Chaos Ransomware: A Proof of Concept With Potentially Dangerous Applications

trendmicro.com/en_us/research/21/h/chaos-ransomware-a-dangerous-proof-of-concept.html

August 10, 2021

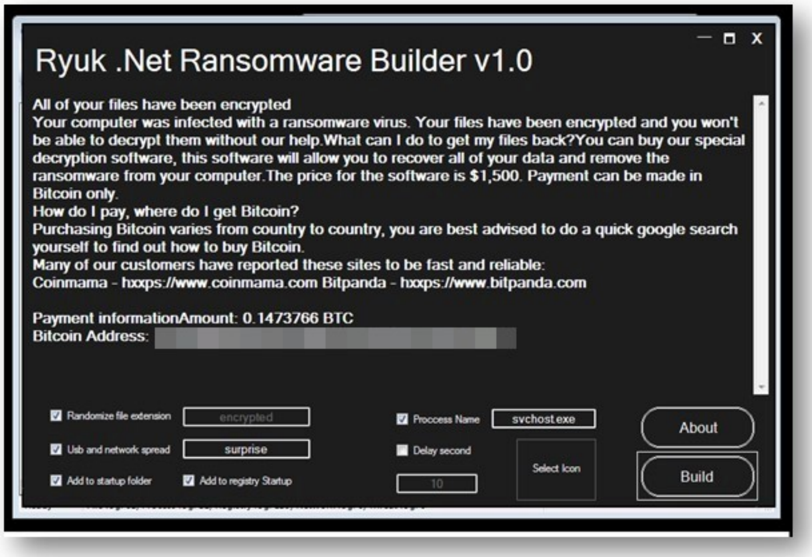
Since June 2021, we've been monitoring an in-development ransomware builder called Chaos, which is being offered for testing on an underground forum. While it's purportedly a .NET version of Ryuk, closer examination of the sample reveals that it doesn't share much with the notorious ransomware. In fact, early versions of Chaos, which is now in its fourth iteration, were more akin to a destructive trojan than to traditional ransomware.

In this blog entry, we take a look at some of the characteristics of the Chaos ransomware builder and how its iterations added new capabilities.

Evolution of the Chaos ransomware builder

Chaos has undergone rapid evolution from its very first version to its current iteration, with version 1.0 having been released on June 9, version 2.0 on June 17, version 3.0 on July 5, and version 4.0 on Aug. 5.

Version 1.0



Ryuk .Net Ransomware Builder v1.0

All of your files have been encrypted
Your computer was infected with a ransomware virus. Your files have been encrypted and you won't be able to decrypt them without our help.What can I do to get my files back?You can buy our special decryption software, this software will allow you to recover all of your data and remove the ransomware from your computer.The price for the software is $1,500. Payment can be made in Bitcoin only.
How do I pay, where do I get Bitcoin?
Purchasing Bitcoin varies from country to country, you are best advised to do a quick google search yourself to find out how to buy Bitcoin.
Many of our customers have reported these sites to be fast and reliable:
Coinmama - hxxps://www.coinmama.com Bitpanda - hxxps://www.bitpanda.com

Payment informationAmount: 0.1473766 BTC
Bitcoin Address: [redacted]

☑ Randomize file extension: encrypted
☑ Usb and network spread: surprise
☑ Add to startup folder
☑ Add to registry Startup
☑ Proccess Name: svchost.exe
□ Delay second: 10

Figure 1. The GUI of Chaos version 1.0

The most notable characteristic of the first version of the Chaos builder was that, despite having the Ryuk branding in its GUI, it had little in common with the ransomware. In fact, it wasn't even traditional ransomware, but rather a destructive trojan. Instead of encrypting files (which could then be decrypted after the target paid the ransom), it replaced the files' contents with random bytes, after which the files were encoded in Base64. This meant that affected files could no longer be restored, providing victims no incentive to pay the ransom.

It did, however, display certain characteristics found in other ransomware families. For example, it searched the following file paths and extensions to infect:

Directories

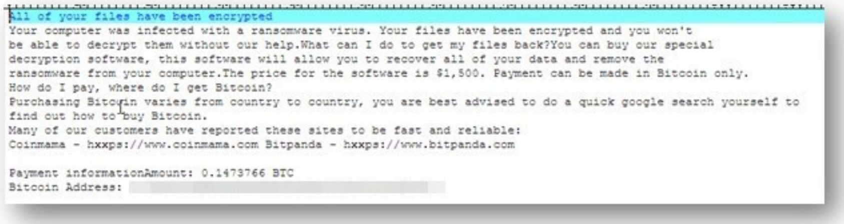
- \\Contacts
- \\Desktop
- \\Desktop
- \\Documents
- \\Downloads
- \\Favorites
- \\Links
- \\Music
- \\OneDrive
- \\Pictures
- \\Saved Games
- \\Searches
- \\Videos

File extensions

- .3gp
- .7z
- .7-zip
- .accdb
- .ace
- .amv
- .apk
- .arj
- .asp
- .aspx
- .avi
- .backup
- .bak
- .bay
- .bk
- .blob
- .bmp
- .bz2
- .cab
- .cer
- .contact
- .core
- .cpp
- .crt
- .cs
- .css
- .csv
- .dat
- .db
- .dll
- .doc
- .docm
- .docx
- .dwg
- .exif
- .flv
- .gzip
- .htm
- .html
- .ibank
- .ico
- .ini
- .iso
- .jar
- .java
- .jpe
- .jpeg
- .jpg
- .js
- .json
- .jsp
- .lnk
- .lzh
- .m4a
- .m4p
- .m4v
- .mdb
- .mkv
- .mov
- .mp3
- .mp3
- .mp3
- .mp4
- .mpeg

- .mpg
- .ods
- .odt
- .p7c
- .pas
- .pdb
- .pdf
- .php
- .png
- .ppt
- .pptx
- .psd
- .py
- .rar
- .rb
- .rtf
- .settings
- .sie
- .sql
- .sum
- .svg
- .tar
- .txt
- .vdi
- .vmdk
- .wallet
- .wav
- .webm
- .wma
- .wmv
- .wps
- .xls
- .xlsb
- .xlsm
- .xlsx
- .xml
- .xz
- .zip

It then dropped a ransomware note named *read_it.txt*, with a demand for a rather sizeable ransom in bitcoin.

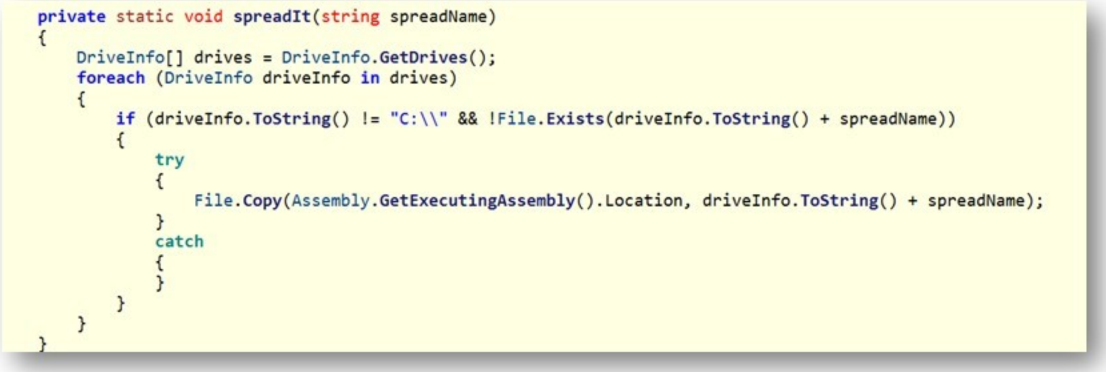


```
All of your files have been encrypted
Your computer was infected with a ransomware virus. Your files have been encrypted and you won't
be able to decrypt them without our help.What can I do to get my files back?You can buy our special
decryption software, this software will allow you to recover all of your data and remove the
ransomware from your computer.The price for the software is $1,500. Payment can be made in Bitcoin only.
How do I pay, where do I get Bitcoin?
Purchasing Bitcoin varies from country to country, you are best advised to do a quick google search yourself to
find out how to buy Bitcoin.
Many of our customers have reported these sites to be fast and reliable:
Coinmama - hxxps://www.coinmama.com Bitpanda - hxxps://www.bitpanda.com

Payment informationAmount: 0.1473766 BTC
Bitcoin Address: [redacted]
```

Figure 2. A ransom note dropped by Chaos

One of the more interesting functions of Chaos version 1.0 was its worming function, which allowed it to spread to all drives found on an affected system. This could permit the malware to jump onto removable drives and escape from air-gapped systems.



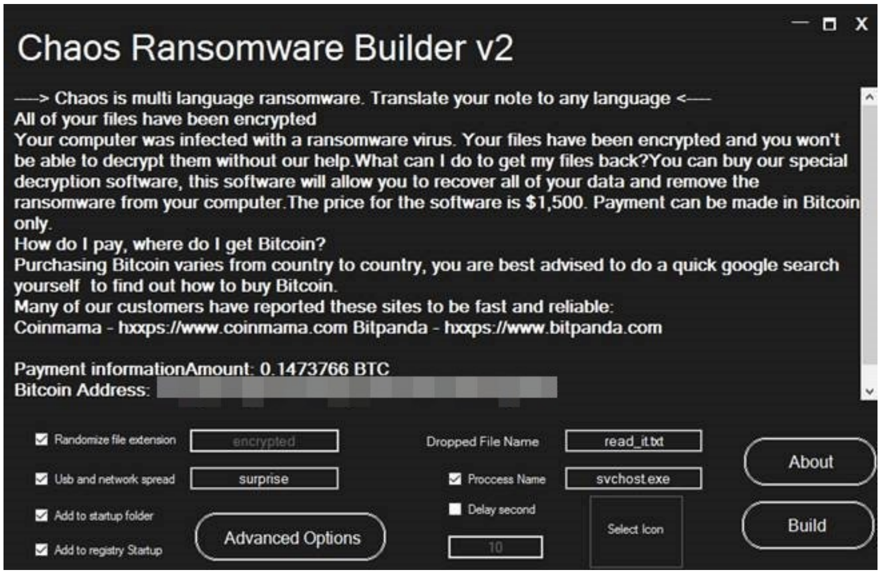
```
private static void spreadIt(string spreadName)
{
    DriveInfo[] drives = DriveInfo.GetDrives();
    foreach (DriveInfo driveInfo in drives)
    {
        if (driveInfo.ToString() != "C:\\" && !File.Exists(driveInfo.ToString() + spreadName))
        {
            try
            {
                File.Copy(Assembly.GetExecutingAssembly().Location, driveInfo.ToString() + spreadName);
            }
            catch
            {
            }
        }
    }
}
```

Figure 3. Code showing the worming function

Version 2.0

The second version of Chaos added advanced options for administrator privileges, the ability to delete all volume shadow copies and the backup catalog, and the ability to disable Windows recovery mode.

However, version 2.0 still overwrote the files of its targets. Members of the forum where it was posted pointed out that victims wouldn't pay the ransom if their files couldn't be restored.



Chaos Ransomware Builder v2

—-> Chaos is multi language ransomware. Translate your note to any language <—-
All of your files have been encrypted
Your computer was infected with a ransomware virus. Your files have been encrypted and you won't be able to decrypt them without our help.What can I do to get my files back?You can buy our special decryption software, this software will allow you to recover all of your data and remove the ransomware from your computer.The price for the software is $1,500. Payment can be made in Bitcoin only.
How do I pay, where do I get Bitcoin?
Purchasing Bitcoin varies from country to country, you are best advised to do a quick google search yourself to find out how to buy Bitcoin.
Many of our customers have reported these sites to be fast and reliable:
Coinmama - hxxps://www.coinmama.com Bitpanda - hxxps://www.bitpanda.com

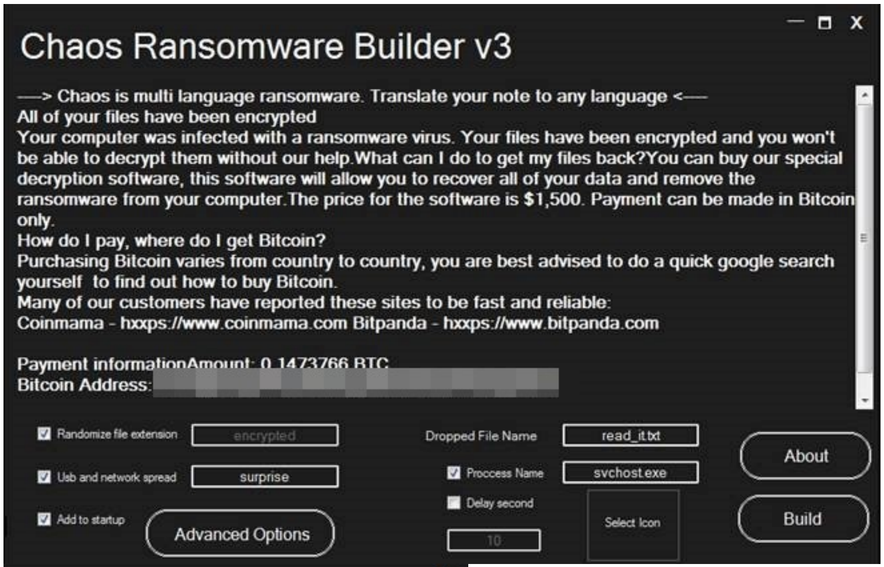
Payment informationAmount: 0.1473766 BTC
Bitcoin Address: [redacted]

☑ Randomize file extension: encrypted
☑ Usb and network spread: surprise
☑ Add to startup folder
☑ Add to registry Startup
Dropped File Name: read_it.txt
☑ Proccess Name: svchost.exe
☐ Delay second: 10

Figure 4. The GUI of Chaos version 2.0

Version 3.0

With version 3.0, the Chaos ransomware builder gained the ability to encrypt files under 1 MB using AES/RSA encryption, making it more in line with traditional ransomware. It also came with its own decrypter builder.



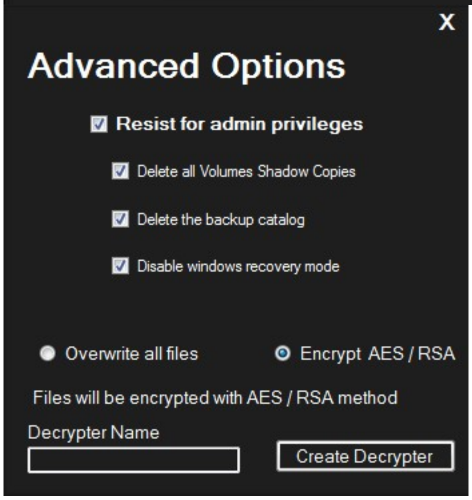
Chaos Ransomware Builder v3

—-> Chaos is multi language ransomware. Translate your note to any language <—-
All of your files have been encrypted
Your computer was infected with a ransomware virus. Your files have been encrypted and you won't be able to decrypt them without our help.What can I do to get my files back?You can buy our special decryption software, this software will allow you to recover all of your data and remove the ransomware from your computer.The price for the software is $1,500. Payment can be made in Bitcoin only.
How do I pay, where do I get Bitcoin?
Purchasing Bitcoin varies from country to country, you are best advised to do a quick google search yourself to find out how to buy Bitcoin.
Many of our customers have reported these sites to be fast and reliable:
Coinmama - hxxps://www.coinmama.com Bitpanda - hxxps://www.bitpanda.com

Payment informationAmount: 0.1473766 BTC
Bitcoin Address: [redacted]

☑ Randomize file extension: encrypted
☑ Usb and network spread: surprise
☑ Add to startup
Dropped File Name: read_it.txt
☑ Proccess Name: svchost.exe
□ Delay second: 10

Figure 5. The GUI of Chaos version 3.0



Advanced Options

☑ Resist for admin privileges

☑ Delete all Volumes Shadow Copies

☑ Delete the backup catalog

☑ Disable windows recovery mode

○ Overwrite all files ● Encrypt AES / RSA

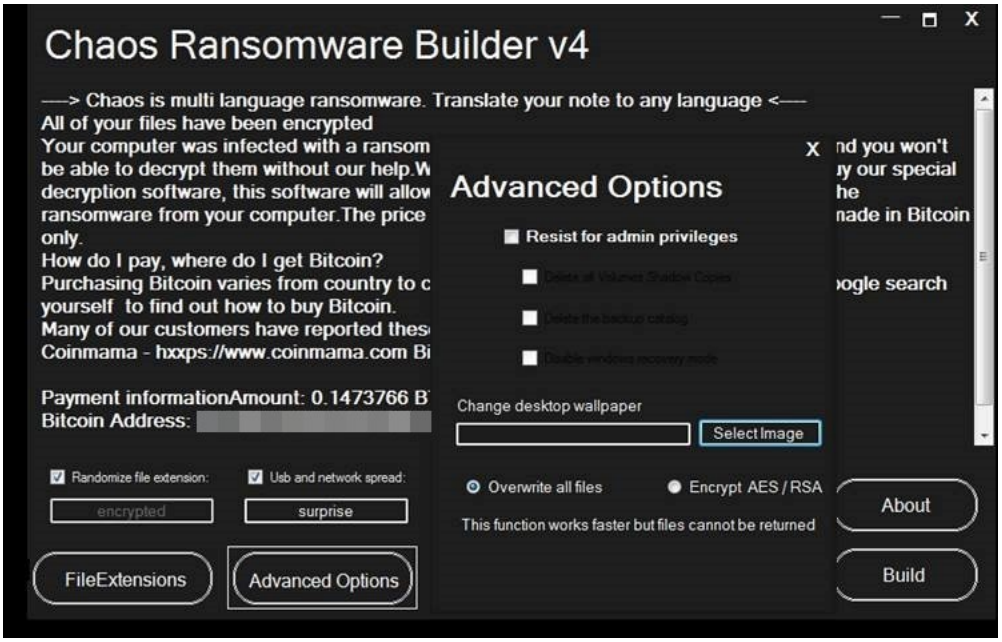
Files will be encrypted with AES / RSA method

Decrypter Name

Figure 6. The advanced options for Chaos version 3.0, including the option to encrypt files via the AES/RSA method and the decrypter builder function

Version 4.0

The fourth iteration of Chaos expands the AES/RSA encryption by increasing the upper limit of files that can be encrypted to 2 MB. In addition, it gives the ransomware builder’s users the ability to add their own extensions to affected files and the ability to change the desktop wallpaper of their victims.



Chaos Ransomware Builder v4

—> Chaos is multi language ransomware. Translate your note to any language <—
All of your files have been encrypted
Your computer was infected with a ransom … nd you won't
be able to decrypt them without our help.W … ıy our special
decryption software, this software will allow … he
ransomware from your computer.The price … nade in Bitcoin
only.
How do I pay, where do I get Bitcoin?
Purchasing Bitcoin varies from country to c … ɔogle search
yourself to find out how to buy Bitcoin.
Many of our customers have reported thes
Coinmama - hxxps://www.coinmama.com Bi

Payment informationAmount: 0.1473766 B
Bitcoin Address: [redacted]

☑ Randomize file extension: encrypted

☑ Usb and network spread: surprise

Advanced Options

□ Resist for admin privileges

□ Delete all Volumes Shadow Copies

□ Delete the backup catalog

□ Disable windows recovery mode

Change desktop wallpaper

● Overwrite all files ○ Encrypt AES / RSA

This function works faster but files cannot be returned

Figure 7. The advanced options for Chaos version 4.0, including the option to change desktop wallpapers

A proof of concept that could be dangerous in the wrong hands

We haven't seen any active infections or victims of the Chaos ransomware. However, in the hands of a malicious actor who has access to malware distribution and deployment infrastructure, it could cause great damage to organizations.

In our view, the Chaos ransomware builder is still far from being a finished product since it lacks features that many modern ransomware families possess, such as the ability to collect data from victims that could be used for further blackmail if the ransom is not paid.

Indicators of compromise

The following are the hashes and our detections for the different Chaos ransomware builder versions:

SHA-256	Detection	TrendX detection
0d8b4a07e91e02335f600332644e8f0e504f75ab19899a58b2c85ecb0887c738	Trojan.MSIL.FAKERYUKBUILD.THFAFBA	N/A
325dfac6172cd279715ca8deb280eefe3544090f1583a2ddb5d43fc7fe3029ed	Trojan.MSIL.FAKERYUKBUILDER.AA	Ransom.Win32.TR
63e28fc93b5843002279fc2ad6fabd9a2bc7f5d2f0b59910bcc447a21673e6c7	Trojan.MSIL.FAKERYUKBUILDER.AA	Ransom.Win32.TR
f2665f89ba53abd3deb81988c0d5194992214053e77fc89b98b64a31a7504d77	Trojan.MSIL.FAKERYUKBUILD.THFAFBA	N/A

We also proactively detect the following components:

Detection	Note
Ransom.MSIL.CHAOSBUILDER.SMYPBHET	Chaos ransomware builder and decrypter

Ransom.MSIL.CHAOS.SMYPBHET	Main Chaos ransomware executable
PUA.MSIL.CHAOS.SMYPBHET.decryptor	Chaos ransomware decrypter

Ransomware

Since June 2021, we’ve been monitoring an in-development ransomware builder called Chaos, which is being offered for testing on an underground forum.

By: Monte de Jesus, Don Ovid Ladores August 10, 2021 Read time: (words)

Content added to Folio