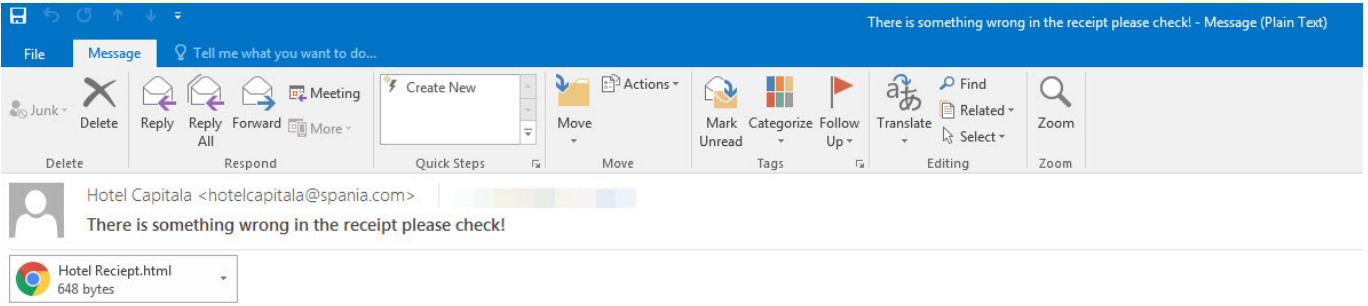


Kaçabilirsin ama Saklanamazsın

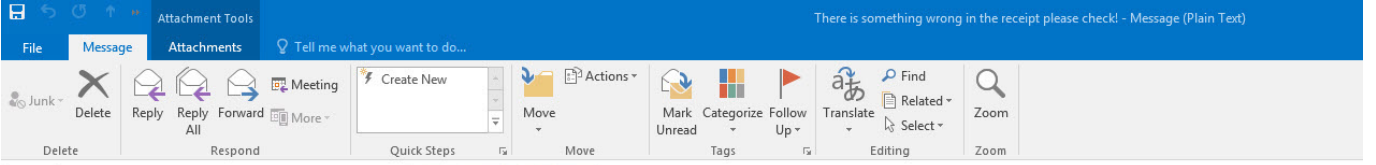
written by Mert SARICA | 1 September 2021

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

Evvel zaman içinde, kalbur saman içinde; pireler berber, develer tellal iken bir tehdit aktörü varmış. Bu tehdit aktörü hedef aldığı kurumlardaki üst düzey çalışanlara ekinde bir HTML dosyası bulunan bir e-posta göndermiş. Bu HTML dosyası açılır ve içindeki bağlantı adresi ([https://google-drive\[.\]blogspot\[.\]com](https://google-drive[.]blogspot[.]com)) takip edilirse, hedef alınan kişi mega.nz isimli dosya saklama ve paylaşım sitesindeki bir adrese ([https://mega\[.\]nz/file/axlmBSxR](https://mega[.]nz/file/axlmBSxR)) yönlendiriliyormuş. Bu dosya indirilip çalıştırılırsa, tehdit aktörü tarafından hedef sistem uzaktan yönetilerek ses, görüntü, tuş kaydı da dahil olmak üzere her türlü kötülük yapılabiliyormuş. Rivayete göre de ağ tabanlı kum havuzu sistemlerinden bazıları, tehdit aktörü tarafından gönderilen bu HTML dosyasında yer alan bağlantı adresini analiz edemiyormuş.



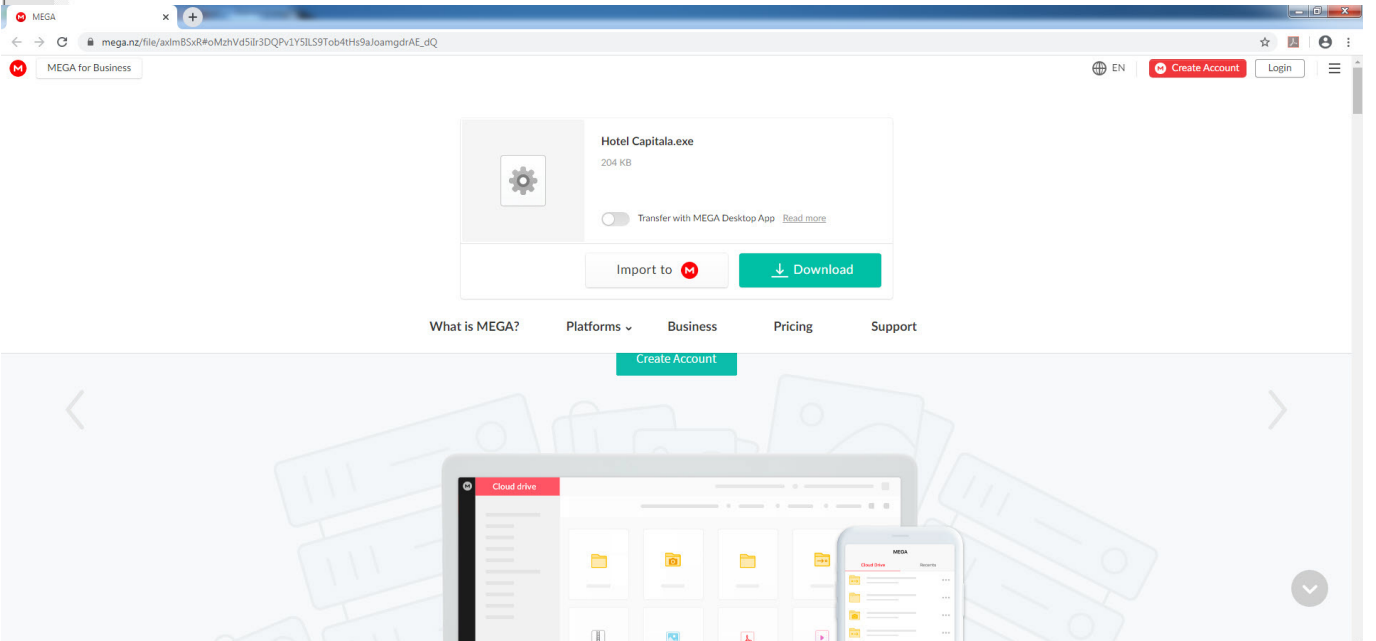
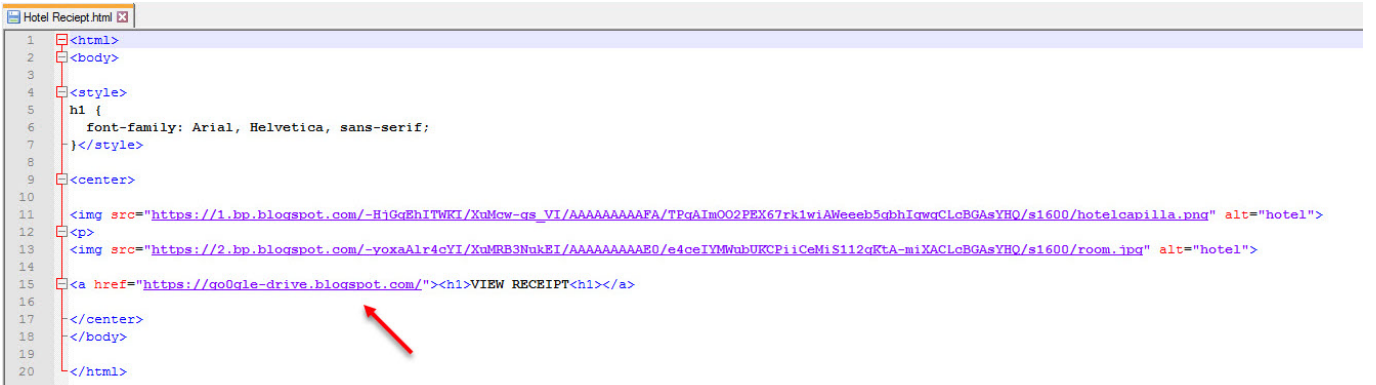
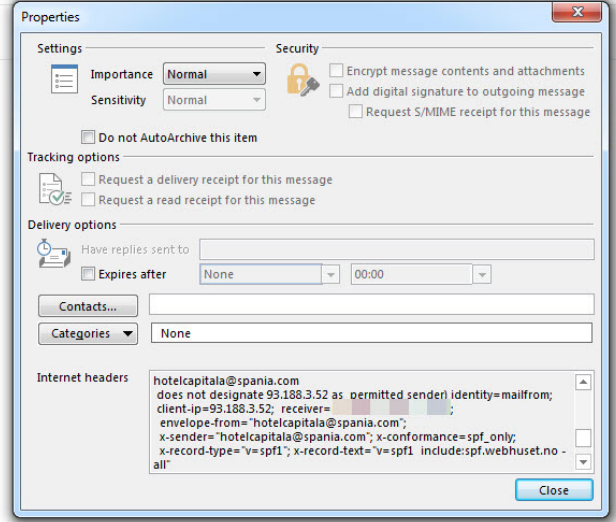
Check Attachment.



Hotel Capitala <hotelcapitala@spania.com>
There is something wrong in the receipt please check!

Hotel Receipt.html
648 bytes

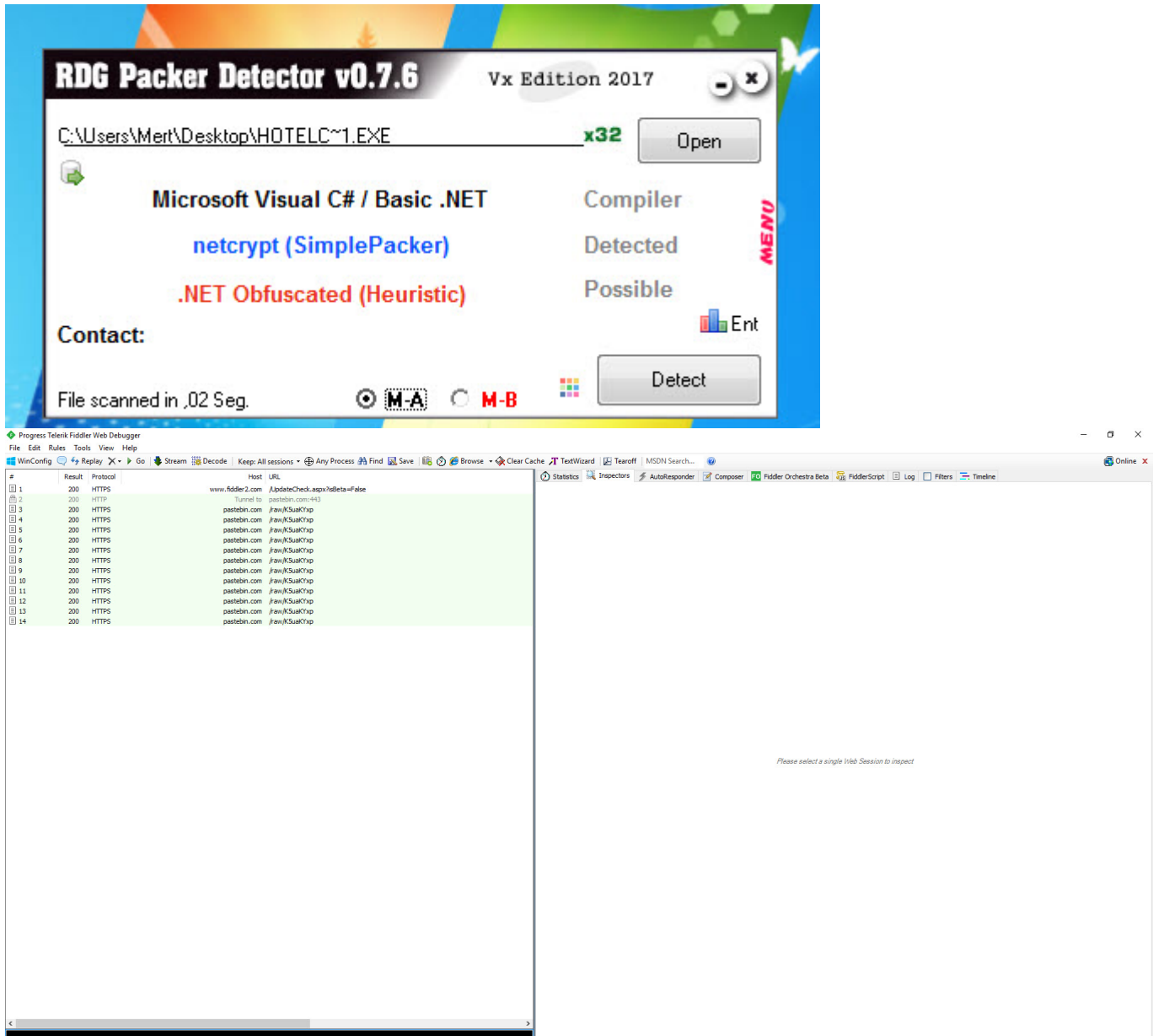
Check Attachment.

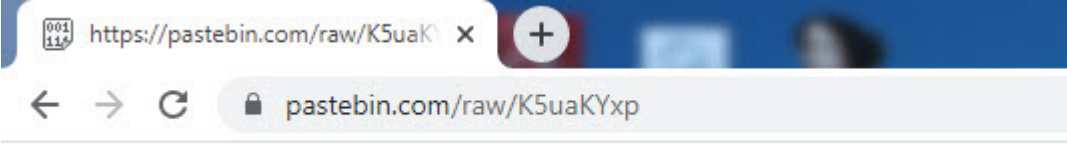


Bir kurum yukardaki gibi bir senaryo ile karřılařtıđında, saldırı giriřimi bařarıya ulařmasa da konuyu b'uy'uk bir dikkatle ele almalıdır 'c'unku bu 'o'nc'u bir sarsıntı olup ardından gelecek b'uy'uk depremin iřaret'cisi olabilir

dolayısıyla bu girişimin hedefli (Spear Phishing), organize mi (APT) yoksa çok sayıda kullanıcıya gerçekleştirilen genel bir kampanyanın parçası mı sorularına da arka planda yanıt araması gerekir. Tabii bu soruların yanıtlarını bulması kimi zaman mümkün olmasa da yapılan analizler sayesinde bir fikir elde edilebilir. Ben de bu yazı ile bu sorulara yanıt aramaya koyuldum.

İlk olarak statik analiz ile dosyanın C# ile geliştirilip, paketlenmiş olduğunu gördüm. Dosyayı sanal bir sistem üzerinde çalıştırıp dinamik olarak analiz ettiğimde zararlı yazılımın Pastebin sitesindeki bir adrese eriştiğini öğrendim. Bu web adresini ziyaret ettiğimde sayfada bir ip adresi (193.161.193.99) ve bağlantı numarasının (port) yer aldığını gördüm.





193.161.193.99:20614

Özellikle APT saldırılarında kullanılan zararlı yazılımlar tehdit aktörleri tarafından özel olarak geliştirildiği ve saldırıdan hemen önce derlendiği için VirusTotal'a yüklendiğinde çoğunlukla genel bir imza adı altında (Backdoor, Trojan vb) tespit edilmektedir. Bu gibi durumlarda Intezer gibi servislerden faydalanarak zararlı yazılımın kodunun başka hangi zararlı yazılımlarda kullanıldığını arayarak eşleştirme yapmanız ve tehdit aktörü konusunda bilgi edinmeniz söz konusu olabilir.

Bu zararlı yazılımı VirusTotal'a yüklediğim spesifik olarak bir zararlı yazılımla eşleştirilmediğini gördüm. Bunun üzerine Intezer üzerinde arama yaptığımda da maalesef yine elim boş kaldı. (Generic Malware)

Pastebin.com sayfasından elde ettiğim ip adresini VirusTotal'da arattığımda bu ip adresinin bağlantı noktası yönlendirmek amacıyla hizmet veren Portmap.io servisine ait olduğunu öğrendim.

193.161.193.99

6 / 93

6 engines detected this IP address

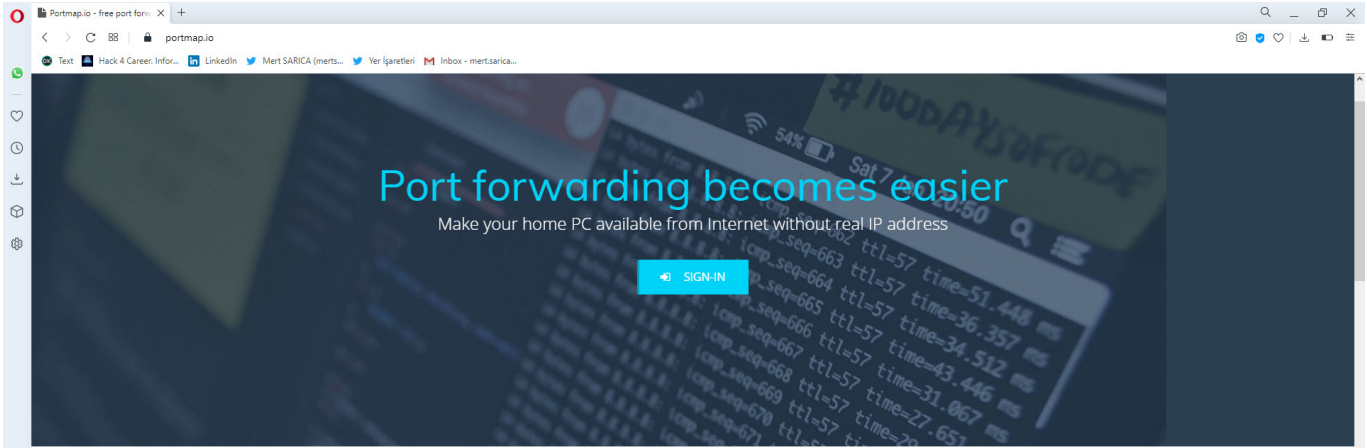
193.161.193.99 (193.161.193.0/24)
AS: 198134 (OOO BİTtree Networks)

RU

DETECTION DETAILS RELATIONS COMMUNITY

Passive DNS Replication

Date resolved	Domain
2020-06-12	spynote102-59531.portmap.io
2020-06-12	xmatlybr.duckdns.org
2020-06-12	anony46-55281.portmap.io
2020-06-11	redisr1-42218.portmap.io
2020-06-11	nickman12-46565.portmap.io
2020-06-11	alexas09website-41137.portmap.io
2020-06-11	coronanancy14-50163.portmap.io
2020-06-11	lrsh16-31376.portmap.host
2020-06-11	celton2241-39412.portmap.io
2020-06-11	willdove-38909.portmap.host
2020-06-11	amaro1510-57297.portmap.io
2020-06-10	chickennuggnew.ml
2020-06-10	mranulis-30061.portmap.host
2020-06-10	risky-22577.portmap.host
2020-06-10	sdsd33-43977.portmap.host
2020-06-10	adidroid555.duckdns.org
2020-06-10	msys-55433.portmap.io
2020-06-10	kyeguy-61442.portmap.host
2020-06-09	alex70-46796.portmap.io
2020-06-09	tanygary-55940.portmap.io
2020-06-09	luckytsingh11-57893.portmap.io
2020-06-09	clarkblank1-22933.portmap.io



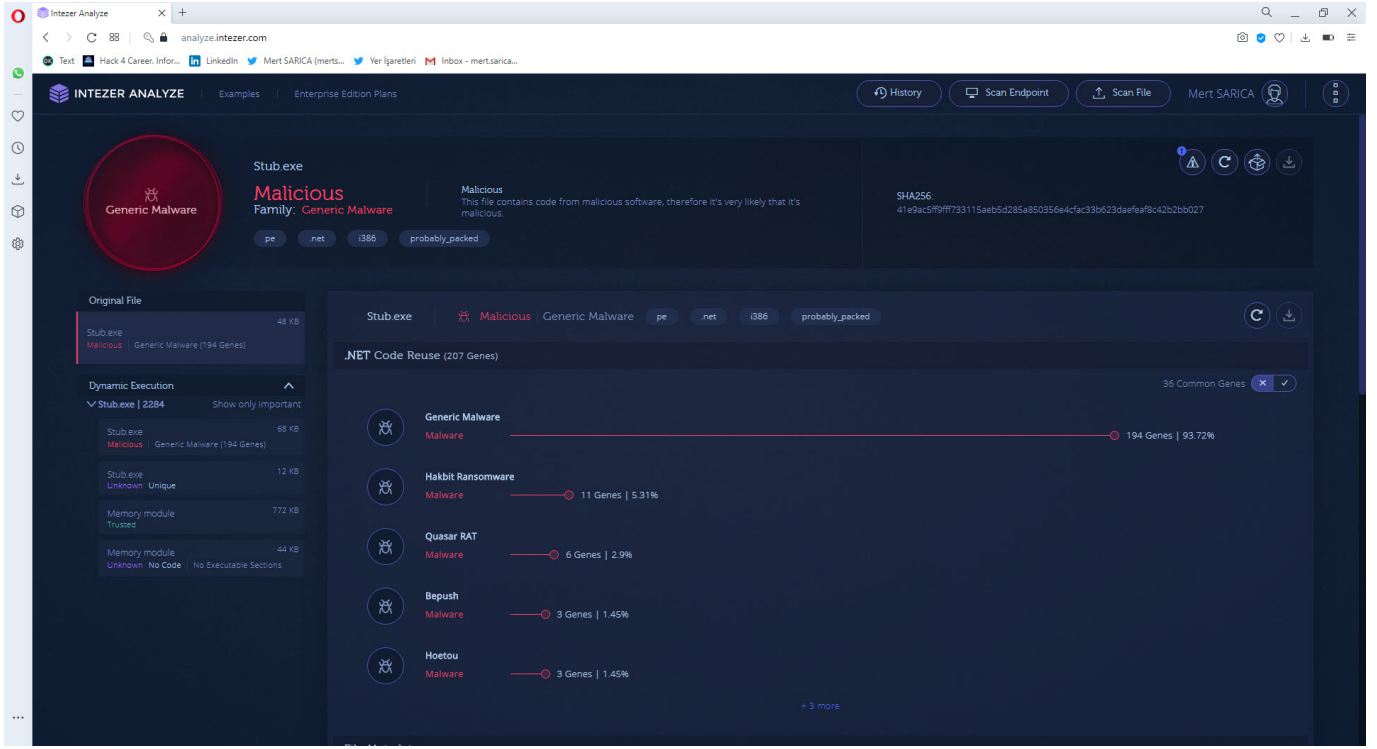
Free port forwarding solution

- Web and mobile development**
 Show your work to the clients
- System administration**
 Access any device behind firewall
- Remote support**
 Provide remote tech support via VNC or RDP
- Video surveillance**
 Connect to CCTV cameras without real IP address

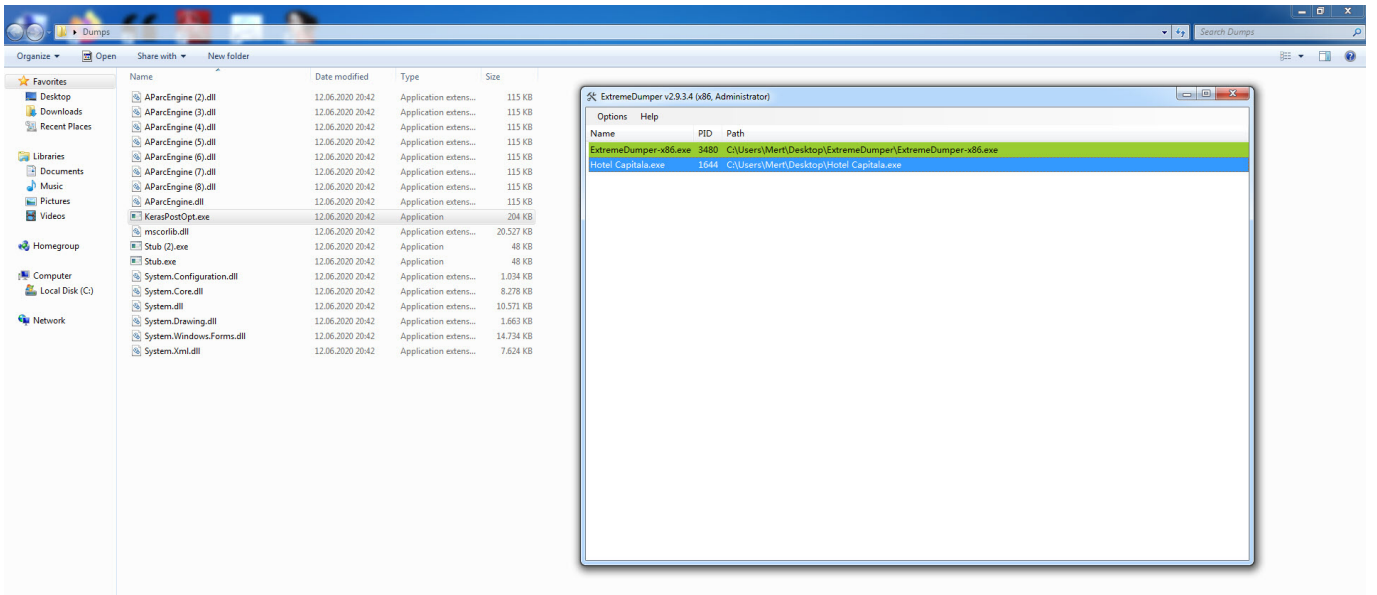
20 engines detected this file

203.50 KB | 2020-06-15 19:57:38 UTC (3 days ago)

DETECTION	DETAILS	RELATIONS	BEHAVIOR	CONTENT	SUBMISSIONS	COMMUNITY
SecureAge APEX	Malicious				Avira (no cloud)	HEUR/AGEN.1118533
BitDefender Theta	Gen.NN.ZemsiIF.34128.mm0@aqOYAJ				CrowdStrike Falcon	Win/malicious_confidence_100% (D)
Cybereason	Malicious fe59a2				Cylance	Unsafe
Cynet	Malicious (score: 85)				eGambit	Unsafe AI_Score_100%
Endgame	Malicious (high Confidence)				ESET-NOD32	A Variant Of MSIL/Kryptik.QME
F-Secure	Heuristic:HEUR/AGEN.1118533				FireEye	Generic.mg.e8186088ba6dc536
Kaspersky	HEUR:Trojan.Win32.Generic				McAfee-GW-Editon	BehavesLike.Win32.Generic.dc
Microsoft	Trojan.Win32/Wacatac.Clm1				Qihoo-360	HEUR/QVM03.0.DAB8.Malware.Gen
Sangfor Engine Zero	Malware				SentinelOne (Static ML)	DFI - Malicious PE
Sophos ML	Heuristic				ZoneAlarm by Check Point	HEUR:Trojan.Win32.Generic
Acronis	Undetected				Ad-Aware	Undetected
AegisLab	Undetected				AhnLab-V3	Undetected
Alibaba	Undetected				ALYac	Undetected



Kendisini gizlemek için elinden geleni yapan tehdit aktörünün geliştirmiş olduğu zararlı yazılımın ne olduğunu öğrenmek için araştırmaya devam ettiğimde sıra dinamik kod analizine geldi ve imdadıma OPSEC başlıklı yazımda kullandığım dnSpy hata ayıklayıcısı yetişti. dnSpy aracı ile hata ayıklamaya başlamadan önce paketlenmiş yazılımın bellekte gizlediği ana modülünü bulmak için ExtremeDumper aracını çalıştırdığımda ortaya kötülüklerin anası Stub.exe çıkmış oldu.



Stub.exe programını adım adım dnSpy ile analiz ettiğim bir noktada AES ile şifrelenmiş olup çözülen 0.5.6B değeri dikkatimi çekti. Bu değeri Google'da "rat 0.5.6B" anahtar kelimeleri ile arattığımda bilin bakalım karşıma ne

çıktı ? Açık kaynak kodlu AsyncRAT! :)

The image shows two screenshots of dnSpy v6.1.4. The top screenshot displays the source code of the `sgEnrQnpUXSed` class, which implements AES encryption. The code includes the following key parts:

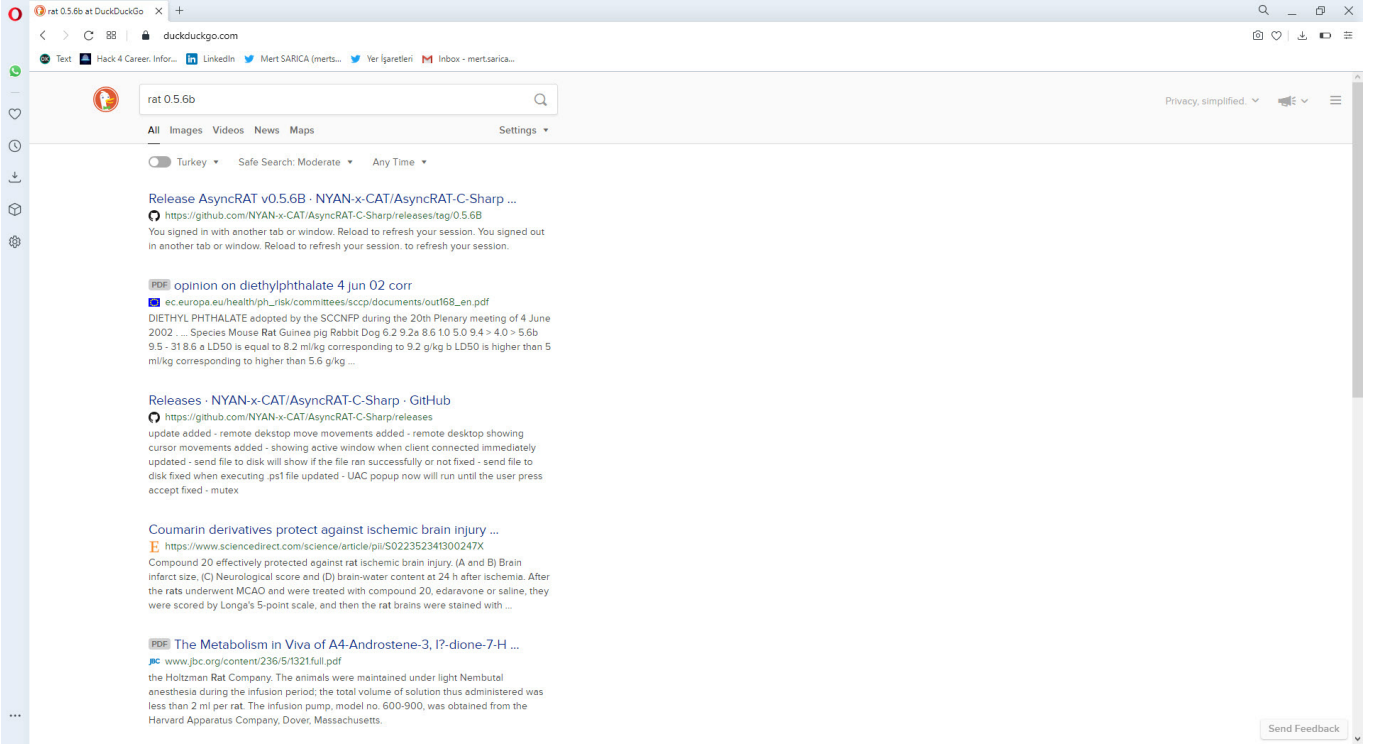
```
using System;
using System.Security.Cryptography;
using System.Security.Cryptography.X509Certificates;
using System.Text;
using CEPWhUvhVdsvmh;
using dJbJslmJkpy;

namespace yQqazXpkKxcharC
{
    // Token: 0x02000003 RID: 3
    public static class sgEnrQnpUXSed
    {
        // Token: 0x00000003 RID: 3 RVA: 0x00002E6B File Offset: 0x000000E8
        public static bool BfVtUdStKcBm()
        {
            bool result;
            try
            {
                sgEnrQnpUXSed.pzEdznkYsb = Encoding.UTF8.GetString(Convert.FromBase64String(sgEnrQnpUXSed.pzEdznkYsb));
                zrhQbBb0uM = new xuSVZBxipI(sgEnrQnpUXSed.pzEdznkYsb);
                dzZbZpCvqDAl = sgEnrQnpUXSed.zrhQbBb0uM.HNRdcccMDF(sgEnrQnpUXSed.dzZbZpCvqDAl);
                sgEnrQnpUXSed.RoofezbFXQvFN = sgEnrQnpUXSed.zrhQbBb0uM.HNRdcccMDF(sgEnrQnpUXSed.RoofezbFXQvFN);
                sgEnrQnpUXSed.xAtthiflywQy = sgEnrQnpUXSed.zrhQbBb0uM.HNRdcccMDF(sgEnrQnpUXSed.xAtthiflywQy);
                sgEnrQnpUXSed.zrhQbBb0uM = new xuSVZBxipI(sgEnrQnpUXSed.pzEdznkYsb);
                sgEnrQnpUXSed.dzZbZpCvqDAl = sgEnrQnpUXSed.zrhQbBb0uM.HNRdcccMDF(sgEnrQnpUXSed.dzZbZpCvqDAl);
                sgEnrQnpUXSed.RoofezbFXQvFN = sgEnrQnpUXSed.zrhQbBb0uM.HNRdcccMDF(sgEnrQnpUXSed.RoofezbFXQvFN);
                sgEnrQnpUXSed.xAtthiflywQy = sgEnrQnpUXSed.zrhQbBb0uM.HNRdcccMDF(sgEnrQnpUXSed.xAtthiflywQy);
                sgEnrQnpUXSed.bfUtgVbCebC = sgEnrQnpUXSed.zrhQbBb0uM.HNRdcccMDF(sgEnrQnpUXSed.bfUtgVbCebC);
                sgEnrQnpUXSed.UhQI0uSnmr = sgEnrQnpUXSed.zrhQbBb0uM.HNRdcccMDF(sgEnrQnpUXSed.UhQI0uSnmr);
                sgEnrQnpUXSed.Wb0QsUkqvq = sgEnrQnpUXSed.zrhQbBb0uM.HNRdcccMDF(sgEnrQnpUXSed.Wb0QsUkqvq);
                sgEnrQnpUXSed.AskI0qVwXJd = new mdLbUlywV6.dvcheKkH0p();
                sgEnrQnpUXSed.NdAgNhzwf0dy = sgEnrQnpUXSed.zrhQbBb0uM.HNRdcccMDF(sgEnrQnpUXSed.NdAgNhzwf0dy);
                DntceZhpVt = new X509Certificate2(Convert.FromBase64String(sgEnrQnpUXSed.zrhQbBb0uM.HNRdcccMDF(sgEnrQnpUXSed.wgZLmTvx0pX1)));
                result = sgEnrQnpUXSed.LaIgcVbVlrf();
            }
            catch
            {
                result = false;
            }
            return result;
        }
    }
}
```

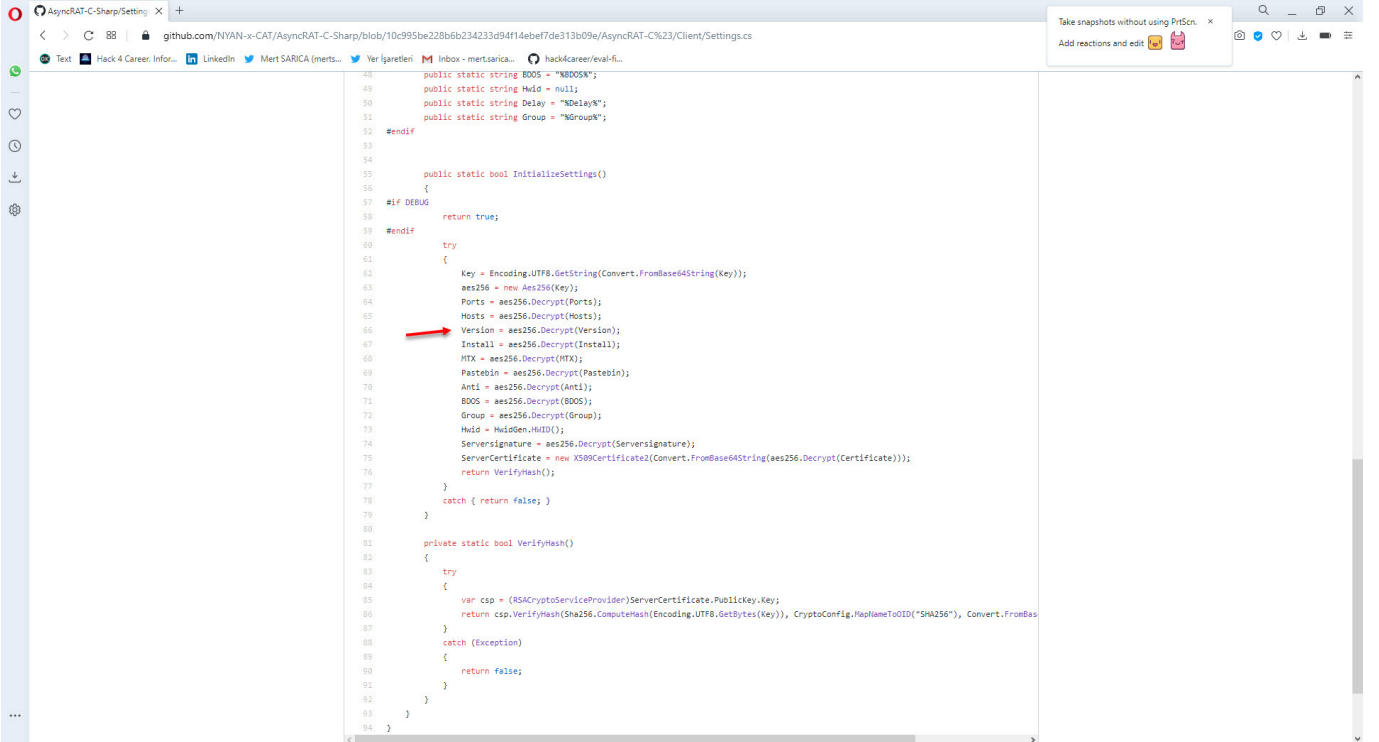
The bottom screenshot shows the local variables window for the `sgEnrQnpUXSed` class. A red callout box points to the `key` variable, which contains the AES encryption key:

Name	Value	Type
key	byte[0x00000020]	byte[]
[0]	0x65	byte
[1]	0x60	byte
[2]	0x22	byte
[3]	0x25	byte
[4]	0x06	byte
[5]	0xEF	byte
[6]	0xEB	byte
[7]	0x5C	byte
[8]	0xD6	byte
[9]	0x23	byte
trim	None	None

A red callout box with the text "AES şifreleme anahtarı" (AES encryption key) points to the `key` variable in the locals window.

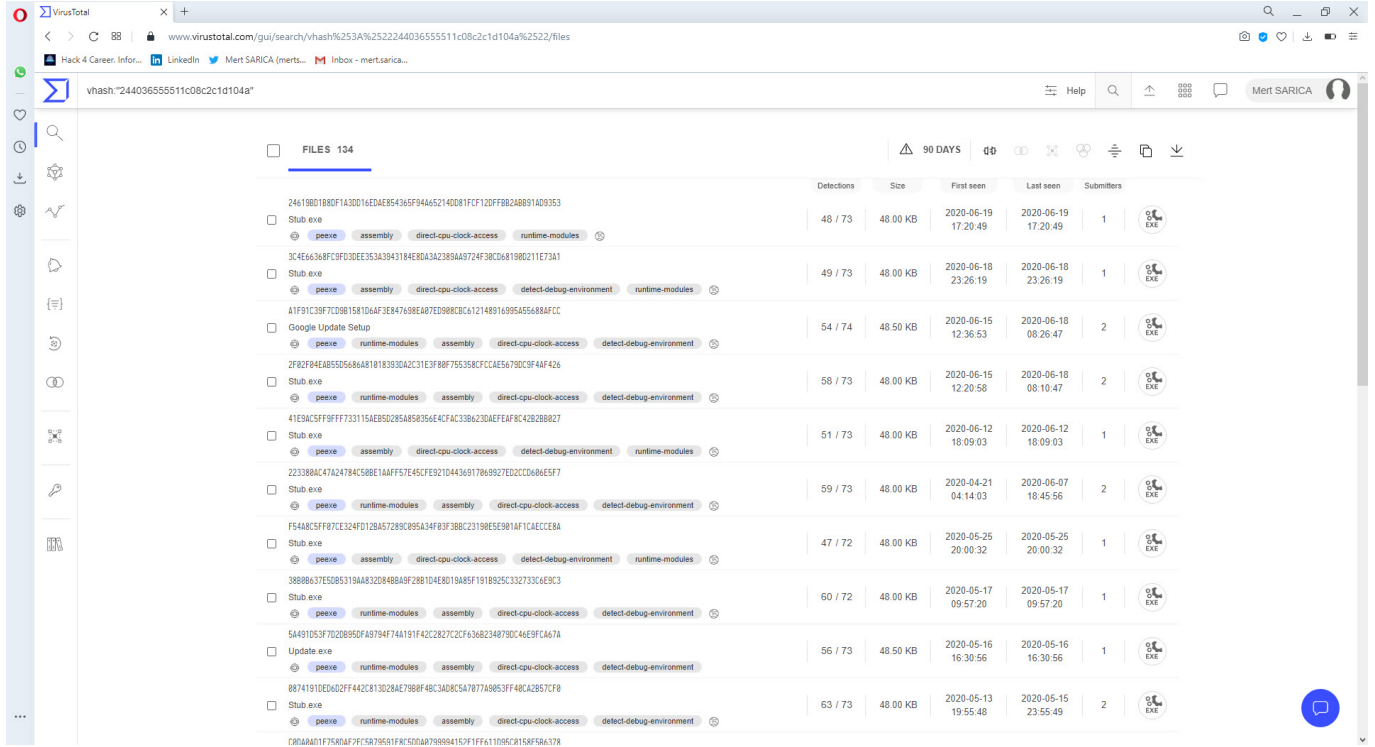


GitHub üzerinde bu projeyi detaylı bir şekilde incelediğimde analiz ettiğim zararlı yazılımın AsyncRAT olduğunu benzer kod bloklarından yola çıkarak doğrulayabildim.



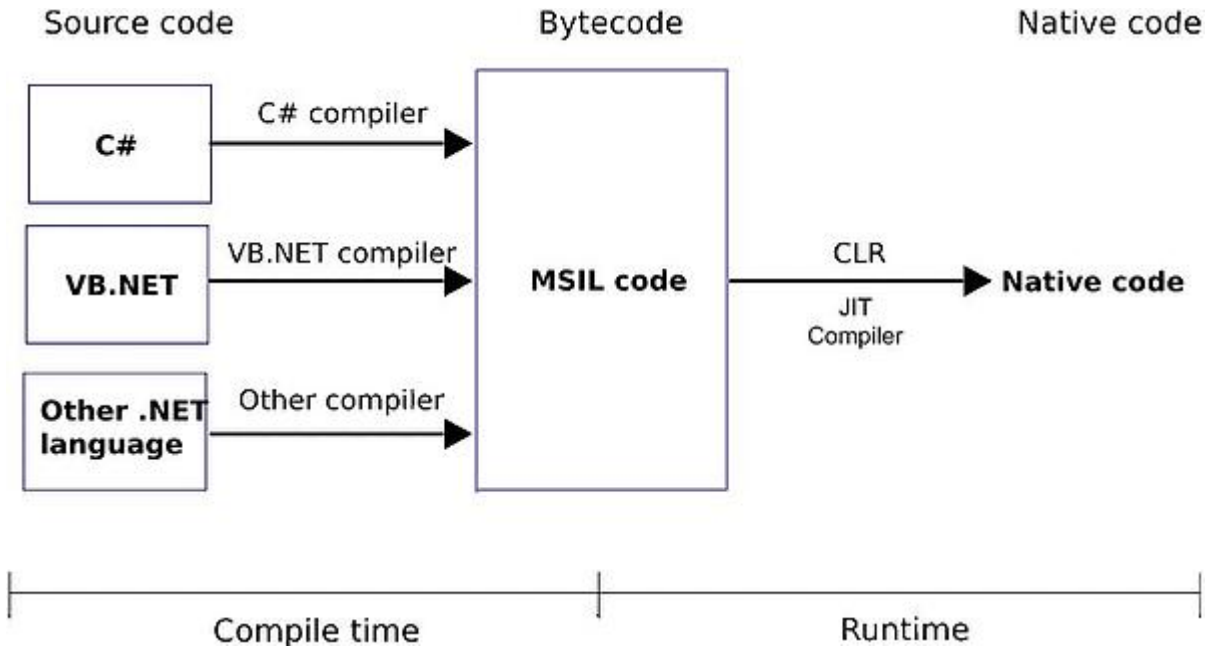
Son aşamada Stub.exe dosyasının benzerlerini vhash ile VirusTotal üzerinde arattığımda çok sayıda örnek ile karşılaştım. Tüm bu örnekler, analiz ettiğim zararlı yazılımdaki Pastebin adresine mi sahip, ortak bir kampanyanın parçası mı diye merak içinde düşünürken ya 50'den fazla her bir örneğin analiz

raporunu inceleyip bunu kontrol edecektim ya da tembellelere yakışır çok kısa ve pratik bir yol bulacaktım. :) Hindi gibi düşünmeye başladıktan sonra aklıma Python ile tüm bu örnekleri statik olarak analiz ederek önce AES şifreleme anahtarını bulan ve ardından da konfigürasyon bilgilerini çıkaran bir araç hazırlama fikri geldi.

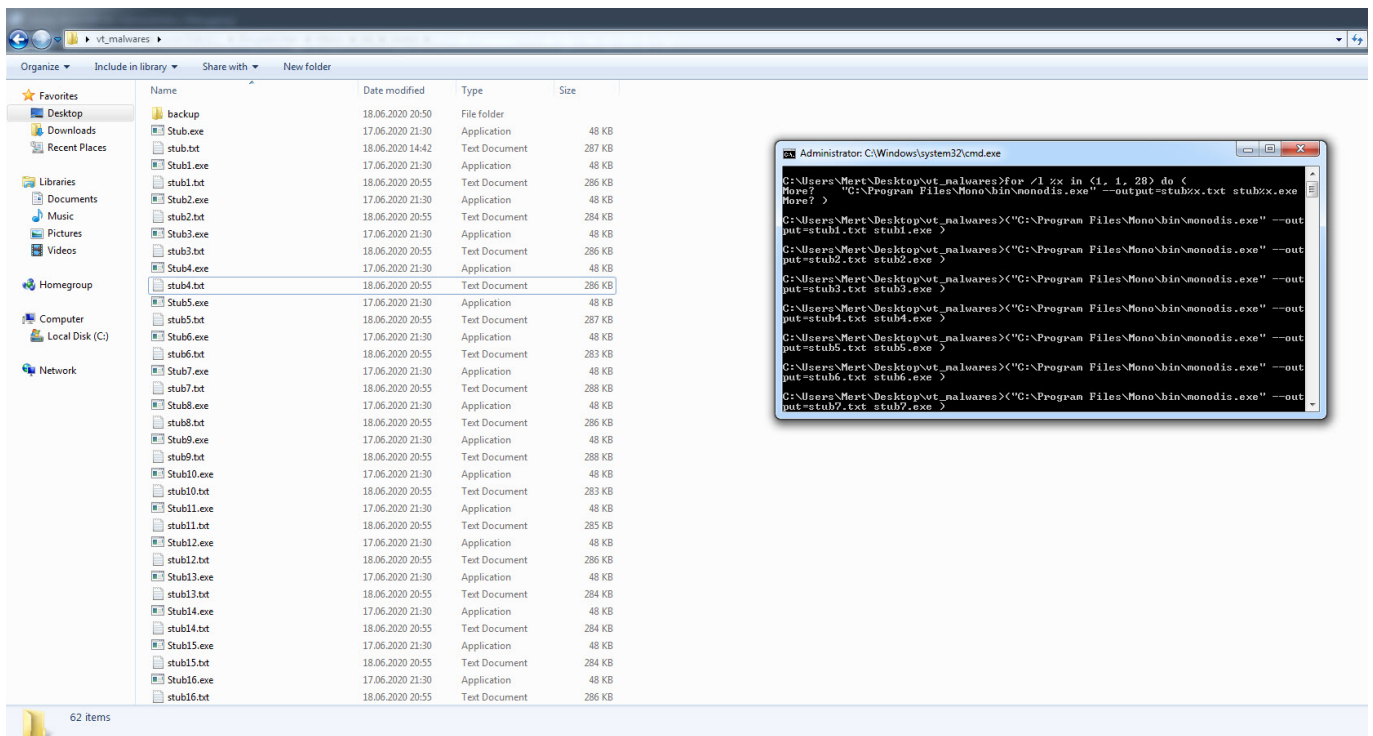


Files	Detections	Size	First seen	Last seen	Submitters
24619B0180DF1A3DD14E0A85436F944652140D81F2F120FF82A8B91A039353 Stub.exe	48 / 73	48.00 KB	2020-06-19 17:20:49	2020-06-19 17:20:49	1
3C4E66368FC9FD02EE353A3943184E80A3A2389AA9724F38CD681980211E173A1 Stub.exe	49 / 73	48.00 KB	2020-06-18 23:26:19	2020-06-18 23:26:19	1
A1F91C39F7CDB1581D6AF3E84768BEA87ED988CB6A121491695A5688AFC Google Update Setup	54 / 74	48.50 KB	2020-06-15 12:36:53	2020-06-18 06:26:47	2
2F82F84AB5505648A818193930A2C31E3F88755358FCFAE5679C9F44F426 Stub.exe	58 / 73	48.00 KB	2020-06-15 12:20:58	2020-06-18 08:10:47	2
41E9ACFF8FF73115AE85D285A858356E4C7AC3B6230AEFA8C42B28B827 Stub.exe	51 / 73	48.00 KB	2020-06-12 18:09:03	2020-06-12 18:09:03	1
223388AC47A24784C588E1AAFF57E45CFE92104369178A9927E02CCD8A6E5F7 Stub.exe	59 / 73	48.00 KB	2020-04-21 04:14:03	2020-06-07 18:45:56	2
F548C5FF87CE324F0128A57289C895A34F83F388C23198E5E901AF7CAECC8A Stub.exe	47 / 72	48.00 KB	2020-05-25 20:00:32	2020-05-25 20:00:32	1
38886A37E5D85319A832D8488A9F281D4E8019A85F191B925C32733C8E3C3 Stub.exe	60 / 72	48.00 KB	2020-05-17 09:57:20	2020-05-17 09:57:20	1
5A491D53F7D2D895DFA9794F74A1914F42C2827C2CF63682348790C46E9FCA7A Update.exe	56 / 73	48.50 KB	2020-05-16 16:30:56	2020-05-16 16:30:56	1
86741910ED002FF442C813028AE7988F48C3A08C5A7877A9853FF48CA2957CF8 Stub.exe	63 / 73	48.00 KB	2020-05-13 19:55:48	2020-05-15 23:55:49	2

Tabii değişken isimleri her bir programda rastgele oluşturulduğu için öncelikle AES anahtarını statik bir değişkenden faydalanarak bulmam gerekiyordu. .Net ile geliştirilen programların derlendiğinde baytkoda (CIL/MSIL) çevrildiğini bildiğimiz için baytkod üzerinde statik değerler aramaya koyuldum.



Bunun için meşhur Mono projesinde yer alan Mono Disassembler (monodis) aracından faydalanmaya karar verdim. Monodis aracı ile tüm Stub.exe örneklerini koda çevirdikten sonra AES şifreleme anahtarının her daim 0x288c değerinden sonra gelen IL_003c değerinde olduğunu tespit ettim. ve bu bilgilerden faydalanarak Python ile AsyncRAT Configuration Extractor aracını geliştirdim. Aracı tüm örnekler üzerinde çalıştırdığımda her birinin konfigürasyonunda yer alan bilgilerin, analiz ettiğim zararlı yazılımdan farklı olduğunu dolayısıyla analiz ettiğim zararlı yazılım ortak bir kampanyanın parçası olmadığını öğrenmiş oldum.



```
IL_0037: call unsigned int8[] class [mscorlib]System.Convert::FromBase64String(string)
IL_0038: callvirt instance bool class [mscorlib]System.Security.Cryptography.RSACryptoServiceProvider::VerifyHash(unsigned int8[], string, unsigned int8[])
IL_0041: stloc.0
IL_0042: leave.s IL_0049
} // end .try 0
catch class [mscorlib]System.Exception { // 0
IL_0044: pop
IL_0045: ldc.i4.0
IL_0046: stloc.0
IL_0047: leave.s IL_0049
} // end handler 0
IL_0049: ldloc.0
IL_004a: ret
} // end of method UPj1GoQHGJmz::ZoFvYnkytXXLLEF
// method line 5
.method private static hidebysig specialname rtspecialname
    default void '.cctor' () cil managed
{
    // Method begins at RVA 0x288c
    // Code size 151 (0x97)
    .maxstack 1
    IL_0000: ldstr "+ZoYbq/fGZAPhtj2npOMXGLGsfwrXKU5S83H8XUj1QdiYXjGu42nGzR4PEWOBIMtF6HY0tO4e7fytFIUp+9Q=="
    IL_0005: stfld string LveFMHugJpKfAW.UPj1GoQHGJmz::rLxHRVvktJ
    IL_000a: ldstr "luq7GHRbtQOL08Ewn9VUWoiYEINiOums33crjUxW9593CxiNMqnpb3WgXcPOVWTM199RmngMwjEJTORok7zaxFA=="
    IL_000f: stfld string LveFMHugJpKfAW.UPj1GoQHGJmz::svdTWYXvrd
    IL_0014: ldstr "Fw0jQRqduSpvq855Fno7awWpCk0InCNUzoHFejjWBIO21+9XMo59v72majGMP8/IttgUwm/Lxu7r7S3NE87w=="
    IL_0019: stfld string LveFMHugJpKfAW.UPj1GoQHGJmz::JgTYyBvoPOX1RmBT
    IL_001e: ldstr "c3R2LaC//AaTuPpNsvyqlug2GZ0k6Q5Dq5vSvKwkszlVPHCAhMhbtGerkeQCNFDQdkik/zCvKbD5jDPRxtKvq=="
    IL_0023: stfld string LveFMHugJpKfAW.UPj1GoQHGJmz::WtxJdUcxhhTm
    IL_0028: ldstr "%AppData%"
    IL_002d: stfld string LveFMHugJpKfAW.UPj1GoQHGJmz::RiFTFGCauJm
    IL_0032: ldstr "Host Process for Windows Host.exe"
    IL_0037: stfld string LveFMHugJpKfAW.UPj1GoQHGJmz::IqQuezn0vept
    IL_003c: ldstr "cg5t8z2uF1QSulnNU9tc3A5NjFkK5QVX1JYmRjWwK="
    IL_0041: stfld string LveFMHugJpKfAW.UPj1GoQHGJmz::bPwIENFAuenePP
    IL_0046: ldstr "wW+9tAGSgSn0ndZHUUFzEP+wk+F7BiDKG3t7cW9tEb6Dysc2Cw9M1W/FAA6B6EMk2qi6c1SAGx+jtAhpG1w=="
    IL_004b: stfld string LveFMHugJpKfAW.UPj1GoQHGJmz::BsgvWQPULSxB
    IL_0050: ldstr
        "uFRcuOb0YG+1IE1IXqM+SgNW/TvtYk6KqIv9V9CGtXPf0JUVOSKwtzgbIAkY+M0yNQ4He2D2Sp2LVhhWuiiuLymrcpU4cgH/HYvYatoimW0cRf6GXBP8QvRukan0yOS2FakpOqdgmiCIwfg/RJv8+ooX7aWJKCo7+mT6j1Iry"
}
```

```
IL_0037: call unsigned int8[] class [mscorlib]System.Convert::FromBase64String(string)
IL_0038: callvirt instance bool class [mscorlib]System.Security.Cryptography.RSACryptoServiceProvider::VerifyHash(unsigned int8[], string, unsigned int8[])
IL_0041: stloc.0
IL_0042: leave.s IL_0049
} // end .try 0
catch class [mscorlib]System.Exception { // 0
IL_0044: pop
IL_0045: ldc.i4.0
IL_0046: stloc.0
IL_0047: leave.s IL_0049
} // end handler 0
IL_0049: ldloc.0
IL_004a: ret
} // end of method vUuBwDus1lr::TM1jBQTGNDfCEWQ
// method line 5
.method private static hidebysig specialname rtspecialname
    default void '.cctor' () cil managed
{
    // Method begins at RVA 0x288c
    // Code size 151 (0x97)
    .maxstack 1
    IL_0000: ldstr "JmPcaie5PV3Cq0EmfV+2XI077H0ufV0wRr2ztSjnrImJOSs6Nt/0/oeUi2DQmR4DYOKfYp3MkHs60SA2dG=="
    IL_0005: stfld string MecuCaiaCqjz.vUuBwDus1lr::wEmhlnbk2HX
    IL_000a: ldstr "i/8hlpMaLMe209YeIWe0u82pzhfcbvBoIT+DFDdowKqII75xtr87t12X1xkuGIRW4t1IaIz6DxeKfwnjxa7bs3lp77QAXhVrvgZyMnVTg=="
    IL_000f: stfld string MecuCaiaCqjz.vUuBwDus1lr::AmbSEfkFvYi
    IL_0014: ldstr "wAZhdLMKC8owycF6513XNF8WBwoz3xIUKjaA2r80JdJAhMrDq38+CG1o71t4qbM1r0+nPue3suc6KC82A=="
    IL_0019: stfld string MecuCaiaCqjz.vUuBwDus1lr::LORepWhkVWE
    IL_001e: ldstr "ndT5oubUi9YDYs+AAxB7xBZiWEDfnfPdeRMBAYQDFvF7JkPt6M46wYx7hRqA/RnXlJfqdBaaziFMD3D0w=="
    IL_0023: stfld string MecuCaiaCqjz.vUuBwDus1lr::MyLRHXIGQFX
    IL_0028: ldstr "%AppData%"
    IL_002d: stfld string MecuCaiaCqjz.vUuBwDus1lr::cbYpYfPwCYi
    IL_0032: ldstr ""
    IL_0037: stfld string MecuCaiaCqjz.vUuBwDus1lr::oEcGiIn2jLGB
    IL_003c: ldstr "XYQ020yMGRXs12Fegx1TGipVXpusD11b29pZU03TFU="
    IL_0041: stfld string MecuCaiaCqjz.vUuBwDus1lr::nkgto2YXkRtgv
    IL_0046: ldstr "26x6P1002ezesi+xxh14Eb4151t9m2ng2pIAYOrz512Mko/jFyCi6aszmCSyx5Yb47al35tESSsvD/dYg7pNQ2EEiciORPvIoKGNdXS5c="
    IL_004b: stfld string MecuCaiaCqjz.vUuBwDus1lr::gEcNdycslalBg
    IL_0050: ldstr
        "gHVg2BMckrUW4h+UPW+YdV6pP9L2tKudotpYEfrJW+Of0bUUGcUNYwKHLTLzWnLdZ1KDJGH15nX/RcYqP8fzIpeIXYGLZGBzqF8MQsO6VtWecI5RPeRsk+JJSzofvBbbrPAN+wQq+cpduvUrTFXoiJ0psXxgUvBi7AtiqKFP5xyPuQz"
}
```

```
308 IL_0037: call unsigned int8[] class [mscorlib]System.Convert::FromBase64String(string)
309 IL_0038: callvirt instance bool class [mscorlib]System.Security.Cryptography.RSACryptoServiceProvider::VerifyHash(unsigned int8[], string, unsigned int8[])
310 IL_0041: stloc.0
311 IL_0042: leave.s IL_0049
312
313 } // end .try 0
314 catch class [mscorlib]System.Exception { // 0
315 IL_0044: pop
316 IL_0045: ldc.i4.0
317 IL_0046: stloc.0
318 IL_0047: leave.s IL_0049
319
320 } // end handler 0
321 IL_0049: ldloc.0
322 IL_004a: ret
323 } // end of method zbgTqalHViUFHWt::sGmuUeoyBYnr
324
325 // method line 5
326 .method private static hidebysig specialname rtspecialname
327 | | default void '.cctor' () cil managed
328 {
329 | | // Method begins at RVA 0x288c
330 | | // Code size 151 (0x97)
331 | | .maxstack 1
332 IL_0000: ldstr "2bSxod6szox1bq2bnUKlvJxcLa5X1407KBe0zAs5TJ/wCRiRB3vOakvztDodRTEjQ/so8HlFQRvvObcckYH/4w=="
333 IL_0005: stfld string MiKCRUQuXTimcp.zbgTqalHViUFHWt::NGswHYqFHetj
334 IL_000a: ldstr "Sz/oQI8Um2lJoEh+RLHl+/aqTWM/v4//yvHYbU+ljWTzx2TPCC32q6valHkGdsDESTpmAw6k5ECGJ9mWa2sWA=="
335 IL_000f: stfld string MiKCRUQuXTimcp.zbgTqalHViUFHWt::dyhWpMOSPwv
336 IL_0014: ldstr "+yEwOEwgIbvXx5f2LXc2xqQHt7+OS5sJ8KJ7rM23KrG81SVx0+4Zu0dzJ37Kv6vMT3S9q+PCaxKj2yhPIHA=="
337 IL_0019: stfld string MiKCRUQuXTimcp.zbgTqalHViUFHWt::tHgFMSfeqgk
338 IL_001e: ldstr "tZAZIRKARk3BzLqyePdePmCuNOT7EfJ9I3e4wWss8Ze7uukigGJIJy5YV+NT3aylkbvPt7dnA5uTyW9/iMuHw=="
339 IL_0023: stfld string MiKCRUQuXTimcp.zbgTqalHViUFHWt::kcPnciqUJTXfcm
340 IL_0028: ldstr "%AppData%"
341 IL_002d: stfld string MiKCRUQuXTimcp.zbgTqalHViUFHWt::iUTvfauwhzOEb
342 IL_0032: ldstr "tasksync.exe"
343 IL_0037: stfld string MiKCRUQuXTimcp.zbgTqalHViUFHWt::brwgbfftiOPhE
344 IL_0038: ldstr "Y2k3V1ZqRzRNNuTYaVdq23hNR29QQ3Nxdndjbc0b04="
345 IL_0041: stfld string MiKCRUQuXTimcp.zbgTqalHViUFHWt::X2muTnrwYta
346 IL_0046: ldstr "lgJvAgU4nQcQm2Fib46gNrnLBwSML+Pxm75cs07XD4Qs/nsbL1183vtW3cXsm6gj2WrPXWE6lm3gmG+Dd+GRQVbntoDuHR6LpZiKNBSb2Y="
347 IL_004b: stfld string MiKCRUQuXTimcp.zbgTqalHViUFHWt::cHIPEjYUqaz
348 IL_0050: ldstr
"eoy7EfVYnBkBY+zrhx6M/Nneiti152ah+orgCGFNfdg50XwKqeM1+piKw4xU49Lw2XQKf+n8xmYk8WC7+oQhvLgY4LlqgGntwMLLXAzWf2hGh/ysDY1NvI1iljLmx2S8NcOJJqi2E2ekwRoVEY4YVb6bdR0oFU090E+deAvsL1d1L9AGRz
```

```
C:\WINDOWS\system32\cmd.exe

=====
AsyncRAT Configuration Extractor v1.0 [https://www.mertsarica.com]
=====
Port: 4782
Host: 24.31.138.57
Version: 0.5.6B
Install: true
Mutex: bqwzfgeszubufqxo
Pastebin: null
```

Command Prompt

```
C:\Users\Mert\Desktop\YeniYazi\HB Malware\stubs>for /l %x in (1, 1, 28) do (
More?   python asynccrat_ext.py stub%x.txt
More? )

C:\Users\Mert\Desktop\YeniYazi\HB Malware\stubs>(python asynccrat_ext.py stub1.txt )
Port: 66
Host: wissam000.ddns.net
Version: 0.5.6B
Install: false
Mutex: glllhiysywrewkfzbbw
Pastebin: null

C:\Users\Mert\Desktop\YeniYazi\HB Malware\stubs>(python asynccrat_ext.py stub2.txt )
Port: null
Host: null
Version: 0.5.6B
Install: true
Mutex: qrpmfkwwjlpixppobq
Pastebin: https://pastebin.com/raw/s14cUU5G

C:\Users\Mert\Desktop\YeniYazi\HB Malware\stubs>(python asynccrat_ext.py stub3.txt )
Port: null
Host: null
Version: 0.5.6B
Install: false
Mutex: bankobankbobobanks
Pastebin: https://pastebin.com/raw/K5uaKYxp

C:\Users\Mert\Desktop\YeniYazi\HB Malware\stubs>(python asynccrat_ext.py stub4.txt )
Port: null
Host: null
Version: 0.5.6B
Install: true
Mutex: rqkumxvanugppuhzu
Pastebin: https://pastebin.com/raw/CQYS13RT

C:\Users\Mert\Desktop\YeniYazi\HB Malware\stubs>(python asynccrat_ext.py stub5.txt )
Port: 6606,7707,8808
Host: 67.253.82.166
Version: 0.5.6B
Install: true
Mutex: kokpwnmunddulla
Pastebin: null

C:\Users\Mert\Desktop\YeniYazi\HB Malware\stubs>(python asynccrat_ext.py stub6.txt )
Port: 39712,1151,1148
Host: boobies383-45890.portmap.host
Version: 0.5.6B
Install: true
Mutex: tdwmqnhstavzoes
Pastebin: null
```

Sonuç itibariyle tüm bu bilgileri derleyip topladıktan sonra bu siber saldırı girişiminin bir APT saldırısı olmasa da hedeflenmiş bir saldırının (Spear Phishing) parçası olması teraziye ağır basmış oldu. Özellikle Covid-19

salgınından sonra artan bu tür hedeflenmiş siber saldırı girişimlerine karşı kurumların ve çalışanlarının çok dikkatli olmasını önerir bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.