Ad Soyad: _____ **Tarih:** _____ **Puan:** _____

Kötü Amaçlı Yazılım Analizi ve Tehdit Azaltma Rehberi

Truva atları, fidye yazılımları, casus yazılımlar, rootkit'ler, sanallaştırma korumalı alanları, sınırlandırma

KÖTÜ AMAÇLI YAZILIM ANALİZİ ÖĞRENME ÖZETİ

GÜVENCEDE
VERİ ŞİFRELEME
256 bit AES Standardı

UYUMLU
KÜRESEL STANDARTLAR
GDPR ve CCPA çerçeveleri

SIFIR GÜVEN
ERİŞİM POLİTİKASI
Çok Faktörlü Kimlik Doğrulama

Hoş geldin! Bu etkinlik paketi sana kötü amaçlı yazılım analizi ve önleme konusunda rehberlik eder. Casus yazılımları, truva atlarını, fidye yazılımı yüklerini, tersine mühendislik araçlarını, rootkit davranışını ve sınırlama stratejilerini keşfedeceksin.

ÇALIŞMA KÂĞIDI KONTROL NOKTALARI

- [ ] **Bölüm 1-4: Siber güvenlikte ve tehdit önlemede ustalaş.**
- [ ] **Bölüm 5-7: Çapraz bulmaca ve kelime avı bulmacalarını çöz.**
- [ ] **Bölüm 8-9: Vaka çalışmalarını ve şifre görevini çöz.**
- [ ] **Bölüm 10: Temel ve ileri düzey SSS sayfalarını gözden geçir.**
- [ ] **Bölüm 11: 10 ilginç gerçek dünya gerçeğini keşfet.**
- [ ] **Bonus: Hızlı Düşün görevi.**

VPN.com siber güvenlik rehberini aç

URL: https://www.vpn.com/tr/siber-guvenlik/kotu-amacli-yazilim/

Kötü Amaçlı Yazılım Azaltma Öğrenme Yol Haritan

- Truva atı, solucan ve rootkit kötü amaçlı yazılım türlerini birbirinden ayır.
- Kod analizi için korumalı alan sanallaştırmasıyla yürütme uygula.
- Aktif fidye yazılımı yüklerine yönelik sınırlandırma ve temizleme planları tasarla.

KÖTÜ AMAÇLI YAZILIM ANALİZİ REHBERİ TALİMATLARI

Çoktan seçmeli ve doğru/yanlış sorularını cevapla, boşluk doldurma cümlelerini kelime bankasını kullanarak tamamla, tanımları eşleştir, çapraz bulmacayı ve kelime avı bulmacasını çöz. Bilgini şu konulara uygula: kötü amaçlı yazılımın etkisini azaltma. Hızlı Düşün bonus etkinliğiyle bitir.

KÖTÜ AMAÇLI YAZILIM ANALİZİ VE TEHDİT KONTROLÜ (GİRİŞ)

Truva atları, solucanlar ve fidye yazılımı gibi kötü amaçlı kodlar, uç noktalar ve sunucular için yüksek etkili tehditler oluşturur. Güvenlik ekipleri kötü amaçlı yazılımı sanal korumalı alanlarda (sandbox) analiz eder ve zararlı yükün yayılmasını durdurmak için hızlı ağ yalıtımı denetimleri uygular.

HER KONTROL NOKTASINI DİKKATLE OKU VE DOĞRU CEVABI SEÇ YA DA YAZ.

Kontrol Noktası 1: Çoktan seçmeli görev

1. Truva atının belirleyici özelliği nedir?

- A. Kullanıcıları çalıştırmaya kandırmak için meşru yazılım gibi görünür
- B. Yerel ağ hatları üzerinden kendiliğinden çoğalır
- C. İzole sanal kum havuzlarındaki dosyaları enfekte eder
- D. İnternet servis sağlayıcı trafiğini yakalar

2. Hangi kötü amaçlı yazılım türü dosyaları şifreler ve ödeme talep eder?

- A. Fidye yazılımı
- B. Casus yazılım
- C. Rootkit
- D. Reklam yazılımı

3. Casus yazılımı ne temsil eder?

- A. Kullanıcı tuş vuruşlarını ve tarayıcı etkinliklerini gizlice izlemek için tasarlanmış kötü amaçlı yazılım
- B. Korumalı bir sanal kapsayıcı içinde çalışan program kodu
- C. Veritabanı kayıt defterlerinden indirilen kötü amaçlı yazılım önleme güncellemeleri
- D. Otomatik ekran parlaklığı ayarı

4. Kötü amaçlı yazılım geliştiricileri neden rootkit kullanır?

- A. Etkin süreçleri ve kötü amaçlı dosyaları işletim sisteminden gizlemek için
- B. Uç noktalarda CPU işlem hızını artırmak
- C. Veritabanı dosyalarını güvenli bulut kasalarına yedeklemek için
- D. Dizüstü bilgisayarlarda pil ömrünü iyileştirmek için

5. Kötü amaçlı yazılım analizinde yalıtılmış ortamda çalıştırma (sandboxing) ne anlama gelir?

- A. Davranışı güvenle gözlemlemek için şüpheli dosyaları yalıtılmış bir sanal kasada çalıştırmak
- B. Dosya özetlerini bilinen tehdit veritabanlarına karşı taramak
- C. Bir saldırıdan sonra veritabanı yedeklerini geri yüklemek
- D. Yerel ağ yönlendiricilerini genel hatlardan ayırmak

Kontrol Noktası 2: Doğru/Yanlış görevi

6 Soru 6

6. Bilgisayar solucanlarının yerel ağlarda yayılması için insan kullanıcı etkileşimi gerekir.

( ) Doğru ( ) Yanlış

7 Soru 7

7. Reklam yazılımı her zaman zararsızdır ve kullanıcı davranışını veya tarama geçmişini izlemez.

( ) Doğru ( ) Yanlış

8 Soru 8

8. Temiz çevrimdışı yedekleri geri yüklemek, mağdurların fidyeyi ödemeden şifrelenmiş dosyaları kurtarmasını sağlar.

( ) Doğru ( ) Yanlış

9 Soru 9

9. İmza tabanlı antivirüs, sıfırıncı gün (zero-day) kötü amaçlı yazılımını, ona ait bir imza oluşmadan önce güvenilir şekilde durdurur.

( ) Doğru ( ) Yanlış

10 Soru 10

10. Dosyasız kötü amaçlı yazılım, kötü amaçlı betikleri sistem belleğinde çalıştırır ve diske dosya yazmaktan kaçınır.

( ) Doğru ( ) Yanlış

Kontrol Noktası 3: Anahtar terim yerleştirme

Aşağıdaki her cümleyi oku ve boşluğu Kelime Bankası'ndaki doğru terimle doldur.

1. Güvenli bir yardımcı program gibi görünen kötü amaçlı yazılım türü: _____ .

2. Veritabanı sistemlerini para karşılığında kilitleyen kötü amaçlı yükler _____ örneğidir.

3. Parolaları gizlice kaydeden tuş kaydediciler _____ örneğidir.

4. İşletim sistemi çekirdeklerinin derinliklerinde saklanmak için bir _____ gerekir.

5. Şüpheli dosyaları yalıtılmış bir kasada analiz etmek için sanal bir _____ kullanılır.

6. Aktif kötü amaçlı yük yayılımını durdurmak için hemen ağ _____ uygulamak gerekir.

KELİME BANKASI

CASUS YAZILIM | DOSYASIZ | FİDYE YAZILIMI | İZOLASYON | KUM HAVUZU | ROOTKIT | SOLUCAN | TRUVA ATI

Cevaplarını buraya yaz:

1.
2.
3.
4.
5.
6.

Kontrol Noktası 4: Güvenlik kavramı eşleştirme

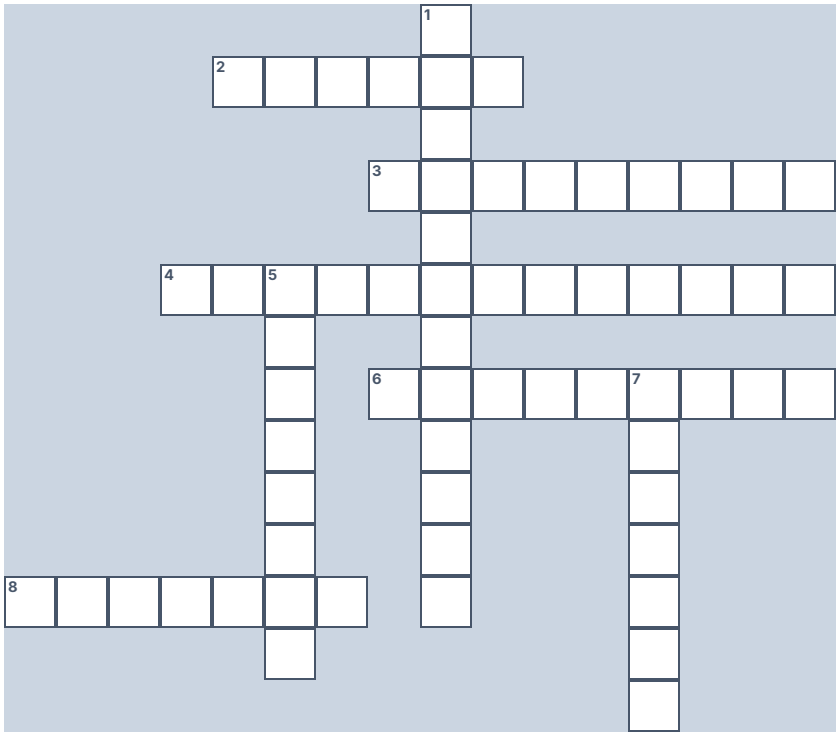
TANIM EŞLEŞTİRME

Soldaki her kelimeyi, doldurulabilir giriş kutusuna ilgili harfi (A-H) yazarak sağdaki doğru tanımıyla eşleştir.

☐	1. TROYA ATI	A	Kullanıcı etkinliğini ve girdilerini gizlice izlemek ve kaydetmek için tasarlanmış program.
☐	2. FİDYE YAZILIMI	B	Disk tarayıcılarından kaçınmak için doğrudan RAM'de çalışan kötü amaçlı yazılım.
☐	3. CASUS YAZILIM	C	Tehdit yüklerinin yayılmasını önlemek için enfekte uç noktaları kısıtlamak.
☐	4. ROOTKIT	D	Zararsız veya yararlı bir yardımcı program gibi görünen kötü amaçlı yazılım.
☐	5. KORUMALI ALAN	E	İnsan müdahalesi olmadan ağlar arasında yayılan kendini kopyalayan kötü amaçlı yazılım.
☐	6. KONTROL ALTINA ALMA	F	Sistem depolamasını şifreleyip anahtarın teslimi için ödeme talep eden kötü amaçlı yazılım.
☐	7. SOLUCAN	G	Kötü amaçlı dosyaları güvenle analiz etmek için kullanılan yalıtılmış sanal ortam.
☐	8. DOSYASIZ	H	Yönetici denetimini sürdürmek için sistem çekirdeklerinin derinlerinde saklanan gizli kötü amaçlı yazılım.

Kontrol Noktası 5: Bulmaca

Bulmacayı, etkin beyaz kutulara harf yazarak çöz. Sayılar aşağıdaki ipuçlarına karşılık gelir.



SOLDAN SAĞA

2. Zararsız veya yararlı bir yardımcı program gibi görünen kötü amaçlı yazılım. (6)

3. Kötü amaçlı dosyaları güvenle analiz etmek için kullanılan yalıtılmış sanal ortam. (9)

4. Sistem depolamasını şifreleyen ve anahtarın teslimi için ödeme talep eden kötü amaçlı yazılım. (13)

6. Tehdit yüklerinin yayılmasını önlemek için enfekte uç noktaları kısıtlama. (9)

8. Yönetici denetimini sürdürmek için sistem çekirdeklerinin derinliklerinde saklanan gizli kötü amaçlı yazılım. (7)

YUKARIDAN AŞAĞI

1. Kullanıcı etkinliklerini ve girdilerini gizlice izlemek ve kaydetmek için tasarlanmış program. (12)

5. Disk tarayıcılarına yakalanmamak için doğrudan RAM'de çalışan kötü amaçlı yazılım. (8)

7. İnsan müdahalesi olmadan ağlar üzerinde yayılan, kendini çoğaltan kötü amaçlı yazılım. (7)

Kontrol Noktası 5, alternatif: Erişilebilir bulmaca ipuçları

Ekran okuyucu ve klavye kullanıcıları, bulmaca cevaplarını aşağıdaki metin alanlarına doğrudan yazabilir.

SOLDAN SAĞA

2 soldan sağa: Zararsız veya yararlı bir yardımcı program gibi görünen kötü amaçlı yazılım. (6 harf):

3 soldan sağa: Kötü amaçlı dosyaları güvenle analiz etmek için kullanılan yalıtılmış sanal ortam. (9 harf):

4 soldan sağa: Sistem depolamasını şifreleyen ve anahtarın teslimi için ödeme talep eden kötü amaçlı yazılım. (13 harf):

6 soldan sağa: Tehdit yüklerinin yayılmasını önlemek için enfekte uç noktaları kısıtlama. (9 harf):

8 soldan sağa: Yönetici denetimini sürdürmek için sistem çekirdeklerinin derinliklerinde saklanan gizli kötü amaçlı yazılım. (7 harf):

YUKARIDAN AŞAĞI

1 yukarıdan aşağı: Kullanıcı etkinliklerini ve girdilerini gizlice izlemek ve kaydetmek için tasarlanmış program. (12 harf):

5 yukarıdan aşağı: Disk tarayıcılarına yakalanmamak için doğrudan RAM'de çalışan kötü amaçlı yazılım. (8 harf):

7 yukarıdan aşağı: İnsan müdahalesi olmadan ağlar üzerinde yayılan, kendini çoğaltan kötü amaçlı yazılım. (7 harf):

Kontrol Noktası 6: Gizli kelime bulmacası

Aşağıdaki ızgarada gizlenmiş 8 temel kelimeyi bul. Kelimeler yatay, dikey veya çapraz olabilir.

M H R Z R F Ö K U E A A Ö N L
I Z O Ş V Ö İ U P Ş İ R Ç L Y
L I N B F R Ü M Ü I Z A P Z Y
I S A Y S J G H H L O P İ K K
Z A J S O N Ğ A Ö Ö L G Z A N
A Y O T L F T V C Y A P Y B Ğ
Y S R K U Z G U I M S O M Ü C
S O T K C Z Y Z F V Y N U T J
U D T O A B M U U S O K G T Ç
S Y T İ N P B Ü Z V N K P Ö V
A F İ D Y E Y A Z I L I M I H
C N D A Ç İ Ö U Ü Ü J I Ğ Ş Ğ
F B R O O T K I T E H İ S R U
P Z E Ğ E R C A J O C Z K İ U
P Ş A R Ü I K K G Ğ L Ğ P F J

KELİME LİSTESİ

TROJAN · FİDYEYAZILIMI · CASUSYAZILIM · ROOTKIT · KUMHAVUZU · İZOLASYON · SOLUCAN · DOSYASIZ

Kontrol Noktası 6, alternatif: Erişilebilir kelime eşleştirme

Kelime Bulmaca'daki 8 kelimenin her birini, boşluğa harfi (A-H) yazarak doğru tanımıyla eşleştir.

KELİME TERİMLERİ

- **A. TROJAN**
- **B. FİDYEYAZILIMI**
- **C. CASUSYAZILIM**
- **D. ROOTKIT**
- **E. KUMHAVUZU**
- **F. İZOLASYON**
- **G. SOLUCAN**
- **H. DOSYASIZ**

TANIMLAR VE EŞLEŞTİRME ALANLARI

1. Yönetici denetimini sürdürmek için sistem çekirdeklerinin derinliklerinde saklanan gizli kötü amaçlı yazılım.
2. Tehdit yüklerinin yayılmasını önlemek için enfekte uç noktaları kısıtlama.
3. Disk tarayıcılarına yakalanmamak için doğrudan RAM'de çalışan kötü amaçlı yazılım.
4. İnsan müdahalesi olmadan ağlar üzerinde yayılan, kendini çoğaltan kötü amaçlı yazılım.
5. Sistem depolamasını şifreleyen ve anahtarın teslimi için ödeme talep eden kötü amaçlı yazılım.
6. Kullanıcı etkinliklerini ve girdilerini gizlice izlemek ve kaydetmek için tasarlanmış program.
7. Zararsız veya yararlı bir yardımcı program gibi görünen kötü amaçlı yazılım.
8. Kötü amaçlı dosyaları güvenle analiz etmek için kullanılan yalıtılmış sanal ortam.

Kontrol Noktası 7: Karışık harflerden kelime bulma görevi

Temel siber güvenlik kavramlarını ve terimlerini ortaya çıkarmak için aşağıdaki harfleri doğru sıraya diz. Cevaplarını verilen giriş kutularına yaz.

1. OTJANR
2. MASYCLISZIAU
3. KVAUUUHZM
4. NOCUASL
5. IIİDZEIYLAFMY
6. IOKRTTO
7. SİONYLZAO
8. YOAZDISS

Bonus etkinlik: Hızlı Düşün

HER KATEGORİ İÇİN 3 CEVAP. LİSTEYİ İLK TAMAMLAYAN KAZANIR.

1	Güvenli uygulama indirebileceğin yerler			
2	Hacklenebilecek cihazlar			
3	Yedeklediğin şeyler			
4	E-postadaki uyarı işaretleri			
5	Bir telefonda kötü amaçlı yazılım olduğunu gösteren işaretler			
6	Bildiğin kötü amaçlı yazılım türleri			
7	Dikkatli olunması gereken dosya türleri			
8	Kötü amaçlı yazılımın bilgisayara bulaşma yolları			
9	Bugün başlayabileceğin güvenli alışkanlıklar			
10	Siber güvenlikle ilgili sözcükler			
11	Veri sızıntısından sonra yapılacaklar			
12	Yazılımı güncelleme nedenleri			
13	Kötü amaçlı yazılım gibi adları olan hayvanlar veya karakterler			
14	Kötü amaçlı yazılımın çalabileceği şeyler			
15	Yanlış bağlantıya tıkladıysan yapılacaklar			

Kontrol Noktası 8: Siber güvenlik vaka çalışmaları

Öğrendiğin kavramları aşağıdaki gerçek dünya senaryolarını çözmek için uygula.

VAKA ÇALIŞMASI 1: KURUMSAL FİDYE YAZILIMI YÜKÜNÜ KONTROL ALTINA ALMA

👷

Senaryo: Kurumsal bir yerel alan ağı, aktif bir fidye yazılımı tarafından ele geçirildi. Önemli dosya sunucuları .locked uzantılı dosyalar göstermeye başladı. Sınırlama politikaları oluştur.

Tartışma sorusu: Sınırlandırma adımlarını ayrıntılı anlat ve veri kurtarma protokolünü özetle.

VAKA ÇALIŞMASI 2: DOSYASIZ KÖTÜ AMAÇLI YAZILIM BELLEK ENJEKSİYONU

👷

Senaryo: Bir analist, standart yönetim araçlarıyla doğrudan geçici sistem RAM'inde çalışan şüpheli betik desenleri tespit ediyor, ancak diskte kötü amaçlı hiçbir dosya yok.

Tartışma sorusu: Bellek analizi stratejisini açıkla ve dosyasız çalıştırmayı engelleyecek araçları belirt.

Kontrol Noktası 9: Şifreyi Çöz

Bir siber güvenlik uzmanı, ağ varlıklarını çevrimiçi tehdit aktörlerine karşı korur. Aşağıdaki Harf-Sayı anahtarını kullanarak, eşleşen harfleri boşluklara yazıp mesajın şifresini çöz.

HARFTEN SAYIYA ŞİFRELEME ANAHTARI

A=1 B=2 C=3 Ç=4 D=5 E=6 F=7 G=8 Ğ=9 H=10

I=11 İ=12 J=13 K=14 L=15 M=16 N=17 O=18 Ö=19 P=20

R=21 S=22 Ş=23 T=24 U=25 Ü=26 V=27 Y=28 Z=29

25 4 17 18 14 24 1 28 26 14 15 6 21 12 17 12

12 29 15 6 16 6 28 15 6 24 6 22 20 12 24 6 24

Çözülen mesaj:

İPUCU: HER SAYI, O HARFİN ALFABEDEKİ SIRASINI GÖSTERİR (ÖR. 1 = A, 2 = B, 29 = Z).

Kontrol Noktası 10: Siber güvenlik hakkında sık sorulan sorular – temel düzey (Bölüm A)

Çevrimiçi tehditlerin azaltılmasına ilişkin sık sorulan soruları ve cevapları incele.

Q1: Kötü amaçlı yazılım nedir?

Tehdit aktörleri tarafından cihazlara ve ağlara zarar vermek, bunları ele geçirmek veya verilerini çalmak için tasarlanmış kötü amaçlı yazılım.

Q2: Virüs ile solucan arasındaki fark nedir?

Virüsün yayılması için insan eylemi (dosya açmak gibi) gerekir; solucan ise ağlar arasında otomatik olarak yayılır.

Q3: Truva atı bir bilgisayara nasıl bulaşır?

Zararsız veya güvenli bir program gibi görünerek kullanıcıları kandırır ve kötü amaçlı yükünü içine gizler.

Q4: Fidye yazılımı nedir?

Hedef sistemdeki dosyaları şifreleyen ve şifre çözme anahtarı karşılığında maddi ödeme talep eden kötü amaçlı yazılım türü. [1]

Q5: Casus yazılım nedir?

Kullanıcının tuş vuruşlarını, parolalarını ve gezinme alışkanlıklarını gizlice kaydedip saldırganlara gönderen kötü amaçlı yazılım.

Kontrol Noktası 10: Siber güvenlik hakkında sık sorulan sorular – temel düzey (Bölüm B)

Çevrimiçi tehditlerin azaltılmasına ilişkin sık sorulan soruları ve cevapları incele.

Q6: Korumalı alanda çalıştırma (sandboxing) ne demektir?

Şüpheli dosyaları, üretim sistemlerine risk oluşturmadan davranışlarını gözlemlemek için güvenli, yalıtılmış bir sanal ortamda çalıştırmak.

Q7: Dosyasız kötü amaçlı yazılım nedir?

Meşru araçları kullanarak doğrudan sistem belleğinde (RAM) çalışan ve temel tarayıcıları atlatmak için diske dosya yazmayan kötü amaçlı yazılım.

Q8: Bir rootkit kötü amaçlı yazılımı nasıl korur?

Kötü amaçlı süreçleri ve dosyaları, çoğunlukla işletim sistemi çekirdeğini bozarak gizler; bu yüzden antivirüs tarayıcıları bunları gözden kaçırabilir.

Q9: Dinamik davranış izleme nedir?

Etkin işlemleri gerçek zamanlı izleyerek toplu dosya şifreleme gibi kötü amaçlı yazılımlara özgü eylemleri engelleyen antivirüs taraması.

Q10: Olay müdahalesi sırasında sınırlandırma neden acildir?

Ele geçirilmiş uç noktaları yalıtmak, etkin kötü amaçlı yazılım yüklerinin diğer ağ cihazlarına yayılmasını önler.

Kontrol Noktası 10: Güvenlik hakkında sık sorulan sorular – ileri düzey (Bölüm C)

Güvenlik çerçevelerinin, kötü amaçlı yazılım analizinin ve veri uyumluluğunun ileri düzey teknik yönlerini keşfet.

Q1: Kötü amaçlı yazılım geliştiricileri imza tabanlı virüsten koruma tarayıcılarını nasıl atlatır?

Polimorfizm kullanırlar; kötü amaçlı davranışı aynı tutarak her enfeksiyonda dosyanın karma değerini ve kod yapısını değiştirirler.

Q2: Kötü amaçlı yazılım kampanyalarında çift kullanımlı araçların riski nedir?

Saldırganlar, normal ağ trafiğine karışmak ve tespiti zorlaştırmak için meşru yönetim araçlarını (PowerShell veya Sysinternals gibi) kullanır.

Q3: İşlem oyma (process hollowing) kötü amaçlı yükleri nasıl çalıştırır?

Meşru bir sistem sürecini askıya alınmış durumda başlatır, bellek kodunu kötü amaçlı yazılımla değiştirir ve yürütmeyi sürdürür.

Q4: Komuta ve Kontrol (C2) sunucusunun rolü nedir?

Ele geçirilmiş makinelerde çalışan kötü amaçlı yazılıma talimat ve yük göndermek için bilgisayar korsanlarının işlettiği uzak sunucu.

Q5: Tuş kaydını (keylogging) tespit etmek neden zordur?

Temel keylogger'lar minimum CPU kaynağı tüketir ve işlemlerini meşru kullanıcı alanı yardımcı programlarının içine gizler.

Kontrol Noktası 10: Güvenlik hakkında sık sorulan sorular – ileri düzey (Bölüm D)

Güvenlik çerçevelerinin, kötü amaçlı yazılım analizinin ve veri uyumluluğunun ileri düzey teknik yönlerini keşfet.

Q6: Kod gizleme, kötü amaçlı yazılım analizini nasıl geciktirir?

Kaynak kodu şifreler veya yeniden düzenler; böylece analist araçları ve güvenlik tarayıcıları tarafından okunamaz hale gelir.

Q7: Bootkit'in işlevi nedir?

Önyükleme sürecini (MBR, önyükleme sektörü veya UEFI ürün yazılımı) bulaştıran, böylece işletim sistemi yüklenmeden önce çalışan rootkit.

Q8: Sezgisel tarama sıfır gün tehditlerini nasıl belirler?

Eşleşen bir veri tabanı özeti aramak yerine şüpheli kod kalıplarını ve yönetim komutlarını tarar.

Q9: DLL kaçırma tehdidi nedir?

Meşru bir uygulamayı, uygulamanın dizin yoluna yerleştirilmiş kötü amaçlı bir dinamik bağlantı kitaplığını (DLL) yüklemeye zorlamak.

Q10: Otomatik kötü amaçlı yazılım analiz hatları sanallaştırmayı nasıl kullanır?

Şüpheli dosyaları birden çok işletim sistemi sanal makinesinde çalıştırır, davranış günlükleri ve ağ PCAP dosyaları otomatik olarak üretirler.

Bölüm 11: Siber güvenlikle ilgili 10 gerçek dünya gerçeği ve içgörüsü

Güvenlik ihlalleri, savunma mekanizmaları ve uyumluluk standartlarıyla ilgili gerçek dünya bilgilerini incele.

1. GÜVENLİK İPUCU

Truva atları, kötü amaçlı kodu zararsız görünen programların içine gizledikleri için yaygın bir bulaşma yöntemi olmayı sürdürür.

2. GÜVENLİK İPUCU

FBI'ın IC3 birimi 2025'te 3.600'den fazla fidye yazılımı şikâyeti aldı; bildirilen kayıplar 32 milyon doları aştı. [3]

3. GÜVENLİK İPUCU

Solucanlar, SMB'deki EternalBlue gibi yamalanmamış protokol açıklarından yararlanarak ağlar üzerinde hızla yayılabilir.

4. GÜVENLİK İPUCU

Dosyasız kötü amaçlı yazılımı tespit etmek zordur, çünkü meşru araçlar üzerinden bellekte çalışır ve diskte çok az iz bırakır.

5. GÜVENLİK İPUCU

Analiz korumalı alanları, her test bilinen bir durumdan başlasın diye genellikle her çalıştırmadan sonra temiz bir anlık görüntüye döner.

6. GÜVENLİK İPUCU

Rootkit'ler çekirdek sistem çağrılarını değiştirerek kötü amaçlı yazılım tarayıcılarına yanlış tanılama sonuçları bildirebilir.

7. GÜVENLİK İÇGÖRÜSÜ

Kod gizleme, kötü amaçlı yazılımın gerçek ikili yük yapısını sıkıştırmak ve gizlemek için paketleyici araçlar kullanır.

8. GÜVENLİK İÇGÖRÜSÜ

Polimorfik kötü amaçlı yazılım, imza denetimlerinden kaçınmak için her yeni kopyada kodunu ve dolayısıyla dosya özetini (hash) değiştirir.

9. GÜVENLİK İÇGÖRÜSÜ

DLL ele geçirme, Windows gibi standart işletim sistemlerindeki arama sırası yapılandırmalarından yararlanır.

10. GÜVENLİK İPUCU

Güvenlik sağlayıcıları her gün çok sayıda yeni kötü amaçlı yazılım örneği buluyor, bu nedenle imzaların sürekli güncellenmesi gerekir.

Teknik Referanslar ve Kaynaklar

Çalışma kılavuzu ve etkileşimli bulmacalar, küresel NIST, OWASP ve veri gizliliği uyum standartlarından derlenmiştir.

AKADEMİK VE SEKTÖREL KAYNAKLAR

[1] CISA. (n.d.). Malware, Phishing, and Ransomware.
https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[2] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

[3] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.
https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[4] FBI Internet Crime Complaint Center. (n.d.). Ransomware.
https://www.ic3.gov/CrimeInfo/Ransomware

[5] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.
https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

Cevap Anahtarı: Kontrol Noktası 1 - Çoktan Seçmeli

1 **Soru 1** — **Doğru cevap: A**

ÖĞRETMEN NOTU

Truva atının belirleyici özelliği nedir? → Kullanıcıları çalıştırmaya kandırmak için meşru yazılım gibi görünür

2 **Soru 2** — **Doğru cevap: A**

ÖĞRETMEN NOTU

Hangi kötü amaçlı yazılım türü dosyaları şifreler ve ödeme talep eder? → Fidye yazılımı

3 **Soru 3** — **Doğru cevap: A**

ÖĞRETMEN NOTU

Casus yazılımı ne temsil eder? → Kullanıcı tuş vuruşlarını ve tarayıcı etkinliklerini gizlice izlemek için tasarlanmış kötü amaçlı yazılım

4 **Soru 4** — **Doğru cevap: A**

ÖĞRETMEN NOTU

Kötü amaçlı yazılım geliştiricileri neden rootkit kullanır? → Etkin süreçleri ve kötü amaçlı dosyaları işletim sisteminden gizlemek için

5 **Soru 5** — **Doğru cevap: A**

ÖĞRETMEN NOTU

Kötü amaçlı yazılım analizinde yalıtılmış ortamda çalıştırma (sandboxing) ne anlama gelir? → Davranışı güvenle gözlemlemek için şüpheli dosyaları yalıtılmış bir sanal kasada çalıştırmak

Cevap Anahtarı: Kontrol Noktası 2 - Doğru veya Yanlış

6 **Soru 6** — **Doğru cevap: Yanlış**

ÖĞRETMEN NOTU

Yanlış: solucanlar kendini kopyalar ve herhangi bir kullanıcı eylemi olmadan ağlar üzerinden yayılır.

7 **Soru 7** — **Doğru cevap: Yanlış**

ÖĞRETMEN NOTU

Yanlış: reklam yazılımı her zaman zararsız değildir; birçoğu reklam hedeflemek için gezinmeyi izler.

8 **Soru 8** — **Doğru cevap: Doğru**

ÖĞRETMEN NOTU

Doğru: temiz çevrimdışı yedekler şifrelenmiş dosyaları ödeme yapmadan geri getirir, ancak çalınan veriler yine de sızabilir.

9 **Soru 9** — **Doğru cevap: Yanlış**

ÖĞRETMEN NOTU

Yanlış: imza tarayıcıları bilinen bir örneğe ihtiyaç duyar, bu yüzden yepyeni sıfırıncı gün (zero-day) kötü amaçlı yazılımı onlardan kaçabilir.

10 **Soru 10** — **Doğru cevap: Doğru**

ÖĞRETMEN NOTU

Dosyasız kötü amaçlı yazılım, kötü amaçlı betikleri sistem belleğinde çalıştırır ve diske dosya yazmaktan kaçınır.

Kelime anahtarları ve puanlama ölçeği

Öğretmen notlandırma ölçeği: 1 puan ver — doğru her eşleştirme için (toplam 8 puan) ve her bağlam terimi için (toplam 6 puan).

KONTROL NOKTASI 4: CEVAP ANAHTARI – KAVRAM EŞLEŞTİRME

D 1. TROYA ATI	F 2. FİDYE YAZILIMI	A 3. CASUS YAZILIM	H 4. ROOTKIT
G 5. KORUMALI ALAN	C 6. KONTROL ALTINA ALMA	E 7. SOLUCAN	B 8. DOSYASIZ

KONTROL NOKTASI 3: CEVAP ANAHTARI – ANAHTAR TERİMLER

1 TRUVA ATI	2 FİDYE YAZILIMI	3 CASUS YAZILIM	4 ROOTKIT
5 KUM HAVUZU	6 İZOLASYON		

KONTROL NOKTASI 6, ALTERNATİF: CEVAP ANAHTARI – KELİME EŞLEŞTİRME

1 D – ROOTKIT	2 F – İZOLASYON	3 H – DOSYASIZ	4 G – SOLUCAN
5 B – FİDYEYAZILIMI	6 C – CASUSYAZILIM	7 A – TROJAN	8 E – KUMHAVUZU

EĞİTMENLER İÇİN TARTIŞMA NOTLARI

Anahtar terimler:
Öğrencilerin TROYA ATI, FİDYE YAZILIMI ve CASUS YAZILIM terimlerini kendi sözcükleriyle açıklayıp her biri için bir örnek verebildiğini kontrol et.

Vaka çalışmaları:
Öğrencilerden önerilerini varsayımlarla değil, çalışma kâğıdındaki bilgilerle desteklemelerini iste.

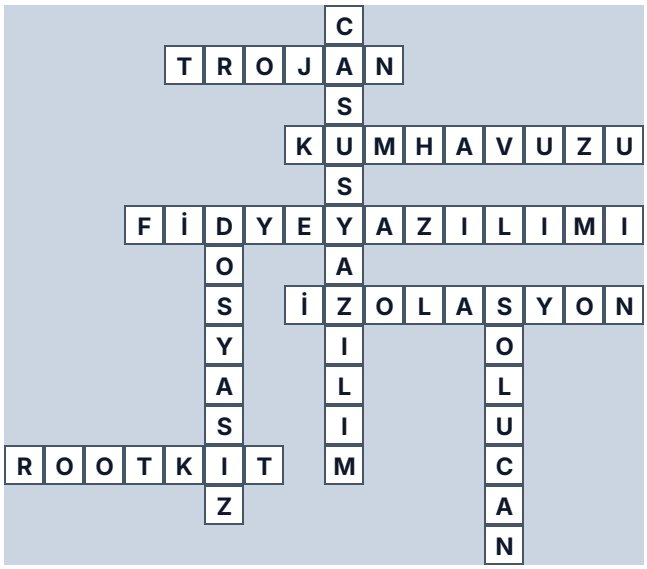
Kaynakların değerlendirilmesi:
Öğrencilerden çalışma kâğıdının kaynaklarında en az bir iddiayı doğrulamalarını iste ve rakamların, fiyatların ve kuralların zamanla neden değişebileceğini tartışın.

Bulmaca anahtarları ve öğretmen notları

KELİME BULMACA ÇÖZÜMÜ

M	H	R	Z	R	F	Ö	K	U	E	A	A	Ö	N	L
I	Z	O	Ş	V	Ö	İ	U	P	Ş	İ	R	Ç	L	Y
L	I	N	B	F	R	Ü	M	Ü	I	Z	A	P	Z	Y
I	S	A	Y	S	J	G	H	H	L	O	P	İ	K	K
Z	A	J	S	O	N	Ğ	A	Ö	Ö	L	G	Z	A	N
A	Y	O	T	L	F	T	V	C	Y	A	P	Y	B	Ğ
Y	S	R	K	U	Z	G	U	I	M	S	O	M	Ü	C
S	O	T	K	C	Z	Y	Z	F	V	Y	N	U	T	J
U	D	T	O	A	B	M	U	U	S	O	K	G	T	Ç
S	Y	T	İ	N	P	B	Ü	Z	V	N	K	P	Ö	V
A	F	İ	D	Y	E	Y	A	Z	I	L	I	M	I	H
C	N	D	A	Ç	İ	Ö	U	Ü	Ü	J	I	Ğ	Ş	Ğ
F	B	R	O	O	T	K	I	T	E	H	İ	S	R	U
P	Z	E	Ğ	E	R	C	A	J	O	C	Z	K	İ	U
P	Ş	A	R	Ü	I	K	K	G	Ğ	L	Ğ	P	F	J

BULMACA ÇÖZÜMÜ



BULMACA ÇÖZÜMLERİ İÇİN ÖĞRETMEN REHBERİ

SOLDAN SAĞA

2 soldan sağa: TROJAN Zararsız veya yararlı bir yardımcı program gibi görünen kötü amaçlı yazılım. (6 harf)

3 soldan sağa: KUMHAVUZU Kötü amaçlı dosyaları güvenle analiz etmek için kullanılan yalıtılmış sanal ortam. (9 harf)

4 soldan sağa: FİDYEYAZILIMI Sistem depolamasını şifreleyen ve anahtarın teslimi için ödeme talep eden kötü amaçlı yazılım. (13 harf)

6 soldan sağa: İZOLASYON Tehdit yüklerinin yayılmasını önlemek için enfekte uç noktaları kısıtlama. (9 harf)

8 soldan sağa: ROOTKIT Yönetici denetimini sürdürmek için sistem çekirdeklerinin derinliklerinde saklanan gizli kötü amaçlı yazılım. (7 harf)

YUKARIDAN AŞAĞI

1 yukarıdan aşağı: CASUSYAZILIM Kullanıcı etkinliklerini ve girdilerini gizlice izlemek ve kaydetmek için tasarlanmış program. (12 harf)

5 yukarıdan aşağı: DOSYASIZ Disk tarayıcılarına yakalanmamak için doğrudan RAM'de çalışan kötü amaçlı yazılım. (8 harf)

7 yukarıdan aşağı: SOLUCAN İnsan müdahalesi olmadan ağlar üzerinde yayılan, kendini çoğaltan kötü amaçlı yazılım. (7 harf)

Karışık Kelimeler ve Şifre Çözüm Anahtarı

Kelime karıştırma etkinliği ve Gizli Şifre Görevi için notlandırma anahtarı.

KELİME KARIŞTIRMA ANAHTARI

1.	OTJANR	TROJAN	5.	IIİDZEIYLAFMY	FİDYEYAZILIMI
2.	MASYCLISZIAU	CASUSYAZILIM	6.	IOKRTTO	ROOTKIT
3.	KVAUUUHZM	KUMHAVUZU	7.	SİONYLZAO	İZOLASYON
4.	NOCUASL	SOLUCAN	8.	YOAZDISS	DOSYASIZ

GİZLİ ŞİFRE GÖREVİ CEVAP ANAHTARI

"UÇ NOKTA YÜKLERİNİ İZLEMEYLE TESPİT ET"

Vaka çalışmaları cevap anahtarı

A Vaka Çalışması 1: Kurumsal Fidye Yazılımı Yükünü Kontrol Altına Alma

Öğretmen çözümü

NOTLANDIRMA YÖNERGESİ

Öğrenci cevapları şu noktaları kapsamalıdır:

- Senaryo analizi: Bir kurumsal yerel ağ, etkin fidye yazılımı tarafından ihlal edildi. Kilit dosya sunucuları .locked uzantılı dosyalar göstermeye başladı. Sınırlama politikalarını oluştur.
- Önerilen strateji ve çözüm: Etkilenen tüm sunucuların yerel ağ bağlantısını kes. Etkin yönetici oturumlarını sonlandır. Etkilenmemiş dosyaları, yazmaya karşı kilitli, güvenli bir çevrimdışı yedekleme sisteminden geri yükle.

B Vaka Çalışması 2: Dosyasız Kötü Amaçlı Yazılım Bellek Enjeksiyonu

Öğretmen çözümü

NOTLANDIRMA YÖNERGESİ

Öğrenci cevapları şu noktaları kapsamalıdır:

- Senaryo analizi: Bir analist, standart yönetim araçlarıyla doğrudan geçici sistem RAM'inde çalışan şüpheli betik kalıpları tespit eder, ancak diskte kötü amaçlı dosya yoktur.
- Önerilen Strateji ve Çözüm: Etkilenen uç noktaları izole et ve önce bir bellek görüntüsü al. PowerShell ve WMI günlüklerini incele, onaylanmamış betikleri AppLocker ile engelle, ardından zararlı yükü temizlemek için yeniden başlat.