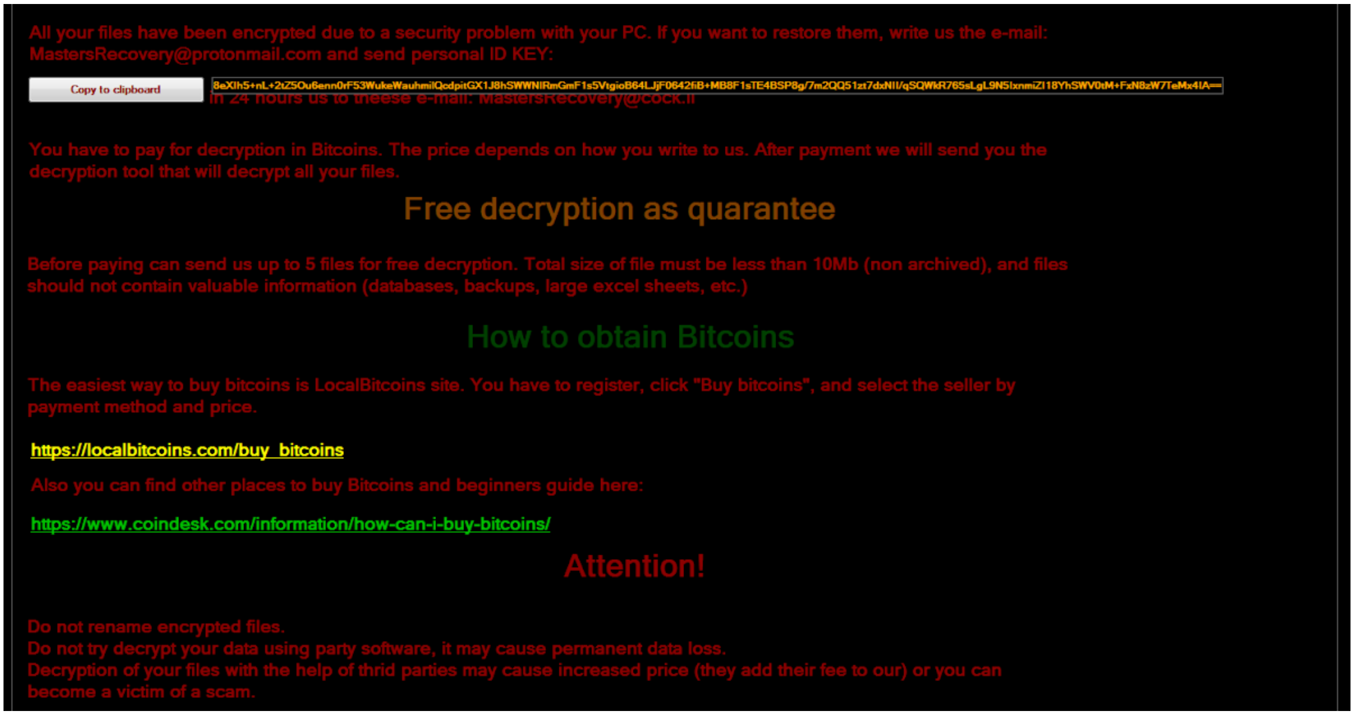
This is Spartacus: new ransomware on the block

bartblaze.blogspot.com/2018/04/this-is-spartacus-new-ransomware-on.html



All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us the e-mail: MastersRecovery@protonmail.com and send personal ID KEY:

8eXIh5+nL+2tZ5Ou6enn0rF53WukeWauhmilQcdpitGX1J8hSWWNIRmGmF1s5VtgioB64LJjF0642fiB+MB8F1sTE4BSP8g/7m2QQ51zt7dxNIl/qSQWkR765sLgL9N5IxnmiZI18YhSWV0tM+FxN8zW7TeMx4IA==

in 24 hours us to theese e-mail: MastersRecovery@cock.li

You have to pay for decryption in Bitcoins. The price depends on how you write to us. After payment we will send you the decryption tool that will decrypt all your files.

Free decryption as quarantee

Before paying can send us up to 5 files for free decryption. Total size of file must be less than 10Mb (non archived), and files should not contain valuable information (databases, backups, large excel sheets, etc.)

How to obtain Bitcoins

The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click "Buy bitcoins", and select the seller by payment method and price.

https://localbitcoins.com/buy_bitcoins

Also you can find other places to buy Bitcoins and beginners guide here:

https://www.coindesk.com/information/how-can-i-buy-bitcoins/

Attention!

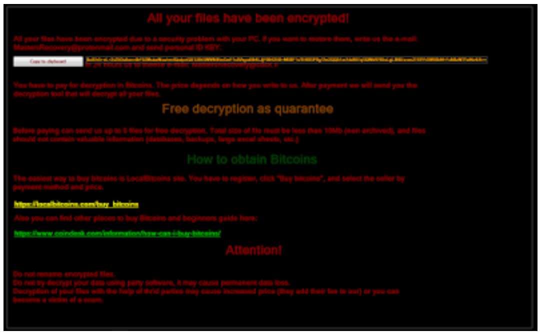
Do not rename encrypted files.
Do not try decrypt your data using party software, it may cause permanent data loss.
Decryption of your files with the help of thrid parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

In this blog post, we'll analyse Spartacus, one of many new ransomware families popping up in 2018.

Analysis

This instance of Spartacus ransomware has the following properties:

- **MD5**; 25dee2e70c931f3fa832a5b189117ce8
- **SHA1**; a01294ffd541229718948e17f791694efb596123
- **SHA256**; ef25bdbcf05fa478df3ddc5f4f717c070e443da04cfc590d44409c815f237cb3
- **Compilation timestamp**: 2018-01-19 20:36:44
- **VirusTotal report**: ef25bdbcf05fa478df3ddc5f4f717c070e443da04cfc590d44409c815f237cb3



All your files have been encrypted!

All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us the e-mail: MastersRecovery@protonmail.com and send personal ID KEY:

[illegible]

in 24 hours us to theese e-mail: MastersRecovery@cock.li

You have to pay for decryption in Bitcoins. The price depends on how you write to us. After payment we will send you the decryption tool that will decrypt all your files.

Free decryption as quarantee

Before paying can send us up to 5 files for free decryption. Total size of file must be less than 10Mb (non archived), and files should not contain valuable information (databases, backups, large excel sheets, etc.)

How to obtain Bitcoins

The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click "Buy bitcoins", and select the seller by payment method and price.

https://localbitcoins.com/buy_bitcoins

Also you can find other places to buy Bitcoins and beginners guide here:

https://www.coindesk.com/information/how-can-i-buy-bitcoins/

Attention!

Do not rename encrypted files.
Do not try decrypt your data using party software, it may cause permanent data loss.
Decryption of your files with the help of thrid parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

Figure 1 - Spartacus ransomware message

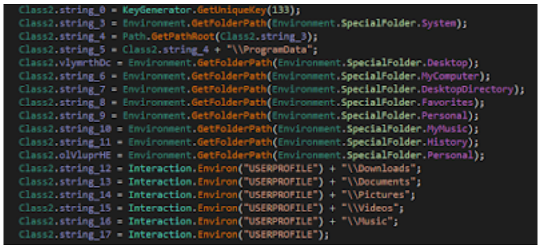
The message reads:

> *All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us the e-mail: MastersRecovery@protonmail.com and send personal ID KEY:*
> *In case of no answer in 24 hours us to theese e-mail: MastersRecovery@cock.li*

The user may send up to 5 files for free decryption, as "guarantee". There's also a warning message at the end of the ransomware screen:

> *Do not rename encrypted files.*
> *Do not try decrypt your data using party software, it may cause permanent data loss.*
> *Decryption of your files with the help of thrid parties may cause increased price (they add their fee to our) or you can become a victim of a scam.*

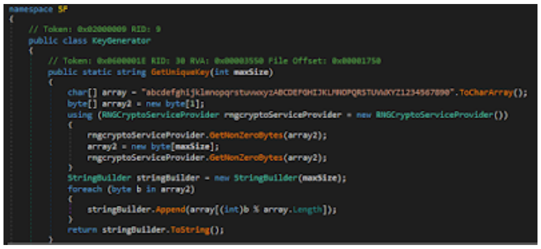
Spartacus will encrypt files, regardless of extension, in the following folders:



```
Class2.string_0 = KeyGenerator.GetUniqueKey(133);
Class2.string_3 = Environment.GetFolderPath(Environment.SpecialFolder.System);
Class2.string_4 = Path.GetPathRoot(Class2.string_3);
Class2.string_5 = Class2.string_4 + "\\ProgramData";
Class2.vlymrthDc = Environment.GetFolderPath(Environment.SpecialFolder.Desktop);
Class2.string_6 = Environment.GetFolderPath(Environment.SpecialFolder.MyComputer);
Class2.string_7 = Environment.GetFolderPath(Environment.SpecialFolder.DesktopDirectory);
Class2.string_8 = Environment.GetFolderPath(Environment.SpecialFolder.Favorites);
Class2.string_9 = Environment.GetFolderPath(Environment.SpecialFolder.Personal);
Class2.string_10 = Environment.GetFolderPath(Environment.SpecialFolder.MyMusic);
Class2.string_11 = Environment.GetFolderPath(Environment.SpecialFolder.History);
Class2.olVluprHE = Environment.GetFolderPath(Environment.SpecialFolder.Personal);
Class2.string_12 = Interaction.Environ("USERPROFILE") + "\\Downloads";
Class2.string_13 = Interaction.Environ("USERPROFILE") + "\\Documents";
Class2.string_14 = Interaction.Environ("USERPROFILE") + "\\Pictures";
Class2.string_15 = Interaction.Environ("USERPROFILE") + "\\Videos";
Class2.string_16 = Interaction.Environ("USERPROFILE") + "\\Music";
Class2.string_17 = Interaction.Environ("USERPROFILE");
```

Figure 2 - Target folders to encrypt

Generating the key:



```
namespace SF
{
    // Token: 0x02000009 RID: 9
    public class KeyGenerator
    {
        // Token: 0x0600001E RID: 30 RVA: 0x00003550 File Offset: 0x00001750
        public static string GetUniqueKey(int maxSize)
        {
            char[] array = "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890".ToCharArray();
            byte[] array2 = new byte[1];
            using (RNGCryptoServiceProvider rngcryptoServiceProvider = new RNGCryptoServiceProvider())
            {
                rngcryptoServiceProvider.GetNonZeroBytes(array2);
                array2 = new byte[maxSize];
                rngcryptoServiceProvider.GetNonZeroBytes(array2);
            }
            StringBuilder stringBuilder = new StringBuilder(maxSize);
            foreach (byte b in array2)
            {
                stringBuilder.Append(array[(int)b % array.Length]);
            }
            return stringBuilder.ToString();
        }
```

Figure 3 - KeyGenerator

As far as I'm aware, Spartacus is the first ransomware who explicitly *asks* you to send the public key (ID KEY), rather than just sending an email, including the Bitcoin address straight away, or sending the key automatically.

Encrypted files will get the extension appended as follows:
.[MastersRecovery@protonmail.com].Spartacus

For example:
Penguins.jpg.[MastersRecovery@protonmail.com].Spartacus

It will also drop the ransomware note, "READ ME.txt" in several locations, such as the user's Desktop:

> *All your data has been locked us. You want to return? Write email MastersRecovery@protonmail.com or MastersRecovery@cock.li Your personal ID KEY:*
> *DvQ9/mvfT3I7U847uKcI0QU3QLd+huv5NOYT2YhfiySde0vhmkzyTtRPlcu73BAJILIPdALjAIy5NLxBHckfyV2XS+GXdjlHMx2V/VEfj4BrZkLB3E*

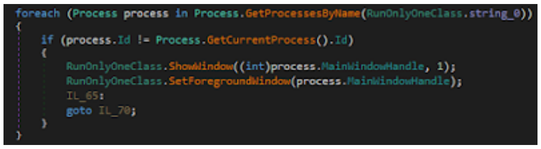
Interestingly enough, Spartacus also embeds what appears to be a hardcoded and private RSA key:

> *xA4fTMirLDPi4rnQUX1GNvHC41PZUR/fDIbHnNBtpY0w2Qc4H2HPaBsKepU33RPXN5EnwGqQ5lhFaNnLGnwYjo7w6OCkU+q0dRev14ndx4*

Spartacus will delete Shadow Volume Copies by issuing the following command:

> *cmd.exe /c vssadmin.exe delete shadows /all /quiet*

A unique mutex of "**Test**" will be created in order to not run the ransomware twice, and Spartacus will also continuously keep the ransomware screen or message from running in the foreground or on top, using the SetForegroundWindow function:



```
foreach (Process process in Process.GetProcessesByName(RunOnlyOneClass.string_0))
{
    if (process.Id != Process.GetCurrentProcess().Id)
    {
        RunOnlyOneClass.ShowWindow((int)process.MainWindowHandle, 1);
        RunOnlyOneClass.SetForegroundWindow(process.MainWindowHandle);
        IL_65:
        goto IL_70;
    }
}
```

Figure 4 - Ransom will stay on top and annoy the user

Repeating, email addresses used are:

> *MastersRecovery@protonmail.com*
> *MastersRecovery@cock.li*

Decryption may be possible if the ransomware is left running, by extracting the key from memory.

Conclusion

Spartacus is again another ransomware family or variant popping up.

Figure 5 - Meme

Make sure to read the dedicated page on ransomware prevention to prevent Spartacus or any other ransomware. **IOCs**