

Home » Blog » Rhadamanthys: New Stealer Spreading Through Google Ads



M A L W A R E

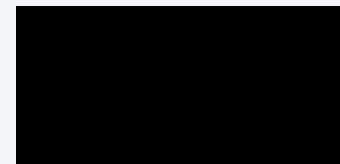
January 12, 2023


Rhadamanthys Stealer Spread Through Google

CRIL Analyzes Rhadamanthys Stealer, A New Spread Via Google Ads To Steal Users' Sensitive

Evasive Infostealer leveraging Phishing and its Delivery

Threat Actors (TAs) are increasingly using spam emails and phishing websites to download malware such as Stealer and Remote Access Trojan (RAT)



 **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](#)

sensitive information.

Cyble Research & Intelligence Labs (CRIL) is actively monitoring various stealer malware and publishing blogs about them to inform and educate its readers.

Recently, we came across a new **strain** of malware called "Rhadamanthys Stealer." This stealer variant is active, and the TA behind the malware stealer is selling this under the Malware as a Service (MaaS) model.

Rhadamanthys stealer spreads by using Google **Ads** that redirect the user to phishing websites that mimic popular software such as Zoom, AnyDesk, Notepad++, Bluestacks, etc. It can also spread via spam email containing an attachment for delivering the malicious payload.

Spam Email

The Rhadamanthys stealer infection starts through spam emails containing a PDF attachment named "Statement.pdf" as shown in the figure below.

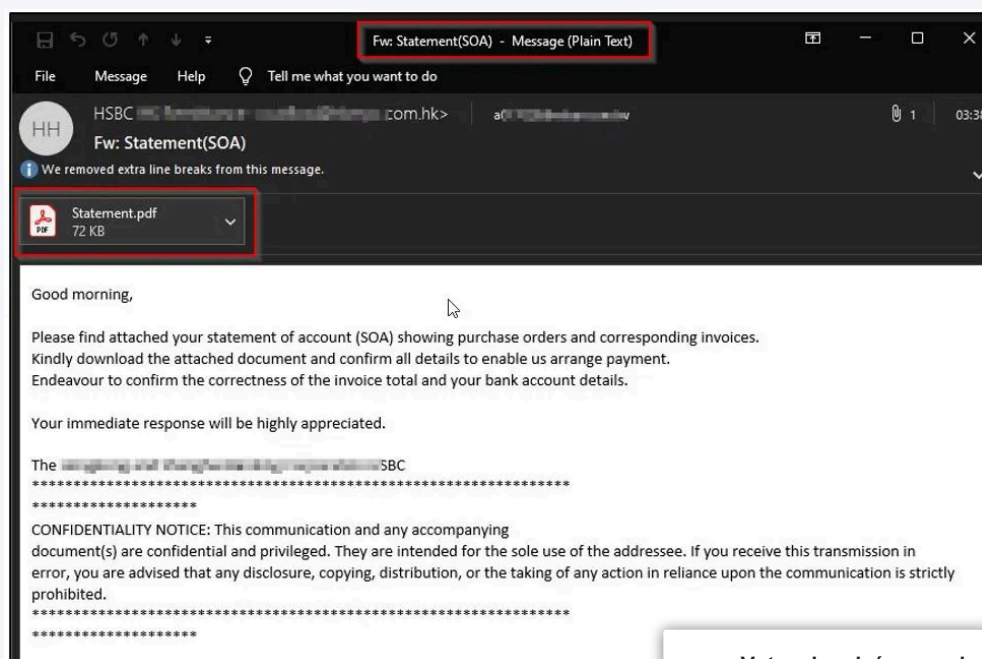
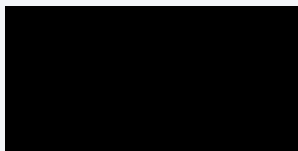



Figure 1 – Spam Email with PDF Attachment

When opening the attachment present in the spam email, it displays a message titled "Acrobat DC Updater" and includes a download link labelled "Download U



 **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](#)

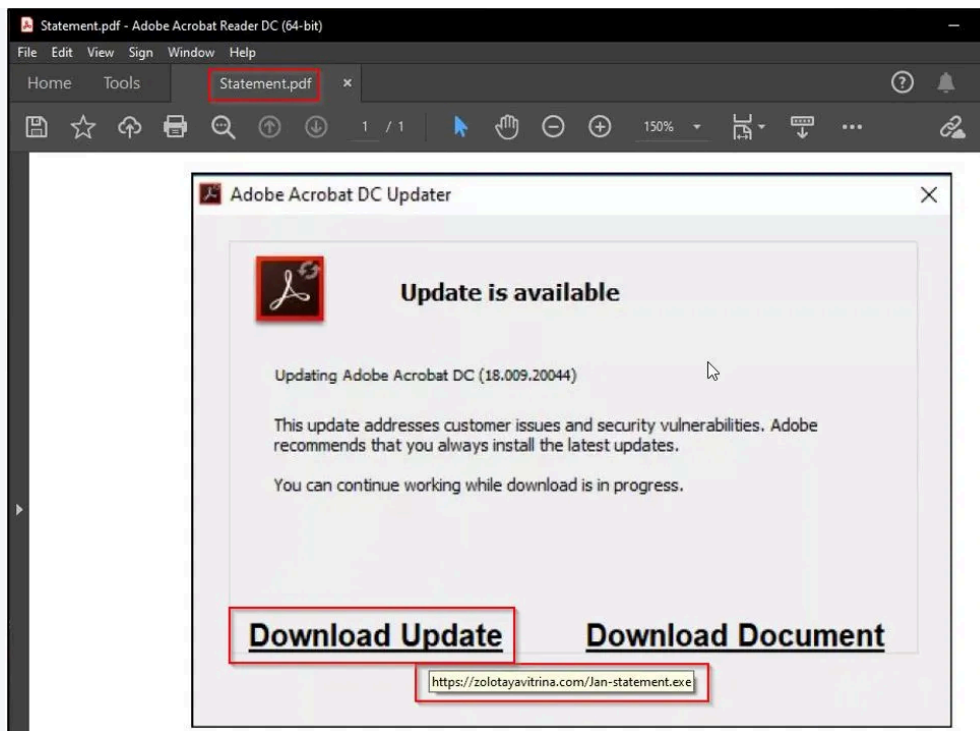


Figure 2 – PDF document with a download link

When a user clicks the “Download Update” link, it downloads a malware executable from an URL “https://zolotayavitrina[.]com/Jan-statement[.]exe” into the Downloads folder.

Upon execution of the "Jan-statement.exe" file, it runs the stealer and allows it to steal sensitive information from the victim's machine. The figure below illustrates the process tree of the Rhadamanthys stealer that was delivered via a spam email.

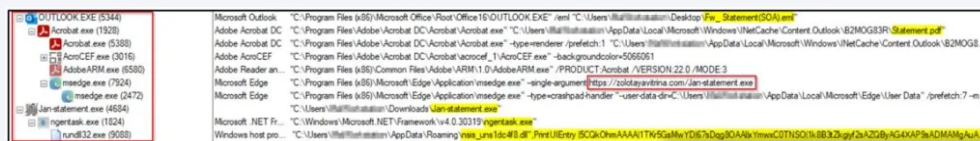



Figure 3 – Process tree of spam email download

Phishing Sites

The TAs behind this campaign also created a highly convincing phishing legitimate websites to trick users into downloading the stealer malware, activities. The link to these phishing websites spreads through Google and phishing domains created to spread this malware. Some of the following

- [bluestacks-install\[.\]com](#)
- [zoomus-install\[.\]com](#)
- [install-zoom\[.\]com](#)
- [install-anydesk\[.\]com](#)
- [install-anydesk\[.\]com](#)
- [zoom-meetings-install\[.\]com](#)
- [zoom-meetings-download\[.\]com](#)
- [anydesk-download\[.\]com](#)
- [zoomvideo-install\[.\]com](#)
- [zoom-video-install\[.\]com](#)
- [installer-zoom\[.\]com](#)
- [noteepad.hasankahrimanoqul\[.\]com\[/\].ltr](#)



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 phishing websites further downloads an installer file disguised as a legitimate installer downloading the respective applications. When installing the respective application, it also silently installs the stealer malware without the user's knowledge. The below figure shows the process tree of the malicious AnyDesk installer deploying Rhadamanthys stealer.

Figure 4 – Process tree of malicious AnyDesk installing Stealer

Payload Analysis

Upon execution of the installer file, it creates a folder named “ST” in the %temp% location and drops two hidden binary executable files.

- *Initialize 4.exe*
- *Runtime Broker.exe*

The loader “Runtime Broker.exe” is a 32-bit PyInstaller executable with SHA256: *db66fc58c07ba0ccbe1b9c2db770179d0d931e5bf73838da9c915581661d4c1a*.

The additional information is shown in the figure below.

Figure 5 – Static file details of “Runtime Broker.exe”

Upon execution of “Runtime Broker.exe”, it drops multiple Python-support files.

These files include “.pyc”, “.pyd”, and “.dll” files, which were extracted from the executable file and shown below.

Figure 6 – Extracted files of PyInstaller executable

The “Binary_Stub_Replacer.pyc” is a python compiled file which contains the stealer code. It was de-obfuscated using replace function and then converted into Binary and Assembly format for getting the




second stage malicious python code as shown below.

Figure 7 – Decompiled python content of Binary_Stub_Replacer.pyc

The decoded python code contains an embedded base64-encoded content which is a shellcode. When executed, this python code decodes the base64-encoded stub, creating a new Portable Executable (PE) payload file. The PE file is then injected into a new "Runtime Broker.exe" process using the CreateThread() API function, as shown in the image below.

Figure 8 – Decoded payload from base64

The below image shows the details of the shellcode, which is a 32-bit ex Microsoft visual C/C++ compiler, as shown below.



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 9 – Payload file details

Upon execution, the shellcode begins by creating a mutex object to ensure that only one copy of the malware is running on the victim's system at any given time. It then checks if it is running on a virtual machine, such as VMware or VirtualBox, by searching for strings associated with virtual machine environments, as shown in the figure below.



**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 10 – AntiVM related strings

This check is designed to prevent the malware from being detected and executed. If the malware detects that it is running in a controlled environment, it will not execute. Otherwise, it will continue and perform the stealer activity as intended.

After the check, the shellcode further drops a DLL file named “nsis_uninstall” and launches it using the “rundll32.exe” with specific parameters shown in the screenshot below.

Figure 11 – Dropped DLL file execution

While investigating this malware, we observed that a steganography image was downloaded from a remote server. We suspect the shellcode decrypts the steganography image and uses it to display a message.



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

Rhadamanthys payload. The memory of rundll32.exe contains all the malicious code responsible for stealer activities.

The Rhadamanthys stealer now starts collecting system information by executing a series of Windows Management Instrumentation (WMI) queries. The collected information includes the computer name, username, OS version, RAM, CPU information, HWID, time zone, user and keyboard language, and others.


After gathering system details, the malware queries the directories of the installed browsers on the victim's machine and searches for browser-related files such as browsing history, bookmarks, cookies, auto-fills, login credentials, etc. It targets different browsers such as Brave, Edge, Chrome, Firefox, Opera Software, Sleipnir5, Pale Moon, CocCoc, etc.

Crypto Wallets

This stealer malware is also designed to target various crypto wallets and collects information from them. While the malware can target a wide range of crypto wallets, the observed stealer samples were found to have specific functionality to target the following crypto wallets:

- *Armory*
- *Binance*
- *Bitcoin*
- *Bytecoin*
- *Electron*
- *Qtum-Electrum*
- *Solar wallet*
- *WalletWasabi*
- *Zap*
- *Zecwallet Lite*
- *Zcash*

Also, the Rhadamanthys stealer steals data from the following crypto wallet browser extensions, which are hard coded in the stealer binary, as shown in the image below.



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 12 – Targeted Crypto wallets with the extension ID

The stealer also targets various applications such as FTP clients (CoreFTP, WinSCP), email clients (Foxmail, Thunderbird, Outlook, TrulyMail, GmailNotifierPro), File managers (Total commanders), password managers (RoboForm, KeePass), VPN services (NordVPN, ProtonVPN, Windscribe VPN, OpenVPN), messaging applications (Tox, Discord, Telegram) and others. Additionally, it captures screenshots of the victim's machine using the *BitBlit()* API function. Finally, it sends all the collected stolen information to the attacker's C&C server.

C&C Panel

The below figure shows the Rhadamanthys stealer's active C&C panel.



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:

Figure 13 – Rhadamanthys stealer C&C p

Conclusion



Information stealers are malicious software used to gain unauthorized access to corporate networks, which has become a serious concern. Threat Actors use various techniques to deploy their malicious payloads into the victim's system. In this case, we observed that the TAs used spam email and phishing websites to deliver the Rhadamanthys Stealer, designed to steal sensitive information from the victim's machine. Additionally, it was also noticed that the malware spreads via Google Ads. It is crucial for users to exercise caution when receiving spam emails or to visit phishing websites and to verify the source before downloading any applications.

Next

Cyble Research and Intelligence Labs will continue to monitor the new payload stealer in the wild and update blogs with actionable intelligence to protect users from such notorious attacks.

Related Posts

Our Recommendations

- The initial infection may happen via spam emails or phishing websites, so enterprises should use security products to detect phishing emails and websites.
- Avoid downloading pirated software from Warez/Torrent websites. The "Hack Tool" present on sites such as YouTube, Torrent sites, etc., contains such malware.
- Use strong passwords and enforce multi-factor authentication wherever possible.
- Turn on the automatic software update feature on your computer, mobile, and other connected devices.
- Use a reputed anti-virus and internet security software package on your connected devices, including PC, laptop, and mobile.
- Refrain from opening untrusted links and email attachments without first verifying their authenticity.
- Educate employees on protecting themselves from threats like phishing/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.

IT Vulnerability Report: Fortinet, SonicWall, Grandd

Exposures Top 1 Million

Cyble Sensors Detect New Attacks on LightSpeed, GutenKit WordPress Plugins

MITRE ATT&CK® Techniques

October 31, 2024

Tactic	Technique ID	Technique Name
Initial Access	T1598	Spearphishing Attachment

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

Privacy Policy

Schedule a Personalized Demo to Uncover Threats That No One

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

Indicators of Compromise (IOCs)



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

Indicators	Indicator Type	Description
046981c818bd26e7c28b12b998847038e6b64c44df6645438dae689d75fb0269	Sha256	Spam email
4f4b5407d607ee32e00477a9f4294600ca86b67729ff4053b95744433117fccf	Sha256	Spam email
4a55c833abf08ecfe4fb3a7f40d34ae5aec5850bc2d79f977c8ee5e8a6f450d4	Sha256	PDF attachment (Statement.pdf)
093a58f36c075644dlc8856acdefad7fd22332444b6aa07fee2ad615d50b743	Sha256	AnyDesk.msi
db66fc58c07ba0ccbelb9c2db770179d0d931e5bf73838da9c915581661d4c1a	Sha256	Runtime Broker.exe
fe99a49596fc6f841b7605021da6fce7f6c817d5247d880227f790388a7cabe4	Sha256	Shellcode exe




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