

Robin Hood Ransomware ‘GOODWILL’ Forces Victim for Charity

blogs.quickheal.com/a-new-ransomware-goodwill-hacks-the-victims-for-charity-read-more-to-know-more-about-this-ransomware-and-how-it-affects-its-victims/

June 13, 2022



Goodwill Ransomware, identified by CloudSEK researchers in March 2022, is known to promote social justice on the internet. It is known to encrypt documents, databases, videos, or photos after it infects the whole system. The files become inaccessible for the victims, where Robinhood’ Goodwill’ asks the victim to donate for socially driven activities to get their files back. For example: ‘Goodwill Ransomware forces victims to donate new clothes to the homeless, provide financial assistance to the poor, and many more. They then ask victims to post it online.

However, a few more ransomware have other motives to force victims to do some act to retrieve their infected files. Quick heal published a blog about Sarbloh Ransomware related to the Farmer Protests and was not demanding any ransom. Similarly, Goodwill ransomware acts as a Robin Hood and forces victims to help the poor. Let us look into more detail about this ransomware and how the attacker gets hold of the files in the system.

Technical Analysis

Let us analyse the hash (MD5: cea1cb418a313bdc8e67dbd6b9ea05ad). This is a .NET Compiled file. This executable is packed with Fody; hence we can see only the main routine. We can also observe references to Costura.

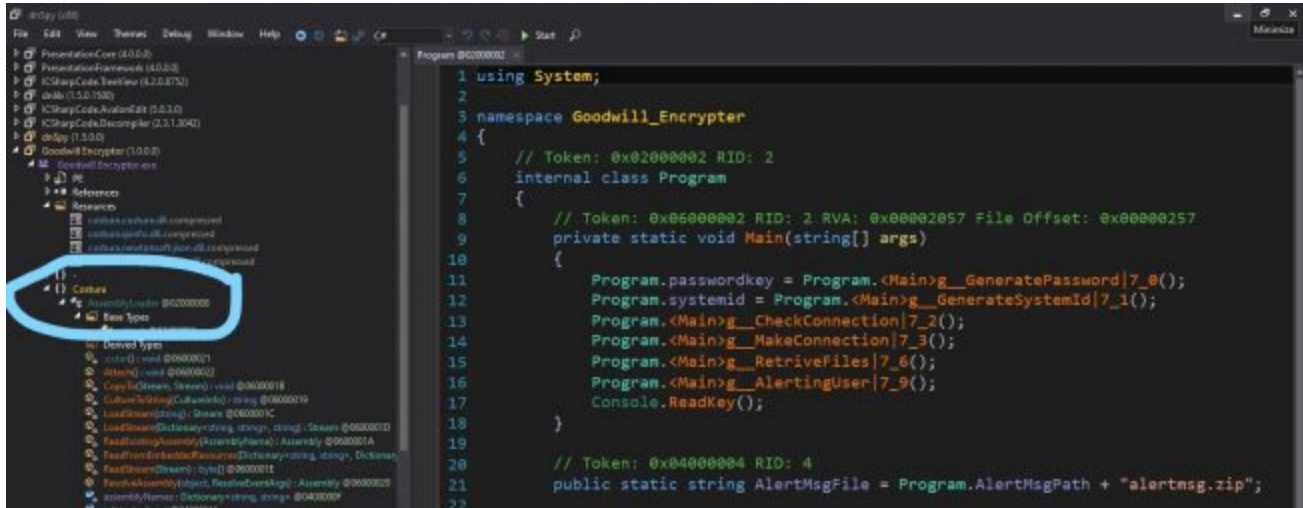


Fig 1: Costura References

This Costura is a plugin for Fody that allows the developers to embed all the dependencies in the form of resources packed inside the final dotNET executable.

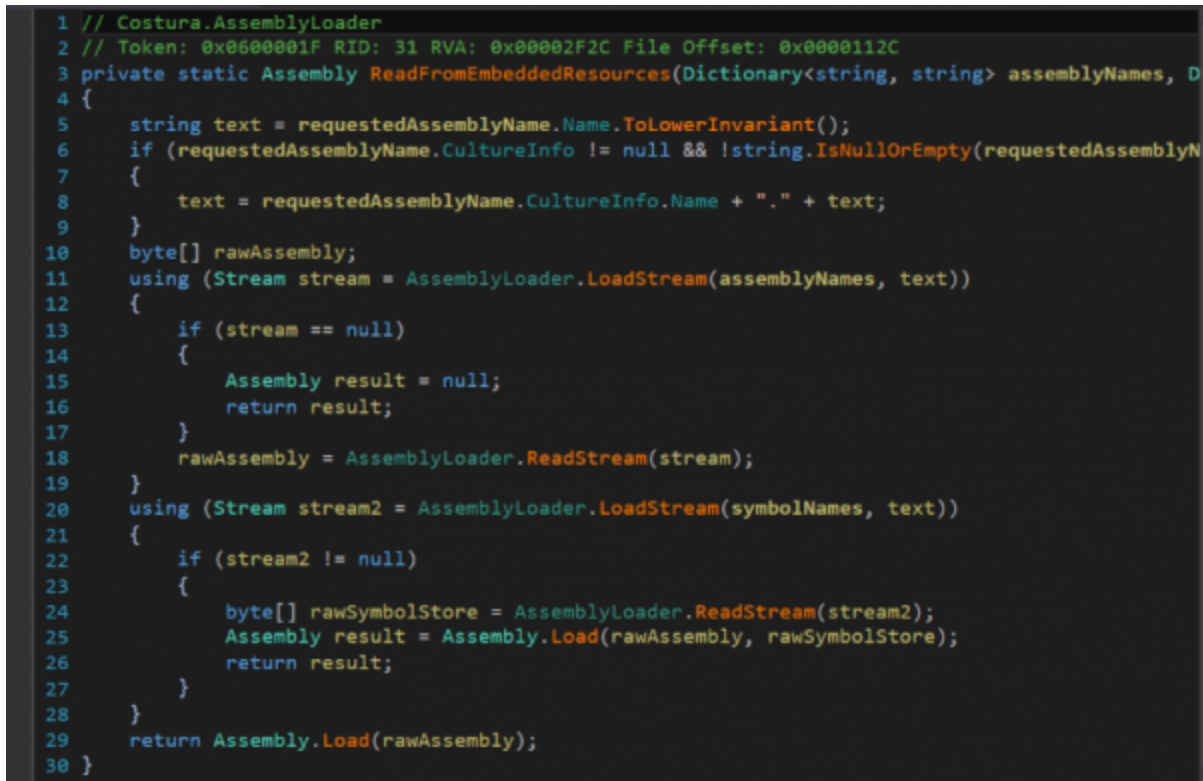


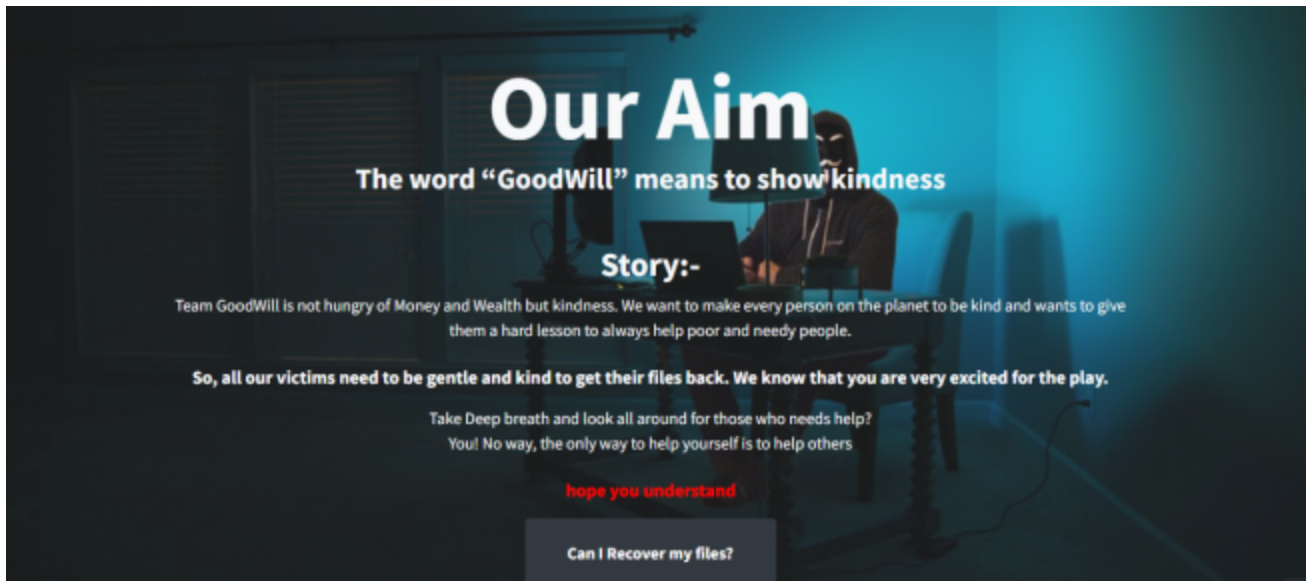
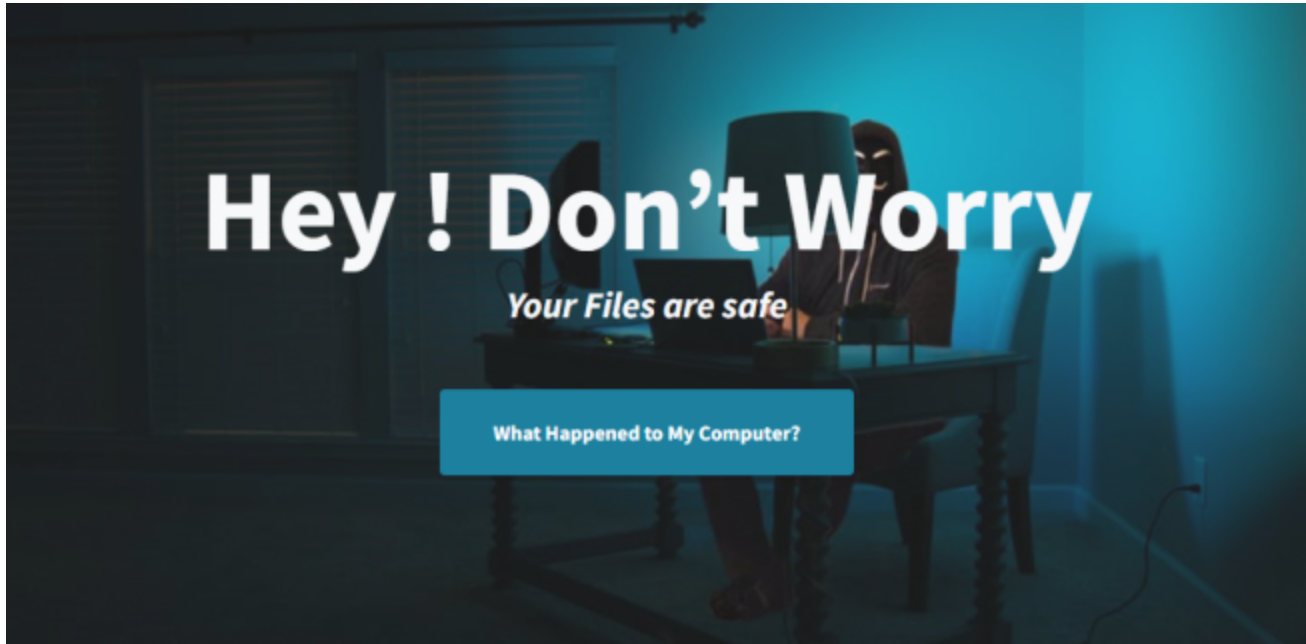
Fig2: Plugin

It can be seen in the above image how the embedded dependencies are fetched and unpacked.

Upon execution it connects to URL [http://hxxp\[://9855-13-235-50-147.ngrok\[.\]io/alertmsg\[.\]zip](http://hxxp[://9855-13-235-50-147.ngrok[.]io/alertmsg[.]zip) and downloads alertmsg.zip file into location: C:\Users\Public\WindowsUI

All the content related to Ransom notes and encryption information is in the zip file. This executable coordinates with the contents of the zip. It encrypts the files with the extension “.gdwill.”

To recover the files, 3 activities need to be performed as shown below:



Activity 1 = "GoodWill 1"

What to do?

That we all know Thousands of people die due to sleeping on the roadside in the cold because they do not have clothes to cover their body

So, your 1st task is to provide new clothes/blankets to needy people of road side and make a video of this event.

Later post this video/photo to your Facebook, Instagram and WhatsApp stories by using photo frame provided by us and encourage other people to help needy people in winters.

Take a screen shot of your post and send email to us with valid post link, later our team will verify the whole case and promotes you for the next activity.

It's Does not costs you high but matters for humanity.

Activity 2 = "GoodWill 2"

After completing the 1st activity you will be promoted for the Activity 2

Thousands of poor children have to sleep hungry in the long cold nights, because those ill-fated people have no luxury to have dinner every night in this cruel world.

You cannot feed them food for life, but you can give them 2 moments of happiness!

How!!

Hmm, Listen.

In the evening, pick any 5 poor children (under 13 years) of your neighborhood and take them to Dominos / Pizza Hut or KFC, then allow them to order the food they love to eat and try to make them feel happy. Treat those kids as your younger brothers.

Take some Selfies of them with full of smiles and happy faces,

Make a beautiful video story on this whole event and again post it on your Facebook and Instagram Stories with photo frame and caption provided by us.

Take a screen shot of your posts, snap of restaurant's bill and send email to us with valid post link, later our team will verify the whole case and promotes you for the next activity.

Help those less fortunate than you, for it is real human existence.

Activity 3 = "The Final GoodWill"

After completing the 1st and 2nd Activity we will promotes you for the Activity 3.

There are so many people in the world who have suffered the pain of losing their loved ones due to lack of money. Lack of money is the biggest misfortune to get medical treatment at the right time.

Hmm, what's your duty now!

Hmm, Listen again!

Visit the nearest hospital in your area and observe the crowd around you inside the hospital premises.

You will see that there will be some people who need certain amount of money urgently for their medical treatment, but they are unable to arrange due to any reason.

You have to go near them and talk to them that they have been supported by you and they do not need to worry now,

Finally Provide them maximum part of required amount.

Again, Take some Selfies of them with full of smiles and happy faces,

Record Audio while whole conversation between you and them and send it to us.

Write a beautiful article in your Facebook and Instagram by sharing your wonderful experience to other peoples that how you transform yourself into a kind human being by becoming Victim of a Ransomware called GoodWill.

Send us post link and later our team will verify the whole case and finally you will able to download the Complete Decryption Kit which includes The Main decryption tool, password file and the video tutorial to recover all your important files

Fig 3: Ransom note

After completing all the given activities, the details must be sent to the email in the below format:



Fig 4: Email Format

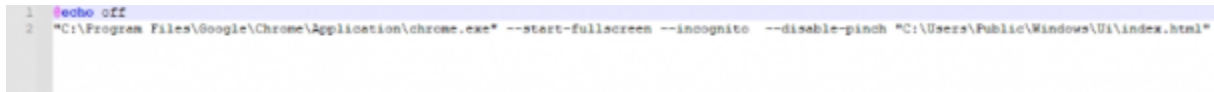
The ransomware attackers ask the victims to provide convincing evidence for the activities to prove it done. After which, the person orchestrating this threat will provide a decryption tool to recover the stolen files. Let us look at how the threat actors hack and encrypt the files via the given below snapshot.

```
Program @02000002
1 using System;
2
3 namespace Goodwill_Encrypter
4 {
5     // Token: 0x02000002 RID: 2
6     internal class Program
7     {
8         // Token: 0x06000002 RID: 2 RVA: 0x00002057 File Offset: 0x00002057
9         private static void Main(string[] args)
10        {
11            Program.passwordkey = Program.<Main>g__GeneratePassword|7_0();
12            Program.systemid = Program.<Main>g__GenerateSystemId|7_1();
13            Program.<Main>g__CheckConnection|7_2();
14            Program.<Main>g__MakeConnection|7_3();
15            Program.<Main>g__RetriveFiles|7_6();
16            Program.<Main>g__AlertingUser|7_9();
17            Console.ReadKey();
18        }
19
20        // Token: 0x04000004 RID: 4
21        public static string AlertMsgFile = Program.AlertMsgPath + "alertmsg.zip";
22
```

Fig 6: Encryption

Encryption Process

1. **GeneratePassword**: A password is randomly generated and then base64 encoded. The SHA256 of this base64 encoded data which later forms the key for encryption (AES)
2. **GenerateSystemId**: SystemID of the victim's machine is obtained
3. **CheckConnection**: Pings google.com and checks if the internet is working
4. **MakeConnection**: Uploads the password and SystemID to the server along with location and IP
5. **RetrieveFiles**: AES Encryption is done on files with extension with a key generated in Step1 .pptx,.docx,.xlsx,.txt,.pdf,.500,.jpeg,.jpg,.png
6. **AlertingUser**: Launches index.html(containing ransom note) via launch.bat present in the alertmsg.zip



```
1 echo off
2 "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-fullscreen --incognito --disable-pinch "C:\Users\Public\Windows\UI\index.html"
```

Fig 7: Batch file for alert

This malware also sleeps for a few seconds to bypass the analysis.

At last, it was found that this ransomware was derived from an Open-source Jasmin Encryptor, which can be found on <https://github.com/codesiddhant/Jasmin-Ransomware>.

How do we prevent such kinds of attacks?

To keep ourselves secure from such attacks, follow the great saying “Prevention is better than Cure”! The infection vector is usually in the form of mails, so do not open attachments from an untrusted sender. Do not enable macros in the Doc received mainly from correspondences. Avoid clicking on unverified links and those in spam emails. Keep your software and antivirus updated. Always remember to back up your data so that you can recover it even in case of a ransomware attack.

Conclusion

In the content above, we have looked into how Goodwill Ransom is related to Open-source Jasmin. It has modified the open-source for, e.g., In Jasmin, files are encrypted with the “.jasmin” extension, whereas GoodWill files are encrypted with “.gdwill.” In Jasmin, hosted points to localhost, whereas Goodwill points to external C2. This ransomware was unique because of its charitable nature instead of demanding money. The strings present in the file, such as “Error h bhaiyya,” seems that the routes of this hack were generated in India.

Indicators of compromise (IOC)

cea1cb418a313bdc8e67dbd6b9ea05ad

QuickHeal Protection

Trojan.YakbeexMSIL.ZZ4



Tejaswini Sandapolla

Follow @