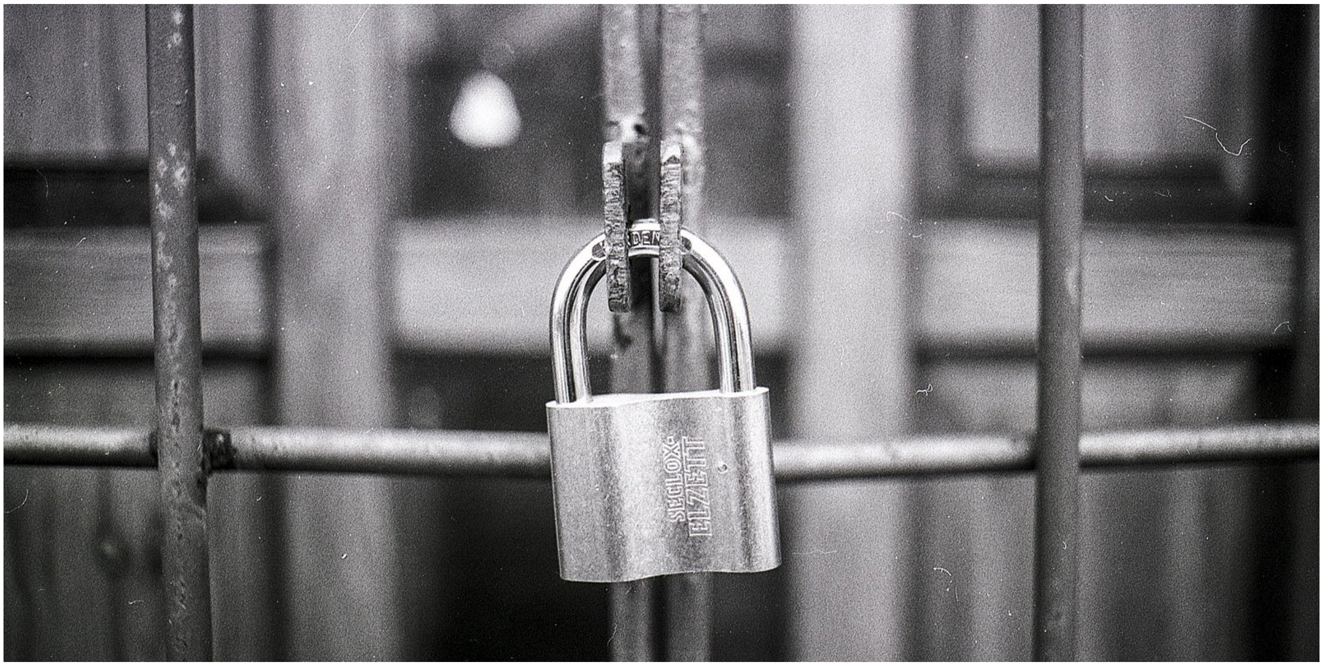
Meet Lorenz — A new ransomware gang targeting the enterprise

bleepingcomputer.com/news/security/meet-lorenz-a-new-ransomware-gang-targeting-the-enterprise/

Lawrence Abrams

By
Lawrence Abrams

- May 13, 2021
- 12:54 PM
- 2



A new ransomware operation known as Lorenz targets organizations worldwide with customized attacks demanding hundreds of thousands of dollars in ransoms.

The Lorenz ransomware gang began operating last month and has since amassed a growing list of victims whose stolen data has been published on a ransomware data leak site.

Michael Gillespie of ID Ransomware has told BleepingComputer that the Lorenz ransomware encryptor is the same as a previous operation known as ThunderCrypt.

It is not clear if Lorenz is the same group or purchased the ransomware source code to create its own variant.

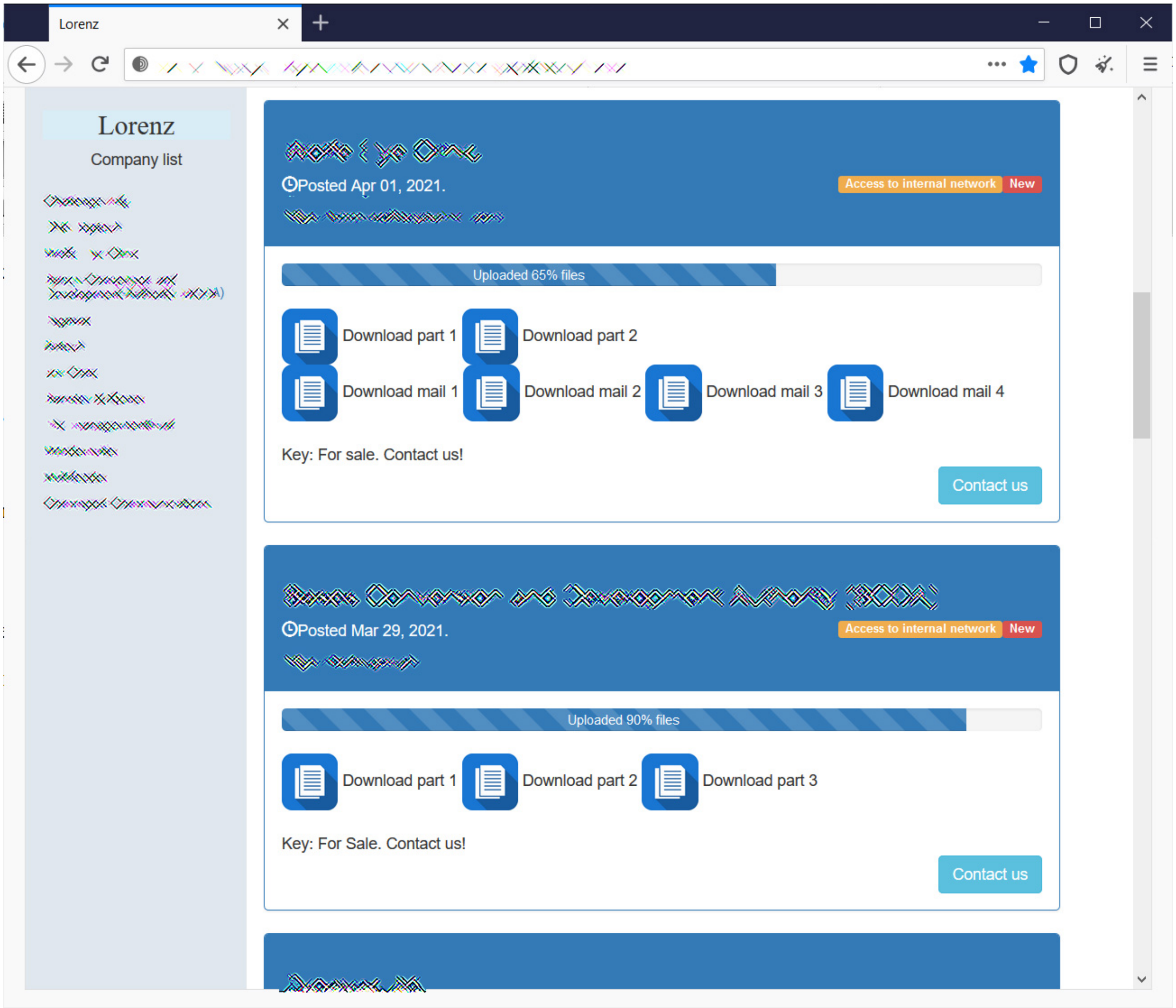
Data leak site launched to extort victims

Like other human-operated ransomware attacks, Lorenz will breach a network and spread laterally to other devices until they gain access to Windows domain administrator credentials.

While spreading throughout the system, they will harvest unencrypted files from victims' servers, which they upload to remote servers under their control.

This stolen data is then published on a dedicated data leak site to pressure victims to pay a ransom or to sell the data to other threat actors.

This Lorenz data leak site currently lists twelve victims, with data released for ten of them.



Lorenz

[redacted]

Lorenz

Company list

[redacted]

[redacted]

Posted Apr 01, 2021.

[redacted]

Uploaded 65% files

Key: For sale. Contact us!

[redacted]

Posted Mar 29, 2021.

[redacted]

Uploaded 90% files

Key: For Sale. Contact us!

[redacted]

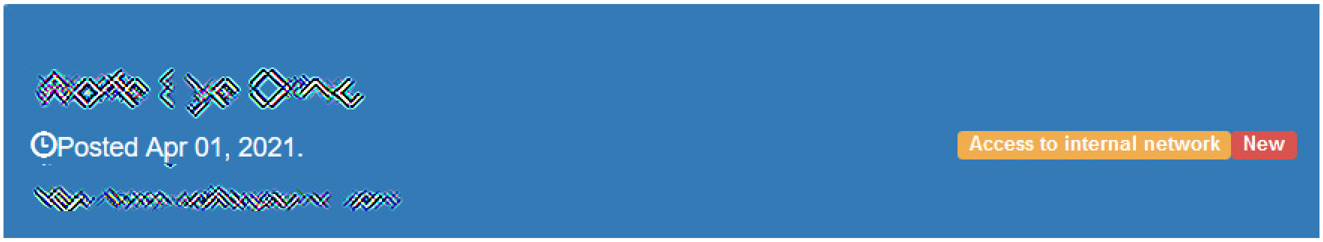
Lorenz data leak site

When the Lorenz gang publishes data, they do things a bit differently compared to other ransomware gangs.

To pressure victims into paying the ransom, Lorenz first makes the data available for sale to other threat actors or possible competitors. As time goes on, they start releasing password-protected RAR archives containing the victim's data.

Ultimately, if no ransom is paid, and the data is not purchased, Lorenz releases the password for the data leak archives so that they are publicly available to anyone who downloads the files.

Another interesting characteristic not seen in other data leak sites is that Lorenz sells access to the victim's internal network along with the data.



[redacted]

Posted Apr 01, 2021.

[redacted]

Offering access to victim's internal network
For some threat actors, access to the networks could be more valuable than the data itself.

The Lorenz encryptor

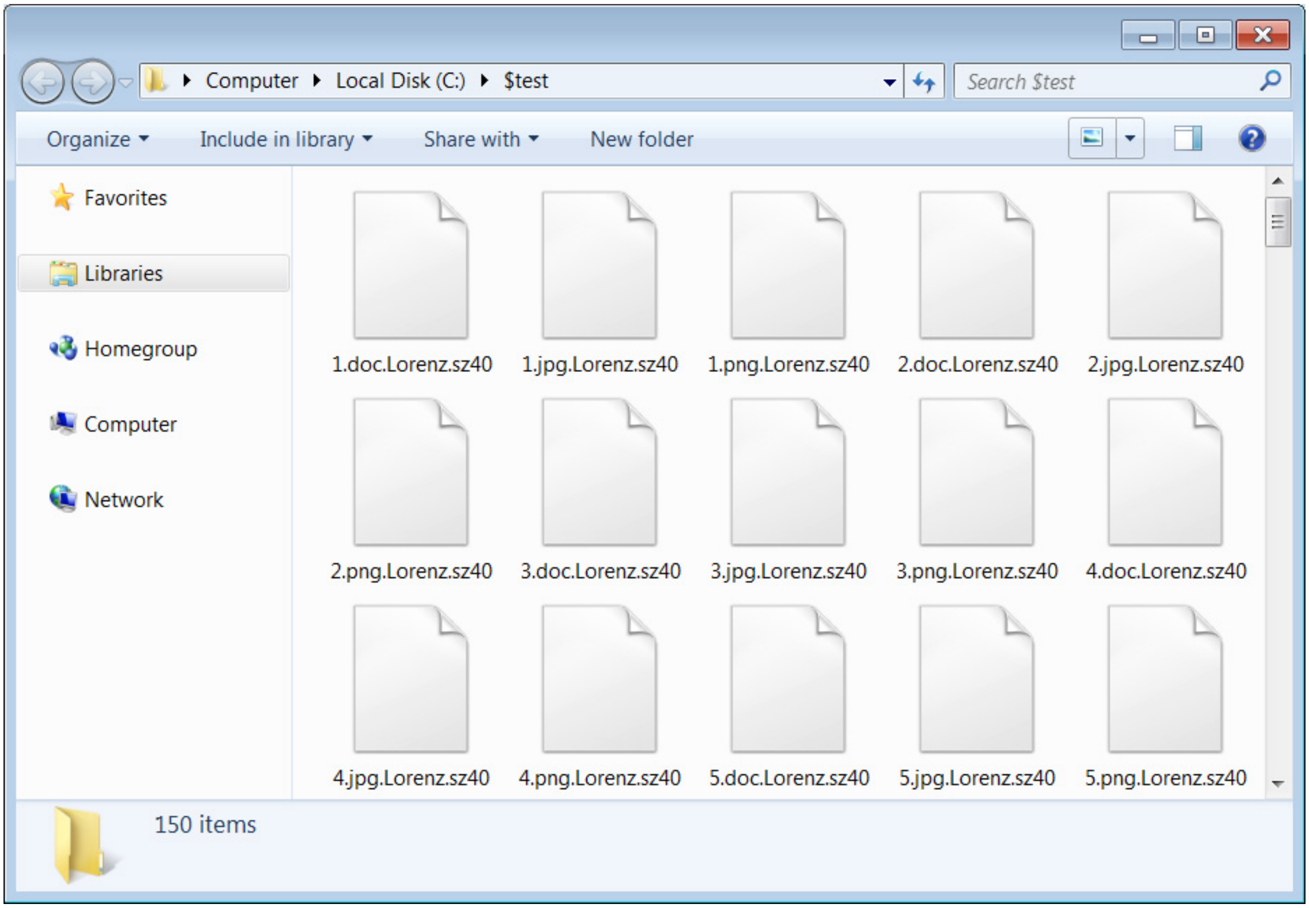
From samples of the Lorenz ransomware seen by BleepingComputer, the threat actors customize the malware executable for the specific organization they are targeting.

In one of the samples shared with BleepingComputer, the ransomware will issue the following commands to launch a file named ScreenCon.exe from what appears to be the local network's domain controller.

```
wmic /node:"0.0.0.0" /USER:"xx.com\Administrator" /PASSWORD:"xx" process call create
"cmd.exe /c schtasks /Create /F /RU System /SC ONLOGON /TN sz402 /TR
"\\xx.com\NETLOGON\MSI_Install\ScreenConn.exe" & SCHTASKS /run /TN sz402&SCHTASKS
/Del
```

When encrypting files, the ransomware uses AES encryption and an embedded RSA key to encrypt the encryption key. For each encrypted file, the **.Lorenz.sz40** extension will be appended to the file's name.

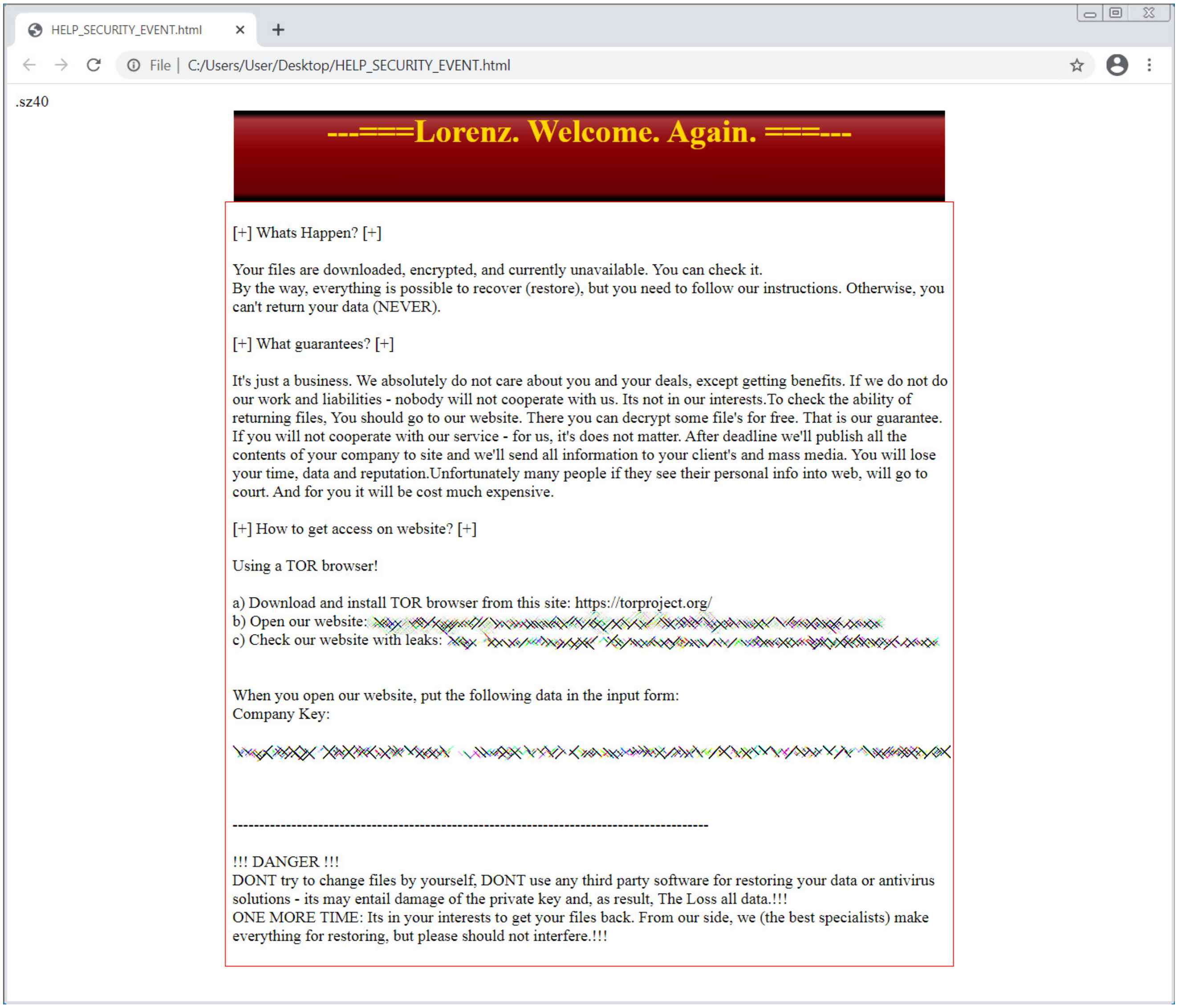
For example, a file named 1.doc would be encrypted and renamed to 1.doc.Lorenz.sz40, as shown in the image of an encrypted folder below.



Lorenz encrypted files

Unlike other enterprise-targeting ransomware, the Lorenz sample we looked at did not kill processes or shut down Windows services before encrypting.

Each folder on the computer will be a ransom note named **HELP_SECURITY_EVENT.html** that contains information about what happened to a victim's files. It will also include a link to the Lorenz data leak site and a link to a unique Tor payment site where the victim can see their ransom demand.



.sz40

---===Lorenz. Welcome. Again. ===---

[+] Whats Happen? [+]

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 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. Its not in our interests.To check the ability of returning files, You should go to our website. There you can decrypt some file's for free. That is our guarantee. If you will not cooperate with our service - for us, it's does not matter. After deadline we'll publish all the contents of your company to site and we'll send all information to your client's and mass media. You will lose your time, data and reputation.Unfortunately many people if they see their personal info into web, will go to court. And for you it will be cost much expensive.

[+] How to get access on website? [+]

Using a TOR browser!

a) Download and install TOR browser from this site: https://torproject.org/
b) Open our website: [redacted]
c) Check our website with leaks: [redacted]

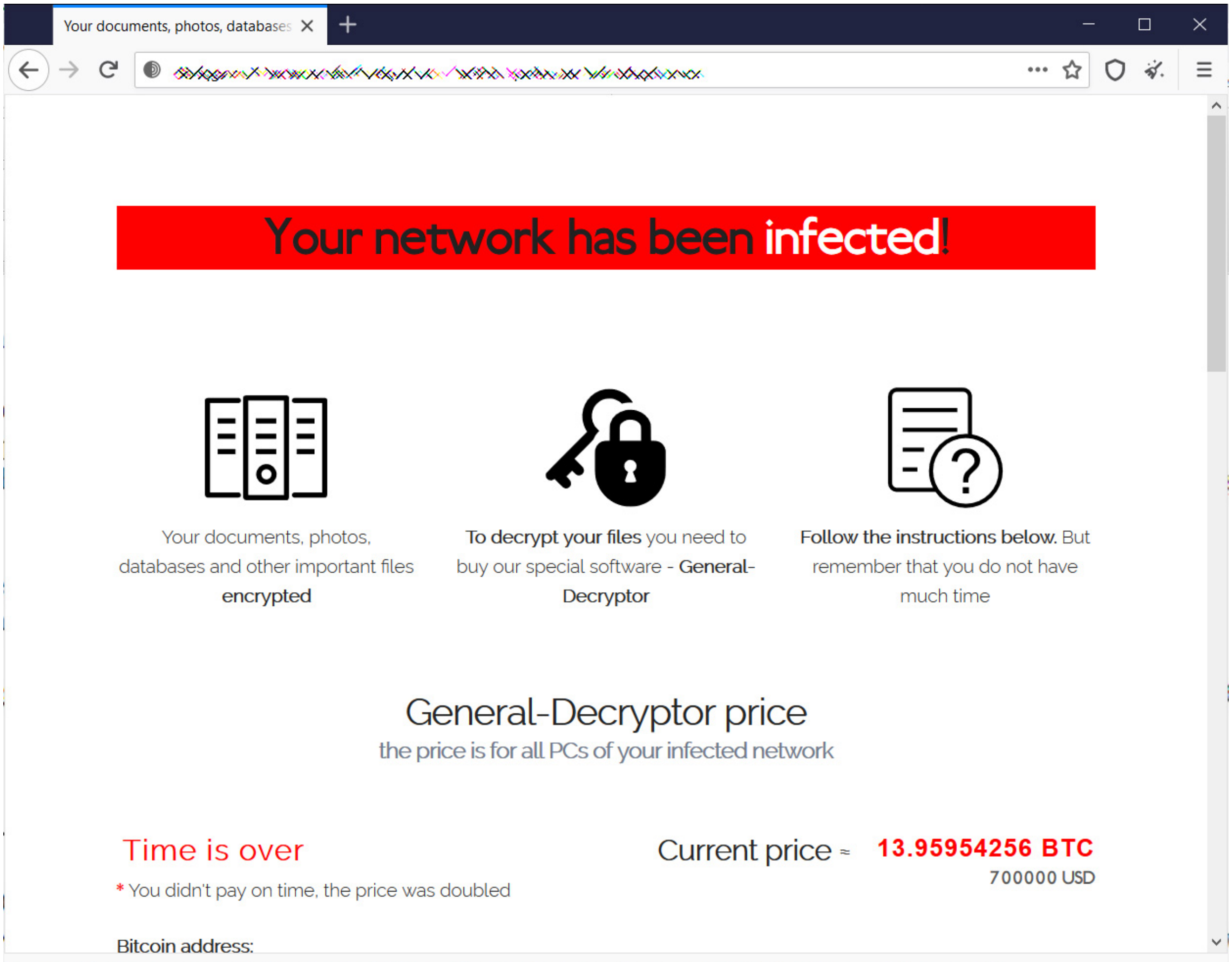
When you open our website, put the following data in the input form:
Company Key:

[redacted]

!!! DANGER !!!
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.!!!

Lorenz ransom note

Each victim has a dedicated Tor payment site that includes the ransom demand in Bitcoin and a chat form that victims can negotiate with the attackers.



Your network has been infected!

Your documents, photos, databases and other important files **encrypted**

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

Follow the instructions below. But remember that you do not have much time

General-Decryptor price

the price is for all PCs of your infected network

Time is over

* You didn't pay on time, the price was doubled

Current price ≈ **13.95954256 BTC**

700000 USD

Bitcoin address:

Lorenz Tor payment page

From ransom notes seen by BleepingComputer, Lorenz ransom demands range from $500,000 to $700,000. Earlier versions of the ransomware included million-dollar ransom demands, but it is unclear if those were affiliated with the same operation.

The ransomware is currently being analyzed for weaknesses, and BleepingComputer does not advise victims to pay the ransom until its determined if a free decryptor can recover files for free.

Related Articles:

Industrial Spy data extortion market gets into the ransomware game

Quantum ransomware seen deployed in rapid network attacks

Snap-on discloses data breach claimed by Conti ransomware gang

Shutterfly discloses data breach after Conti ransomware attack

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.