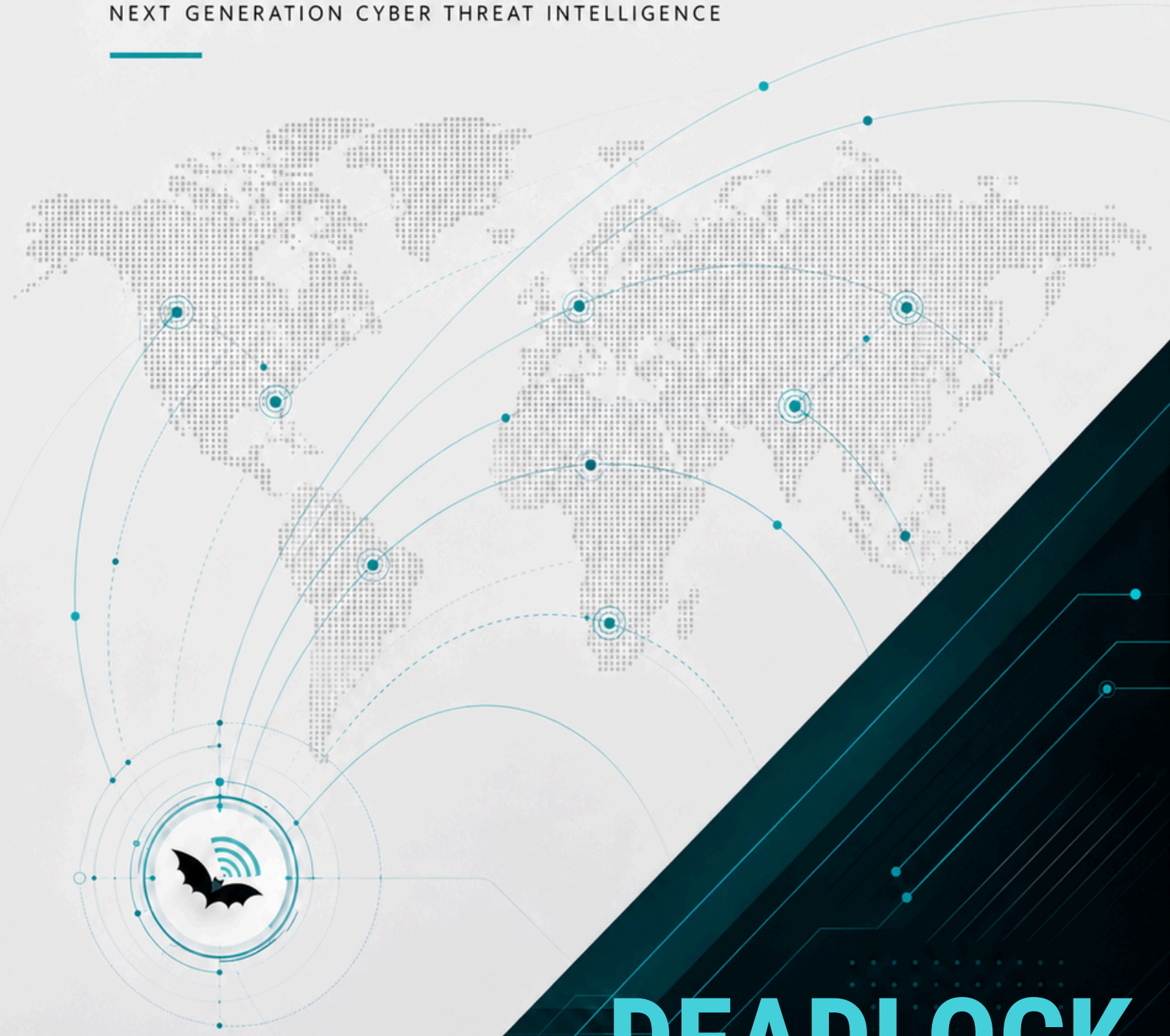
LeakSonar

NEXT GENERATION CYBER THREAT INTELLIGENCE



DEADLOCK

TEHDİT AKTÖRÜ RAPORU

İÇİNDEKİLER

01

YÖNETİCİ ÖZETİ

Bu rapor, DeadLock fidye yazılımı grubunu bir teknik döküm olarak değil, bir karakter olarak anlatmayı amaçlar. Grubun ne yaptığından çok, nasıl bir aktör olduğunu; neyin peşinde olduğunu, kurbanlarına nasıl davrandığını, hangi anlarda hangi hamleyi yaptığını ve bir sonraki hedefinin neye benzeyebileceğini ortaya koyar.

Ne? Mevcut açık kaynak bulguları, DeadLock'un finansal amaçlı bir siber suç operasyonu olduğuna işaret ediyor; bilinen bir devlet veya APT kümesiyle güvenilir bir bağlantı tespit edilmedi.

Nasıl gelişti? Grup 2025 ortasında sessizce ortaya çıktı, bir yıl içinde tekniğini olgunlaştırdı ve 2026 yazında sızıntı sitesinde onlarca kurbanı kamuya açık biçimde listeleyerek daha görünür bir baskı aşamasına geçti.

Şimdi ne yapmalı? Grubun imza hamlelerini tanımak ve aşağıda anlatılan birkaç temel savunma önceliğini hayata geçirmek, bu tehdide karşı en yüksek getiriyi sağlıyor.

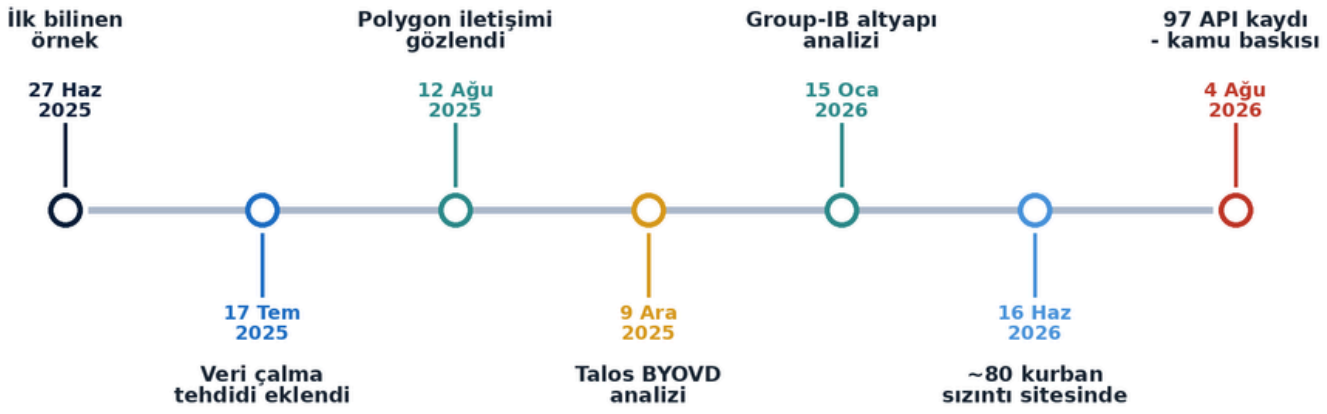
Temel değerlendirme
DeadLock'u ayırt eden şey, güçlü teknik kapasitesi ile zaman zaman görülen operasyonel özensizliğin bir arada bulunmasıdır. Bir yandan güvenlik yazılımını içeriden etkisiz hâle getiren alışılmadık bir yöntem ve blok zinciri üzerinden gizlenen bir iletişim altyapısı kullanır; diğer yandan sızıntı sitesindeki kontrol zafiyetleri, henüz yayınlanmamış kurbanların yanlışlıkla açığa çıkmasına yol açmıştır. Zararlı yazılımın teknik yapısına dair bulgularımız güçlü kanıtlara dayanıyor; ancak kurban sayıları ve olayın kapsamı büyük ölçüde grubun kendi beyanına dayandığından, bu noktada temkinli olmakta fayda var.

Yönetim için karar noktası

En yüksek getirili kontroller karmaşık değildir: zafiyetli sürücülerin engellenmesi, güvenlik yazılımı kapatıldığında anında alarm üreten bir yapı, uzaktan erişim araçlarının sıkı kontrolü, kimlik avına dayanıklı çok faktörlü doğrulama ve **silinemeyen, düzenli test edilen yedekler**. Bu beş başlık, grubun bel bağladığı hamlelerin çoğunu doğrudan işlevsiz bırakır.

2. Grubun Hikâyesi: Sessizlikten Kamu Baskısına

Her tehdit aktörünün bir gelişim çizgisi vardır ve DeadLock'unki oldukça öğreticidir. Grup birdenbire ortaya çıkmadı; adım adım olgunlaştı ve her aşamada daha görünür ve iddialı hâle geldi.



Şekil 1. DeadLock'un açık kaynaklarda gözlenen operasyonel evrimi. Tarihler; örneklerin ilk gözlemlerini, araştırma yayın tarihlerini ve sızıntı sitesi kesitlerini yansıtır.

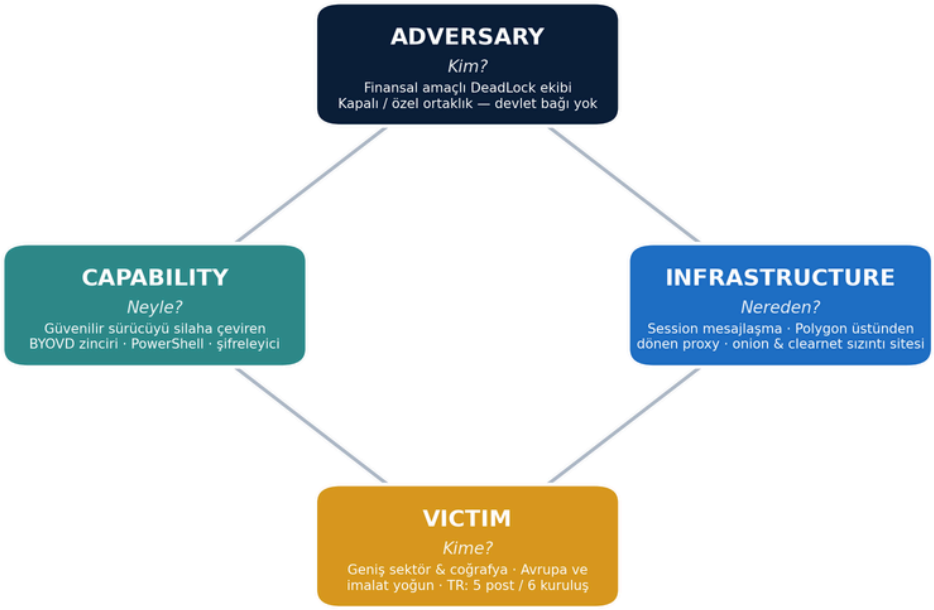
2025 ortasındaki ilk örnekler, grubun şifreleme ailesinin oluşum dönemini gösterir. Ağustos 2025 tarihli örnekte Polygon akıllı sözleşmesi üzerinden Session proxy adresi dağıtımı gözlenmiştir. Aralık 2025'te Cisco Talos, BYOVD tabanlı EDR susturma ve kurtarma önleme zincirini yayımlamış; Ocak 2026'da Group-IB blok zinciri altyapısını ayrıntılı biçimde analiz etmiştir. 2026 yazında ise DeadLock, kurbanları toplu hâlde sızıntı sitesinde listeleyerek klasik **çifte şantaj** baskısını merkezine almıştır.

Analist değerlendirmesi

DeadLock'un düşük görünürlüklü bir şifreleyiciden geniş çaplı bir veri gaspı operasyonuna evrildiği değerlendirilmektedir. 2026 yazındaki ani kurban artışı, hem gerçek büyümeyi hem de geçmiş vakaların geriye dönük toplu listelenmesini birlikte yansıtıyor olabilir; tek başına yüzlerce doğrulanmış ihlal anlamına gelmez.

3. Aktör Profili: Kim Bu Grup?

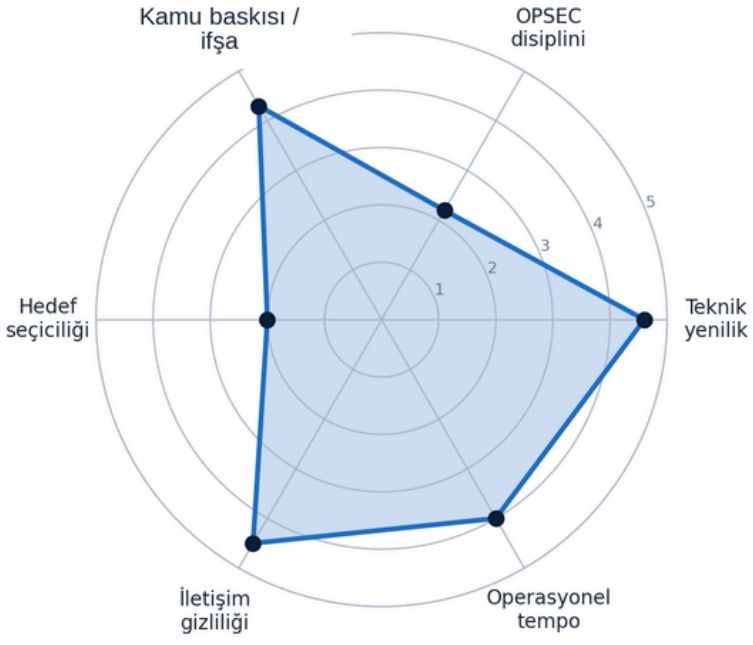
DeadLock'u anlamanın en hızlı yolu, onu dört soruyla tarif etmektir: ***Kim, neyle, nereden ve kime?*** İstihbarat dünyasında buna **Diamond Model** denir — bir aktörü dört köşesiyle bir çırpıda kavramanızı sağlar.



Şekil 2. DeadLock vakasının Diamond Model ile analist sentezi.

Kişilik ve davranış imzası

Bir grubu tanımak, sadece kullandığı araçları bilmek değildir; nasıl *davrandığını* okuyabilmektir. Aşağıdaki profil, DeadLock'un davranışsal eğilimlerini analist değerlendirmesiyle görselleştirir. Grup teknik olarak yenilikçi, iletişimini gizlemeye önem veren ve kamuoyu baskısını yoğun biçimde kullanan bir aktördür; buna karşılık operasyon güvenliği (OPSEC) disiplini değişkendir ve belirli bir sektöre sıkı biçimde bağlı görünmemektedir.



Şekil 3. DeadLock davranışsal imza profili (1 = düşük, 5 = yüksek; analist değerlendirmesi).

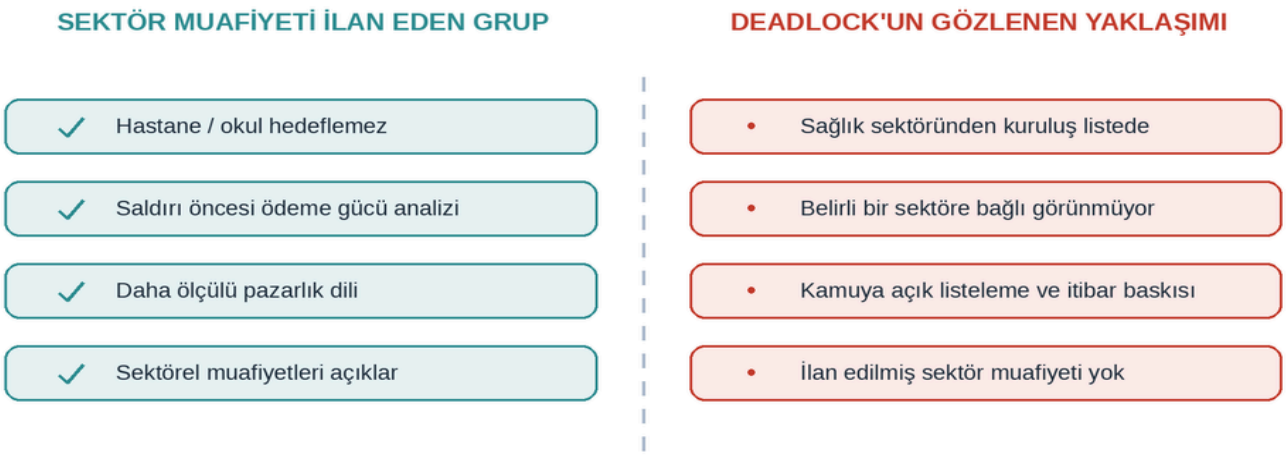
"Bu skorlar nicel bir risk modeli değildir; açık kaynaklarda gözlenen davranışların nitel analist değerlendirmesidir."

Bunun pratikte anlamı

Düşük hedef seçiciliği ve yüksek operasyonel tempo, DeadLock'un fırsat temelli hedeflemeye açık olduğunu düşündürür. Belirli bir sektörde bulunmamak tek başına koruma sağlamaz; grubun geniş bir hedef havuzuna yöneldiği görülmektedir. Bu nedenle savunma, *"bizi hedef alır mı?"* sorusundan çok ***"hamlelerini yakalayabilir miyiz?"*** sorusuna odaklanmalıdır.

Hedef felsefesi ve kronik davranış kalıpları

Bir fidye grubunu gerçekten tanımak, onun *yazılı olmayan kurallarını* okuyabilmektir. Bazı gruplar hastane, okul veya kâr amacı gütmeyen kuruluşlara dokunmayacaklarını açıkça ilan eder ve saldırı öncesi kurbanın **ödeme gücünü** analiz eder — yani planlı bir ticari yaklaşımla hareket ederler. DeadLock'un böyle bir kırmızı çizgi ilan ettiğine dair bir kanıt yoktur; kurban listesinde bir sağlık laboratuvarının bulunması, grubun bu sektörü kategorik olarak dışlamadığını düşündürür.



Şekil 4. Sektör muafiyeti açıklayan bir fidye grubuyla DeadLock'un gözlenen yaklaşımının karşılaştırması.

Şekil 5. Ele geçirilmiş hesaplar ile RDP/AnyDesk erişimleri tamamen temizlenmeden olayın kapatılması yeniden erişim riskini sürdürebilir; bu, DeadLock'a özgü doğrulanmış bir "ısrar döngüsü" değildir.

Grubun teknik yeniliğini operasyon sırasında bıraktığı izlerle birlikte okumak gerekir. Gelişmiş yöntemler kullansa da takip edilebilir izler bırakabilmesi, savunma ekipleri için önemli bir tespit fırsatı oluşturur.

Sınıflandırma Özeti

Aşağıdaki tablo, grubu bir bakışta konumlandırır.

Başlık	Değerlendirme	Güven
Sınıf	Finansal amaçlı fidye yazılımı / veri gaspı operasyonu	**Yüksek**
Motivasyon	Para kazanımı — çifte şantaj (şifreleme + veri ifşası tehdidi)	**Yüksek**
İş modeli	Kamuya doğrulanmış bir ortaklık programı yok; kapalı ekip hipotezi açık	**Orta-Yüksek**
Olgunluk	Teknik yenilik güçlü; sızıntı sitesi ve OPSEC disiplini değişken	**Orta-Yüksek**
Hedefleme	Geniş sektör ve coğrafya; Avrupa ve imalat yoğunluğu belirgin	**Yüksek**
Atıf	Bilinen bir devlet/APT kümesine güvenilir bağ bulunamadı	**Yüksek**

Analitik disiplin
Bu raporda **"aktör iddiası"**, **"bağımsız doğrulama"** ve **"analist değerlendirmesi"** özenle ayrı tutulmuştur. Bir kuruluşun sızıntı sitesinde listelenmesi, tek başına o kurumda ihlal yaşandığını kanıtlamaz.

4. Nasıl Saldırıyor? Adım Adım Bir DeadLock Baskını

DeadLock'un saldırıları rastgele değil, tekrar eden bir *koreografiye* sahiptir. Grubun kronik davranış kalıbını anlamak, onu erken yakalamanın anahtarıdır. Aşağıdaki altı adım, güvenilir teknik araştırmalarda (Cisco Talos, Group-IB) gözlenen tipik akışı, teknik jargondan arındırılmış biçimde özetler.

Not: Grubun ağa ilk nasıl girdiği (phishing mi, VPN açığı mı) güvenilir kaynaklarda doğrulanmamıştır.

Şekil 6. DeadLock'un tipik saldırı zinciri. Grubun ağa ilk girişi güvenilir kaynaklarda doğrulanmamıştır.

En kritik hamle: kalkanı içeriden indirmek

DeadLock'un en ayırt edici hamlesi dördüncü adımdır. Çoğu saldırgan güvenlik yazılımından kaçmaya çalışır; DeadLock ise onu doğrudan **kapatır**. Bunu yaparken de ilginç bir yöntem kullanır: kötü amaçlı bir araç yüklemek yerine, Windows'un *kendi güvenilir kabul ettiği*, ama içinde bir açık barındıran eski bir sürücüyü sisteme sokar ve bu açığı kullanarak güvenlik yazılımını çekirdek seviyesinde sonlandırır.

Güvenlik dünyasında buna **"kendi zafiyetli sürücünü getir"** (BYOVD) denir. Mantığı basittir: bekçi köpeğini dışarıdan bir tehditle değil, bahçe kapısının kendi anahtarıyla etkisiz hâle getirmek. Bu yüzden savunma, *"tanıdığım kötü dosyaları engellerim"* mantığıyla çalışmamalıdır; çünkü kullanılan sürücü teknik olarak **meşrudur**. Doğru yaklaşım, bilinen zafiyetli sürücülerin en baştan yüklenmesini engellemek ve güvenlik yazılımı beklenmedik şekilde susunca **anında alarm üretmektir**.

İlk giriş boşluğu

Grubun ağa *ilk* nasıl girdiği güvenilir kaynaklarda kesinleştirilmemiştir. Cisco Talos'un incelediği tek vakada aktörün fidye yazılımı dağıtımından beş gün önce ağda bulunduğu, ele geçirilmiş geçerli hesap kullanmış olabileceği, RDP erişimini etkinleştirerek TCP/3389 için güvenlik duvarı kuralı açtığı ve şifrelemeden bir gün önce yeni bir AnyDesk kurulumu yaptığı gözlenmiştir. Bunlar vaka-özel bulgulardır; DeadLock'un tüm saldırıları için değişmez bir ilk erişim modeli olarak değerlendirilmemelidir.

5. MITRE ATT&CK Eşleşmesi

DeadLock'un saldırı davranışları MITRE ATT&CK çerçevesiyle eşleştirildiğinde, operasyonun özellikle uzaktan erişim, güvenlik kontrollerini etkisizleştirme, sistem kurtarmasını engelleme ve dosyaları şifreleyerek operasyonel etki oluşturma aşamalarında yoğunlaştığı görülmektedir. Group-IB'nin DeadLock analizinde PowerShell, Windows Command Shell, dosya silme, servis durdurma, sistem kurtarmasını engelleme, AnyDesk kullanımı ve veri şifreleme davranışları ATT&CK teknikleriyle doğrudan eşleştirilmiştir. Cisco Talos'un incelediği vakada ise RDP kullanımı, güvenlik duvarı değişiklikleri ve BYOVD yoluyla EDR süreçlerinin sonlandırılması gibi ek davranışlar gözlenmiştir.

TAKTİK	TEKNİK	DEADLOCK'TAKİ KARŞILIĞI
EXECUTION	T1059.001 - PowerShell	Şifreleme öncesi PowerShell betikleriyle güvenlik, yedekleme ve bazı servisler durdurulur.
EXECUTION	T1059.003 - Windows Command Shell	CMD/batch dosyaları çalıştırılarak saldırı hazırlığı ve ransomware yürütme işlemleri gerçekleştirilir.
COMMAND & CONTROL	T1219.002 - Remote Desktop Software	AnyDesk, saldırganın uzaktan ve kalıcı erişim sağlaması için kullanılır.
LATERAL MOVEMENT	T1021.001 - Remote Desktop Protocol	Talos vakasında RDP etkinleştirilmiş; mstsc üzerinden ağ içindeki sistemlere erişim denenmiştir.
DEFENSE IMPAIRMENT	T1685 - Disable or Modify Tools	BYOVD ve zafiyetli Baidu sürücüsü kullanılarak EDR süreçleri sonlandırılmış; Defender korumaları devre dışı bırakılmıştır.
DEFENSE IMPAIRMENT	T1686.003 - Windows Host Firewall	Talos vakasında TCP/3389 için gelen RDP trafiğine izin veren yeni Windows güvenlik duvarı kuralı oluşturulmuştur.
IMPACT	T1489 - Service Stop	Güvenlik, yedekleme ve bazı uygulama servisleri durdurularak şifreleme öncesi savunma kapasitesi azaltılır.
IMPACT	T1490 - Inhibit System Recovery	Volume Shadow Copy ve yedekler hedef alınarak sistemin fidye ödemeden geri yüklenmesi zorlaştırılır.
IMPACT	T1486 - Data Encrypted for Impact	Dosyalar şifrelenir, .dlock uzantısı eklenir ve erişimin geri verilmesi karşılığında fidye talep edilir.

Analist değerlendirmesi

ATT&CK; eşleşmesi, DeadLock'un şifrelemeden önce savunmayı sistematik biçimde zayıflattığını gösterir. En değerli tespit noktaları; EDR süreçlerinin beklenmedik sonlanması, yeni AnyDesk kurulumu, RDP/3389 kural değişiklikleri, Volume Shadow Copy silme ve toplu servis durdurmadır. İlk erişim yöntemi kesinleştirilmediği için T1078 - Valid Accounts bu tabloda kesin DeadLock davranışı olarak gösterilmemiştir.

6. Gizli İletişim: Blok Zinciri Neden Devrede?

Sıradan bir suç grubu, kurbanla pazarlık için sabit bir adres kullanır - bu adres tespit edilip kapatılabilir. DeadLock, sabit bir adrese bağlı kalmak yerine iletişim adresini **Polygon blok zinciri** üzerindeki bir akıllı sözleşmeden alır.

Kurban tarafındaki proxy adresi sorgusu, zincir üzerinde yeni işlem oluşturmayan ve ağ ücreti gerektirmeyen bir *eth_call* okuma çağrısıdır. Buna karşılık aktörün proxy adresini değiştirmek için kullandığı *setProxy* işlemi zincir üstü bir işlem gerektirir, düşük de olsa ücretlidir ve herkese açık işlem geçmişinde iz bırakır. Merkezi bir alan adına bağlı olmaması altyapının engellenmesini zorlaştırsa da faaliyet tamamen görünmez değildir. Group-IB'nin analizine göre bu mekanizma, **Session** tabanlı mesajlaşma akışına değiştirilebilir bir proxy adresi sağlar.

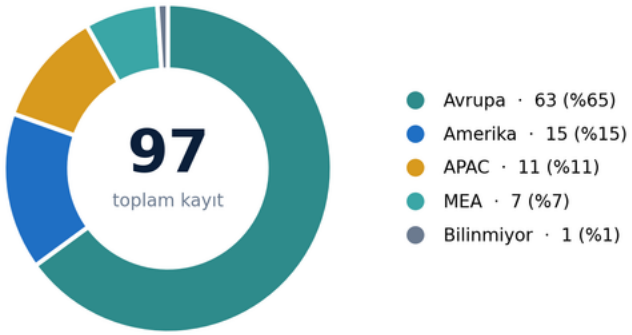
Şekil 7. Fidye notundan gizli mesajlaşmaya uzanan iletişim zinciri. Ortadaki blok zinciri halkası, adresin istendiği an değiştirilmesine izin verir.

Savunma çıkarımı

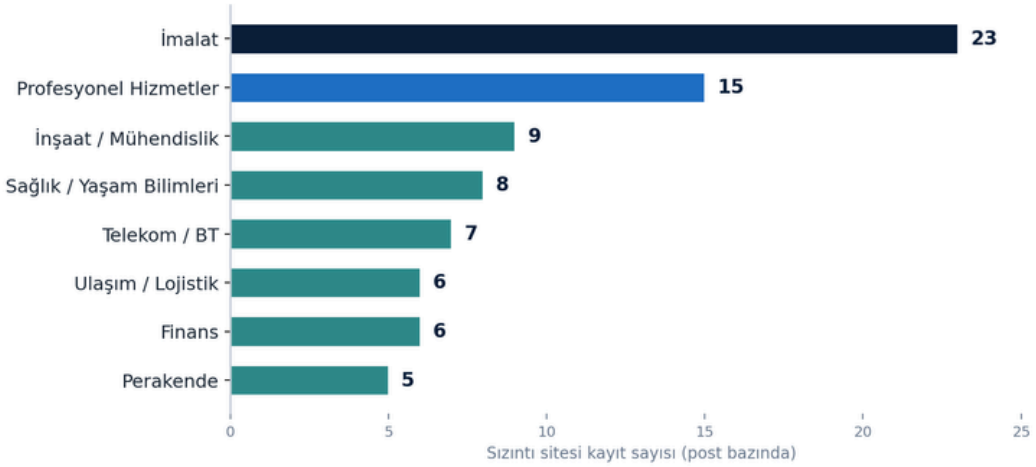
Tek bir adresi engellemek yetersizdir. Bunun yerine **davranış** izlenmelidir: bir kurumsal makinenin beklenmedik biçimde blok zinciri servisleriyle konuşmaya başlaması, fidye notu dosyalarının belirmesi ve Session trafiği — bunlar tek tek masum görünse de, bir arada güçlü bir alarm sinyalidir.

7. Hedef Profili ve Kurban Dağılımı

Grubun kimi hedef aldığı, niyetini okumanın bir başka yoludur. DeadLock'un sızıntı sitesindeki 4 Ağustos 2026 kesitinde 97 kayıt bulunmaktadır. Bu kayıtların coğrafi ve sektörel dağılımı, grubun **Avrupa ve imalat** ağırlıklı bir yoğunlaşma sergilediğini gösterir.



Şekil 8. 97 kaydın analist-normalize bölgesel dağılımı. Bir kayıt birden fazla kuruluş içerebilir; değerler aktör iddiasıdır.



Şekil 9. Sektörel yoğunluk. İmalat, 23 kayıtla açık ara en büyük kategoridir; profesyonel hizmetler ve mühendislik onu takip eder.

Bu dağılım dikkat çekicidir. İmalat ve mühendislik kuruluşları, hem üretim sürekliliğine bağımlı oldukları için *fidyeye açık*, hem de tasarım, sözleşme ve tedarik zinciri verileri nedeniyle *gasp için değerli* hedeflerdir. DeadLock'un geniş hedefleme yaklaşımıyla birleştiğinde, bu sektörlerdeki orta-büyük ölçekli kurumlar öncelikli risk grubunu oluşturur.

Sayım notu

Bölge ve sektör grafikleri kayıt (post) bazındadır. Bir sızıntı kaydı birden fazla kuruluş içerebileceğinden, kuruluş sayısı ile kayıt sayısı birebir örtüşmez.

Güncel bir örnek: her yeni ilan bir kanıt değildir

Grubun temposunu somutlaştırmak için yakın tarihli bir örnek: açık kaynak izleme kayıtlarına göre DeadLock, 10 Temmuz 2026'da **ONE Contact** adlı kuruluşu sızıntı sitesine kurban olarak eklemiştir. Ancak bu ilan yayımlandığında; saldırının yöntemi, dosyaların şifrelenip şifrelenmediği, veri çalınıp çalınmadığı ve etkilenen verinin büyüklüğü hakkında **kamuya açık hiçbir doğrulama yoktu**.

Bu, tüm rapor boyunca vurguladığımız ilkenin canlı bir örneğidir: bir kurumun adının sızıntı sitesinde belirmesi, o kurumda başarılı bir saldırı gerçekleştiğini ***kanıtlamaz***. Bu tür ilanlar çoğu zaman, kurumu, müşterilerini ve yatırımcılarını — henüz hiçbir inceleme tamamlanmadan — ciddi bir hasar yaşandığına inandırmaya yönelik bir **psikolojik baskı aracıdır**. Doğru refleks paniklemek değil, teknik kanıt aramaktır.

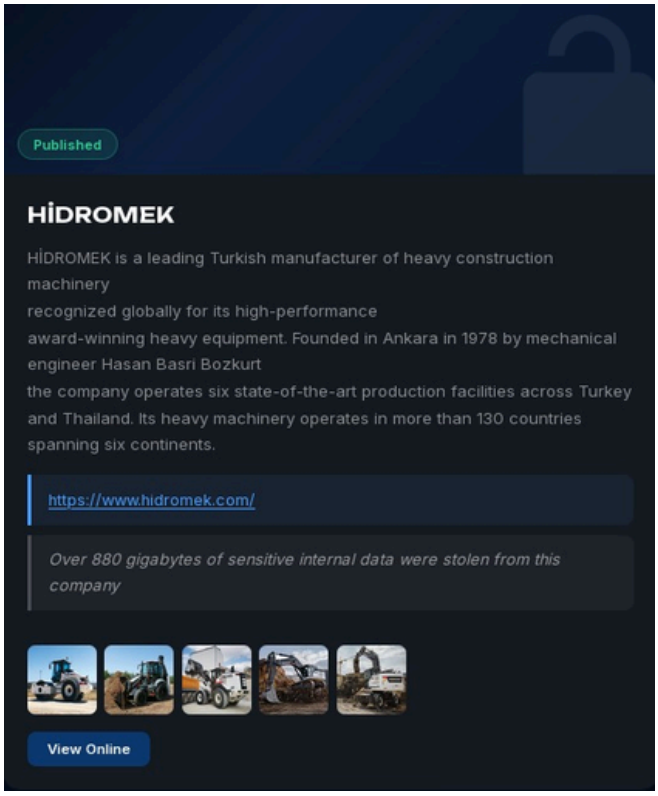
Şekil 10. Bir sızıntı sitesi ilanının kanıtladığı ile kanıtlamadığı şeylerin ayrımı.

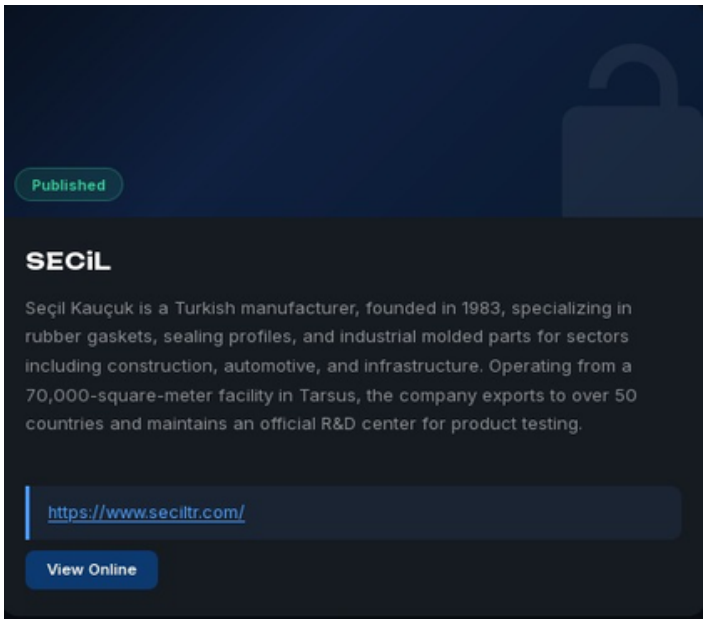
8. Türkiye'ye Bakan Yüzü

DeadLock'un sızıntı sitesinde, Türkiye bağlantılı altı kuruluş beş ayrı kayıtta yer almaktadır. Bu kuruluşların tamamı **aktör iddiasıdır**; yani grubun beyanına dayanır ve hiçbiri bağımsız olarak doğrulanmış bir ihlal anlamına gelmez.

Şekil 11. DeadLock sızıntı sitesinde listelenen Türkiye bağlantılı kuruluşlar (aktör iddiası).

Sağlık sektöründe faaliyet göstermesi nedeniyle, hassas sağlık verilerinin etkilenmesi durumunda gizlilik etkisi yüksek olabilir. Ancak mevcut açık kaynak bulguları etkilenen veri türlerini doğrulamamaktadır.. Maxplast ve Senoco ise tek bir kayıtta birlikte listelenmiştir. Bu birlikteliğin nedeni açık kaynak bulgularıyla belirlenememiştir.





Örnek vaka: HİDROMEK ve "880 GB" iddiası

HİDROMEK vakasında grubun iddia ettiği 880 GB'lık veri hacmi doğrulanamamış olsa da, yapılan inceleme sızıntının içeriğine dair önemli bulgular ortaya koymuştur. Sızdırıldığı öne sürülen veri kümesi içerisinde çalışanlara ait OneDrive yedeklerine, kişisel indirilenler ve masaüstü klasörlerine ait dosyalara erişilebildiği tespit edilmiştir. Bu içerikler arasında şirket içi yazışmalar, tedarikçilerle yapılan belge alışverişleri ve makine çizimleri gibi hassas nitelikte materyaller de yer almaktadır. Dolayısıyla kurban kaydındaki görsellerin bir kısmının kamuya açık ürün fotoğraflarıyla örtüşmesi, iddianın bütünüyle asılsız olduğu anlamına gelmemektedir; toplam veri hacmi teyit edilememiş olsa da, sızıntının gerçek ve hassas kurumsal veri içerdiği gözlemlenmiştir.

Sonuç
HİDROMEK kaydında aktör kimliğine güvenimiz **"yüksek"**, ancak 880 GB'lık veri hırsızlığı iddiası doğrulanmamıştır.

Türkiye bağlantılı kuruluşlar — özet

Kuruluş	Sektör	Kanıt durumu
AHENK Laboratuvarı	Tıbbi / teşhis laboratuvarı	Yayımlanmış kayıt; bağımsız teyit yok
HİDROMEK	Ağır iş makineleri imalatı	Yayımlanmış kayıt; 880 GB iddiası doğrulanmadı
Seçil Kauçuk	Endüstriyel kauçuk / sızdırmazlık	Yayımlanmış kayıt; kapsam doğrulanmadı
Maxplast	Plastik ambalaj	Senoco ile tek postta; teyit yok
Senoco Nonwoven	Nonwoven tekstil imalatı	Maxplast ile aynı post; teyit yok
Güven Müh. Makina	Özel amaçlı makine imalatı	Yayımlanmış kayıt; teyit yok

Sınıflandırma notu
Kurum adları grubun sızıntı sitesi beyanıdır. Sektör bilgileri kuruluşların kamuya açık tanımlarına dayanır. Aktif tarama yapılmamış, hiçbir kurumun sistemine erişilmemiştir.

9. İddia ile Gerçeği Ayırmak

Fidye yazılımı gruplarının en güçlü silahlarından biri **abartıdır**. Kurbanı korkutmak ve pazarlık gücünü artırmak için ele geçirdikleri veriyi, erişim süresini ve yetkilerini olduğundan büyük gösterirler. Bir istihbarat raporunun görevi, bu gürültüyü ayıklayıp *elimizde gerçekten ne olduğunu* söylemektir.

Şekil 12. DeadLock hakkındaki aktör iddiaları ve doğrulanmamış çıkarımlar (solda) ile bağımsız gözlemler (sağda) ayrımı.

Sağ sütundaki maddeler - güvenlik yazılımının içeriden susturulması, blok zinciri tabanlı iletişim, **.dlock** şifreleme ailesi ve 97 kaydın sızıntı sitesi/API kesitinde bulunması - bağımsız teknik araştırmalar veya birincil koleksiyonla **gözlemlenmiştir**. Sol sütundaki 880 GB veri açıklaması aktör beyanıdır; 97 kaydın 97 doğrulanmış ihlal anlamına geldiği yorumu ise mevcut kanıtlarla **desteklenmeyen bir çıkarımdır**. Karar alırken bu kategorileri birbirine karıştırmamak gerekir.

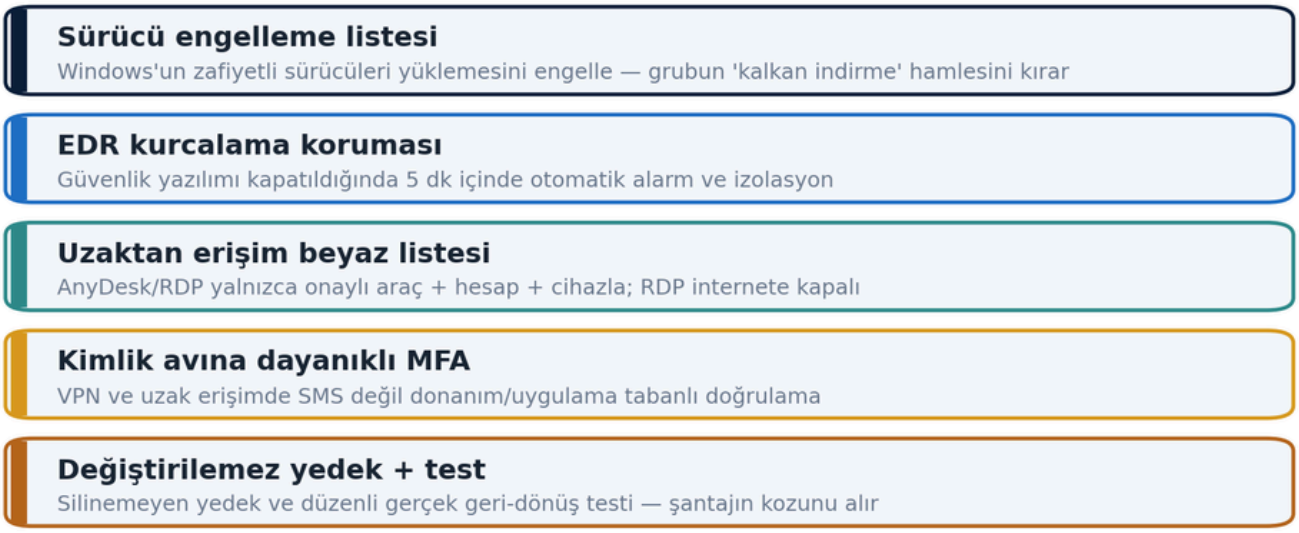
10. Risk Değerlendirmesi ve Savunma Öncelikleri

DeadLock'un oluşturduğu riski değerlendirirken iki boyutu ayırmak gerekir: **olasılık** (bizi vurma ihtimali) ve **etki** (vurursa ne kaybederiz). Grubun Türkiye görünürlüğü henüz sınırlı olduğundan olasılık orta seviyededir; ancak başarılı bir saldırının operasyonel etkisi — üretim durması, yedeklerin yok edilmesi, veri ifşası — **çok yüksektir**. Bu, DeadLock'u orta olasılıklı ancak çok yüksek etkili bir tehdit hâline getirir.

Boyut	Puan	Gerekçe
Olasılık	3 / 5	Türkiye bağlantılı tekrar eden görünürlük var; kuruluş-özel aktif gösterge yok
Operasyonel etki	5 / 5	Güvenlik yazılımı susturma, servis durdurma, yedek silme ve şifreleme
Gizlilik etkisi	4 / 5	Veri çalma/ifşa iddiaları; kapsam vaka bazında doğrulanmamış
Tedarik zinciri	4 / 5	İmalat ve mühendislik kurumlarında iş ortağı verisi riski
Tespit zorluğu	4 / 5	Meşru sürücü/araç ve blok zinciri tabanlı gizlenme
Genel risk	**YÜKSEK**	**Orta olasılık, çok yüksek etki — etki odaklı yüksek risk**

Beş öncelikli savunma hamlesi

İyi haber şu: DeadLock'un bel bağladığı hamlelerin çoğu, birkaç temel kontrolle doğrudan kırılabilir. Aşağıdaki beş başlık, en yüksek getiriyi sağlayan önlemlerdir.



Şekil 13. DeadLock'a karşı en yüksek getirili savunma öncelikleri.

Uygulama yol haritası

Öncelikleri zamana yayarak uygulanabilir adımlara dönüştüren örnek bir plan aşağıdadır.

Zaman	Aksiyon	Başarı ölçütü
İlk 24 saat	Bilinen zararlı dosya izlerini tara; şüpheli makineleri doğrula ve izole et	Şüpheli hostların tespiti ve izolasyonu
İlk 72 saat	Uzaktan erişim araçlarının envanterini çıkar; yetkisiz kurulumları kaldır	Her uzak erişim aracının sahibi belli
İlk 72 saat	İnternete açık uzak masaüstü (RDP) noktalarını incele ve kapat	İnternete açık RDP = 0
İlk hafta	Zafiyetli sürücü engelleme listesini ve uygulama kontrolünü devreye al	Test sürücüsü başarıyla engellendi
İlk hafta	Güvenlik yazılımı susunca <5 dk içinde alarm/izolasyon otomasyonu kur	Ölçülen alarm süresi < 5 dakika
İlk hafta	Silinemeyen (immutable) yedek al ve gerçek geri-dönüş testi yap	Başarılı restore ve ölçülmüş RTO/RPO
İlk ay	Uzak erişim ve VPN için kimlik avına dayanıklı çok faktörlü doğrulama	Ayrıcalıklı erişimde %100 kapsam

11. Sonuç

DeadLock, teknik kapasitesi yüksek ancak disiplini değişken, para odaklı ve fırsat temelli hedeflemeye açık bir fidye yazılımı operasyonudur. Grubun hikâyesi, sessiz bir başlangıçtan daha görünür bir kamu baskısı aşamasına doğru evrilen tanıdık bir yayı izler; ayırt edici imzası ise güvenlik yazılımını *içeriden* susturması ve iletişimini blok zinciri üzerine taşımasıdır.

Bu raporun en önemli mesajı, **iddia ile gerçeği ayırmaktır**. Grubun sızıntı sitesindeki kayıtları — Türkiye bağlantılı kuruluşlar dâhil — birer hedef ilanıdır; hiçbiri tek başına o kurumların doğrudan ihlal edildiğini, sistemlerinin şifrelendiğini kanıtlamaz. 880 GB gibi veri hacmi açıklamaları ve kurban kartlarında yer alan olay kapsamı iddiaları, bağımsız olarak doğrulanana kadar **aktör beyanı** olarak değerlendirilmelidir.

Buna karşılık, grubun temel teknik davranışları iyi belgelenmiştir ve tam da bu, savunma için en değerli bilgidir. DeadLock vakalarında gözlenen temel hamleleri - kalkanı içeriden indirmek, yedekleri yok etmek, veriyle şantaj yapmak - tanıyan bir kurum, onu erkenden yakalayabilir. Zafiyetli sürücü engelleme, güvenlik yazılımı sağlık takibi, uzak erişim kontrolü, dayanıklı çok faktörlü doğrulama ve **silinemeyen yedekler** - bu beş kontrol, grubun operasyon zincirinin önemli bir bölümünü bozar.

Son değerlendirme
DeadLock tamamen öngörülemez bir tehdit değildir; anlaşılır kalıpları vardır ve bu nedenle savunulabilir. Onu yalnızca teknik ayrıntılardan oluşan bir liste olarak değil, davranışları okunabilir bir aktör olarak ele almak, hem doğru önceliklendirmeyi hem de sağlam bir müdahaleyi mümkün kılar.

Kaynaklar ve güven notu

Teknik bulgular Cisco Talos ve Group-IB araştırmalarına; zafiyet ayrıntısı resmî kayıtlara (NIST NVD); davranış eşlemeleri MITRE ATT&CK çerçevesine; kurban ölçeği ise ZeroFox, WatchGuard ve 4 Ağustos 2026 tarihli birincil sızıntı sitesi kesitine dayanır. Güncel kurban iddiaları (örneğin ONE Contact) ThreatMon'un açık kaynak sızıntı sitesi izlemesinden alınmıştır.

Bu raporun **profilleme yaklaşımı** — aktörü bir teknik döküm yerine davranışları okunabilir bir karakter olarak ele almak — Curated Intelligence'ın "Threat Actor Profile Guide" metodolojisinden ve Mandiant'ın APT41 gibi köklü aktör profillerinden ilham almıştır. Canlı sızıntı sitesi hızla değişebileceğinden, tüm sayısal bulgular 4 Ağustos 2026 kesitini temsil eder; sonraki değişiklikler raporun tarihsel doğruluğunu etkilemez.

12. Kaynakça

01 **Cisco Talos Intelligence Group**
Dunk, J. & Raghuprasad, C.
NewBYOVD LoaderBehind DeadLock Ransomware Attack.
TEKNİK ARAŞTIRMA — 9 Aralık 2025

02 **Group-IB**
Eizaguirre,X.
DeadLock Ransomware: Smart Contracts for Malicious Purposes.
TEKNİK ARAŞTIRMA — 15 Ocak 2026

03 **NIST NVD**
CVE-2024-51324.
ZAFİYET KAYDI — Sürekli güncellenir

04 **MITRE**
MITREATT&CK - Enterprise Matrix.
ÇERÇEVE — Sürekli güncellenir

05 **ZeroFox Intelligence**
Flash Report: DeadLock'sRansomware Leak Site Lists over 80 Victims.
TEHDİT İSTİHBARATI — 29 Haziran 2026

06 **WatchGuard Threat Lab**
RansomwareTracker - DeadLock.
TEHDİT İSTİHBARATI — Sürekli güncellenir

07 **DeadLock Data Leak Site / API**
LeakSonar CTI Birincil Koleksiyonu.
BİRİNCİL KOLEKSİYON — 4 Ağustos 2026

08 **DeadLock - HİDROMEK**
KurbanKaydı veAktörTarafından Paylaşılan Materyallerin İncelemesi.
BİRİNCİL KOLEKSİYON — 4 Ağustos 2026

09 **Curated Intelligence**
TheThreatActorProfileGuide for CTI Analysts.
METODOLOJİ — 13 Temmuz 2023

10 **Mandiant**
Fraser, N. et al.
APT41:ADualEspionage and Cyber Crime Operation.
METODOLOJİ — 7 Ağustos 2019

Güven notu

Bu raporun **profilleme yaklaşımı** — aktörü bir teknik döküm yerine davranışları okunabilir bir karakter olarak ele almak — Curated Intelligence'ın "Threat Actor Profile Guide" metodolojisinden ve Mandiant'ın APT41 gibi köklü aktör profillerinden ilham almıştır. Canlı sızıntı sitesi hızla değişebileceğinden, tüm sayısal bulgular 4 Ağustos 2026 kesitini temsil eder; sonraki değişiklikler raporun tarihsel doğruluğunu etkilemez.