The Syrian Electronic Army malware

1. Introduction

In 2012, the Syrian Electronic Army (SEA) started a new malware campaign which targeted Syrian rebels. The hacking group used common Remote Administration Tools (RAT) like DarkComet and BlackShades. Once the creator of DarkComet learned of the use by the Syrian government, development and the distribution sites were shut down. The malware was spreading itself through social networks and fake revolutionary documents. In this paper, we will analyse the DarkComet malware which was mainly spread through Skype. The tools that we are going to use are: RDG Packer Detector, Ollydbg, UPX packer

2. The Dropper

The first step is to scan the dropper with the RDG Packer Detector (Figure 1), hoping to give us useful information. The malware dropper (MD5: 8c9f9ccffbd2c888b9b5300412f8e580) is compressed as SFX (Self-extracting archive). By default, this means that when the user executes the file, the malware, and other functionalities of it, will execute. In order to understand and see what the dropper is going to do, we are going to open it with WINRAR (Figure 2).

Figure 1

Figure 2

As you can see in Figure 2, we have one executable, one PDF file and an OLE file. If the user runs the dropper, these three files will be extracted in the temp folder(Figure 3). After the successfully extraction, the PDF file will get firstly executed and then silently the "Explorer.exe" file which is the malware. The PDF file name, translated

as “A paper on Leadership Council” in English, and its content is written in Arabic(Figure 4) .The purpose of the PDF file is to make the user think that in reality a PDF file was downloaded.

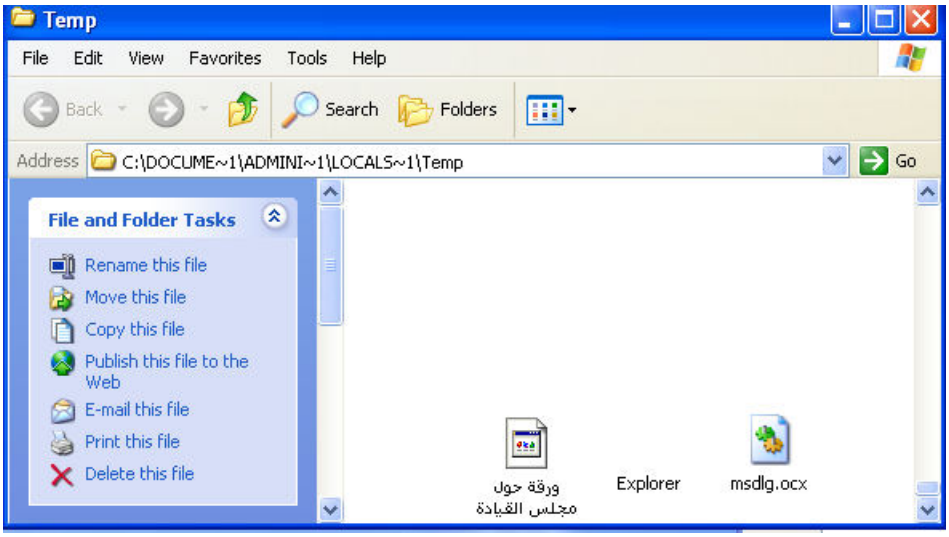
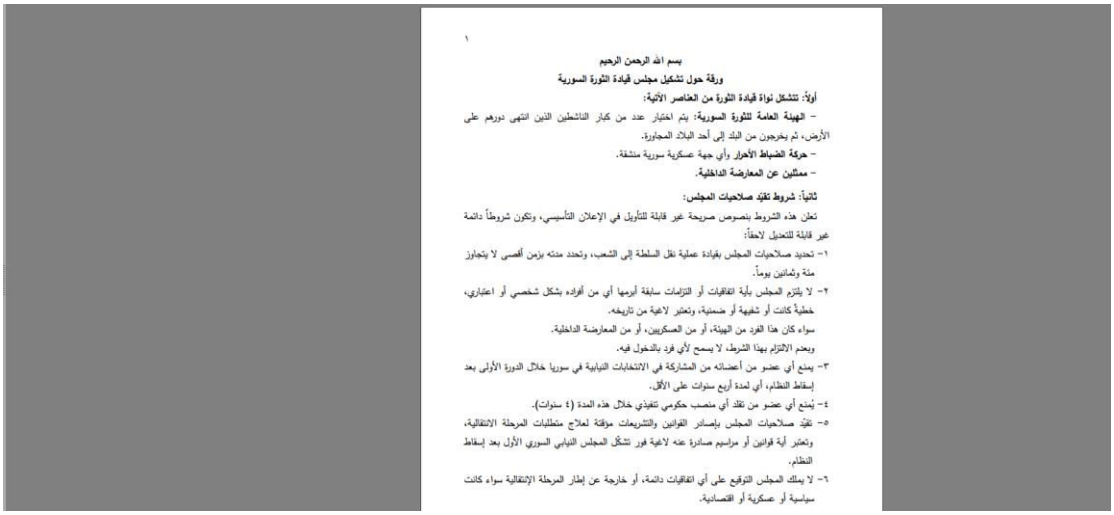


Figure 3



بسم الله الرحمن الرحيم

ورقة حول تشكيل مجلس قيادة الثورة السورية

أولاً: تتشكل نواة قيادة الثورة من العناصر الآتية:

- الهيئة العامة للثورة السورية: يتم اختيار عدد من كبار الناشطين الذين انتهى دورهم على الأرض، ثم يخرجون من البلد إلى أحد البلاد المجاورة.
- حركة الضباط الأحرار وأي جهة عسكرية سورية منشقة.
- ممثلين عن المعارضة الداخلية.

ثانياً: شروط تقيّد صلاحيات المجلس:

تعلن هذه الشروط بنصوص صريحة غير قابلة للتأويل في الإعلان التأسيسي، وتكون شروطاً دائمة غير قابلة للتعديل لاحقاً:

١- تحديد صلاحيات المجلس بقيادة عملية نقل السلطة إلى الشعب، وتحدد مدته بزمن أقصى لا يتجاوز مئة وثمانين يوماً.

٢- لا يلتزم المجلس بأية اتفاقيات أو التزامات سابقة أبرمها أي من أفراده بشكل شخصي أو اعتباري، خطية كانت أو شفهية أو ضمنية، وتعتبر لاغية من تاريخه.

سواء كان هذا الفرد من الهيئة، أو من العسكريين، أو من المعارضة الداخلية.

ويحتم الالتزام بهذا الشرط، لا يسمح لأي فرد بالدخول فيه.

٣- يمنع أي عضو من أعضائه من المشاركة في الانتخابات النيابية في سوريا خلال الدورة الأولى بعد إسقاط النظام، أي لمدة أربع سنوات على الأقل.

٤- يُمنع أي عضو من تقلد أي منصب حكومي تنفيذي خلال هذه المدة (٤ سنوات).

٥- تقيّد صلاحيات المجلس بإصدار القوانين والتشريعات مؤقتة لمعالج متطلبات المرحلة الانتقالية، وتعتبر أية قوانين أو مراسيم صادرة عنه لاغية فور تشكّل المجلس النيابي السوري الأول بعد إسقاط النظام.

٦- لا يملك المجلس التوقيع على أي اتفاقيات دائمة، أو خارجة عن إطار المرحلة الإنتقالية سواء كانت سياسية أو عسكرية أو اقتصادية.

Figure 4

3. Unpacking

As we said previously, the “Explorer.exe”, with MD5:fc0488cb54bc4b25b74607d7f9402a0c, is the malware. The malware is packed with a Visual Basic (VB) Crypter (Figure 5). Unpacking Visual Basic Crypters can be done with multiple ways, in this example we will set a breakpoint in the WriteProcessMemory function.

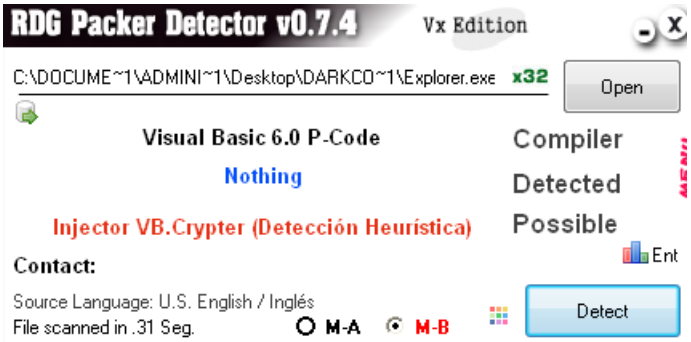


Figure 5

Open Ollydbg, set a breakpoint in WriteProcessMemory and execute the malware. After hitting six times in the breakpoint, we go in the stack window, choose the "buffer" argument of the function, right click on it and select "Follow in Dump". If everything is ok, you should see this in the dump window (Figure 6).

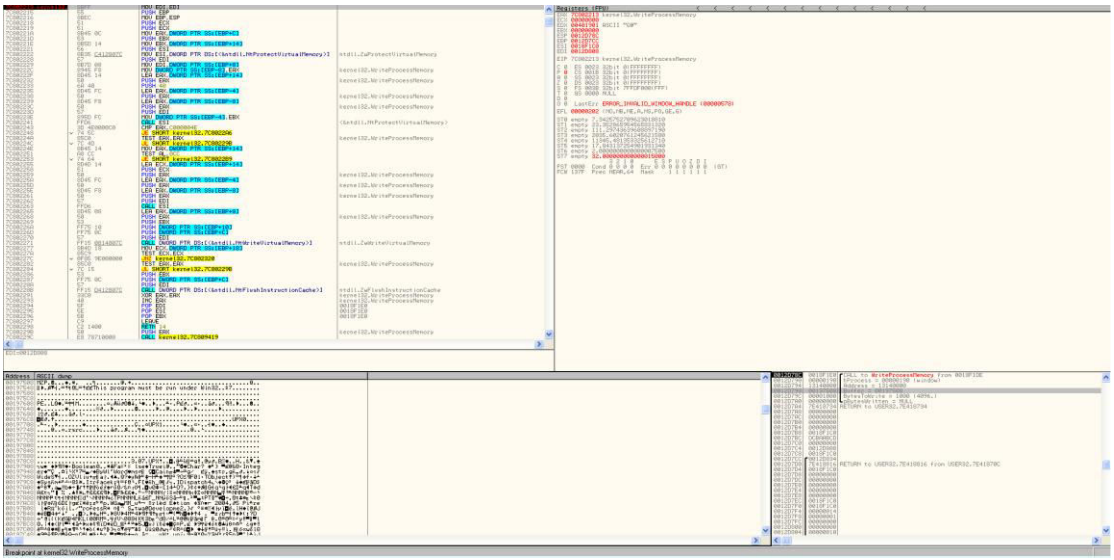


Figure 6

We can see the malware being unpacked. Lastly, right click in the dump window, then Backup->Sava Data to file. After the saving is done, open the .mem file in a hex editor and delete everything until the MZP string, save the file as .exe. Scanning the unpacked file with RDG Packer Detector, we see that it has been packed with UPX (Figure 7).

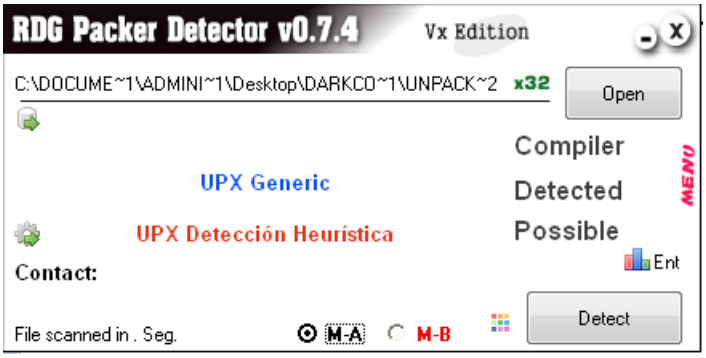


Figure 7

Unpacking UPX is easy, we will use the official unpacker tool which is created by the developers of UPX (Figure 8). In case that you want to unpack it manually, open the file in Ollydbg, click ok or Yes in any warning, set a breakpoint in the last jmp instruction and execute the malware, ollydbg will stop you in the jmp instruction, step over it(F8) and you can the Original Entry Point (OEP). After unpacking the UPX, we scan the malware again with RDG Packer Detector and we see that the file is unpacked and is recognized as DarkComet malware (Figure 9).

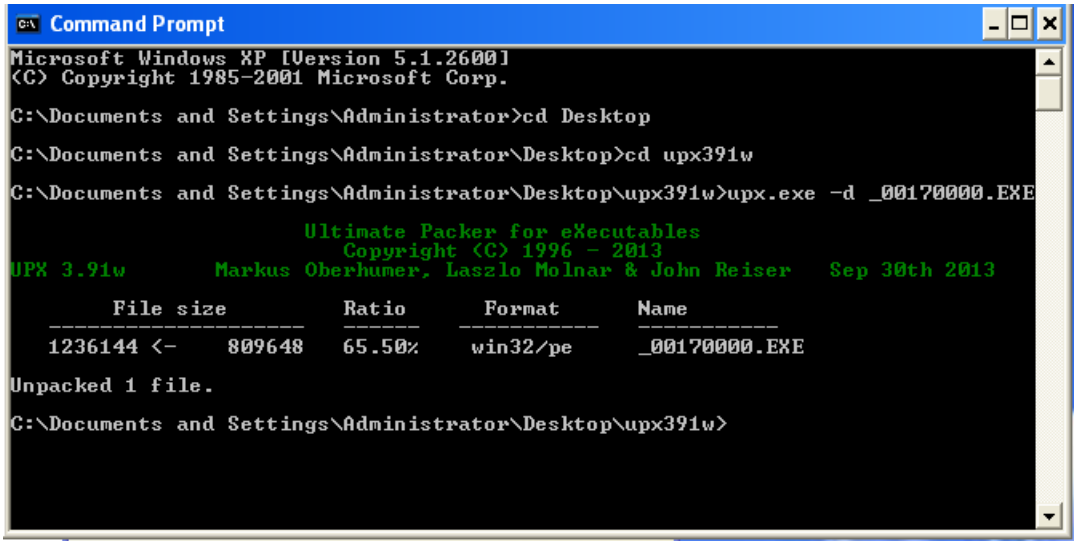


Figure 8

Figure 9

4. Decrypting the Config

DarkComet provides the attacker with a lot of spy functionalities such as web camera capture, keylogging, network scanners. In this topic, we will decrypt the config of the malware, which includes the domain which the stolen data are sent and the MUTEX. Opening the file in Resource Hacker, we see the following information (Figure 10).

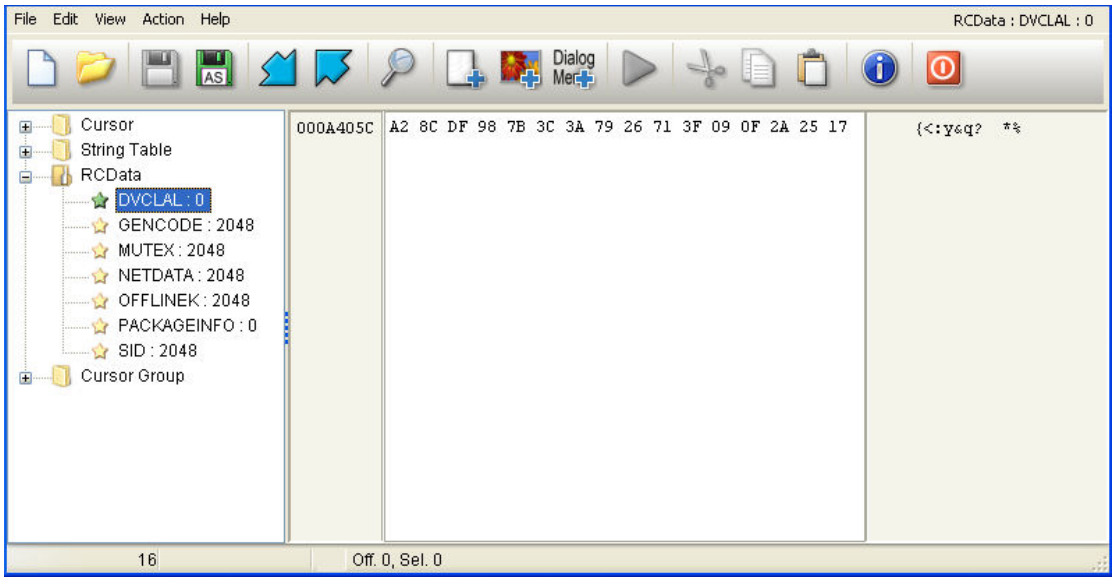


Figure 10

It is clear that the config of the malware is stored in the resources. In order to start decrypting it, the malware uses a Windows API call to find the data to decrypt, this API function is the FindResourceA. Open up Ollydbg and load the unpacked malware, set a breakpoint in FindResourceA function and run it. We break here (Figure 11), the "MUTEX" word can be seen in the registers window, which means that we are close in the decryption loop. Keep stepping over until you reach this point (Figure 12). The decryption key is hardcoded and you can see it before a call is made ("#KCMDDC2#-"), stepping into the call before the XOR EAX,EAX, we can see the decryption loop. An experienced eye can see that it's a RC4 encryption, step over until the end of the last loop and you will see the MUTEX decrypted (Figure 13).

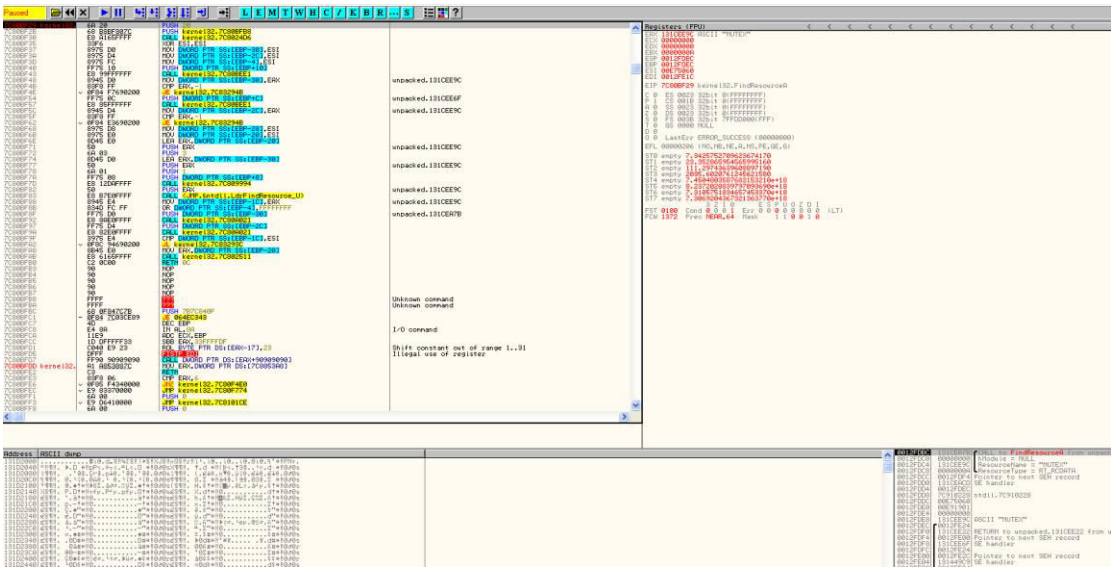


Figure 11

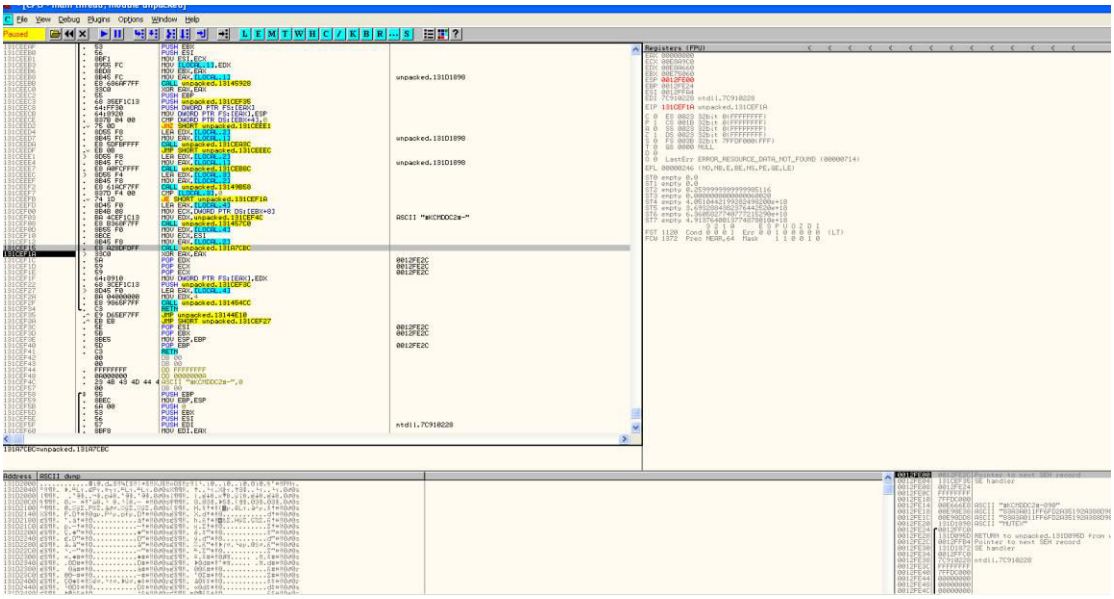


Figure 12

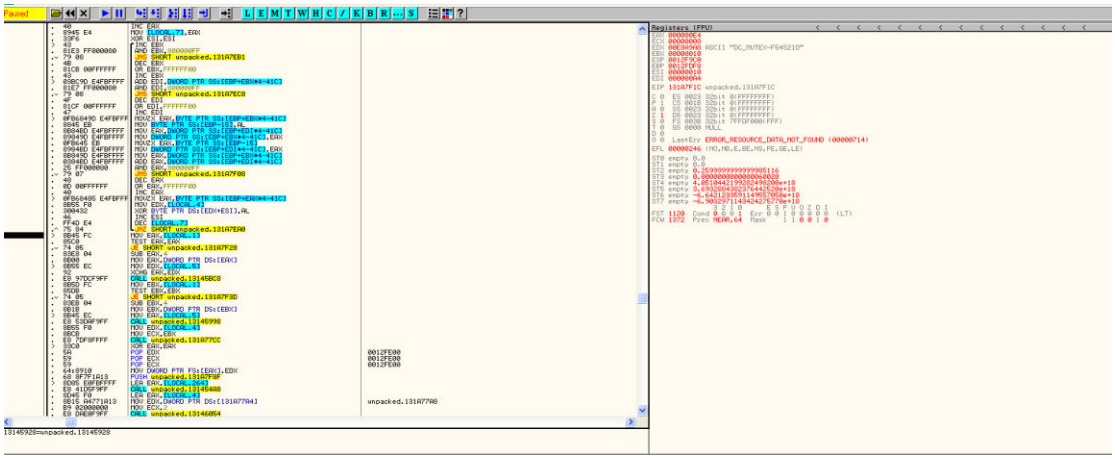


Figure 13

At this moment, you can set a breakpoint in the end of the last loop, run the malware, and see the config getting decrypted. For example, in the following picture we can see the host (Figure 14).

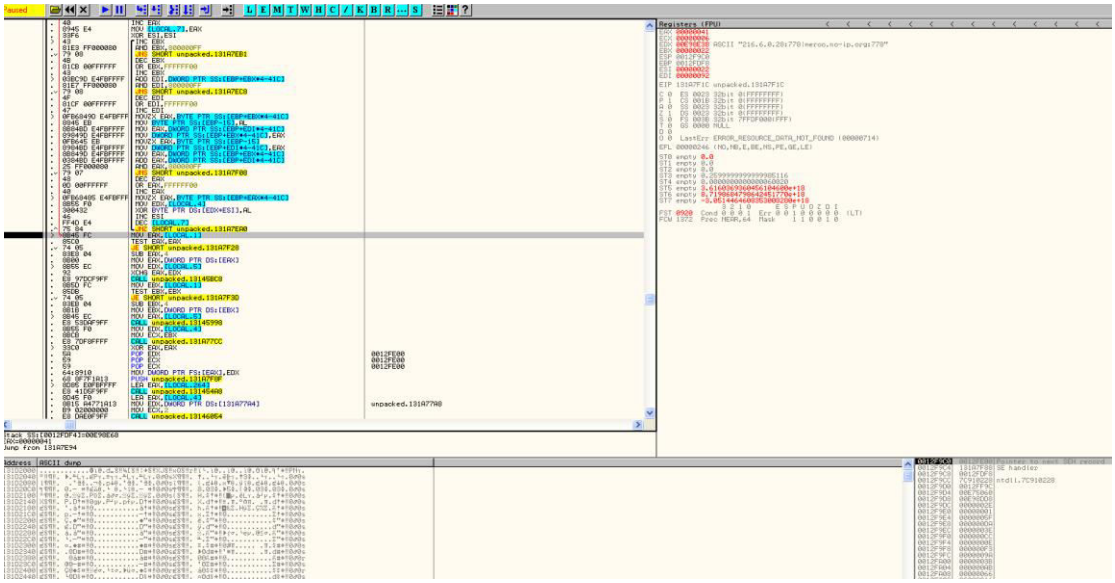


Figure 14

In case that you don't want to follow the debugger way, you can get the encrypted text from the resource, as we saw in the resource hacker, and decrypted it in an online website with the hardcoded key.

5. Conclusion

The malware doesn't have any advanced encryption layers or packing abilities. The hacking group didn't use any sophisticated attack or any 0-days exploits. The crypter which they used was probably bought from an underground forum.

6. References

1. https://threatpost.com/darkcomet-rat-used-new-attack-syrian-activists-081612/76919/
2. https://en.wikipedia.org/wiki/DarkComet