd17b39833ee0fae6cc8549dfa602adff3cf002cd0a0e`



### 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](#)

Golang executable file. The unique build ID of the Go compiled binary is shown below.

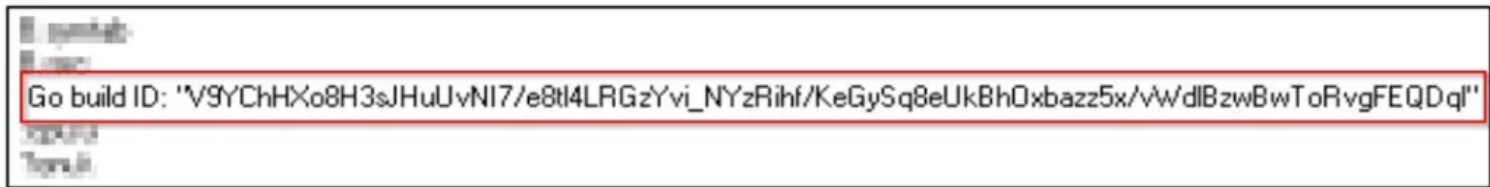


Figure 2 – Go build ID

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.

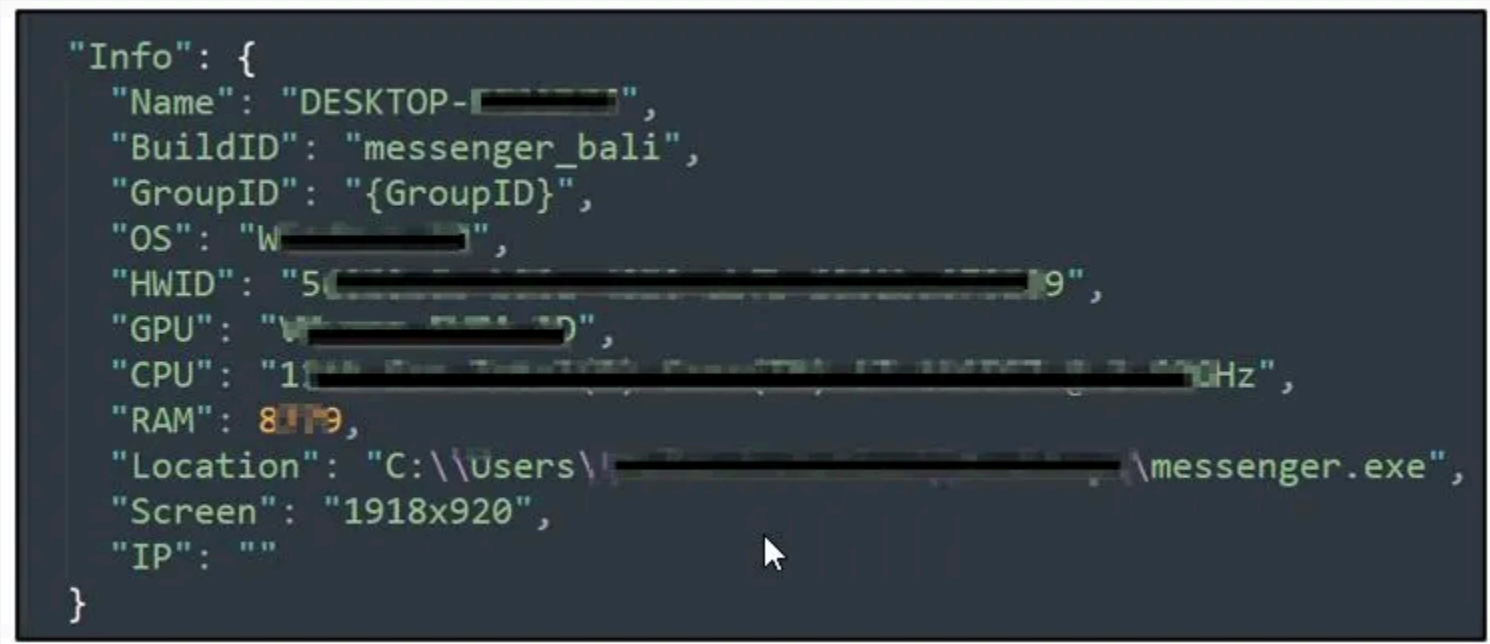


Figure 3 – Collected system information

After collecting system information, the malware queries the victim’s registry for specific keys on the victim’s machine and searches for specific browser data, including:

- *Cookies*
- *History*
- *Login Data*
- *Web Data*

Then, the stealer begins to extract information related to cryptocurrency wallets by reading files from specific directories. The stealer targets the following directories:

- “\\AppData\\Roaming\\Armory”
- “\\AppData\\Roaming\\bytecoin”
- “\\AppData\\Roaming\\Exodus”
- “\\AppData\\Roaming\\Ethereum\\keystore”
- “\\AppData\\Roaming\\Electrum\\wallets”
- “\\AppData\\Roaming\\com.libertyjaxx\\Index.dat”
- “\\AppData\\Roaming\\Guarda\\Local Storage”

### 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


- “\\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

The malware continues its data collection by searching for Discord, and Steam applications in the victim’s machine. It then searches for these applications from their config and session data files. The malware also searches for files like the Desktop and Documents and takes screenshots of the victim’s desktop.

Finally, the Aurora stealer processes the stolen information into a JSON file, creating a GZIP archive of it, and encoding the GZIP archive with a base64 string. The figure below illustrates the structure of the JSON file, showing how the stealer stores the stolen information.



### 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









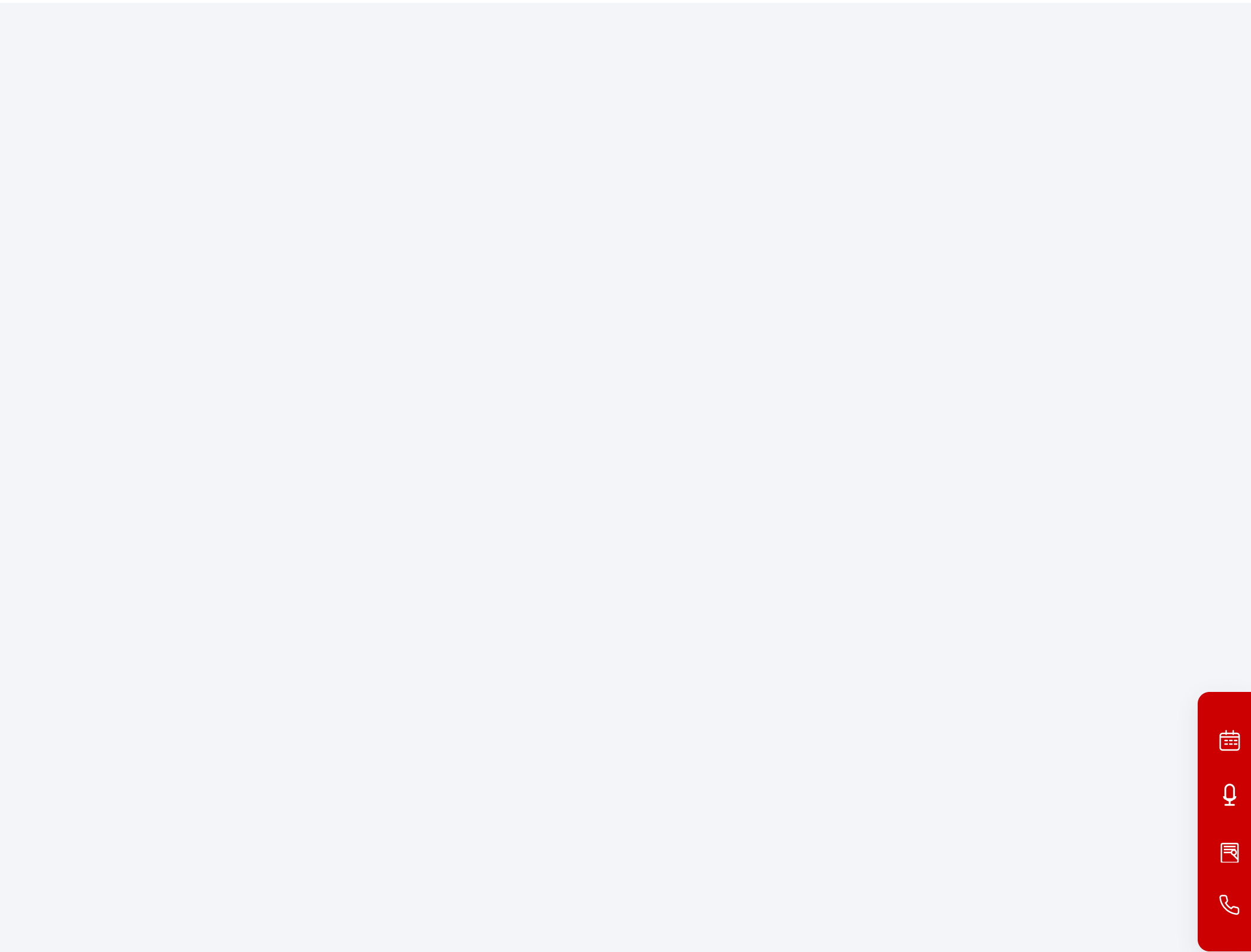


Figure 5 – JSON format to store stolen data

The table below describes the keys of the JSON content.

Type	Type of the stolen data (Browsers, OS, etc.)
Info { Name BuildID GroupID OS HWID GPU CPU RAM Location Screen IP }	Victims’ device name Browser name Operating system version Graphics card information Malware file path Victims’ system IP, empty if not available
Browser	Browser name (Chrome, Firefox, etc.)
Cache	Encoded in base64 content of the browser cache
Type_Grab	Target file info (Cookie, Password, etc.)
FileP	Target browser file (Cookie, Password, etc.)

### Command & Control

Aurora Stealer communicates with the below C&C server to receive information.



### 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 new malware strains and phishing campaigns in the wild and update blogs with actionable intelligence to protect users from such notorious attacks.

## Our Recommendations

- The initial infection may happen via phishing websites, so use security products to detect phishing websites.
- Avoid downloading pirated software from Warzone, as they are present on sites such as YouTube, Torrent sites, etc.
- Use strong passwords and enforce multi-factor authentication.
- Turn on the automatic software update feature for all your connected devices.
- Use a reputed antivirus and internet security software on all devices, including PC, laptop, and mobile.
- Refrain from opening untrusted links and email attachments to verify authenticity.
- Educate employees on protecting themselves from phishing attacks.
- Block URLs that could be used to spread the malware.
- Monitor the beacon on the network level to block malicious connections.

## 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	T1204 T1059 T1047	User Execution Command and Scripting Interpreter Windows Management Instrumentation
Defense Evasion	T1027 T1497	Obfuscated Files or Information Virtualization/Sandbox Evasion
Credential Access	T1003 T1056 T1552	OS Credential Dumping Input Capture Credentials in Registry
Discovery	T1082 T1518 T1083 T1087	System Information Discovery Security Software Discovery File and Directory Discovery Account Discovery
Collection	T1005	Data from Local System
Command and Control	T1071 T1095	Application Layer Protocol Non-Application Layer Protocol

## Indicators of Compromise (IOCs)

Indicators	Indicator Type	Description
b810b7d416251367ef790bc9a8a9830a69760ba5c1b83055e9a0647270629d9c	Sha256	me
fd17b39833ee0fae6cc8549dfa602adff3cf002cd0a0ef8fa63876ec50a74552	Sha256	me rer pa
44b64cb2be0a5e9fd51528f00a308df7lead226c7cf733ed2568ada07c9044a8	Sha256	tec
c7f43e2afe62a622f77f888f56712a41aec56d5a765a95585f69e870359119c9	Sha256	tec rer pa
hxxps[:]//messenger-download[.]top	Domain	Ph
hxxps[:]//download[.]balint[.]info[.]hu/messenger[.]e		
hxxps[:]//kodfem[.]hemsida[.]eu/downloads/teamv		
45[.]15[.]156[.]210:8081		

**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

Share the Post:



Previous

Ransomware Extortion Techniques: A Growing Concern For O...Gigabud RAT: New Android RAT Masquerading As Governme...

Next

## 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

### 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