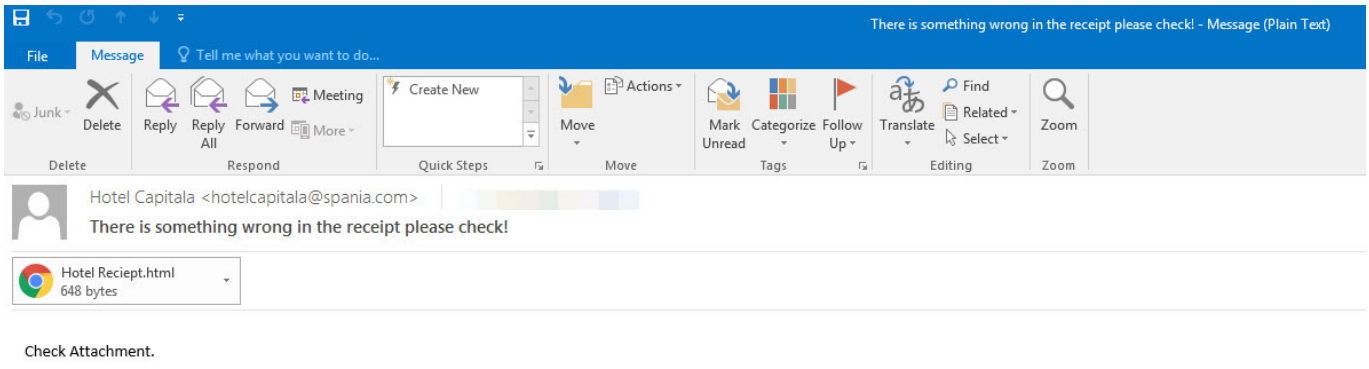
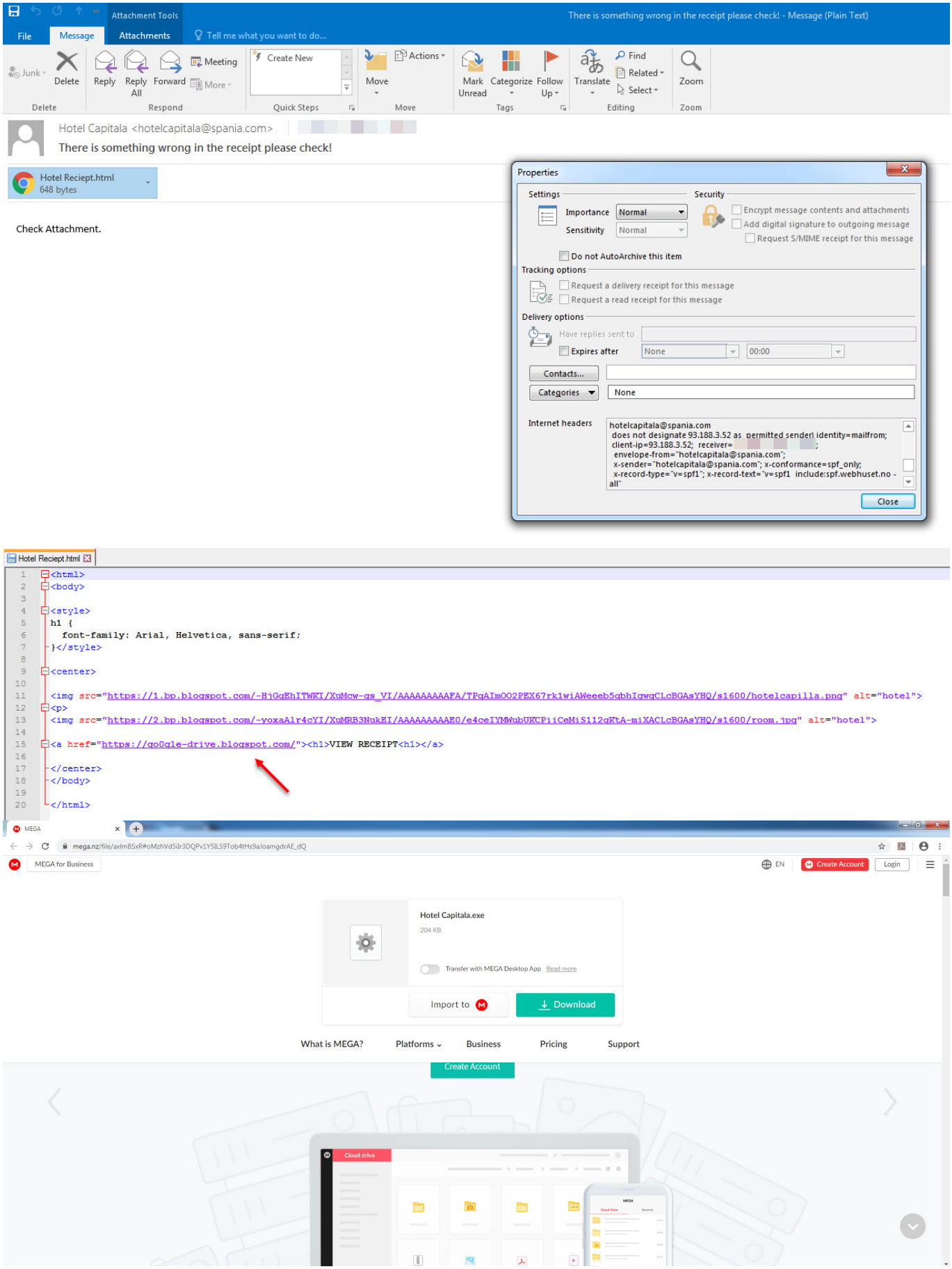
Kaçabilirsin ama Saklanamazsın

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://go0gle-drive[.]blogspot[.]com) takip edilirse, hedef alınan kişi mega.nz isimli dosya saklama ve paylaşım sitesindeki bir adrese (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.

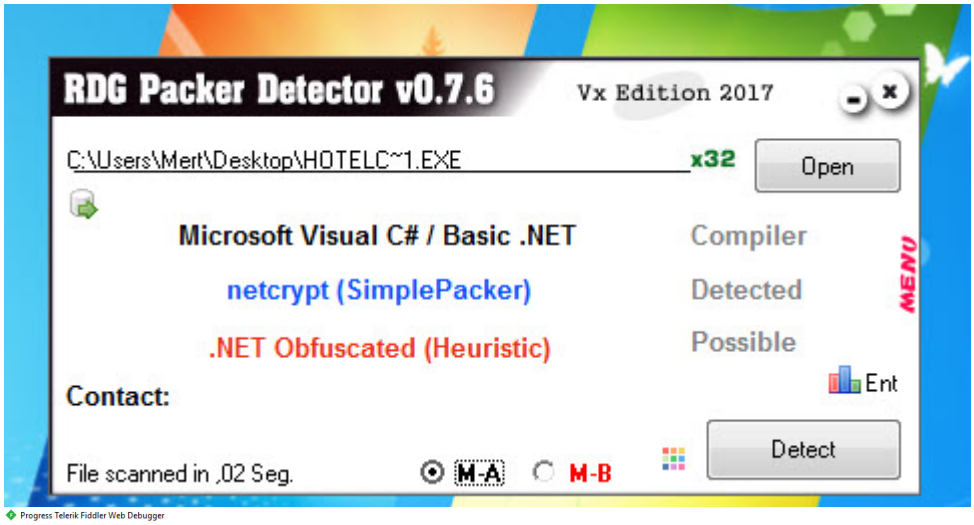


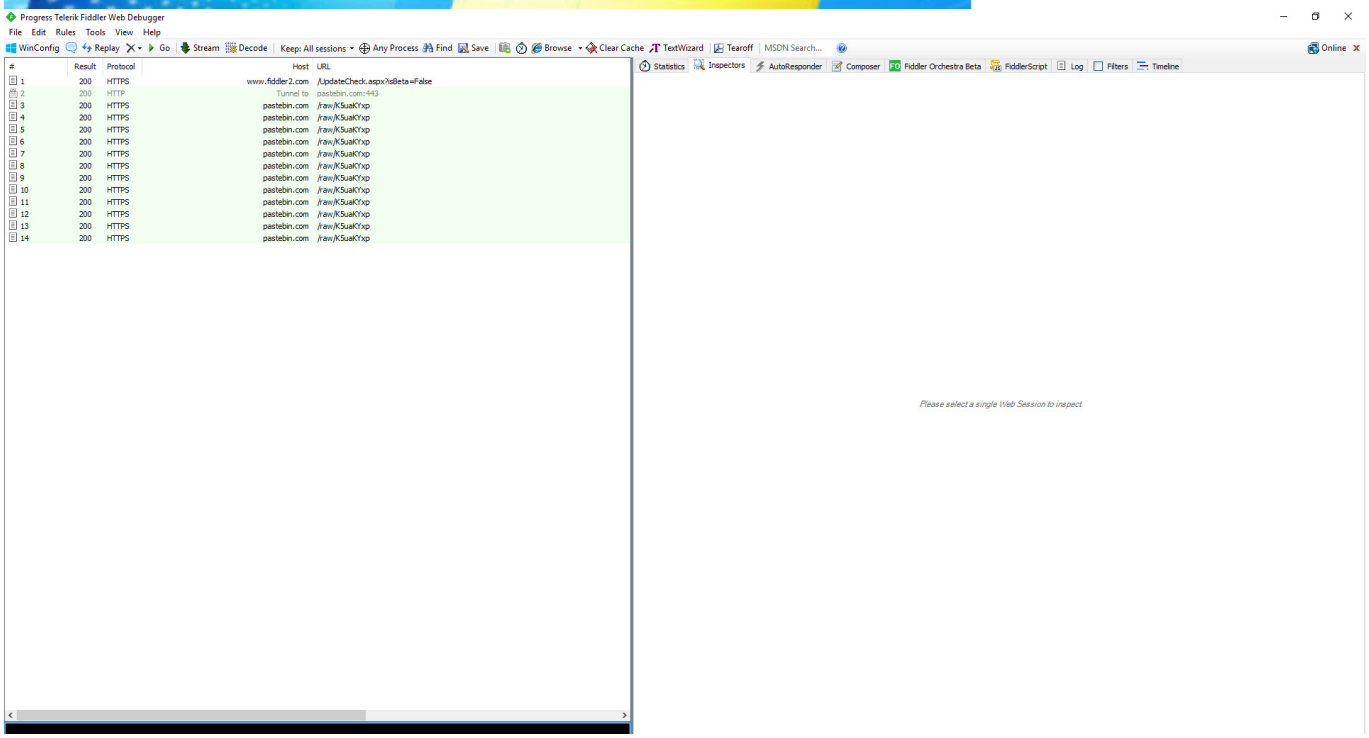


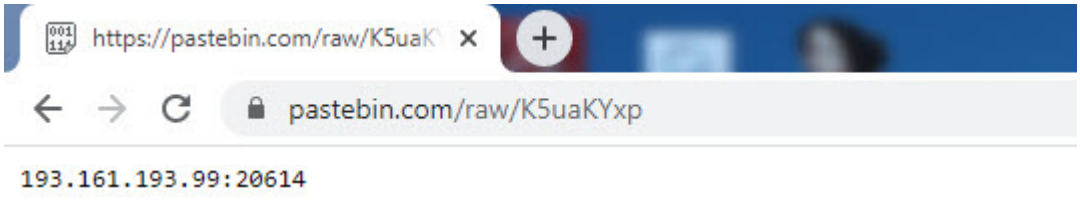
Bir kurum yukardaki gibi bir senaryo ile karşılaştığında, saldırı girişimi başarıya ulaşmasa da konuyu büyük bir dikkatle ele almalıdır çünkü bu öncü bir sarsıntı olup ardından gelecek büyük depremin işaretçisi olabilir

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.



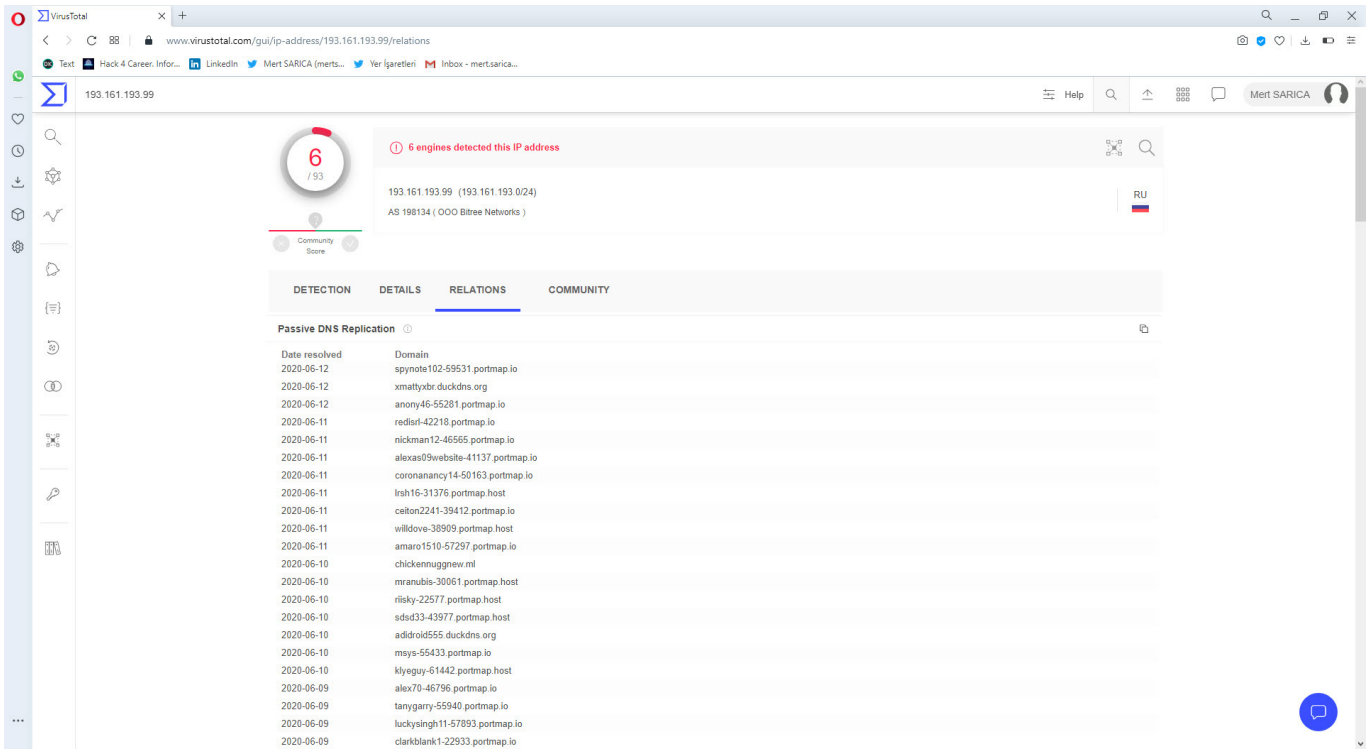


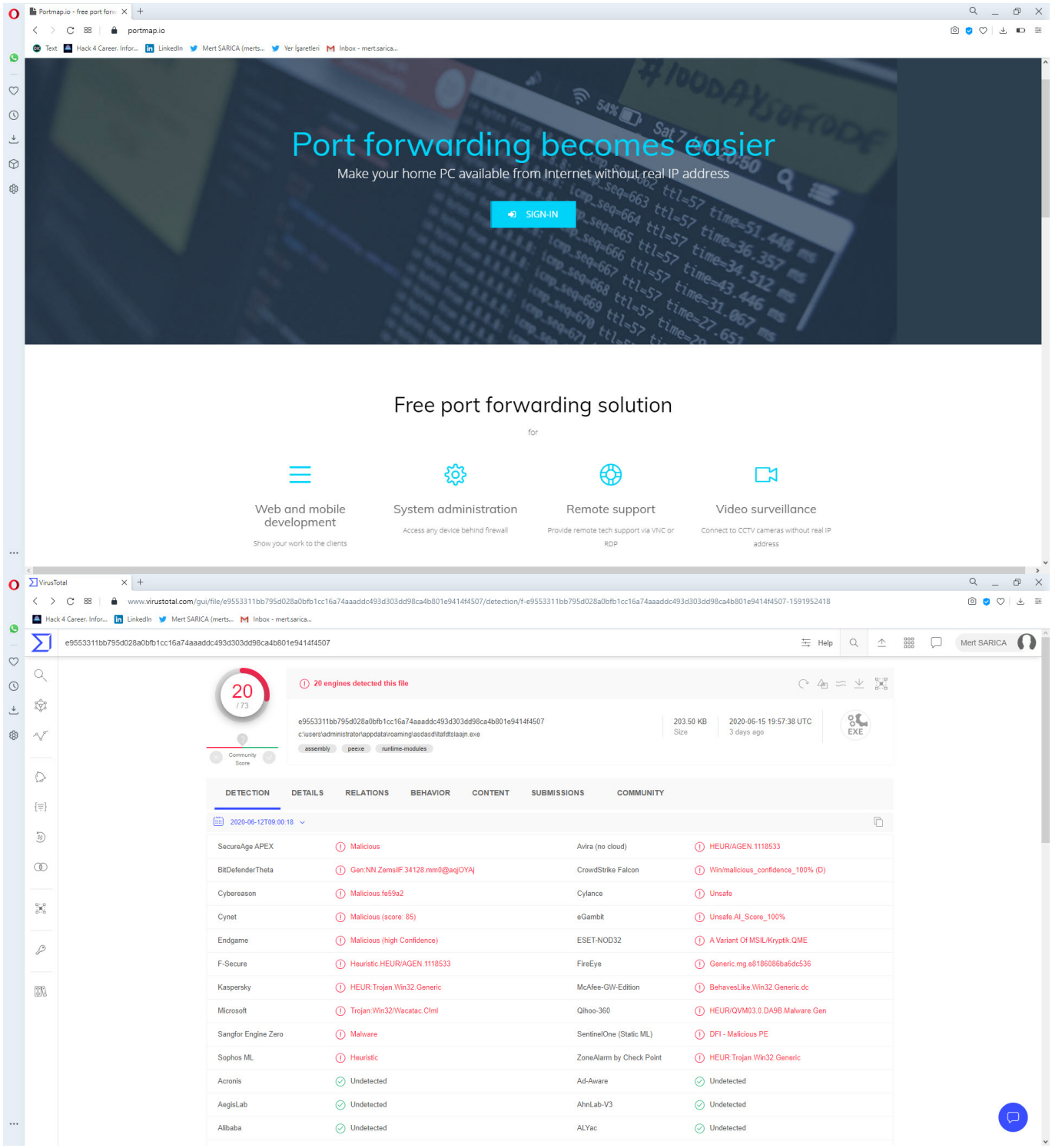


Özellikle APT saldırılarında kullanılan zararlı yazılımlar tehdit aktörleri tarafından özel olarak geliştirildiği ve saldırıdan hemen önce derlendiği için VirusTotal'a yüklendiğinde çoğunlukla genel bir imza adı altında (Backdoor, Trojan vb) tespit edilmektedir. Bu gibi durumlarda Intezer gibi servislerden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

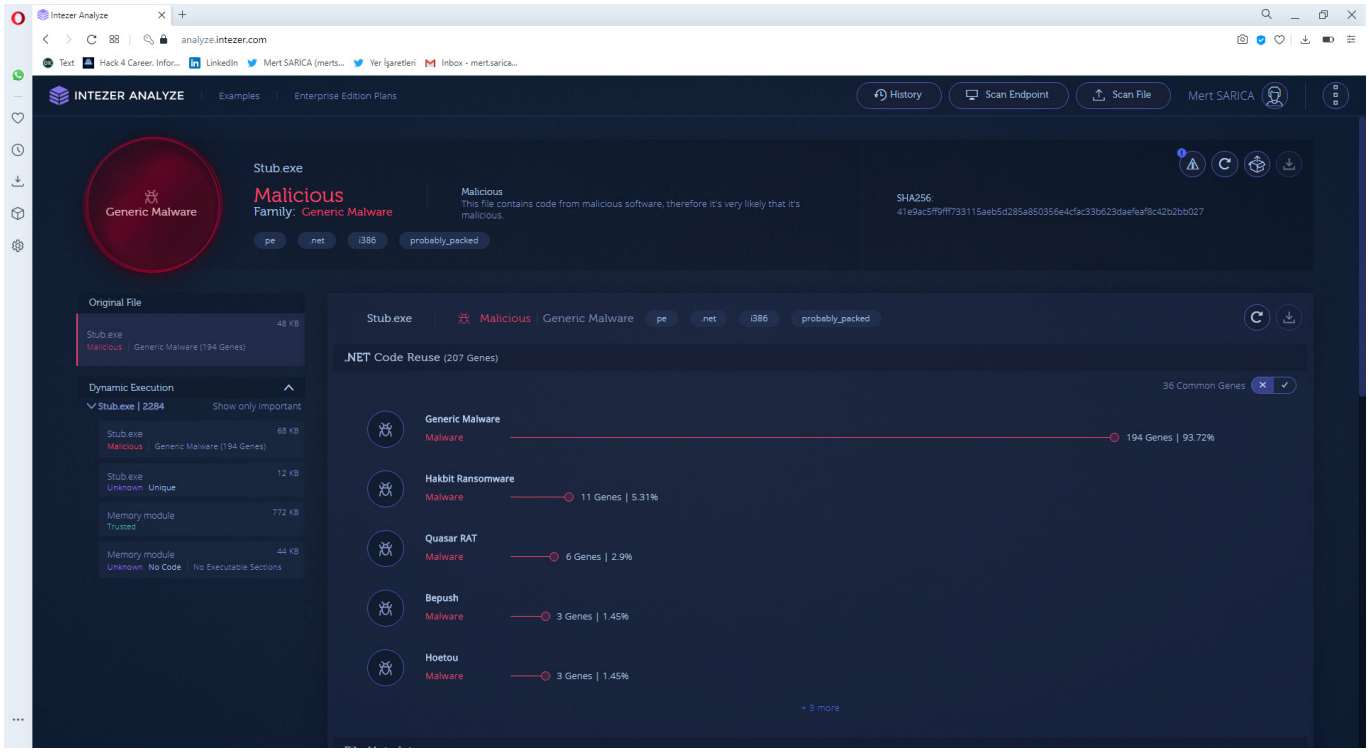
Bu zararlı yazılımı VirusTotal'a yüklediğim spesifik olarak bir zararlı yazılımla eşleştirilmediğini gördüm. Bunun üzerine Intezer üzerinde arama yaptığımda da maalesef yine elim boş kaldı. (Generic Malware)

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.

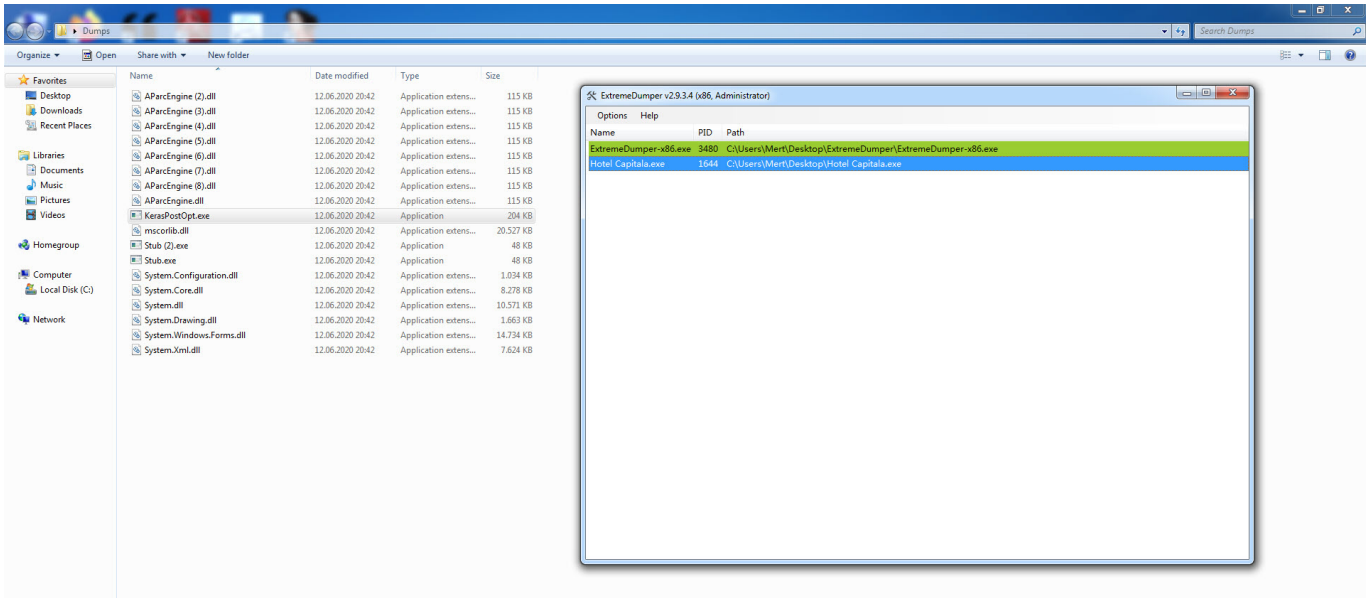



Portmap.io - free port forw
portmap.io
Port forwarding becomes easier
Make your home PC available from Internet without real IP address
SIGN-IN
Free port forwarding solution
for
Web and mobile development
Show your work to the clients
System administration
Access any device behind firewall
Remote support
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
e9553311bb795d028a0bfb1cc16a74aaaddc493d303dd98ca4b801e9414f4507
Help
Mert SARICA
20
/73
20 engines detected this file
e9553311bb795d028a0bfb1cc16a74aaaddc493d303dd98ca4b801e9414f4507
c:\users\administrator\appdata\roaming\asdasdfiltafdtslaajn.exe
assembly
peexe
runtime-modules
203.50 KB
Size
2020-06-15 19:57:38 UTC
3 days ago
EXE
DETECTION
DETAILS
RELATIONS
BEHAVIOR
CONTENT
SUBMISSIONS
COMMUNITY
2020-06-12T09:00:18
SecureAge APEX
Malicious
Avira (no cloud)
HEUR/AGEN.1118533
BitDefenderTheta
Gen:NN.ZemsilF.34128.mm0@aqjOYAj
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.e8186086ba6dc536
Kaspersky
HEUR:Trojan.Win32.Generic
McAfee-GW-Edition
BehavesLike.Win32.Generic.dc
Microsoft
Trojan:Win32/Wacatac.C!ml
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

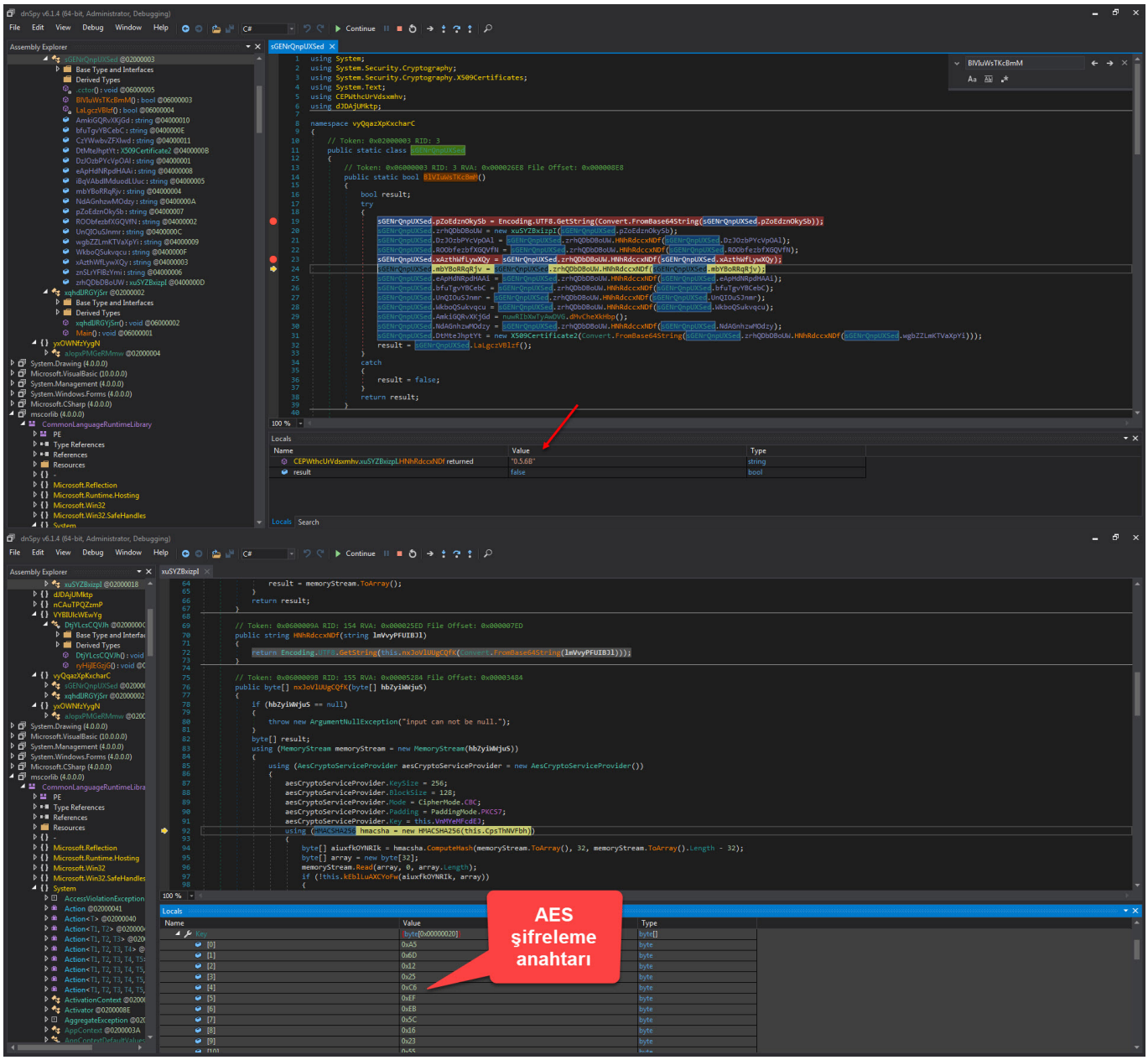


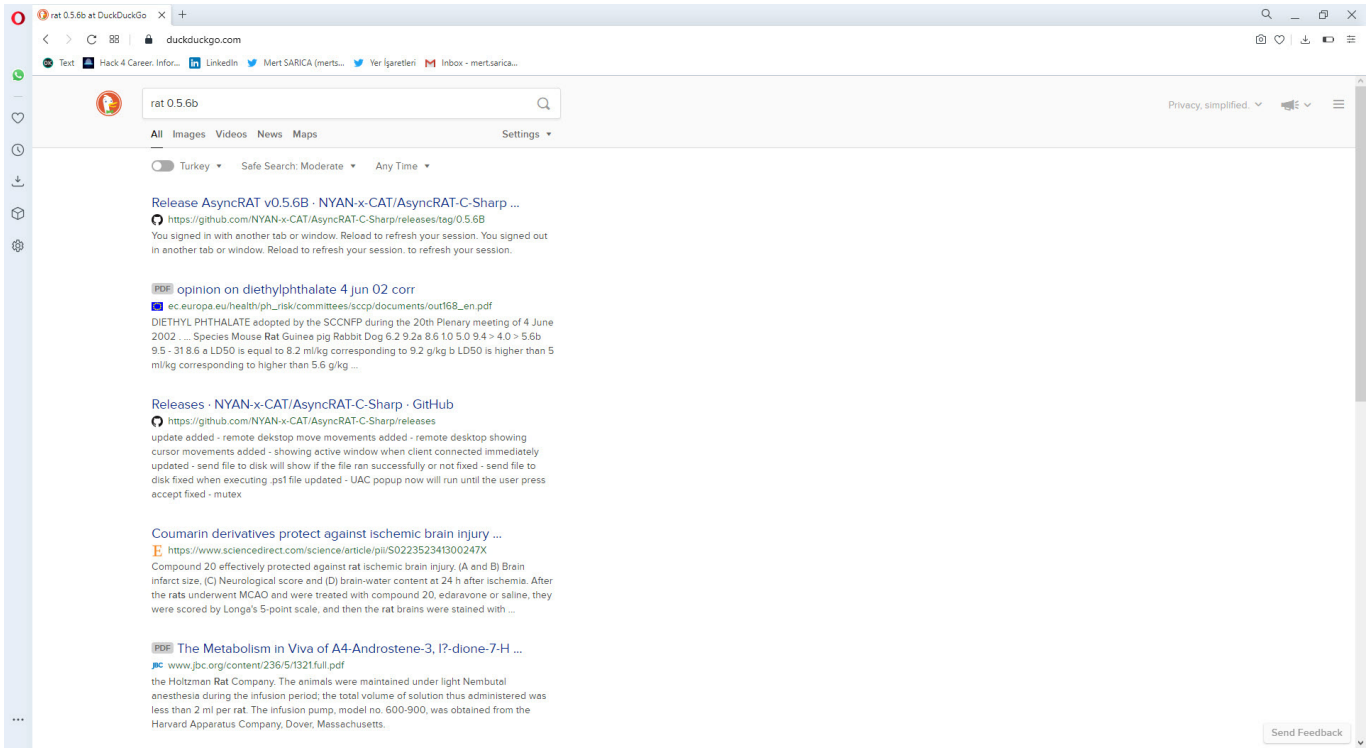
Kendisini gizlemek için elinden geleni yapan tehdit aktörünün geliştirmiş olduğu zararlı yazılımın ne olduğunu öğrenmek için araştırmaya devam ettiğimde sıra dinamik kod analizine geldi ve imdadıma OPSEC başlıklı yazımda kullandığım dnSpy hata ayıklayıcısı yetişti. dnSpy aracı ile hata ayıklamaya başlamadan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



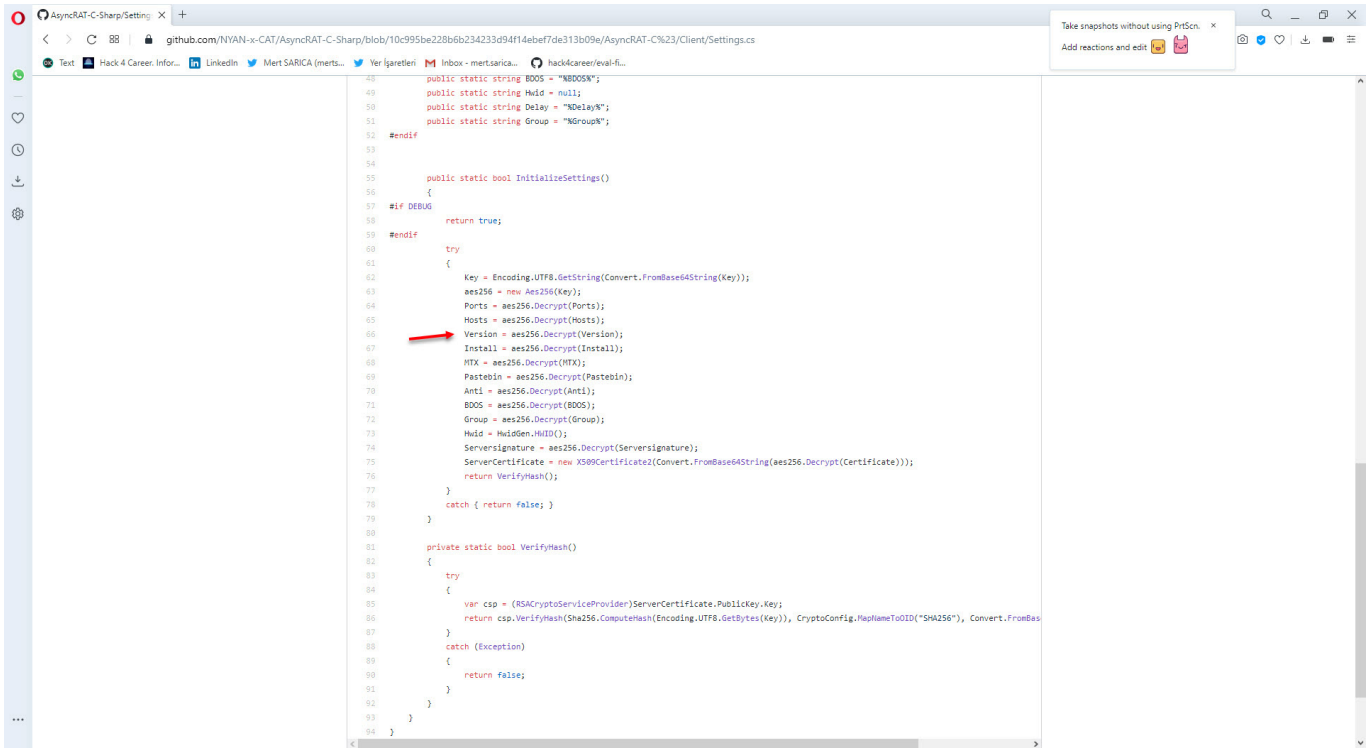
Stub.exe programını adım adım dnSpy ile analiz ettiğim bir noktada AES ile şifrelenmiş olup çözülen 0.5.6B değeri dikkatimi çekti. Bu değeri Google'da "rat 0.5.6B" anahtar kelimeleri ile arattığımda bilin bakalım karşıma ne

çıktı ? Açık kaynak kodlu AsyncRAT! :)



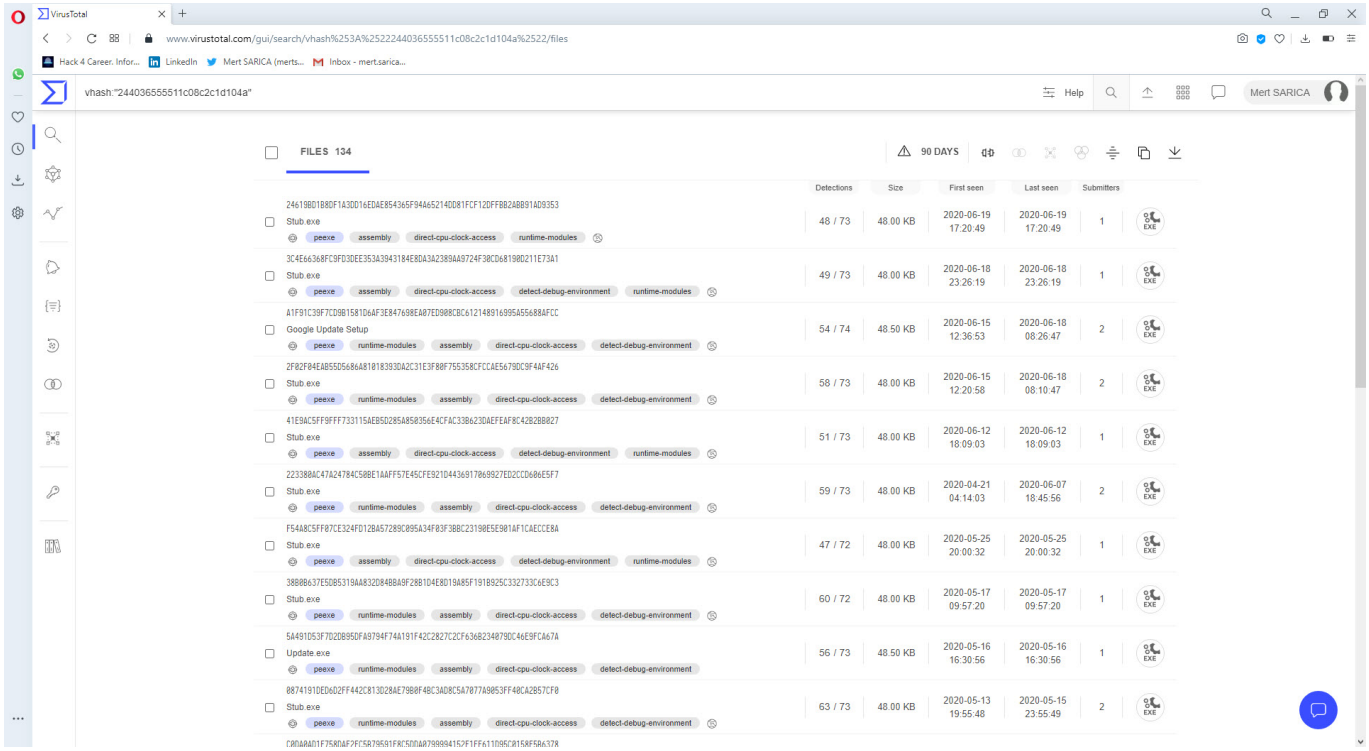


GitHub üzerinde bu projeyi detaylı bir şekilde incelediğimde analiz ettiğim zararlı yazılımın AsyncRAT olduğunu benzer kod bloklarından yola çıkarak doğrulayabildim.

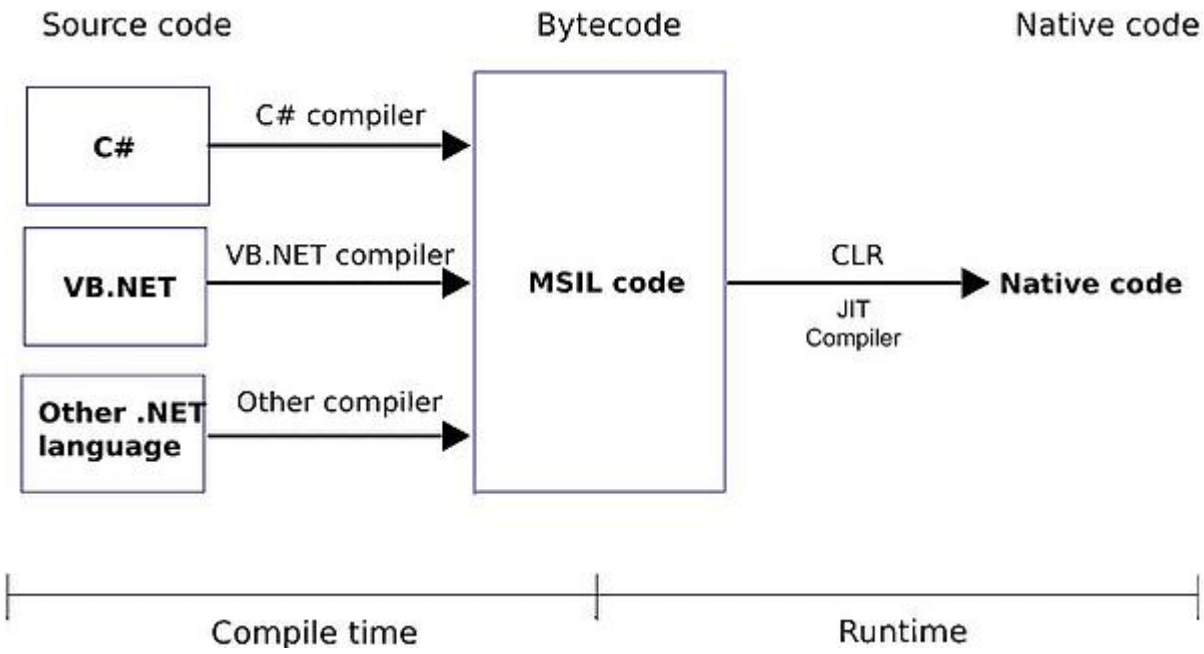


Son aşamada Stub.exe dosyasının benzerlerini vhash ile VirusTotal üzerinde arattığımda çok sayıda örnek ile karşılaştım. Tüm bu örnekler, analiz ettiğim zararlı yazılımdaki Pastebin adresine mi sahip, ortak bir kampanyanın parçası mı diye merak içinde düşünürken ya 50’den fazla her bir örneğin analiz

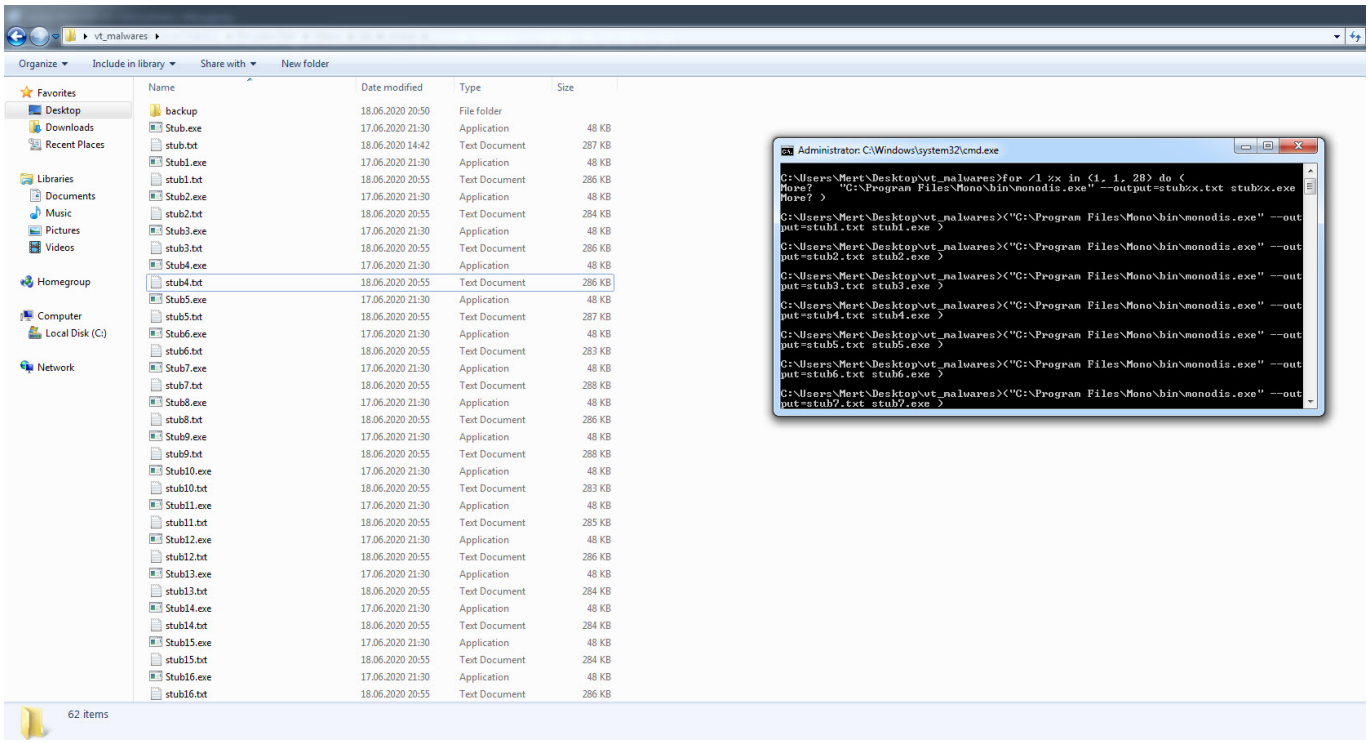
raporunu inceleyip bunu kontrol edecektim ya da tembellere yakışır çok kısa ve pratik bir yol bulacaktım. :) Hindi gibi düşünmeye başladıktan sonra aklıma Python ile tüm bu örnekleri statik olarak analiz ederek önce AES şifreleme anahtarını bulan ve ardından da konfigürasyon bilgilerini çıkaran bir araç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



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.



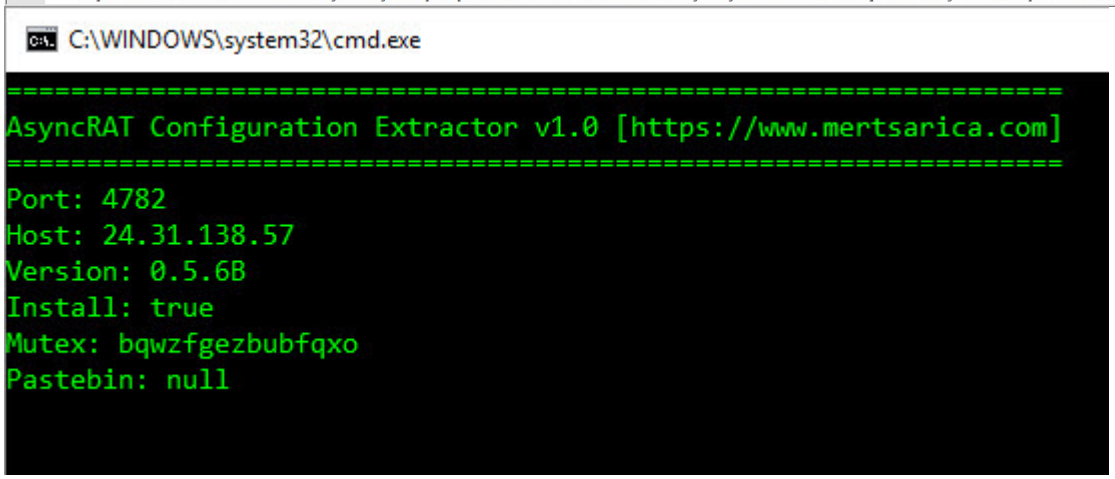
Bunun için meşhur Mono projesinde yer alan Mono Disassembler (monodis) aracından faydalanmaya karar verdim. Monodis aracı ile tüm Stub.exe örneklerini koda çevirdikten sonra AES şifreleme anahtarının her daim 0x288c değerinden sonra gelen IL_003c değerinde olduğunu tespit ettim. ve bu bilgilerden faydalanarak 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.

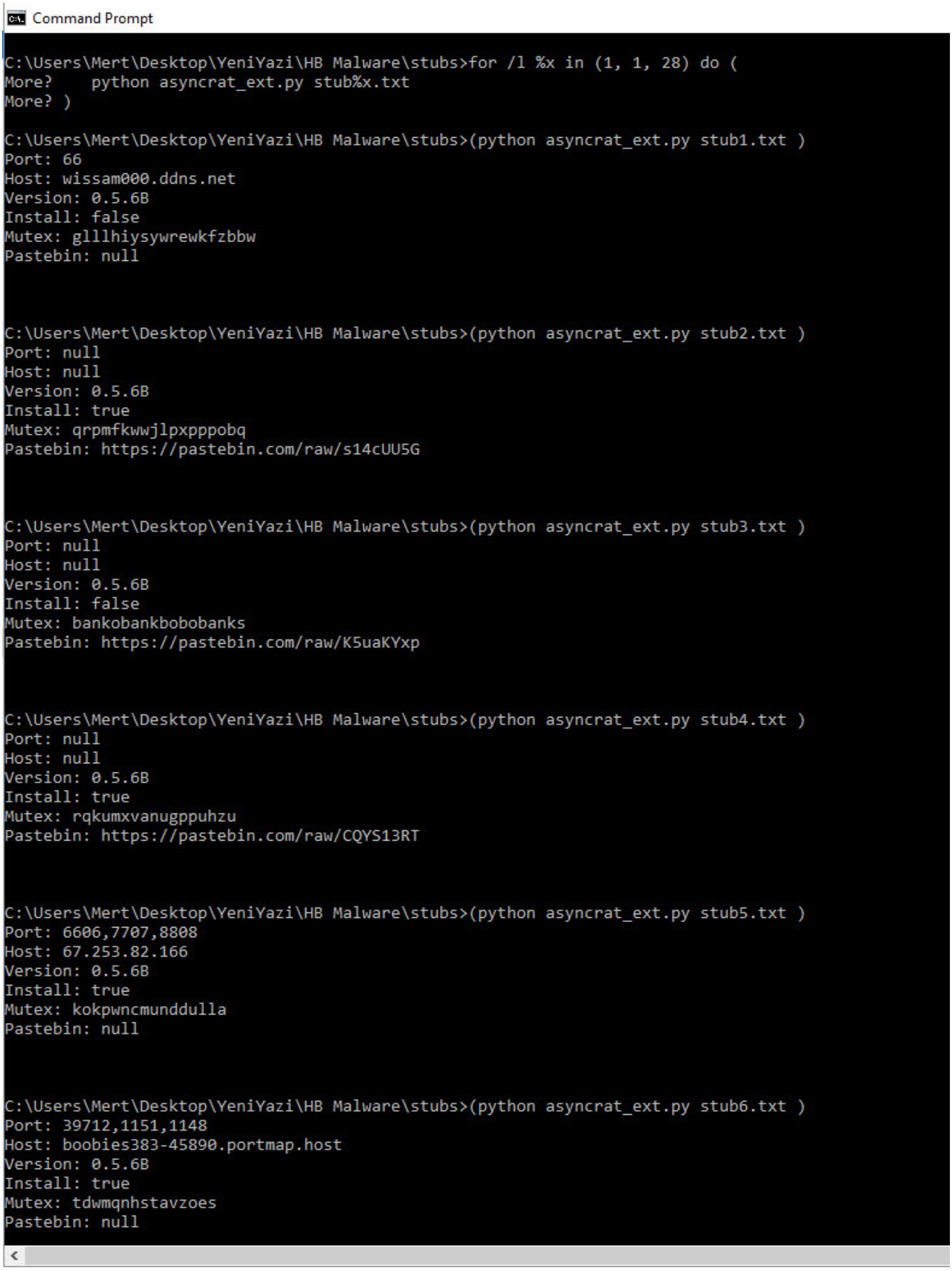


```
    IL_0037:  call unsigned int8[] class [mscorlib]System.Convert::FromBase64String(string)
    IL_003c:  callvirt instance bool class [mscorlib]System.Security.Cryptography.RSACryptoServiceProvider::VerifyHash(unsigned int8[], string, unsigned int8[])
    IL_0041:  stloc.0
    IL_0042:  leave.s 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 UPjlGoQHGJmz::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/fGZAPhtjZnpOMXGLgsfwrXKU5S83HK8xUjlQdiYXjGu42snGzR4PEwQBLMtP6HY0tO4e7fytfIUp+9Q=="
  IL_0005:  stsfld string LVefMHugJpKfAW.UPjlGoQHGJmz::rLxHRVvktJ
  IL_000a:  ldstr "iuq7GHKbtQ0LOSEwn9VUWoiYE1Ni0ums33crjUxW593CxiMMqnpb3WgXcPOVWTMl99RmnGMwjEJTORok7zaxPA=="
  IL_000f:  stsfld string LVefMHugJpKfAW.UPjlGoQHGJmz::svdTwYYxvrD
  IL_0014:  ldstr "rFw0jQKqdu9pvq855FnO7awWPcX0InCNuZoHPejjWBIO21+9XMo59v72jmajGMP8/IttgUWm/lxu7r7S3NE87w=="
  IL_0019:  stsfld string LVefMHugJpKfAW.UPjlGoQHGJmz::JqTYyBvoPQXlKmBT
  IL_001e:  ldstr "c3R2LaC//AaIuPpNsvyqluG2GZ0k6Q5Dq5vSkwkSzlvPHCAhMhbLtGerkeQCNFdQDkik/zCvKBd5jDPRxtKvqw=="
  IL_0023:  stsfld string LVefMHugJpKfAW.UPjlGoQHGJmz::WtxJdUcxhhTm
  IL_0028:  ldstr "%AppData%"
  IL_002d:  stsfld string LVefMHugJpKfAW.UPjlGoQHGJmz::RifTFGCauJoM
  IL_0032:  ldstr "Host Process for Windows Host.exe"
  IL_0037:  stsfld string LVefMHugJpKfAW.UPjlGoQHGJmz::IgQueznoVept
  IL_003c:  ldstr "cG5tSzZuUFlQSUlnNU9Ic3A5NjFkbk5QVXlJYmRJWWk="
  IL_0041:  stsfld string LVefMHugJpKfAW.UPjlGoQHGJmz::bPwIENFAunePP
  IL_0046:  ldstr "wW+9tAG5gSnOnDZHUUFzEP+Wk+F7BiDKG3t7cWs9tEb6DyScZCw9gMlW/PAA6B6BMkI2qi6c1SAGX+jtAhpGiw=="
  IL_004b:  stsfld string LVefMHugJpKfAW.UPjlGoQHGJmz::BsgvWQPUlSxB
  IL_0050:  ldstr
  "ufKCuObOYG+E1IE1XqM+sKgnW/TvtYk6KqIv9V9CGtXPfOJUVOSKCwtzgbiAkY+M0yNQ4He2DZSp2LVhhhWuiiuLymnrcpU4jcgH/HYvjYatoimWOcRF6gOXBP8QvRukan0yOS2FakIpOqdgmG1CIwfq/RJV8+ooX7aWJkCo7+mT6jjIry
```


```
    IL_0037:  call unsigned int8[] class [mscorlib]System.Convert::FromBase64String(string)
    IL_003c:  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 vUuBwDuSlIr::TMIjBQTGNDfcEWQ

  // 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 "JmPCaie5PV3CgOEmfV+2XI077HOufVoWrR2ztSJnRlmJOSs6Nt/0/osUi2DQmMR4DYOOKfyGYp3MkHs6OSA2dg=="
  IL_0005:  stsfld string McuCAiaCqjz.vUuBwDuSlIr::wEmhlNbkZHX
  IL_000a:  ldstr "i/8hlpMa6LMe2U9YeIWe0u82pzhfebvBoIT+DFDdowKqII75xtr87tlZXlxkuGIRW4t1IaIz6DxeKFwnjxa7bs3lp77QAXbXvrgZsYMnVTg="
  IL_000f:  stsfld string McuCAiaCqjz.vUuBwDuSlIr::AmbSEfkFVyi
  IL_0014:  ldstr "wWaZHdLMXC8owyCDF65L3XNF8WBwozg3xIUkjaAh2rS0JdjAhMrDq38+CQ1O71t4qbMt1R0+nPUe3Suc6KC82A=="
  IL_0019:  stsfld string McuCAiaCqjz.vUuBwDuSlIr::LOrEpVhkVWE
  IL_001e:  ldstr "ndT5oubUi9YDYYs+AaXtB7xBZiwBEDfnfPdeRBMBAYQDFvf7JkPt6M46wYx7hRqA/RnxLjfqdBaAaziFMD3D0w=="
  IL_0023:  stsfld string McuCAiaCqjz.vUuBwDuSlIr::MyLHXiGQFX
  IL_0028:  ldstr "%AppData%"
  IL_002d:  stsfld string McuCAiaCqjz.vUuBwDuSlIr::cbYpYfFwcYi
  IL_0032:  ldstr ""
  IL_0037:  stsfld string McuCAiaCqjz.vUuBwDuSlIr::oEcGIinZjLGB
  IL_003c:  ldstr "TXY0Q20yMGRXSlZFeGx1TGlpVXpuSDllb29pZU03TFU="
  IL_0041:  stsfld string McuCAiaCqjz.vUuBwDuSlIr::nkgtoZYXkRtgv
  IL_0046:  ldstr "Z6x6P100ZrezSi+xxHl4Eb4151t9m2nGZpIAYOrz5l2MKo/jFyCiC6aszmCSyx5YbB47al35tESSSVD/dYg7pNQZEEici0RPvIoKGNdSX5c="
  IL_004b:  stsfld string McuCAiaCqjz.vUuBwDuSlIr::gEcNdyclaLbg
  IL_0050:  ldstr
  "gHVqZBMckrUWw4h+UFW+YdV6pPJ9L2tKudoLpYEfrJW+Of0bUUgcUNYwKHLTLzwNLdZlKDJGH15nX/RcYGp8fzIPeIxYGLZGBzqF8MQsO6VThVEci5RPwRsk+JJSzofvBbbrPAN+wQq+cPduvUrTfXoij0psXxGUvBi7AIiqKFP5XyPuQz
```

```
    IL_0037:  call unsigned int8[] class [mscorlib]System.Convert::FromBase64String(string)
    IL_003c:  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 zbgTqalHViUFHwT::sGmuUeoyBYnr

  // 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 "ZbSxod6szox1bq2bnUKlvJXcLa5X14O7KBe0zAs5TJ/wCRiRB3vOakvztdOdRTEjQ/so8HlFQRvvObcxkyH/4w=="
  IL_0005:  stsfld string MiKCRUQuxTimcp.zbgTqalHViUFHwT::NGswHYqFHetj
  IL_000a:  ldstr "Sz/oQI8Um2lJoEh+RLHl+/aqTwM/v4//yvHYbU+1jWTzx2TPcC3Zq6valHkGDsdDESTpmAw6k5ECGJ9mWaZsWA=="
  IL_000f:  stsfld string MiKCRUQuxTimcp.zbgTqalHViUFHwT::dyhWpMOSPUwv
  IL_0014:  ldstr "o+yEwOEwqIbvXx5f2LIXc2xqQHit7+OS5sJSKJ7rMZ3KrGSlSVx0+4Zu0dzJ37Kv6vMT3Syq+FCaxKj2yhPIHA=="
  IL_0019:  stsfld string MiKCRUQuxTimcp.zbgTqalHViUFHwT::tHqFMSfeqgk
  IL_001e:  ldstr "zTzAZIRKARk3BzLqyePdEpMcuNOT7EfJ9I3e4wWss8Ze7uukigGJIJy5YV+NT3aylkvbPt7dnA5uTyW9/iMuHw=="
  IL_0023:  stsfld string MiKCRUQuxTimcp.zbgTqalHViUFHwT::kcPNciqUJTXfqm
  IL_0028:  ldstr "%AppData%"
  IL_002d:  stsfld string MiKCRUQuxTimcp.zbgTqalHViUFHwT::iUTvfauwhzOEb
  IL_0032:  ldstr "tasksync.exe"
  IL_0037:  stsfld string MiKCRUQuxTimcp.zbgTqalHViUFHwT::brwgbffTiOPhE
  IL_003c:  ldstr "Y2k3V1ZqRzRNNUtYaVdqZ3hNR29QQ3NxdndjbDc0b04="
  IL_0041:  stsfld string MiKCRUQuxTimcp.zbgTqalHViUFHwT::XZmuTNrwYTa
  IL_0046:  ldstr "lgJvAgU4nQcQqM2Pib46gNrNLBwSmL+Pxm75cs07XD4Qs/nsbLll83VtWJcXsm8gjzWrPXWE6lm3gmg+Dd+GKQVbntoDuHK6LpZ1KNBSb2Y="
  IL_004b:  stsfld string MiKCRUQuxTimcp.zbgTqalHViUFHwT::cHIPEjYUqaz
  IL_0050:  ldstr
  "eoy7EfvYnBkBY+zrhx6M/Nneit1i52ah+orgCGFNfdg5OXwKqeM1+pikW4xU49LwZXQKP+n8xmYk8WC7+oQhvLgY4L1gxGNtwMTLrXAzWf2hGh/ysDY1NvI1iljLmxZSNrOJJqi2E2ekwRoVEY4YVb6bdK8OfUO90E+deAvsLldlL9AGRz
```





Sonuç itibariyle tüm bu bilgileri derleyip topladıktan sonra bu siber saldırı girişiminin bir APT saldırısı olmasa da hedeflenmiş bir saldırının (Spear Phishing) parçası olması terazide 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.