

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 çođunluklukla 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), gerçekleştirilen operasyona dair kritik bilgilerin korunarak karşı istihbarat birimleri tarafından ele geçirilmesini engellemektir.

2-4 Ekim 2019 tarihinde Londra’da katıldıđım Virus Bulletin etkinliđinde Kaspersky tarafından gerçekleştirilen 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 yüklö 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 yüklö sistemden alıp, analiz edebilmiřti.

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

← → ↻ <https://www.virustotal.com/gui/search/positives%25A1%252B%2520f%253A2019-01-01T00%253A00%252B%2520submitter%253A%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 ÖDEME SİPARİŞLERİ İÇİN Fatura.7z	7 / 54	249.59 KB	2019-07-24 13:36:00	2019-07-24 13:36:00	1
☐	c3551f4ca271b933d0eb96ba1ba6240f1f72202523c44079101490a5aa61aad4 Fatura.pdf	9 / 55	4.71 MB	2019-07-16 13:06:38	2019-07-16 13:06:38	1
☐	a7cf65beb414420a5f9f3b84199f613a3ed3d6e06529320d38c0a8fd64e310 Fatura_001.pdf	30 / 54	7.29 KB	2019-07-16 07:06:21	2019-07-16 07:06:21	1
☐	d25656db3d159dd97fd634b0d0d74e355a362c6442e5ec941703e9cafcec875 fatura1.exe	50 / 70	452.5 KB	2019-07-07 13:55:25	2019-07-12 21:27:10	2
☐	1b0c9588f3aee2b033b3158725f2641851d82cb8b0183c98050ed9a02eebda Downloads.zip	1 / 56	28.46 MB	2019-07-10 06:36:42	2019-07-10 06:36:42	1
☐	a58012fd8111bb5a3f461fdde40e7727dd73bfb4702f76ed7f3d5349bd265ed fatura.rar	1 / 58	639.64 KB	2019-07-03 08:57:06	2019-07-03 08:57:06	1

← → ↻ <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
fatura1.exe

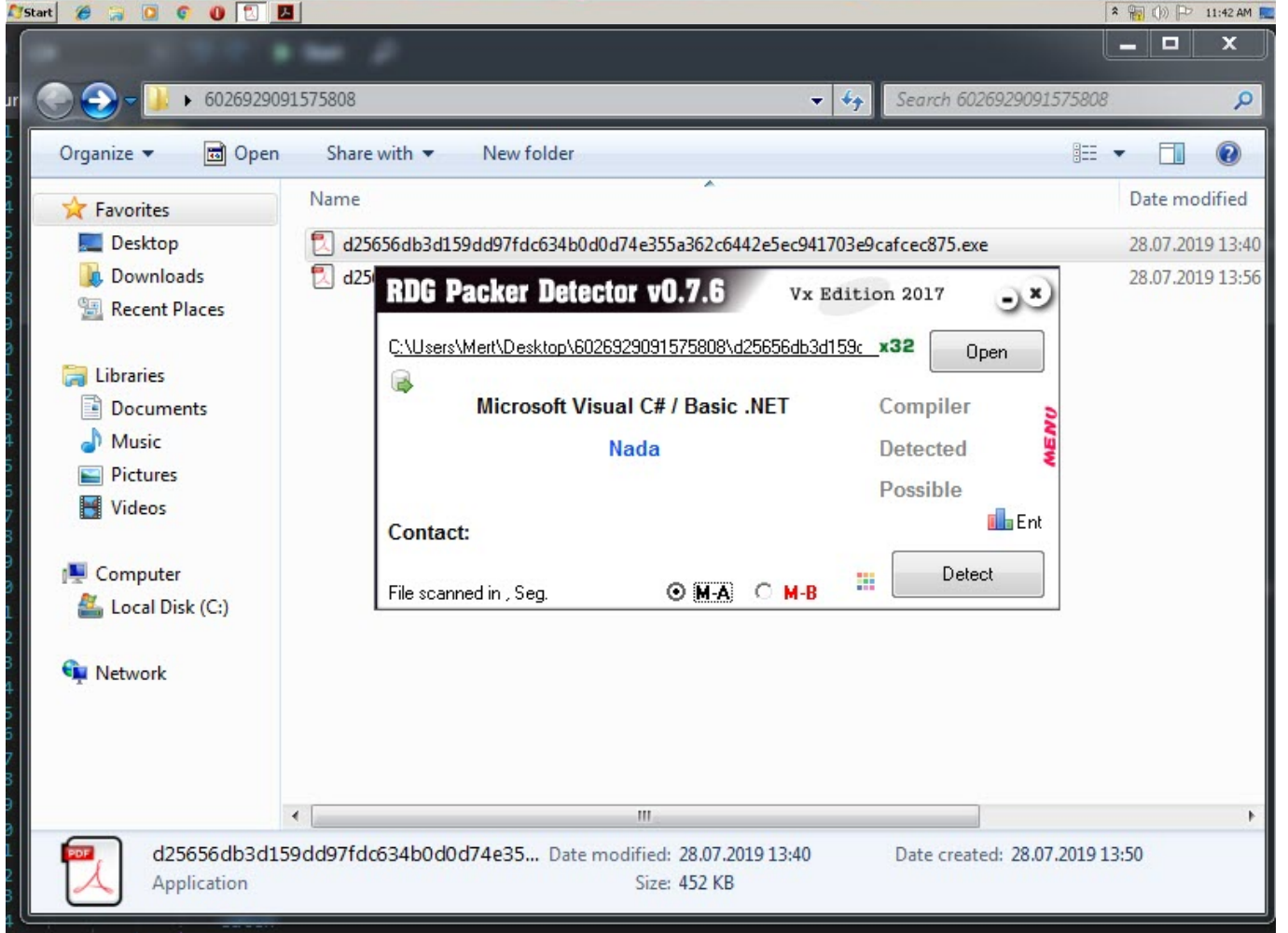
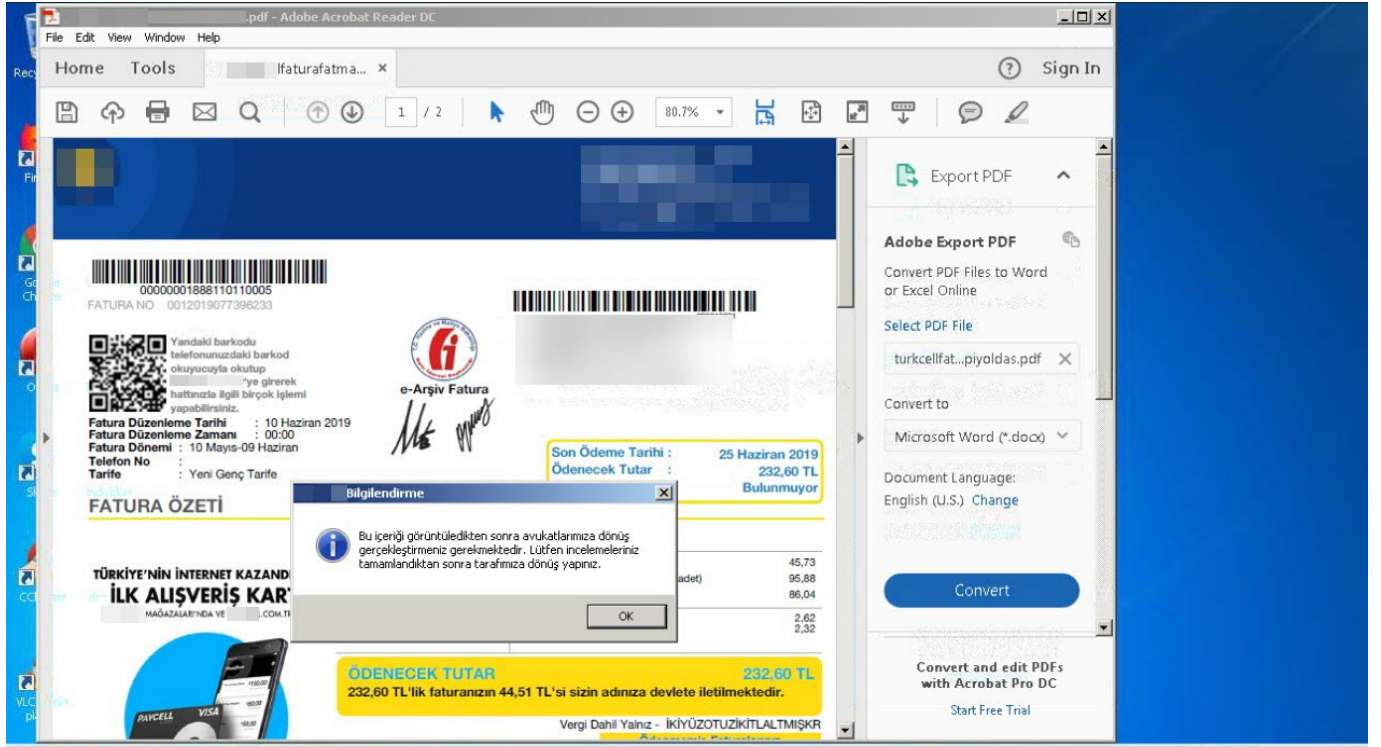
452.5 KB Size
2019-07-12 21:27:10 UTC
15 days ago

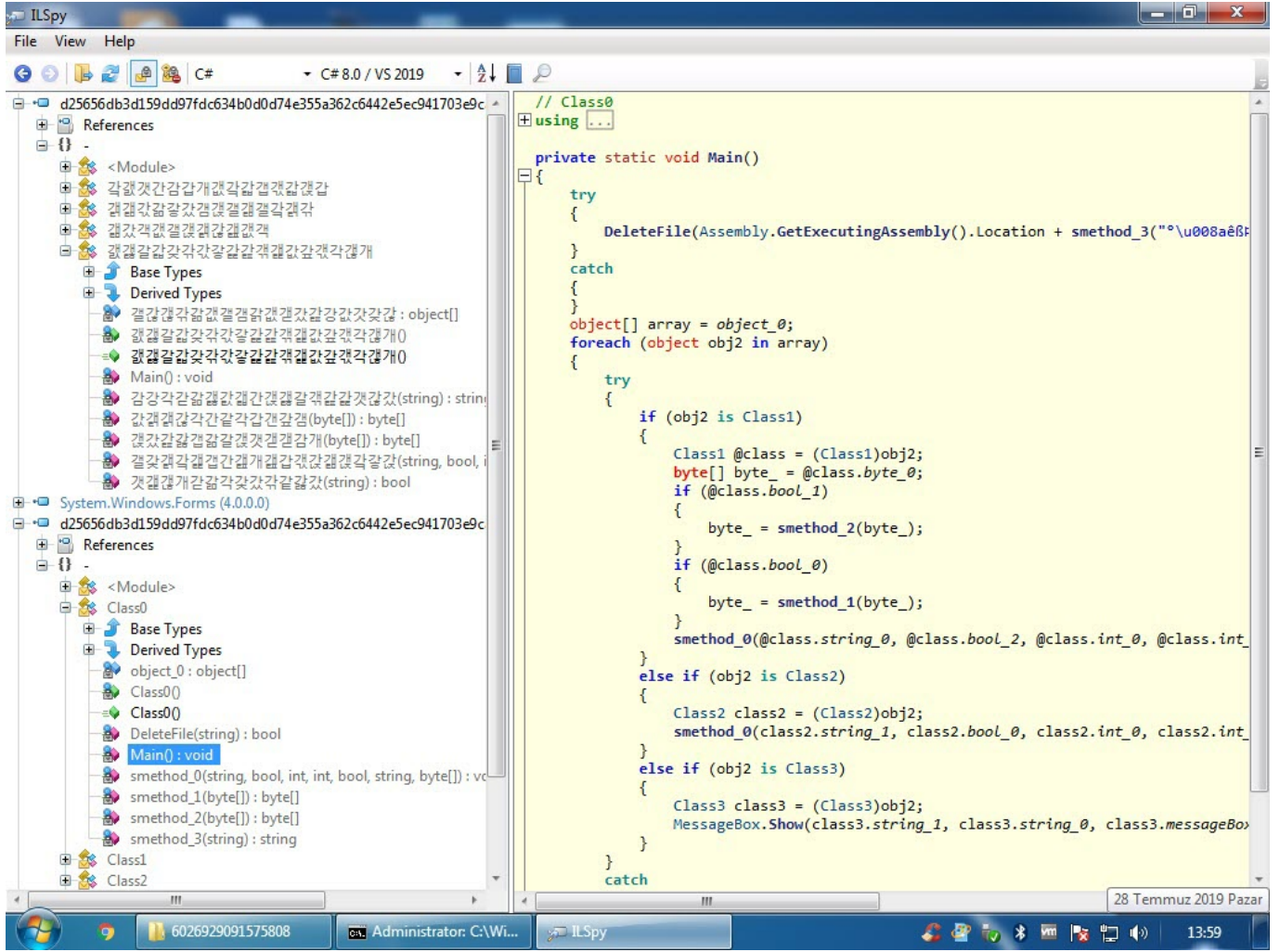
EXE

Community Score

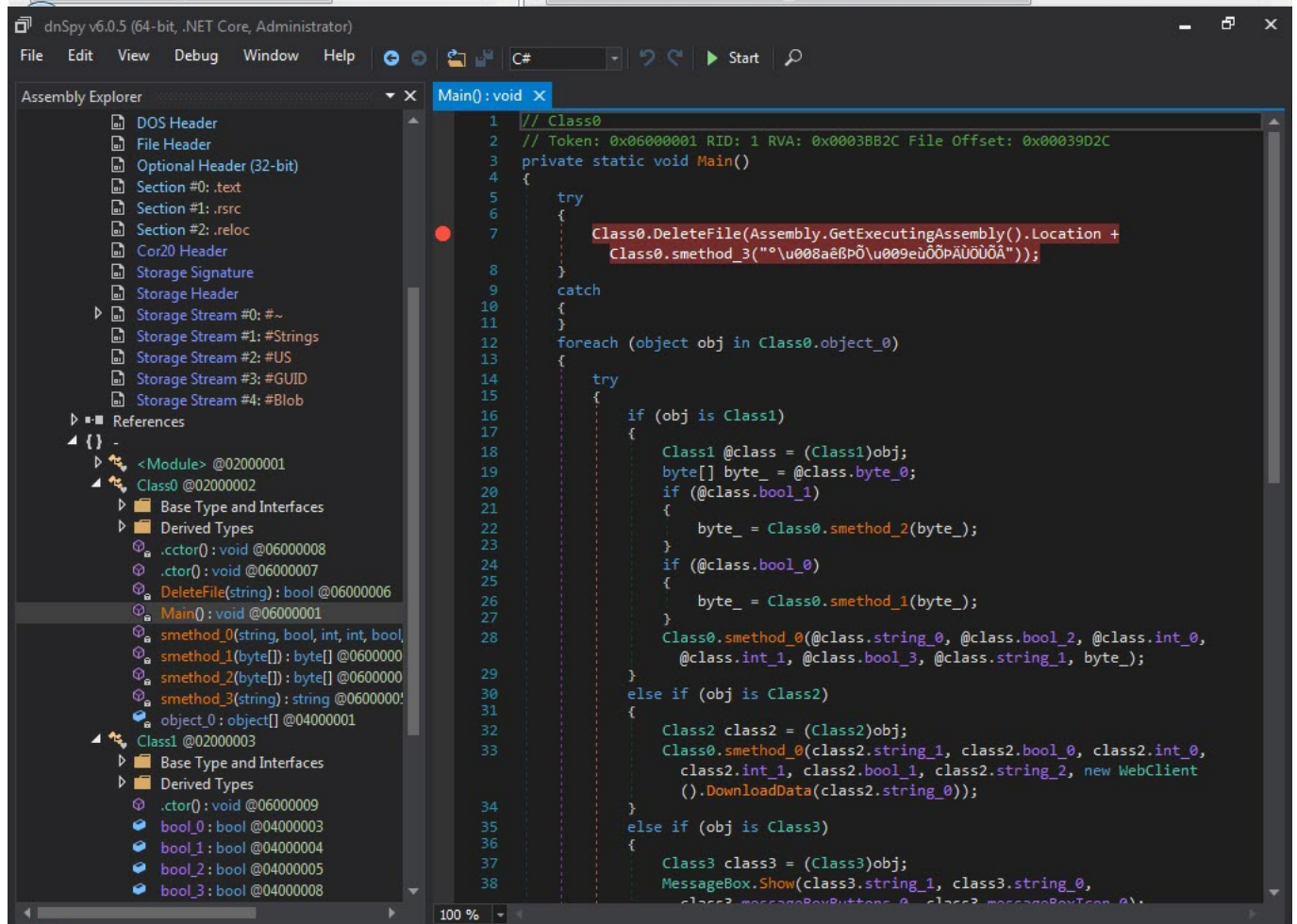
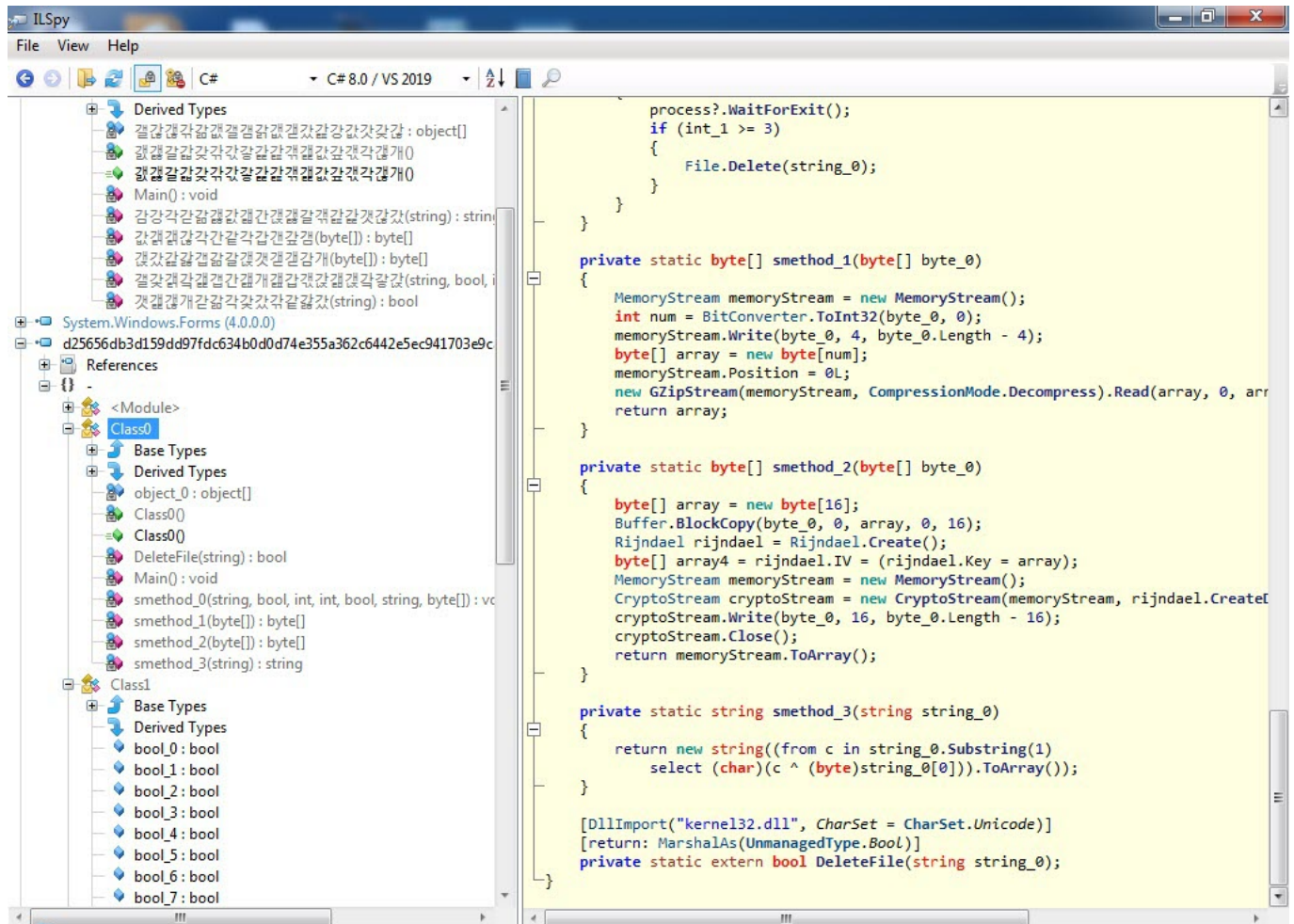
DETECTION	DETAILS	RELATIONS	BEHAVIOR	CONTENT	SUBMISSIONS	COMMUNITY
2019-07-12T21:27:10						
Acronis	⚠ Suspicious			Ad-Aware	⚠ Gen.Variant.Razy.261495	
AegisLab	⚠ Trojan.Win32.Agent.4lc			Alibaba	⚠ Trojan.MSIL/Agent.433c9bea	
ALYac	⚠ Gen.Variant.Razy.261495			Antiy-AVL	⚠ Trojan/Win32.Agent	
SecureAge 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.DOZltr	

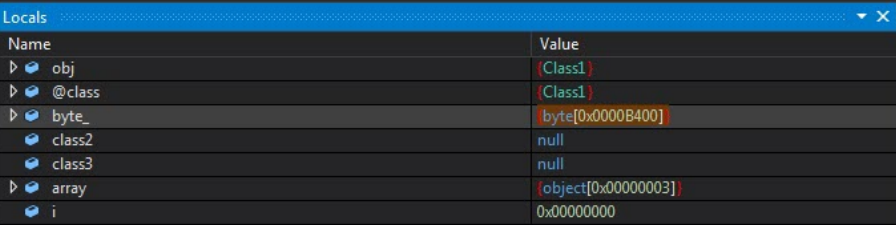
fatura1.exe isimli zararlı yazılımı analiz sistemimde çalıştırdığımda karşıma sahte bir telefon faturası ve uyarı mesajı çıktı. fatura1.exe dosyasını RDG Packer Detector aracı ile incelediğimde aracın C# programlama dili ile geliştirildiğini öğrendim. ILSpy kaynak kodu çeviricisi ile kodlara kısaca göz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

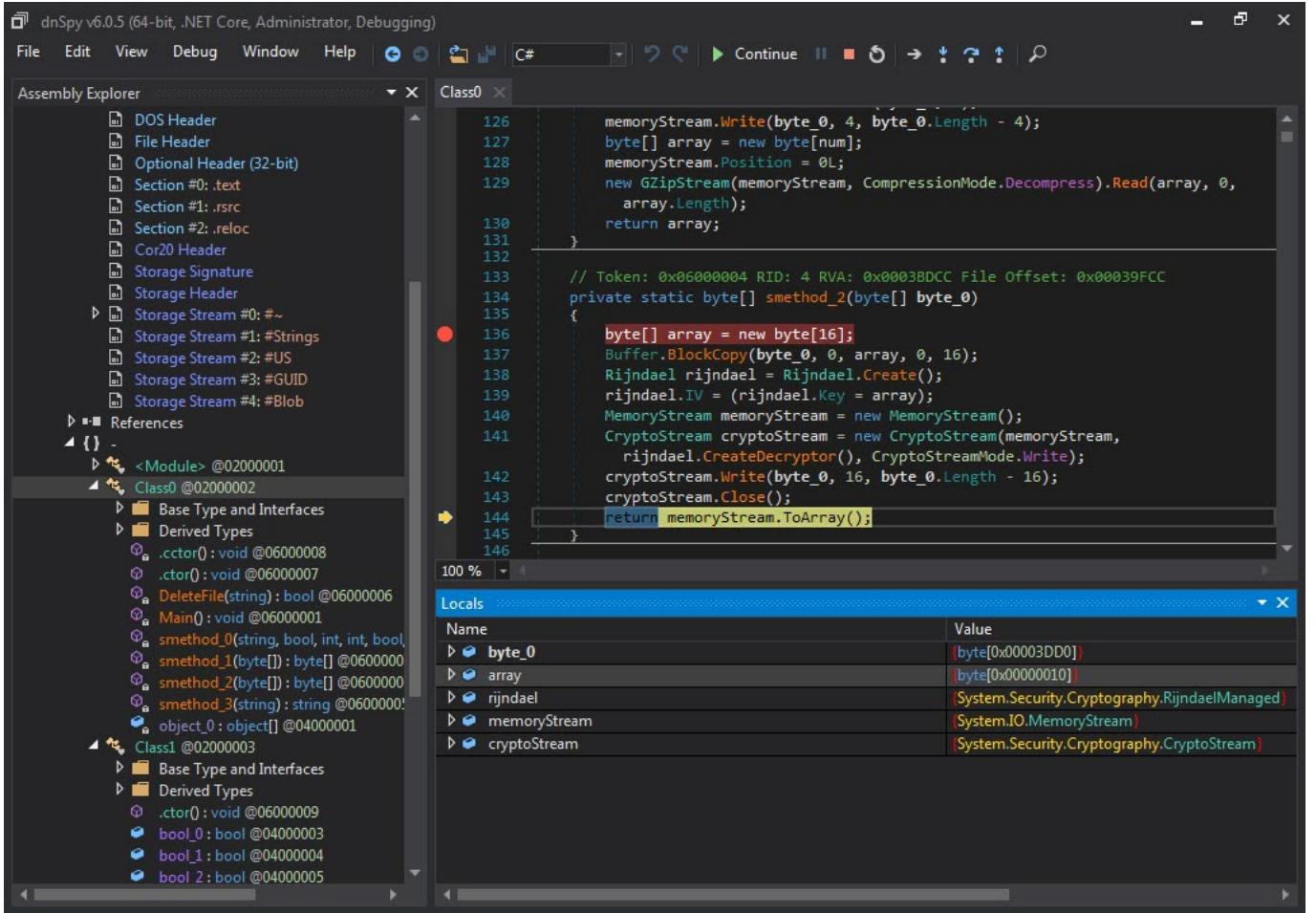




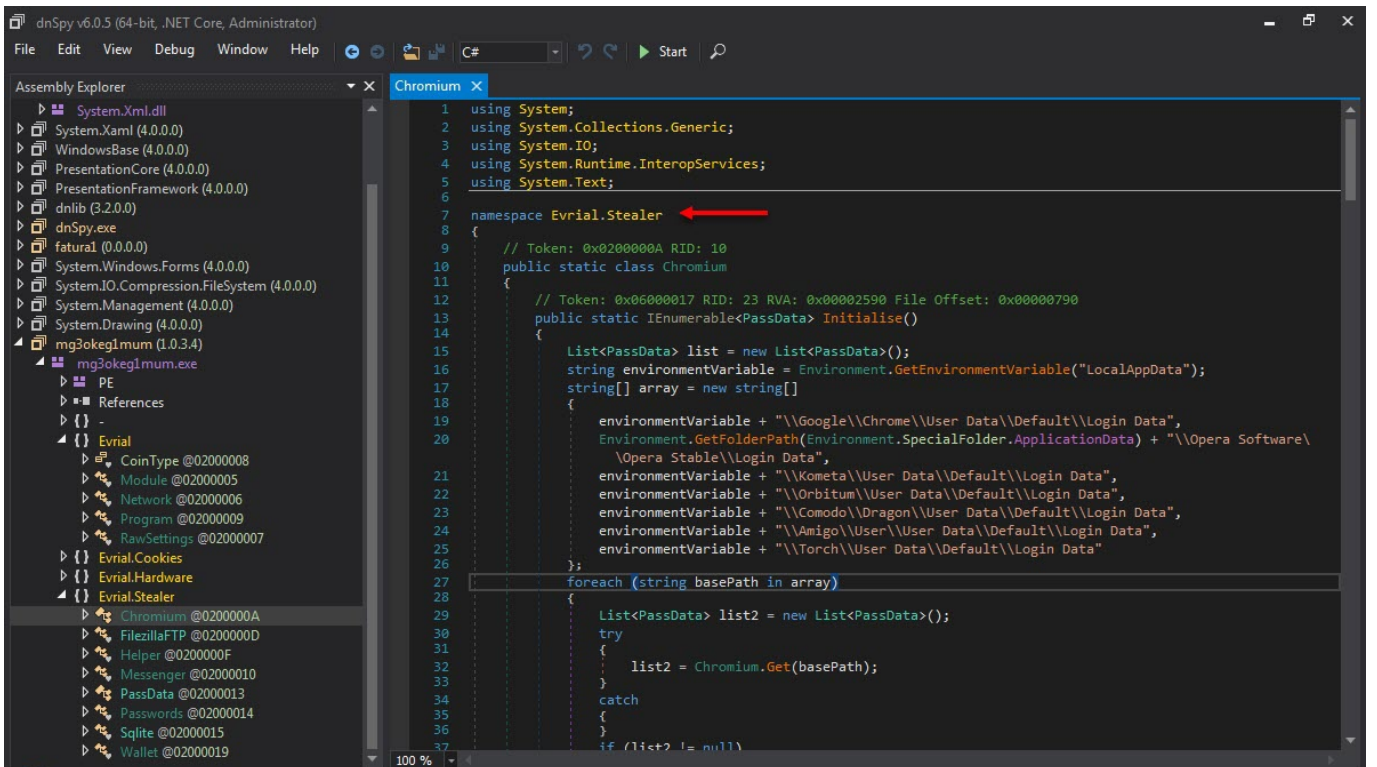
Kaynak koduna göz attığımda AES ile şifrelenmiş olan verileri çözen `s_method2()` fonksiyonu dikkatimi çekti. dnSpy hata ayıklayıcısı ile `Main()` fonksiyonunu adım adım analiz etmeye başladıktan kısa bir süre sonra `s_method0()` fonksiyonunun şifrelenmiş verileri çözüp `byte_0` değişkenine atadıktan sonra bunu bir dosyaya kaydedip çalıştırdığını farkettilim. Bunu öğrendikten sonra `byte_0` değişkeninde yer alan veriyi diske kaydedip analiz etmeye karar verdim.

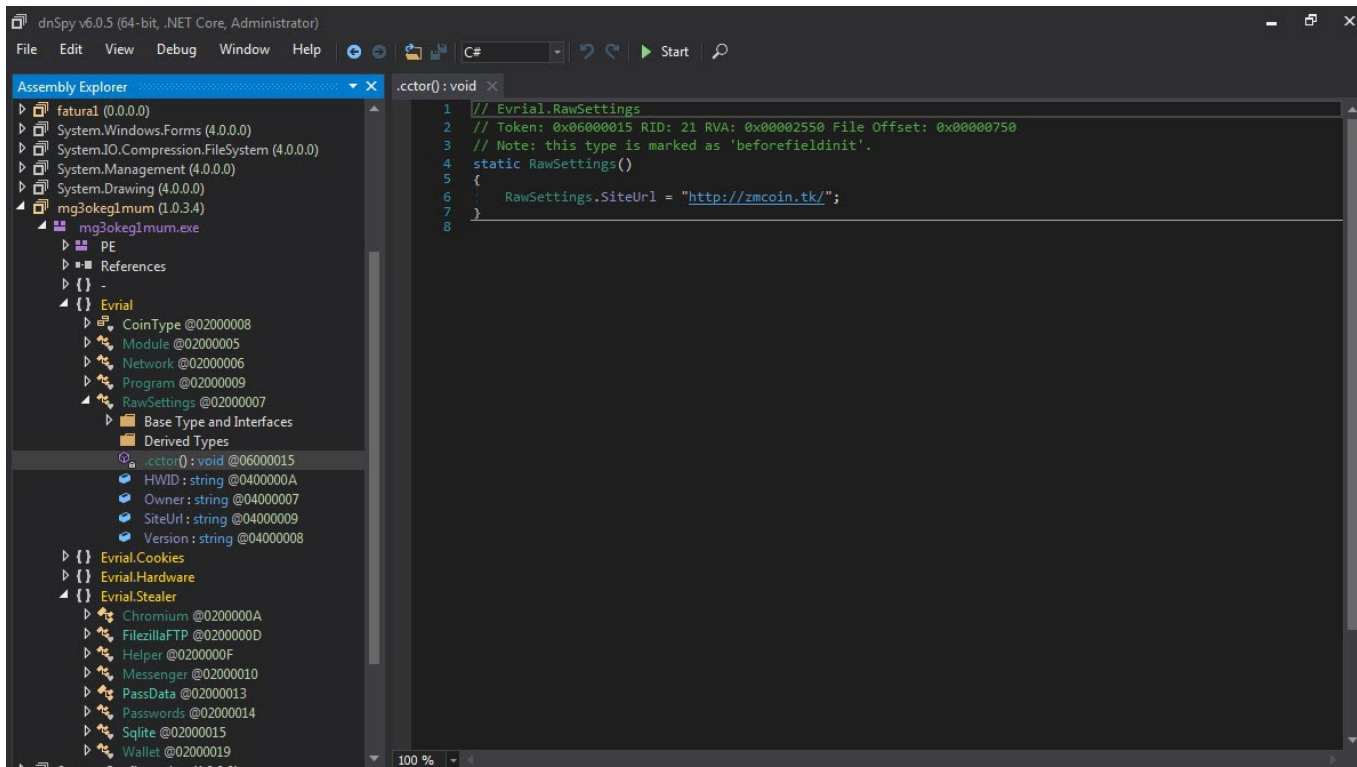






Bu dosyayı da dnSpy ve ayrıca ANY.RUN kum havuzu sistemi ile analiz ettiğimde Project Evrial isimli bir parola ve kripto para cüzdanı hırsızının (stealer) kırılmış sürümü (cracked) olduğunu gördüm.





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
}

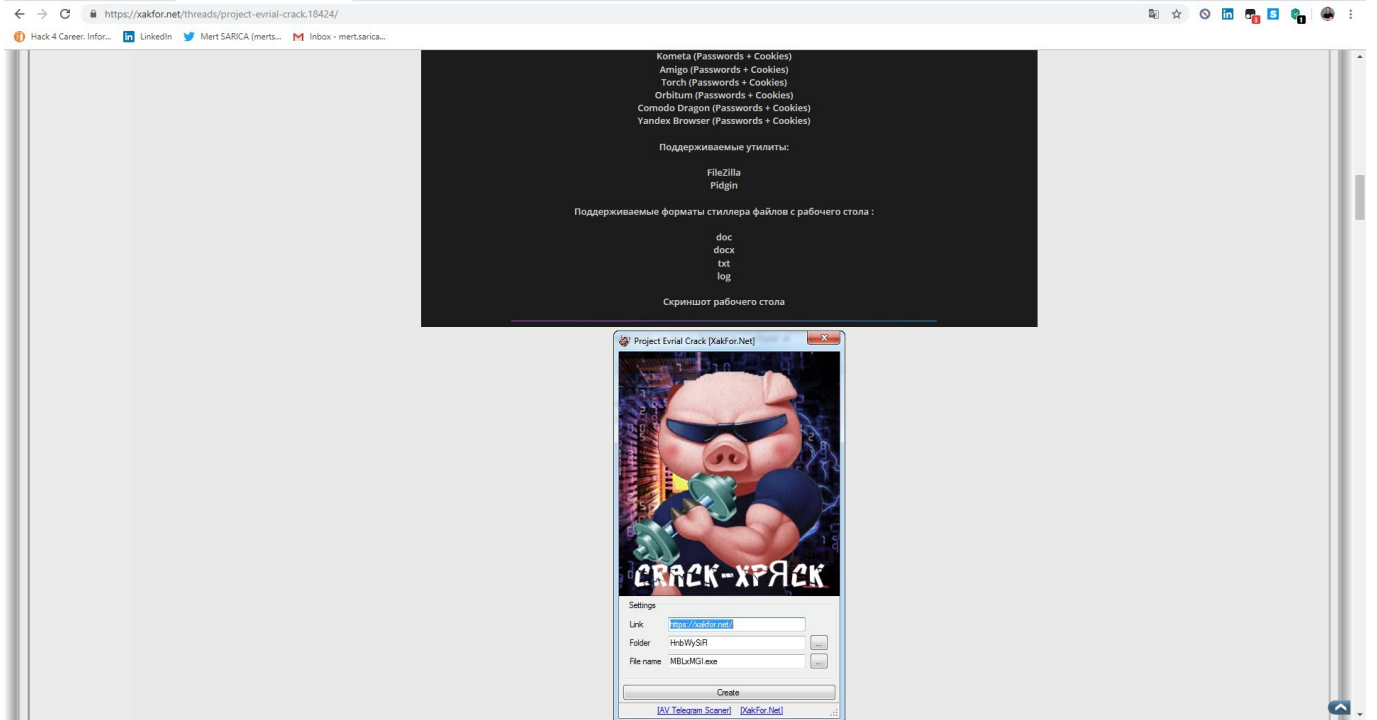
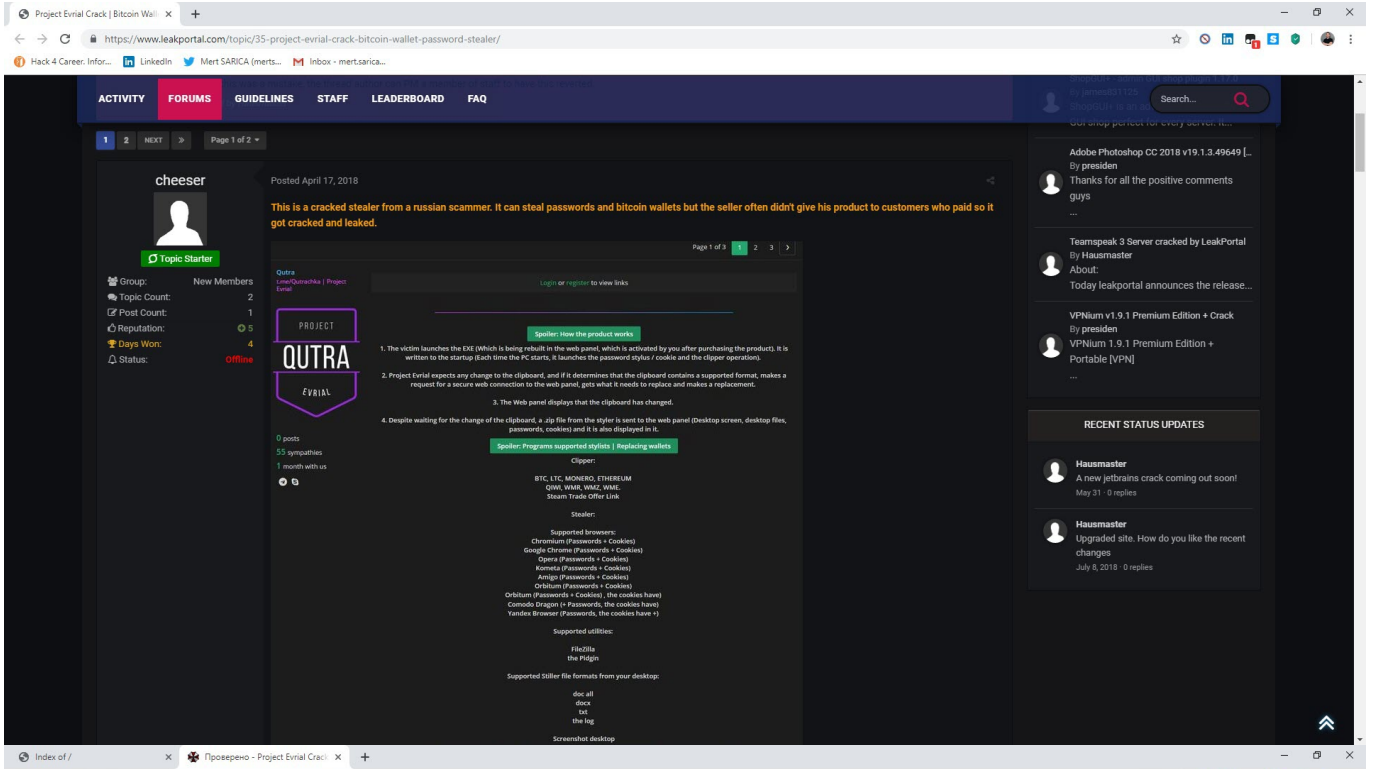
private static string text = "";

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



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. :)

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			
Name	Last modified	Size	Description
Parent Directory		-	
2aipnse03x3.zip	2019-07-07 13:54	175K	
bdsjattf4h03.zip	2019-07-07 14:01	180K	
cgtkxdi8ry0.zip	2019-07-12 21:27	18K	
cqzbalzibvd.zip	2019-07-08 21:58	9.1K	
egzok2ynph4.zip	2019-07-08 20:21	15K	
gsm3ggrp3h.zip	2019-07-07 16:36	24K	
jdomvvtogok1.zip	2019-07-23 03:57	27K	
lnldeocf2d5.zip	2019-07-06 19:49	218K	
m4tuckk3pxtp.zip	2019-07-07 15:12	327K	
nd0a2g5yva1a.zip	2019-07-03 15:23	213K	
o5nmrfk0n1i.zip	2019-07-08 21:36	322K	
ossq5oorfw.zip	2019-07-07 15:25	100K	
qvzvhyhflgu.zip	2019-07-03 15:22	213K	
tmp/	2018-02-08 10:48	-	
rvcb8mm7jm3.zip	2019-07-06 15:12	1.0K	
upload.php	2018-02-24 22:46	4.0K	
vparawza2i3.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
```

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.