

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%2520fs%253A2019-01-01T00%253A00%252B%2520submitter%253ATR%2520Fatura/files

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

	FILES 6	7z	pdf	autoaction	file-embedded	js-embedded	peexe	assembly	cve-2008-2992	exploit	rar	zip	contains-pe
1ee11857672c87ed09b9ce0891bf1c08127ae357ce9af1d03eca24a13829224e	ÖDEME SIPARIŞLARI İÇİN Fatura.7z	7 / 54											
c3551f4ca271b933d0eb96ba1ba6240f1f72202523c44079101490a5aa61aad4	Fatura.pdf	9 / 55											
a7c6bbeb414420a59f3b84199f613a3ed3d6ed065293320dd38c0a8fd64e310	Fatura_001.pdf	30 / 54											
d25656db3d159dd97fd6c34b0d0d74e355a362c6442e5ec941703e9cafcec875	fatura1.exe	50 / 70											
1b0c9588f3aee2b033b3158725f2641851d82cb8b0183c98050ed9a02eebda	Downloads.zip	1 / 56											
a58012fd8111bb5a3f461fdded40e7727dd73bfb4702f76ed7f3d5349bd265ed	fatura.rar	1 / 58											

https://www.virustotal.com/gui/file/d25656db3d159dd97fd6c34b0d0d74e355a362c6442e5ec941703e9cafcec875/detection

d25656db3d159dd97fd6c34b0d0d74e355a362c6442e5ec941703e9cafcec875

50 / 70

Community Score

452.5 KB Size

2019-07-12 21:27:10 UTC
15 days ago

DETECTION

DETAILS

RELATIONS

BEHAVIOR

CONTENT

SUBMISSIONS

COMMUNITY

Vendor	Detection Name	Category	Confidence
Acronis	Suspicious	Ad-Aware	Gen.Variant.Razy.261495
AegisLab	Trojan.Win32.Agent.4lc	Allibaba	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.

Adobe Acrobat Reader DC

File Edit View Window Help

Home Tools

1 / 2 80.7%

Export PDF

Adobe Export PDF

Convert PDF Files to Word or Excel Online

Select PDF File

turkcellfat...piyodas.pdf

Convert to

Microsoft Word (*.docx)

Document Language:

English (U.S.) Change

Convert

Convert and edit PDFs with Acrobat Pro DC

Start Free Trial

FATURA NO 0012019077396233

0000001888110110005

Yandaki barkodu telefonunuzdaki barkod okuyucuyla okutup hattınızla ilgili birçok işlemi yapabilirsiniz.

e-Arşiv Fatura

Fatura Düzenleme Tarihi : 10 Haziran 2019

Fatura Düzenleme Zamanı : 00:00

Fatura Dönemi : 10 Mayıs-09 Haziran

Telefon No : Yeni Genç Tarife

Tarife

Son Ödeme Tarihi : 25 Haziran 2019

Ödenecek Tutar : 232,60 TL

Bulunmuyor

FATURA ÖZETİ

TÜRKİYE'NİN İNTERNET KAZAND

İLK ALIŞVERİŞ KAR'

MAĞAZALARINDA VE .COM.TR

45,73

95,88

86,04

2,62

2,32

ÖDENECEK TUTAR 232,60 TL

232,60 TL'lik faturanızın 44,51 TL'si sizin adınıza devlete iletilmektedir.

Vergi Dahil Yalnız - İKİYÜZOTUZİKİTALTIMIŞKR

Bilgilendirme

Bu içeriği görüntüledikten sonra avukatlarımıza dönüş gerçekleştirmeniz gerekmektedir. Lütfen incelemeleriniz tamamlandıktan sonra tarafımıza dönüş yapınız.

OK

Start

6026929091575808

Search 6026929091575808

Organize Open Share with New folder

Favorites

Desktop

Downloads

Recent Places

Libraries

Documents

Music

Pictures

Videos

Computer

Local Disk (C:)

Network

Name

Date modified

d25656db3d159dd97fdc634b0d0d74e355a362c6442e5ec941703e9cafcec875.exe 28.07.2019 13:40

d25656db3d159dd97fdc634b0d0d74e355a362c6442e5ec941703e9cafcec875.exe 28.07.2019 13:56

RDG Packer Detector v0.7.6 Vx Edition 2017

C:\Users\Mert\Desktop\6026929091575808\d25656db3d159c x32 Open

Microsoft Visual C# / Basic .NET

Compiler

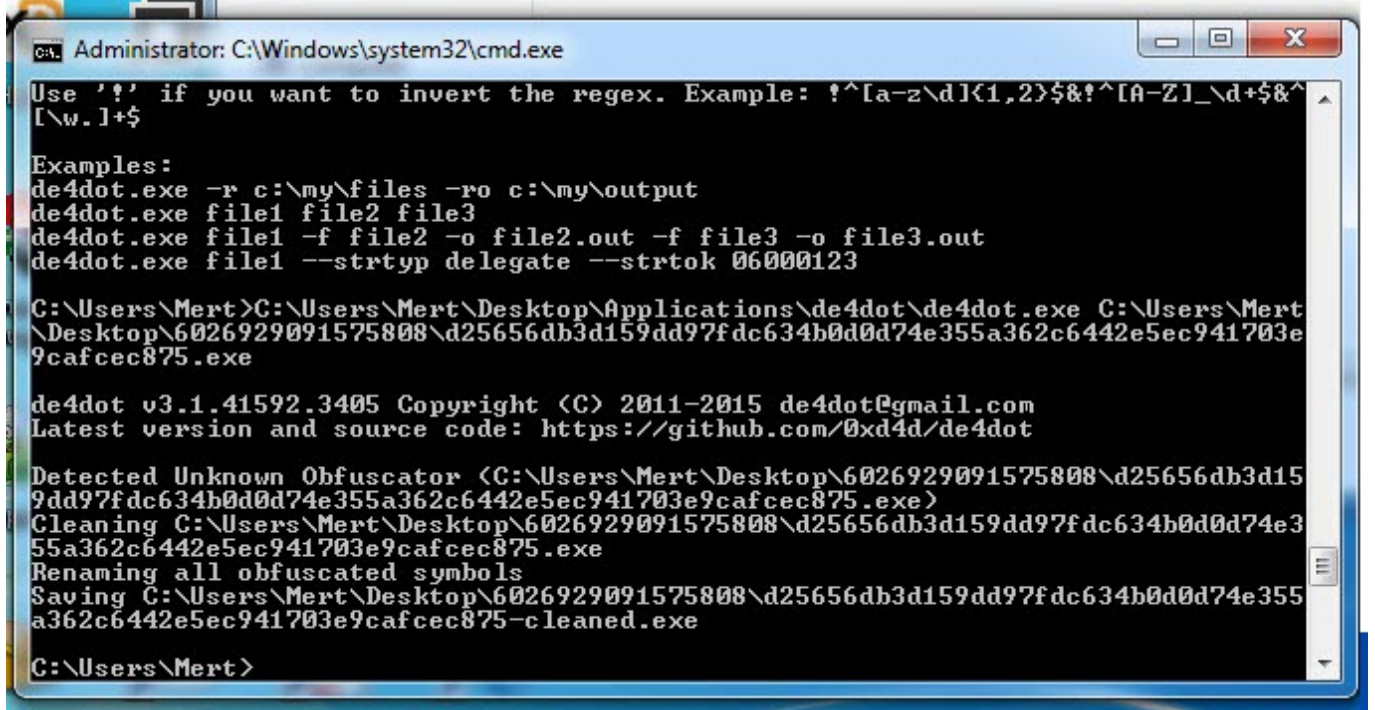
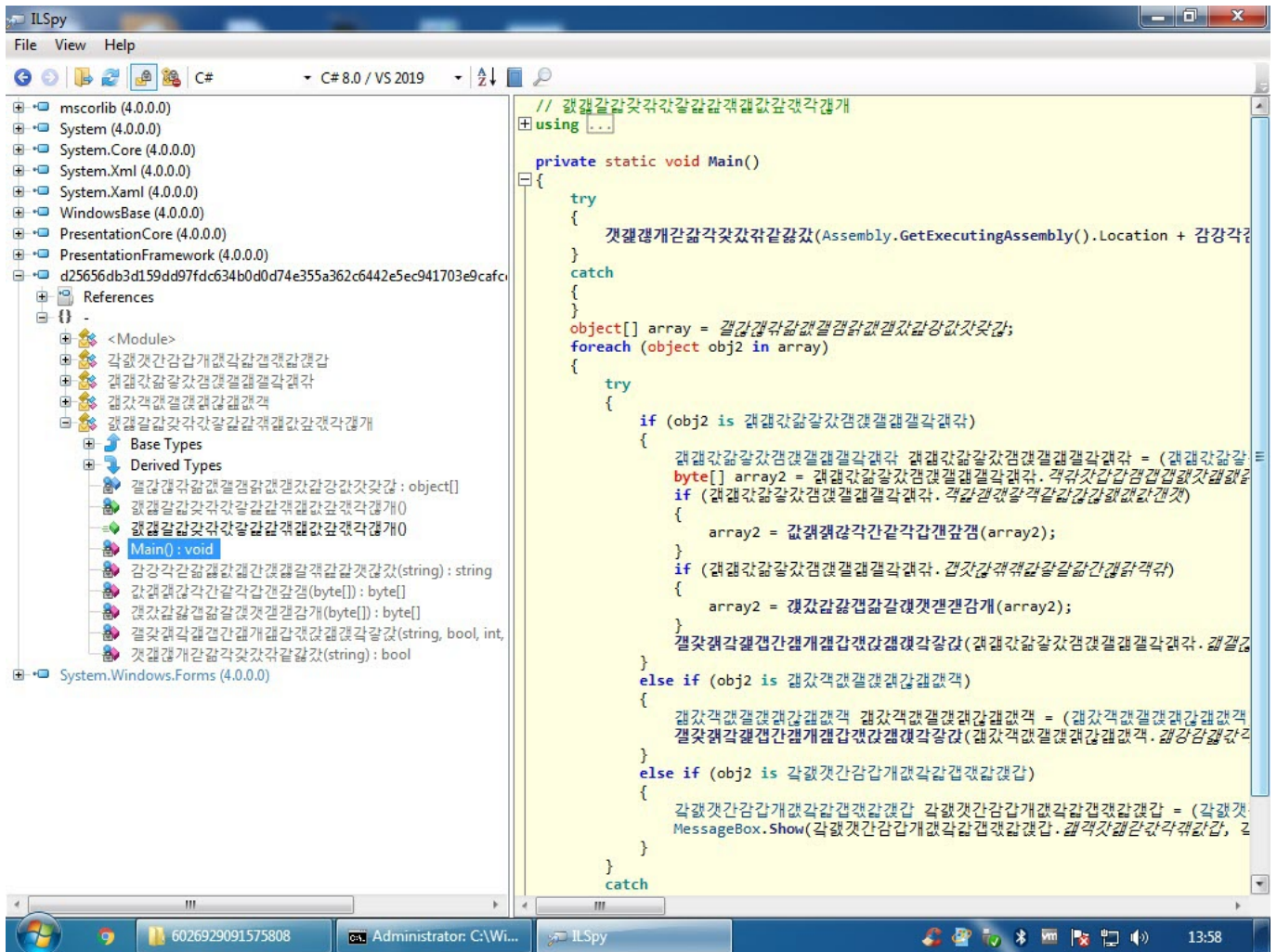
Nada Detected Possible

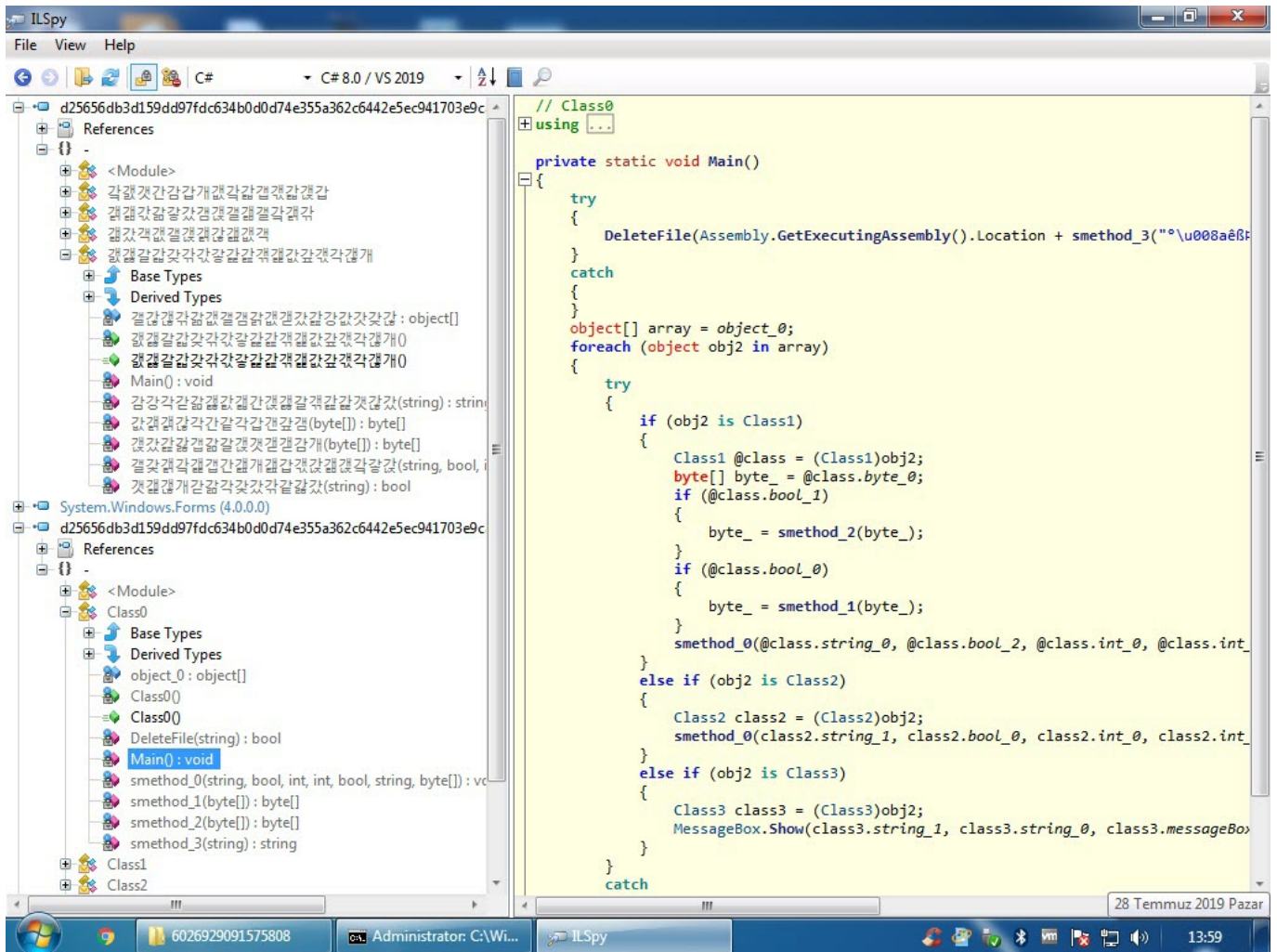
Contact: Ent

File scanned in , Seg. M-A M-B Detect

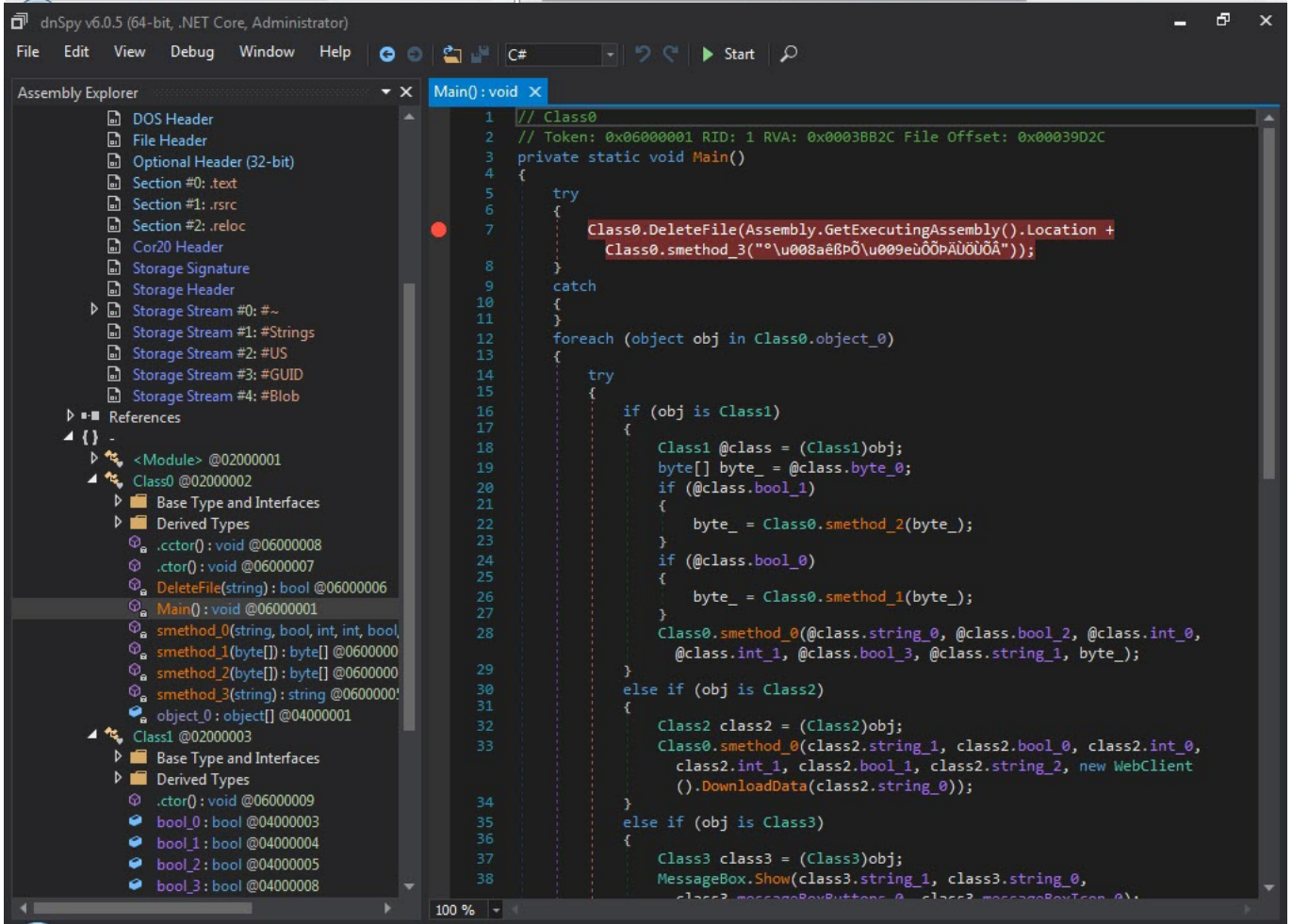
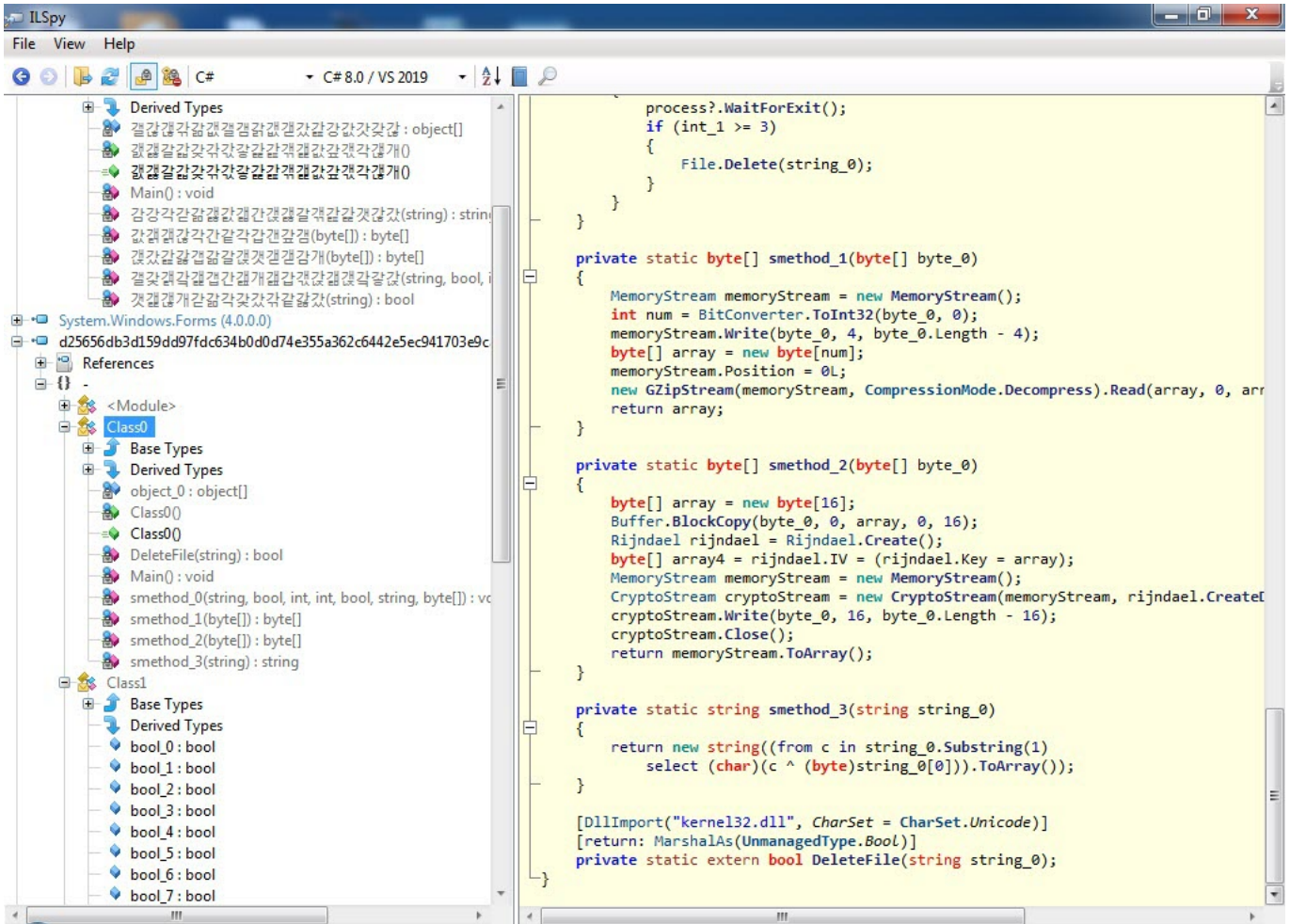
d25656db3d159dd97fdc634b0d0d74e35... Date modified: 28.07.2019 13:40 Date created: 28.07.2019 13:50

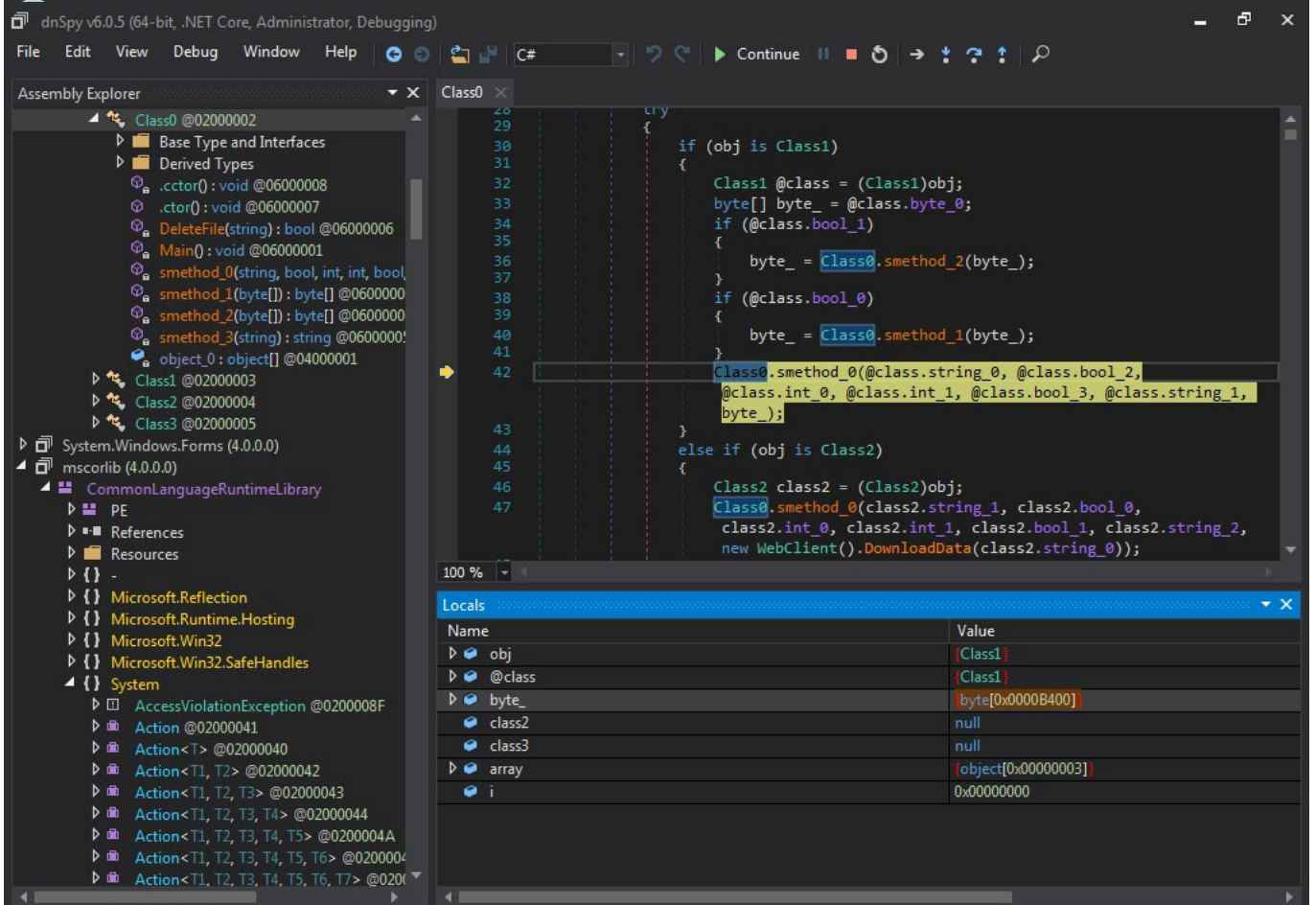
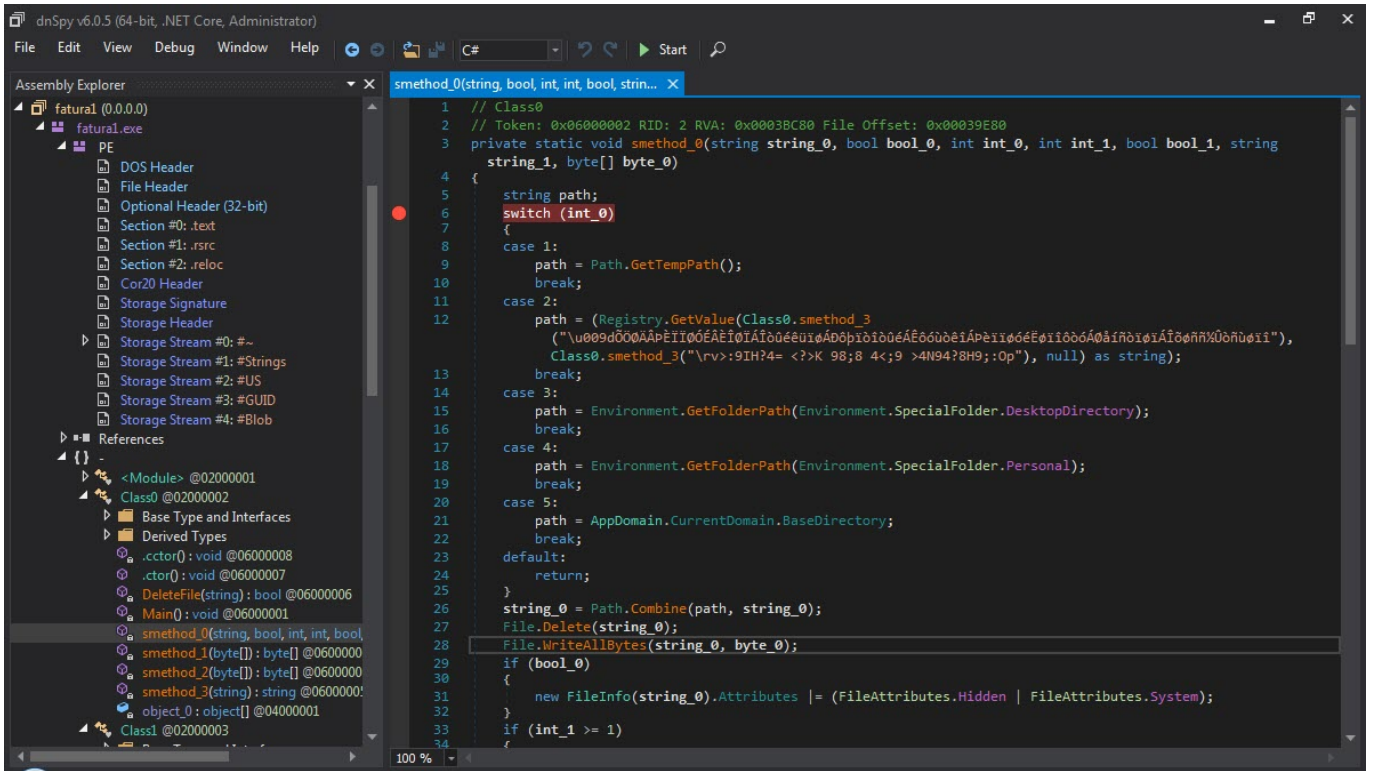
Application Size: 452 KB

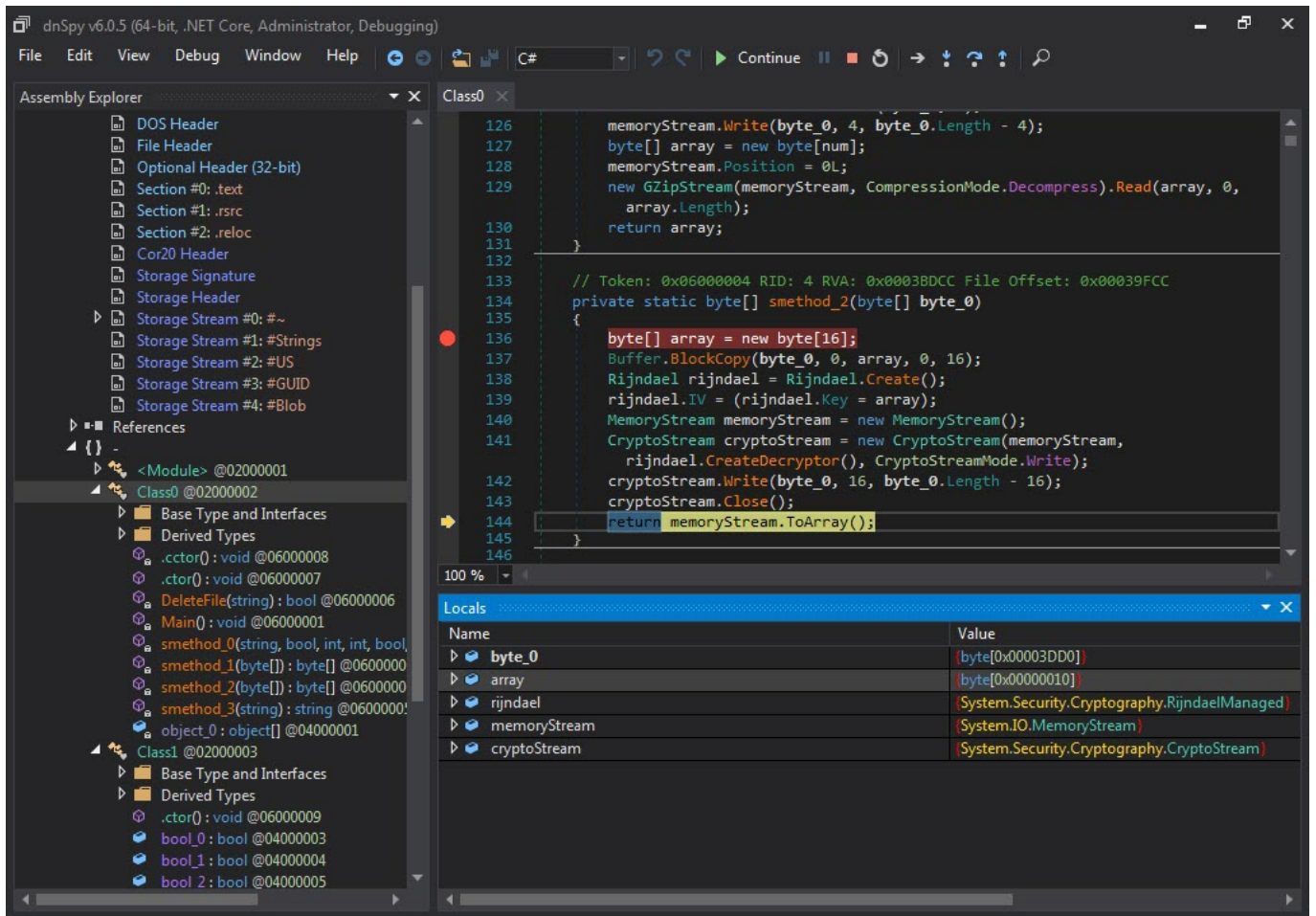




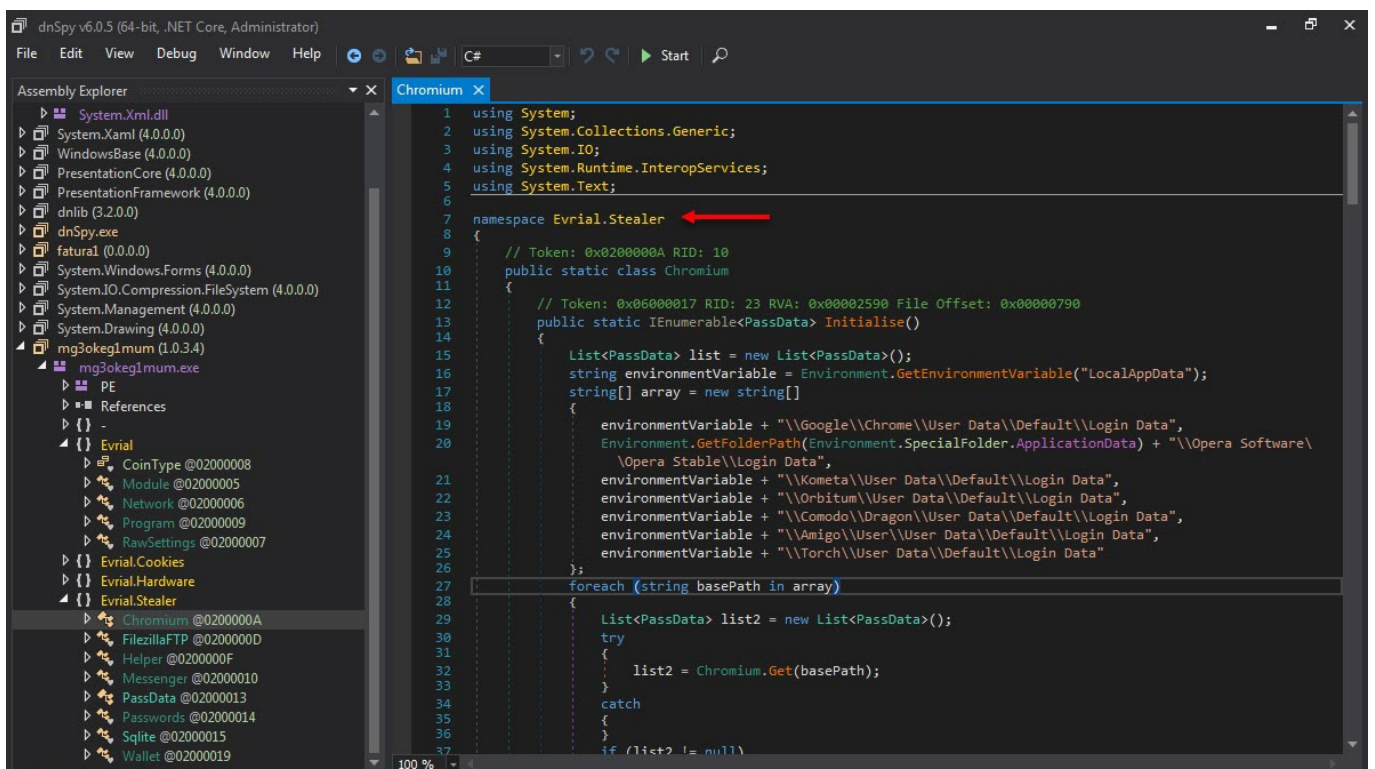
When I looked at the source code, the function `s_method2()` which decrypted the data encrypted with AES caught my attention. After a short time of analyzing the `Main()` function step by step with the dnSpy debugger, I noticed that the `s_method0()` function decrypted the encrypted data and saved it 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.



dnSpy v6.0.5 (64-bit, .NET Core, Administrator)

File Edit View Debug Window Help

Assembly Explorer

- fatural (0.0.0)
- System.Windows.Forms (4.0.0.0)
- System.IO.Compression.FileSystem (4.0.0.0)
- System.Management (4.0.0.0)
- System.Drawing (4.0.0.0)
- mg3okeg1mum (1.0.3.4)
 - mg3okeg1mum.exe
 - PE
 - References
 -
 - Evrial
 - CoinType @02000008
 - Module @02000005
 - Network @02000006
 - Program @02000009
 - RawSettings @02000007
 - Base Type and Interfaces
 - Derived Types
 - .cctor():void @06000015
 - HWID: string @0400000A
 - Owner: string @04000007
 - SiteUrl: string @04000009
 - Version: string @04000008
 - Evrial.Cookies
 - Evrial.Hardware
 - Evrial.Stealer
 - Chromium @0200000A
 - FilezillaFTP @0200000D
 - Helper @0200000F
 - Messenger @02000010
 - PassData @02000013
 - Passwords @02000014
 - SQLite @02000015
 - Wallet @02000019

```

1 // Evrial.RawSettings
2 // Token: 0x06000015 RID: 21 RVA: 0x0002550 File Offset: 0x0000750
3 // Note: this type is marked as 'beforefieldinit'.
4 static RawSettings()
5 {
6     RawSettings.SiteUrl = "http://zmcoin.tk/";
7 }
8

```

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 7B77E8328EB64C022098D9CEE8CEC489
 SHA1 1EDDC24CFBD6D44FEF884281578751FA144D636
 SHA256 B94AA33FA57B612B354F6C88AE38DBA34D1EC815877EAAA472EDA511B29DC8EFB
 SSDEEP 96:JoF1V0TgU2AiGqwcP8GaBd2DTIJ3EFYy1LtB5JewheYeJdhKVRjcnvUSXSp+U:yP1FYy1LWe5Y4gVRj_

PREVIEW

HEX

```

}

private static string text = "";

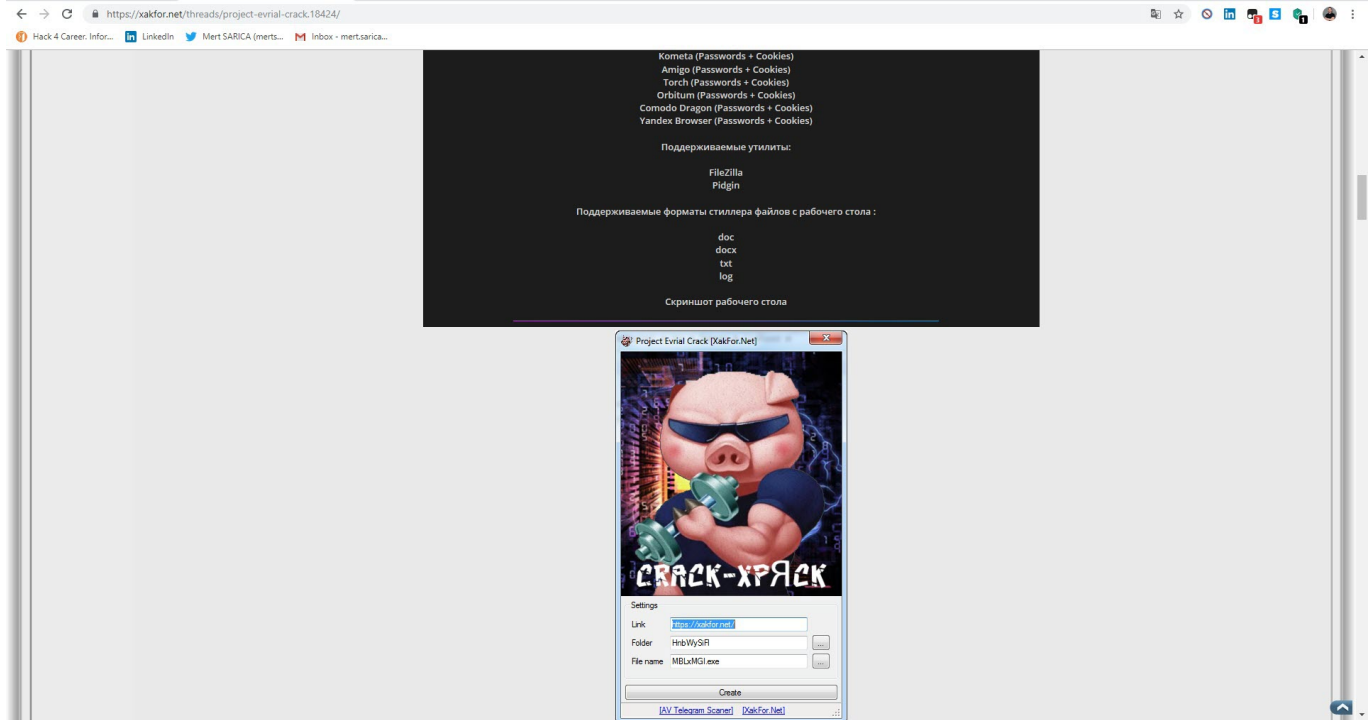
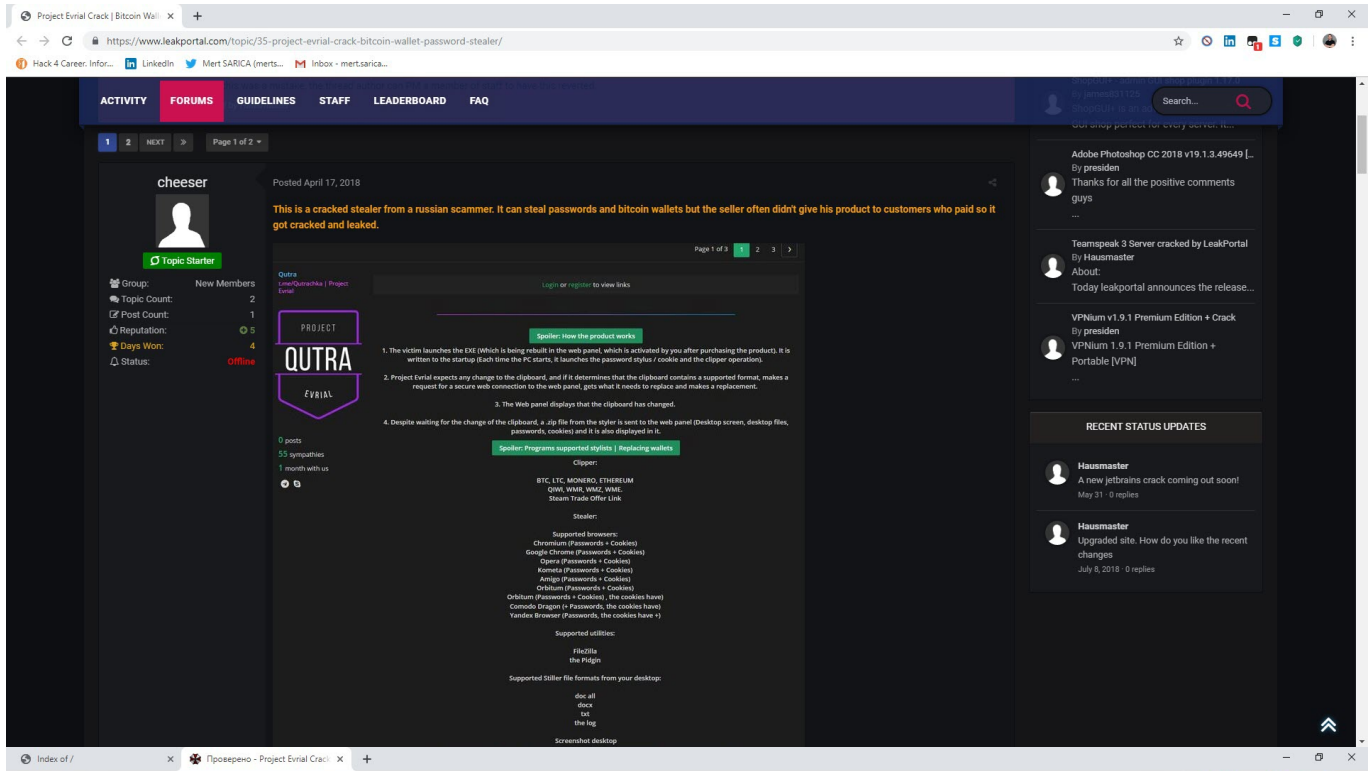
private static void Main(string[] args)
{
    RawSettings.Owner = "XakFor.Net";
    RawSettings.Version = "1.0.3";
    RawSettings.HWID = "EEEE5D54788042A7B542739BBC26CF4B";

    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. :)

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	-	

Name	Last modified	Size	Description
Parent Directory		-	
2aipms03z2.zip	2019-07-07 13:54	175K	
bdsjartfh03.zip	2019-07-07 14:01	180K	
c9jksdibry0.zip	2019-07-12 21:27	18K	
cqzbalabwd.zip	2019-07-08 21:58	9.1K	
egzok2vnpht.zip	2019-07-08 20:21	15K	
gswi3agrp3h.zip	2019-07-07 16:36	24K	
jdomwtoqok1.zip	2019-07-23 03:57	27K	
hndecf2d5.zip	2019-07-06 19:49	218K	
m4uckk3paxp.zip	2019-07-07 15:12	327K	
nd0a2s5yw1a.zip	2019-07-03 15:23	213K	
o5mrnf0n1i.zip	2019-07-08 21:36	322K	
osq5oorfhw.zip	2019-07-07 15:25	100K	
qvexhvhflgw.zip	2019-07-03 15:22	213K	
tmp/	2018-02-08 10:48	-	
rvc8mm7jm2.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	
xucizvkd5fk.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.