Kapsamlı Malware Davranış Analiz Aracı için Gelişmiş Teknikler ve Eğilimler Raporu (2025 ve Sonrası)

Yönetici Özeti

Bu rapor, 2025 ve sonrasında sağlam bir Malware Davranış Analiz Aracı geliştirmek için kritik öneme sahip statik ve dinamik kötü amaçlı yazılım analizindeki gelişmiş teknikleri ve eğilimleri detaylandırmaktadır. Siber güvenlik ortamı, gelişmiş kaçınma taktikleri (örn. polimorfizm, metamorfizm, gizleme) kullanan saldırganlar ile en son yapay zeka (YZ) ve makine öğrenimi (ML) tekniklerini, özellikle Derin Öğrenme ve Büyük Dil Modellerini (LLM'ler) kullanan savunucular arasındaki tırmanan bir "silahlanma yarışı" ile karakterize edilmektedir. Temel eğilimler arasında YZ odaklı statik özellik çıkarımı, gizleme tespiti için Çizge Sinir Ağları (GNN'ler), LLM tabanlı anlamsal analiz ve gizleme giderme, CNN'ler aracılığıyla gelişmiş davranışsal izleme, bellek adli bilişimi için birleşik öğrenme ve siber menzillerde tam sistem emülasyonu yer almaktadır. Kapsamlı ve uyarlanabilir savunma stratejileri için statik ve dinamik analizi YZ destekli otomasyon ve tehdit istihbaratı ile entegre eden hibrit yaklaşımlar büyük önem taşımaktadır. Rapor, gelişen tehditlere karşı koymak için imza tabanlı tespitten davranış merkezli ve YZ destekli metodolojilere geçişi vurgulamaktadır.

Giriş: 2025'te Kötü Amaçlı Yazılım Analizinin Gelişen Manzarası

Dijital ekosistem, masaüstü bilgisayarlardan Nesnelerin İnterneti (IoT) cihazlarına kadar çeşitli platformları hedef alan, kalıcı ve giderek daha karmaşık kötü amaçlı yazılım tehditleriyle karşı karşıyadır.[1] Siber saldırılardaki artışla birlikte, kötü amaçlı yazılım tespiti, bireylerin ve kuruluşların dijital varlıklarını ve hassas bilgilerini korumak için kritik hale gelmiştir.[3] Özellikle fidye yazılımları, 2024'te saldırılarda ve ödemelerde önemli bir artışla birlikte, Living-Off-the-Land (LOTL) taktikleri gibi gelişen taktiklerle

birlikte birincil tehdit olmaya devam etmektedir.[4] 2025'te tehdit aktörleri, YZ odaklı kötü amaçlı yazılımlar aracılığıyla Windows güvenlik açıklarını giderek daha fazla istismar etmektedir.[1]

Geleneksel imza tabanlı tespit, modern, hızla gelişen kötü amaçlı yazılımlara karşı yetersiz kalmaktadır. Saldırganlar, kötü amaçlı yazılımların görünümünü ve yapısını değiştirerek tespitten kaçınmak için gizleme, şifreleme, kod mutasyonu, polimorfizm ve metamorfizm gibi gelişmiş kaçınma teknikleri kullanmaktadır.[1] Kodu çalıştırmadan inceleyen statik analiz, bu teknikler tarafından özellikle zorlanmaktadır; zira paketleyiciler ve şifreleyiciler, gerçek işlevselliği çalışma zamanına kadar gizleyerek geleneksel araçları "yüke karşı kör" hale getirmektedir.[5] "Yanlışlanabilir kanıtlara" dayanma, bu yaklaşımın temel bir sınırlamasıdır ve bu durum, bu tür özelliklere dayanan bazı makine öğrenimi tabanlı dedektörler için de geçerlidir.[9]

Statik imza eşleştirmenin sınırlamaları, uyum sağlayan sistemlere, nüansı anlayan ekiplere ve bilinen tehditleri kontrol etmenin ötesine geçen araçlara acil ihtiyacı vurgulamaktadır.[5] Bu durum, şifrelenmiş yükler veya anti-sandbox teknikleri gibi statik yöntemlerle gözden kaçırılabilecek davranışları ortaya çıkarabilen davranışsal analiz, makine öğrenimi ve dinamik analiz gibi yenilikçi tekniklere geçişi zorunlu kılmaktadır.[1] Amaç, reaktif savunmadan proaktif, sağlam ve açıklanabilir çözümlere geçmektir.[9]

Siber güvenlik alanındaki gelişmeler, kötü amaçlı yazılım tehditleriyle mücadelede sürekli bir tırmanışı gözler önüne sermektedir. Yapay zeka, sadece savunucular için değil, aynı zamanda saldırganlar için de önemli bir araç haline gelmiştir. "Yapay zeka odaklı kötü amaçlı yazılım" terimi [1] ve "ajanik yapay zeka modellerinin" yapay zekayı "görevleri planlayabilen, dünyayla etkileşime girebilen ve sorunları yardımsız çözebilen akranlara, hatta uzmanlara" dönüştürmesi [4] gibi ifadeler, her iki tarafın da yapay zekayı kullanarak sürekli olarak yeteneklerini geliştirdiği dinamik bir tehdit ortamına işaret etmektedir. Bu durum, bir "yapay zeka silahlanma yarışı"nı ortaya koymaktadır.[9] Bu rekabetçi evrim, uyarlanabilir, sağlam yapay zeka modellerine sürekli araştırma ve geliştirme ihtiyacını doğurmaktadır. Bu modellerin, farklı veri kümeleri ve ortamlarda iyi genelleme yapabilmesi ve sofistike, kaçamak kötü amaçlı yazılımlarla başa çıkabilmesi gerekmektedir.[3]

Bu "silahlanma yarışı" ile birlikte, kötü amaçlı yazılım analizinde temel bir paradigma değişimi yaşanmaktadır. Polimorfik ve metamorfik kötü amaçlı yazılımlara karşı imza tabanlı tespitin başarısızlığı [1], davranışsal analiz ve anlamsal anlama olan talebi doğrudan artırmaktadır.[1] Kötü amaçlı yazılımların kodunu ve yapısını sürekli olarak değiştirmesi, geleneksel imza tabanlı yöntemlerin hızla eskimesine neden olmuştur. Bu durum, analistlerin kötü amaçlı yazılımın gerçek niyetini ve çalışma zamanındaki

eylemlerini gözlemlemesini gerektiren davranışsal analiz ve kod yapısının ötesinde niyetini anlayan anlamsal analiz gibi yaklaşımlara yönelimi zorunlu kılmaktadır. Örneğin, Büyük Dil Modelleri (LLM'ler) aracılığıyla anlamsal analiz, ikili dosyaları "uzman bakış açısıyla" anlamanın bir yolu olarak ortaya çıkmaktadır.[12] Bu değişim, araç tasarımını etkilemekte, gerçek zamanlı izleme, derinlemesine kod anlama ve potansiyel olarak kötü amaçlı yazılım davranışlarının insanlar tarafından yorumlanabilir açıklamalarını gerektirmektedir.

I. Gelişmiş Statik Kötü Amaçlı Yazılım Analiz Teknikleri ve Eğilimleri (2025+)

Statik analiz, kötü amaçlı yazılımı çalıştırmadan inceleyerek kod yapısına, meta verilere ve gömülü yapay zekaya odaklanır. Geleneksel olarak kaçınma teknikleri tarafından zorlansa da, yapay zeka ve çizge tabanlı yöntemlerdeki gelişmeler, rolünü yeniden canlandırmaktadır.

1. Statik Özellik Çıkarımı ve Sınıflandırma için Yapay Zeka/Derin Öğrenme

1. **Kısa ve Öz Başlık:** Görselleştirme Tabanlı Kötü Amaçlı Yazılım Tespiti için Evrişimli Sinir Ağları (CNN'ler).
2. **Açıklama:** Bu teknik, kötü amaçlı yazılım örneklerinin ikili temsilini gri tonlamalı veya RGB görüntülere dönüştürerek statik özelliklerini analiz etmek için Evrişimli Sinir Ağları (CNN'ler) gibi Derin Öğrenme (DL) modellerini kullanır.[1] Bu yöntem, alan uzmanlarının yardımına ihtiyaç duymadan ikili verilerden otomatik olarak özellikler çıkarır ve böylece geleneksel imza tabanlı yöntemlerin sınırlamalarını aşar.[1] Görüntü tabanlı analiz, özellikle polimorfik ve metamorfik kötü amaçlı yazılımlar gibi kodlarını veya yapılarını sürekli değiştiren tehditleri tespit etmede etkilidir, çünkü bu tür kötü amaçlı yazılımlar davranışlarını değiştirmeden görünüşlerini değiştirebilirler.[7]
3. **2025'teki Potansiyel Etkileri ve Uygulama Alanları:** 2025'te görselleştirme tabanlı kötü amaçlı yazılım tespiti, masaüstü, mobil ve IoT platformları dahil olmak üzere çeşitli platformlarda kötü amaçlı davranışları tespit etmek ve anlamak için ölçeklenebilir ve yorumlanabilir çözümler sunmaktadır.[1] API çağrı dizilerini

görüntülere dönüştürerek ve bunları CNN'lerle sınıflandırarak, bu yaklaşım, çalışma zamanı etkileşimlerinden kötü amaçlı niyeti ayırt etmek için zengin bir özellik seti sunar.[7] Bu, özellikle kaynak kısıtlı IoT ortamlarında ve dağıtılmış senaryolarda, yüksek doğruluk oranları (örneğin %99'a kadar) ile evasif tehditlerin tespitini artırmaktadır.[7] Ayrıca, bu teknikler, Derin Öğrenme sınıflandırıcılarına yönelik düşmanca saldırı yöntemlerini keşfederek ve görselleştirme tabanlı kötü amaçlı yazılım sınıflandırıcılarının düşmanca sağlamlığını artırmak için savunma stratejileri geliştirerek model sağlamlığını artırmaya yardımcı olmaktadır.[1]

4. **Güvenilir Kaynak/Referans:** Gulshan & Neetu Sharma / IJETT, 73(1), 371-384, 2025 [1]; Sk Tanzir Mehedi et al., arXiv:2505.24231v1 [7]; M. Ahmad et al., arXiv:2505.07574v1 [1]; Mdpi.com, 2079-9292/14/1/167.[14]

2. Büyük Dil Modelleri (LLM'ler) ile Anlamsal Ön İşleme

1. **Kısa ve Öz Başlık:** LLM Tabanlı Anlamsal Ön İşleme ve Açıklanabilirlik.
2. **Açıklama:** Bu teknik, ikili dosyaları, özellikle Taşınabilir Yürütülebilir (PE) dosyalarını, makine öğrenimi modelleriyle kullanılmak üzere uygun bir biçime dönüştürmek için Büyük Dil Modellerini (LLM'ler) kullanır. Süreç, statik ve davranışsal analizden (örneğin, paketleyici imza tespiti, MITRE ATT&CK ve Kötü Amaçlı Yazılım Davranış Kataloğu (MBC) bilgisi) önemli bilgileri çıkarır ve bunları JSON raporları olarak biçimlendirir.[12] Geleneksel YZ tekniklerinin veri görünümlerine odaklanmasının aksine, bu yaklaşım uzman bilgisini önceliklendirerek kötü amaçlı yazılımın anlamsal analizini ve sonuçların yorumlanabilirliğini artırmayı amaçlar.[12] Raporlar, dosya bilgileri, bölüm detayları, içe aktarılan işlevler, paketleyici imzaları ve MITRE ATT&CK/MBC eşlemeleri gibi somut bilgiler içerir ve bu da analistler tarafından doğrudan anlaşılmasını sağlar.[13]
3. **2025'teki Potansiyel Etkileri ve Uygulama Alanları:** 2025 itibarıyla, bu ön işleme yöntemi, LLM'leri kullanarak kötü amaçlı yazılım kategorilerini sınıflandırmada yüksek performans (örneğin, %0,94 ağırlıklı ortalama F1 puanı) göstermiştir.[12] Bu, özellikle kötü amaçlı yazılım analizi için YZ modellerinin açıklanabilirliğini artırması açısından önemlidir, çünkü analistlerin kötü amaçlı yazılımın işlevselliği ve hedefleri hakkında derinlemesine bilgi edinmesini sağlar. Gelecekteki uygulamalar, raporlara dinamik analiz verilerini dahil ederek PE dosyalarının daha kapsamlı ön işlemesini içerebilir, ayrıca kötü amaçlı yazılım ailelerini daha hassas bir şekilde tespit etmek ve LLM dikkat mekanizmalarını kullanarak örnek davranışları özetlemek için sınıflandırmayı iyileştirmeyi de hedefler.[13] Bu, tehdit avcılığı ve gelişmiş kötü amaçlı yazılım tasnifi için kritik olan

daha yüksek düzeyli anlamsal sinyalleri yakalayarak mevcut veri kümelerini tamamlar.[12]

4. **Güvenilir Kaynak/Referans:** G. L'Hostis et al., arXiv:2506.12113v1.[12]

3. Gizleme Tespiti için Çizge Sinir Ağları (GNN'ler)

1. **Kısa ve Öz Başlık:** Çizge Sinir Ağları ile Fonksiyon Seviyesi Gizleme Tespiti.
2. **Açıklama:** Çizge Sinir Ağları (GNN'ler), statik kötü amaçlı yazılım analizinde, ikili fonksiyonların Nitelikli Kontrol Akış Grafikleri (CFG'ler) işlenerek gizleme tespiti için kullanılır. Bir CFG, fonksiyonun yürütme akışını temsil eder; burada düğümler Temel Bloklardır (talimatların atomik dizileri) ve yönlendirilmiş kenarlar yürütme yollarını temsil eder.[16] GNN'ler, bu çizge yapısını düğüm seviyesi özellikleriyle birlikte girdi olarak alır. Bilgi, komşu düğümlerden toplanır ve mevcut düğümün özellikleriyle birleştirilir. Bu yinelemeli "mesaj geçirme" süreci, GNN'lerin tek tek düğümler veya tüm çizge için temsiller öğrenmesini sağlar.[16] Araştırmalar, GNN'lerin başlangıç özelliklerinin zenginleştirilmesinin daha iyi performans için temel olduğunu, özellikle anlamsal ve sayma Pcode anımsatıcıları gibi zengin temsillerin en iyi sonuçları verdiğini göstermektedir.[16]
3. **2025'teki Potansiyel Etkileri ve Uygulama Alanları:** 2025'te GNN'ler, ikili dosyalardaki gizlenmiş fonksiyonları ve kullanılan belirli gizleme tekniklerini belirlemede kritik bir rol oynamaktadır. Bu, geliştiricilerin genellikle yalnızca kritik fonksiyonları gizlemesi nedeniyle önemlidir. GNN'ler, gizlemeyi tespit etmenin ötesinde, kullanılan gizleme türünü sınıflandırabilir, bu da otomatik saldırıların belirli gizleme şemalarına karşı geliştirildiği durumlarda hayati önem taşır ve analistlerin ilgili gizleme giderme araçlarını uygulamasını sağlar.[16] Ayrıca, GNN'ler bir gizleme yönteminin ne kadar tespit edilemez olduğuna dair ince taneli bir ölçüm sağlayarak, program koruma değerlendirmesi ve kötü amaçlı yazılım tespiti için temel oluşturur.[16] GNN'ler, anlamsal özelliklerle birleştirildiğinde, hem ikili hem de çok sınıflı sınıflandırma görevlerinde geleneksel makine öğrenimi tabanlı yöntemlerden daha iyi performans gösterebilir.[16] Gelecekteki araştırmalar, daha kapsamlı fonksiyon anlamsal özelliklerini yakalamak için yeni çizge temsilleri (örn. Anlamsal Odaklı Grafikler) geliştirmeye ve GNN'lerin gerçek dünya uygulamaları için performansını optimize etmeye odaklanacaktır.[16]
4. **Güvenilir Kaynak/Referans:** L. Marot et al., arXiv:2504.01481.[16]

4. LLM Tabanlı Montaj Seviyesi Kod Gizleme Giderme

1. **Kısa ve Öz Başlık:** LLM'ler ile Montaj Seviyesi Kod Gizleme Giderme.
2. **Açıklama:** Büyük Dil Modelleri (LLM'ler), montaj seviyesi kod gizleme giderme için ham montaj talimatlarını doğal dil cümlelerine benzer şekilde belirteç dizileri olarak ele alarak kullanılmaktadır. Bu yaklaşım, genel amaçlı LLM'lerin, geniş metin ve kod veri kümeleri üzerinde eğitilmiş olarak, özel ince ayar veya alan bilgisi gerektirmeden montaj seviyesi gizleme gidermeyi otomatikleştirip otomatikleştiremeyeceğini test etmektedir.[17] Araştırma, gizleme gidermeyi bir çeviri görevi olarak görmekte, burada LLM'ler gizlenmiş kodu daha anlaşılır biçimlere dönüştürebilir, doğal diller arasında çeviri yapmaya benzer şekilde.[17] Bu, geleneksel gizleme giderme yöntemlerinin önemli manuel müdahale gerektirmesi ve gelişmiş gizleme tekniklerine karşı zorlanması sorununu ele almaktadır.[19]
3. **2025'teki Potansiyel Etkileri ve Uygulama Alanları:** 2025 itibarıyla, en son ticari LLM'ler montaj seviyesi kod gizleme giderme için kapsamlı bir şekilde değerlendirilmektedir. Bu değerlendirmeler, farklı gizleme teknikleri ve modeller arasında önemli performans farklılıkları ortaya koymaktadır; bu, otonom gizleme gidermeden tamamen başarısızlığa kadar değişmektedir.[17] LLM'ler, gizlenmiş mantığın anlamsal özetlerini ve yüksek seviyeli yorumlarını sağlayarak insan analistlere kodun gerçek amacını anlamalarında önemli ölçüde yardımcı olabilir.[18] Bu, insan-YZ işbirliğinin yeni bir paradigmasına işaret etmektedir; burada LLM'ler tersine mühendisliğin belirli yönleri için uzmanlık engellerini azaltırken, karmaşık gizleme giderme görevleri için hala insan rehberliği gerektirmektedir.[17] Mevcut LLM'lerin birleşik gizleme tekniklerine karşı evrensel başarısızlığı, mevcut yeteneklerinin açık bir üst sınırını tanımlamakta ve sofistike koruma mekanizmalarının gelişmiş LLM'lere karşı bile etkili kaldığını göstermektedir.[18] Bu araştırma, ortaya çıkan yetenekleri değerlendirmek, daha dirençli gizleme teknikleri geliştirmek ve LLM'lerin 2025 ve sonrasında güvenlik iş akışlarını nasıl dönüştürebileceğini anlamak için bir temel oluşturmaktadır.[18]
4. **Güvenilir Kaynak/Referans:** E. A. Lachaux et al., arXiv:2505.19887v2 [17]; B. De Sutter, arXiv:2502.14093v1.[19]

II. Gelişmiş Dinamik Kötü Amaçlı Yazılım Analiz Teknikleri ve Eğilimleri (2025+)

Dinamik analiz, kötü amaçlı yazılımı kontrollü bir ortamda çalıştırarak davranışını gerçek zamanlı olarak gözlemlemeyi içerir. Bu yaklaşım, statik analizle kaçırılabilecek gizli veya şifreli kötü amaçlı yazılım davranışlarını ortaya çıkarmak için hayati öneme sahiptir.

1. Davranışsal İzleme ve Gerçek Zamanlı Etkileşim

1. **Kısa ve Öz Başlık:** Dinamik Analizde Gelişmiş Davranışsal İzleme.
2. **Açıklama:** Dinamik kötü amaçlı yazılım analizi, şüpheli dosyayı bir Sanal Makine (VM) veya sanal alan gibi güvenli, izole bir ortamda çalıştırarak programın davranışını gerçek zamanlı olarak gözlemlemeyi içerir.[10] Bu ortamlar, kötü amaçlı yazılımın dosya, işlem, bellek ve ağ etkinliğindeki değişikliklerini izleyerek kötü amaçlı eylemlerin belirtilerini tespit etmeye olanak tanır.[10] Gelişmiş araçlar, analistlerin kötü amaçlı yazılım davranışlarını tetiklemek için normal kullanıcı eylemlerini (tıklama, yazma vb.) taklit etmelerine olanak tanıyan gerçek zamanlı etkileşim yetenekleri sunar.[10] Bu izleme, şifrelenmiş yükler veya anti-sandbox teknikleri gibi statik analizde gözden kaçırılabilecek davranışları ortaya çıkarabilir.[10]
3. **2025'teki Potansiyel Etkileri ve Uygulama Alanları:** 2025'te dinamik analiz araçları, dosya manipülasyonları, kayıt defteri değişiklikleri ve ağ etkinliğinin dinamik görselleştirmelerini sağlayarak kötü amaçlı yazılımın eylemlerinin net bir resmini sunmaktadır.[10] Bu araçlar, kötü amaçlı IP'ler, URL'ler ve dosya karmaları gibi Uzlaşma Göstergelerinin (IoC'ler) otomatik olarak çıkarılmasıyla tehdit istihbaratını artırır.[10] Davranışsal izleme, fidye yazılımı, dosyasız kötü amaçlı yazılım ve bankacılık Truva atları gibi gerçek niyetlerini yürütmeye kadar gizleyen gelişmiş tehditleri tespit etmek için kritik öneme sahiptir.[10] Bu, güvenlik ekiplerinin hasarı hızlı bir şekilde yanıtlamasına ve azaltmasına olanak tanır.[10]
4. **Güvenilir Kaynak/Referans:** Cyberinfos.in, Top 10 Dynamic Malware Analysis Tools in 2025 [10]; GeeksforGeeks, Dynamic Malware Analysis.[20]

2. API Çağrı Dizilerinden CNN'ler ve Gri Tonlamalı Görüntüler

1. **Kısa ve Öz Başlık:** API Çağrı Dizileriyle CNN Tabanlı Kötü Amaçlı Yazılım Sınıflandırması.
2. **Açıklama:** Bu teknik, kötü amaçlı yazılım davranışlarını tespit etmek ve sınıflandırmak için API çağrı dizilerinden elde edilen zengin davranışsal bilgileri

kullanır. Kötü amaçlı yazılım örnekleri bir sanal alanda çalıştırılır ve sistemle çalışma zamanı etkileşimlerini kapsayan API çağrı dizileri toplanır.[14] Bu diziler daha sonra gri tonlamalı veya RGB görüntülere dönüştürülür ve bu görüntüler, uzamsal özellikleri etkili bir şekilde çıkarmak için Evrişimli Sinir Ağları (CNN'ler) gibi Derin Öğrenme modelleri tarafından sınıflandırılır.[7] Bu yaklaşım, tek özellik çıkarma yöntemlerinin sınırlamalarını aşarak görüntü ve anlamsal özelliklerin tamamlayıcı avantajlarını vurgular ve sınıflandırıcının ifade gücünü artırır.[14]

3. **2025'teki Potansiyel Etkileri ve Uygulama Alanları:** 2025'te API çağrı dizileri ve CNN'lerin kullanılması, polimorfik ve metamorfik kötü amaçlı yazılımlar gibi geleneksel kod tabanlı kontrolleri atlatabilen gelişmiş tehditlerin tespitinde önemli faydalar sağlamaktadır.[7] Bu yöntem, kötü amaçlı yazılımın zamanla geliştiği ve istatistiksel özelliklerinin değiştiği "kavram kayması" gibi zorlukları ele alarak yüksek doğruluk oranlarına (örneğin %99'a kadar) ulaşabilir.[14] Bu teknik, kötü amaçlı yazılım ailelerini davranışsal imzalarına göre sınıflandırmak için kullanılır ve bu da kötü amaçlı niyeti ayırt etmek için zengin bir özellik seti sunar.[15] Gelecekteki gelişmeler, derin öğrenme modelini sürekli olarak iyileştirmek için genetik algoritmalar içinde mutasyon operasyonları ve uygunluk puanı değerlendirmelerini içerebilir, böylece gelişen kötü amaçlı yazılım tehditlerine karşı sağlamlık sağlanır.[15]
4. **Güvenilir Kaynak/Referans:** Sk Tanzir Mehedi et al., arXiv:2505.24231v1 [7]; Mdpi.com, 2079-9292/14/1/167 [14]; arXiv:2502.08679v2.[15]

3. Bellek Adli Bilişimi ve Dosyasız Kötü Amaçlı Yazılım Tespiti

1. **Kısa ve Öz Başlık:** Birleşik Öğrenme ile Canlı Bellek Adli Bilişimi.
2. **Açıklama:** Canlı Bellek Adli Bilişimi (LMF), bellek içi kötü amaçlı yazılım veya dosyasız kötü amaçlı yazılımın izini ortaya çıkarmak için geçici bellek yapıtlarının edinimi ve analizini ele alır.[21] Geleneksel olarak, dijital adli tıp yöntemleri merkezi bir şekilde çalışarak gizlilik endişeleri, zincir muhafazasını sürdürme zorlukları, yavaş analiz süreleri ve ölçeklenebilirlik sorunları gibi birçok zorluğa yol açmıştır.[21] Birleşik öğrenme, makine öğrenimi modellerinin çeşitli yerel cihazlarda veya düğümlerde bağımsız olarak eğitilmesine izin vererek bu sınırlamaları ele alan merkezi olmayan bir yaklaşım sunar; zeka, gerektiğinde merkezi bir toplayıcı tarafından toplanır.[21] Bu merkezi olmayan mimari, ham veri toplama veya paylaşma ihtiyacını ortadan kaldırarak gizlilik sorunlarını çözer.[21]
3. **2025'teki Potansiyel Etkileri ve Uygulama Alanları:** 2025 itibarıyla, birleşik öğrenme tabanlı LMF modelleri, özellikle dosyasız kötü amaçlı yazılımların tespitinde yüksek doğruluk (%92,5'e kadar) göstermiştir.[21] Dosyasız kötü amaçlı

yazılımlar, tüm kötü amaçlı yazılımların %40'ını oluşturabilen, yalnızca bellekte çalışan ve sistemin fiziksel belleğinde iz bırakmayan gelişmiş siber saldırılardır.[21] Birleşik öğrenme, hassas bellek dökümlerini toplayan merkezi depolama riskini azaltarak gizliliği korur.[21] Ayrıca, bu yaklaşım, büyük ölçekli canlı ortamlarla mücadele eden ve toplu işlemle sınırlı olan merkezi yaklaşımların aksine, çeşitli cihazlarda kolayca ölçeklenebilir ve gerçek zamanlı analiz ile artımlı öğrenmeyi mümkün kılar.[21] Bu, yeni tehditlere hızlı uyum sağlamayı kolaylaştırır, bu da kötü amaçlı yazılımın sürekli gelişen doğası göz önüne alındığında çok önemlidir.[21]

4. **Güvenilir Kaynak/Referans:** S. S. Shinde et al., International Journal of Advanced Computer Science and Applications, Vol. 16, No. 4, 2025 [21]; arXiv:2502.12863.[22]

4. Tam Sistem Emülasyonu ve Siber Menziller

1. **Kısa ve Öz Başlık:** Siber Menzillerde Tam Sistem Emülasyonu.
2. **Açıklama:** Siber Menziller (CR'ler), bir kuruluşun yerel ağının, sisteminin, araçlarının ve uygulamalarının simüle edilmiş bir İnternet düzeyindeki ortama bağlı etkileşimli, simüle edilmiş temsilleridir.[23] Bunlar, siber güvenlik becerileri ve yetenekleri geliştirmek için eğitim ortamları olarak hizmet etmenin yanı sıra, güvenlik açıklarını analiz etmek ve tasarlanmış karşı önlemlerin etkinliğini denemek için güvenli ve yasal bir ortam sağlarlar.[23] Emülasyon, fiziksel altyapıyı siber menzilin kendisine dönüştüren bir CR oluşturma yaklaşımıdır.[23] Bu, birden fazla birbirine bağlı bileşenden oluşan kapalı ağ ortamları sağlar ve çeşitli protokolleri, kaynak modellerini, trafik akışlarını ve saldırıları taklit eden trafik üretimini içerir.[23]
3. **2025'teki Potansiyel Etkileri ve Uygulama Alanları:** 2025'te CR'ler, hedefli saldırılarda kullanılan kötü amaçlı yazılımların dinamik analizini güvenli bir şekilde mümkün kılmak için uygulama bulmuştur; burada amacını belirlemek için kötü amaçlı kodun yürütülmesi gereklidir.[23] Emülasyon, eğitim alanlara önceden programlanmış eylemler yerine otantik bir deneyim sunar ve Ulusal Siber Menzil (NCR) bunun dikkate değer bir örneğidir.[23] Ayrıca, Büyük Dil Modelleri (LLM'ler) ile otomatik siber saldırı emülasyonu, YZ destekli kötü amaçlı yazılım analizi için gerçekçi veri kümeleri oluşturmada önemli bir rol oynamaktadır.[24] Aurora gibi sistemler, klasik planlama ve LLM'leri kullanarak üçüncü taraf saldırı araçlarını ve tehdit istihbaratı raporlarını entegre ederek çok adımlı saldırıları otonom olarak taklit edebilir.[24] Bu, savunma sistemlerinin performansını karşılaştırmak ve zayıf yönlerini belirlemek için kapsamlı ve güncel siber saldırı veri kümeleri oluşturmak açısından kritik öneme sahiptir.[25]

4. **Güvenilir Kaynak/Referans:** M. Ahmad et al., arXiv:2504.12143 [23]; J. H. Al-Yasiri et al., arXiv:2407.16928v3.[24]

III. Hibrit Yaklaşımlar, Otomasyon ve Tehdit İstihbaratı Entegrasyonu (2025+)

Modern kötü amaçlı yazılımların artan karmaşıklığı, tek başına statik veya dinamik analiz yöntemlerinin yetersiz kalmasına neden olmuştur. Bu durum, her iki yaklaşımın güçlü yönlerini birleştiren hibrit metodolojilerin, yapay zeka destekli otomasyonun ve kapsamlı tehdit istihbaratının entegrasyonunun gerekliliğini ortaya koymaktadır.

1. Hibrit Statik-Dinamik Analiz Metodolojileri

1. **Kısa ve Öz Başlık:** Hibrit Kötü Amaçlı Yazılım Analizinde Gelişmeler.
2. **Açıklama:** Hibrit kötü amaçlı yazılım analizi teknikleri, yazılım davranışının daha kapsamlı bir şekilde anlaşılması için hem statik hem de dinamik analiz yöntemlerini farklı aşamalarda birleştirir.[2] Bu yaklaşım, kod yapısı veya izinler gibi statik özelliklerin, sistem çağrıları veya bellek kullanımı gibi dinamik davranışlarla entegrasyonunu içerebilir.[26] Amaç, tek modlu analizlerin sınırlamalarını, özellikle çok aşamalı kötü amaçlı yazılım yürütme, uzaktan erişim aktivasyonu ve dinamik yük oluşturma gibi yeni nesil saldırılarda yeterli görünürlük eksikliğini gidermektir.[26] Hibrit veri kümeleri, verimlilik ve derinliği dengelemek için meta veri ve statik kod özelliklerini birleştirir, ancak yine de kurulum zamanı davranışsal verilerin eksikliği nedeniyle sınırlıdır.[26]
3. **2025'teki Potansiyel Etkileri ve Uygulama Alanları:** 2025'te hibrit yaklaşımlar, kod yapıları ile çalışma zamanı davranışları arasındaki boşluğu kapatarak daha güvenli kod üretimine, yüksek kapsama alanlı testlere ve eyleme geçirilebilir kötü amaçlı yazılım analizine yol açmaktadır.[27] Bu entegrasyon, yanlış pozitifler, performans yükü ve çeşitli sistemlerde otomasyonu manuel müdahale olmadan sağlamanın zorluğu gibi geleneksel yöntemlerin sınırlamalarını azaltmaya yardımcı olur.[27] Örneğin, Python Paket Dizini (PyPI) ekosistemindeki tedarik zinciri saldırılarını tespit etmek için tasarlanmış QUT-DV25 gibi dinamik analiz veri kümeleri, kurulum ve kurulum sonrası zaman izlerini yakalayarak statik analizle

kaçırılabilecek davranışları ortaya çıkarır.[26] Bu, gelişen Açık Kaynak Yazılım (OSS) tedarik zinciri tehditlerine karşı sağlam savunmalar geliştirmek için güçlü bir temel sunar.[26]

4. **Güvenilir Kaynak/Referans:** Sk Tanzir Mehedi et al., arXiv:2505.13804 [26]; A. Al-Yasiri et al., arXiv:2502.18474 [27]; M. Ahmad et al., arXiv:2505.07574.[2]

2. LLM'ler ile Kötü Amaçlı Yazılım Analiz İş Akışında Otomasyon

1. **Kısa ve Öz Başlık:** LLM'ler ile Otomatik Kötü Amaçlı Yazılım Davranışı Anlama ve Kural Oluşturma.
2. **Açıklama:** Büyük Dil Modelleri (LLM'ler), kötü amaçlı yazılım analiz iş akışında, sandbox raporlarından kötü amaçlı yazılım davranışını otomatik olarak anlamak ve tespit kuralları oluşturmak için kullanılmaktadır. MaLAware gibi araçlar, Cuckoo Sandbox tarafından oluşturulan raporları işleyerek, ilgili bölümleri filtreleyerek ve bunları LLM'ye besleyerek kötü amaçlı yazılım davranışını otomatikleştirir.[28] LLM, yürütme sırasında kötü amaçlı yazılımın çeşitli olaylarını ve eylemlerini analiz eder ve ilişkilendirir, kapsamlı bir metinsel özet oluşturur.[28] RULELLM gibi başka bir yaklaşım ise, LLM'leri kullanarak OSS ekosistemlerindeki kötü amaçlı yazılım paketlerini tespit etmek için YARA ve Semgrep kurallarını otomatik olarak oluşturur.[29] Bu, manuel olarak kural oluşturmanın gerektirdiği önemli çabayı ve alan bilgisini azaltır.[29]
3. **2025'teki Potansiyel Etkileri ve Uygulama Alanları:** 2025'te LLM'ler, analistlerin bilişsel yükünü azaltarak ve olay müdahalesini hızlandırarak kötü amaçlı yazılım analizi sürecini önemli ölçüde basitleştirmektedir.[28] MaLAware gibi araçlar, güvenlik ekiplerinin sandbox raporlarını işlemesine, temel davranışsal bilgileri çıkarmasına ve yapılandırılmış özetler oluşturmasına olanak tanıyarak manuel çabayı azaltır.[28] Bu, veri sızdırma veya kalıcılık mekanizmaları gibi kötü amaçlı yazılım taktikleri hakkında kısa bilgiler sağlayarak karar alma süreçlerini iyileştirir ve ekiplerin uzlaşmaya uğramış sistemleri izole ederek veya kötü amaçlı iletişim kanallarını engelleyerek hızla yanıt vermesini sağlar.[28] RULELLM, geleneksel güvenlik araçlarının sınırlamalarını gidererek kural oluşturmayı otomatikleştirir ve OSS tedarik zinciri saldırılarının hızla ortaya çıkmasına daha iyi uyum sağlar.[29] Bu otomasyon, ölçeklenebilirliği artırır ve hem bilinen hem de ortaya çıkan tehditleri tespit etmek için uyarlanmış kuralların oluşturulmasını sağlar.[29]
4. **Güvenilir Kaynak/Referans:** B. Kumar et al., arXiv:2504.01145 [28]; F. K. Al-Yasiri et al., arXiv:2504.17198v1 [29]; Q. Qian et al., arXiv:2504.00694v1.[30]

3. Tehdit İstihbaratı Entegrasyonu ve YZ Odaklı Siber Tehdit İstihbaratı (CTI)

1. **Kısa ve Öz Başlık:** YZ ve ML ile Siber Tehdit İstihbaratının Geliştirilmesi.
2. **Açıklama:** Yapay Zeka (YZ) ve Makine Öğrenimi (ML) tekniklerinin Siber Tehdit İstihbaratı (CTI) ile entegrasyonu, siber tehditlerin veri toplama, ön işleme ve analiz verimliliğini artırarak siber güvenliği geliştirmek için kritik öneme sahiptir.[31] Bu entegrasyon, giderek karmaşıklaşan ve gelişen siber tehditlere karşı daha proaktif ve sağlam savunmalar sağlar.[31] YZ, özellikle CTI ön işlemesini optimize etmede çok önemli bir rol oynar, bu da modern siber tehditlerin dinamik doğasını anlamak ve daha güçlü siber güvenlik çerçeveleri için bir temel oluşturmak için hayati öneme sahiptir.[31]
3. **2025'teki Potansiyel Etkileri ve Uygulama Alanları:** 2025'te YZ ve ML, hem bilinen hem de bilinmeyen tehditlerin tespitini ve azaltılmasını önemli ölçüde artırmaktadır.[31] Bu, sistemlerin büyük miktarda veriyi hızlı ve doğru bir şekilde işlemesini sağlayarak kuruluşların siber güvenliğe yaklaşımını dönüştürmektedir.[31] Tehdit analizi, farklı kaynaklardan gelen büyük hacimli veriler ve çok dilli bağlamlar gibi zorluklarla karşılaştığından, YZ ve ML odaklı yöntemler tehdit tespiti ve olay çıkarımının doğruluğunu önemli ölçüde artırır.[31] Siber Güvenlik Bilgi Grafikleri (CSKG'ler), YZ destekli CTI bilgi çıkarımı için önemli bir araç olarak ortaya çıkmaktadır. CSKG'ler, düğümlerin varlıkları ve kenarların ilişkileri temsil ettiği, siber tehditler için bütünsel bir profil sağlayan, daha iyi görselleştirme sunan ve aşağı akış uygulamalarına entegrasyona daha uygun olan bir yapı sunar.[32] Bu, güvenlik operasyonlarını desteklemekte ve bilgi sistemlerinin giderek karmaşıklaşan siber tehditlere karşı genel dayanıklılığını güçlendirmektedir.[31]
4. **Güvenilir Kaynak/Referans:** J. H. Al-Yasiri et al., arXiv:2506.03551v1 [31]; Y. Liu et al., arXiv:2410.21060v2.[32]

Sonuç ve Öneriler

Kötü amaçlı yazılım analizi alanı, saldırganların sürekli gelişen kaçınma teknikleri ve yapay zeka odaklı saldırılarıyla karakterize edilen dinamik bir "silahlanma yarışı" içindedir. Bu durum, geleneksel imza tabanlı tespit yöntemlerinin yetersiz kalmasına ve davranışsal, anlamsal ve hibrit analiz yaklaşımlarına doğru temel bir paradigma

kaymasına neden olmuştur.

Kapsamlı bir Malware Davranış Analiz Aracı geliştirmek için aşağıdaki temel çıkarımlar ve öneriler sunulmaktadır:

1. **YZ Destekli Statik Analizin Önemi:** Kötü amaçlı yazılımın giderek artan gizleme ve polimorfik yetenekleri karşısında, statik analiz tek başına yeterli değildir. Ancak, görselleştirme tabanlı CNN'ler ve LLM tabanlı anlamsal ön işleme gibi YZ/DL teknikleri, ikili dosyalardan anlamlı özellikler çıkarmak ve analistlere yorumlanabilir bilgiler sağlamak için statik analizin yeteneklerini önemli ölçüde artırmaktadır. Bu, özellikle gizlenmiş kodun ve yeni kötü amaçlı yazılım ailelerinin ilk tespiti için kritik öneme sahiptir.
2. **Gelişmiş Dinamik Analiz Yetenekleri:** Kötü amaçlı yazılımın gerçek çalışma zamanı davranışını anlamak için dinamik analiz vazgeçilmezdir. Araç, API çağrı dizilerinden gri tonlamalı görüntüler oluşturmak için CNN'ler gibi gelişmiş davranışsal izleme tekniklerini entegre etmelidir. Ayrıca, dosyasız kötü amaçlı yazılımları tespit etmek ve gizlilik endişelerini gidermek için birleşik öğrenme tabanlı canlı bellek adli bilişimi yetenekleri dahil edilmelidir. Tam sistem emülasyonu ve siber menziller, gerçekçi kötü amaçlı yazılım davranışlarını gözlemlemek ve test etmek için güvenli ve kontrollü ortamlar sağlamalıdır.
3. **Hibrit Yaklaşımların Entegrasyonu:** Statik ve dinamik analiz arasındaki boşluğu kapatmak için hibrit metodolojiler zorunludur. Araç, her iki analiz türünden elde edilen verileri birleştirerek kötü amaçlı yazılımın hem iç yapısı hem de çalışma zamanı davranışı hakkında kapsamlı bir görünüm sunmalıdır. Bu, özellikle çok aşamalı veya bağlama duyarlı kötü amaçlı yazılımların tespitinde daha yüksek doğruluk ve daha derinlemesine anlama sağlar.
4. **LLM Destekli Otomasyon ve Açıklanabilirlik:** Büyük Dil Modelleri (LLM'ler), kötü amaçlı yazılım analiz iş akışında otomasyonu ve verimliliği artırmak için merkezi bir rol oynamaktadır. Araç, sandbox raporlarından kötü amaçlı yazılım davranışının otomatik özetlenmesi (MaLAware gibi) ve YARA/Semgrep kurallarının otomatik oluşturulması (RULELLM gibi) için LLM'leri kullanmalıdır. Bu otomasyon, analistlerin bilişsel yükünü azaltır, olay müdahalesini hızlandırır ve teknik olmayan paydaşlar için kötü amaçlı yazılım davranışının açıklanabilirliğini artırır.
5. **Tehdit İstihbaratı Entegrasyonu:** Tehdit istihbaratının sürekli evrimi göz önüne alındığında, aracın YZ ve ML destekli Siber Tehdit İstihbaratı (CTI) sistemleriyle sorunsuz bir şekilde entegre olması gerekmektedir. Bu, CTI raporlarından Uzlaşma Göstergeleri (IoC'ler) ve Taktikler, Teknikler ve Prosedürler (TTP'ler) gibi yapılandırılmış bilgilerin otomatik olarak çıkarılmasını içermelidir. Siber Güvenlik Bilgi Grafikleri (CSKG'ler) gibi yaklaşımlar, tehdit profillerinin bütünsel bir görünümünü sağlamak için kullanılabilir ve böylece proaktif tehdit avcılığı ve

savunma stratejileri güçlendirilir.

Özetle, 2025 ve sonrasında etkili bir Malware Davranış Analiz Aracı, YZ ve ML'nin en son gelişmelerini kullanarak, statik ve dinamik analizin güçlü yönlerini birleştiren uyarlanabilir, hibrit bir mimariyi benimsemelidir. Bu, sadece gelişen tehditlere karşı koymakla kalmayacak, aynı zamanda siber güvenlik analistlerinin verimliliğini ve karar alma süreçlerini de önemli ölçüde artıracaktır.

Alıntılanan çalışmalar

1. Security through the Eyes of AI: How Visualization is Shaping Malware Detection - arXiv, erişim tarihi Haziran 18, 2025, https://arxiv.org/html/2505.07574v1
2. Security through the Eyes of AI: How Visualization is Shaping Malware Detection - arXiv, erişim tarihi Haziran 18, 2025, https://arxiv.org/pdf/2505.07574
3. (PDF) Malware Analysis and Detection using ML tools: Current State ..., erişim tarihi Haziran 18, 2025, https://www.researchgate.net/publication/390089938_Malware_Analysis_and_Detection_using_ML_tools_Current_State_and_Challenges
4. ThreatDown State of Malware report 2025, erişim tarihi Haziran 18, 2025, https://www.threatdown.com/blog/threatdown-state-of-malware-report-2025/
5. Why static analysis can't keep up with modern malware | Okoone, erişim tarihi Haziran 18, 2025, https://www.okoone.com/spark/technology-innovation/why-static-analysis-cant-keep-up-with-modern-malware/
6. Dynamic Malware Analysis | INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT - IJNRD, erişim tarihi Haziran 18, 2025, https://ijnrd.org/viewpaperforall.php?paper=IJNRD2504437
7. Dynamic Malware Classification of Windows PE Files using CNNs and Greyscale Images Derived from Runtime API Call Argument Conversion - arXiv, erişim tarihi Haziran 18, 2025, https://arxiv.org/html/2505.24231v1
8. A Survey on Reinforcement Learning-Driven Adversarial Sample Generation for PE Malware - MDPI, erişim tarihi Haziran 18, 2025, https://www.mdpi.com/2079-9292/14/12/2422
9. 4th Workshop on Rethinking Malware Analysis (WoRMA 2025), erişim tarihi Haziran 18, 2025, https://worma.gitlab.io/2025/
10. Top 10 Best Dynamic Malware Analysis Tools in 2025 – Cyber infos, erişim tarihi Haziran 18, 2025, https://www.cyberinfos.in/top-10-dynamic-malware-analysis-tools-in-2025/
11. arXiv:2502.13055v1 [cs.CR] 18 Feb 2025, erişim tarihi Haziran 18, 2025, https://arxiv.org/abs/2502.13055
12. Semantic Preprocessing for LLM-based Malware Analysis - arXiv, erişim tarihi Haziran 18, 2025, https://arxiv.org/html/2506.12113v1
13. Semantic Preprocessing for LLM-based Malware Analysis - arXiv, erişim tarihi Haziran 18, 2025, https://arxiv.org/pdf/2506.12113

14. A Malware-Detection Method Using Deep Learning to Fully Extract ..., erişim tarihi Haziran 18, 2025, https://www.mdpi.com/2079-9292/14/1/167
15. Deep Learning-Driven Malware Classification with API Call Sequence Analysis and Concept Drift Handling - arXiv, erişim tarihi Haziran 18, 2025, https://arxiv.org/html/2502.08679v2
16. Identifying Obfuscated Code through Graph-Based Semantic ..., erişim tarihi Haziran 18, 2025, https://arxiv.org/pdf/2504.01481
17. Deconstructing Obfuscation: A four-dimensional framework for evaluating Large Language Models assembly code deobfuscation capabilities - arXiv, erişim tarihi Haziran 18, 2025, https://arxiv.org/html/2505.19887v2
18. Deconstructing Obfuscation: A four-dimensional framework ... - arXiv, erişim tarihi Haziran 18, 2025, https://arxiv.org/pdf/2505.19887
19. A New Framework of Software Obfuscation Evaluation Criteria - arXiv, erişim tarihi Haziran 18, 2025, https://www.arxiv.org/pdf/2502.14093
20. Dynamic Malware Analysis (Types and Working) - GeeksforGeeks, erişim tarihi Haziran 18, 2025, https://www.geeksforgeeks.org/dynamic-malware-analysis/
21. LIFT: Lightweight Incremental and Federated Techniques for Live ..., erişim tarihi Haziran 18, 2025, https://thesai.org/Downloads/Volume16No4/Paper_45-LIFT_Lightweight_Incremental_and_Federated_Techniques.pdf
22. arXiv:2502.12863v1 [cs.CR] 18 Feb 2025, erişim tarihi Haziran 18, 2025, https://arxiv.org/pdf/2502.12863
23. ARCeR: an Agentic RAG for the Automated Definition of Cyber ..., erişim tarihi Haziran 18, 2025, https://arxiv.org/pdf/2504.12143
24. From Sands to Mansions: Towards Automated Cyberattack Emulation with Classical Planning and Large Language Models - arXiv, erişim tarihi Haziran 18, 2025, https://arxiv.org/html/2407.16928v3
25. arXiv:2407.16928v3 [cs.CR] 17 Apr 2025, erişim tarihi Haziran 18, 2025, https://arxiv.org/pdf/2407.16928
26. QUT-DV25: A Dataset for Dynamic Analysis of Next-Gen ... - arXiv, erişim tarihi Haziran 18, 2025, https://arxiv.org/pdf/2505.13804
27. A Contemporary Survey of Large Language Model Assisted ... - arXiv, erişim tarihi Haziran 18, 2025, https://arxiv.org/pdf/2502.18474
28. MaLAware: Automating the Comprehension of Malicious ... - arXiv, erişim tarihi Haziran 18, 2025, https://arxiv.org/pdf/2504.01145
29. Automatically Generating Rules of Malicious Software ... - arXiv, erişim tarihi Haziran 18, 2025, https://arxiv.org/pdf/2504.17198
30. On Benchmarking Code LLMs for Android Malware Analysis - arXiv, erişim tarihi Haziran 18, 2025, https://arxiv.org/html/2504.00694v1
31. A Threat Intelligence Event Extraction Conceptual Model for ... - arXiv, erişim tarihi Haziran 18, 2025, https://arxiv.org/pdf/2506.03551
32. arXiv:2410.21060v2 [cs.CR] 21 Apr 2025, erişim tarihi Haziran 18, 2025, https://arxiv.org/pdf/2410.21060