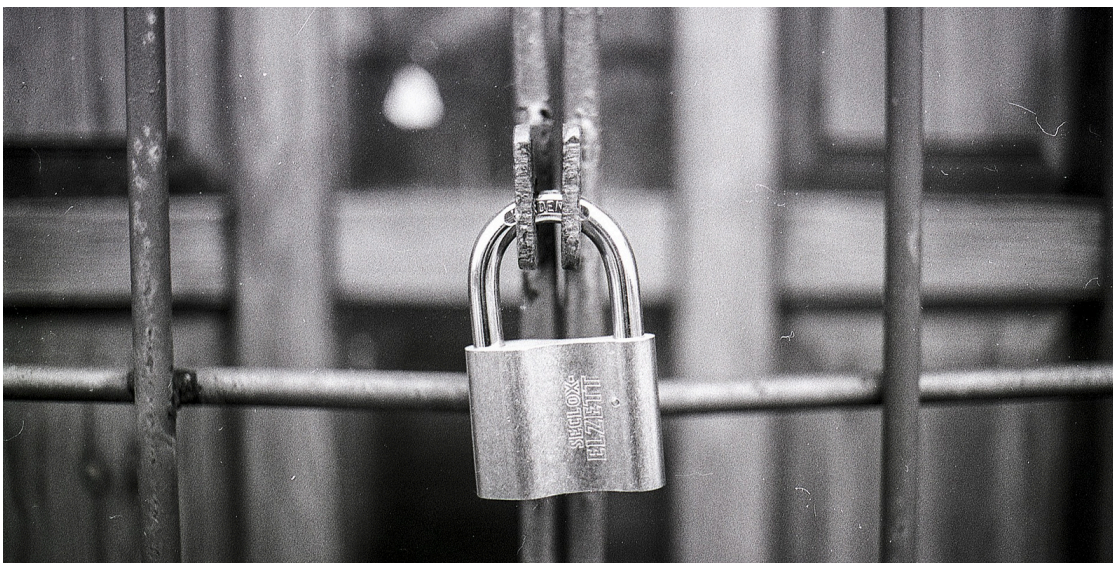


Meet Lorenz — A new ransomware gang targeting the enterprise

By Lawrence Abrams

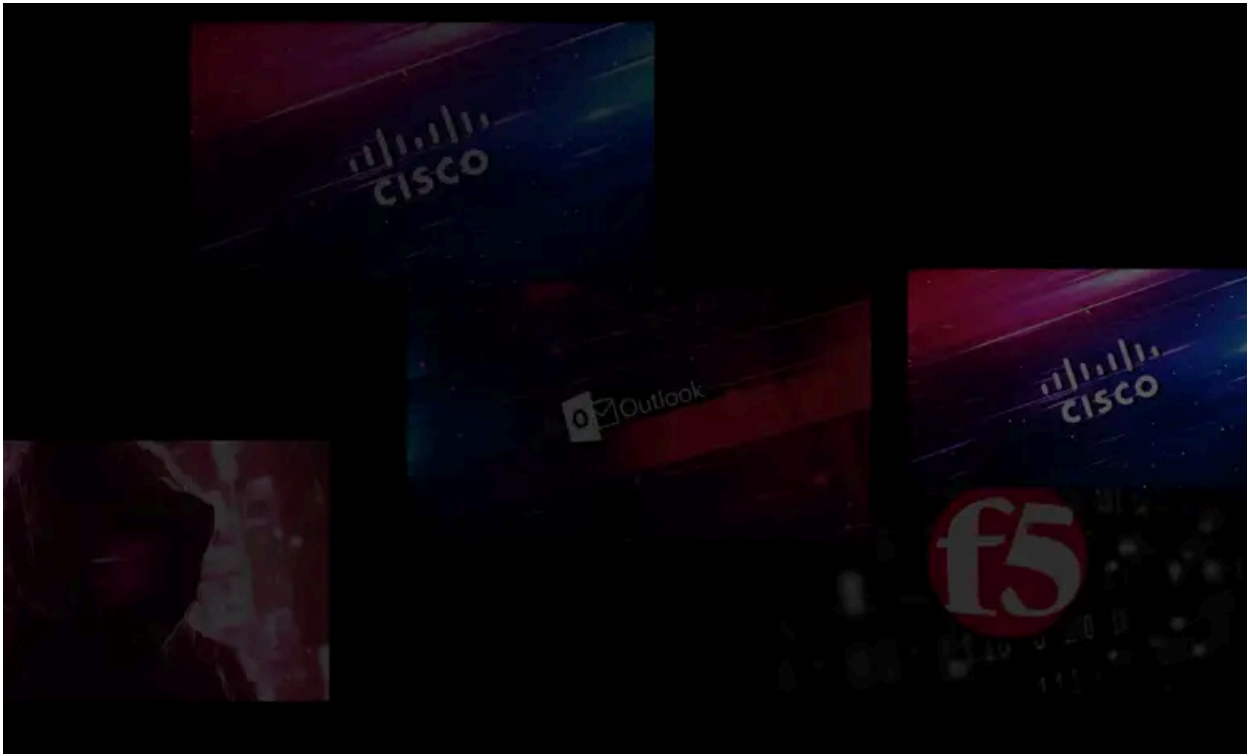
Published: 2021-05-13 · Archived: 2026-04-02 12:23:35 UTC



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.



Visit Advertiser website [GO TO PAGE](#)

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

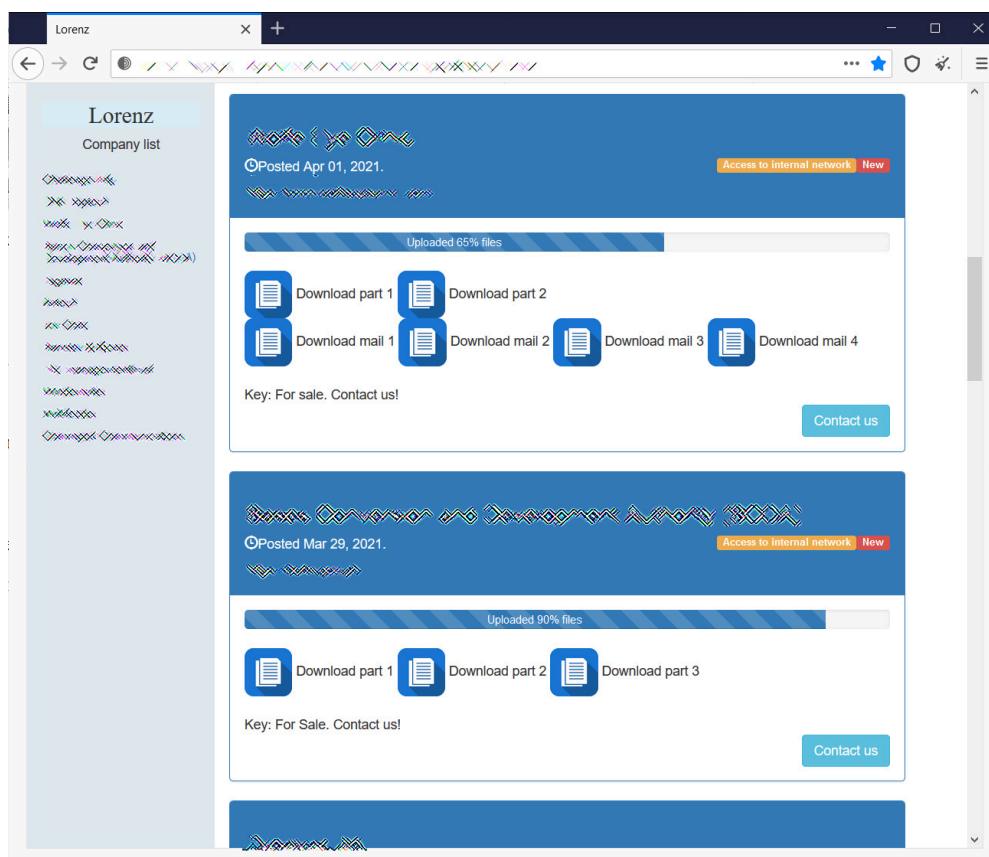
Data leak site launched to extort victims

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 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.



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

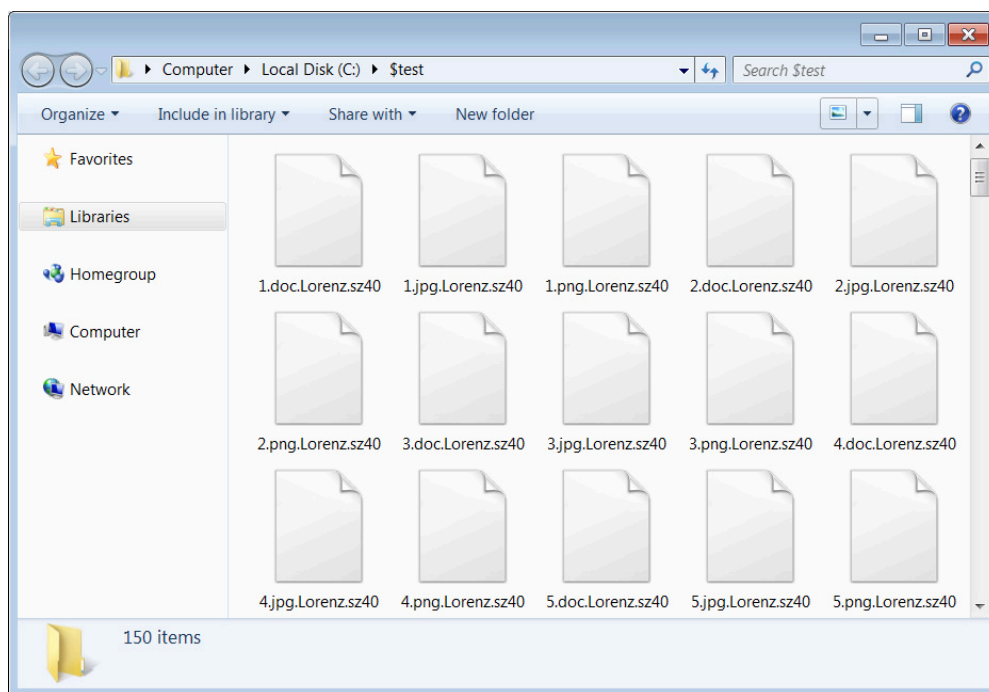
From samples of the Lorenz ransomware seen by BleepingComputer, the threat actors customize the malware executable for the specific organization they are targeting.

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
```

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.

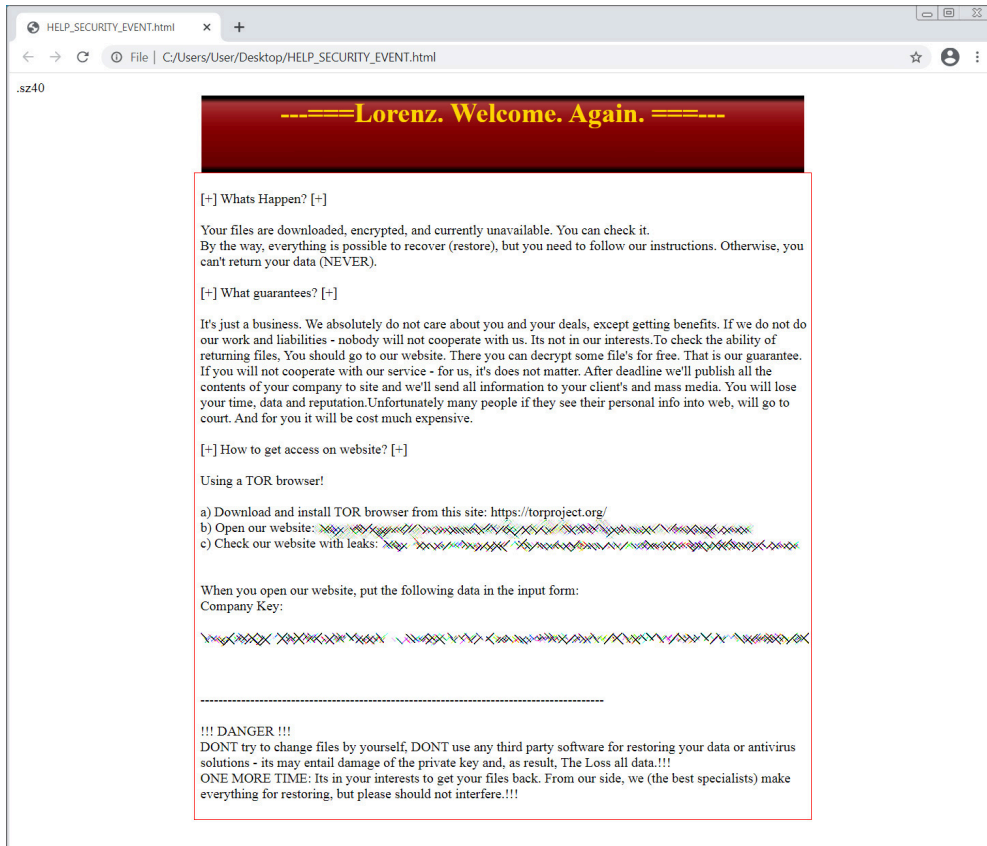
For example, a file named 1.doc would be encrypted and renamed to 1.doc.Lorenz.sz40, as shown in the image of an encrypted folder below.



Lorenz encrypted files

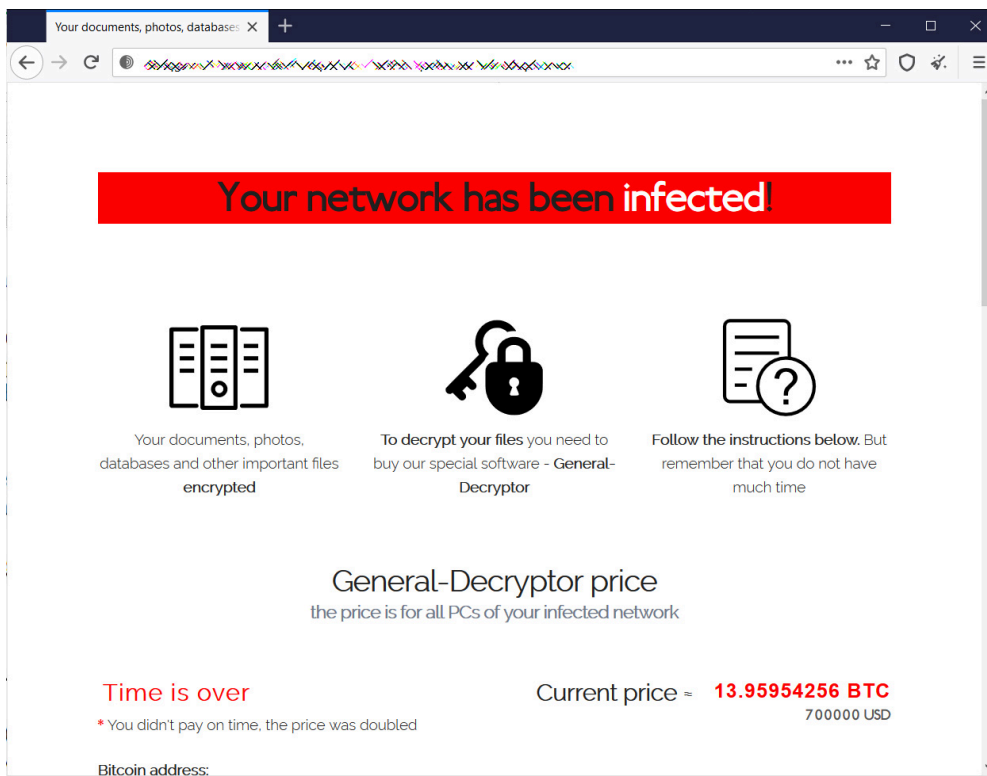
Unlike other enterprise-targeting ransomware, the Lorenz sample we looked at did not kill processes or shut down Windows services before encrypting.

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.



Lorenz ransom note

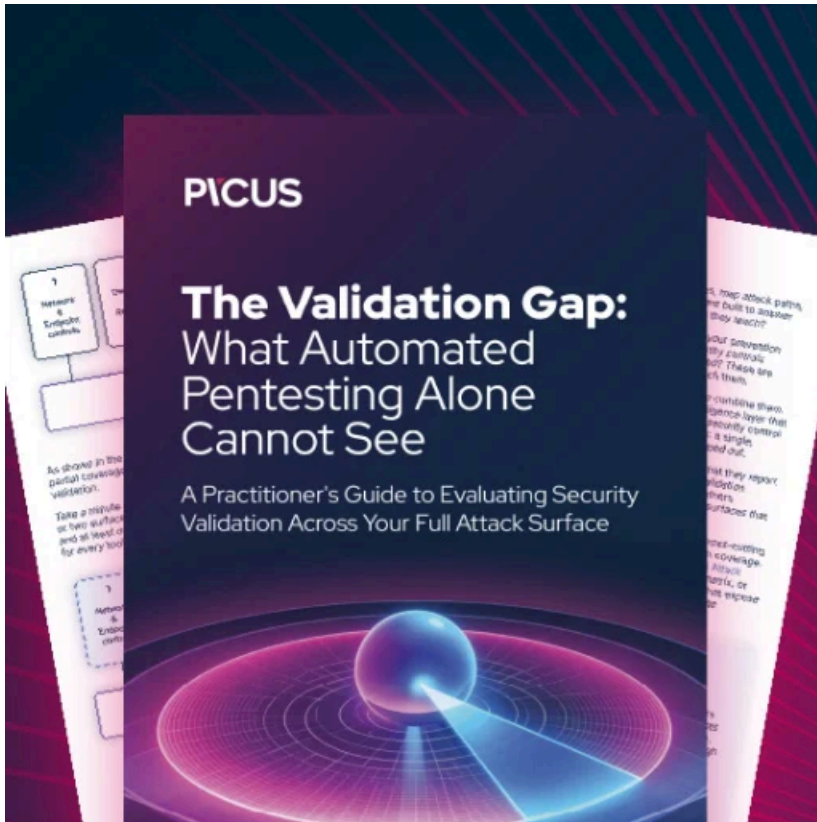
Each victim has a dedicated Tor payment site that includes the ransom demand in Bitcoin and a chat form that victims can negotiate with the attackers.



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.



[Automated Pentesting Covers Only 1 of 6 Surfaces.](#)

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: <https://www.bleepingcomputer.com/news/security/meet-lorenz-a-new-ransomware-gang-targeting-the-enterprise/>