



YÖNETİCİ ÖZETİ

CROWDSTRIKE

2025  
KÜRESEL TEHDİT  
RAPORU

# Yenilikçi Saldırganların Yılı

CrowdStrike Küresel Tehdit Raporu, her yıl bir önceki yılın tehdit ortamının kapsamlı bir analizini siber güvenlik sektörüyle paylaşır. Tehdit ortamını şekillendiren saldırıcı davranışları ve yöntemleri ayrıntılı olarak incelenir. Bu raporda, 2024'e damga vuran trendler ve olaylar, saldırıcıların kullandığı yöntemler ve gelişen tehditler karşısında kuruluşların alması gereken önlemler yer alıyor.

Saldırganlar 2024'te típkı bir işletme gibi daha hızlı ve verimli çalışmanın yollarını aradı. Yeni teknolojiler keşfettiler ve başarısı kanıtlanan stratejilerini daha da iyileştirdi ve ölçeklendirdiler. Çağımızın saldırıcıları azimleri ve profesyonellikleriyle öne çıkmak istiyor. Savunma stratejilerindeki değişiklikleri hızlıca tespit edebiliyor ve bunlara uyum sağlıyorlar. Hedeflerine tam anlamıyla odaklıyorlar.

Saldırganları durdurmak için onları iyi tanımak gerekiyor. Saldırganların davranışlarını, motivasyonlarını ve tekniklerini öğrenmek faaliyetlerini daha iyi anlamamızı ve daha güçlü savunma stratejileri geliştirmemizi sağlayabilir.

CrowdStrike 2025 Küresel Tehdit Raporu, okuyucuların karşı karşıya oldukları tehditlerle ilgili daha kapsamlı bilgiler edinmesi için 2024 yılındaki trendlere yer veriyor. Bu raporda, yapay zeka tabanlı CrowdStrike Falcon® platformundan gelen trilyonlarca telemetri olayı ve özel tehdit avıcılarının hızı sayesinde tehdit istihbaratının gücüne güç katan seçkin CrowdStrike Saldırgan Karşıtı Operasyonlar Ekibi'nin gözlemleri yer almaktadır.

Bu yönetici özeti, güvenlik ekiplerinin giderek karmaşıklaşan tehdit ortamına dair bilmesi ve uygulaması gereken kritik bilgileri ayrıntılarıyla açıklayan raporun temel bulgularına yer verir.



BU YÖNETİCİ ÖZETİ'NDE ADI GEÇEN  
VE SEKTÖRÜNÜZÜ VEYA BÖLGİNİZİ  
HEDEF ALAN SALDIRGANLAR  
HAKKINDA DAHA FAZLA BİLGİ  
EDİNMEK İÇİN CROWDSTRIKE  
ADVERSARY UNIVERSE'E GÖZ ATIN.

# Tehdit Ortamına Genel Bakış



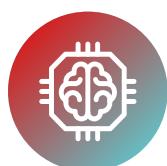
**Saldırganlar giderek hızlanıyor:** Ortalama e-suç yayılma süresi (saldırganın hedef organizasyonda sizdiği ilk sisteme diğerine geçme süresi) 2024'te **48 dakikaya** düştü ve en hızlı e-suç yayılma süresi **51 saniye** oldu.



**Erişim yöntemleri gelişiyor:** Saldırganlar hedefledikleri ağlara sızmak için sesli kimlik avı (vishing), geri arama kimlik avı ve destek ekibi gibi sosyal mühendislik uygulamalarını kullanıyor. Ayrıca çalıntı kimlik bilgileri sık sık kullanılıyor: Geçerli kimlik bilgisi satan erişim aracı reklamları **önceki yıla göre %50** arttı. CrowdStrike'nin 2024'te tespit ettiği **güvenlik açıklarının yarısından fazlası (%52)** ilk erişimle ilgili.



**Gizlilik öncelik sırasını koruyor:** Modern tehditlerin çoğu, klavye üzerinden etkileşimli saldırı tekniklerine dayanıyor. 2024'te **tespit edilen tehditlerin %79'unda kötü amaçlı yazılım kullanılmadı**. CrowdStrike, etkileşimli saldırı kampanyalarında **yıllık %35'lük bir artış** gözlemledi.



**Saldırganlar üretken yapay zekayı sık sık kullanıyor:** Saldırganlar 2024'te, sosyal mühendislik girişimlerini geliştirmek, yanıltma operasyonlarını daha hızlı gerçekleştirmek ve kötü amaçlı ağ etkinliklerini güçlendirmek için üretken yapay zekayı daha sık kullanmaya başladı.



**Çin, siber faaliyetlerini artırıyor:** Çin bağlantılı faaliyetler **tüm sektörlerde %150 artarken** finansal hizmetler, medya, imalat ve endüstri/mühendislik gibi temel hedeflere yapılan saldırılarda **%200-300** oranında şaşırtıcı bir artış yaşandı.

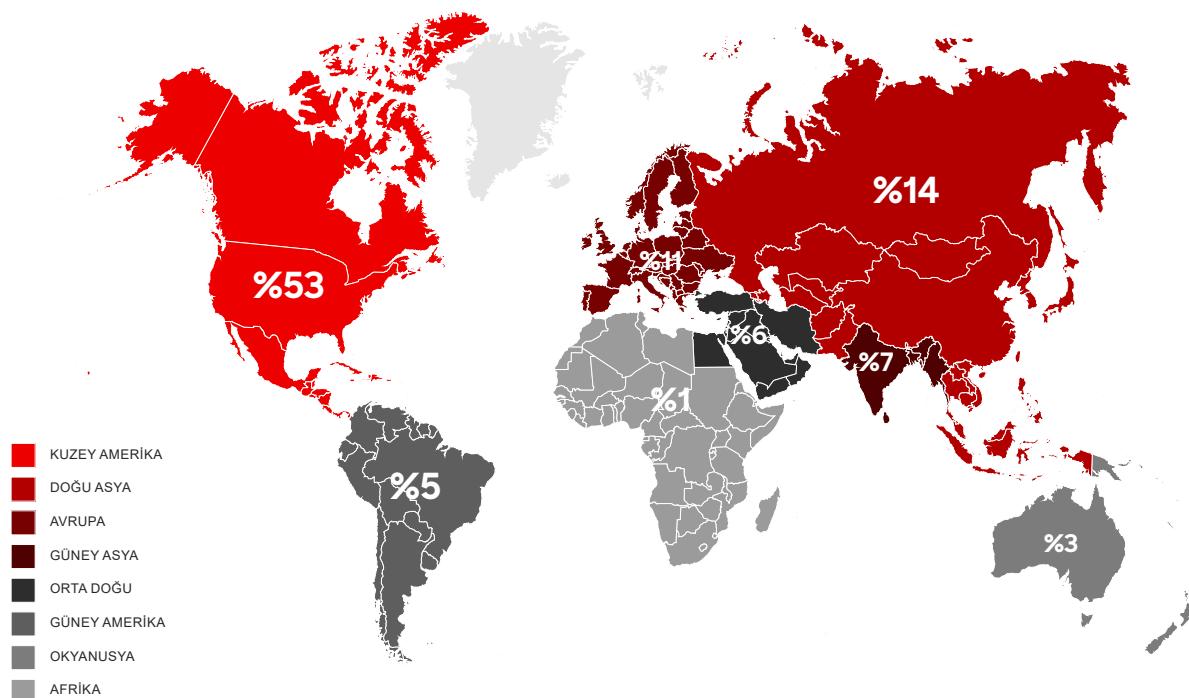


**Bulut ortamları kuşatma altında:** Bulut; büyük miktarda veri barındırması, ölçeklenebilir olması ve kötü amaçla kullanılabilen yanlış yapılandırmalar uygulanması nedeniyle temel hedeflerden biri olmaya devam ediyor. CrowdStrike, 2024'te yeni ve saldırganın henüz belirlenemediği bulut saldırılarda **%26'lık bir artış** tespit etti. Artık daha fazla saldırgan bulut hizmetlerini hedef alıyor.

**AD REHBERİ**

SALDIRGAN	ULUS-DEVLET VEYA KATEGORİ
	<b>BEAR</b> RUSYA
	<b>BUFFALO</b> VIETNAM
	<b>CHOLLIMA</b> KUZEY KORE
	<b>CRANE</b> GÜNEY KORE
	<b>HAWK</b> SURIYE
	<b>JACKAL</b> HACKTİVİST
	<b>KITTEN</b> İRAN
	<b>LEOPARD</b> PAKİSTAN
	<b>LYNX</b> GÜRCİSTAN
	<b>OCELOT</b> KOLOMBİYA
	<b>PANDA</b> ÇİN HALK CUMHURİYETİ
	<b>SAIGA</b> KAZAKİSTAN
	<b>SPHINX</b> MISIR
	<b>SPIDER</b> BİLİŞİM SUÇU
	<b>TIGER</b> HİNDİSTAN
	<b>WOLF</b> TÜRKİYE

## Bölgeye Göre Etkileşimli Saldırılar



Şekil 1. Bölgelere göre etkileşimli saldırılar (Ocak-Aralık 2024)

## Etkileşimli Saldırılarda Hedef Alınan İlk 10 Sektör



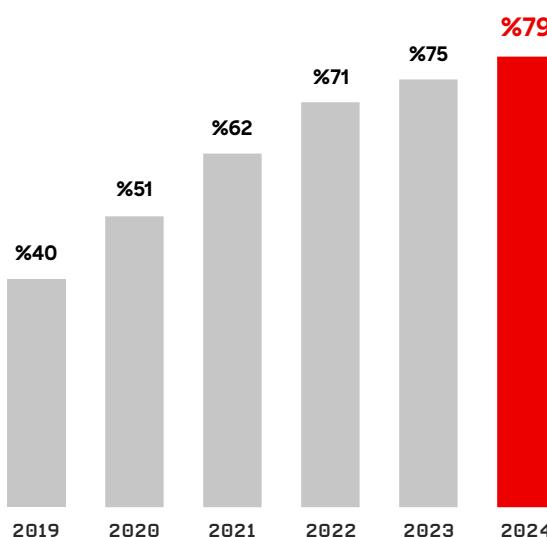
Şekil 2. Etkileşimli saldırınlarda hedef alınan ilk 10 sektör (Ocak-Aralık 2024)



Bu istatistikler, saldırganların gerçekleştirdiği operasyonların küresel erişimine dikkat çekmektedir. Kimlik ihlali, sistemler arası hareket ve bulut tabanlı saldırı vektörlerini hesaba katan alanlar arası güvenlik stratejilerinin önemini vurgulamaktadır.

Saldırganlar son beş yıldır, kötü amaçlı yazılım içermeyen saldırı tekniklerine yöneliyor.

Kötü amaçlı yazılım içermeyen faaliyetlerin oranı, büyük bir artış göstererek 2024'te %79'a ulaştı. Bu oran 2019'da %40'tı.



Şekil 3. Kötü amaçlı yazılım içermeyen saldırıların yüzdesi (2019-2024)

# Öne Çıkan Temalar

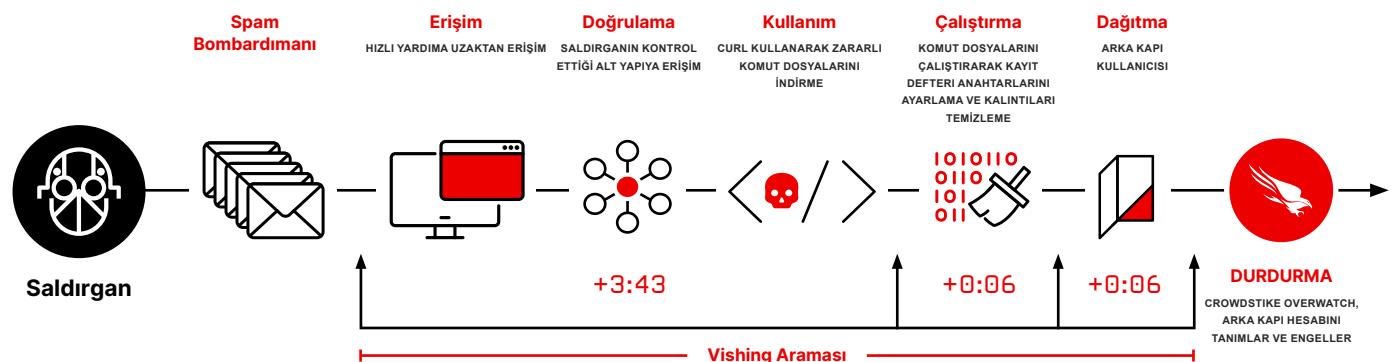
## SOSYAL MÜHENDİSLİK AÇIKLARI

2024'te saldırganlar, insanların açıklarını hedef almaya başladığı için ilk erişim teknikleri de değişti. Sistemlere erişmek ve kuruluş içinde sistemler arası hareket edebilmek için canlı kimlik bilgileri ve sosyal mühendislik uygulamaları sık sık kullanılıyor. CrowdStrike olarak, telefon odaklı sosyal mühendislik kampanyalarında ve destek ekibini taklit ederek kişilere ulaşma girişimlerinde artış gözlemliyoruz. Bu gelişmeler, e-suç taktiklerinde yeni yaklaşımlara işaret ediyor.

- Vishing operasyonları 2024 yılının ilk yarısından ikinci yarısına %442 oranında arttı.
- CURLY SPIDER, CHATTY SPIDER ve PLUMP SPIDER gibi deneyimli e-suç grupları kimlik bilgilerini çalmak, uzaktan erişim sağlamak ve savunma uzmanlarına yakalanmamak için bu taktikleri kullandı.
- CrowdStrike, 2024'te BT personelini taklit ederek hedeflerini arayan ve uzaktan destek oturumu başlatmaya ikna etmeye çalışan, birbirinden farklı ama birbirile alakalı en az altı kampanya tespit etti.

## ÖRNEK OLAY

## CURLY SPIDER



**Şekil 4.** CrowdStrike OverWatch, saldırgandan hızlı hareket ederek CURLY SPIDER'ın sosyal mühendislik saldırısını dört dakikadan kısa sürede durduruyor

2024 yılında CURLY SPIDER, en hızlı ve en fazla gelişen e-suç saldırganlarından biri oldu.

Bu örnek olayda, ilk cihazdan başka bir cihaza geçmeden hedeflerine ulaşmaya çalışırlar.

İlk kullanıcı etkileşiminden sosyal mühendisliğe, ardından sisteme yerleşmek için arka kapı hesabı açmaya kadarki tüm saldırı süreci, dört dakikadan kısa sürdü.

CURLY SPIDER'in ilk erişiminin ardından fırsat penceresi sınırlıydı. Sadece telefon görüşmesi sonlandırılana kadar vakitleri vardı. Sistemde kalıcılık sağlamak için bunu görüşme sona ermeden yapmaları gerekiyordu.

Uzaktan erişim sağlandıktan sonra CURLY SPIDER, hızlı bir şekilde hareket ederek (çoğu zaman görüşme hâlâ devam ederken) yükleri dağıtıp kalıcılık sağladı. Saldırının büyük kısmı, bulutta barındırılan kötü amaçlı komut dosyalarına ulaşmak için bağlantı kurmak ve erişim sorunlarını gidermekle geçti.

## Üretken Yapay Zeka ve Yenilikçi Saldırganlar

Üretken yapay zeka nispeten yeni olsa da saldırganlar tarafından kullanıldığı birçok olay tespit ettik. Üretken yapay zeka, giriş noktalarında yeterince güçlü önlemler olmaması ve son derece kullanışlı bir araç olması nedeniyle saldırganların ilgisini çekiyor. Tehdit aktörleri; sahte kimlik avi e-postaları hazırlamak, yanlıltıcı kampanyalar yürütmek ve kötü amaçlı komut dosyaları geliştirmek için üretken yapay zekayı kullanıyor. Bu trendin 2025'te de devam edeceğini öngörüyoruz.

- Gerçekçi görüntüler oluşturabilen büyük dil modelleri (LLM) ve üretken yapay zeka modelleri sayesinde yaniltıcı görseller üretmek son derece kolaylaştı. Bu araçlar, sosyal mühendislik girişimlerinde veya bilgi alma operasyonlarında kullanılabilir.
- CrowdStrike, [FAMOUS CHOLLIMA](#) ile **yıl boyunca 304 olayda karşı karşıya geldi**. Bunların **%40'ı iç tehdit olarak sınıflandırıldı**. Saldırılardan bazlarında, saldırgan sahte LinkedIn profilleri oluşturmak için üretken yapay zekadan yararlanmıştır.
- [NITRO SPIDER](#), kötü amaçlı reklam kampanyalarında kullandığı web sitelerini yapay zeka ile oluşturuyor. Hedeflerini kötü amaçlı reklamlar aracılığıyla filtreleyip reklama tıklayan diğer kullanıcıları yapay zeka tarafından oluşturulan sahte sayfalara yönlendiriyor.

## Çin'in Artan Siber Girişimleri

Çin'in siber casusluk girişimleri, 2024'te daha cüretkar hedeflemelere, daha gizli taktiklere ve geniş bir operasyonel kapasiteye ulaşarak kritik bir dönüm noktasına vardı. Bu ilerlemeler; Çin'in bögesel nüfuz, teknoloji edinimi ve rejim istikrarına yönelik tehditlerin bastırılması gibi stratejik istihbarat önceliklerini yansıtıyor.

- Çin bağlantılı saldırganlar, 2024'te küresel ölçekte her sektör ve bölgede faaliyetlerini sürdürdü. Operasyonlarının kapsamı korunurken ölçüği de arttı.
- CrowdStrike, 2024 yılında Çin bağlantılı yedi yeni saldırgan tespit etti. Çin'in saldırıcıları, daha hedefli ve görevde dayalı izler taşıyor. Bu saldırılardan beşi, uzmanlık ve gelişmişlik düzeyi açısından birbirinden farklıydı.
- [LIMAL PANDA](#), [LOCKSMITH PANDA](#) ve [OPERATOR PANDA](#), benzersiz telekom ağı hedefleme görevleri ve araç setlerine sahip, son derece yetenekli saldırganlardır. [VAULT PANDA](#), dünya çapında finansal hizmetler sektörüne odaklanır. [ENVOY PANDA](#) geçmişte başarı düzeyi düşük bir saldırgan olsa da operasyon güvenliğini (OPSEC) önemli ölçüde artırmıştır.

## Bulutu Hedefleyen Saldırganlar Yeni Yöntemler Geliştirmeye Devam Ediyor

Bulut odaklı saldırganlar sistemlere sızmak, sistemler arasında hareket etmek ve veri hırsızlığı ve fidye yazılımı dağıtım gibi kötü amaçlı faaliyetler gerçekleştirmek için kalıcı erişimi sürdürmeye ihtiyaç duyar. Bu amaçla yanlış yapılandırmaları, çalıntı kimlik bilgilerini ve bulut yönetim araçlarını kullanırlar. Çin ve Kuzey Kore bağlantılı aktörler bulut platformlarına yönelik hedeflerini artırırken e-suç grupları, bulut kaynaklarına sızmak için kişiler arası güveni kötüye kullanma ve içерiden tehdit oluşturma gibi gelişmiş taktikler benimsemeye başladı.

- Geçerli hesapların kötüye kullanımı, 2024'ün ilk yarısında **bulut olaylarının %35'ini** oluşturarak bir numaralı ilk erişim taktiği haline geldi. Saldırganlar, gizliliğe yönelik taktikleri giderek daha sık kullanmaya başlıyor ve geçerli hesapları hedef almak için kimlik bilgilerine erişmeye çalışıyor.
- E-suç alanında faaliyet gösteren [SCATTERED SPIDER](#), 2023'teki tüm bulut saldırıcılarının **%30'undan** sorumluydu. Bu sayı **2024'te %13'e** geriledi çünkü birçok ulus-devlet ve fırsatçı tehdit aktörü bulutu hedef almaya başladı.
- Buluta saldıran aktörler, **tespit edilen saldırıcıların %75'inde** tespit edilmekten kaçınmak amacıyla günlüklerdeki göstergeleri kaldırdı.



## Güvenlik Açıklarına Yapılan Yenilikçi Saldırılar

Saldırganlar, uç nokta algılama ve yanıt (EDR) görünürüğünün sınırlı olduğu alanlarda ilk erişimi elde etmeye çalışıyor. Bunun için yerleşik güvenlik açıklarından yararlanabildikleri, internete bağlanan ağ cihazlarını hedef alıyorlar. Kodları uzaktan yürütmek (RCE) için zincirleme saldırısı veya ürünlerin meşru özelliklerini kötüye kullanma gibi teknikler kullanılıyor. Bilinen güvenlik açıkları yeniden kullanılıyor ve aynı cihazlar tekrar tekrar tehlkiye atılıyor. Kullanım ömrü dolmuş cihazların güvenlik açıklarına yama yapılmadığı için saldırırganlar, kolay erişim sağlamak amacıyla bu cihazları hedef alıyor.

- Tehdit aktörleri, ağ cihazının tescilli işletim sistemindeki (OS) güvenlik açıklarına saldırıyor. Bu güvenlik açıkları nedeniyle, aynı işletim sistemindeki birden fazla ürünü hedefleyen saldırırganların tek bir kusuru kötüye kullanması yeterli oluyor.
- Birden fazla zafiyeti birleştiren saldırırganlar, çok sayıda avantaj elde ediyor. İlk olarak, birden fazla açıktan tek bir saldırısında yararlanmak kimliği doğrulanmamış RCE olanağı sunuyor. İkinci olarak, zincirleme kötüye kullanım birçok işletmenin uyguladığı önem düzeyine dayalı yama uygulama sürecini baltalıyor.
- Saldırganlarınümüzdeki yıllarda yeni güvenlik açıklarını keşfetmek veya ürünlerin meşru özelliklerini kötüye kullanmak için teknik bloglarda dikkat çekilen açıkları ve herkese açık POC paylaşımımlarını daha sık kötüye kullanması bekleniyor.

## SaaS'lardaki Kötüye Kullanımın Devam Etmesi Bekleniyor

CrowdStrike Intelligence, 2024'te e-suç ve hedefli saldırının alanlarında faaliyet gösteren birçok saldırırganın sistemler arası hareket, veri gaspı ve üçüncü taraf hedefleme gibi eylemleri kolaylaştıracak verileri elde etmek için bulut tabanlı yazılım hizmeti (SaaS) uygulamalarına saldırıldığını tespit etti. Tehdit aktörleri, bu uygulamalara erişmek için genellikle tek oturum açma (SSO) kimliklerini çaldı. Daha fazla kişi ve işletme bulutu kullanmaya başladıkça saldırırganların da deneyim kazanacağını ve 2025'te SaaS saldırının kritik bir tehdit haline geleceğini öngörüyoruz.

- 2024'ün ilk yarısında buluta saldırın tehdit aktörleri sıklıkla Microsoft 365'i hedef aldı; **saldırıların %22'sinde SharePoint'e, %17'sinde ise Outlook'a erişildi.**
- SCATTERED SPIDER; sohbet, müşteri ilişkileri yönetimi, kimlik bilgisi yönetimi, belge depolama, üretkenlik ve güvenlik araçları da dahil olmak üzere birden çok entegre SaaS uygulamasına erişmek için çalıntı SSO hesapları kullandı.
- Birçok saldırırgan SaaS uygulamalarında şu bilgilere odaklandı: 1) Sistemler arası harekete olanak tanıyan hesap bilgileri ve ağ mimarisine dair belgeler, 2) Gasp sonucunda doğacak hak taleplerini hesaplayabilmek için siber sigorta ve gelir verileri.



# Sonuç

Siber güvenlik alanı, 2025'te de hızla gelişmeye devam edecek. Siber saldırılar, tüm sektörlerde ve coğrafyalarda birbirinden farklı kuruluşları zorlayacak. Saldırganların dayanma, yenilenme ve uyum sağlama becerileri, mevcut tehditlerin her alanda kapsamlı bir şekilde araştırılması gerektiğini gösteriyor.

Saldırganların güvenlik önlemlerini aşmak için yeni ilk erişim yöntemlerini keşfetmesi, 2024'te sosyal mühendislik uygulamalarının yaygınlaşmasına yol açtı. Üretken yapay zeka, özellikle sosyal mühendislik kampanyalarının ve yüksek tempolu istihbarat operasyonlarının (IO) önemli bir parçası haline geldi. CrowdStrike, saldırganların üretken yapay zekayı 2025'te sıkılıkla kullanmasını öngörüyor.

Hedefli e-suç saldırıları, belirli sektörleri tehdit etmeye devam ediyor. Saldırganlar 2024'te gerçekleştirdikleri hedefli saldırırlarda azimleriyle öne çıktı. Hedefleri hakkında yeterince bilgiye sahip olmamaktan doğan sorunları gidermek için kurbanlarının faaliyet gösterdiği sektörü, coğrafyaları ve kullandıkları teknolojileri daha iyi öğrendiler.

2024'te gerçekleşen hedefli saldırılar, dinamik ve yenilikçiydı. Jeopolitik ve stratejik hedeflerine ulaşırken gelişmiş savunma yöntemlerinden kaçınmak için kullandıkları taktikleri uyarladılar. Rusya bağlantılı saldırganlar, Ukrayna'da zafer elde etmek için saldırılarını sürdürdü. Ukrayna ve NATO üyelerini hedef alan istihbarat operasyonlarına odaklandılar. Çin bağlantılı saldırganlar, siber programlara yapılan uzun vadeli yatırımlardan fayda sağlayacak gibi görünüyor. Bunun etkisini artan OPSEC uygulamalarında, uzun süre yüksek tempolu saldırılar gerçekleştirilebilmelerinde ve verimli küresel saldırı faaliyetlerinde göreceğiz.

Güvenlik açığı istismarları, büyük önem arz etmeye devam ediyor. Tehdit aktörlerinin, başta ağ cihazları olmak üzere ağ bağlantısı kurulan her tür cihazı agresif bir şekilde hedef almaya devam etmesi bekleniyor. Saldırganlar, SaaS uygulamalarına büyük bir ilgi gösteriyor. CrowdStrike, e-suç saldırıları ve hedefli saldırılar gerçekleştiren saldırganların bulut tabanlı SaaS uygulamalarına erişim sağlayarak sistemler arası hareketlerde, gasp amacıyla ve üçüncü taraf hedeflemelerinde kullanılacak verileri elde ettiğini gözlemledi. SaaS istismarı, 2025 yılında yakından takip edilmesi gereken bir tehdit olacak gibi görünüyor.

Yenilikçi saldırganlar, 2024 boyunca çeşitli sektörlerde ve coğrafyalarda operasyonlarını geliştirdi ve daha karmaşık hale getirdi. Bu tehditler 2025'te de gelişmeye devam edecek. CrowdStrike'nın Saldırgan Karşıtı Operasyonlar Ekibi, tehdit aktörlerini belirleme, izleme ve engelleme çabalarını mümkün olan her yerde ve her zaman südürecektir.

# Öneriler

1

## Kimlik ekosisteminin tamamında güvenlik sağlayın

Saldırganlar, kullanıcılar arasındaki güven bağını istismar ederek şirket içi, bulut ve SaaS ortamlarında sistemler arası eylemler gerçekleştiriyor. Bunun için kimlik bilgisi hırsızlığı, çok faktörlü kimlik doğrulama (MFA) atlatma ve sosyal mühendislik gibi yöntemlere başvuruluyor. Bu sayede meşru kullanıcıları taklit edebiliyor, erişimlerini artırıyor ve tespit edilmekten kaçınıyorlar.

Kuruluşlar, yetkisiz erişimi önlemek için donanım güvenlik anahtarları gibi kimlik avına dayanıklı MFA çözümlerini benimsemelidir. Tam zamanında erişim, hesapların düzenli olarak incelenmesi ve koşullu erişim kontrolleri de dahil olmak üzere güçlü kimlik ve erişim politikalarından yararlanmak önemlidir. Kimlik tehdidi algılama araçları; ayrıcalık yükseltme, yetkisiz erişim veya arka kapı hesap oluşturma işlemlerini yakalamak için uç noktalardaki ve şirket içi, bulut ve SaaS ortamlarındaki faaliyetleri takip etmelidir. Bu araçların genişletilmiş tespit ve yanıt (XDR) platformlarıyla entegre edilmesi kapsamlı görünürlük sağlar ve saldırganlara karşı birleşik savunma uygulanır.

Ayrıca kuruluşlar, kimlik tabanlı tehditleri proaktif bir şekilde tespit edip bu tehditleri ortadan kaldırırken kullanıcılarını da vishing ve kimlik avı girişimlerini konusunda eğitmeliidir.

2

## Alanlar arasındaki bilgi boşluklarını ortadan kaldırın

Saldırganların klavye üzerinden yapılan saldırının tekniklerine ve meşru araçlara giderek daha fazla başvurması tespit ve müdahale eylemlerini daha da zorlaştırıyor. Geleneksel kötü amaçlı yazılımların aksine bu yöntemler kullanıldığından saldırganlar, komut yürütmek ve olağan işlemleri taklit etmek için meşru yazılımları kullanır ve geleneksel güvenlik önlemlerini kolayca aşar.

Kuruluşların bu tekniğin önüne geçmek için daha modern tespit ve müdahale stratejileri belirlemesi gerekiyor. XDR ve yeni nesil güvenlik bilgisi ve olay yönetimi (SIEM) çözümleri; uç noktalar, ağlar, bulut ortamları ve kimlik sistemleri genelinde birleşik bir görünüm sağlar. Bu sayede analiz uzmanları, şüpheli davranışları birbirleriyle ilişkilendirebilir ve saldırı yolunu tam olarak görebilir.

Proaktif tehdit avcılığı ve tehdit istihbaratı faaliyetleri, olası saldırının modellerini belirleyerek ve saldırganların kullandığı taktikler, teknikler ve prosedürler hakkında analizler sağlayarak tehdit tespitini kolaylaştırır. Gerçek zamanlı istihbarat sayesinde kuruluşlar, tehditler hakkında bilgi sahibi olabilir, saldıruları öngörebilir ve kritik güvenlik faaliyetlerine öncelik verebilir.

3

## Bulutu savunmayı atlamayın

Bulut odaklı saldırganlar sistemlere sızmak, sistemler arasında hareket etmek ve veri hırsızlığı ve fidye yazılımı dağıtım gibi kötü amaçlı faaliyetler gerçekleştirmek için kalıcı erişimi sürdürmeye ihtiyaç duyar. Bu amaçla yanlış yapılandırmaları, çalıntı kimlik bilgilerini ve bulut yönetim araçlarını kullanırlar.

Sistemlerinizi bu tehditlere karşı savunurken bulut algılama ve yanıt (CDR) yeteneklerine sahip bulut tabanlı uygulama koruma platformları (CNAPP'ler) kritik öneme sahiptir.

Bu çözümler, operatörlerin bulutun güvenlik durumuna bütüncül bir bakış atabilmesini sağlar. Yanlış yapılandırmalar, güvenlik açıkları ve saldırıcı tehditleri hızla tespit edilir, önceliklendirilir ve giderilir. Ayrıca, role dayalı erişim ve koşullu politikalar gibi sıkı kontroller uygulandığında kritik sistemlere erişim sınırlanır. Beklenmeyen konumlardan oturum açılması da dahil olmak üzere çeşitli anormal etkinlikler sürekli takip edilir.

Düzenli denetimler de güvenliğin sağlanması kritik öneme sahiptir. Otomatik araçlar, izin konusunda seçici olmayan depolama ayarlarını, açığa çıkan API'leri ve yamalanmamış güvenlik açıklarını ortaya çıkarabilir. Bulut ortamlarının sık sık kontrol edilmesi kullanılmayan izinlerin ve güncel olmayan yapılandırmaların kısa sürede incelenmesini sağlar.

## 4 Saldırgan merkezli bir yaklaşımla güvenlik açıklarını önceliklendirin

Saldırganlar, internet ortamında yayınlanan güvenlik açıklarını giderek daha fazla istismar ediyor. Zincirleme kötüye kullanım yaklaşımıyla birden fazla güvenlik açığını birleştirerek sistemlere hızla erişim elde ediyor, ayrıcalıklarını artırıyor ve savunma önlemlerini aşıyor. Bu çok aşamalı saldırılarda saldırılar, POC (güvenlik açıklarının kullanılmasıyla ilgili bilgiler) ve teknik bloglar gibi kamuya açık kaynakları kötü amaçla kullanarak etkili ve tespit edilmesi zor yükler oluşturuyor.

Kuruluşların bu tehditlere karşı koymak için başta sıklıkla hedef alınan internete bağlı hizmetler (ör. web sunucuları ve VPN ağ geçitleri) olmak üzere kritik sistemlerini düzenli olarak yamalaması veya yükseltilmesi gerekiyor. Zincirleme kötüye kullanımına işaret eden (ör. beklenmeyen çökmelere veya ayrıcalık yükselme) girişimleri takip etmek saldırıcıları erkenden tespit etmeye yardımcı olabilir.

Yerel yapay zeka önceliklendirmesine sahip [CrowdStrike Falcon® Exposure Management](#) gibi araçlar, ekiplerin gürültüyü azaltmasına yardımcı olur. Önemli ve yüksek riskli sistemleri etkileyen kritik güvenlik açıklarına odaklanmasını sağlar. Proaktif güvenlik yaklaşımını benimseyen, saldırı yüzeyindeki güvenlik açıklarını tespit eden ve otomasyondan yararlanan kuruluşlar, karmaşık tehditleri ve saldırı fırsatlarını azaltabilir.

## 5 Saldırganları tanıyın ve hazırlıklı olun

Siber saldırılar dakikalar, hatta saniyeler içinde gerçekleşebilir. Saldırılar hazırlıklı olmak, durumu ilerlemeden kontrol altına almanızı sağlayabilir. İstihbarat odaklı yaklaşımda güvenlik ekipleri sadece saldırı anında karşılık vermekle kalmaz. Kendilerini hedef alan saldırıcıları, saldırının nasıl faaliyet gösterdiğini ve neyi hedeflediğini daha iyi anlar. Tehdit istihbaratı, saldırıcı profillemesi ve yöntem analizi gibi stratejilerden yararlanan güvenlik ekipleri, kullanılacak kaynakları önceliklendirebilir, savunma yöntemini değiştirebilir ve tehditleri gelişmelerine fırsat tanımadan ortadan kaldırabilir. CrowdStrike'nin tehdit istihbaratı hizmeti, bilinen tehditleri tespit etmekle kalmaz. Aynı zamanda yeni ve gelişen yöntemleri de öngörür ve savunma uzmanlarının her zaman bir adım önde olmasını sağlar. Kuruluşlar, istihbaratı güvenlik iş akışlarına sorunsuz bir şekilde entegre ederek tehditlere daha hızlı karşılık verebilir, saldırıcıların etkisini azaltabilir ve istihbaratı eyleme dönüştürebilir.

Kullanılan teknoloji, saldırıcıları tespit etmede ve durdurmadı kritik öneme sahip olsa da güvenlik ihlallerini engelleme konusunda son kullanıcılarla önemli bir rol döşer. Kuruluşlar, kimlik avı ve buna benzer sosyal mühendislik teknikleriyle mücadele etmek için kullanıcı farkındalık programları başlatmalıdır. Güvenlik ekipleri için başarının anahtarı pratik yapmaktır. Siber güvenlik uygulamalarınızda ve müdahalelerinizdeki boşlukları belirlemek ve zayıflıkları ortadan kaldırmak için düzenli tatbikat düzenleyin. Tatbikatlarda ekibinizi ikiye ayırp birbirleriyle mücadele etmelerini isteyebilir ve ardından bulgularınızı tartışabilirisiniz.

# Raporun Tamamını İndirin

CrowdStrike 2025 Küresel Tehdit Raporu, 2024 yılında siber tehdit faaliyetlerinde gözlemlenen önemli eğilimlere ve olaylara dair kapsamlı analizler sunar. Raporu <https://www.crowdstrike.com/global-threat-report/> adresinden ücretsiz olarak indirebilirsiniz.



## CrowdStrike Hakkında

Küresel siber güvenlik lideri [CrowdStrike](#) (Nasdaq: CRWD), kurumsal risklerin kritik alanlarını (ör. uç noktalar ve bulut iş yükleri, kimlik ve veriler) korumak için dünyanın en gelişmiş bulut tabanlı platformıyla modern güvenliği yeniden tanımlamıştır.

CrowdStrike Güvenlik Bulutu ve dünya standartlarındaki yapay zeka ile desteklenen CrowdStrike Falcon® platformu, saldırının gerçek zamanlı göstergelerini, tehdit istihbaratını, gelişen saldırı tekniklerini ve kuruluş genelindeki zenginleştirilmiş telemetriyi kullanarak son derece doğru algılamalar, otomatik koruma ve düzeltme, üst düzey tehdit avcılığı ve güvenlik açıklarının öncelikli gözlemlenebilirliğini sağlar.

Bulutta tek bir hafif aracı mimarisile özel olarak geliştirilen Falcon platformu, hızlı ve ölçülebilir dağıtım, üstün koruma ve performans, azaltılmış karmaşıklık ve anında değer elde etme olanağı sunar.

**CrowdStrike: İhlalleri durduruyoruz.**

Daha fazla bilgi: [www.crowdstrike.com](https://www.crowdstrike.com)

Bizi takip edin: [Blog](#) | [X](#) | [LinkedIn](#) | [Facebook](#) | [Instagram](#) | [YouTube](#)

Bugün ücretsiz denemeye başlayın: [www.crowdstrike.com/free-trial-guide](https://www.crowdstrike.com/free-trial-guide)