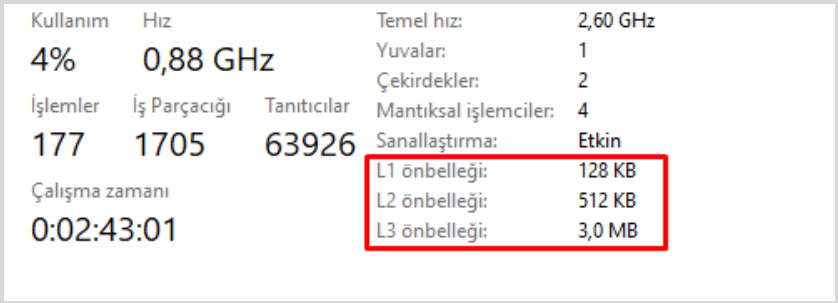
1.Cihaz güvenligi:

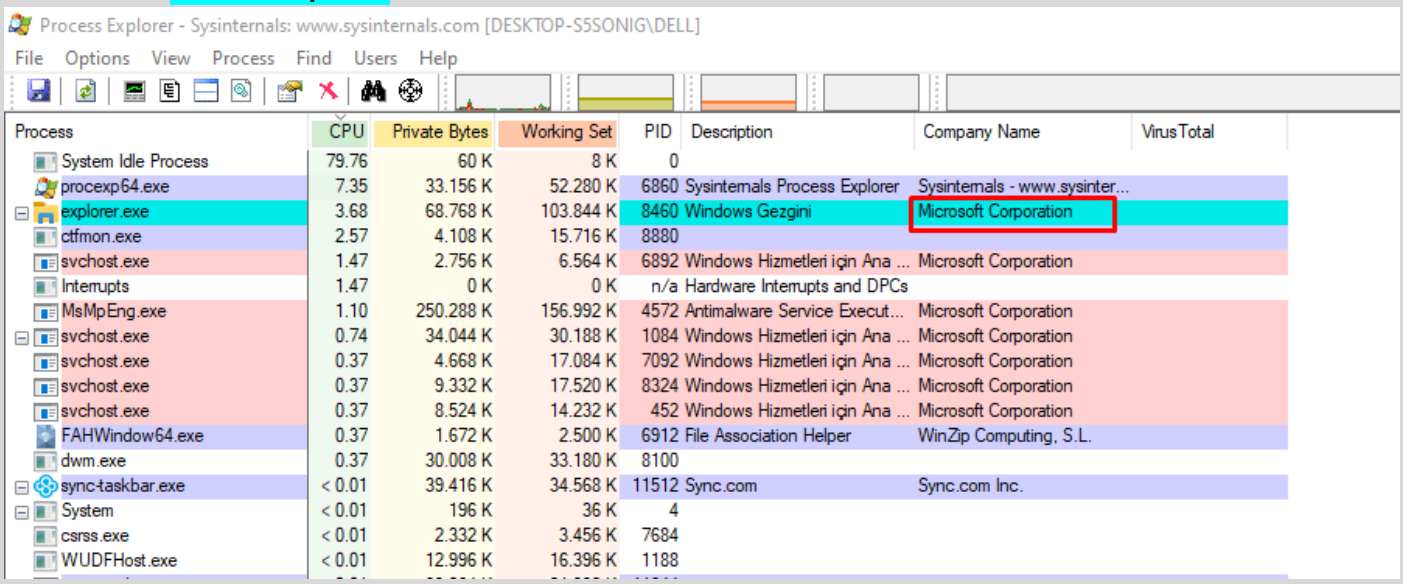
Virus tesbiti:
imza, virüsün yazılı komutlarından bir bölümü alınarak imza kayıt defterine eklenir. Bu virüsün imzasıdır. Virüsten kesilen bir parcadır. Ve bilgisayardsaki dosyalarla karşılaştırılır. Virüs programlarının imza kayıt defteri sürekli güncel tutulmalıdır.

➔Dosya alışverişinizi bulut sistemler kullanarak internet üzerinden yapınız.

ctrl + shift + Esc →**Görev Yöneticisi**



Alternatif == **Process Explorer**



Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	VirusTotal
System Idle Process	79.76	60 K	8 K	0			
procexp64.exe	7.35	33.156 K	52.280 K	6860	Sysinternals Process Explorer	Sysinternals - www.sysinter...	
explorer.exe	3.68	68.768 K	103.844 K	8460	Windows Gezgini	Microsoft Corporation	
ctfmon.exe	2.57	4.108 K	15.716 K	8880			
svchost.exe	1.47	2.756 K	6.564 K	6892	Windows Hizmetleri için Ana ...	Microsoft Corporation	
Interrupts	1.47	0 K	0 K	n/a	Hardware Interrupts and DPCs		
MsMpEng.exe	1.10	250.288 K	156.992 K	4572	Antimalware Service Execut...	Microsoft Corporation	
svchost.exe	0.74	34.044 K	30.188 K	1084	Windows Hizmetleri için Ana ...	Microsoft Corporation	
svchost.exe	0.37	4.668 K	17.084 K	7092	Windows Hizmetleri için Ana ...	Microsoft Corporation	
svchost.exe	0.37	9.332 K	17.520 K	8324	Windows Hizmetleri için Ana ...	Microsoft Corporation	
svchost.exe	0.37	8.524 K	14.232 K	452	Windows Hizmetleri için Ana ...	Microsoft Corporation	
FAHWindow64.exe	0.37	1.672 K	2.500 K	6912	File Association Helper	WinZip Computing, S.L.	
dwm.exe	0.37	30.008 K	33.180 K	8100			
sync-taskbar.exe	< 0.01	39.416 K	34.568 K	11512	Sync.com	Sync.com Inc.	
System	< 0.01	196 K	36 K	4			
csrss.exe	< 0.01	2.332 K	3.456 K	7684			
WUDFHost.exe	< 0.01	12.996 K	16.396 K	1188			

Mor Şüpheli
Turkuaz Şüpheli

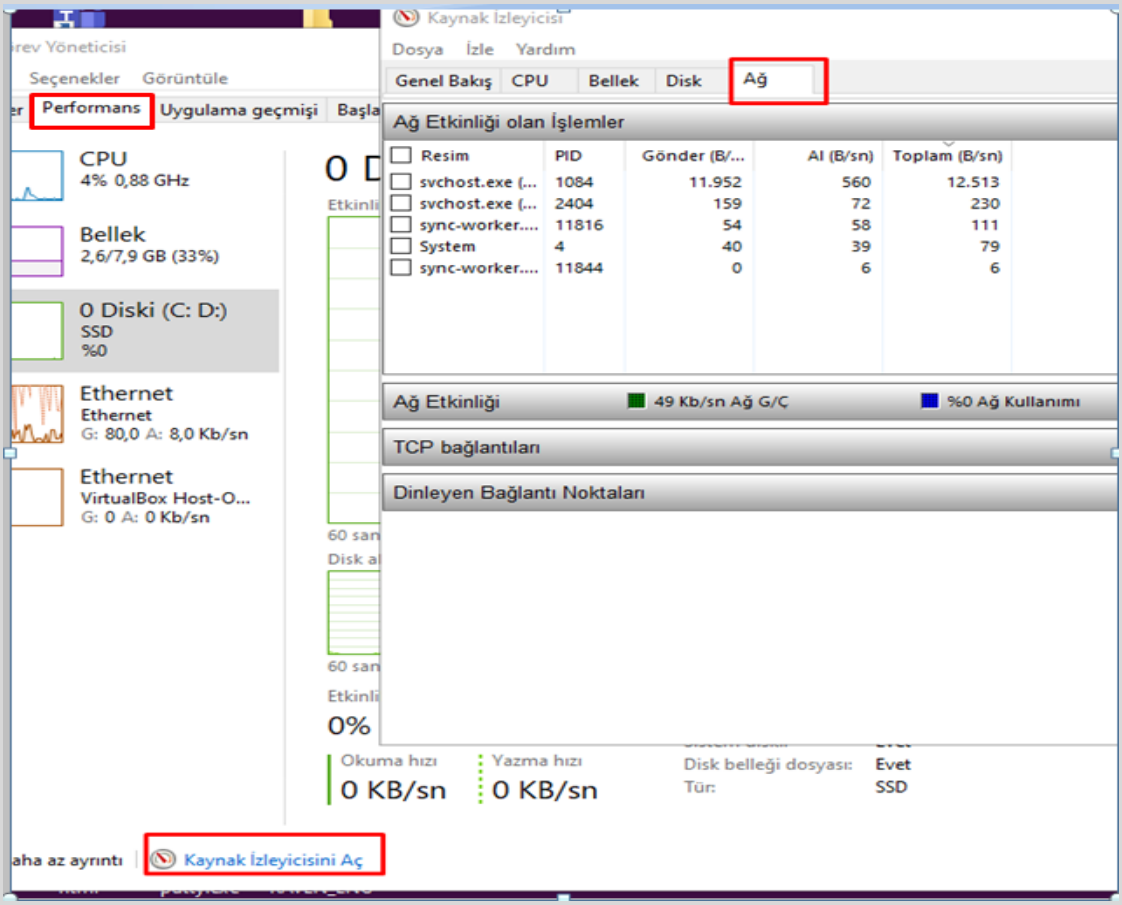
***Şüphelendigimiz uygulama varsa ilğili uygulamaya sağ tıklayıp **Check Virus Total diyerek Virus Total İnternet sitesinde uygulamayı taratabilirsiniz !?**

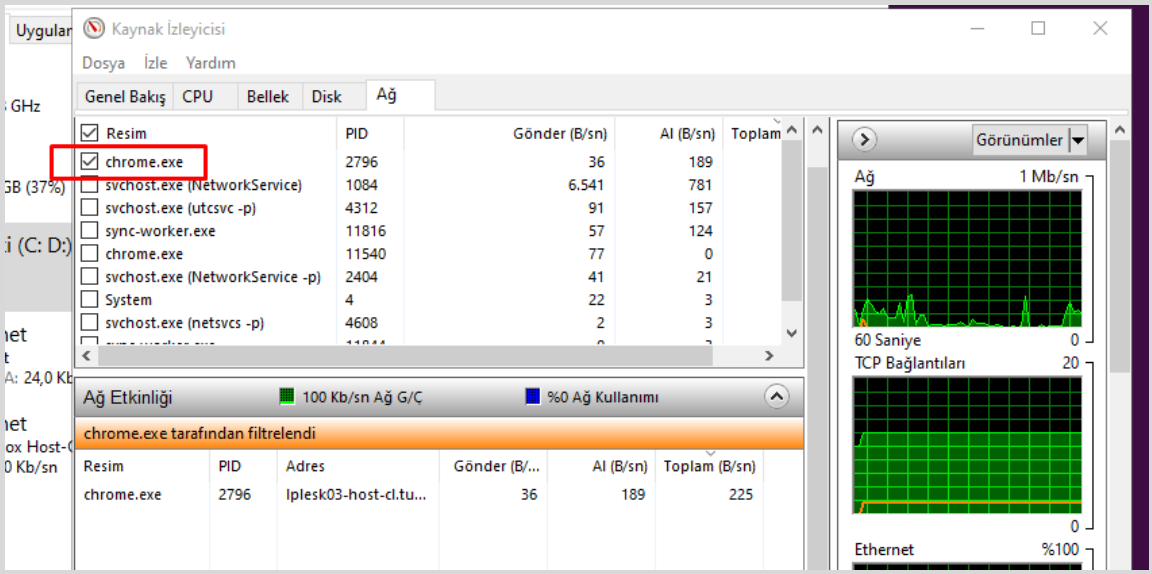
Company Name'ye dikkat **!!!**

Windows Defender Kullanımı: (an antivürus application…)

➔Antiviru programlarının puanlaması **av-test.org**
https://www.av-test.org/en/antivirus/business-windows-client

2.Ağ trafiğnin İzlenmesi: **…with Task Manager**





Filtreleme…

Bu kısımda internete bağlanan programları ve internet kullanım oranlarını görülebilir. Şüphelendiginiz bir proğram olursa **Process Explorer** programı ile virüs kontrolü yapılabilir.

***ClassWire https://www.glasswire.com/

Ağ trafiginin izlenmesiniz daha kolay ve basit olarak yapılabilir.
internet trafiğini izlemek ve interneti kullanan virüs vb… bulmak.

***İnternet trafiğini izleyebilir, güvenlik duvarı özelligini açarak internete bağlanan programları görebilir ve kısıtlayabilirsiniz. Chrome ile test et…

Şüphelenilen bir program varsa Windows Defender yerine başka bir antivirüs programı da kullanabilirsiniz. malwarebytest.com adresinden **Malwarebytes** programını indirip kullanabilirsiniz.
https://www.malwarebytes.com/

……. . …….. . ……. . ……. . ……. . ……. . ……. . ……. . ……. . ….

İşletim Sistemini Güncel Tutun…
Güvenlik duvarınızı kapatmayın…
Bilgilerinizi yedekleyin…

……. . …….. . ……. . ……. . ……. . ……. . ……. . ……. . ……. . ….

Mobil Cihaz Güvenligi:

Bilgisayardan farklı olarak,
>>Arama yapma
>>Mesaj gönderme ve alma
>>Konum tesbiti yapma
>>Hesapların doğrulama yöntemi

Güvenlik:

***Kilit ekranı
***Kilit ekran bildirimlerini devre dışı burakın
***Sm kartına PIN kodu koyun
***Kasa uygulamaları kullanın (Kritik dosyalarınızı bir kasa uygulaması ile şifreleyin)
***Antivirü programı kullanın
***Bilinmeyen kaynaklardan program indirmeyin
IOS haraci kaynaklardan program indirmeye izin vermez.
Android bir sınırlama koymaz.

***Telefonunuza Root yapmayın (Root yada Jailbreak yapmayın)

***Uygulama izinlerini kontrol edin.

*Mesela bir uygulama resimlerinizi düzenleyeceğini iddia ediyorsa **depolama alanına erişim izni** istemesi gayet normaldir. Ancak, **telefonun konumunu, mesajlara,kişi listesine erişmek istiyorsa** bir sorun var demektir.*

***Cihaz yöneticilerini (yönetici yetkisine sahip uygulamalar) kontrol edin

*Cihazın "**bul**" uygulaması. Cihaz kaybolduğunda uzaktan cihazın kilitlenmesini ve istenirse içindeki bilgilerin silinmesini sağlar. Bu uygulama yönetici izinlerine sahiptir.*

***Konum bilgisini kapatın:

Fotoğrafa konum bilgisi eklenmesin… Tarih,Telefon modeli, ışık değere.. (Exif değerleri denir.)
Exif görüntüleme programlarıyla görülebilirler.

***SnoopSnicth Uygulaması: **For Android**…

Telefonun gerekli güvenlik yamalarını alıp almadığını inceleyen çok iyi bir uygulamadır.

Güvenlik test aracıdır! ☺

➔Bu uygulama **SS7** ataklarını da inceleyebilir. SS7, **GSM** iletişiminin bir zafiyetidir.

Mesajların okunmasına olanak sağlar… Çok önemlidir…

Ancak bu özellik sadece **Qualcomm chipsetine** sahip telefonlarda çalışıyor!

***Zararsız gibi görünen uygulamalar:

Kayıtlı olmayan numaralardan arayan kişilerin kimliğini gösterme vaadi, sizi takipten çıkanları.. vb

Wİ-fi Güvenligi:

WPS kullanmayın:
Modem üzerinde bulunan WPS düğmesine ve internete baglanacak cihaz üzerinde bulunan WPS düğmesine aynı anda basılmasıyla ilgili cihazın internete baglanması sağlanır.

Üzerinde WPS düğmesi olmayan cihazlar ise WPS piniyle internete bağlanabilir. Bu pinler 10 haneli ve genelde rakamlardan parolalardır. WPS özelliği aktif olan cihazın parolası çok kolay bir şekilde kırılabilir. Bu özellik kapatılmalıdır.

Şifreleme Türleri: (Modem ile internete Bağlanan cihaz arasında)

AÇIK
WEP
WPA-PSK
WPA2-PSK
WPA3

WPA → TKIP ve AES olaral iki türü vardır. AES iyidir…

Evil Twin Atak:

INTERNET GÜVENLİĞİ

Brute Force
>> Tek tek denenerek…

8 haneli sadece rakamlar ➔100 milyon deneme

Parola saklama programları:
LastPass – **1Password** --

Uygulamalar parolaları sizin cihazınızda tutar.
Parolaları sadece siz görebilirsiniz.

Parola Tuzlama: -OK- !?

>> Uygulamada kaydetmeyi öner veotomatik olarak giriş yap seçeneklerini kaldırın.
Bir kısmını otomatik olarak girdirip | bir kısmınıda sen yazabilirsin.

Çift Faktörlü Kimlik Doğrulama:

One factor
two factor
three factor
for factor

Two factor için:
Microsoft Authenticator,
Duo Mobile
Google Authenticator,

SMS Doğrulamasını Kullanmayın:

…
GSM haberleşme sisteminde bulunan **bir açık ile** saldırganlar, hedef seçtikleri telefondan mesajları okuyabiliyordu. Bu yöntem ile telefon ile GSM arasına girilebiliyor.

Güvenli anahtar:
USB Bellek ile…

Phising Saldırısı:

…
havaibeenpwned.com →Parolanın ele geçirip geçirimedigi…

…

Surface web
Deep web **→Arama motorları indexleyemez.**
Dark web

SMS dogrulaması == 3D Secure olarak yapar.

*** Gizlilik için kullanılacak en iyi browser Brave ve Mozilla Firefox tur.
Brave tarayıcıda Tor ağına bağlanabileleceğiniz bir gizli sekme vardır.

Google Chrome deki gizli sekmesi – sadece Google dışındaki gözlerden korur ve web tarayıcı geçmişinde iz burakmadan internette dolaşmanızı sağlar ama gizlilik sağlayamaz. Yani Google hala sizi izler.

Mesajlaşma gizliliği: Signal E_posta Gizliliği: ProtonMail