

# Operations Security (OPSEC)

written by Mert SARICA | 3 August 2020

Sometimes when you follow cybersecurity experts on social media or look at cybersecurity presentations, you may come across phrases like “OPSEC FAIL.” These usually refer to significant operational errors made by APT groups and/or malware developers. For those who are curious about what operasyon güvenliği (OPSEC) is, it stands for Operational Security, which is a process of protecting critical information about an operation to prevent it from being acquired by opposing intelligence units.

At the Virus Bulletin event held in London from October 2-4, 2019, I participated in a presentation entitled “Who is SandCat: an unveiling of a lesser-known threat actor” by Kaspersky. The presentation covered the OPSEC errors made by the SandCat group, believed to be a unit of Uzbekistan intelligence. One of the errors was that the group used a command and control center with the address registered under the name of a military unit (Military Unit 02616) when testing 0-day exploit codes on systems with Kaspersky Antivirus software that had telemetry feature enabled. This showed that the group did not take OPSEC very seriously. Kaspersky researchers were able to take advantage of the opportunity and collect the 0-day exploit codes used by the group from systems with Kaspersky Antivirus software and analyze them.

As a cyber security researcher who takes advantage of opportunities to hunt for threats on VirusTotal, I recently encountered a malicious software developer who was not paying attention to the topic of OPSEC (Operations Security) in the past months.

https://www.virustotal.com/gui/search/positives%253A1%252B%2520f%253A2019-01-01T00%253A00%252B%2520submitter%253ATR%2520fatura/files

Hack 4 Career. Infor... LinkedIn Mert SARICA (merts... Inbox - mertsarica...

positives:1+ fs.2019-01-01T00:00:00+ submitter:TR Fatura

Help

FILES 6

90 DAYS

			First submission	Last submission	Submitters	
1ee11857672c87ed09b9ce0891bf1c08127ae357ce9af1d03eca24a13829224e	7 / 54	249.59 KB	2019-07-24 13:36:00	2019-07-24 13:36:00	1	72
ÖDEME SİPARİŞLERİ İÇİN Fatura.7z						
c3551f4ca271b933d0eb96ba1ba6240f1f72202523c44079101490a5aa61aad4	9 / 55	4.71 MB	2019-07-16 13:06:38	2019-07-16 13:06:38	1	
Fatura.pdf						
a7cf65beb414420a5f9f3b84199f613a3ed3d6e065293320dd38c0a8fd64e310	30 / 54	7.29 KB	2019-07-16 07:06:21	2019-07-16 07:06:21	1	
Fatura_001.pdf						
d25656db3d159dd97fd634b0d0d74e355a362c6442e5ec941703e9cafcec875	50 / 70	452.5 KB	2019-07-07 13:55:25	2019-07-12 21:27:10	2	
fatura1.exe						
1b0c9588f3aee2b033b3158725f2641851d82cb8b0183c98050ed9a02eebda	1 / 56	28.46 MB	2019-07-10 06:36:42	2019-07-10 06:36:42	1	
Downloads.zip						
a58012fd8111bb5a3f461fddcf40e7727dd73bfb4702f76ed7f3d5349bd265ed	1 / 58	639.64 KB	2019-07-03 08:57:06	2019-07-03 08:57:06	1	
fatura.rar						

https://www.virustotal.com/gui/file/d25656db3d159dd97fd634b0d0d74e355a362c6442e5ec941703e9cafcec875/detection

Hack 4 Career. Infor... LinkedIn Mert SARICA (merts... Inbox - mertsarica...

d25656db3d159dd97fd634b0d0d74e355a362c6442e5ec941703e9cafcec875

Help

50 / 70

50 engines detected this file

d25656db3d159dd97fd634b0d0d74e355a362c6442e5ec941703e9cafcec875

452.5 KB Size

2019-07-12 21:27:10 UTC

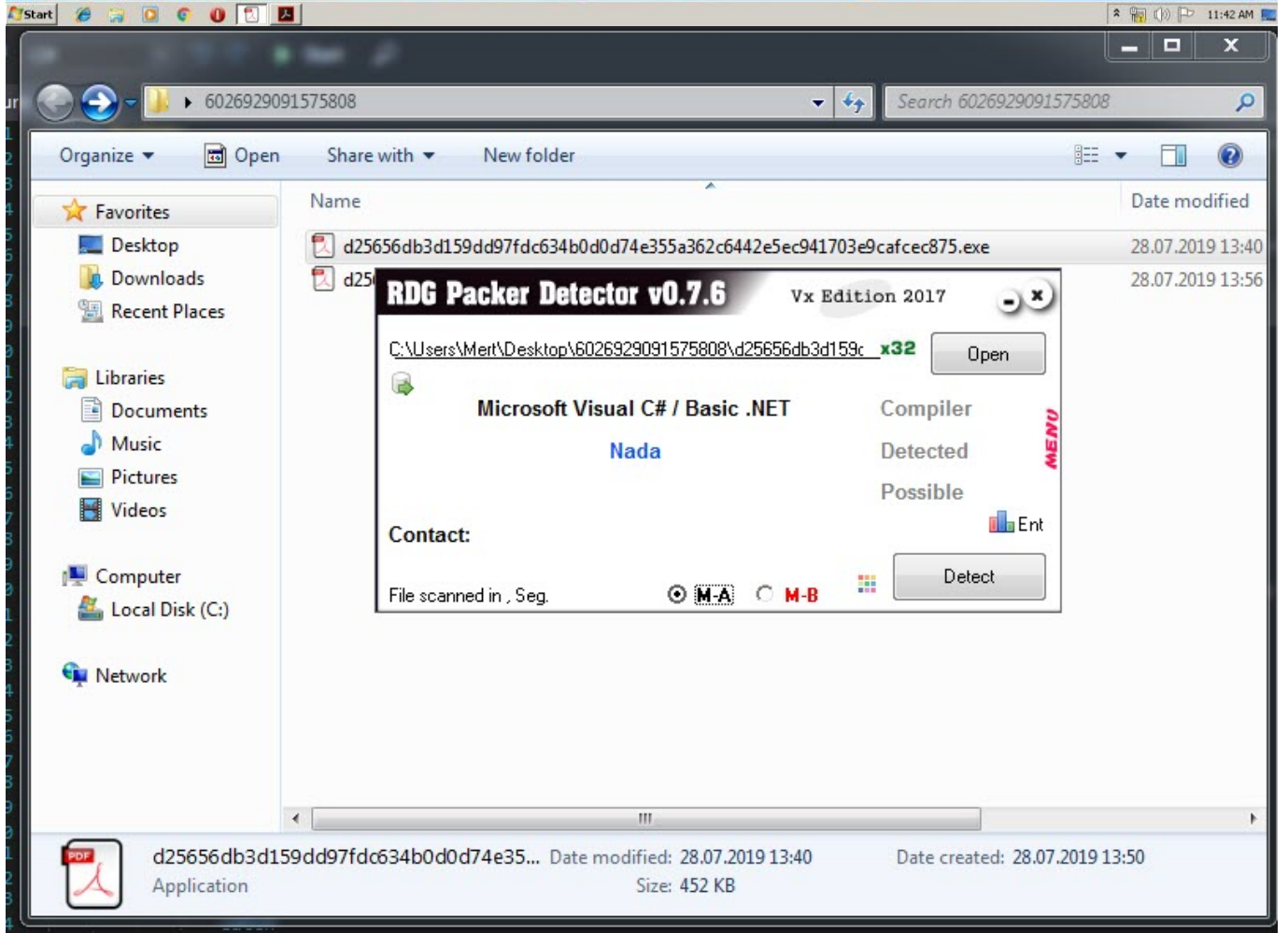
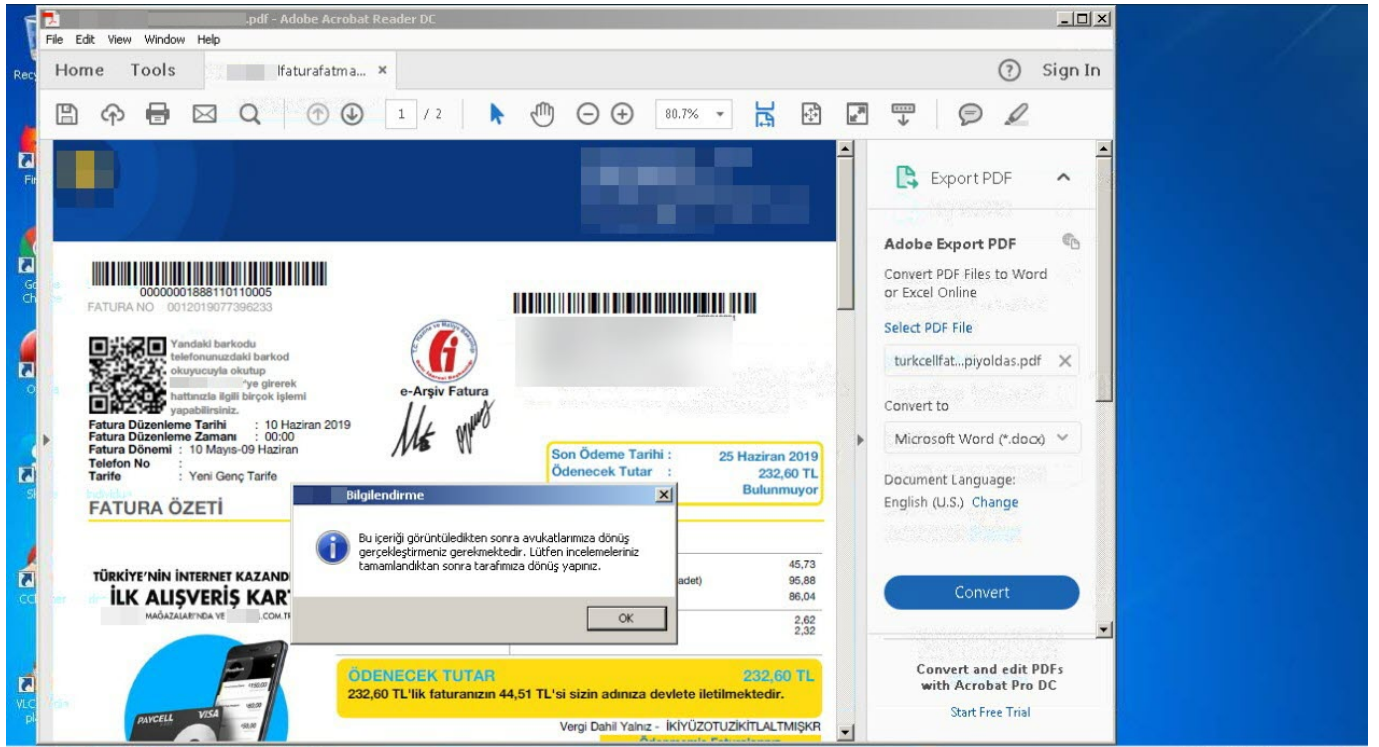
15 days ago

EXE

Community Score

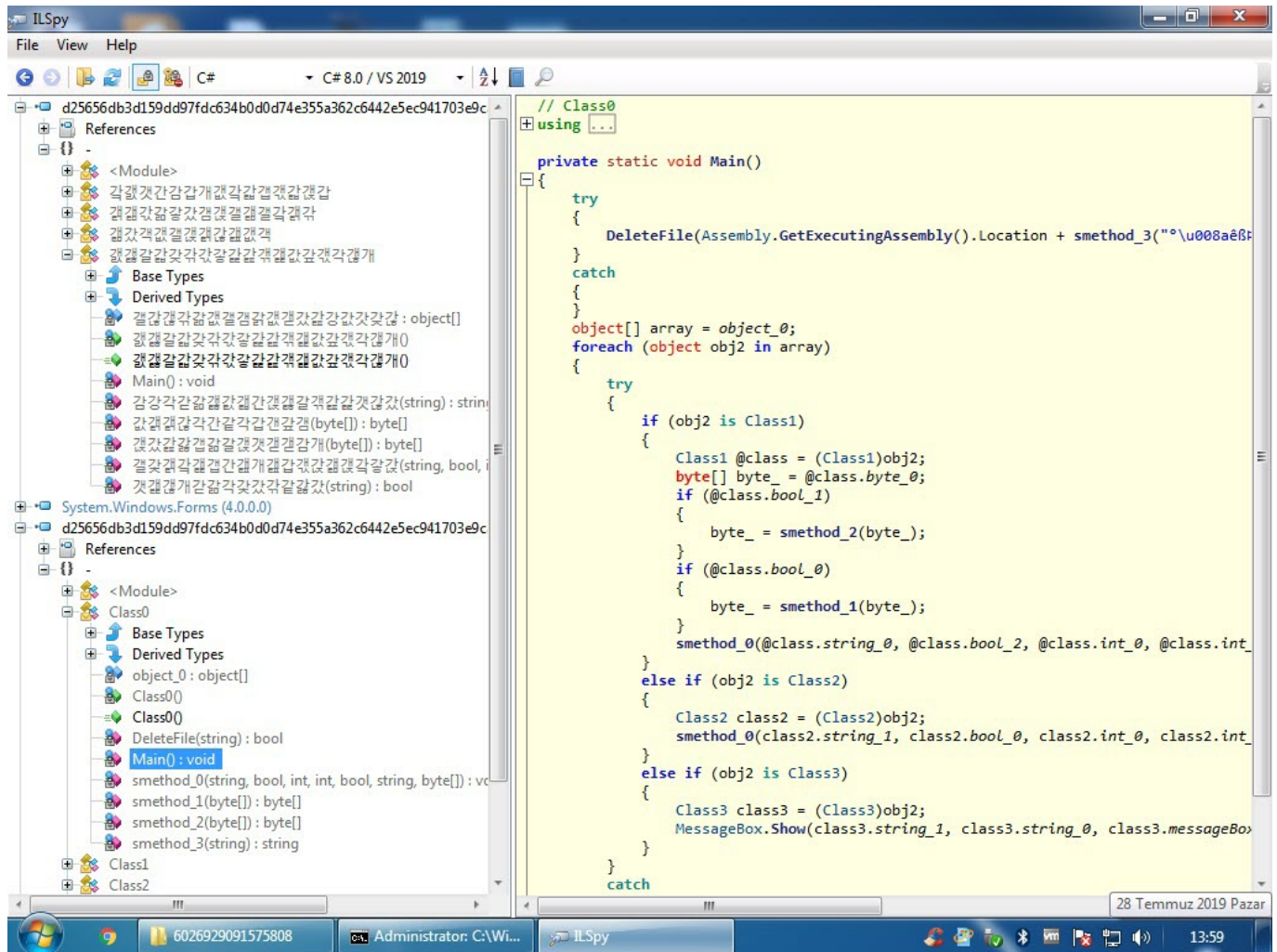
DETECTION	DETAILS	RELATIONS	BEHAVIOR	CONTENT	SUBMISSIONS	COMMUNITY
2019-07-12T21:27:10						
Acronis	⚠ Suspicious				Ad-Aware	⚠ Gen.Variant.Razy.261495
AegisLab	⚠ Trojan.Win32.Agent.4lc				Alibaba	⚠ Trojan.MSIL/Agent.433c9bea
ALYac	⚠ Gen.Variant.Razy.261495				Antiy-AVL	⚠ Trojan/Win32.Agent
SecureAge APEX	⚠ Malicious				Avast	⚠ Win32.Malware-gen
AVG	⚠ Win32.Malware-gen				Avira (no cloud)	⚠ TR/Dropper.MSIL.Gen
BitDefender	⚠ Gen.Variant.Razy.261495				CAT-QuickHeal	⚠ Trojan.Agent
ClamAV	⚠ Win.Malware.Generic-6922521-0				CrowdStrike Falcon	⚠ Win/malicious_confidence_100% (W)
Cybereason	⚠ Malicious.4edfdb				Cylance	⚠ Unsafe
Cyren	⚠ W32/MSIL_Troj_GL.gen/Eldorado				DrWeb	⚠ Trojan.Inject3.16777
Emsisoft	⚠ Gen.Variant.Razy.261495 (B)				Endgame	⚠ Malicious (high Confidence)
eScan	⚠ Gen.Variant.Razy.261495				ESET-NOD32	⚠ A Variant Of MSIL/TrojanDropper.Agent....
F-Prot	⚠ W32/MSIL_Troj_GL.gen/Eldorado				F-Secure	⚠ Trojan.TR/Dropper.MSIL.Gen
FireEye	⚠ Generic.mg.80858174edfdb39b				Fortinet	⚠ MSIL/Agent.DOZlfr

When I ran the malware named “fatura1.exe” on my analysis system, a fake phone bill and warning message appeared. When I examined the “fatura1.exe” file with the RDG Packer Detector tool, I learned that it was developed with the C# programming language. When I briefly looked at the code with the ILSpy source code translator, I saw that the code was obscured (obfuscated). To make the source code readable, I used the de4dot tool.



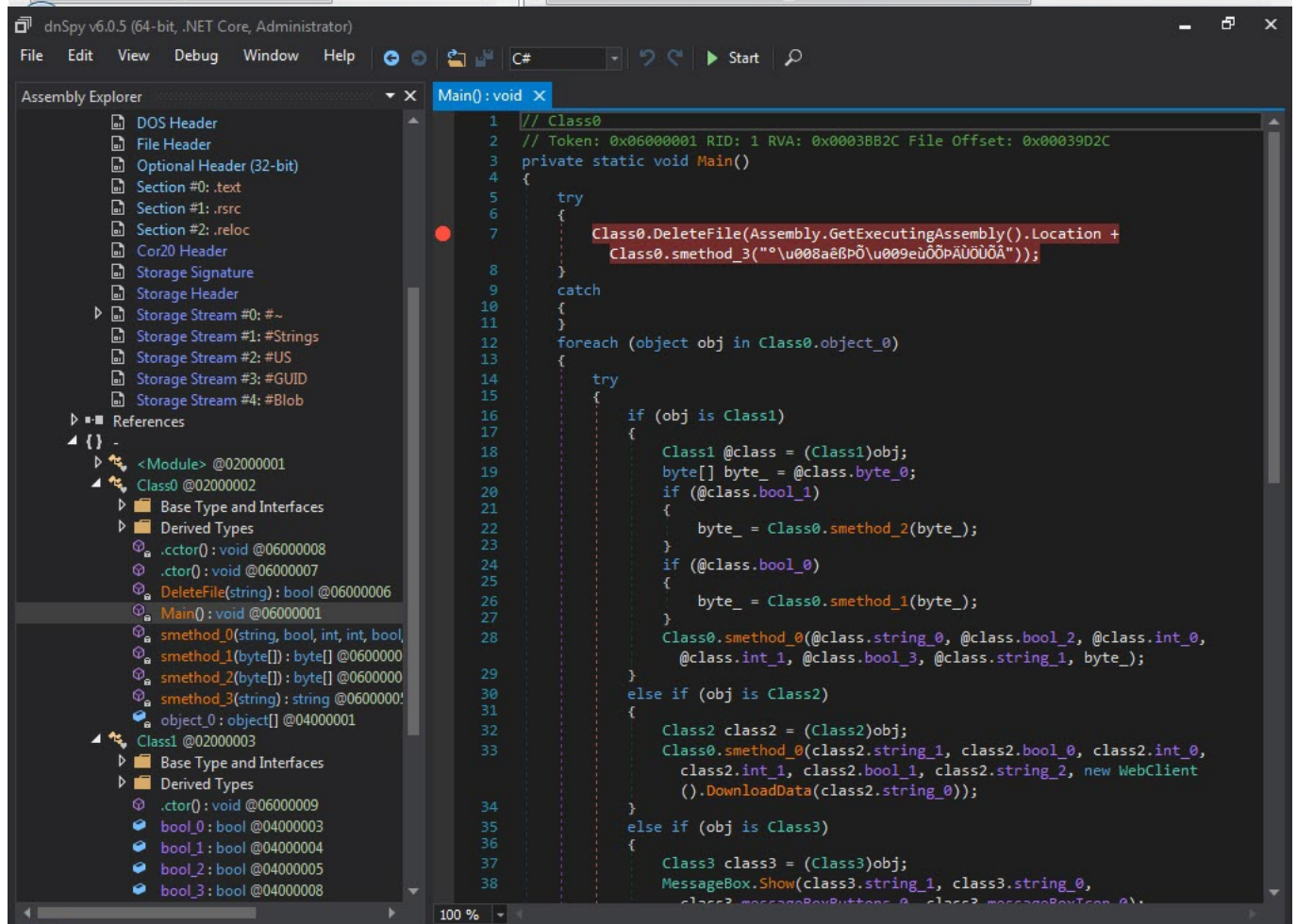
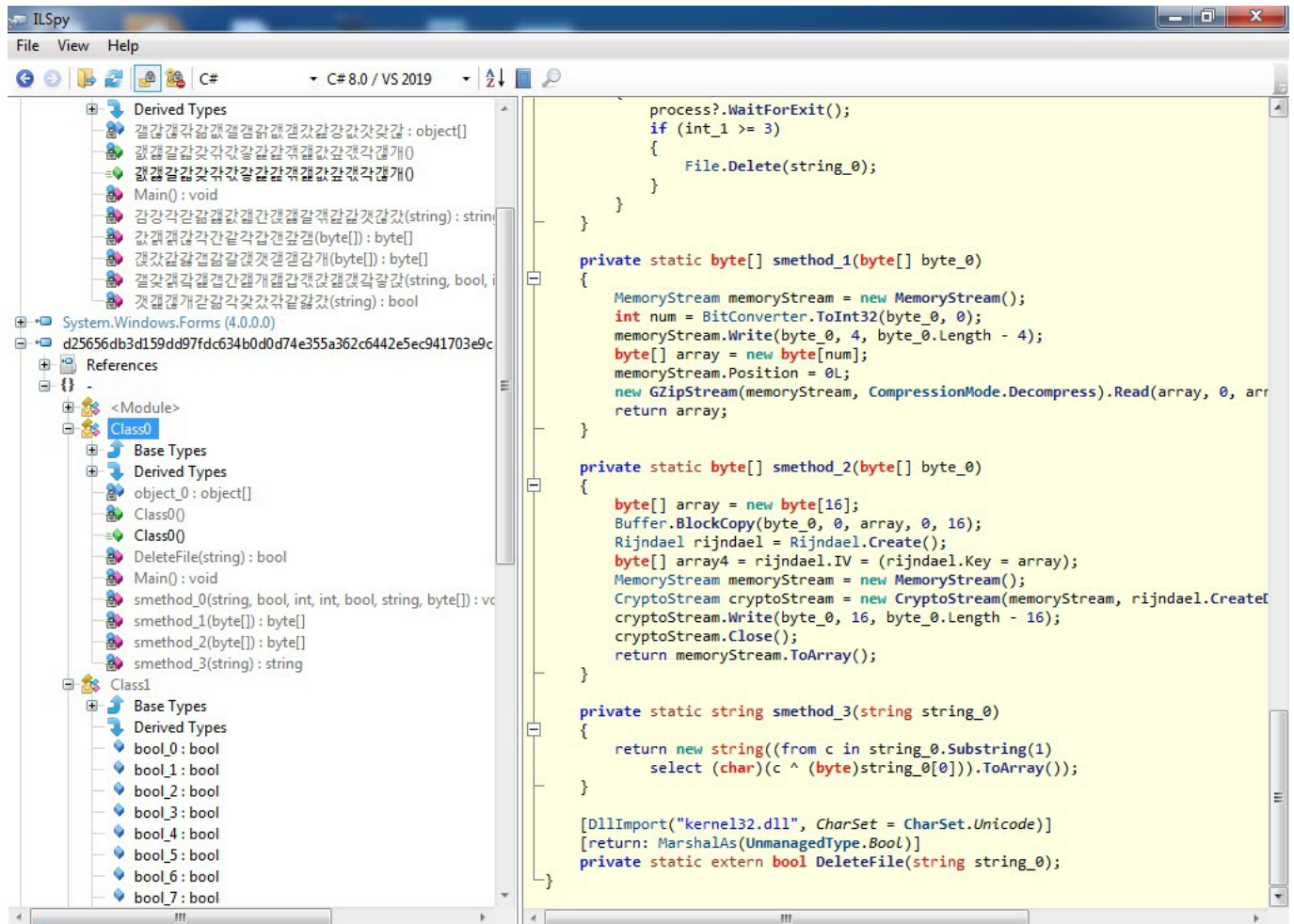


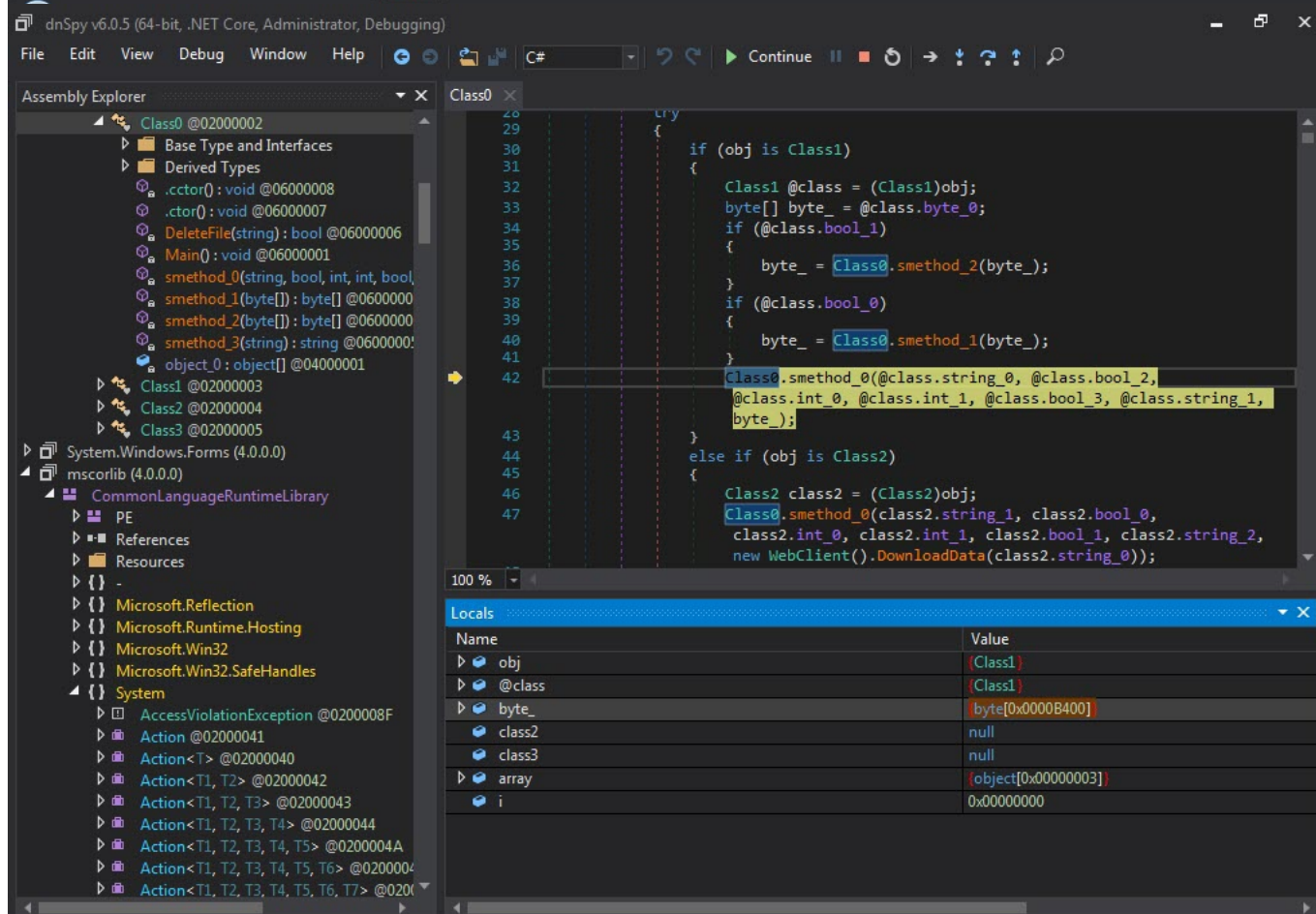
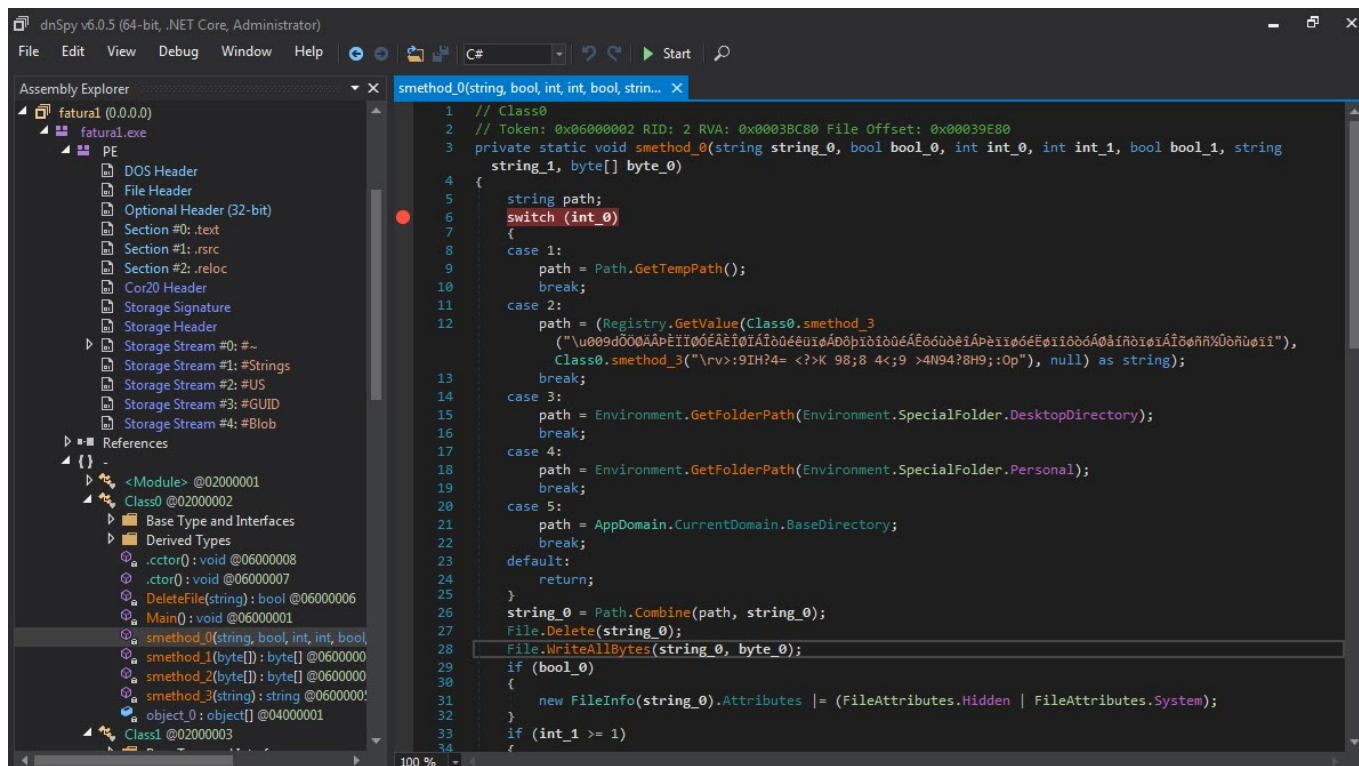




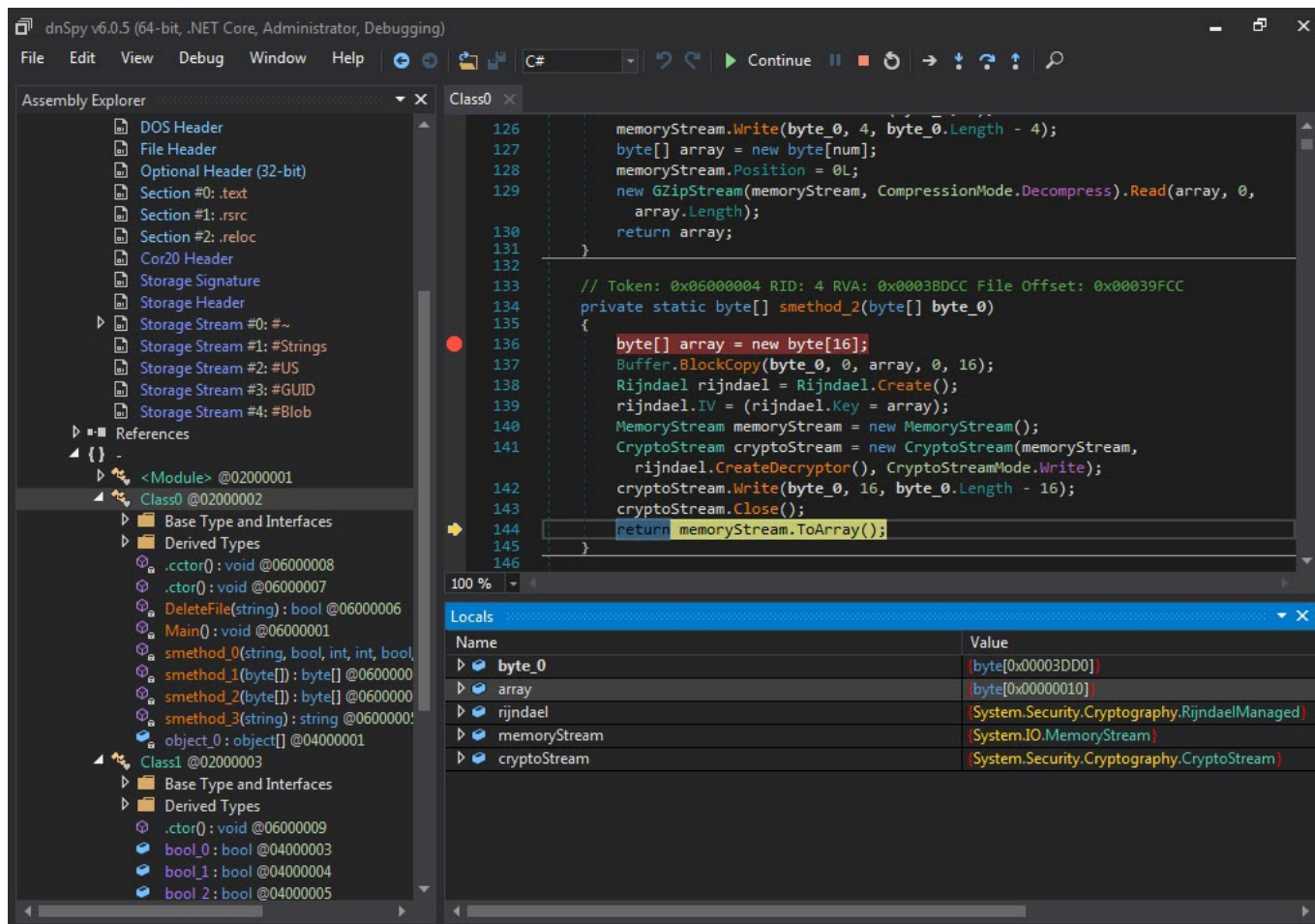
When I looked at the source code, the function `s_method2()` which decrypted the data encrypted with AES caught my attention. After a short time of analyzing the `Main()` function step by step with the dnSpy debugger, I noticed that the `s_method0()` function decrypted the encrypted data and saved it in the variable `byte_0` and then saves it to a file and runs it. After I learned this, I decided to save the data in the `byte_0` variable to disk and analyze it.



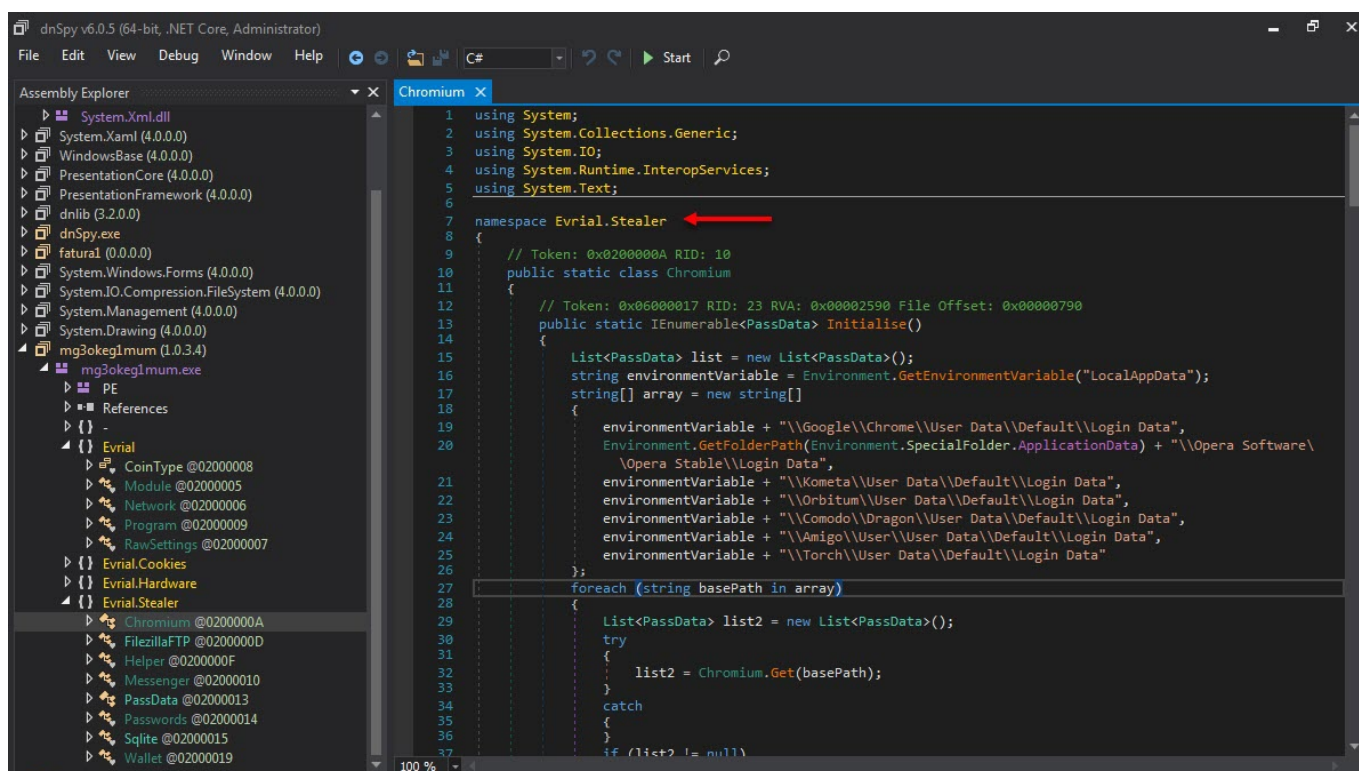




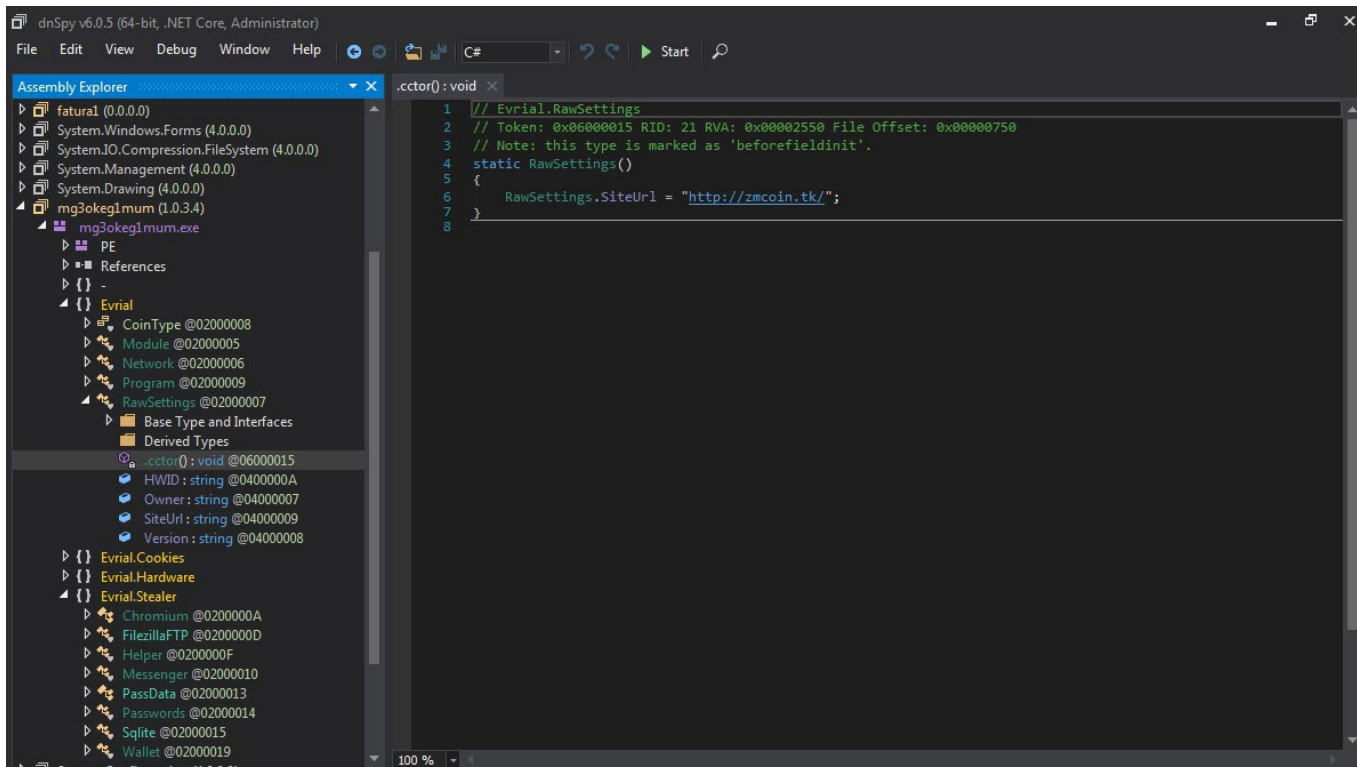




After analyzing this file with dnSpy and also the ANY.RUN sandbox system, I found that it was a cracked version of a password and crypto wallet stealer called Project Evrial.







## Static Discovering

3ytepucz.0.cs

3ytepucz.0.cs

Dropped from process

Look up on VirusTotal

Submit to analysis

Download

Mime: text/plain

Size: 7.16 Kb

### TrID - File Identifier

100% | Text - UTF-8 encoded

### Hashes

MD5 7B77E8328EB64C022998D9CEE8CEC489  
SHA1 1EDCCD24CFBD6D44FEF884281578751FA144D636  
SHA256 B94AA33FA57B612B354F6CB8AE38DBA34D1EC815877EAA472EDA511B29DC8EFB  
SSDEEP 96:JoF1V0TgU2AiGqwcprB0GaBd2DTIJ3EFYyILtBSJewheYeJdhKVRjcNvUSXSp+U:yP1FYyILWe5Y4gVRj\_

### PREVIEW

### HEX

```
Text
}

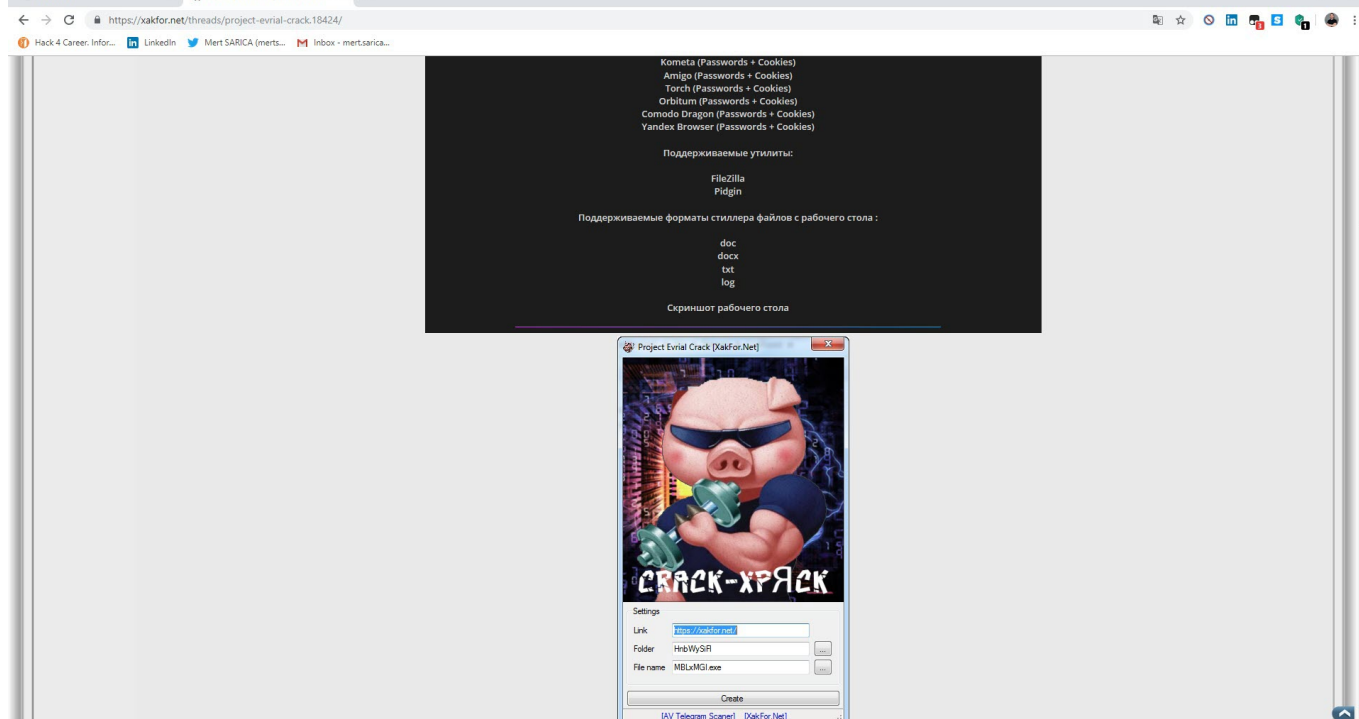
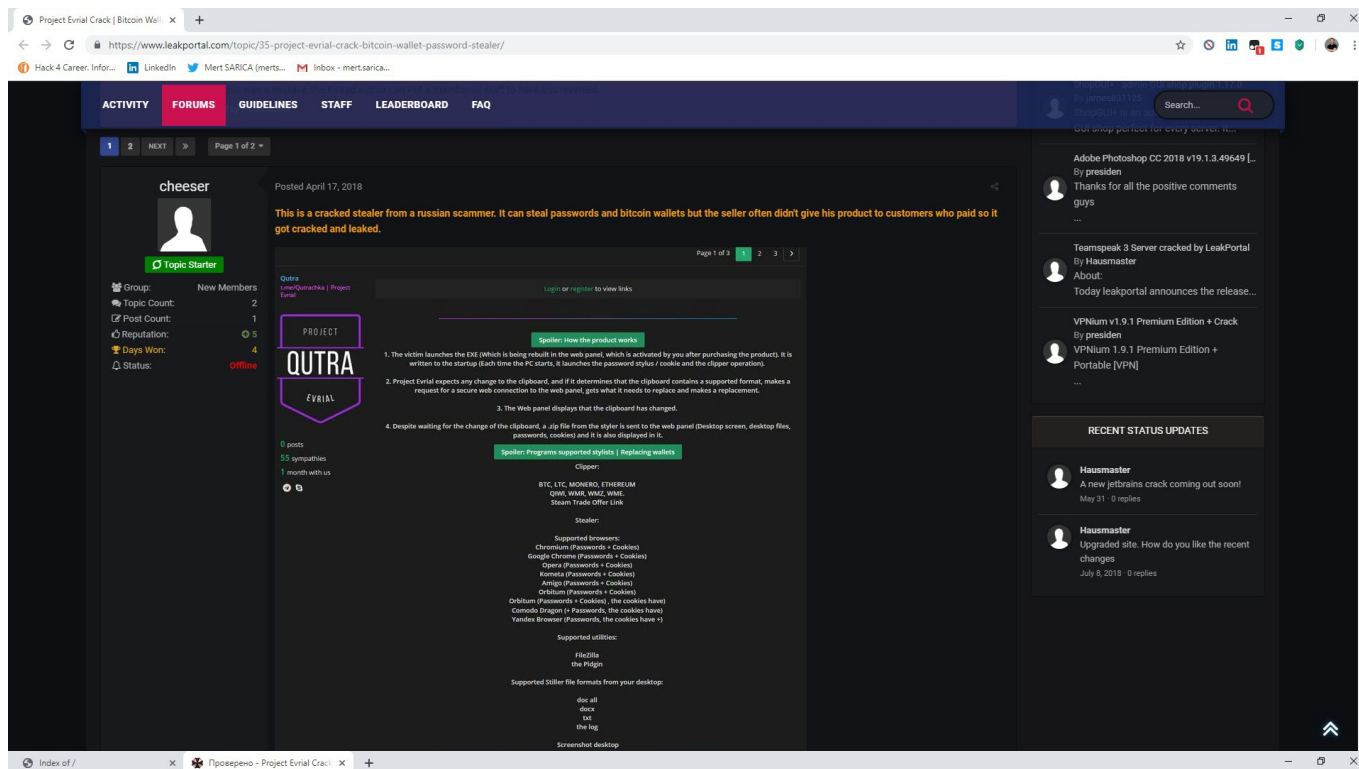
private static string text = "";

private static void Main(string[] args)
{
    RawSettings.Owner = "XakFor.Net";
    RawSettings.Version = "1.0.3";
    RawSettings.HWID = "EEEE5D54788042A7B542739BBC26CF4B";

    OnClipboardChange += ClipboardMonitor_OnClipboardChange;
    Start();
}

public static void ClipboardMonitor_OnClipboardChange(ClipboardFormat format, object data)
{
    try
    {
        if (format != ClipboardFormat.Text) return;
    }
}
```

Close



After the analysis, I found the command and control center's address (<http://zmcoin.tk>) and decided to visit it. With the directory browsing feature enabled, I was able to view the files stolen by the malware in a folder. When I sorted the files by date and downloaded the oldest file to examine it, I saw that the malicious person had first tested this malware on their own test system. Of course, this test system was not only used to test the malware but also for personal business, which resulted in a failure of OPSEC (Operations Security) as the malware had also stolen personal information such as name, surname, email address, etc. from the system. The

malicious person fell into the well he dug himself. :)

Index of /

Not secure | zmcoin.tk

Hack 4 Career. Inform... | LinkedIn | Mert SARICA (merts... | Inbox - mert.sarica...

Index of /

Name	Last modified	Size	Description
h/	2019-05-03 16:22	-	
files.zip	2019-07-04 15:27	1.2M	
files/	2019-07-23 03:57	-	
shuffler.php	2018-02-24 22:46	1.1K	
steal/	2019-07-24 22:59	-	
stealer/	2018-02-24 22:46	-	

Index of /files

Not secure | zmcoin.tk/files/

Hack 4 Career. Inform... | LinkedIn | Mert SARICA (merts... | Inbox - mert.sarica...

Index of /files

Name	Last modified	Size	Description
Parent Directory		-	
2aipms03x3.zip	2019-07-07 13:54	175K	
bdcsjartfh03.zip	2019-07-07 14:01	180K	
cgjksdibry0.zip	2019-07-12 21:27	18K	
cqzbalnbnwd.zip	2019-07-08 21:58	9.1K	
egzok2vnph4.zip	2019-07-08 20:21	15K	
gswi3ggrp3h.zip	2019-07-07 16:36	24K	
jdomwvtoqok1.zip	2019-07-23 03:57	27K	
lnldeocf2d5.zip	2019-07-06 19:49	218K	
m4tuckk3paxp.zip	2019-07-07 15:12	327K	
nd0a2g5yvc1a.zip	2019-07-03 15:23	213K	
o5mrnf0n1i.zip	2019-07-08 21:36	322K	
oasq5oorfw.zip	2019-07-07 15:25	100K	
qvexdyhtlgu.zip	2019-07-03 15:22	213K	
tmp/	2018-02-08 10:48	-	
rvcb8mm7jm2.zip	2019-07-06 15:12	1.0K	
upload.php	2018-02-24 22:46	4.0K	
yparawza2i3.zip	2019-07-07 14:01	208K	
xcuzvkd5fk.zip	2019-07-21 18:17	33K	



```
.txt - Notepad
File Edit Format View Help

Username:
Customer ID:
IP Address:
81.213.254.6
Language:
en
Disabled:
N
Created at:
2019-03-10 13:49:46
E-Mail:
First Name:
Last Name:
Country:
TR
Grid ID:
1
Avatar First Name:
Avatar Last Name:
Secret TIN:
Has traded:
N
Partner:
N
Grid Name:
SL
Grid Long Name:
Grid Currency:
SLL

An email containing information for activating your acco
```

As it can be seen, it is possible to obtain important information about cyber operations and the people who carry them out, thanks to malicious actors who do not pay attention to operational security.

Hope to see you in the following articles.