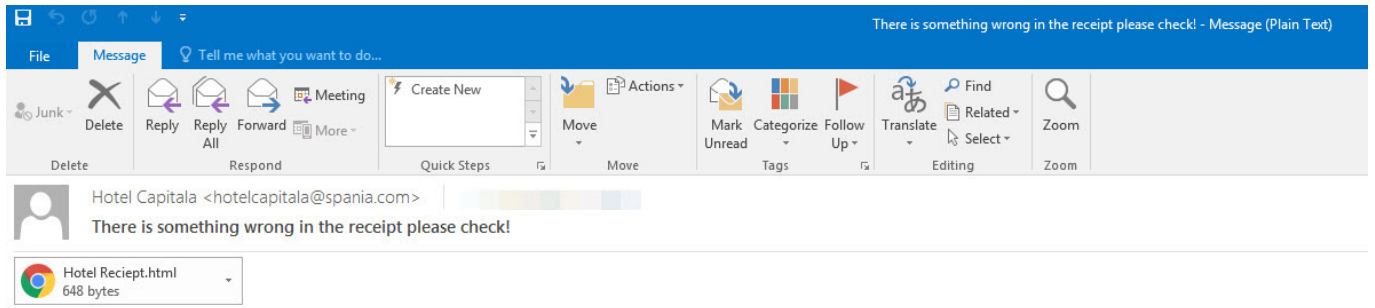


Kaçabilirsin ama Saklanamazsın

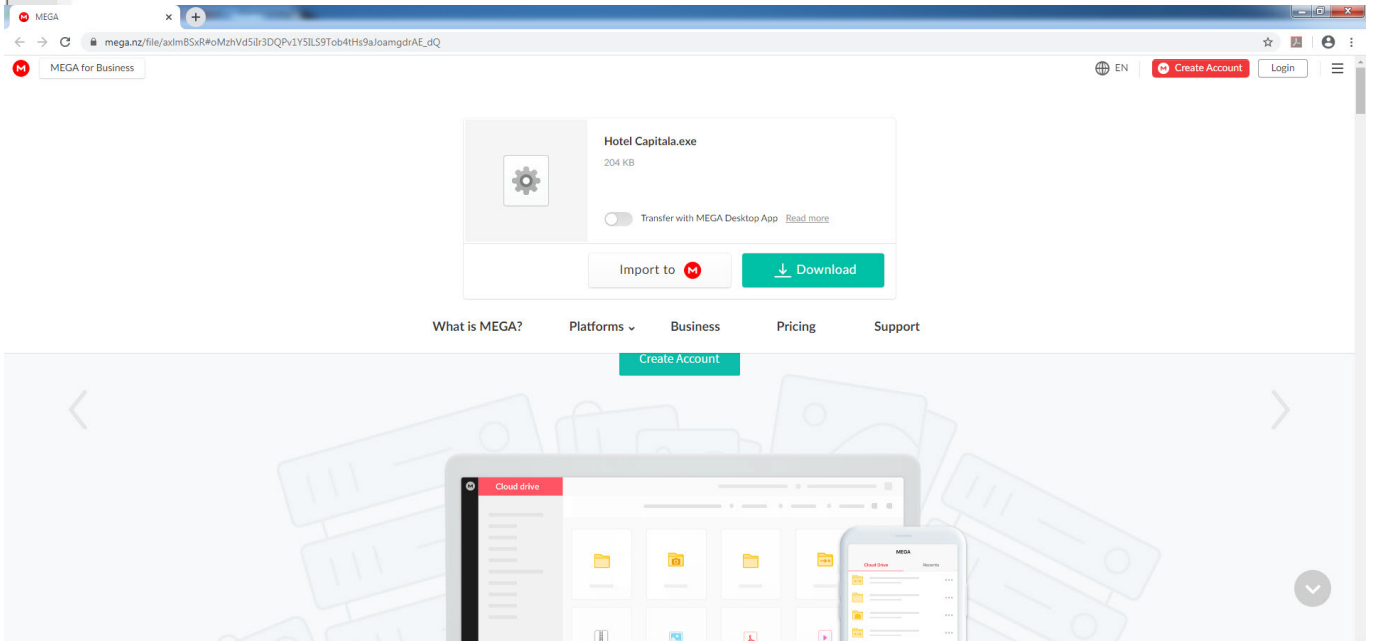
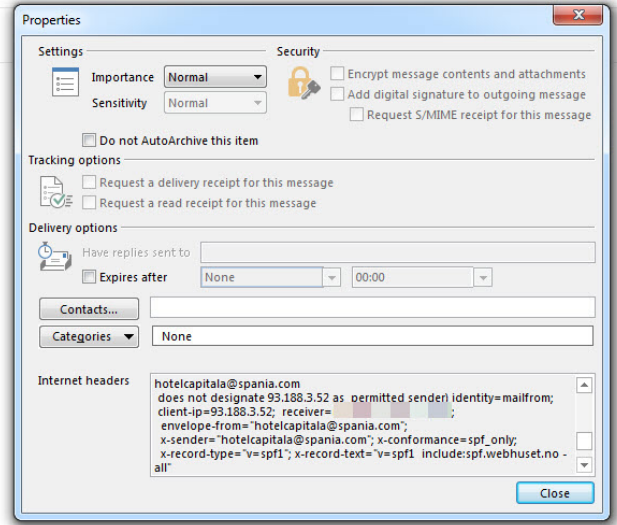
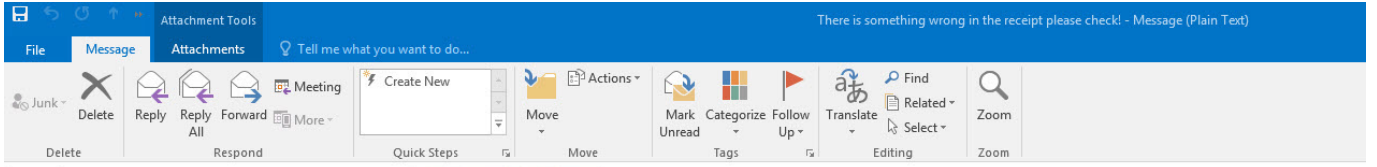
written by Mert SARICA | 1 September 2021

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.



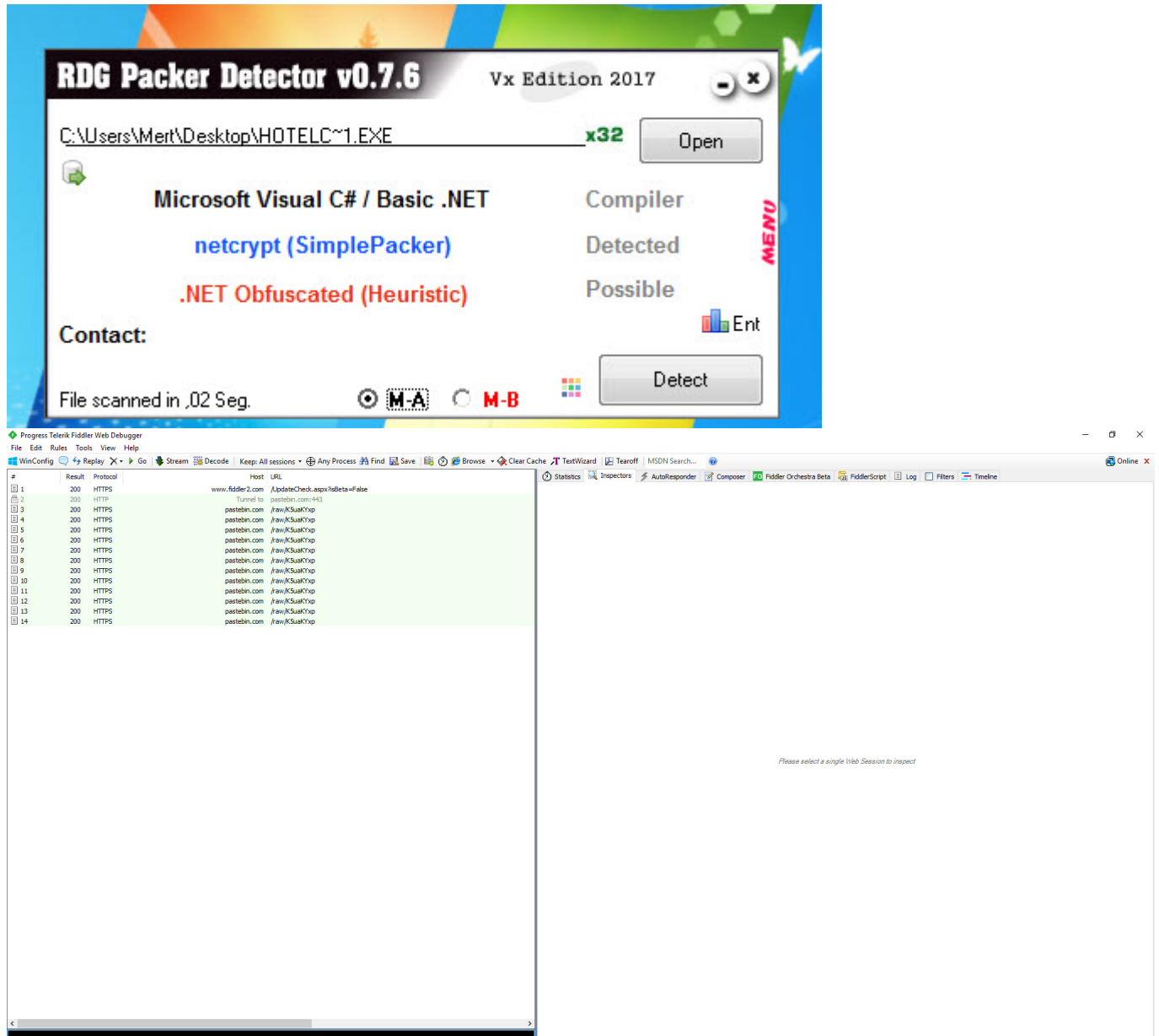
Check Attachment.

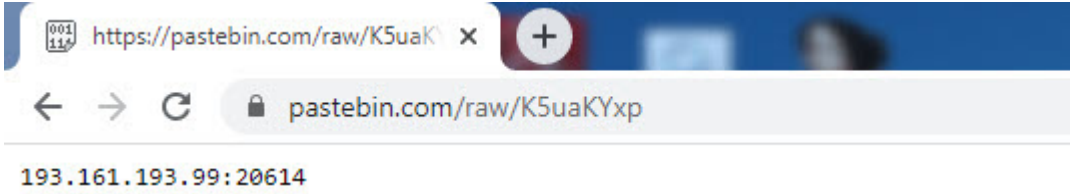


Bir kurum yukardaki gibi bir senaryo ile karřılařtıęında, saldırı giriřimi bařarıya ulařmasa da konuyu b y k bir dikkatle ele almalıdır   nk  bu  nc  bir sarsıntı olup ardından gelecek b y k depremin iřaret isi olabilir

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.





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.

6 / 93

6 engines detected this IP address

193.161.193.99 (193.161.193.0/24)
AS 198134 (OOO Bittree Networks)

RU

DETECTION	DETAILS	RELATIONS	COMMUNITY
Passive DNS Replication			
Date resolved	Domain		
2020-06-12	spynote102-59531.portmap.io		
2020-06-12	xmallyxbr.duckdns.org		
2020-06-12	anony-46-55281.portmap.io		
2020-06-11	redisrl-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	amano1510-57297.portmap.io		
2020-06-10	chickennuggnew.ml		
2020-06-10	mranubis-30061.portmap.host		
2020-06-10	rlisky-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	klyeguy-61442.portmap.host		
2020-06-09	alex70-46796.portmap.io		
2020-06-09	tanygary-55940.portmap.io		
2020-06-09	luckyislingh11-57893.portmap.io		
2020-06-09	clarkblank1-22933.portmap.io		

Portmap.io - free port forwarding solution

portmap.io

Text Hack 4 Career: Inform... LinkedIn Mert SARICA (mertsarica) Her İşaretleri! Inbox - mertsarica...

Port forwarding becomes easier

Make your home PC available from Internet without real IP address

SIGN-IN

Free port forwarding solution

for



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

VirusTotal

www.virustotal.com/gui/file/e9553311bb795d028a0bfb1cc16a74aaaddc493d303dd98ca4b801e9414f4507/detection/f-e9553311bb795d028a0bfb1cc16a74aaaddc493d303dd98ca4b801e9414f4507-1591952418

Hack 4 Career: Inform... LinkedIn Mert SARICA (mertsarica) Inbox - mertsarica...

e9553311bb795d028a0bfb1cc16a74aaaddc493d303dd98ca4b801e9414f4507

Help

Mert SARICA

20

73

Community Score

20 engines detected this file

e9553311bb795d028a0bfb1cc16a74aaaddc493d303dd98ca4b801e9414f4507

c:\users\administrator\appdata\roaming\asdasd\itafdsiajn.exe

203.50 KB Size

2020-06-15 19:57:38 UTC 3 days ago

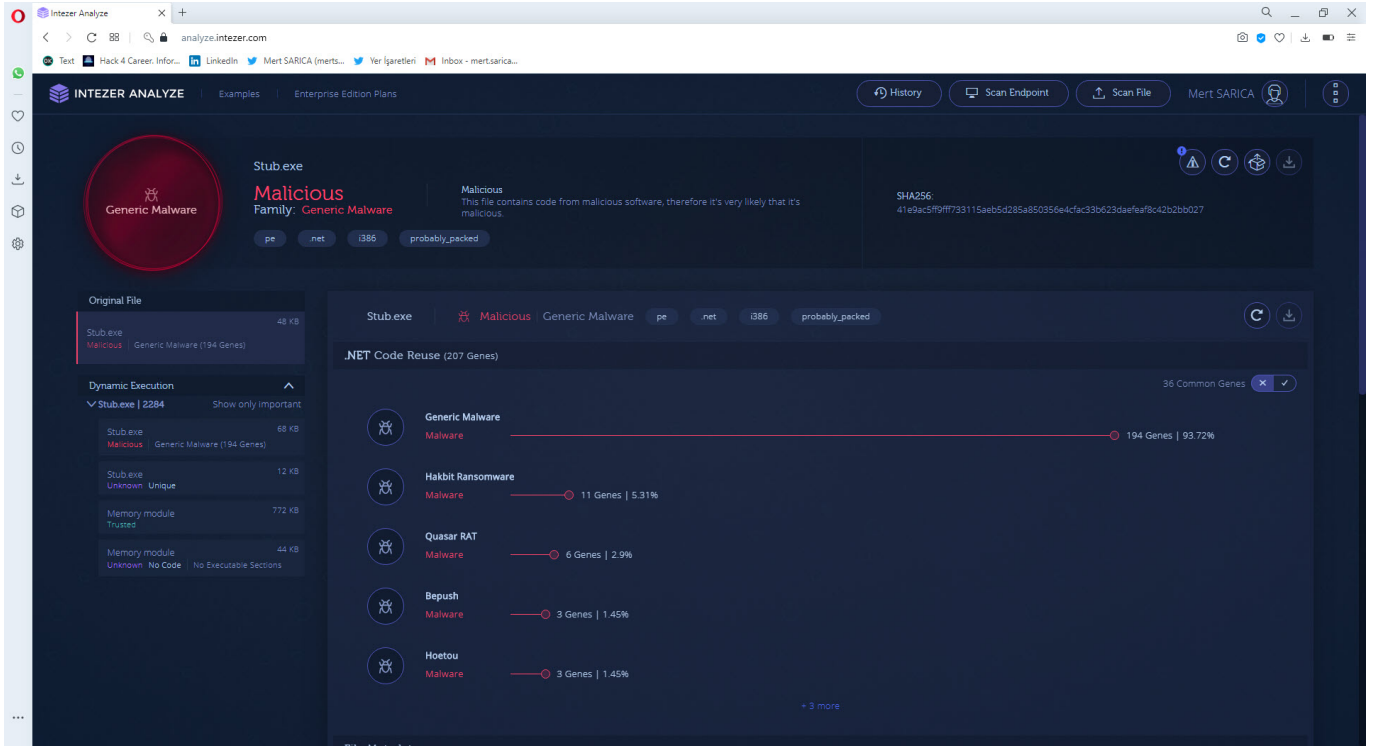
EXE

assembly

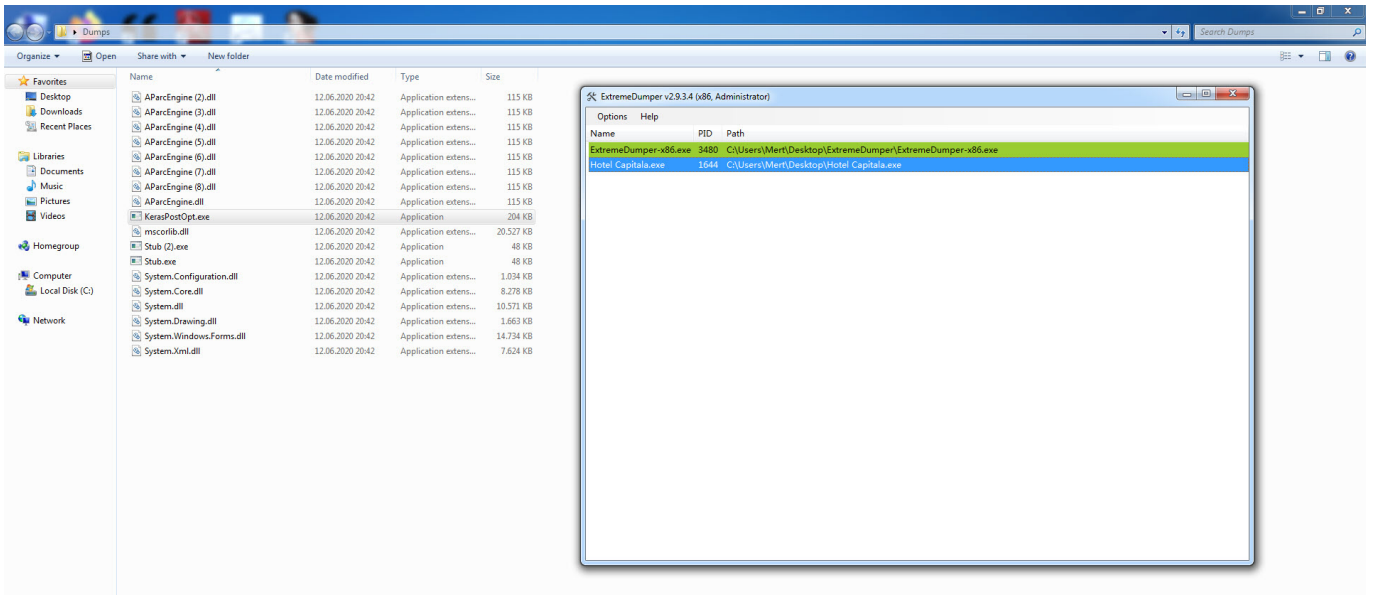
peexe

runtime-modules

DETECTION	DETAILS	RELATIONS	BEHAVIOR	CONTENT	SUBMISSIONS	COMMUNITY
SecureAge APEX	Malicious				Avira (no cloud)	HEUR/AGEN.1118533
BitDefender Theta	Gen:NN.Zemsi.F.34128.mm@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.e818608b6a6dc536
Kaspersky	HEUR: Trojan.Win32.Generic				McAfee-GW-Edition	BehavesLike.Win32.Generic.dc
Microsoft	Trojan.Win32/Vacattac.Cml				Qihoo-360	HEUR/QVM03.0.DA9B.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

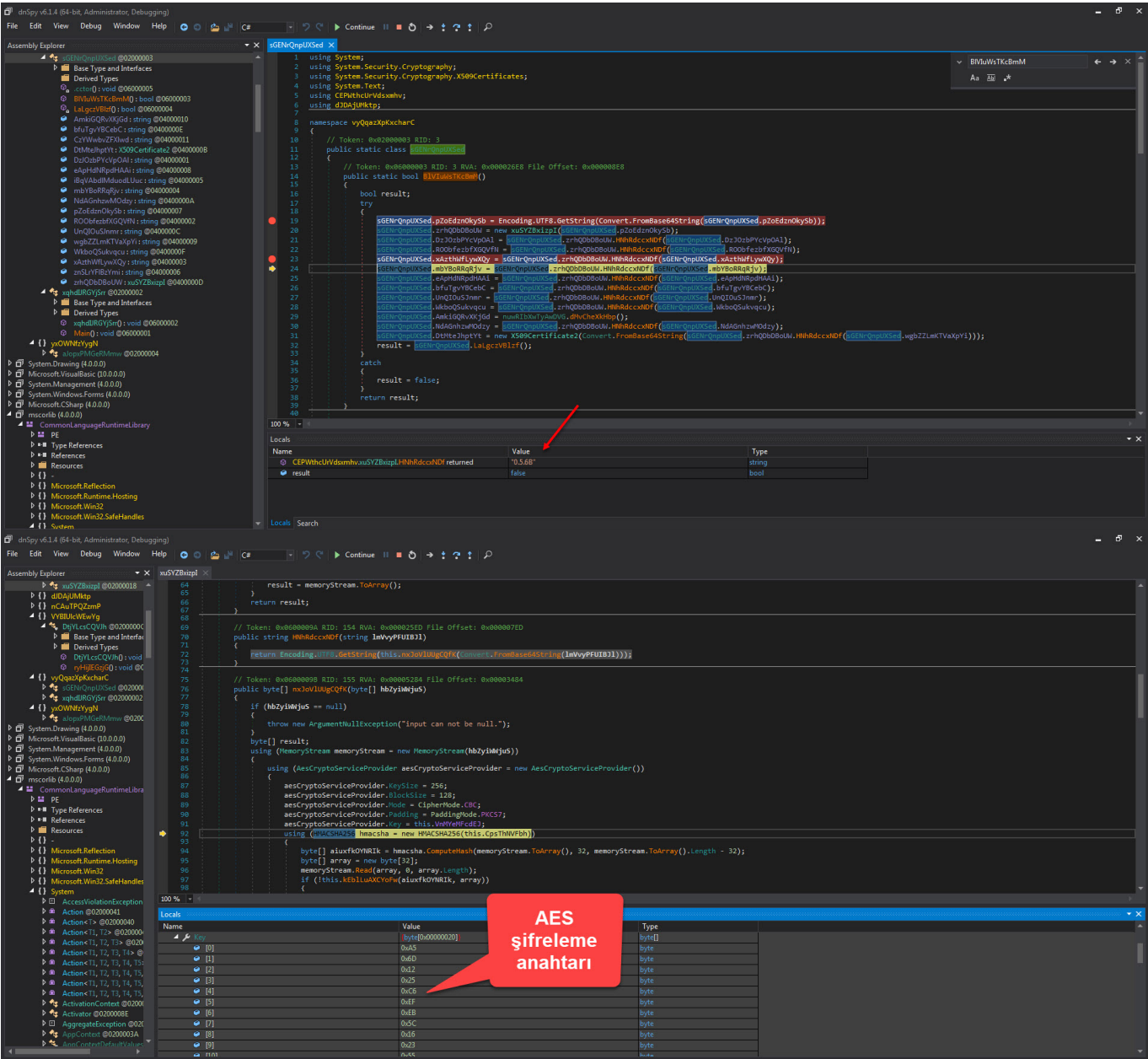


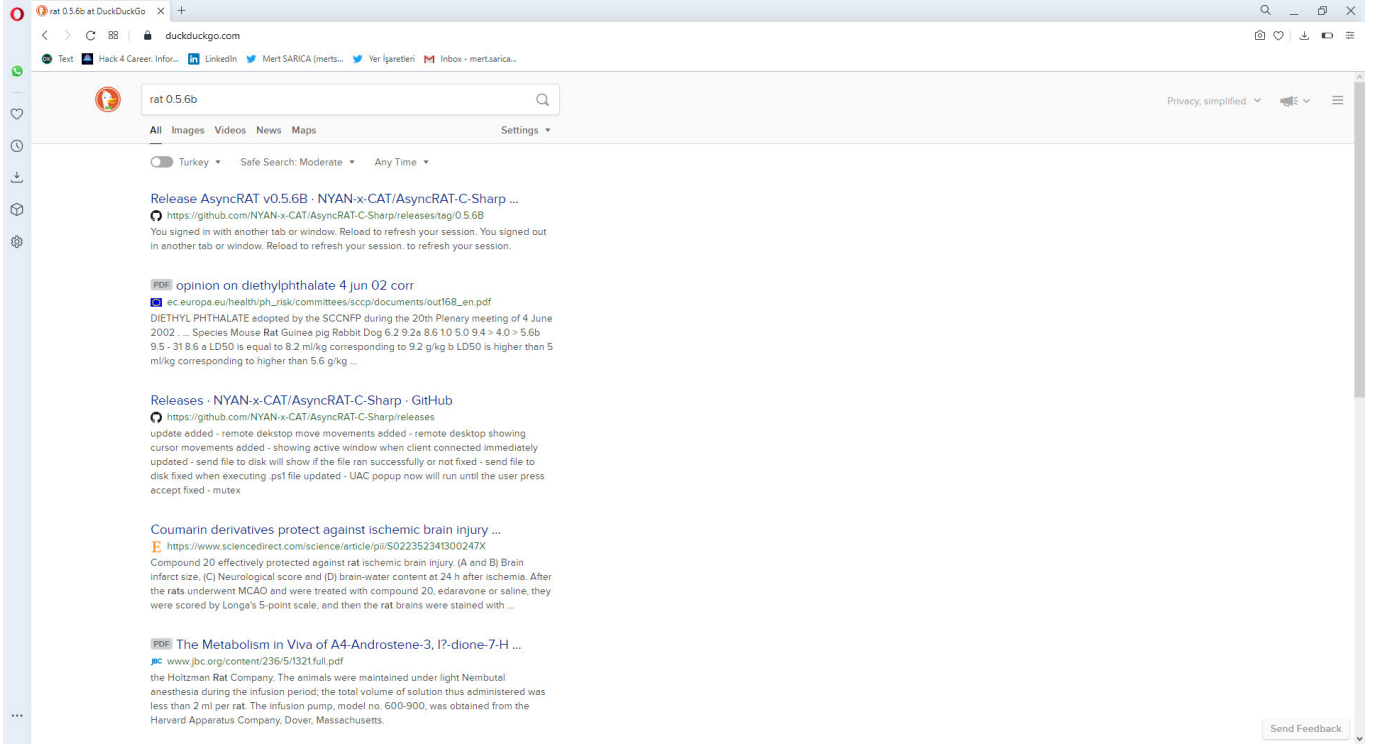
Kendisini gizlemek için elinden geleni yapan tehdit aktörünün geliştirmiş olduğu zararlı yazılımın ne olduğunu öğrenmek için araştırmaya devam ettiğimde sıra dinamik kod analizine geldi ve imdadıma OPSEC başlıklı yazımda kullandığım dnSpy hata ayıklayıcısı yetişti. dnSpy aracı ile hata ayıklamaya başlamadan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



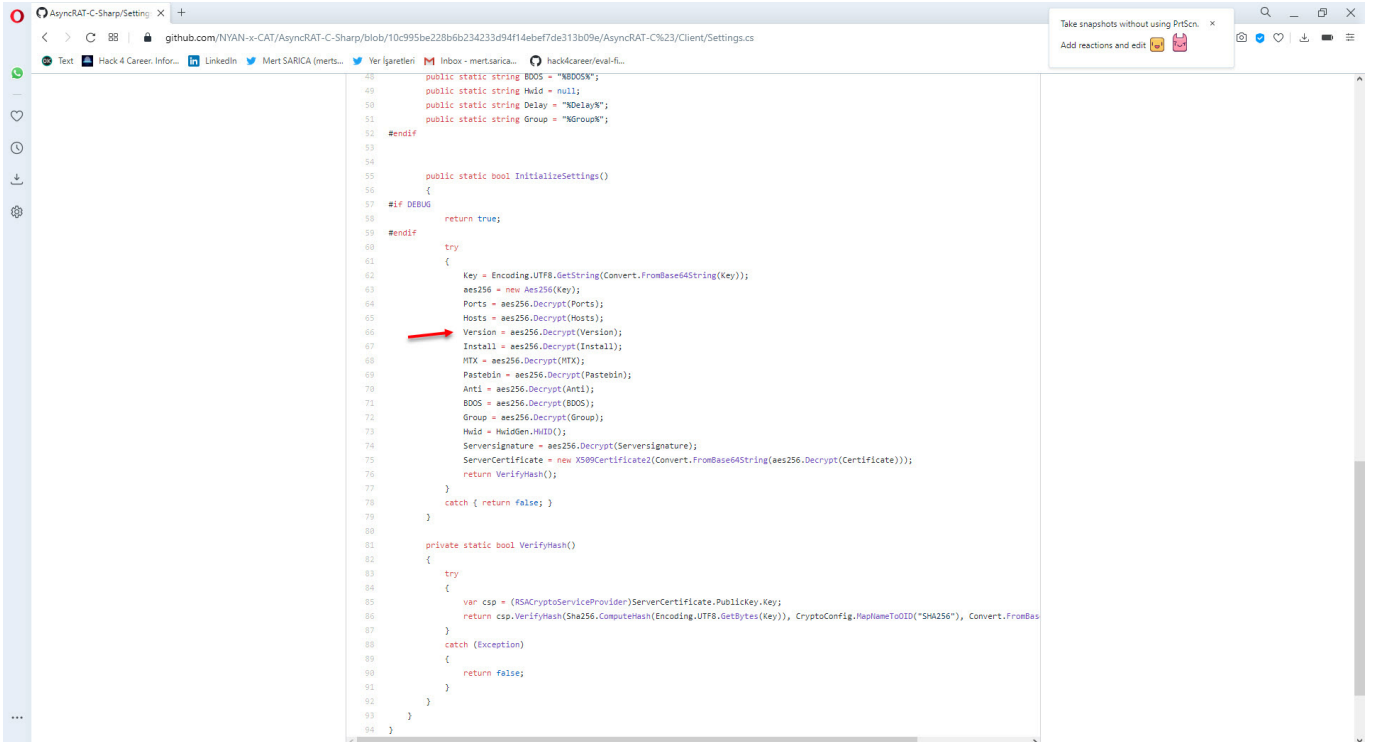
Stub.exe programını adım adım dnSpy ile analiz ettiğim bir noktada AES ile şifrelenmiş olup çözülen 0.5.6B değeri dikkatimi çekti. Bu değeri Google'da "rat 0.5.6B" anahtar kelimeleri ile arattığımda bilin bakalım karşıma ne

çıktı ? Açık kaynak kodlu AsyncRAT! :)



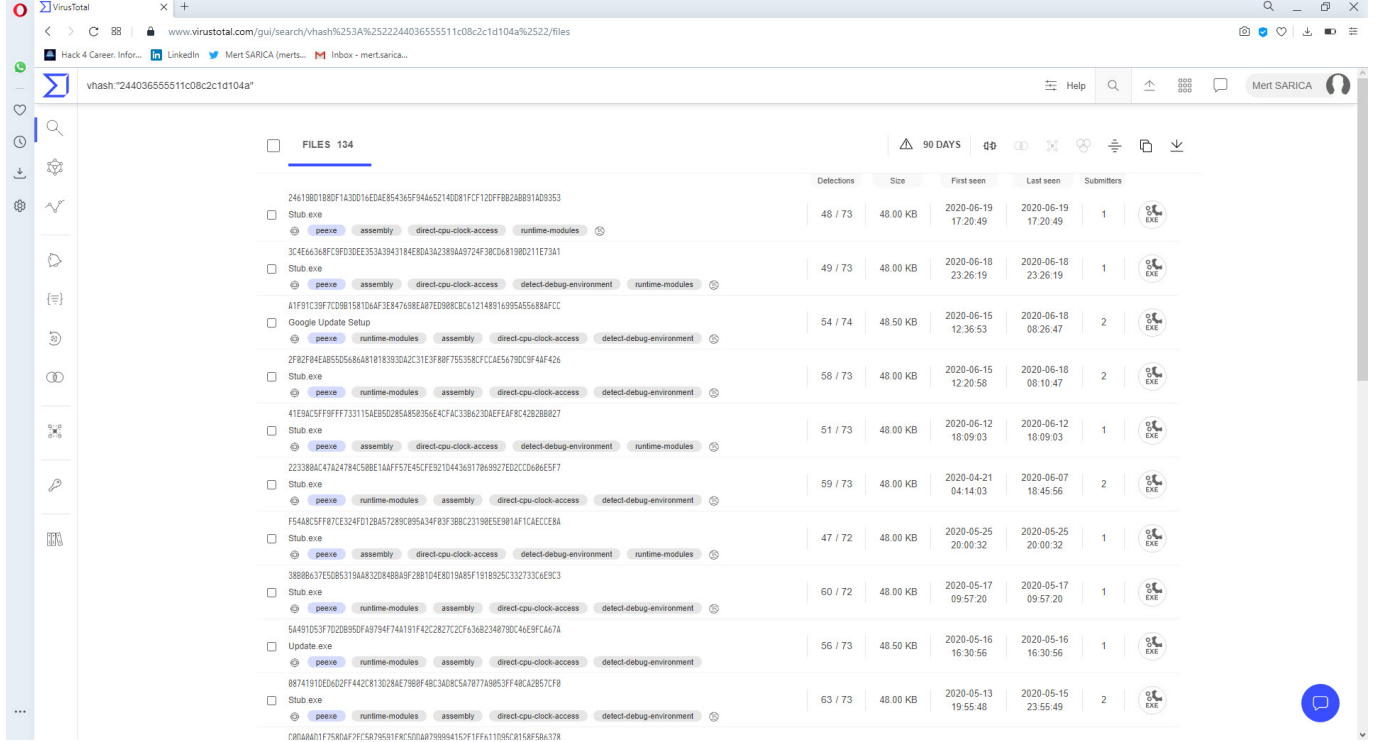


GitHub üzerinde bu projeyi detaylı bir şekilde incelediğimde analiz ettiğim zararlı yazılımın AsyncRAT olduğunu benzer kod bloklarından yola çıkarak doğrulayabildim.



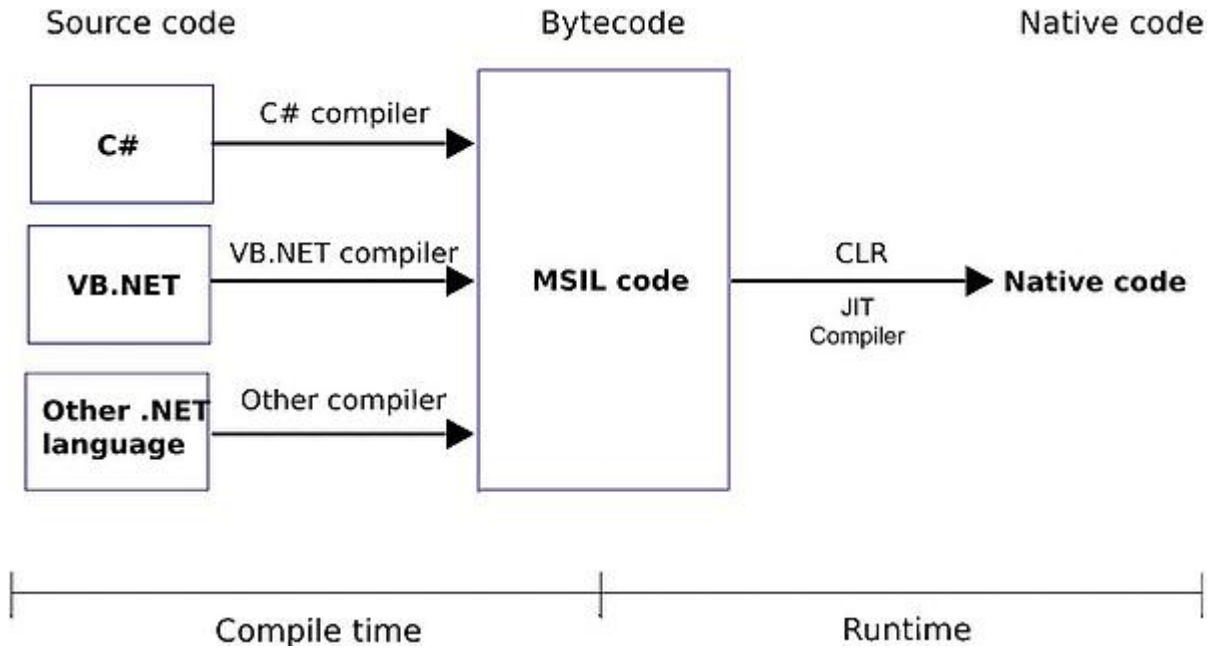
Son aşamada Stub.exe dosyasının benzerlerini vhash ile VirusTotal üzerinde arattığımda çok sayıda örnek ile karşılaştım. Tüm bu örnekler, analiz ettiğim zararlı yazılımdaki Pastebin adresine mi sahip, ortak bir kampanyanın parçası mı diye merak içinde düşünürken ya 50'den fazla her bir örneğin analiz

raporunu inceleyip bunu kontrol edecektim ya da tembellere 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.

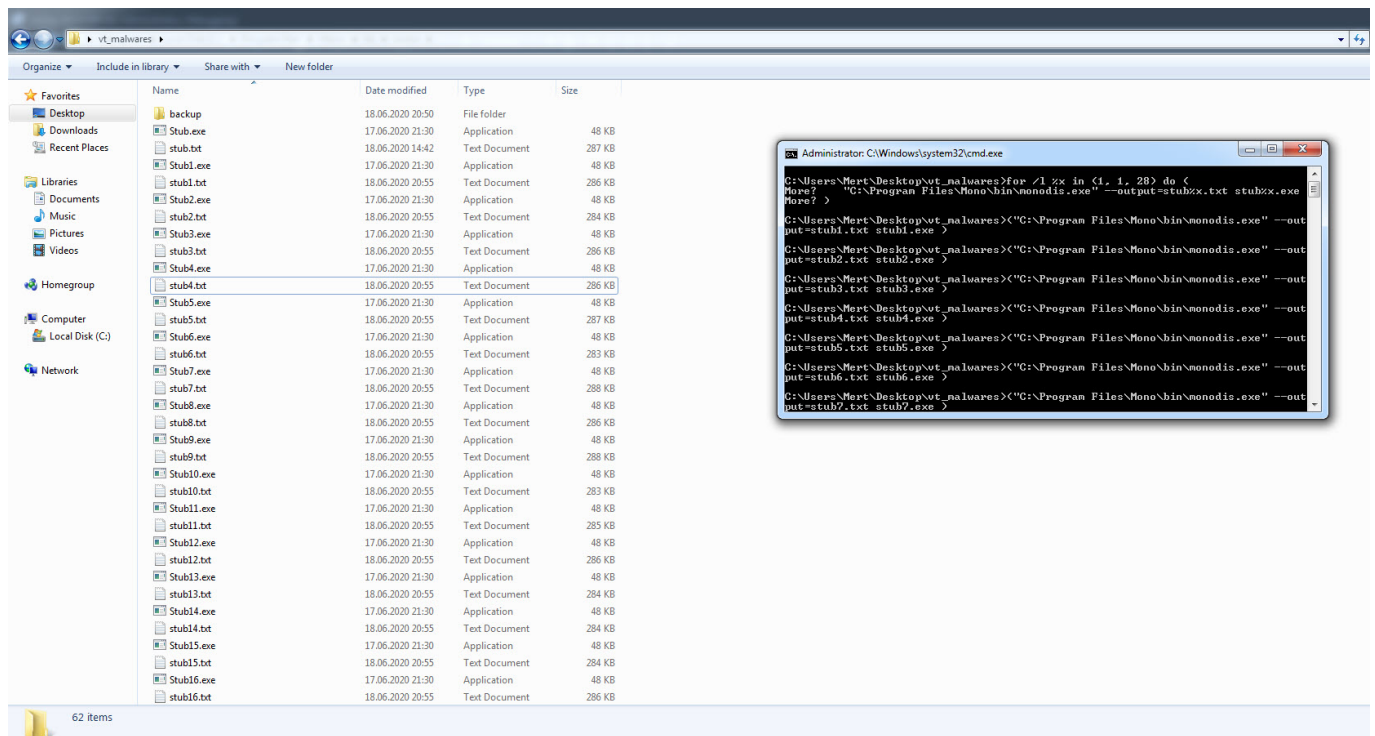


	Detections	Size	First seen	Last seen	Submitters
24619B0180F1A3D01AEDAE85456F94A652140D81FCF120F8B98A8B01A0B353	48 / 73	48.00 KB	2020-06-19 17:20:49	2020-06-19 17:20:49	1
Stub.exe					
3C4E66368CF9D30EE353A3943184E8D43A2389A872F38CD6819B0D211E73A1	49 / 73	48.00 KB	2020-06-18 23:26:19	2020-06-18 23:26:19	1
Stub.exe					
A1F91C39F7CDB1581D6AF3E84768BEA87ED988CB61214931695A55688AFC	54 / 74	48.50 KB	2020-06-15 12:36:53	2020-06-18 06:26:47	2
Google Update Setup					
2F82F84EAB50568A81818393DA2C31E3F88F755358CFCACAE5679C9F44F426	58 / 73	48.00 KB	2020-06-15 12:20:58	2020-06-18 08:10:47	2
Stub.exe					
41E9AC5FF8FF73315AEB50285A85836A64C7AC3B6230AEFA8C42B2BB27	51 / 73	48.00 KB	2020-06-12 18:09:03	2020-06-12 18:09:03	1
Stub.exe					
223388AC47A24784C58BE1A8F57E45CFE9210436917849927E32CCD8A8E5F7	59 / 73	48.00 KB	2020-04-21 04:14:03	2020-06-07 18:45:56	2
Stub.exe					
F548C5FF87CE324F0128A57289C895A34F83F38BC23198E5E901AF1CAECC8A	47 / 72	48.00 KB	2020-05-25 20:00:32	2020-05-25 20:00:32	1
Stub.exe					
3888B637E50B5319A832D8488A9F28B1D4E8019A85F191B925332733CAE9C3	60 / 72	48.00 KB	2020-05-17 09:57:20	2020-05-17 09:57:20	1
Stub.exe					
5A491D53F7D2B950FAB9744191F42C2827C2CF63682348790C46E9FCA67A	56 / 73	48.50 KB	2020-05-16 16:30:56	2020-05-16 16:30:56	1
Update.exe					
86741910ED002FF442C813028AE798BF48C3A08C5A7877A8659FF48CA2957CF8	63 / 73	48.00 KB	2020-05-13 19:55:48	2020-05-15 23:55:49	2
Stub.exe					

Tabii değişken isimleri her bir programda rastgele oluşturulduğu için öncelikle AES anahtarını statik bir değişkenden faydalananarak 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.



```

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 UPjlgOQH6Jmz::2oFvYnkYtXXLEF
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 "+2oYbq/fGzAPhtjZnpOMXGlsfwrXKU5S83HK8xUjlgQdiYXJGu42snGzR4PewQBIMtP6HY0tO4e7fytfIU+9Q=="
333 IL_0005: stsfld string LVEFMHugJpKfAW.UPjlgOQH6Jmz::rLxHRVvktJ
334 IL_000a: ldstr "iug7GHRbtOQLOSEwn9VUWoiYELM1Oums33crJuxW593CxiMMqnpb3WgXcPOVWTM199RmnGMwJEJTORok7zaxFA=="
335 IL_000f: stsfld string LVEFMHugJpKfAW.UPjlgOQH6Jmz::svdWvYtYvrd
336 IL_0014: ldstr "rPw0jQKdu9pvg855Fn7awWpK01nCuZ0hPwjWBIQZ1+9XMo59v72jmaJGMP8/IttgUwM/1xu7r783NE87w=="
337 IL_0019: stsfld string LVEFMHugJpKfAW.UPjlgOQH6Jmz::JgTlyvvoPOKlRmBT
338 IL_001e: ldstr "C3R2LaC/AAuTupNsvrylug2GZ0k6G5Dq5v8kvkz2lvPHCAhMhbLterGeKcQCNFdqdkik/czvKbD5jDPxrtKvq=="
339 IL_0023: stsfld string LVEFMHugJpKfAW.UPjlgOQH6Jmz::Wcx3dUcxhhTm
340 IL_0028: ldstr "%AppData%"
341 IL_002d: stsfld string LVEFMHugJpKfAW.UPjlgOQH6Jmz::RifTFGCaJom
342 IL_0032: ldstr "Host Process for Windows Host.exe"
343 IL_0037: stsfld string LVEFMHugJpKfAW.UPjlgOQH6Jmz::IgQueZnoVept
344 IL_003c: ldstr "c65t8z2nUF1QSULnNU9ic3A5NjFkbk5QVX1JYmRJWwk="
345 IL_0041: stsfld string LVEFMHugJpKfAW.UPjlgOQH6Jmz::bWvENFAunePP
346 IL_0046: ldstr "wW+9tAg5GsnOnDZHUFEF+Kk+F7BiDKG37CwS9tEbDysC2Cw9gM1W/PAAB6B6BMkI2i6c1SAGx+jtAhpGiw=="
347 IL_004b: stsfld string LVEFMHugJpKfAW.UPjlgOQH6Jmz::BsgWQULPSxB
348 IL_0050: ldstr
349 "ufKCUobOYg+e1E1Xgk+eKgnW/PztVtK6Kiv9V9GtXPF0JUVOSKcFgZbiAkY+M0YnQ4H62D2SpL2VhhWuiiYlYmnrCP4jcgH/HYvYatoimWOCRF6gOXBp8QvRukan0yOS2FakIpQdgmGciWf/RJV8+ocX7aWJkCo7mT6jJiry
350
351 IL_0037: call unsigned int8[] class [mscorlib]System.Convert::FromBase64String(string)
352 IL_0038: callvirt instance bool class [mscorlib]System.Security.Cryptography.RSACryptoServiceProvider::VerifyHash(unsigned int8[], string, unsigned int8[])
353 IL_0041: stloc.0
354 IL_0042: leave.s IL_0049
355
356 } // end .try 0
357 catch class [mscorlib]System.Exception { // 0
358 IL_0044: pop
359 IL_0045: ldc.i4.0
360 IL_0046: stloc.0
361 IL_0047: leave.s IL_0049
362
363 } // end handler 0
364 IL_0049: ldloc.0
365 IL_004a: ret
366 } // end of method vUuBwDuS1lr::TMIjBOTGNDfCEWQ
367
368 // method line 5
369 .method private static hidebysig specialname rtspecialname
370 | default void '.cctor' () cil managed
371 {
372 | // Method begins at RVA 0x288c
373 |// Code size 151 (0x97)
374 |.maxstack 1
375 IL_0000: ldstr "JmPCaie5F3vCQEmfV+2XI077HoufVowR2ztSjnr1mJOS6Nc/0/osU12DQmMR4DY0ORfyGYP3MKHs6OSA2dg=="
376 IL_0005: stsfld string McuCaiaCqjz.vUuBwDuS1lr::wEmhLnk2HX
377 IL_000a: ldstr "i/8hipMa6LMe2U9YeIWe0u82pzhfebvBoIT+DFDdowKqIi75xtr87t12X1xkuGIRW4t1aIa6DxekFvwnjxa7bs3lp7QAXbXvrgZsYmVtnq=="
378 IL_000f: stsfld string McuCaiaCqjz.vUuBwDuS1lr::AmbSEfKfVyi
379 IL_0014: ldstr "wzaHdLAKC0wocYCF6513KMF8Wbwoz3XUkjaAh2rS0JdJAhMrDq38+CQ1071t4qbMt1R0+nPU638ucKc82A=="
380 IL_0019: stsfld string McuCaiaCqjz.vUuBwDuS1lr::LorEpVhKvWe
381 IL_001e: ldstr "ndT5oubUy9YDYVe+AAxU87bZiWBEDfndFdeRBMAYODFvF7JkPt6M46w1x7hRqA/RnxLjfqdBaAaziFMD3D0w=="
382 IL_0023: stsfld string McuCaiaCqjz.vUuBwDuS1lr::MyLHXIGOFX
383 IL_0028: ldstr "%AppData%"
384 IL_002d: stsfld string McuCaiaCqjz.vUuBwDuS1lr::cbYpYfPwYi
385 IL_0032: ldstr ""
386 IL_0037: stsfld string McuCaiaCqjz.vUuBwDuS1lr::oEcGinZjIGB
387 IL_003c: ldstr "TXyQ020ymGRXS12FeGx1TgipVXpusD11b29pZU03TFU="
388 IL_0041: stsfld string McuCaiaCqjz.vUuBwDuS1lr::nkgtoXYXkrTgV
389 IL_0046: ldstr "Z6K6P100rezSi+xxH14Eh41519m2nGZpIAYORzS12Mko/jfYcic6aszmxCSy5Yb47a135tESSVD/ydY7pNq2EEici0RPvciKGNdXS5c=="
390 IL_004b: stsfld string McuCaiaCqjz.vUuBwDuS1lr::gEcndXaLbq
391 IL_0050: ldstr
392 "gHVqZ2BMckrUWw4h+UFw+YdY6pP39J12tRudoLpVfFrJw+Of0bUUGuUNYwKLTzLwNLD1KDJH15Nk/RcYQ8fzIpeIXYGLZBzqF8MQos0VTHVciSRPvRsk+JJSzofvBbbRfAN+wQq+cPduvUrfTfXoiJ9pxXsGUVBi7AiigKFP5XyPuZ

```

```

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 "2bSxod6szoxlbq2bnUKlvJxcLa5Xl4O7KBe0zAs5TJ/wCIRB3vOakvztdDdRTEjQ/so8HlFQRvvObcxkyH/4w=="
333     IL_0005: stsfld string MiKCRUQuXTimcp.zbgTqalHViUFHwT::NGswHYqPHetj
334     IL_000a: ldstr "Sz/oQI8Um2lJoEh+RLHl+/aqTwM/v4//yvHYbU+ljWTzx2TpcC3Zq6valHkGDsdDESTpmAw6k5ECGJ9mWa2sWA=="
335     IL_000f: stsfld string MiKCRUQuXTimcp.zbgTqalHViUFHwT::dyhWpMOSFuwv
336     IL_0014: ldstr "o+yEwOEwgIbvXx5f2LIXc2xqQHt7+OS5sJSKJ7rM23KrGS1SVx0+4Zu0dzJ37Kv6vMT3Syq+PCaxKj2yhPIHA=="
337     IL_0019: stsfld string MiKCRUQuXTimcp.zbgTqalHViUFHwT::tHgFMSfeqgk
338     IL_001e: ldstr "zTzAZIRKARK3BzLqyePdEpMcunOT7EfJ9I3e4vWss8Ze7uukigGJIJy5YV+NT3aylkvbPt7dnA5uTyW9/iMuHw=="
339     IL_0023: stsfld string MiKCRUQuXTimcp.zbgTqalHViUFHwT::kcPNciqUJTXfcm
340     IL_0028: ldstr "%AppData%"
341     IL_002d: stsfld string MiKCRUQuXTimcp.zbgTqalHViUFHwT::iUTvfauwhzOEb
342     IL_0032: ldstr "tasksync.exe"
343     IL_0037: stsfld string MiKCRUQuXTimcp.zbgTqalHViUFHwT::brwgbfftiOPhE
344     IL_0038: ldstr "Y2k3V1ZqRzRNNUtYaVdq23hNR29QQ3Nxdndjbc0b04="
345     IL_0041: stsfld string MiKCRUQuXTimcp.zbgTqalHViUFHwT::X2muTNrwTta
346     IL_0046: ldstr "lgJvAgU4nQcQm2Fib46gNrnLBwSml+Pxm75cs07XD4Qs/nsbLl183vtWJcXsm6gjeWPrPXWE6lm3gmg+Dd+GRQVbntoDuHRK6LpZiKNBSb2Y="
347     IL_004b: stsfld string MiKCRUQuXTimcp.zbgTqalHViUFHwT::cHIPEjYUqaz
348     IL_0050: ldstr
349     "eoy7EfVYnBkBY+zrhx6M/Nneiti152ah+orgcGFNFdgsOXwKqeMl+piKW4xu49Lw2XQKP+n8xmYk8WC7+oQhvLgY4L1gxGntwMTLrXAZwF2hGh/ysDY1NvIi1ljImx2SNrOJJqi2E2ekwRoVEY4YVb6bdR0fU090E+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: bqwzfgezbfqx0

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: glllhiysywwkfbzbbw
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: qrpmfkwjlpjppobq
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.