Güvenlik Raporu

2023

Ağ bağlantıları raporu

İZINSIZ VE IZLEME YÖNTEMIYLE UZAKTAN ERIŞIM SERVISI

Açıklama :

Windows Yardım Komutunda bulunduğu gibi Uzaktan Yardıma izin ver bilgisayarlarda açıksa bu durum bir çok veri izleme takibine yol açabilecek küresel internet hattı üzerinde İp adreslerinizin kolay bulunabilmesine karşılıklı izin sonucu Hizmetler ayarlarında yeni kurulum ve kayıt dosyaları oluşturabilen zararlı yada takip amaçlı veri geliştirmesine
dayalı bilgi işlem kanunları olacaktır.

İZINSIZ VE SERTIFIKASıZ DEVRE Dışı BıRAKıLAN WIFI YADA Ağ BAğLANTıLARı

Açıklama: İnternet sertifikanızın size ait olduğundan emin olmak için bilgisayarınızın servis sağlayıcı tarafından
bilgisayarlarınızda hazır bulunan ağ sertifikalarının en az 1 tanesinin kurulu olduğundan emin olunuz.
bu durum sertifikası olmayan servis sağlayıcıların yaşadıkları zorluklardan bir tanesi
ağ bağlantılarınızın anlık olarak gitmesi.

İstem Dışı İşletim sisteminin kendini Kapatması

Açıklama: Windows yada herhangi bir işletim sisteminizin kendini kapatması yada kendine reset atması sürekli
yaşanan konulardan birisi değildir.
bu durumda resetlenmeye neden olan masaüstü yada laptoplar üzerinde Bios ayarlarınızın
güncel olduğundan işletim sistemleri sahibi olduğunuz bilgisayar modelinizin anakart modelinize
göre Bios sürümünü sorunsuz bir şekilde güncellemek için kurmanız gerekecektir.
mavi ekran hatası aniden kapanma Bios sorunlarından doğan büyük problemler üzerinde çözüm odaklı en etkili çözüm servisidir.

İşletim sisteminizin yeniden geriye Döndürülmesi için Kendini Yedeklenen tarihe döndürmesi

Açıklama: İstemediğiniz bir anda Windows yada herhangi bir işletim sistemi kendini
yedeğe döndürmek için size uyarı veriyorsa bu durum ana konsol komutlarının bozulduğuna dair
en önemli ipucunuzdur.
bu durumu yaşamamak için mutlaka lisans bir kullanıcı ve hard disk yada ssd disk sorunu olmayan
bir kullanıcı olmanız önemlidir.
Donanımların yanarak çalıştığı en nadir görülen bir arıza sonucu çeşitli kazalar meydana gelebilir.
uygun modeller üstünde yeterli sistem bilgisine sahip olmanız kullandığınız bilgisayarlar için
en üst donanım kullanmanıza gerek kalmadan hangi özelliklerin hangi işe yaradığına odaklanırsanız.
işlerinizin çözüm ve ilerletme yolunda daha iyi sonuçlar alabilirsiniz.

Kullanıcının izin yada emri olmadan veri iletmesi yada veri alması

Açıklama:

farkında olamadan başlangıç ve sürekli çalışan öğelerinizde bir uygulama gördünüz

bu durumda bu durumu Windows'a yada herhangi bir işletim sistemine bildirmek için çokgeç kalmış olabilirsiniz.

kurulmuş olan program yazılım ve uygulamalar sizinle olan ilişkisini ana konsol komutlarına

zarar verdikten sonra kendini belli etme özelliği taşıyan Solucan deliği Trojan virüsleridir.

bellek üzerinde Temp dosyaları üretip bütün donanımlarınıza zarar vermeye başlamış bir güvenlik açığıdır.

Konsol komutları ile tespit edilen İP adresine İzinsiz erişim

Açıklama:

Sıradan yada ileri seviyede bir bilgisayar korsanı olduğunuzu düşünüyor olabilir ve kendinizi mükemmel siber saldırı uzmanı olduğunuzu düşünüyor olabilirsiniz. sıçrama yöntemiyle uzaktan pencere dışı bağlantı kurabilirsiniz ve daha önemlisi pencere içinden açılan oturum sahibi gibi davranabilir
asıl kullanıcı bunun farkında bile olmayabilir.
Bu durum bilgisayar kullanıcısı oturumunu kapattıktan sonra devam eden saldırganın veri izleme yönetimiyle Bios u açık tutmasından kaynaknır çoğu zaman güvenlik programları
bu yol ve yöntem üzerinde çalışarak lisanslı antivirüs kullanıcıları için farklı çalışmalar yapmak için
kullandığı bir yöntemdir. Korsan olarak veri elde etmeye çalışan sanal bilgisayarlar hızsızları
bu durumu bilmedikleri için asıl bilgisayar sahibi oturumunu açmak için yeniden güç tuşuna bastığında
bilgisayarının hemen açılıyor olmasıdır.

İnternet Hattında bulunan İP adreslerinin Kayıtlı Firmaları Yaptırım altına Alması

Statik olarak servis dağıtımında bulunan internet servis sağlayıcıları kullanıcılara yönelik bir çok işlemin ek güvenliğini kayıt altına almamaktadır. Durum yaşanabilir olduğunuzdan bir bilgisayar içinde ip sahibi ek güvenildiğini tehdit altına alacak bir çok faktör ve yapılandırmalar üzerinden anlık olarak ip adresinin delist ederek kullanıcıların bir program ve işlem içindeyken
kullanıcıların izni olmaksızın güvenlik duvarın dışında bırakılarak dışarıya atılmasına
neden olan
bir diğer faktörlerdir.

Hizmetlerde Etkinleştirilen veya Bilinmeyen Uygulamalar

Farkında olmadığınız işlemlerin ne kadar büyük fonksiyonları durdurup kendi isteğiniz üzerinde çalışmadığını hizmetler faktörlerinde kolaylıkla fark edebilirsiniz.

mevcut bilgisayar özelliğinizin tam fonksiyonlar üzerinde çalışmasını hizmetler bölümünde

istediğiniz yada istemediğiniz olayları seçip kaldırabilirsiniz.

Bilinmeyen bir kaynaktan hizmetlere küme oluşturulması

kümeler fonksiyonların kayıt defterinde yazılımların bilgi toplanması amacıyla oluşturulan kümelerin donanımsal olarak etkilendiği yapılandırmaların başına gelen
klavye ve Mouse üzerinde çeşitli donmalara ve kırılmalara sebep olabileceğini sebep olunan donmaların yada Windows çalışmayı durdurdu gibi hataların önünüze çıkmasını sağlamaktadır.
bu sorun genellikle tam imza yetkisi olmayan firmaların oyun üretip
oyun dağıtımında bulunan server ve ağ tabanlarında yada internet sitelerinden indirip
bilgisayarınıza kurulması ile gerçekleşmektedir.

Kaldırılamayan Başlangıç öğeleri

yüklenen bir uygulama yazılım ve program kaldırılmak istenildiği zaman çoğu zaman bu uygulama yada program kaldırılamadı gibi kullanıcı istediği zaman
kaldırmak istenildiğinde halen çalışmakta olan uzantılarını durdurması ve kaldırması
gerektiğini hatırlarız.
aslında bu durum çeşitli bilgisayar kullanıcıları arasında ve ilerleyen veri tabanında hedefin
system32 ana konsol ayarlarının değiştirmesinden kaynaklanır.
eğer System 32 klasörünüzü bir kilitleme altına alıp yada alınan ve verilen değerlerin sabit olmasını sağlarsanız ana dağıtım hücreleri kullanıldığınız bilgisayarlarınızı faydalanmadan işlem yapabilir.

Güvenlik Duvarı verisinin üst partner antivirüs Programları

antivirüs programlarının sizi korumak için bilgi akışında güncellemeler yapıldığını ve sürekli olarak verilerinizin belirlenen virüs olaylarına karşı bilgisayarınız açık kaldığı sürece koruduğunu düşünebilirsiniz. bu durum kullanıcı kayıtları yaptığınız güvenlik ve antivirüs programları üretici firmalara göre değişiklik sağlar öyleki bir bilgisayar kullanıcısı beklemediği anda antivirüs programlarından sıyrılmış bir değişlik algılandığında küçük virüsçü direk güvenlik duvarı karantinasına alınır yani sadece antivirüs programları tespit işlemi üzerinde çalışır kimsenin bilmediği ve güvenlik programlarının anlamadığı virüsler için konuşabilirsek saldırının bir antivirüs genel merkezini hedef bütün sistemi çökerttiğinde güvenlik ve antivirüs firmaların bu duruma güvenlik tedbiri olarak geliştildiğini görebiliriz.

System32 ve silinemeyen Virüsler

Silinemeyen virüsler sizi şaşırtabilir.
çünkü değiştirilemeyen dosyalarınızda aynı dosyayı değiştirip kilitlenmesi ile yola çıkmıştır Vardığı noktada System 32 nin içinde bir çok ayar ve fonksiyonel işlemleri yerine getirdiğinden kullanıcılar sadece göz kararı
antivirüs programlarının uyarıdan kurtulmak ve virüsü temizlendiğini bilmesi gereken konu durumların kullanıcıların sorunları hafifletmek için farklı olay ve günlükler üstünde yoğunlaşmalar yapılmaktadır.
bu çalışma günlüğünde olaylar kayıt defterleri ve hizmet fonksiyonlar ve hedeflenen işlemlerin System 32 de çalışmasını sağlamaktadır.

Truva Atı ile Ağ bağlantılarında İzole edilme (solucan Deliği)

Açıklama:

Truva atı güvenlik duvarını kolaylıkla aşıp istediği alanda kendisini dezenfekte edebilen virüs türüdür.

Truva atları kilitlenme ve fonksiyonlar gelişiminde kontrol edilebilir altyapıya sahiptir.

virüsü oluşturan korsan istediği işlem ve fonksiyonları hazırlayabilir ve program ve yazılımlar arası

sorunlara veri toplamaya çalışabilir.

eğer virüs tam yetkinlik izinleri arasında bağlantı kuruyorsa bu fidye yazılımları olarak hazırlanabilir.

ve kullanıcılara zor ve maddi anlamda tehlikeli günler yaşatabilir.

Truva Atı ile Ağ bağlantılarında İzole edilme (solucan Deliği)

Açıklama:

Truva atı güvenlik duvarını kolaylıkla aşıp istediği alanda kendisini dezenfekte edebilen virüs türüdür.

Truva atları kilitlenme ve fonksiyonlar gelişiminde kontrol edilebilir altyapıya sahiptir.

virüsü oluşturan korsan istediği işlem ve fonksiyonları hazırlayabilir ve program ve yazılımlar arası

sorunlara veri toplamaya çalışabilir.

eğer virüs tam yetkinlik izinleri arasında bağlantı kuruyorsa bu fidye yazılımları olarak hazırlanabilir.

ve kullanıcılara zor ve maddi anlamda tehlikeli günler yaşatabilir.

Trojan İle Kayıt defterlerini Askıya Alma (solucan Deliği)

Trojan virüsleri bulunacakları ortam gereği kayıt defterlerine yönelik birçok alternatif seçenekler olarak çeşitli zararlar ve system32 nin kayıt defterlerine birçok ayar değiştirme seçenekleri sunar.

bilgisayar kullanıcıları tamamen virüsü izole etmek yerine kaldırdıktan sonra hangi bilgileri değiştirip sildiklerini bilmedikleri için Trojan virüsleri silindikten sonra

önemli olan kullanıcı ayarlarınızı yeniden yapılandırmanız ve gerekiyorsa gelişmiş bir güvenlik katmanı

kurmanız gerekmektedir.

Solucan virüsü ile Mail ve içine gömük Dosya ,resim , mail üstünden zararlı bilgi sızdırmak (Solucan deliği)

solucan virüsleri panel açmak ve anahtar üretip kendini saklamak ve yayınlaştırmak için üretilen ve mailler üzerinde ve diğer işlemler üzerinde sahiplik amacıyla üretilen virüs çeşitleridir.
kullanıcılar solucan virüslerinin basit bir sürümü ile karşılaştıklarında önemli olan hedeflenen alanların yetki kontrollerinin kendisinde olmasını sağlamaktadır.
kullanıcıların diğer beklenmedik bir işlem değeri ise tehlikeli olabilecek yazılım türlerine saldırganlık özelliği taşımasıdır.
burda kullanıcıların kayıtlı şifre ve isimlerini çalabilir.
virüs temizlemeden yapılan her işlem sizi virüsün kayıt defterlerinde takip altına almasına neden olabilir.
ağ birimleri üzerinde alınan ve verilen bilgi değerlerinizi kendi istediğine göre yeniden tasarlama ve solucan virüsleri üreten kişilerin güncellemeye dayalı kontrol mekanizmasına bağlı olarak yanlış bilgi ve veri yöneltmesine neden olan yaygın bir virüs türüdür.

Windows Kullanıcı girişlerindeki Hatalı şifre erişimi ve bloke (solucan deliği)

kullanıcıların farkında olmadığı bir solucan virüsü bilgisayarınızda tanımlanamazsa

emir aldığı virüs anatomisi bir diğer virüs anatomisini harekete geçirebilir ve dahada büyüyerek tamamen bilgisayar açılış kapanış mekanizmasını devre dışı bırakabilir.

bu örnek standart bir bilgisayar kullanıcısı için çok yaygın bir işlemdir. hatta profesyonel virüs üreten korsanlar istediklerini zorla yaptırmak için fidye yazılımları olarak hedeflenen ip aracılığıyla yönlendirme çekerek gönderim sağladıkları virüs türüdür.

Reboot Servislerinin yüklü olduğu Windows oturumlarında yüklenmemesi (solucan deliği)

tamamen devre dışı bırakılmış Windows komut sistemi orta segment bir bilgisayar kullanıcısının
rebootlamak yada formatlamak için tasarlattığı alternatif zaman kaybına yönelik üretim sağlandığı
solucan değilinin açık olmasına kaynak olarak Bios sistemlerinizin bozulmasına yönelik işlemlerin yapıldığı
ana sunucular üzerinde yetki erişimi ile uzaktan yardıma izin ver açık olması ve bu durumun
bir diğer saldırganın alternatif olarak izlediği takip durumudur.
bu alana ise solucan deliği adı verilir.

Api İle Devre Dışı Bırakılan Ekran Kartları (solucan deliği)

yaklaşık olarak kurulu ekran kartlarınıza yönelik yapılan diğer işlemler üzerinde yapılan
çalışmalar Api yönetimiyle devre dışı bırakılan ekran kartları ve sertifikası dolmuş ekran kartlarının
devre dışı bırakılmasına olanak tanıyan bir diğer faktördür.
Herhangi bir ekran kartı üreticisi dilediği zaman üretilen ekran kartlarına yönelik sertifika süresini
bahane ederek ekran kartlarınızın devre dışı kalmasına olanak tanır.

Hatalı yönlendirme üzerinde zararlı yazılım ve programların donanımlara Etkisi (Solucan Deliği)

ekran kartı destekleyici fakat ekran kartı üreticisi ile bir ilgisi olmayan donanım yazılımları bu durumu rekabet durumuna göre fazladan kendi piyasa koşullarını yerine getirmeye çalışmasından kaynaklanan

bir diğer ekran kartı üreticisi için üretim sağladığı konsol bozucu ve devre dışı bırakıcı özellikler taşıyan yazılım ve programların bilgisayarınızda kurulu olmasından kaynaklanır.

istediğiniz bir çalışma programında çalışmak için çeşitli komutları takip ederek bilgisayarınıza taşımak istediğinizde

herhangi bir dosya yok yada beklenen durum çalışmadı gibi alternatif sorunları karşınıza çıkarmanıza yarayan solucan deliğidir.

hız yükseltmek ve herhangi bir dağıtım firması tarafından altyapısında tarafınızdan bir imza alınmadığı için video oyun üretici firma ile ekran kartı üreticisi olan 2 firmanın ortak kullanıcılar üzerinde imzalamış olduğu çıkar ilişkisinden kaynaklanır.

yani siz bir video klip hazırlamak isterken -aslında ekran kartı üreticileri sizin adınıza çoktan karar almıştır.

kurmak için ise Windows formatlamak yapıldığı gibi çalışmayan program ve yazılımlar için ise görevini tamamlamış sayılır.

Bios Faktörlerinin Silinmesi (Solucan Deliği)

Bios sistemleri bilgisayar iç mimarisine dayalı olan ve geliştirilmeye fazla açık olmayan bir altyapı sistemdir.
aslında işletim sistemlerinin ihtiyaç duydukları sistem ise Bios sistemleridir.
donanımların üretilmesi ile yüklenen ve beraberinde herhangi bir işletim sistemini kurulum yapmak için kendisine tanımlayan ve kodlayan mimari sistemleridir.
Bios faktörlerinin silinmesi ve geriye dönük işlemlerin yapılması için kullanıcının bir çok Bios özelliği silinmiş ve bu durumu güncellemek için yaptığını ve onarmak için çalıştığını düşünsede aslında solucan deliği tarafından hedeflenen makina olduğunu
ve genel Bios üretim hatlarının kendisine yapılan farklı bir işlem olduğundan habersizdir.
Bu duruma Bios solucan deliği adı verilir.
yönetim mekanizması sağlayıcı firma tarafından bölgesel olarak değişiklik gösterir

Bios ayarlarında Algılanamayan Donanım Özellikleri

yeni bir donanım satın aldığınız fakat bu durumu Bios ve diğer işletim sistemlerinde görüntüleyemediniz.

bu durumun en net çözümü ise desteklenen anakart ve diğer bağdaştırıcı özelliklere uygun olmayan

bir donanım satın aldınız demektir.

algılanamayan donanımlar ise tarafınıza bozuk olarak satılmış olabilir.

yada entegre ettiğiniz bilgisayar bölümleriniz bozulmuş olabilir.

mevcut olanda ve algılanamayan modellerde genel özellikler uyumlu

kontrolleri yapmanızda fayda gösterecektir.

yeni bir donanım işletim sisteminizi açıyor fakat görmüyorsa sertifika ayarlamlarından emin olmanız gerekir.

Sorunun başka bir çözümü ise donanım takıldıktan sonra yeni Bios güncellemesi ile üstünden geçmektedir.

UPTADENET 2023 Güvenlik Raporu

Sistem Mimari

uptadenet@outlook.com

uptadenet@gmail.com

https://uptadenet.com