Çevrimiçi Akış Platformları için Gelişmiş Ağ Trafiği Analizi ve Altyapı Tespiti: Yayıncı Avı Projesi için 2025 Yılı Teknikleri ve Eğilimleri

I. Yönetici Özeti

"Yayıncı Avı Projesi", Twitch, YouTube Stream, Microsoft Teams, Google Meet ve Zoom gibi başlıca çevrimiçi yayın ve iletişim platformları tarafından kullanılan IP adreslerini, sunucuları ve port numaralarını hassas bir şekilde belirlemeyi amaçlayan kapsamlı bir ağ analizi girişimidir. Bu proje, yayın yaparken veya yayın izlerken ortaya çıkan ağ trafiğinin derinlemesine incelenmesini, iletişim kurulan sunucuların tespitini ve Wireshark gibi paket analiz araçları kullanılarak trafiğin detaylı bir şekilde yakalanıp analiz edilmesini içermektedir. Proje kapsamında, yayın trafiğini seçici olarak yakalamak için yakalama filtreleri (capture filter'lar) ve yakalanan trafiği sınıflandırmak ve incelemek için görüntüleme filtreleri (display filter'lar) oluşturulmaktadır. Her platformun kullandığı altyapı, İçerik Dağıtım Ağları (CDN'ler) ve bağlantı protokolleri analiz edilmektedir. Nihai hedef, bu platformların ağ düzeyinde nasıl çalıştığını ortaya koymaktır. Projenin ileri aşamalarında, tüm bu analiz sürecini otomatikleştirecek bir Python betiği geliştirilerek IP tespiti ve filtreleme işlemleri komut satırından yürütülebilir hale getirilecektir. Bu otomasyon, benzer projelerde veya adli analizlerde hızlı ve otomatik trafik inceleme imkanı sunarak ağ güvenliği, tersine mühendislik ve yayın altyapısı analizi konularında pratik bilgi kazandırmayı hedeflemektedir.

Modern ağ ortamı, yaygın şifreleme (QUIC, TLS 1.3), dinamik bulut altyapıları ve sofistike tehdit aktörleri ile karakterize edildiğinden, geleneksel ağ analizi yöntemleri giderek etkisiz hale gelmektedir. Bu durum, "Yayıncı Avı Projesi"nin hedeflerine ulaşabilmesi için ileri düzey tekniklere ve eğilimlere yönelmesini zorunlu kılmaktadır. Bu rapor, 2025 yılı için bu zorlukların üstesinden gelmek ve projenin amaçlarını gerçekleştirmek için gerekli olan en son ve en etkili on tekniği ve eğilimi detaylandırmaktadır. Bu teknikler, şifrelenmiş trafiğin analizinden otomasyona, davranışsal profillemeden altyapı haritalamasına kadar geniş bir yelpazeyi kapsamaktadır.

II. Çevrimiçi Akış ve İletişim Altyapısının Gelişen Manzarası

Çevrimiçi akış ve iletişim platformları, internet trafiğinin önemli bir bölümünü oluşturmakta ve sürekli gelişen ağ teknolojileriyle birlikte karmaşık bir altyapı sunmaktadır. Bu altyapının anlaşılması, "Yayıncı Avı Projesi" gibi ağ analizi girişimleri için kritik öneme sahiptir.

Modern Akış ve İletişim Protokollerine Genel Bakış

Günümüz web trafiği, özellikle Google, Facebook ve Cloudflare gibi büyük platformlar tarafından benimsenen QUIC (Quick UDP Internet Connections) protokolünün yaygınlaşmasıyla köklü bir dönüşüm geçirmiştir. QUIC, hem güvenlik hem de performans açısından önemli iyileştirmeler sunmaktadır.[1] HTTP/3, QUIC üzerine inşa edilmiş olup, 2023 yılında HTTP isteklerinin yaklaşık %30'unu oluşturarak giderek yaygınlaşmaktadır ve büyümesinin devam etmesi beklenmektedir.[2]

Taşıma Katmanı Güvenliği (TLS) protokolünün en son sürümü olan TLS 1.3, her oturum için Mükemmel İleri Gizlilik (PFS) sağlamak amacıyla geçici Diffie-Hellman anahtar değişimi kullanımını zorunlu kılmaktadır.[3] Bu değişiklik, sunucu özel anahtarlarına erişim olsa bile trafiğin pasif olarak şifresinin çözülmesini önemli ölçüde zorlaştırmaktadır.[3]

Hem QUIC hem de TLS 1.3, el sıkışmanın ve başlıkların önemli kısımları da dahil olmak üzere tüm iletişimi şifrelemektedir. Bu durum, geleneksel Derin Paket İncelemesi (DPI) ve Saldırı Tespit/Önleme Sistemlerini (IDS/IPS) büyük ölçüde etkisiz hale getirmektedir.[2] QUIC'in bağlantı geçişi ve Bağlantı Kimliklerinin (CID'ler) sık rotasyonu gibi doğal özellikleri, trafik analizini daha da karmaşıklaştırmakta ve ağ müdahalesine karşı daha dirençli hale getirmektedir.[2] Bu durum, "Yayıncı Avı Projesi"nin geleneksel yük incelemesine dayalı yaklaşımlardan uzaklaşmasını gerektirmektedir.

İçerik Dağıtım Ağlarının (CDN'ler) Merkezi Rolü

CDN'ler, yalnızca içerik dağıtımına odaklanmaktan, güvenli, yüksek performanslı ve gerçek zamanlı içerik dağıtımı, uç bilişim ve bulut tabanlı hizmetler sunan kapsamlı hizmet paketlerine dönüşmüştür.[6] Video akış hizmetleri, 4K ve 8K gibi yüksek çözünürlüklü içeriklere olan artan talep ve düşük gecikme süresi gereksinimleri için vazgeçilmezdirler.[6]

CDN'ler, kullanıcı isteklerini en yakın uç sunucuya yönlendirmek için Anycast DNS gibi teknikleri kullanarak performansı optimize etmekte ve ağ tıkanıklığını yönetmektedir.[7] Alan adlarını CDN altyapısına eşlemek için CNAME ve A/AAAA kayıtları gibi DNS yönlendirme yöntemleri kritik öneme sahiptir.[7] Ayrıca, IP tabanlı coğrafi konumlandırma, CDN'ler tarafından son kullanıcının yaklaşık fiziksel konumunu belirlemek için kullanılmaktadır. Bu, bölgeye özgü içerik sunumunu mümkün kılmakta ve içerik dağıtımındaki lisans kısıtlamalarını uygulamak için kullanılmaktadır.[9]

Ağ Trafiği Analizindeki Temel Zorluklar

Ağ trafiği analizinde karşılaşılan en önemli zorluk, QUIC ve TLS 1.3 ile birlikte ağ trafiğinin giderek artan şifrelenmesidir. Bu durum, geleneksel yük incelemesine dayalı

yöntemleri geçersiz kılmaktadır.[1] Bu durum, analizde meta veri ve davranışsal analize doğru bir kaymayı zorunlu kılmaktadır.

Bulut bilişimin yükselişi ve 5G ağlarının benimsenmesi, sofistike DPI çözümlerine olan ihtiyacı artırmaktadır.[14] Ancak, bulut depolamanın dağıtık yapısı ve dinamik iş yükleri, veri izlemeyi ve analizi karmaşıklaştırmaktadır. Kanıtlar coğrafi olarak dağınık sunucular arasında parçalanmış olabilir.[15] Bu durum, akış platformlarının belirli IP'lerini ve sunucularını belirleme yeteneğini doğrudan etkilemektedir.

Gelişmiş Kalıcı Tehditler (APT'ler) de dahil olmak üzere modern tehditler, normal ağ trafiğiyle harmanlanacak şekilde tasarlanmıştır ve bu da tespit edilmelerini son derece zorlaştırmaktadır.[16] Bulut ortamlarında insan dışı kimliklerin (NHI) yaygınlaşması, güvenlik uzmanları için yeni kimlik yönetimi zorlukları yaratmaktadır.[17]

Ortaya Çıkan Modeller ve Daha Geniş Çıkarımlar

Şifreleme, modern ağ analizinde bir paradoks yaratmaktadır: güvenlik artarken görünürlük azalmaktadır. QUIC ve TLS 1.3 gibi protokoller, trafiğin neredeyse tamamını şifreleyerek geleneksel Derin Paket İncelemesini (DPI) etkisiz hale getirmektedir.[2] Bu durum, "Yayıncı Avı Projesi"nin akış protokollerini veya içeriğini belirlemek için geleneksel yük incelemesine güvenemeyeceği anlamına gelmektedir. Bu durum, "paketin içinde ne var"dan "paketin nasıl davrandığına" doğru bir paradigma kaymasını zorunlu kılmaktadır. Bu eğilim, ağ güvenliği ve adli bilişim araçlarının imza tabanlı tespitten davranışsal ve meta veri odaklı analize doğru evrilmesi gerektiğini göstermektedir. Aynı zamanda, kullanıcı gizliliği ve performansı ile güvenlik ve yönetim için ağ gözlemlenebilirliği arasında bir gerilim olduğunu da ortaya koymaktadır.

CDN'lerin karmaşıklığı, altyapı haritalaması için iki ucu keskin bir kılıç görevi görmektedir. CDN'ler, akış performansının vazgeçilmez bir parçasıdır.[6] Anycast DNS [7] ve dinamik yönlendirme [7] gibi teknikler kullanarak kullanıcıları en yakın uç sunucuya yönlendirmektedirler. Bu durum, tek bir akış platformunun "IP adresinin" statik veya tekil olmadığı, bunun yerine coğrafi olarak dinamik bir IP'ler kümesi olduğu anlamına gelmektedir. Bu, kullanıcılar için faydalı olsa da, "Yayıncı Avı Projesi" için belirli bir platform için kesin bir IP ve sunucu kümesi belirlemede önemli bir karmaşıklık yaratmaktadır. Bu durum, basit IP aramalarının yetersiz olduğu; DNS, ASN ve coğrafi konumlandırmayı içeren dinamik, çok yönlü bir yaklaşımın gerekli olduğu anlamına gelmektedir. Modern internet hizmetlerinin CDN'ler ve bulut bilişim tarafından yönlendirilen dağıtık doğası, ağ keşif ve adli soruşturmaların nasıl yürütülmesi gerektiğini temelden değiştirmektedir. Odak noktası, statik ana bilgisayar merkezli analizden dinamik akış merkezli ve altyapı merkezli haritalamaya kaymaktadır.

Şifreleme ve ölçek zorluklarının üstesinden gelmede Yapay Zeka (YZ) ve Makine Öğrenimi (ML) zorunluluğu açıkça görülmektedir. Derin Paket İncelemesi (DPI) şifreli trafik nedeniyle zorluklarla karşılaşmaktadır.[5] Ancak[11] gibi kaynaklar, YZ/ML'nin şifreli trafiğin şifresini çözmeden tehdit tespiti, anomali tespiti ve sınıflandırılması için giderek daha fazla benimsendiğini vurgulamaktadır. Bu durum, şifreleme zorluğunun ve modern trafiğin ölçeğinin [14] YZ/ML'nin birincil çözüm olarak benimsenmesini tetiklediğini göstermektedir. "Yayıncı Avı Projesi" için bu, YZ/ML'nin 2025 yılında akış trafiğini tanımlamak ve karakterize etmek için sadece bir iyileştirme değil, bir *gereklilik* olduğu anlamına gelmektedir. YZ/ML, daha önce opak olan trafiğe ilişkin bilgiler sağlamakta ve büyük ölçekte insanlar için imkansız olan görevleri otomatikleştirmektedir. Bu durum, bu modelleri eğitmek için veri kalitesi hakkında da soruları gündeme getirmektedir.[1]

III. Yayıncı Avı Projesi için 2025 Yılının En İyi 10 Gelişmiş Tekniği ve Eğilimi

1. Şifrelenmiş Trafik Sınıflandırması ve Anomali Tespiti için Yapay Zeka/Makine Öğrenimi

Geleneksel Derin Paket İncelemesinin (DPI) yaygın şifreleme (QUIC, TLS 1.3) nedeniyle sınırlamaları göz önüne alındığında, Yapay Zeka (YZ) ve Makine Öğrenimi (ML), şifrelenmiş trafiği şifre çözmeye gerek kalmadan sınıflandırmak ve anormallikleri tespit etmek için vazgeçilmez hale gelmektedir.[1] Bu yaklaşım, yük içeriği yerine gözlemlenebilir meta veri özelliklerinin analizine odaklanmaktadır.

Şifrelenmiş Trafik Sınıflandırma Teknikleri:

- **Meta Veri Analizi:** Paket boyutu, paketler arası varış süreleri, akış süresi, paket yönü ve akışlardaki bayt dağılımı gibi özelliklere odaklanılmaktadır.[11] Bu "gözlemlenebilir paket özellikleri", protokol sınıflandırması ve şifrelenmiş trafik parmak izi için yüksek doğruluk (örneğin, VisQUIC verileri kullanılarak HTTP/3 yanıt tahmini için %97) sağlayabilmektedir.[1]
- **Dalgacık Dönüşümleri ve Eğilim Özellikleri:** Dalgacık Dönüşümleri (WT) gibi gelişmiş özellik çıkarma teknikleri, ağ trafiğinin hem zaman hem de frekans alanı özelliklerini yakalayarak trafiğin davranışına kapsamlı bir bakış sunmaktadır.[11] Eğilim analizi ile birleştirildiğinde, bu özellikler YZ modellerinin sağlamlığını artırarak dinamik internet trafiği modellerine karşı dirençli hale gelmelerini sağlamaktadır.[11] Bu yaklaşım, veri kümesi filtrelemesiyle bile yüksek F1 puanları (örneğin, Random Forest ile VPN tespiti için %99) göstermiştir.[12]
- **Makine Öğrenimi Modelleri:** Çeşitli ML ve Derin Öğrenme (DL) algoritmaları kullanılmaktadır. Random Forest (RF) ve Sinir Ağları (NN), şifrelenmiş trafik

sınıflandırmasında güçlü performans sergilemektedir.[12] Otomatik kodlayıcılar (Autoencoders) karmaşık desen tespiti için uygundur.[19]

Anomali Tespitine Uygulama:

- **Gerçek Zamanlı Anomali Tespiti:** YZ destekli çözümler, ağ anormalliklerini daha hızlı tespit etmekte, trafik davranışını analiz ederek sıfırıncı gün saldırılarını belirlemekte ve tahmine dayalı analizler aracılığıyla düzeltme eylemlerini otomatikleştirebilmektedir.[18] Bu, tehlikeye atılmış bir akış hesabını veya yeni bir saldırı vektörünü gösterebilecek olağandışı iletişim modellerini belirlemek için kritik öneme sahiptir.[19]
- **Temel Çizgilerin Oluşturulması:** ML modelleri, geçmiş verilerden "normal" ağ davranışını öğrenmekte ve sapmaları anomali olarak işaretlemektedir.[19] Bu, istatistiksel aykırı değerlerin (örneğin, ortalama trafiğin standart sapmasının ötesindeki trafik artışları) belirlenmesini içermektedir.[21]

Yayıncı Avı için Pratik Çıkarımlar: Bu teknik, akış platformu trafiğinin ve özelliklerinin şifreli olsa bile belirlenmesini sağlamakta, basit port/IP tespitinin ötesine geçerek davranışsal parmak izine yönelmektedir. Ayrıca, bilinen akış IP'lerinden gelen beklenmedik trafik modellerini işaretleyerek potansiyel kötüye kullanımı veya yeni hizmet özelliklerini gösterebilmektedir.

Şifreleme, geleneksel DPI'yi işe yaramaz hale getirdiğinden, ML/YZ'nin sınıflandırma için meta veriler (paket boyutu, zamanlama, akış modelleri) üzerindeki başarısı, ağ analizinde temel bir değişim olduğunu göstermektedir. Bu, neyin iletişim kurulduğundan çok, nasıl iletişim kurulduğuna odaklanıldığı anlamına gelmektedir. Bu durum, ağ analistleri için veri bilimi ve istatistiksel analiz becerilerinin geleneksel protokol çözümlemesinin önüne geçtiği yeni bir yetkinlik setinin gerekliliğini ortaya koymaktadır. Ayrıca, gelecekteki ağ adli bilişiminin büyük ölçüde toplanmış akış verilerine ve davranışsal modellere dayanacağını da düşündürmektedir.

QUIC trafik analizindeki ilerlemenin, "şifreli QUIC izleri ve ML modellerini kıyaslamak için yapılandırılmış meta veriler içeren herkese açık veri kümelerinin eksikliği" nedeniyle sınırlı olduğu belirtilmektedir.[1] VisQUIC'in 100.000'den fazla etiketli QUIC izi ve kontrollü şifre çözme için SSL anahtarlarıyla tanıtılması, kritik bir ihtiyacı vurgulamaktadır. Bu durum, ML'nin gözlemlenebilir özellikler üzerinde çalışabilmesine rağmen, etkinliğinin doğrudan eğitim verilerinin kalitesi ve kapsamlılığına bağlı olduğunu göstermektedir. Bu, "Yayıncı Avı Projesi" için, akış platformu trafiğinin (canlı akış, VOD, sohbet, ekran paylaşımı gibi farklı aktiviteler dahil) titizlikle etiketlenmiş çeşitli bir veri kümesinin toplanmasının, güçlü YZ/ML sınıflandırma modelleri oluşturmak için sadece faydalı değil, aynı zamanda temel bir adım olduğu anlamına

gelmektedir. Zemin doğruluk etiketlemesi için şifre çözme anahtarlarına erişim (gerçek zamanlı analiz için olmasa bile) paha biçilmezdir.

Aşağıdaki tablo, şifrelenmiş trafik sınıflandırması ve anomali tespiti için 2025 yılındaki YZ/ML modellerinin mevcut durumunu özetlemektedir.

Tablo 1: Şifrelenmiş Trafik Sınıflandırması ve Anomali Tespiti için YZ/ML Modelleri (2025)

Model Tipi	Analiz Edilen Temel Özellikler	Birincil Uygulama	Bildirilen Doğruluk/F1-Skoru (İlgili Görevler İçin)	Güçlü Yönler	Sınırlamalar
Random Forest (RF)	Paket boyutu, paketler arası varış süresi, akış süresi, dalgacık özellikleri	Uygulama Sınıflandırması, Anomali Tespiti, VPN Tespiti	%99 F1-skoru (VPN tespiti) [12]	Yüksek doğruluk, veri kümesi filtrelemesine karşı sağlamlık, karmaşık ilişkileri yakalama yeteneği	Büyük veri kümelerinde hesaplama yoğunluğu, "kara kutu" doğası yorumlamayı zorlaştırabilir
Sinir Ağları (NN)	Paket boyutu, akış süresi, trafik modelleri, dalgacık özellikleri	Uygulama Sınıflandırması, Anomali Tespiti, Protokol Parmak İzi	%98 F1-skoru (VPN tespiti) [12], %97 doğruluk (HTTP/3 yanıt tahmini) [1]	Karmaşık, doğrusal olmayan modelleri öğrenebilme, büyük veri kümeleriyle iyi ölçeklenebilme	Yüksek hesaplama maliyeti, aşırı uyum riski, eğitim verisi kalitesine bağımlılık
Otomatik Kodlayıcılar (Autoencoders)	Karmaşık paket modelleri, akış özellikleri	Karmaşık Desen Tespiti, Anomali Tespiti	Belirtilmemiş (genel anomali tespiti için uygundur) [19]	Etiketlenmemiş verilerle anormallikleri tespit etme yeteneği, boyut	Eğitim için büyük miktarda "normal" veri gerektirir, anormallikler

				indirgeme	in yorumlanması zor olabilir
K-Means Kümeleme	Grup davranışı, trafik akışı istatistikleri	Grup Davranışı Tespiti, Web Sitesi Saldırıları [19]	Belirtilmemiş (genel anomali tespiti için uygundur) [19]	Basit ve hızlı, büyük veri kümeleriyle iyi çalışır	Küme sayısının önceden belirlenmesi gerekir, küre şekilli kümeler varsayar
Isolation Forest	Nadir olaylar, aykırı değerler	Dolandırıcılık Tespiti, Nadir Olay Tespiti [19]	Belirtilmemiş (genel anomali tespiti için uygundur) [19]	Yüksek boyutlu verilerde etkilidir, hızlıdır, aykırı değerleri doğrudan izole eder	Yoğun kümelerdeki anormallikleri tespit etmek zor olabilir

2. Python (PyShark/Scapy) ile Gelişmiş Wireshark Betikleme ve Otomasyonu

Wireshark, ağ analizi için temel bir araç olmaya devam etmekte, güçlü paket yakalama, filtreleme, görselleştirme, protokol desteği ve istatistiksel analiz yetenekleri sunmaktadır.[22] Ağ sorun giderme, güvenlik denetimi, adli bilişim ve performans optimizasyonu için kritik öneme sahiptir.[22]

Otomasyon için Python (PyShark/Scapy):

- **PyShark bir TShark Sarmalayıcısı Olarak:** PyShark, Wireshark'ın komut satırı arayüzü olan TShark için güçlü bir Python sarmalayıcısı olarak hizmet vermektedir.[24] Paket verilerine programatik erişim sağlayarak, ağ arayüzlerinden canlı trafik analizine veya mevcut PCAP dosyalarının işlenmesine olanak tanımaktadır.[24]
- **Otomatik İş Akışları:** PyShark, hem BPF yakalama filtrelerini (yakalama sırasında alakasız paketleri göz ardı ederek kaynak tasarrufu yapmak için) hem de görüntüleme filtrelerini (yakalama sonrası analiz için) desteklemektedir.[24] Bu, karmaşık tehdit avcılığını, veri çözmeyi/şifre çözmeyi (anahtarlar mevcutsa), davranışsal analizi ve diğer güvenlik araçlarıyla entegrasyonu otomatikleştirmek için hayati öneme sahiptir.[24]
- **Scapy Entegrasyonu:** Başka bir Python kütüphanesi olan Scapy, paket oluşturma

ve manipülasyonuna olanak tanıyarak PyShark'ı tamamlamaktadır. Bu, aktif testler veya analiz için belirli akış davranışlarını simüle etmek için faydalı olabilir.[25]

Özel Dissektör Geliştirme (Lua/C):

- **Tescilli Protokolleri Ele Alma:** Tescilli veya daha az yaygın protokoller kullanan akış platformları için, derin yük incelemesi ve detaylı protokol analizi için özel Wireshark dissektörleri (Lua betikleme veya yerel entegrasyon için C kullanılarak) geliştirmek esastır.[26]
- **Dissektör İşlevselliği:** Özel bir dissektör, protokol alanlarını ayrıştırır, görüntüleme filtresi yeteneklerini tanımlar ve Wireshark içinde detaylı görselleştirmeye olanak tanır.[27] Tam bir spesifikasyon olmasa bile, gözlemlenen kalıplara (örneğin, belirli bayt dizileri, uzunluk alanları) dayanarak bilinmeyen protokolleri tanımlamak için sezgisel dissektörler geliştirilebilir.[27]

Yayıncı Avı için Pratik Çıkarımlar: Bu, projenin otomasyon aşamasını mümkün kılmakta, hızlı, tekrarlanabilir ve ölçeklenebilir IP tespiti ve filtrelemesi sağlamaktadır. Özel dissektörler, akış platformlarının tescilli yönlerini tersine mühendislik yapmak için kritik öneme sahiptir ve genel protokol çözücülerin sunduğundan daha ayrıntılı bilgiler sunmaktadır.

Wireshark güçlü bir manuel araç olsa da [22], "Yayıncı Avı Projesi" açıkça otomasyonu hedeflemektedir. PyShark ve Scapy [24], Wireshark'ın yeteneklerine (TShark) Pythonik bir arayüz sağlamaktadır. Bu durum, Python'ı paket yakalama, filtreleme, analiz ve raporlamayı birbirine bağlayan kritik bir *orkestrasyon katmanı* olarak konumlandırmaktadır. "Büyük miktarda ağ verisini verimli bir şekilde işleme" ve "belirli tehditlere göre uyarlanmış özel, yeniden kullanılabilir avcılık betikleri oluşturma" yeteneği [24], bu otomasyonun doğrudan bir sonucudur. Bu, ağ adli bilişimi ve analizinin geleceğinin, verinin hacmini ve karmaşıklığını yönetmek için giderek artan bir şekilde betikleme ve otomasyona dayanacağını göstermektedir. Manuel analiz, otomatik ön işlem ve filtreleme ilgi alanlarını belirledikten sonra derinlemesine bir adım haline gelmektedir.

Proje, platformların altyapısı ve protokolleri de dahil olmak üzere nasıl çalıştığını anlamayı amaçlamaktadır. Birçok akış platformu tescilli öğeler kullanmaktadır. Şifreleme yük incelemesini sınırlasa da, özel dissektörler [27], şifre çözme mümkünse (örneğin, kontrollü şifre çözme için SSL anahtarları aracılığıyla [1]) veya belirli kısımlar şifrelenmemişse, bu tescilli protokolleri *programatik olarak anlamanın* tek yoludur. Özel alanlar ve filtreler tanımlama yeteneği [27], tersine mühendislik için doğrudan bir *kolaylaştırıcı*dır. Bu, şifreli tüneller içinde bile özel protokollerin artan kullanımının, özel tersine mühendislik becerileri ve araçları gerektirdiğini göstermektedir. Sezgisel

dissektörlerin geliştirilmesi [27], tam spesifikasyonlar mevcut olmadığında ilk analiz için pratik bir yaklaşım olduğunu göstermektedir.

3. Uygulama ve Kullanıcı Haritalaması için Davranışsal Profilleme ve Akış Tabanlı Analiz

Şifreleme paket içeriğini gizlediğinden, ağ akışlarının davranışsal özelliklerini analiz etmek büyük önem taşımaktadır. Bu, oturum süresi, veri hacmi, bağlantı modelleri ve etkileşim dizilerini içermektedir.[20]

Akış Tabanlı İzleme (NetFlow, sFlow, IPFIX):

- **Üst Düzey Görünürlük:** Akış tabanlı izleme, ağ trafiğini paket akışlarını yakalayıp inceleyerek analiz etmekte, trafik modelleri, uygulama kullanımı ve genel ağ davranışı hakkında üst düzey bilgiler sağlamaktadır.[18] Hibrit, çoklu bulut ve IoT odaklı ağları yönetmek için kritik öneme sahiptir.[18]
- **Gerçek Zamanlı Anomali Tespiti:** Akış verileri, özellikle YZ/ML ile geliştirildiğinde, anormallikleri anında tespit edebilmekte, şüpheli modelleri belirleyebilmekte ve bant genişliği yönetimini optimize edebilmektedir.[18]

Paket Yakalama ile Entegrasyon: Akış verileri üst düzey bilgiler sağlarken, bunu Wireshark gibi detaylı paket yakalama araçlarıyla birleştirmek, belirli ağ sorunlarını teşhis etmek ve daha derinlemesine bilgi edinmek için en iyi uygulamadır.[18] Bu, akış verilerinin makro düzeyde "ne" olduğunu, paket verilerinin ise mikro düzeyde "nasıl" olduğunu açıkladığı çok katmanlı bir yaklaşıma olanak tanımaktadır.

Kullanıcı ve Uygulama Haritalaması için Davranışsal Analiz:

- **IP Adreslerinin Ötesi:** Geleneksel ağ analizi genellikle IP adreslerine odaklanmaktadır, ancak bunlar kullanıcı kimlikleriyle eş anlamlı değildir.[20] Yeni yaklaşımlar, şifrelenmiş ağ trafiğinden kullanıcıları ve uygulama kullanımlarını, paketlerin gerçek içeriğine erişmeye gerek kalmadan meta verileri, paket boyutlarını, zamanlamayı ve uç noktaları titizlikle inceleyerek belirlemeyi amaçlamaktadır.[20]
- **YZ Odaklı Davranışsal Analiz:** Doğal Dil İşleme (NLP) ve Makine Öğrenimi dahil olmak üzere YZ teknikleri, şüpheli davranışları, duygu eğilimlerini veya suç niyetini gösteren kalıpları analiz etmek için toplanan verileri kullanmaktadır.[29] Esas olarak sosyal medya için tartışılsa da, aktiviteden kalıpları belirleme temel prensipleri ağ trafiğine uyarlanabilir.

Yayıncı Avı için Pratik Çıkarımlar: Bu teknik, farklı akış platformlarının tipik ağ davranışlarına dayanarak "parmak izini" karakterize etmeye yardımcı olmaktadır, içerik

şifreli olsa bile. Ayrıca, belirli bir kullanıcının bir platformla olağandışı bir şekilde etkileşimde bulunup bulunmadığını belirlemeye de yardımcı olabilir, bu da potansiyel bir tehdidi veya benzersiz bir aktiviteyi gösterebilir.

Şifreli trafiğin zorluğu [2], içerik incelemesinden uzaklaşmayı zorunlu kılmaktadır. [20] numaralı kaynak, yeni N-FAT yaklaşımlarının, kullanıcıları ve uygulama kullanımlarını *şifreli* trafikten "meta verileri, paket boyutlarını, zamanlamayı ve uç noktaları" inceleyerek belirlediğini açıkça belirtmektedir. Bu durum, şifrelemenin, aktiviteyi açık verilerden ziyade gözlemlenebilir *davranışsal modellerden* çıkarmak için bir *neden* oluşturduğunu göstermektedir. Bu, diğer adli bilişim bağlamlarında YZ'nin "duygu ve davranışsal analiz" için kullanılmasıyla daha da desteklenmektedir.[29] Ağ adli bilişimi, davranış bilimleri ve veri analitiğinden metodolojileri birleştirmek için evrimleşmektedir. Bu durum, son derece şifreli ortamlarda bile ağ aktivitesinin "kim" ve "nasıl" olduğunu anlamak için kritik öneme sahiptir.

4. Gelişmiş CDN Altyapı Haritalaması ve Tanımlaması

DNS Çözümlemesi Yoluyla Doğru CDN Haritalaması:

- **DNS Yönlendirme:** CDN'ler, kullanıcı isteklerini en uygun uç sunucuya yönlendirmek için öncelikle DNS yönlendirme yöntemlerini (CDN alan adlarına eşlenen CNAME kayıtları veya doğrudan A/AAAA kayıtları) kullanmaktadır.[7] Bu DNS kayıtlarının analizi, CDN kullanımını belirlemede birincil adımdır.
- **Anycast DNS ve EDNS-Client-Subnet (ECS):** CDN'ler, sorguları en yakın kullanılabilir sunucuya yönlendirmek için Anycast DNS'i kullanmakta [7], bu da gecikmeyi azaltmaktadır.[8] EDNS-Client-Subnet (ECS) DNS uzantısı, genel DNS çözümleyicilerinin sorgulara istemci alt ağ bilgilerini dahil ederek yüksek kaliteli CDN eşlemeleri sağlamasına yardımcı olmakta, böylece CDN'lerin coğrafi olarak optimize edilmiş yanıtlar döndürmesine olanak tanımaktadır.[30] DNS sorgu yanıtlarının, gecikme ve döndürülen IP adresleri dahil olmak üzere analiz edilmesi, CDN eşleme stratejilerini ortaya çıkarabilir.[30]
- **Genel DNS Çözümleyici Performansı:** Farklı genel DNS çözümleyicileri (Google, Cloudflare, OpenDNS, Quad9), sorgu yanıt süreleri ve CDN istemciden uç sunucuya eşlemelerinin kalitesi açısından farklılık göstermektedir.[30] Cloudflare-R, genel çözümleyiciler arasında genellikle daha düşük gecikme süreleri göstermektedir.[30]

Otonom Sistem Numaralarından (ASN'ler) ve IP Coğrafi Konumlandırmadan Yararlanma:

- **ASN Arama:** Tek bir yönlendirme politikasına sahip büyük bir ağ veya ağ grubu olan her Otonom Sisteme (AS) benzersiz bir ASN atanmaktadır.[31] Tanımlanan IP

adresleri için ASN aramaları yapmak, sahibi olan şirketi veya kuruluşu (örneğin, bir İSS, büyük bir teknoloji şirketi veya bir CDN sağlayıcısı) ve ağ kimliğini belirlemeye yardımcı olmaktadır.[31] Bu, akış altyapısının ağ sınırlarını ve bağlantılarını anlamak için kritik öneme sahiptir.
- **IP Coğrafi Konumlandırma:** Fastly'nin Digital Element verileriyle entegrasyonu gibi IP tabanlı coğrafi konumlandırma hizmetleri, bir IP adresinin yaklaşık fiziksel konumunu belirlemektedir.[9] Doğruluk değişebilir (örneğin, işletmeler yerel kullanıcılardan daha doğru, mobil cihazlar daha az hassas), ancak CDN uç sunucularının genel bölgesini ve ülkesini belirlemek için faydalıdır.[10]
- **Veri Korelasyonu:** DNS çözümleme sonuçları, ASN bilgileri ve IP coğrafi konumlandırma verilerinin birleştirilmesi, akış platformu altyapısının dağıtık doğasının kapsamlı bir şekilde anlaşılmasını sağlamakta, içeriğin en yakın uç sunucudan sunulup sunulmadığını doğrulamakta ve eşleme anormalliklerini belirlemektedir.[7]

Yayıncı Avı için Pratik Çıkarımlar: Bu teknik, akış platformlarının oldukça dağıtık ve dinamik altyapısını doğru bir şekilde haritalama metodolojisini sağlamakta, sadece bir IP'yi değil, hangi CDN'ye ait olduğunu, coğrafi konumunu ve kullanıcıların ona nasıl yönlendirildiğini belirlemektedir. Bu, bir platformun ağ varlığının tam kapsamını anlamak için esastır.

[7] numaralı kaynaklar, DNS'in kullanıcıların "kaynak içerik sunucularından CDN'lere yönlendirildiği" [30] ve CDN'lerin "DNS yönlendirme yöntemlerini" [7] kullandığı mekanizma olduğunu sürekli olarak vurgulamaktadır. Bu durum, DNS çözümlemesini CDN haritalaması için ilk ve en kritik istihbarat toplama noktası olarak belirlemektedir. Genel DNS çözümleyicilerinin performansı ve kalitesi [30], bu haritalamanın doğruluğunu doğrudan *etkilemekte*, çözümleyici seçimi ile haritalama etkinliği arasında nedensel bir bağlantı oluşturmaktadır. Ağ analistleri için, gelişmiş DNS sorgu tekniklerinde (ECS anlayışı dahil) ustalaşmak ve en uygun çözümleyicileri seçmek, basit ping veya traceroute'un ötesine geçerek doğru altyapı keşfi için temel bir beceri haline gelmektedir.

DNS bir isteğin *nereye* yönlendirildiğini söylerken, ASN araması [31] ağ bloğunun *kime ait olduğunu*, IP coğrafi konumlandırma ise [9] *yaklaşık fiziksel konumunu* belirtmektedir. Bu üç veri noktası (DNS, ASN, GeoIP) birbirini *tamamlamaktadır*. Örneğin, bir DNS aramasından elde edilen bir IP bir CDN ucu olabilir, ancak ASN araması bunun büyük bir CDN sağlayıcısı (örneğin, Akamai, Cloudflare) olduğunu doğrular ve coğrafi konumlandırma onu belirli bir şehre yerleştirir. Bu çok katmanlı yaklaşım, dağıtılmış akış altyapısının daha sağlam ve doğru bir şekilde tanımlanmasını *sağlar*. 2025 yılında kapsamlı ağ haritalaması, bütünsel bir resim oluşturmak için birden fazla kaynaktan

gelen verileri ilişkilendirmeyi gerektirmektedir. Bu, özellikle ağ etkinliğini belirli kuruluşlara veya hizmetlere atfetmek için önemlidir.

Aşağıdaki tablo, CDN altyapısının belirlenmesi için kullanılan metodolojileri özetlemektedir.

Tablo 2: CDN Altyapı Tanımlama Metodolojileri

Metodoloji	Temel Göstergeler/Veri Noktaları	Araçlar/Teknikler	Yayıncı Avı Projesi İçin Değeri	Sınırlamalar
DNS CNAME/A/AAAA Kayıt Analizi	_edge.net gibi CNAME'ler, CDN'ye işaret eden A/AAAA kayıtları	dig, nslookup, Python DNS kütüphaneleri (örn. dnspython)	Platformların CDN kullanımını ve ana alan adlarını belirlemek için ilk adım. Hangi CDN sağlayıcısının kullanıldığını gösterir.	Statik DNS kayıtları, dinamik yönlendirmeyi tam olarak yansıtmayabilir. Bazı CDN'ler doğrudan IP'ler kullanabilir.
Anycast DNS Sorgu Analizi	ECS (EDNS-Client-Subnet) yanıtları, farklı coğrafi konumlardan sorgulandığında dönen farklı IP'ler	Özel DNS sorgu araçları, farklı coğrafi konumlardan test proxy'leri	Kullanıcıların en yakın uç sunucuya nasıl yönlendirildiğini anlamak. Coğrafi eşleme kalitesini değerlendirmek.	Karmaşık yapılandırma gerektirebilir. Tüm genel çözümleyiciler ECS'yi desteklemeyebilir.
ASN (Otonom Sistem Numarası) Arama	AS numaraları (örn. AS15169), AS adı (örn. Google LLC)	ASN arama araçları (örn. dnschecker.org, hackertarget.com), whois	Belirli IP adres bloklarının sahibi olan kuruluşu (CDN sağlayıcısı, İSS) belirlemek. Ağ sınırlarını ve ilişkilerini anlamak.	IP'nin fiziksel konumu ile ASN'nin kayıtlı konumu uyuşmayabilir. Büyük kuruluşların ASN'leri geniş alanlara yayılabilir.

IP Coğrafi Konumlandırma	Ülke kodu, şehir, enlem, boylam, bağlantı hızı	GeoIP veritabanları (örn. MaxMind), Fastly gibi CDN'lerin dahili coğrafi konumlandırma hizmetleri [9]	CDN uç sunucularının yaklaşık fiziksel konumunu belirlemek. Bölgesel içerik dağıtımını doğrulamak.	Doğruluk değişebilir (işletmeler daha doğru, mobil cihazlar daha az). Bazı IP'ler için konum verisi eksik olabilir.[10]

5. Akış Protokollerinin Hedefli Tersine Mühendisliği

Birçok çevrimiçi akış ve iletişim platformu, özellikle benzersiz özelliklere veya performans optimizasyonlarına sahip olanlar, tescilli veya belgelenmemiş protokoller veya standart protokollerin özel uygulamalarını kullanabilir. Geleneksel Wireshark dissektörleri bunları tam olarak çözemeyebilir, bu da tersine mühendisliği gerekli kılmaktadır.

Protokol Çıkarımı için Metodolojiler:

- **Veri Odaklı Konkolik Yürütme (ICEPRE prensipleri):** ICEPRE, özellikle Endüstriyel Kontrol Sistemleri (ICS) protokolleri için tasarlanmış olsa da, protokol sözdizimini, anlambilimini ve durum makinelerini ağ izlerinden ve statik analizden çıkarmak için kullandığı temel metodoloji [33] uyarlanabilir. Bu, belirli girdi mesajları için program ayrıştırma süreçlerini statik olarak izlemeyi ve bir protokol ayrıştırıcısının farklı alanları nasıl işlediğini analiz ederek alan sınırı çıkarım stratejilerini kullanmayı içerir.[33]
- **Sezgisel Dissector Geliştirme:** İlk analiz için, Wireshark'ın sezgisel dissektörleri, paket başlıklarında veya yüklerinde gözlemlenen kalıplara dayanarak geliştirilebilir.[27] Bu, sihirli baytları, belirli tip alanlarını, bayrakları veya uzunluk alanlarını tanımlamayı içerir.[27] Bu, tam bir spesifikasyon olmasa bile kısmi ayrıştırma ve tanımlama sağlar.
- **Desen Tanıma ve İstatistiksel Analiz:** Paket uzunluğu dağılımları, zamanlama modelleri ve bayt frekanslarının analizi, bilinmeyen bir protokolün yapısal öğelerini ortaya çıkarabilir. Wireshark'ın istatistiksel araçları [23], bu konuda yardımcı olabilir, ortak paket boyutlarını, akış özelliklerini ve protokol hiyerarşilerini belirleyebilir.
- **Kontrollü Ortam Analizi:** Platformla sistematik olarak etkileşimde bulunurken kontrollü bir ortamdan (örneğin, akış istemcisini çalıştıran bir sanal makine) trafik yakalamak, istek/yanıt yapılarını ve veri kodlamasını belirlemeye yardımcı olan tahmin edilebilir trafik modelleri üretebilir.

Özel Dissector Geliştirmeyi Etkinleştirme: Tersine mühendislikten elde edilen bilgiler doğrudan özel Wireshark dissektörlerinin (Lua veya C) geliştirilmesine

beslenmektedir [27], bu da Wireshark içinde tescilli protokolün otomatik ve detaylı analizine olanak tanımaktadır.

Yayıncı Avı için Pratik Çıkarımlar: Bu eğilim, belirli akış platformlarının ağ katmanında nasıl çalıştığına dair derinlemesine bilgi edinmek için kritik öneme sahiptir, özellikle protokollerini kasıtlı olarak gizleyenler için. Projenin genel trafik tanımlamasının ötesine geçerek bir platformun iletişiminin nüanslarını anlamasına olanak tanır, bu da adli analiz ve rekabetçi istihbarat için hayati öneme sahiptir.

Kullanıcı sorgusu açıkça "tersine mühendislik"i bir proje hedefi olarak belirtmektedir. Bazı akış protokollerinin tescilli doğası ("Yayıncı Avı" ihtiyacı ve özel uygulamaların genel eğilimi tarafından ima edilmektedir) ve şifreli trafik analizinin sınırlamaları [2] göz önüne alındığında, tersine mühendislik [33], bu platformların altında yatan mekanizmaları anlamanın *kritik bir yolu* haline gelmektedir. Bu, satıcıların spesifikasyonları yayınlamamasının doğrudan bir sonucudur. "Yayıncı Avı Projesi", tersine mühendislik tekniklerinde uzmanlaşmaya yatırım yapmalı veya bu konuda uzmanlık edinmelidir, çünkü hazır araçlar ve standart protokol bilgisi, tüm hedef platformların kapsamlı analizi için yetersiz kalacaktır. Bu aynı zamanda, protokoller geliştikçe sürekli bir çaba gerektirdiği anlamına gelmektedir.

6. Bulut Güvenliği Adli Bilişimi ve Dağıtık Veri Analizi

Bulut bilişimin artan benimsenmesi, 2025 yılına kadar yeni üretilen verilerin %60'ından fazlasının bulutta bulunacağı anlamına gelmektedir.[15] Bu dağıtık yapı, dijital adli bilişim için, coğrafi olarak dağınık sunucular arasında veri parçalanması ve yargı yetkisi karmaşıklıkları dahil olmak üzere önemli zorluklar ortaya koymaktadır.[15]

Adli Bilişim Araçlarının Uyarlanması: Geleneksel adli bilişim araçları, tipik olarak şirket içi sistemler için tasarlanmış olup, dinamik bulut altyapılarına genellikle uygulanamamaktadır.[34] Bu nedenle, bulut güvenliği adli bilişimi bir zorunluluk haline gelmektedir.[34]

Bulut Trafik Analizi Stratejileri:

- **Bulut Yerel Akış İzleme:** Modern akış tabanlı izleme çözümleri, buluttan buluta trafik izleme, bölgeler arası veri akışı görünürlüğü ve bulut yerel güvenlik araçlarıyla entegrasyon sunmaktadır.[18] Bu, dağıtık ağ etkinliğine gerekli görünürlüğü sağlamaktadır.
- **Çoklu Akış Toplama Noktaları:** Veri merkezleri, bulut ortamları, şube ofisleri ve uç bilişim konumları boyunca akış toplayıcıların dağıtılması, kapsamlı görünürlük için esastır.[18]

- **Akış ve Paket Verilerinin Birleştirilmesi:** Akış verileri üst düzey bilgiler sağlarken, bunu Wireshark gibi paket yakalama araçlarıyla birleştirmek, bulut ortamlarındaki belirli ağ sorunlarını teşhis etmek için kritik öneme sahiptir.[18]
- **Veri Parçalanmasını Ele Alma:** Araştırmacılar, veri toplama süresini önemli ölçüde uzatabilen platformlar arası, yargı yetkisi arası veri izleme ve analizine uyum sağlamalıdır.[15]

Yayıncı Avı için Pratik Çıkarımlar: Büyük akış platformlarının bulut altyapısına ve CDN'lere (temelde dağıtık bulut uç hizmetleridir) yoğun bir şekilde güvendiği göz önüne alındığında, proje bulut farkındalıklı adli metodolojileri benimsemelidir. Bu, sanallaştırılmış veya kapsayıcılı ortamlardan trafik toplama ve analiz etme ile farklı bulut bölgeleri veya sağlayıcılar arasındaki verileri ilişkilendirme yeteneğini anlamak anlamına gelmektedir.

[15] ve [34] numaralı kaynaklar, bulut bilişimin yaygın olmasına rağmen, "dağıtık depolamada dijital adli bilişim zorlukları" sunduğunu ve "geleneksel adli bilişim araçlarının... bu dinamik altyapılara uygulanamadığını" vurgulamaktadır. Bu durum, yalnızca geleneksel şirket içi ağ yakalamasına güvenirse "Yayıncı Avı Projesi" için *potansiyel bir kör nokta* oluşturmaktadır. Çözüm, bulut yerel izleme ve dağıtık akış toplama [18] ile bu zorluğu doğrudan *ele almaktadır*. Ağ adli bilişimi artık kurumsal çevreyle sınırlı değildir. Kamu ve özel bulut ortamlarının karmaşık, dinamik ve genellikle opak alanına yayılmalı, yeni araçlar, teknikler ve veri egemenliği için yasal hususlar gerektirmelidir.

7. YZ Odaklı Bilgilerle Proaktif Tehdit Avcılığı

YZ destekli siber güvenlik, reaktif tespitten proaktif tehdit modellemesi ve müdahaleye doğru kaymaktadır.[34] Bu, YZ'yi yalnızca bilinen tehditleri belirlemek için değil, aynı zamanda saldırıları tahmin etmek ve önlemek için de kullanmayı içermektedir.

Sofistike Tehditlerin Belirlenmesi:

- **Normal Trafikle Harmanlama:** Gelişmiş Kalıcı Tehditler (APT'ler), normal ağ trafiğiyle harmanlanacak şekilde tasarlanmıştır ve bu da tespit edilmelerini son derece zorlaştırmaktadır.[16] YZ odaklı anomali tespiti, bu ince sapmaları belirlemek için kritik öneme sahiptir.[19]
- **QUIC Üzerinden Komuta ve Kontrol (C2):** QUIC'in şifrelemesi ve doğal özellikleri (örneğin, bağlantı geçişi, dinamik IP değişiklikleri), QUIC tabanlı veri sızdırma ve C2 kanallarının tespitini zorlaştırmaktadır.[2] Ancak, QUIC el sıkışması, ana paket türleri ve Bağlantı Kimliklerinin RITA, Wireshark, Zeek ve özel Python uygulamaları gibi araçlar kullanılarak analizi, tespit fırsatlarını belirleyebilir.[35] Değişen gecikme

ayarlarıyla bile kalıcı QUIC bağlantıları, yüksek önem derecesine sahip uzun bağlantılar olarak işaretlenebilir.[35]
- **İnsan Dışı Kimlikler (NHI):** Makine kimliklerinin yaygınlaşması, saldırılar için kullanılabilecek yeni bir zorluk teşkil etmektedir.[17] YZ, karmaşık bulut ortamlarında NHI'leri yönetmeye ve güvence altına almaya yardımcı olabilir.[17]

YZ Odaklı Anomali Tespiti: YZ tabanlı akış analizi araçları, manuel araştırma çabalarını azaltmakta, davranışsal anormallikleri daha hızlı belirlemekte ve olay müdahale sürelerini iyileştirmektedir.[18] Bu, nadir olaylar için Isolation Forest, grup davranışı için K-Means Kümeleme ve karmaşık desenler için Autoencoders gibi teknikleri kullanmayı içermektedir.[19]

Yayıncı Avı için Pratik Çıkarımlar: Proje, meşru akış altyapısını belirlemeye odaklanırken, tehdit avcılığı tekniklerini anlamak, iyi huylu platform trafiğini taklit edebilecek kötü niyetli etkinliklerden ayırmak için kritik öneme sahiptir. Örneğin, QUIC üzerinden C2'yi belirlemek, meşru akış bağlantılarını gizli kanallardan veya tehlikeye atılmış uç noktalardan ayırmaya yardımcı olabilir.

[17] numaralı kaynaklar, YZ'nin siber güvenlik için güçlü bir araç olduğunu, proaktif tehdit avcılığı ve anomali tespiti sağladığını vurgulamaktadır. Ancak[17] ve [36] numaralı kaynaklar, tehdit aktörlerinin YZ'yi kötü niyetli amaçlar (sosyal mühendislik, kimlik avı, kötü amaçlı kod oluşturma) için kullanabileceği ve "ajan YZ" ile Büyük Dil Modellerinin (LLM) güvenlik açıklarına yol açabileceği riskleri konusunda uyarmaktadır. Bu durum, bir *çelişki* veya *ikili doğa*yı vurgulamaktadır: YZ, ağ analizi için bir çözüm olmasının yanı sıra, ağ analizinin mücadele etmesi gereken sofistike tehditlerin yeni bir kaynağıdır. "Yayıncı Avı Projesi", kendi analizi için YZ'yi benimsemekle kalmamalı, aynı zamanda düşmanların YZ'yi faaliyetlerini gizlemek veya meşru akış trafiğini taklit etmek için nasıl kullanabileceği konusunda da farkında olmalı, bu da daha nüanslı ve uyarlanabilir bir tespit stratejisi gerektirmektedir.

8. Ağ Analizinin Dijital Kimlik Maruziyeti İstihbaratıyla Entegrasyonu

Saldırganlar, kullanıcı adları, parolalar, kişisel olarak tanımlanabilir bilgiler (PII), cihaz ayrıntıları ve oturum çerezleri dahil olmak üzere karanlık ağdaki geniş kullanıcı ayak izlerini kullanmaktadır.[37] Bu "kimlik savaşı" tırmanmakta olup, SpyCloud'un yeniden ele geçirilen verilerde %22'lik bir büyüme bildirmesiyle bu durum daha da belirginleşmektedir.[37]

Bütünsel Kimlik Merkezli Model: Bütünsel bir model, ihlal, kötü amaçlı yazılım, kombinasyon listesi ve kimlik avı maruziyetlerini, tek bir bireye ait çevrimiçi kişilikleri boyunca bir araya getirmektedir.[37] Bu, suçluların kullanabileceği çalınan verilerin

kapsamını vurgulayan kapsamlı bir kimlik maruziyeti resmi sunmaktadır.[37]

Ağ Trafiğini Kimlik Verileriyle İlişkilendirme:

- **İçeriden Tehditler ve Kimlik Bilgisi Sızıntıları:** Ağ analizi, şüpheli iletişim modellerini veya veri sızdırmayı tespit edebilir.[22] Bu, maruz kalmış kimlik bilgileri [16] veya oturum çerezleri [37] hakkındaki istihbaratla ilişkilendirildiğinde, tehlikeye atılmış hesapları veya içeriden tehditleri gösterebilir.
- **Kullanıcı Tanımlaması için Davranışsal Profilleme:** Ağ trafiği analizi tipik olarak IP'lere odaklanırken, yeni yaklaşımlar, meta verileri, paket boyutlarını, zamanlamayı ve uç noktaları inceleyerek şifreli trafikten kullanıcıları ve uygulama kullanımlarını belirlemeyi amaçlamaktadır.[20] Bu dahili ağ davranışı daha sonra harici kimlik maruziyeti verileriyle çapraz referans edilebilir.
- **İnsan Dışı Kimlikler (NHI):** Makine kimliklerinin yaygınlaşması [17], ağ trafiğinin otomatik süreçlerden kaynaklanabileceği anlamına gelmektedir. Bunu kimlik maruziyeti istihbaratıyla ilişkilendirmek, tehlikeye atılmış NHI'leri belirlemeye yardımcı olabilir.

Yayıncı Avı için Pratik Çıkarımlar: Bu eğilim, projenin sadece *platformu* belirlemesinin ötesine geçerek, platformla ilgili *potansiyel tehlikeleri* de belirlemesini sağlamaktadır. Örneğin, belirli bir kullanıcının akış etkinliği olağandışı modeller gösteriyorsa ve kimlik bilgileri bir ihlal veritabanında bulunuyorsa, bu, kötü niyetli amaçlar için kullanılan tehlikeye atılmış bir hesabı gösterebilir. Bu, "Yayıncı Avı"na kritik bir güvenlik boyutu eklemektedir.

[37] ve [16] numaralı kaynaklar, dijital kimlik maruziyetinin (çalınan kimlik bilgileri, çerezler, PII) muazzam ölçeğini ve saldırganların yetkisiz erişim için bunlardan nasıl yararlandığını vurgulamaktadır. Aynı zamanda, ağ analizi "olağandışı ağ etkinliğini" veya "şüpheli veri erişimini" tespit edebilir.[19] Mantıksal nedensel bağlantı, olağandışı ağ trafik modellerinin, bilinen kimlik maruziyetleriyle ilişkilendirildiğinde, akış platformları bağlamında tehlikeye atılmış bir kullanıcı hesabının veya içeriden tehdidin güçlü bir göstergesi olarak hizmet edebileceğidir. Ağ adli bilişimi, tamamen teknik analizden daha geniş tehdit istihbaratı ve kimlik yönetimiyle entegrasyona doğru ilerlemekte, daha bütünsel ve proaktif bir güvenlik duruşu sağlamaktadır. Bu, ağ güvenliği ekipleri ile kimlik ve erişim yönetimi ekipleri arasında işbirliği gerektirmektedir.

9. Kuantum Dirençli Kriptografi Farkındalığı ve Gelecekteki Analiz Üzerindeki Etkisi

Kuantum bilişim pratik olgunluğa ulaştığında, günümüzün asimetrik şifrelemesi için önemli bir tehdit oluşturacak ve simetrik şifrelemeyi zayıflatacaktır.[34] Bu durum,

halihazırda imzalanmış belgeleri ve gelecekteki iletişimleri tehlikeye atabilir.

Kripto-Çeviklik: Kuantum çağı, kuruluşların yeni, kuantum dirençli kriptografik algoritmalara hızla geçiş yapmaya hazır olmaları anlamına gelen "kripto-çeviklik"i gerektirmektedir.[34]

Ağ Analizi için Çıkarımlar:

- **Gelecekteki Şifreleme Zorlukları:** 2025 için acil bir endişe olmasa da, uzun vadeli çıkarım, yeni kuantum dirençli algoritmaların benimsenmesiyle ağ trafiği analizi için bir başka karmaşıklık katmanı getireceğidir. Bu yeni algoritmalar, farklı el sıkışma özelliklerine, anahtar değişim mekanizmalarına veya yeni analiz teknikleri gerektiren trafik modellerine sahip olabilir.
- **Geriye Dönük Uyumluluk Sorunları:** Geçiş dönemi, geleneksel ve kuantum dirençli kriptografinin bir karışımını içerebilir, bu da analizi karmaşıklaştırır ve araçların çeşitli şifreleme şemalarına uyum sağlamasını gerektirir.
- **Veri Şifre Çözme (Kuantum Sonrası):** Mevcut şifreleme kuantum bilgisayarlar tarafından kırılabilir hale gelirse, teorik olarak geçmiş trafik yakalamalarının şifresini çözme olasılıklarını açabilir, ancak bu aynı zamanda kötü niyetli aktörler benzer yetenekler edinirse önemli yeni güvenlik riskleri de yaratır.

Yayıncı Avı için Pratik Çıkarımlar: 2025 için bu, acil bir teknikten ziyade bir farkındalık eğilimidir. Ancak proje, gelecekte ağ trafiğini daha da gizleyebilecek veya yeni analiz zorlukları yaratabilecek kriptografik standartlardaki gelecekteki değişiklikleri öngörerek modülerlik ve uyarlanabilirlik göz önünde bulundurularak tasarlanmalıdır.

[34] numaralı kaynak, "Kuantum çağı kripto-çeviklik gerektiriyor" ve kuantum bilişimin mevcut şifrelemeyi kırma tehdidini açıkça vurgulamaktadır. Bu, 2025 için doğrudan bir teknik olmasa da, ağ trafiği analizinde daha fazla karmaşıklığa *neden olacak* önemli bir *gelecek zorluğunu* temsil etmektedir. TLS 1.3 ve QUIC ile ilgili mevcut zorluklar [2], kuantum dirençli protokoller gerekli gözlemlenebilirlik düzeyini göz önünde bulundurularak tasarlanmazsa daha da opak bir gelecek ağ ortamının habercisidir. Ağ güvenliği ve adli bilişim araştırmaları, trafik analizi üzerindeki etkilerini anlamak için kuantum sonrası kriptografiyle proaktif olarak ilgilenmeli, potansiyel olarak gelecekteki protokollerin tasarımını güvenlik ile savunma için gerekli gözlemlenebilirlik arasında bir denge sağlamak üzere etkilemelidir.

10. Ağ Adli Bilişiminde Etik ve Yasal Uyumluluk

Etik ve yasal hususlar siber güvenlikte çok önemlidir; sorumlu karar vermeye rehberlik eder, güvenlik ihtiyaçlarını gizlilik haklarıyla dengelemeyi sağlar ve kamu güvenini

sürdürür.[38]

Temel Etik İlkeler:

- **Kişilere Saygı:** Kişisel verileri toplamadan önce bilgilendirilmiş onay almayı, gizliliği ve mahremiyeti korumayı ve adil muameleyi sağlamayı gerektirir.[38]
- **Yararlılık ve Zarar Vermeme:** Başkalarına fayda sağlayan eylemlerde bulunmak ve zarardan veya gereksiz risklerden kaçınmak.[38]
- **Adalet, Dürüstlük, Hesap Verebilirlik:** Adil muameleyi, şeffaflığı ve eylemlerden sorumluluğu sağlamak.[38]

Veri Gizliliği Düzenlemelerinde (GDPR, CCPA) Gezinme:

- **Uygulanabilirlik:** Hem GDPR (Genel Veri Koruma Yönetmeliği) hem de CCPA (California Tüketici Gizliliği Yasası), kişisel verileri işleyen kuruluşlar için katı gereksinimler getirmektedir.[39] CCPA, yıllık brüt geliri 25 milyon doları aşan veya 50.000'den fazla tüketici/cihazın kişisel verilerini ticari amaçlarla işleyen veya yıllık gelirinin %50'sinden fazlasını kişisel bilgi satışından elde eden işletmeler için geçerlidir.[40]
- **Uyumluluk Adımları:**
  - **Veri Haritalaması:** Hangi kişisel verilerin toplandığını, nasıl işlendiğini, saklandığını ve paylaşıldığını anlamak.[39]
  - **Gizlilik Politikaları:** Tüketicileri veri uygulamaları hakkında şeffaf bir şekilde bilgilendirmek.[39]
  - **Vazgeçme Mekanizmaları:** Tüketicilere veri satışından vazgeçmeleri için (CCPA) açık yollar sağlamak.[39]
  - **Sağlam Veri Güvenliği:** Şifreleme (örneğin, ağ trafiği için TLS 1.3 [16]), güvenlik duvarları, erişim kontrolleri ve düzenli güvenlik denetimleri uygulamak.[39]
  - **Çalışan Eğitimi:** Personelin uyumluluk gereksinimlerini anlamasını sağlamak.[40]
  - **Olay Müdahale Planı:** Veri ihlallerine karşı hazırlıklı olmak.[40]
- **Cezalar:** Uygunsuzluk, önemli para cezalarına yol açabilir (örneğin, CCPA için ihlal başına 2.500-7.500 dolar, GDPR için ciddiyete göre önemli cezalar).[39]

Yayıncı Avı için Pratik Çıkarımlar: "Yayıncı Avı Projesi", ağ trafiğini yakalama ve analiz etmeyi içermektedir; bu da kaçınılmaz olarak kişisel verileri (IP adresleri, iletişim modelleri, şifrelenmemişse potansiyel olarak kullanıcı kimlikleri) içermektedir. Bu düzenlemelere sıkı sıkıya bağlı kalmak isteğe bağlı değildir. Bu, veri toplama için bilgilendirilmiş onay (uygulanabilirse), mümkün olduğunca verileri anonimleştirme veya takma ad kullanma, yakalanan veriler için sağlam güvenlik uygulama ve açık veri saklama ve silme politikalarına sahip olma anlamına gelmektedir.

[38] numaralı kaynaklar, etik ve yasal hususların siber güvenlikte "kritik" ve "temel" olduğunu, uyumsuzluk durumunda önemli cezalar olduğunu açıkça belirtmektedir. "Yayıncı Avı Projesi", kişisel veri olan ağ trafiğini toplamayı içermektedir. Bu durum, doğrudan bir *kısıtlama* yaratmaktadır: projenin teknik metodolojileri, veri haritalaması, onay, güvenlik ve saklama dahil olmak üzere GDPR ve CCPA gibi gizlilik düzenlemelerine uyacak şekilde *en başından itibaren tasarlanmalıdır*. Bunu yapmamak, yasal ve itibari risklere *neden olur*. Ağ analizi daha sofistike hale geldikçe ve daha fazla kişisel veri içerdiğinde, yasal ve etik çerçeveler artık sonradan düşünülen bir şey değil, herhangi bir ağ adli bilişim veya güvenlik projesinin fizibilitesini ve metodolojisini şekillendiren temel bir unsur haline gelmektedir. Bu, hukuki ve gizlilik uzmanlığını teknik becerilerle birleştiren çok disiplinli bir yaklaşım gerektirmektedir.

IV. Sonuç ve Tavsiyeler

"Yayıncı Avı Projesi"nin hedeflerine ulaşması, modern ağ ortamının karmaşık zorluklarını aşmak için ileri düzey tekniklerin ve stratejilerin benimsenmesini gerektirmektedir. Bu rapor, şifreli trafiğin yaygınlaşması, dinamik altyapılar ve otomasyon ihtiyacı gibi temel zorlukları ele alan on kritik eğilimi ortaya koymuştur. Geleneksel Derin Paket İncelemesinden (DPI) YZ/ML odaklı meta veri analizine geçiş, ölçeklenebilirlik için Python betiklemenin gerekliliği ve altyapı haritalaması için çok kaynaklı istihbaratın önemi, projenin başarısı için merkezi unsurlardır.

Eyleme Dönük Tavsiyeler:

1. **YZ/ML Yeteneklerine Yatırım Yapın:** Şifreli trafik sınıflandırması ve anomali tespiti için YZ/ML uzmanlığının ve araçlarının geliştirilmesine veya edinilmesine öncelik verilmelidir. Meta verilerden özellik mühendisliğine ve model eğitimi için VisQUIC gibi veri kümelerinden yararlanmaya odaklanılmalıdır.
2. **Otomasyonu Benimseyin:** Otomatik paket yakalama, filtreleme, analiz ve raporlama için Python (PyShark, Scapy) projenin tüm aşamalarına tam olarak entegre edilmelidir. Bu, verimliliği ve tekrarlanabilirliği önemli ölçüde artıracaktır.
3. **Özel Dissector Uzmanlığı Geliştirin:** Tescilli akış protokollerini analiz etmek için tersine mühendislik ve özel Wireshark dissector geliştirme (Lua/C) becerileri geliştirilmelidir. Bu, platformların iç işleyişine dair derinlemesine bilgi sağlayacaktır.
4. **Bütünsel Altyapı Haritalaması:** Gelişmiş DNS sorguları, ASN aramaları ve IP coğrafi konumlandırmayı birleştirerek CDN ve sunucu tanımlamasına çok katmanlı bir yaklaşım uygulanmalıdır. Bu, akış altyapısının dağıtık ve dinamik doğasının kapsamlı bir şekilde anlaşılmasını sağlayacaktır.
5. **Bulut Farkındalıklı Adli Bilişim:** Bulut tabanlı altyapıyı hesaba katmak için metodolojiler uyarlanmalı, bulut yerel izleme araçlarından yararlanılmalı ve veri

parçalanması sorunları ele alınmalıdır.

6. **Tehdit İstihbaratını Entegre Edin:** Potansiyel tehlikeleri ve içeriden tehditleri belirlemek için ağ analizi bulguları dijital kimlik maruziyeti istihbaratıyla ilişkilendirilmelidir. Bu, projenin güvenlik boyutunu güçlendirecektir.
7. **Proaktif Güvenlik Duruşu:** Meşru akış trafiğini onu taklit eden kötü niyetli etkinliklerden ayırmak için tehdit avcılığı prensipleri uygulanmalıdır.
8. **Etik ve Yasal Uyumluluğa Öncelik Verin:** Veri gizliliği düzenlemeleri (GDPR, CCPA), veri toplama ve depolamadan analiz ve raporlamaya kadar projenin her aşamasına dahil edilmeli, bilgilendirilmiş onay ve veri minimizasyonu sağlanmalıdır.

Geleceğe Bakış:

Şifrelemenin (örneğin, kuantum dirençli kriptografi) sürekli evrimi, analiz tekniklerinin sürekli adaptasyonunu gerektirecektir. Ağ mimarilerinin (5G, IoT, uç bilişim) artan karmaşıklığı, daha sofistike, gerçek zamanlı ve otomatik çözümlerin gerekliliğini ortaya koyacaktır. Ağ analizinin YZ, davranışsal analitik ve kimlik istihbaratıyla yakınlaşması, ağ güvenliği ve adli bilişimin geleceğini tanımlayacak, "Yayıncı Avı" gibi projeleri giderek artan bir şekilde disiplinlerarası uzmanlığa bağımlı hale getirecektir.

Alıntılanan çalışmalar

1. Exploring QUIC Dynamics: A Large-Scale Dataset for Encrypted Traffic Analysis - arXiv, erişim tarihi Haziran 5, 2025, https://arxiv.org/html/2410.03728v6
2. Exploiting QUIC's Server Preferred Address Feature to Perform Data Exfiltration Attacks - arXiv, erişim tarihi Haziran 5, 2025, https://arxiv.org/html/2505.05292v1
3. Part 1 - Passive Inspection of TLS 1.3 Within The Enterprise | Mira Security, erişim tarihi Haziran 5, 2025, https://mirasecurity.com/enterprise-passive-inspection-tls-1-3-pt1/
4. A Cryptographic Analysis of the TLS 1.3 Handshake Protocol - Cryptology ePrint Archive, erişim tarihi Haziran 5, 2025, https://eprint.iacr.org/2020/1044.pdf
5. Deep Packet Inspection: The Cybersecurity Microscope - Akitra, erişim tarihi Haziran 5, 2025, https://akitra.com/deep-packet-inspection/
6. Next-gen Content Delivery Networks and Edge Services Report - GlobeNewswire, erişim tarihi Haziran 5, 2025, https://www.globenewswire.com/news-release/2025/05/26/3088156/0/en/Next-gen-Content-Delivery-Networks-and-Edge-Services-Report-2025-High-Performance-and-Low-Latency-Revolutionizing-Content-Delivery.html
7. CDN Monitoring - Catchpoint, erişim tarihi Haziran 5, 2025, https://www.catchpoint.com/guide-to-synthetic-monitoring/cdn-monitoring
8. What is DNS and CDN ? - DEV Community, erişim tarihi Haziran 5, 2025, https://dev.to/rajrathod/what-is-dns-and-cdn--3o38
9. www.fastly.com, erişim tarihi Haziran 5, 2025, https://www.fastly.com/documentation/guides/concepts/geolocation/#:~:text=Fas

tly%20is%20able%20to%20determine,licensing%20restrictions%20on%20content%20distribution.
10. IP-based geolocation and intelligence | Fastly Documentation, erişim tarihi Haziran 5, 2025, https://www.fastly.com/documentation/guides/concepts/geolocation/
11. Enisoglu Thesis 2025 PDF-A.pdf - City Research Online, erişim tarihi Haziran 5, 2025, https://openaccess.city.ac.uk/id/eprint/34739/1/Enisoglu%20Thesis%202025%20PDF-A.pdf
12. arXiv:2502.13804v1 [cs.NI] 19 Feb 2025, erişim tarihi Haziran 5, 2025, https://www.arxiv.org/pdf/2502.13804
13. Deep Learning for Encrypted Traffic Classification and Unknown Data Detection - PMC, erişim tarihi Haziran 5, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC9570541/
14. Unlocking the Future of Deep Packet Inspection and Processing: Growth and Trends 2025-2033, erişim tarihi Haziran 5, 2025, https://www.datainsightsmarket.com/reports/deep-packet-inspection-and-processing-1977238
15. Key Trends in Digital Forensics for 2025: Technological Innovation and Core Challenges, erişim tarihi Haziran 5, 2025, https://www.salvationdata.com/knowledge/key-trends-in-digital-forensics-for-2025/
16. What Is Data Security In 2025? | Wiz, erişim tarihi Haziran 5, 2025, https://www.wiz.io/academy/data-security
17. RSAC 2025 Conference Submission Trends, erişim tarihi Haziran 5, 2025, https://www.rsaconference.com/library/blog/rsac-2025-conference-submission-trends-report
18. Flow-Based Monitoring in 2025: Enhancing Network Visibility and Security - SecureMyOrg, erişim tarihi Haziran 5, 2025, https://securemyorg.com/flow-based-monitoring-in-2025/
19. Anomaly Detection Machine Learning: How It Works in 2025 | Label Your Data, erişim tarihi Haziran 5, 2025, https://labelyourdata.com/articles/anomaly-detection-machine-learning
20. (PDF) An Identity and Interaction Based Network Forensic Analysis - ResearchGate, erişim tarihi Haziran 5, 2025, https://www.researchgate.net/publication/390142456_An_Identity_and_Interaction_Based_Network_Forensic_Analysis
21. Network Anomaly Detection: A Comprehensive Guide - Kentik, erişim tarihi Haziran 5, 2025, https://www.kentik.com/kentipedia/network-anomaly-detection/
22. Network Analysis with Wireshark on Kali Linux - DataFlair, erişim tarihi Haziran 5, 2025, https://data-flair.training/blogs/network-analysis-with-wireshark-on-kali-linux/
23. Using statistical tools in Wireshark for packet analysis [Tutorial] - Packt, erişim tarihi Haziran 5, 2025, https://www.packtpub.com/en-us/learning/how-to-tutorials/statistical-tools-in-wi

reshark-for-packet-analysis
24. Threat Hunting with Pyshark: Using Open Source Python Libraries to Automate Threat Hunting - Insane Cyber, erişim tarihi Haziran 5, 2025, https://insanecyber.com/threat-hunting-with-pyshark/
25. Analyzing and Monitoring Network Traffic Using Python and Wireshark | IJSREM Journal, erişim tarihi Haziran 5, 2025, https://ijsrem.com/download/network-traffic-tracer-analyzing-and-monitoring-network-traffic-using-python-and-wireshark/
26. shubham-s-pandey/WiresharkMCP: Wireshark Packet Analyzer with MCP Integration This project integrates the MCP (Message Communication Protocol) server with Wireshark to analyze and interact with network packets. The tool enables packet capture, analysis, and management using MCP while leveraging Wireshark's Lua scripting capabilities. - GitHub, erişim tarihi Haziran 5, 2025, https://github.com/shubham-s-pandey/WiresharkMCP
27. How to Write Wireshark Dissector - Sewio RTLS, erişim tarihi Haziran 5, 2025, https://www.sewio.net/open-sniffer/develop/how-to-write-wireshark-dissector/
28. 9.2. Adding a basic dissector - Wireshark, erişim tarihi Haziran 5, 2025, https://www.wireshark.org/docs/wsdg_html_chunked/ChDissectAdd.html
29. AUTOMATED SCRAPING AND AI-DRIVEN BEHAVIORAL ANALYSIS OF SUSPECT'S SOCIAL MEDIA PROFILES - IRJMETS, erişim tarihi Haziran 5, 2025, https://www.irjmets.com/uploadedfiles/paper//issue_4_april_2025/73247/final/fin_irjmets1745920684.pdf
30. Public DNS Resolvers Meet Content Delivery Networks: A Performance Assessment of the Interplay - arXiv, erişim tarihi Haziran 5, 2025, https://arxiv.org/html/2502.05763v1
31. ASN Lookup - ASN Search Online - DNS Checker, erişim tarihi Haziran 5, 2025, https://dnschecker.org/asn-whois-lookup.php
32. Autonomous System Lookup (AS / ASN / IP) - HackerTarget.com, erişim tarihi Haziran 5, 2025, https://hackertarget.com/as-ip-lookup/
33. ICEPRE: ICS protocol reverse engineering via data-driven concolic execution (ISSTA 2025 - Research Papers) - Researchr, erişim tarihi Haziran 5, 2025, https://conf.researchr.org/details/issta-2025/issta-2025-papers/104/ICEPRE-ICS-protocol-reverse-engineering-via-data-driven-concolic-execution
34. RSA Conference 2025 Key Cybersecurity Trends - Apriorit, erişim tarihi Haziran 5, 2025, https://www.apriorit.com/dev-blog/rsa-conference-trends-2025
35. A Network Threat Hunter's Guide to C2 over QUIC - Active Countermeasures, erişim tarihi Haziran 5, 2025, https://www.activecountermeasures.com/a-network-threat-hunters-guide-to-c2-over-quic/
36. RSA Conference 2025: A Barometer for Cybersecurity's Future | TFiR, erişim tarihi Haziran 5, 2025, https://tfir.io/rsa-conference-2025-a-barometer-for-cybersecuritys-future/
37. SpyCloud Annual Identity Exposure Report 2025, erişim tarihi Haziran 5, 2025, https://spycloud.com/resource/spycloud-annual-identity-exposure-report-2025/
38. Ethical and legal considerations | Network Security and Forensics Class Notes -

Fiveable, erişim tarihi Haziran 5, 2025, https://library.fiveable.me/network-security-and-forensics/unit-9/ethical-legal-considerations/study-guide/xKnweJ2XG10LbhKr
39. Navigating CCPA and GDPR Compliance: Essential Steps for US Businesses in 2025, erişim tarihi Haziran 5, 2025, https://consilien.com/news/navigating-ccpa-and-gdpr-compliance-essential-steps-for-us-businesses-in-2025
40. CCPA Compliance Checklist: A Detailed Guide for 2025 - Sprinto, erişim tarihi Haziran 5, 2025, https://sprinto.com/blog/ccpa-compliance-checklist/