New RURansom Wiper Targets Russia

: 3/8/2022

We analyze RURansom, a malware variant discovered to be targeting Russia. Originally suspected to be a ransomware because of its name, analysis reveals RURansom to be a wiper.

By: Jaromir Horejsi, Cedric Pernet March 08, 2022

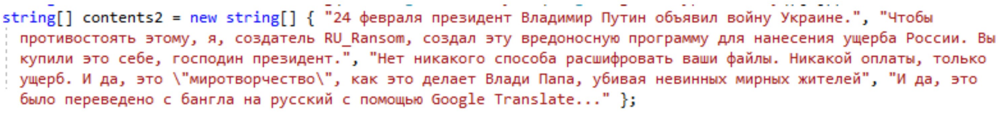
A conflict in cyberspace is unfolding parallel to the conflict between Russia and Ukraine on the ground. Cyberattacks are being lobbed against both Russian and Ukrainian sides, with a new wiper directed against Russia joining the fray.

On March 1, a tweet from MalwareHunterTeam about a possible ransomware variant caught our attention and set our immediate analysis into motion. We found several additional samples of this malware, which has been dubbed as "RURansom" by its developer. Despite its name, analysis has revealed it to be a wiper and not a ransomware variant because of its irreversible destruction of encrypted files.

Targeting Russia

Based on our telemetry, we have not yet observed active targets for this malware family. One possible reason for this is that the wiper has only targeted a few entries in Russia so far.

RURansom's code, however, makes its author's motives clear. Figure 1 shows the code variable responsible for the malware's ransom note.



```
string[] contents2 = new string[] { "24 февраля президент Владимир Путин объявил войну Украине.", "Чтобы
  противостоять этому, я, создатель RU_Ransom, создал эту вредоносную программу для нанесения ущерба России. Вы
  купили это себе, господин президент.", "Нет никакого способа расшифровать ваши файлы. Никакой оплаты, только
  ущерб. И да, это \"миротворчество\", как это делает Влади Папа, убивая невинных мирных жителей", "И да, это
  было переведено с бангла на русский с помощью Google Translate..." };
```

Figure 1. Code snippet of what will be written in the ransom note file

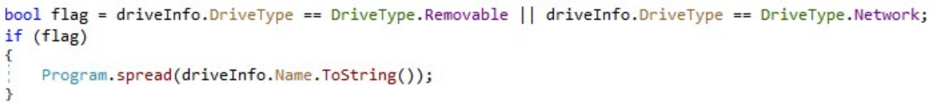
The note reads in English as follows:

On February 24, President Vladimir Putin declared war on Ukraine.", "To counter this, I, the creator of RU_Ransom, created this malware to harm Russia. You bought this for yourself, Mr. President.", "There is no way to decrypt your files. No payment, only damage. And yes, this is \"peacekeeping\" like Vladi Papa does, killing innocent civilians", "And yes, it was translated from Bangla into Russian using Google Translate... (This is a direct translation.)

We detected different versions of the malware between February 26 and March 2, 2022. Upon further analysis, we have learned more details about its capabilities.

RURansom: A new wiper

The malware is written in .NET programming language and spreads as a worm by copying itself under the file name "Россия-Украина_Война-Обновление.doc.exe" to all removable disks and mapped network shares. Translated into English, the file name reads as "Russia-Ukraine_War-Update.doc.exe."

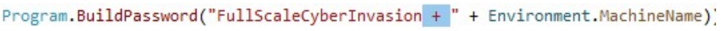


```
bool flag = driveInfo.DriveType == DriveType.Removable || driveInfo.DriveType == DriveType.Network;
if (flag)
{
    Program.spread(driveInfo.Name.ToString());
}
```

Figure 2. Code snippet showing RURansom's spreading mechanism

After successfully spreading, the malware then begins encryption. If the assigned disk letter is "C:\," for example, the files in the folder "C:\\Users\\<UserName>" are encrypted. For other removable and mapped network drives, all files that recursively branch from the root directory are encrypted.

Encryption is applied to all file extensions except for ".bak" files, which are deleted. The files are encrypted with a randomly generated key with length equal to base64 ("FullScaleCyberInvasion + " + MachineName).



```
Program.BuildPassword("FullScaleCyberInvasion + " + Environment.MachineName);
```

Figure 3. Code showing the length of the randomly generated key for encryption, with an extra "+," which is likely a typo

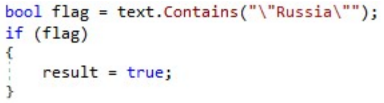
The encryption algorithm is AES-CBC using a hard-coded salt. The keys are unique for each encrypted file and are not stored anywhere, making the encryption irreversible and marking the malware as a wiper rather than a ransomware variant.

The "ransom" note, which is the file "Полномасштабное_кибервторжение.txt" (translated as "Full-blown_cyber-invasion.txt"), is then dropped into each directory. However, it is more accurate to say that this is a wiper note.

As seen in the code in Figure 1, the note states its developer's sentiments and also reveals that the author used Google Translate to convey their message in Russian from the original Bangla.

Still in development

We have discovered several versions of RURansom. Some of these versions check if the IP address where the software is launched is in Russia. In cases where the software is launched outside of Russia, these versions will stop execution, showing a conscious effort to target only Russian-based computers. While most samples were unobfuscated, we found one version using ConfuserEx for obfuscation.



```
bool flag = text.Contains("\"Russia\"");
if (flag)
{
    result = true;
}
```

Figure 4. Code snippet where the malware tests if it is being run from Russia

Other versions also attempt to start the process with elevated privileges. These different versions and modifications might indicate that the malware was still undergoing development at the time of writing.

Other activities from the same author

Aside from RURansom, the developer appears to have been working on another "wiper" dubbed as "dnWipe." Its payload is executed every Tuesday.

We analyzed dnWipe and found that it simply encodes content in base64 for the following file extensions: .doc, .docx, .png, .gif, .jpeg, .jpg, .mp4, .txt, .flv, .mp3, .ppt, .pptx, .xls, and .xlsx. Therefore, just as RURansom is not really a ransomware variant, dnWipe also cannot be classified as an example of a wiper malware because its encoding can be decoded easily.

Other binaries that we can attribute with high confidence to the same developer indicate their other interests. For one, they have also compiled a downloader for an XMRig binary, showing an inclination for cryptocurrency mining.

Conclusion

No one can be indifferent to the conflict between Ukraine and Russia. People all over the world are actively taking sides, and malware developers are no exception.

As this blog entry shows, the exchange of attacks in cyberspace is reflective of this conflict: Leaks have exposed Russian-based cybercriminal groups behind Conti and TrickBot, while a destructive wiper has attacked organizations in Ukraine. Now, the RURansom wiper is seeking out Russian targets.

We see RURansom as just one attempt among a growing list of attacks that aim to support a position espoused strongly by an individual or a group. While we have not yet found any victims of this malware, seeing the evolution in its code leads us believe that its developer will keep updating their malware in an effort to deal some form of damage on Russia.

In general, the tense geopolitical situation has added an edge to cyberattacks. Ultimately, keeping defenses up, staying vigilant against misinformation, and monitoring the situation is essential in order to navigate this uncertain state of affairs.

For more guidance on managing today's cyber risks, please see our earlier blog post here.

Indicators of Compromise (IOCs)

SHA256	**Detection name**
107da216ad99b7c0171745fe7f826e51b27b1812d435b55c3ddb801e23137d8f	Ransom.MSIL.RUCRYPT.YXCCD
1f36898228197ee30c7b0ec0e48e804caa6edec33e3a91eeaf7aa2c5bbb9c6e0	Ransom.MSIL.RUCRYPT.YXCCD
610ec163e7b34abd5587616db8dac7e34b1aef68d0260510854d6b3912fb0008	Ransom.MSIL.RUCRYPT.YXCCD
696b6b9f43e53387f7cef14c5da9b6c02b6bf4095849885d36479f8996e7e473	Ransom.MSIL.RUCRYPT.YXCCD
8f2ea18ed82085574888a03547a020b7009e05ae0ecbf4e9e0b8fe8502059aae	Ransom.MSIL.RUCRYPT.YXCCD
979f9d1e019d9172af73428a1b3cbdff8aec8fdbe0f67cba48971a36f5001da9	Ransom.MSIL.RUCRYPT.YXCCD