Shodan.io: İnternet Bağlantılı Cihazların Keşfi ve Siber Güvenlikteki Rolü (2025 ve Sonrası)

1. Giriş

1.1. Projenin Amacı ve Kapsamı

Bu rapor, "Ağdaki Yazılımcıları Wireshark ile Tespit Etmek" projesinin metodolojik yaklaşımını benimseyerek, Shodan.io platformunu internete bağlı cihazların keşfi, analizi ve siber güvenlik bağlamındaki rolü açısından 2025 yılı ve sonrası için detaylı bir şekilde değerlendirmeyi amaçlamaktadır. Rapor, Shodan.io'nun temel işleyiş prensiplerini, veri toplama metodolojilerini, gelişmiş arama yeteneklerini, siber güvenlik ve Nesnelerin İnterneti (IoT) alanındaki pratik uygulama senaryolarını, gerçek zamanlı izleme özelliklerini (Shodan Monitor), etik ve gizlilik boyutlarını ve piyasadaki alternatiflerini kapsamlı bir şekilde ele alacaktır.[1] Temel hedef, Shodan.io'nun teknik derinliğini, stratejik önemini ve sorumlu kullanımının gerekliliğini vurgulayarak, siber güvenlik profesyonelleri, araştırmacılar ve geliştiriciler için değerli, kanıta dayalı ve güncel bilgiler sunmaktır.

1.2. Shodan.io'nun Siber Güvenlikteki Yeri ve Önemi

Shodan.io, geleneksel arama motorlarından farklı bir işlevsellik sunarak, web sayfaları yerine internete bağlı cihazları ve üzerlerinde çalışan servisleri indeksleyen özel bir arama motoru olarak öne çıkmaktadır.[1] Bu benzersiz yeteneği sayesinde, kuruluşların kendi sistemlerindeki zafiyetleri tespit etmelerine, potansiyel tehditler hakkında istihbarat toplamalarına ve siber güvenlik duruşlarını proaktif bir şekilde

güçlendirmelerine yardımcı olmaktadır.[2] Özellikle IoT cihazları, endüstriyel kontrol sistemleri (ICS), güvenlik kameraları, yönlendiriciler, sunucular ve yazıcılar gibi geniş bir yelpazedeki internete açık cihazların güvenlik açıklarını ve yanlış yapılandırmalarını ortaya çıkarmada kritik bir rol oynamaktadır.[2]

1.3. Raporun Yapısı

Bu rapor, Shodan.io'nun temel işleyişinden başlayarak, gelişmiş arama filtrelerine, çeşitli uygulama senaryolarına, izleme özelliklerine, etik ve gizlilik boyutlarına ve alternatif araçlara kadar altı ana bölümden oluşmaktadır. Her bölüm, derinlemesine analizler, pratik kullanım önerileri ve ilgili kaynak referansları ile desteklenerek, okuyucuya kapsamlı bir bakış açısı sunmayı hedeflemektedir.

2. Shodan.io'nun Temel İşleyişi ve Veri Toplama Mekanizmaları

Shodan.io Nedir ve Nasıl Çalışır?

Shodan, internete bağlı çeşitli sunucuları (webcamler, yönlendiriciler, sunucular vb.) çeşitli filtreler kullanarak arayan özel bir arama motorudur.[1] Geleneksel arama motorlarının aksine, Shodan web sayfalarını değil, internete bağlı cihazları ve sistemleri taramak üzere tasarlanmıştır. Bu tarama işlemi, açık portları tespit ederek ve bu portlara bağlı cihaz ve hizmet türlerini belirleyerek gerçekleştirilir.[2] Shodan, interneti sürekli olarak tarayarak IP adreslerini tanımlar ve bu cihazlardan aldığı yanıtlar aracılığıyla bilgi toplar.[6] Topladığı bilgiler arasında cihazların IP adresleri, işletim sistemleri, açık portları, üzerinde çalışan servisler ve coğrafi konumları gibi kritik meta veriler bulunmaktadır.[2]

Banner Verileri ve Toplama Süreci

Shodan'ın topladığı verilerin büyük çoğunluğu, bir cihaz üzerinde çalışan yazılımlar hakkında meta veri sağlayan "banner" adı verilen bilgilerden oluşur.[5] Bu bannerlar, sunucu yazılımı, hizmetin desteklediği seçenekler, bir karşılama mesajı veya istemcinin sunucuyla etkileşime geçmeden önce bilmek isteyebileceği herhangi bir bilgiyi içerebilir. Örneğin, bir FTP banner'ı sunucu adı, FTP sunucu türü ve sürümü hakkında detaylı bilgi sağlayabilir.[5] Shodan, web hizmetleriyle etkileşime girerek bu banner bilgilerini toplar ve bunları "banner" adı verilen yapılandırılmış bir nesnede saklar. Bu banner, Shodan'ın topladığı temel veri birimidir ve platformdaki tüm aramaların temelini oluşturur.[8]

Veri İndeksleme ve Güncelleme Yaklaşımları

Shodan, internete doğrudan bağlı tüm cihazlar hakkında bilgi toplar ve bunları kapsamlı bir şekilde indeksler. İndekslenen cihaz türleri, küçük masaüstü bilgisayarlardan nükleer santral kontrol sistemlerine kadar geniş bir yelpazeyi kapsayabilir.[5] Arama sorguları varsayılan olarak son 30 gün içinde toplanan verilere odaklanır, bu da sonuçların internetin mevcut durumuna dair güncel ve doğru bir görünüm sunmasını sağlar.[10] Shodan Monitor özelliği sayesinde, kullanıcılar kendi ağ aralıklarındaki cihazları gerçek zamanlı olarak izleyebilir ve beklenmedik bir cihaz veya hizmet ortaya çıktığında anında bildirim alabilirler.[11] İsteğe bağlı taramalar (On-Demand Scanning) da mevcuttur; kullanıcılar belirli IP adreslerini veya ağ bloklarını tarama talebinde bulunabilirler. Bu taramalar asenkron olarak gerçekleştirilir ve elde edilen sonuçlar Shodan API'si veya gerçek zamanlı akışlar aracılığıyla alınabilir, bu da esneklik ve otomasyon sağlar.[12]

Derinlemesine Analizler

Shodan'ın web sayfaları yerine internete bağlı cihazları indekslemesi, geleneksel arama motorlarından temel bir farklılık arz eder.[1] Bu yaklaşım, siber güvenlik alanında yeni bir boyut açmaktadır. Shodan'ın cihazları ve hizmet bannerlarını indekslemesi, küresel saldırı yüzeyinin "dışarıdan" bir görünümünü sunar. Bu durum, siber güvenlik odağını "bir web sitesinde hangi bilgiler var" sorusundan "internete hangi hizmetler açık ve

bunların özellikleri/zafiyetleri nelerdir" sorusuna kaydırmaktadır. Bu, proaktif güvenlik için kritik bir değişimdir. Shodan, son kullanıcının doğrudan, müdahaleci tarama yapmasına gerek kalmadan, dışa açık varlıkların küresel bir envanterini sunar ki bu da tehdit istihbaratı, risk değerlendirmesi ve uyumluluk için paha biçilmezdir. Ayrıca, web içeriği yerine hizmet bannerlarının birincil istihbarat kaynağı olarak önemini vurgulamaktadır. Bu paradigma değişimi, kuruluşların siber güvenlik duruşlarını reaktif olmaktan proaktif olmaya dönüştürmelerine olanak tanır. Shodan'ın sağladığı görünürlük, güvenlik ekiplerinin potansiyel zafiyetleri ve yanlış yapılandırmaları, kötü niyetli aktörler tarafından istismar edilmeden önce tespit etmelerini sağlar. Bu, özellikle hızla genişleyen dijital ayak izi olan modern kuruluşlar için vazgeçilmez bir yetenektir.

Ağ iletişiminin giderek artan bir şekilde şifrelenmesi (TLS/SSH), Shodan'ın geleneksel banner toplama yöntemleri için bir zorluk teşkil etmektedir. Veritabanları veya IoT cihaz yönetim arayüzleri gibi web dışı hizmetlerin bile şifreli iletişim kullanmaya başlaması, bannerların daha opak hale gelmesine neden olabilir. Wireshark raporunda belirtildiği gibi, günümüz ortamında ağ trafiğinin büyük bir kısmı şifreli olduğundan, geleneksel açık metin tabanlı analizler yetersiz kalmaktadır.[14] Bu bağlamda, Shodan'ın, Wireshark'ın bahsettiği JA3/JA4+ parmak izi alma tekniklerine benzer şekilde, şifreli el sıkışma meta verilerinden anlamlı bilgiler çıkarabilme yeteneği, platformun gelecekteki etkinliği için kritik olacaktır.[14] Bu durum, tespit ve kaçınma teknikleri arasındaki sürekli "kedi-fare" oyununu Shodan'ın veri toplama süreçlerine de taşımaktadır. Shodan'ın 2025 ve sonrasında relevansını sürdürebilmesi için, şifreli trafiğin meta verilerini daha etkin bir şekilde analiz etmesi ve belki de sertifika bilgileri veya gözlemlenen iletişim desenleri gibi dolaylı göstergelerden hizmet türlerini çıkarabilmesi gerekecektir. Bu, Shodan'ın tarama ve indeksleme metodolojilerinde sürekli adaptasyon ve yenilikçilik ihtiyacını işaret eder.

Shodan'ın tarama modelinin asenkron olması, sonuçların anında gelmemesi anlamına gelir.[12] Ancak, kullanıcılar isteğe bağlı taramalar yapabilir ve gerçek zamanlı akışlara abone olabilirler.[11] Asenkron tarama, Shodan'ın tüm interneti kapsama ve altyapısını aşırı yüklememe yeteneği için temeldir. Bu model, geniş ölçekli keşif için idealdir. Ancak, güvenlik operasyonlarında "gerçek zamanlı" tehdit tespiti genellikle anında görünürlük gerektirir. Shodan, bu ihtiyacı "Monitor" ve "Network Alerts" akışları ile adresler [11], izlenen aralıklardaki

değişiklikleri neredeyse gerçek zamanlı olarak sunar. Bu, ilk taramanın zaman almasına rağmen, değişikliklerin izlenmesinin hızlı olabileceği anlamına gelir. Bu model, hem geniş çaplı keşif hem de hedefe yönelik, sürekli izleme yeteneklerini desteklemektedir. Büyük kuruluşlar için, Shodan'ın API'sini ve gerçek zamanlı akışlarını mevcut Güvenlik Bilgileri ve Olay Yönetimi (SIEM) veya Güvenlik Orkestrasyonu, Otomasyon ve Yanıt

(SOAR) platformlarına entegre etmek, proaktif savunma için kritik hale gelmektedir. Asenkron yapı, ilk taramanın süresini uzatsa da, yeni ortaya çıkan veya tehlikeye atılmış varlıklara hızlı yanıt verilmesini sağlayarak güvenlik ekiplerinin verimliliğini artırmaktadır.

3. Shodan.io'nun Gelişmiş Arama Yetenekleri ve Filtreleri (Dorklar)

Temel Arama Operatörleri ve Söz Dizimi

Shodan, arama sorgularında "filtre:değer" formatında özel filtreler kullanma yeteneği sunar. Bu, kullanıcıların aramalarını son derece hassas bir şekilde daraltmalarına olanak tanır. Örneğin, Almanya'da bulunan Apache web sunucularını tespit etmek için "apache country:DE" gibi bir sorgu kullanılabilir.[13] Varsayılan olarak, Shodan yalnızca bir hizmetin "data" özelliğini arar. Arama değeri boşluk içeriyorsa, doğru sonuçlar elde etmek için tırnak içine alınması gerekmektedir (örn.

org:"SingTel Mobile").[8] Filtreler, arama sonuçlarını daha da daraltmak ve daha spesifik hedefler bulmak için mantıksal operatörlerle birleştirilebilir (örn.

port:443 product:Apache).[15]

Özel Filtreler ve Gelişmiş Sorgulama Teknikleri

Shodan, IP adresleri, port numaraları, organizasyon adı, ülke kodu ve işletim sistemi gibi çeşitli özelliklere göre detaylı filtreleme yapılmasına olanak tanır.[8] Popüler ve etkili "Shodan dorkları" şunları içerir:

org (hedef alanla ilgili tüm varlıkları bulma), asn (hedef şirkete ait tüm internete bağlı varlıkları bulma), port (belirli açık portları bulma), http.html (web sitesinin kaynak kodundaki belirli teknolojileri veya kelimeleri arama), http.status (HTTP durum koduna göre filtreleme), http.waf (Web Uygulama Güvenlik Duvarı'na göre filtreleme) ve

ssl.alpn (TLS Uygulama Katmanı Protokol Anlaşması değerlerini belirleme).[9]

vuln filtresi, bilinen zafiyetlere sahip cihazları bulmak için kritik bir araçtır (örn. vuln:CVE-2014-0160).[3]

has_screenshot:true filtresi, güvenlik kameraları veya VNC sistemleri gibi ekran görüntüsü olan cihazları tespit etmek için özellikle faydalıdır.[4]

Topluluk Sorguları ve Paylaşılan Bilgi Havuzu

Shodan, kullanıcıların kendi arama sorgularını tanımlamasına, etiketlemesine ve diğer kullanıcılarla paylaşmasına olanak tanıyan bir arama dizini sunar. Bu özellik, özellikle platforma yeni başlayan veya belirli bir zafiyeti arayan kullanıcılar için değerli bir bilgi kaynağıdır.[10] Paylaşılan arama sorguları halka açık olduğundan, kullanıcıların hassas veya gizli bilgileri içeren sorguları paylaşmaktan kaçınmaları önemlidir.[10]

Derinlemesine Analizler

Shodan filtrelerinin gelişimi, platformun basit bir cihaz tarayıcısından, yüksek düzeyde hedeflenmiş tehdit istihbaratı sağlayan güçlü bir Açık Kaynak İstihbaratı (OSINT) aracına dönüştüğünü göstermektedir. Bu detay seviyesi, güvenlik araştırmacılarının bilinen CVE'lere sahip belirli yazılım sürümlerini tanımlamasına, yanlış yapılandırmaları (örneğin, "default password") tespit etmesine ve hatta belirli geliştirme ortamlarının (örneğin, Jenkins örnekleri) varlığını çıkarmasına olanak tanır. has_screenshot filtresiyle doğrudan görsel verilerin ifşa edilmesi, gizlilik açısından özellikle endişe vericidir.[4] Bu detaylı filtreleme yeteneği, sızma testlerinde veya zafiyet değerlendirmelerinde ilk keşif için gereken çabayı önemli ölçüde azaltır. Ancak, bu güç kötüye kullanım potansiyelini de artırır, çünkü kötü niyetli aktörler aynı filtreleri büyük ölçekte zafiyetli hedefleri belirlemek için kullanabilir. Shodan'ın yetenekleri daha ayrıntılı hale geldikçe, meşru güvenlik araştırması ile potansiyel kötüye kullanım arasındaki çizgi incelir, bu da daha katı etik yönergeler ve sorumlu açıklama uygulamaları gerektirir.

"Dork" teriminin benimsenmesi, Shodan kullanıcı tabanının platformun indeksleme yeteneklerinin nüanslarını aktif olarak keşfettiğini ve bunlardan faydalandığını gösterir.[9]

Bu "dorkların" topluluk içinde paylaşılması [10], belirli zafiyetleri veya cihaz türlerini belirlemek için etkili arama stratejilerinin hızla yayılmasını sağlayan bir kolektif zeka yaratır. Bu "dorking" kültürü, dışa açık sistemleri belirleme bariyerini önemli ölçüde düşürür ve daha az deneyimli kişilerin bile kritik zafiyetleri bulmasına olanak tanır. Bu durum, bir bilgi asimetrisi yaratır: kuruluşlar maruz kalmış varlıklarından habersiz olabilirken, küresel bir kullanıcı topluluğu (hem etik hem de kötü niyetli) bunları kolayca keşfedebilir. Bu trend, kuruluşların kendi dış saldırı yüzeylerini proaktif olarak belirlemek ve düzeltmek için Shodan gibi araçları kullanma veya bu konuda uzman güvenlik profesyonelleriyle çalışma ihtiyacının aciliyetini vurgulamaktadır.

Shodan, statik bannerlar ve bilinen özelliklere dayanarak cihazları tanımlamada üstün olsa da [3], Wireshark raporunun "Makine Öğrenimi Destekli Davranışsal Analiz" vurgusu [14], basit imza tabanlı tespitin yetersiz kalacağı bir geleceğe işaret eder. Geliştirici araçları gibi unsurların ağ imzaları sık sık değişebilir.[14] Kötü niyetli aktörler de tespit edilmekten kaçınmak için ağ ayak izlerini aktif olarak değiştirmeye çalışır. Shodan, keşif için güçlü olsa da, gelecekte daha fazla davranışsal analiz yeteneği entegre etmesi veya harici ML destekli içgörülerden yararlanması gerekebilir. Shodan'ın temel gücü pasif tarama ve indeksleme olsa da, "geliştirici avcılığı" veya "tehdit avcılığı"nın geleceği, Shodan'ın geniş görünürlüğünü gelişmiş davranışsal analiz araçlarıyla (örneğin, gelişmiş NTA veya ML modelleri) birleştirmeyi gerektirebilir. Bu, Shodan benzeri keşif ile gelişmiş davranışsal analitik platformları arasında daha bütünsel bir tehdit ortamı görünümü sağlamak için potansiyel bir yakınsama veya entegrasyon noktasını düşündürmektedir.

Tablo 1: Shodan.io Temel Filtreleri ve Kullanım Örnekleri

Filtre Adı	Açıklama	Kullanım Örneği	Amaç
port	Belirli bir açık porta sahip cihazları bulur.	port:22	SSH sunucularını tespit etme.[3]
country	Sonuçları belirli bir ülkeyle sınırlar.	apache country:DE	Coğrafi konum bazlı hedefleme veya risk analizi.[3]
org	Belirli bir kuruluşa ait cihazları arar.	org:"Google"	Kurumsal varlık keşfi, gölge BT tespiti.[3]

product	Belirli bir yazılım ürünü veya teknolojisi çalıştıran cihazları bulur.	product:"MongoDB"	Belirli teknoloji yığınlarını veya zafiyetli yazılımları belirleme.[3]
vuln	Bilinen zafiyetlere (CVE) sahip cihazları tespit eder.	vuln:CVE-2014-0160	Hedefli zafiyet taraması ve risk değerlendirmesi.[3]
http.html	Web sitesinin kaynak kodundaki belirli kelimeleri veya teknolojileri arar.	http.html:"Drupal 8.0"	Web uygulamalarındaki özel imzaları veya teknolojileri bulma.[9]
ssl.alpn	TLS el sıkışmasındaki Uygulama Katmanı Protokol Anlaşması (ALPN) değerlerini belirler.	ssl.alpn:"h2"	Belirli protokollerin (örn. HTTP/2) kullanımını veya istemci/sunucu parmak izlerini tespit etme.[9]
has_screenshot	Ekran görüntüsü alınabilen cihazları (örn. web kameraları, VNC) bulur.	has_screenshot:true	Görsel maruziyetleri ve gizlilik ihlallerini tespit etme.[4]
os	Belirli bir işletim sistemi çalıştıran cihazları arar.	os:"Linux"	İşletim sistemi dağılımını veya belirli OS zafiyetlerini araştırma.[13]
asn	Belirli bir Otonom Sistem Numarası'na (ASN) ait tüm internete bağlı varlıkları bulur.	asn:15169	Bir kuruluşa ait tüm internet varlıklarını haritalama.[9]

4. Shodan.io'nun Siber Güvenlik ve IoT Alanındaki Uygulama Senaryoları

Zafiyet Tespiti ve Risk Değerlendirmesi

Shodan, siber güvenlik araştırmacılarının ve geliştiricilerin, internete bağlı zafiyetli cihazları doğrudan ve müdahaleci taramalar yapmadan tespit etmeleri için güçlü bir araç sağlar.[4] Açık portları tarayarak ve bunlara bağlı cihaz ve hizmet türlerini belirleyerek, BT ve güvenlik uzmanlarının kendi sistemlerinde keşif yapmalarına ve potansiyel zafiyetler hakkında istihbarat toplamalarına yardımcı olur.[2] Eski veya bilinen zafiyetler içeren yazılım çalıştıran cihazları belirlemek için kullanılabilir. Bilinen zafiyetler içeren belirli yazılım sürümlerini arayarak potansiyel saldırı vektörleri proaktif olarak tespit edilebilir.[6]

vuln filtresi ile Heartbleed gibi belirli zafiyetlere sahip cihazlar kolayca bulunabilir, bu da hedefli zafiyet taramasına olanak tanır.[3] Varsayılan parolalarla veya kimlik doğrulama olmadan açıkta kalan MongoDB veritabanları, Telnet sunucuları, VNC sistemleri, MQTT brokerları gibi yanlış yapılandırılmış veya korumasız sistemleri tespit edebilir.[3]

Kurumsal Ağ Güvenliği ve Varlık Yönetimi

Kuruluşların, kendi ağ aralıklarındaki internete bağlı cihazları izlemesine ve beklenmedik bir şey ortaya çıktığında gerçek zamanlı bildirimler almasına olanak tanır. Bu, "gölge BT" (shadow IT) varlıklarının tespitinde kritik öneme sahiptir.[11] Veri sızıntılarını (buluta sızan kurumsal veriler), kimlik avı web sitelerini ve ele geçirilmiş veritabanlarını tespit etmeye yardımcı olur, bu da dışarıya maruz kalmış hassas bilgilerin izlenmesini sağlar.[11] Kurumsal ağlarda yetkisiz veya güncel olmayan geliştirici araçlarının veya kütüphanelerinin (örneğin, IDE'ler, Git istemcileri) ağ üzerindeki izlerini dolaylı olarak belirlemede kullanılabilir, ancak bu doğrudan Shodan'ın birincil kullanım alanı değildir, daha çok Wireshark gibi araçlarla birleştiğinde anlam kazanır.[14]

IoT Cihaz Güvenliği ve İzleme

Shodan, güvenlik kameraları, tıbbi cihazlar, akıllı ev aletleri (buzdolapları, kapı zilleri) gibi geniş bir yelpazedeki IoT cihazlarını aramak için yaygın olarak kullanılır.[2] IoT sistemlerinde zayıf güvenlik mekanizmaları veya yanlış yapılandırmalarla ilgili zafiyetleri tespit etmek için özel olarak tasarlanmıştır.[4] Örnek sorgular:

camera (tüm web kameralarını bulma), WVC80N (eski Linksys web kameraları), AXIS webcams (port:80 has_screenshot:true), linux upnp avtech (AVTECH cihazları), ikettle (akıllı su ısıtıcıları), webiopi (Raspberry Pi IoT uygulamaları) gibi sorgular, belirli IoT cihazlarını ve onların güvenlik durumunu ortaya çıkarabilir.[3]

Geliştiriciler ve Araştırmacılar İçin Kullanım Alanları

Shodan, geliştiricilerin kendi sistemlerindeki dışa açık servisleri ve potansiyel zafiyetleri anlamalarına yardımcı olur, bu da "güvenli kodlama" ve "güvenli dağıtım" pratiklerini destekler.[2] API'si aracılığıyla aramaları otomatikleştirmeye ve Shodan'ı mevcut güvenlik araçlarına entegre etmeye olanak tanır, bu da büyük ölçekli güvenlik denetimleri ve sürekli izleme için idealdir.[3] Trend analizi ve tahminler yapmak için kullanılabilir; zaman içindeki verileri karşılaştırarak zafiyet salgınlarını tahmin etmeye ve proaktif savunma stratejileri geliştirmeye yardımcı olur.[6] Pazarlama ekipleri ve yazılım satıcıları için de farklı yazılım sürümlerini ve belirli bir coğrafi bölgede çalışan örnek sayısını filtreleyerek pazar araştırması yapma imkanı sunar.[16]

Derinlemesine Analizler

Shodan, bir kuruluşun internete açık varlıklarına dışarıdan, bir saldırganın gözünden bakış açısı sunarak, reaktif olay müdahalesinden proaktif saldırı yüzeyi yönetimine geçişi mümkün kılar. Kuruluşlar, Shodan'ı kullanarak bilinmeyen veya unutulmuş varlıkları (gölge BT), yanlış yapılandırmaları (örneğin, varsayılan kimlik bilgileri, açık veritabanları) ve zafiyetli yazılım sürümlerinin maruziyetini, kötü niyetli aktörler tarafından istismar edilmeden *önce* sürekli olarak keşfedebilir ve izleyebilir.[2] Bu, "bozulmadan önce düzelt" yaklaşımını benimsemeyi sağlayarak saldırganlar için fırsat penceresini önemli ölçüde daraltır. Modern BT ortamlarının (bulut, IoT, uzaktan çalışma) artan karmaşıklığı, saldırı yüzeyinin sürekli genişlemesi ve değişmesi anlamına gelir. Shodan, bu dinamik yüzeyi haritalamak ve izlemek için kritik, ölçeklenebilir bir

mekanizma sağlar. Zafiyet yönetimi ve sürekli izleme programlarına entegrasyonu, olgun güvenlik operasyonları için standart bir uygulama haline gelecektir. Bu aynı zamanda güvenlik ekiplerinin, Shodan gibi harici tarayıcılar tarafından algılanan kendi dijital ayak izlerini anlamaları ve dış maruziyetlerini düzenli olarak denetlemeleri gerektiği anlamına gelir.

IoT cihazlarının hızlı yayılımı, genellikle minimum güvenlik önlemleriyle (örneğin, varsayılan parolalar, yamalanmamış yazılımlar, güvensiz protokoller) dağıtılması, büyük ve genişleyen bir saldırı vektörü yaratmaktadır. Shodan'ın bu güvensiz cihazları kolayca tanımlama yeteneği [4], IoT güvenliğindeki sistemik bir sorunu vurgular. Bu sadece bireysel cihazlarla ilgili değil; tüm akıllı şehirlerin, kritik altyapının ve IoT'ye giderek daha fazla bağımlı olan kurumsal ortamların güvenlik duruşuyla ilgilidir. Shodan'ın IoT zafiyetlerine ilişkin sağladığı bilgiler, IoT üretiminde ve dağıtımında "tasarımla güvenlik" (security by design) yaklaşımına duyulan acil ihtiyacın altını çizmektedir. Ayrıca, üçüncü taraf satıcılardan gelen güvensiz bileşenlerin veya cihazların bir kuruluşun ağına önemli zafiyetler sokabileceği potansiyel tedarik zinciri risklerini de ortaya koyar. Güvenlik profesyonelleri için Shodan, IoT dağıtımlarını denetlemek, güvenlik politikalarını uygulamak ve IoT satıcılarından daha iyi güvenlik uygulamaları talep etmek için temel bir araç haline gelir. Shodan tarafından kolayca istismar edilebilir IoT cihazlarının sürekli olarak ifşa edilmesi, kullanıcı farkındalığı ve üretici sorumluluğunda kalıcı bir boşluk olduğunu göstermekte, bu da Shodan'ı IoT güvenliği için fiili bir kamu denetçisi haline getirmektedir.

Wireshark raporu geliştiricilerin *dahili* ağ trafik desenlerine odaklanırken [14], Shodan dışarıdan maruz kalan geliştirme altyapısının

harici bir görünümünü sağlar. Shodan aracılığıyla Jenkins sunucularının [16], Git depolarının veya yanlış yapılandırılmış ve herkese açık API test ortamlarının (Postman/Insomnia gibi) bulunması, bir kuruluşun geliştirme uygulamalarını ve yazılım geliştirme yaşam döngüsü (SDLC) ile ilgili potansiyel dış saldırı vektörlerini gösterebilir. Bir "Developer Hunter" projesi için Shodan, bir kuruluşun halka açık geliştirme varlıklarını belirlemek için bir ilk keşif aracı olarak hizmet edebilir. Bu dış istihbarat, geliştiricilerin dışarıdan hangi teknolojiler ve hizmetlerle etkileşim kurabileceği konusunda bağlam sağlayarak dahili Wireshark tabanlı analizi bilgilendirebilir. Örneğin, Shodan açıkta bir Jenkins sunucusu ortaya çıkarırsa, dahili Wireshark analizi daha sonra CI/CD boru hatları, belirli derleme araçları veya o Jenkins örneğiyle etkileşimlerle ilgili trafik desenlerine odaklanabilir. Bu, kapsamlı geliştirici etkinliği profilleme ve güvenlik için harici (Shodan) ve dahili (Wireshark) ağ analizi arasında sinerjik bir ilişkiyi vurgulamaktadır.

5. Shodan Monitor: Gerçek Zamanlı Ağ İzleme ve Uyarılar

Shodan Monitor'ün İşleyişi ve Özellikleri

Shodan Monitor, kullanıcıların kendi ağ aralıklarındaki internete açık cihazları sürekli olarak izlemelerine yardımcı olmak için tasarlanmış kapsamlı bir hizmettir.[11] Beklenmedik bir cihaz veya hizmet ortaya çıktığında anında gerçek zamanlı bildirimler sağlayarak güvenlik ekiplerinin hızlı tepki vermesine olanak tanır.[11] Tek bir IP adresinden milyonlarca müşteriye sahip büyük İnternet Servis Sağlayıcılarına (ISP) kadar her boyuttaki ağı etkin bir şekilde yönetmek için tasarlanmış yüksek ölçeklenebilir bir platformdur.[11] Sadece bilinen ağ varlıklarını izlemekle kalmaz, aynı zamanda internet üzerindeki diğer cihazları da keşfetmeye yardımcı olur; buluta veri sızıntılarını, kimlik avı web sitelerini ve ele geçirilmiş veritabanlarını tespit edebilir.[11]

Otomatik Tarama ve Bildirim Mekanizmaları

Kullanıcıların manuel olarak tarama göndermesine gerek yoktur; Shodan Monitor, izlenen ağ aralıklarını otomatik ve sürekli olarak tarar, bu da sürekli bir güvenlik duruşu sağlar.[11] İsteğe bağlı taramalar, belirli bir güvenlik sorununun (örneğin, bir zafiyetin yamalanması) çözülüp çözülmediğini doğrulamak için kullanılabilir, bu da doğrulama süreçlerini hızlandırır.[11] Shodan Monitor, E-posta, Slack, MS Teams, Discord, Telegram, Gitter, Pagerduty ve Webhook gibi çeşitli bildirim seçenekleri sunarak güvenlik ekiplerinin tercih ettikleri iletişim kanalları üzerinden anında uyarı almasını sağlar.[11] Uyarılar, IP aralığı veya CIDR notasyonu kullanılarak belirli filtrelerle (örneğin,

ip filtresi) tetiklenebilir, bu da uyarıların hedeflenmiş ve ilgili olmasını sağlar.[13]

API Entegrasyonu ile Gelişmiş İzleme

Shodan Monitor web sitesindeki tüm özellikler, Shodan API ve komut satırı arayüzü (CLI) aracılığıyla da erişilebilir, bu da otomasyon ve entegrasyon için esneklik sunar.[11] Geliştiriciler ve güvenlik ekipleri, aramaları otomatikleştirmek, özel izleme araçları oluşturmak ve maruziyetleri gerçek zamanlı olarak takip etmek için Shodan API'sini kullanabilirler. Bu, özellikle binlerce cihazı yöneten büyük kuruluşlar için faydalıdır.[7] Ham olay verilerine, mevcut Shodan API'si aracılığıyla, özellikle belirtilen ağ aralıkları için tüm olayları içeren Ağ Uyarıları akışı (Network Alerts stream) üzerinden erişilebilir. Bu, güvenlik analistlerinin derinlemesine inceleme ve korelasyon yapmasına olanak tanır.[11]

Derinlemesine Analizler

Shodan'ın temel arama motoru, internetin bir anlık görüntüsünü sağlayan pasif bir keşif aracıdır. Ancak Shodan Monitor, bunu aktif, sürekli bir güvenlik duruşu yönetim çözümüne dönüştürür. Taramaları otomatikleştirerek ve gerçek zamanlı uyarılar sağlayarak, kuruluşların yeni maruziyetleri, yanlış yapılandırmaları veya ihlalleri neredeyse anında tespit etmelerini sağlar.[11] Bu, periyodik zafiyet taramasından sürekli harici saldırı yüzeyi izlemesine doğru kritik bir geçiştir. Bu özellik, geniş ve dinamik IP alanlarını yöneten büyük işletmeler ve ISP'ler için paha biçilmezdir.[11] Yeni ortaya çıkan hizmetleri, kazara veri sızıntılarını veya tehlikeye atılmış sistemleri istismar edilmeden önce hızla tespit etmelerini ve düzeltmelerini sağlar. Çeşitli bildirim kanallarıyla (Slack, Pagerduty, Webhook) entegrasyon [11], güvenlik ekiplerinin derhal bilgilendirilmesini sağlayarak hızlı olay müdahalesini kolaylaştırır. Bu, kuruluşları hızlı bulut benimseme ve dinamik altyapı çağında daha olgun, otomatik ve gerçek zamanlı bir harici güvenlik stratejisine iter.

Shodan Monitor için kapsamlı bir API'nin bulunması [11], güvenlik otomasyonu için önemli bir yetenek sunmaktadır. Kuruluşların Shodan'ın harici istihbaratını mevcut güvenlik araçlarına ve iş akışlarına (SIEM'ler, SOAR platformları veya özel komut dosyaları) doğrudan entegre etmelerine olanak tanır. Bu, manuel kontroller yerine, Shodan'dan gelen uyarıların otomatik olarak inceleme, diğer tehdit istihbaratı kaynaklarıyla zenginleştirme veya hatta otomatik düzeltme eylemleri (örneğin, güvenlik duvarı değişikliklerini tetikleme veya biletleme sistemleri) için playbook'ları tetikleyebileceği anlamına gelir. Bu düzeydeki API entegrasyonu, karmaşık ortamlarda güvenlik operasyonlarını ölçeklendirmek için gereklidir. Manuel iş yükünü azaltır, tespit ve yanıt sürelerini hızlandırır ve daha proaktif ve verimli bir güvenlik duruşu sağlar. "Developer

Hunter" türündeki projeler için, açıkta kalan geliştirme ortamları veya araçları için sürekli izlemenin tamamen otomatikleştirilebileceği, politika ihlalleri veya kazara maruziyetler hakkında gerçek zamanlı uyarılar sağlayarak SDLC'nin genel güvenliğini artırabileceği anlamına gelir. "Ham olaylar"a yapılan vurgu [11], özel işlemeye ve korelasyona izin vererek derinlemesine analitik entegrasyonu daha da destekler.

6. Shodan.io'nun Etik Boyutları, Gizlilik Endişeleri ve Sorumlu Kullanım

Veri Toplama Pratiklerinin Etik İncelemesi

Shodan'ın interneti tarayarak cihazları kataloglama yeteneği, ağ güvenliği risklerini anlama ve azaltmada kritik bir rol oynar.[17] Ancak, Shodan benzeri arama motorlarının şeffaflık, zararsızlık ve anonimlik eksikliği gibi önemli etik sorunları olduğu belirtilmiştir.[17] Bu motorların, kullanıcıların taramalardan vazgeçmesine izin vermediği ve kötü biçimlendirilmiş istekler gönderdiği, yetkisiz olarak aşırı ayrıntılara erişmeye çalıştığı ve hatta kişisel olarak tanımlanabilir bilgileri (PII) ve ekran görüntülerini arama sonuçlarında yayınlayabildiği gözlemlenmiştir.[17] Bu uygulamalar, kullanıcı gizliliğini tehlikeye atar ve cihazları kötü niyetli varlıklar tarafından daha fazla riske maruz bırakır.[17]

Gizlilik İhlalleri ve Potansiyel Kötüye Kullanım Senaryoları

Shodan'ın IoT cihazlarını indeksleme yaklaşımı, bireyler, şirketler ve altyapılar hakkında hassas bilgileri, bazen de kişisel olarak tanımlanabilir verileri (PII) ortaya çıkarabilir.[18] Bu durum, kötü niyetli aktörler tarafından yetkisiz erişim, veri ihlalleri veya gözetim amaçlı kötüye kullanım için ciddi bir risk oluşturur.[18] Özellikle varsayılan kimlik bilgileri veya kimlik doğrulama olmadan açıkta kalan web kameraları gibi cihazların bulunması ve ekran görüntülerinin yayınlanması, ciddi gizlilik sorunlarına yol açabilir.[4] Shodan'ın kullanımı yasal olsa da, elde edilen bilgileri yetkisiz erişim sağlamak için kullanmak yasa

dışıdır ve ciddi sonuçları olabilir.[3]

Yasal Çerçeveler ve Sorumlu Kullanım İlkeleri

Shodan'ı kullanırken sorumlu ve etik yönergelere sıkı sıkıya uymak hayati öneme sahiptir.[3] Sızma testi yapacak profesyonellerin, Shodan kullanarak keşfedilen sistemleri incelemeden veya zafiyetleri istismar etmeden önce açık ve yazılı izin almaları gerekmektedir. Yetkisiz testler yasa dışıdır ve ciddi cezai yaptırımlara yol açabilir.[6] Veri koruma önlemleri ve siber güvenlik en iyi uygulamalarına sıkı sıkıya bağlı kalmak, Shodan ve benzeri araçların sorumlu ve yasalara uygun kullanımı için elzemdir.[18] Kuruluşlar, kendi IoT cihazlarını güvence altına almalı ve istenmeyen maruziyeti önlemek için ağlarını düzenli olarak kontrol etmelidir.[3]

Derinlemesine Analizler

Shodan'ın kapsamlı indekslemeyi önceliklendiren tasarımı, güvenlik için faydası ile gizlilik ihlali ve kötüye kullanım potansiyeli arasında hassas bir denge yaratmaktadır. Shodan, internete açık cihazların güvenlik durumunu ortaya koyarak siber güvenlik profesyonellerine değerli bilgiler sunarken [3], aynı zamanda kişisel olarak tanımlanabilir bilgileri (PII) ve ekran görüntülerini (örneğin, web kameralarından) ifşa etme potansiyeli taşır.[17] Bu, Shodan'ın pasif tarama yaklaşımının, cihazların ve hizmetlerin varsayılan yapılandırmalarından kaynaklanan güvenlik ve gizlilik risklerini istemeden de olsa artırabileceği anlamına gelir. Bu durum, "hackerlar için arama motoru" [2] olarak anılmasına yol açarken, aynı zamanda etik kullanımın ve yasal sınırlamalara uymanın önemini de vurgular.[3] Gelişen dijital çağda, bu tür araçların yaygınlaşması, bireylerin ve kuruluşların kendi dijital ayak izlerinin farkında olmalarını ve proaktif güvenlik önlemleri almalarını zorunlu kılmaktadır.

Shodan'ın yasal bir araç olmasına rağmen [3], kötüye kullanım potansiyeli, siber güvenlik alanında "amaç aracı meşrulaştırır mı?" sorusunu gündeme getirmektedir. Shodan'ın sağladığı bilgiler, yetkisiz erişim girişimleri, veri sızıntıları ve gözetim için kullanılabilir.[18] Bu, Shodan'ın kendisinin bir saldırı aracı olmasa da, kötü niyetli aktörler için bir "hazine haritası" işlevi görebileceği anlamına gelir.[7] Bu durum, siber güvenlik topluluğunun, bu tür araçların sorumlu kullanımına ilişkin sıkı etik kurallar geliştirmesi ve uygulamasının

yanı sıra, yasal çerçevelerin de bu hızla değişen teknolojik ortama uyum sağlamasının gerekliliğini ortaya koymaktadır. Kuruluşların, kendi dışa açık varlıklarını düzenli olarak Shodan gibi araçlarla denetlemesi ve tespit edilen zafiyetleri derhal gidermesi, bu potansiyel kötüye kullanım riskini azaltmanın temel yoludur. Bu, sürekli bir güvenlik denetimi ve iyileştirme döngüsünü zorunlu kılar.

Shodan'ın sürekli olarak maruz kalmış ve zafiyetli sistemleri ifşa etmesi, siber güvenlikte "tasarımla güvenlik" ve "varsayılan olarak güvenlik" ilkelerinin yetersiz uygulandığına dair sistemik bir kanıt sunmaktadır. Birçok cihaz ve hizmet, varsayılan olarak güvensiz yapılandırmalarla veya zayıf kimlik doğrulama mekanizmalarıyla internete açılmaktadır.[3] Bu, sadece teknik bir sorun değil, aynı zamanda yazılım ve donanım üreticilerinin güvenlik sorumluluğuna ilişkin daha geniş bir endüstri sorunudur. Shodan, bu sistemik zayıflıkları görünür kılarak, üreticiler ve geliştiriciler üzerinde daha güvenli ürünler tasarlama ve dağıtma konusunda bir baskı unsuru oluşturmaktadır. Ayrıca, son kullanıcıların ve kuruluşların, kullandıkları cihazların ve hizmetlerin güvenlik yapılandırmalarını aktif olarak yönetmeleri ve güncelleme yamalarını uygulamaları gerektiği konusunda sürekli bir hatırlatıcı görevi görür. Bu durum, siber güvenlik farkındalığının ve eğitiminin, teknolojik çözümler kadar önemli olduğunu göstermektedir.

7. Sonuç ve Değerlendirme

Shodan.io, 2025 yılı ve sonrasında internete bağlı cihazların keşfi ve siber güvenlik analizinde merkezi bir araç olmaya devam edecektir. Geleneksel arama motorlarının ötesine geçerek cihazları ve hizmet bannerlarını indekslemesi, küresel saldırı yüzeyine dışarıdan bir bakış açısı sunarak proaktif güvenlik duruşlarının benimsenmesini sağlamaktadır. Şifreli trafiğin yaygınlaşması, Shodan'ın banner toplama yetenekleri için bir zorluk teşkil etse de, platformun meta veri analizi ve dolaylı göstergelerden bilgi çıkarma yeteneklerini geliştirmesi, gelecekteki etkinliği için kritik olacaktır. Bu durum, Wireshark gibi araçlarla davranışsal analiz yeteneklerinin entegrasyonu ihtiyacını da beraberinde getirmektedir.

Shodan'ın gelişmiş arama filtreleri ve "dorking" kültürü, hedeflenmiş zafiyet istihbaratı toplamayı kolaylaştırmakta, ancak aynı zamanda kötüye kullanım potansiyelini de artırmaktadır. Bu, bilgi asimetrisini vurgulayarak kuruluşların kendi dış saldırı yüzeylerini sürekli denetlemesini zorunlu kılmaktadır. Shodan Monitor özelliği, pasif keşfi sürekli,

gerçek zamanlı izlemeye dönüştürerek, yeni maruziyetlerin ve yanlış yapılandırmaların anında tespit edilmesini sağlamaktadır. API odaklı otomasyon yetenekleri ise Shodan'ın mevcut güvenlik operasyon merkezlerine entegrasyonunu kolaylaştırarak, güvenlik yanıt sürelerini hızlandırmakta ve verimliliği artırmaktadır.

Ancak, Shodan'ın etik boyutları ve gizlilik endişeleri göz ardı edilemez. Kişisel olarak tanımlanabilir bilgilerin ve ekran görüntülerinin ifşa edilmesi, sorumlu kullanım ilkelerine ve yasal çerçevelere sıkı sıkıya uyulmasını gerektirmektedir. Shodan, yasal bir araç olsa da, kötüye kullanım potansiyeli, siber güvenlik topluluğunun etik yönergeleri ve yasal düzenlemeleri sürekli olarak gözden geçirmesini zorunlu kılmaktadır. Son olarak, Shodan'ın sürekli olarak maruz kalmış ve zafiyetli sistemleri ifşa etmesi, "tasarımla güvenlik" ve "varsayılan olarak güvenlik" ilkelerinin endüstri genelinde daha iyi uygulanması gerektiğine dair sistemik bir kanıt sunmaktadır. Kuruluşlar ve bireyler için Shodan, kendi dijital ayak izlerini anlamak, proaktif güvenlik önlemleri almak ve siber güvenlik farkındalığını artırmak için vazgeçilmez bir referans noktasıdır.

Alıntılanan çalışmalar

1. en.wikipedia.org, erişim tarihi Haziran 26, 2025, https://en.wikipedia.org/wiki/Shodan_(website)#:~:text=Shodan%20is%20a%20search%20engine,sends%20back%20to%20the%20client.
2. Shodan: The Search Engine For Hackers | @Bugcrowd, erişim tarihi Haziran 26, 2025, https://www.bugcrowd.com/blog/shodan-the-search-engine-for-hackers/
3. How To Discover IoT Devices With Shodan - ITU Online IT Training, erişim tarihi Haziran 26, 2025, https://www.ituonline.com/how-to/how-to-discover-iot-devices-with-shodan/
4. Teaching and Learning IoT Cybersecurity and Vulnerability Assessment with Shodan through Practical Use Cases - PubMed Central, erişim tarihi Haziran 26, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC7309102/
5. What is Shodan?, erişim tarihi Haziran 26, 2025, https://help.shodan.io/the-basics/what-is-shodan
6. Illuminating the Digital Shadows with Shodan | Evolve Security, erişim tarihi Haziran 26, 2025, https://www.evolvesecurity.com/blog-posts/illuminating-the-digital-shadows-with-shodan
7. Shodan: The Search Engine for Hackers - Uproot Security, erişim tarihi Haziran 26, 2025, https://www.uprootsecurity.com/blog/shodan-the-search-engine-for-hackers-and-security-professionals
8. Search Query Fundamentals - Shodan Help Center, erişim tarihi Haziran 26, 2025, https://help.shodan.io/the-basics/search-query-fundamentals
9. Shodan Dorks - The God's Eye. Summary : | by Jerry Shah (Jerry) | Medium, erişim tarihi Haziran 26, 2025,

https://shahjerry33.medium.com/shodan-dorks-the-gods-eye-f224f9b3984f
10. Navigating the Website - Shodan Help Center, erişim tarihi Haziran 26, 2025, https://help.shodan.io/the-basics/navigating-the-website
11. Shodan Monitor, erişim tarihi Haziran 26, 2025, https://monitor.shodan.io/
12. On-Demand Scanning - Shodan Help Center, erişim tarihi Haziran 26, 2025, https://help.shodan.io/the-basics/on-demand-scanning
13. REST API Documentation - Shodan Developer, erişim tarihi Haziran 26, 2025, https://developer.shodan.io/api
14. deepsearch.01.result.pdf
15. Working with Shodan Data Files, erişim tarihi Haziran 26, 2025, https://help.shodan.io/mastery/working-with-shodan-data-files
16. Top 40 Shodan Dorks to find sensve itiinformation in 2023 - SecurityTrails, erişim tarihi Haziran 26, 2025, https://securitytrails.com/blog/top-shodan-dorks
17. Revealing the Black Box of Device Search Engine: Scanning Assets, Strategies, and Ethical Consideration - arXiv, erişim tarihi Haziran 26, 2025, https://arxiv.org/html/2412.15696v1
18. Abstract Conclusions References Methodology Results and Discussion Introduction Background Problem Author: Paula A. Nevárez Rom, erişim tarihi Haziran 26, 2025, https://prcr.cobimet.org/bitstreams/c9e8a2fa-86b0-4a2e-ab26-ed9ff9439f61/download
19. Introduction to cyber security: stay safe online: Week 1: 2.1 | OpenLearn - Open University, erişim tarihi Haziran 26, 2025, https://www.open.edu/openlearn/mod/oucontent/view.php?id=48261§ion=2.1