Roblox Game Pass store used to sell ransomware decryptor

bleepingcomputer.com/news/security/roblox-game-pass-store-used-to-sell-ransomware-decryptor/

Lawrence Abrams

By
Lawrence Abrams

- June 9, 2022
- 03:29 PM
- 0

A new ransomware is taking the unusual approach of selling its decryptor on the Roblox gaming platform using the service's in-game Robux currency.

Roblox is an online kids gaming platform where members can create their own games and monetize them by selling Game Passes, which provide in-game items, special access, or enhanced features.

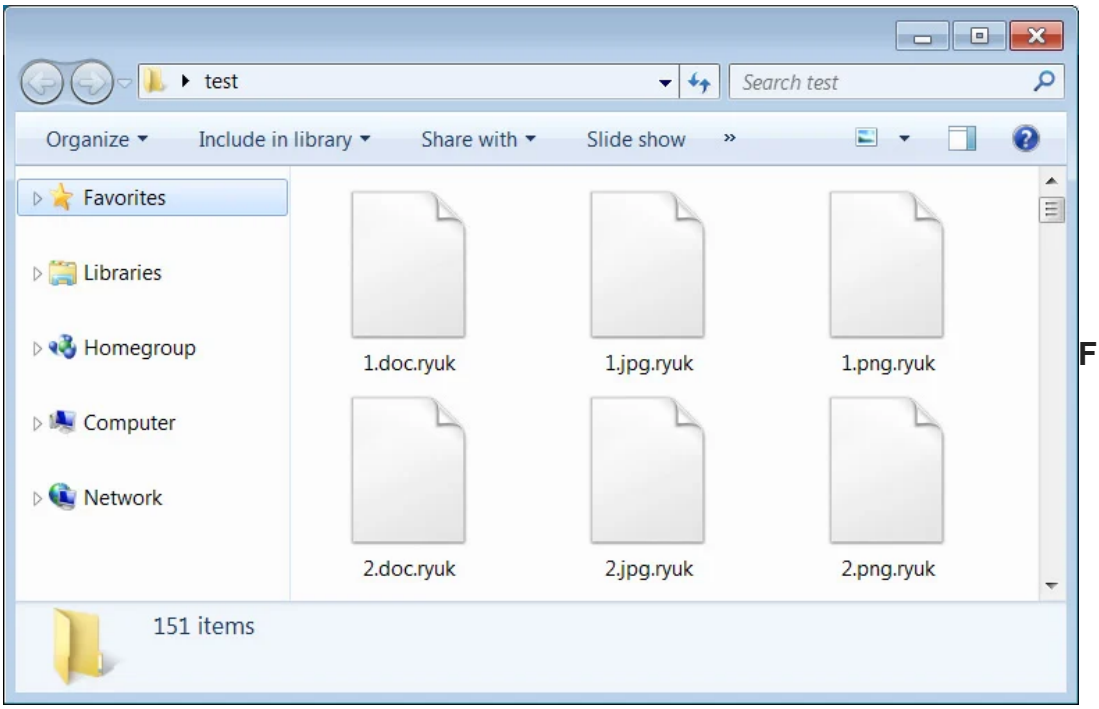
To pay for these Game Passes, members must purchase them using an in-game currency called Robux.

Selling decryptors on Roblox

Today, security researcher MalwareHunterTeam found a new ransomware named 'WannaFriendMe' that impersonates the notorious Ryuk Ransomware. However, in reality, it is a variant of the Chaos Ransomware.

In June 2021, a threat actor began selling a Chaos ransomware builder that allowed wannabe criminals to create their very own ransomware infection with customized ransom notes, encrypted file extensions, and other features.

By default, the Chaos builder pretends to be Ryuk, using the **.ryuk** extension for encrypted files, as shown below.



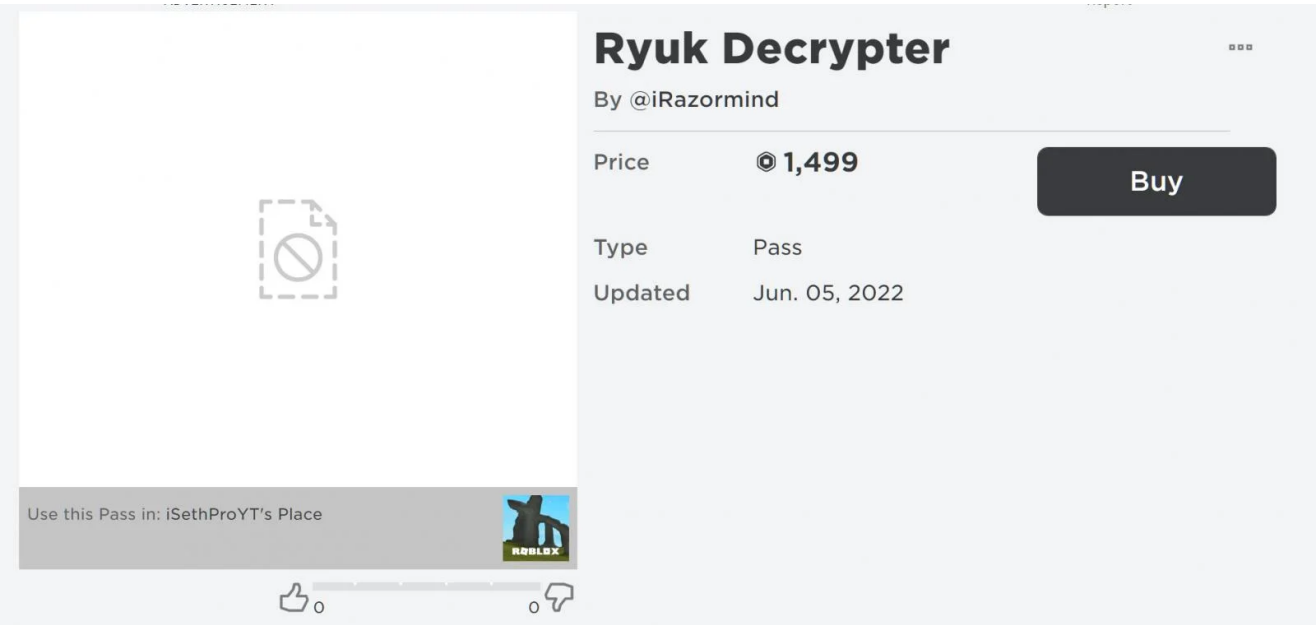
Files encrypted by the Chaos ransomware variant

Source: BleepingComputer

What makes the new WannaFriendMe ransomware stand out is that instead of demanding cryptocurrency as a ransom payment, it requires victims to purchase a decryptor from Roblox's Game Pass store using Robux, as can be read in the ransom note below:

> ----- YOUR FILES HAVE BEEN ENCRYPTED! -----
>
> Don't panic, your files are decryptable, But your files can only be decrypted with our own decrypter tool! To get this decrypter, you must buy this gamepass: https://www.roblox.com/game-pass/49955147/Ryuk-Decrypter
>
> YOU MUST HAVE A ROBLOX ACCOUNT TO BUY THE GAMEPASS, BUY 1700 ROBUX AND THEN BUY THE GAMEPASS ABOVE.
>
> AFTER BUYING THE GAMEPASS, CONTACT xxx@icloud.com WITH YOUR USERNAME AND SCREENSHOT OF YOU OWNING THE GAMEPASS. DO NOT DELETE THE GAMEPASS OTHERWISE YOU WILL DISOWN THE GAMEPASS.

When visiting the URL to the Roblox Game Pass store, you can see that the 'Ryuk Decrypter' is being sold by a user named 'iRazormind' for 1,499 Robux and was last updated on June 5th.



Decryptor sold as a Roblox Game Pass

Source: BleepingComputer

The problem with Chaos ransomware variants is that they not only encrypt your data but also destroy it in many cases.

While encrypting a device, any file greater than 2MB in size will be overwritten with random data and not encrypted. This means that even if you purchase a decryptor, only files smaller than 2MB can be recovered.

```
string extension = Path.GetExtension(files[i]);
string fileName = Path.GetFileName(files[i]);
if (Array.Exists<string>(Program.validExtensions, (string E) => E == extension.ToLower()) && fileName != Program.droppedMessageTextbox)
{
    FileInfo fileInfo = new FileInfo(files[i]);
    fileInfo.Attributes = FileAttributes.Normal;
    if (fileInfo.Length < 2117152L)
    {
        if (Program.encryptionAesRsa)
        {
            Program.EncryptFile(files[i]);
        }
    }
    else if (fileInfo.Length > 200000000L)
    {
        Random random = new Random();
        int length = random.Next(200000000, 300000000);
        string @string = Encoding.UTF8.GetString(Program.random_bytes(length));
        File.WriteAllText(files[i], Program.randomEncode(@string));
        File.Move(files[i], files[i] + "." + Program.RandomStringForExtension(4));
    }
    else
    {
        string string2 = Encoding.UTF8.GetString(Program.random_bytes(Convert.ToInt32(fileInfo.Length) / 4));
        File.WriteAllText(files[i], Program.randomEncode(string2));
        File.Move(files[i], files[i] + "." + Program.RandomStringForExtension(4));
    }
    if (flag)
    {
        flag = false;
        File.WriteAllLines(location + "/" + Program.droppedMessageTextbox, Program.messages);
    }
}
```

WannaFriendMe source code showing how it destroys files

Source: BleepingComputer

While it is unclear how this ransomware is distributed or if it has been used in attacks, its destructive nature and its targeting of young gamers could lead to significant damage.

This is not the first time Chaos ransomware variants have targeted gamers.

In October, threat actors targeted Japanese Minecraft players with 'alt lists' allegedly containing stolen Minecraft accounts but encrypted devices with the Chaos ransomware variant instead.

Related Articles:

Beware: Onyx ransomware destroys files instead of encrypting them

Free decryptor released for Yanluowang ransomware victims

Hello XD ransomware now drops a backdoor while encrypting

Confluence servers hacked to deploy AvosLocker, Cerber2021 ransomware

The Week in Ransomware - June 10th 2022 - Targeting Linux

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.