# HACKER GRUBU ARAŞTIRMASI

# “AKİRA RANSOMWARE”

**Hazırlayan:** Onur Ege Tarhan

**Öğrenci No:** 125692029

# 1. Giriş

Bu çalışma kapsamında 2023 yılından itibaren küresel ölçekte etkili olan Akira Ransomware grubu incelenmektedir. Akira yalnızca teknik bir fidye yazılımı grubu olarak değil, aynı zamanda mağdurlar üzerinde hukuki, ekonomik ve operasyonel sonuçlar doğuran bir siber suç yapılanması olarak ele alınacaktır.

## 1.1 Akira'nın Kimliği

Akira, 2023 yılının ilk aylarından itibaren gözlenen bir ransomware grubudur. Kaynaklarda Akira Ransomware Group, GOLD SAHARA, PUNK SPIDER ve Howling Scorpius gibi adlarla da anılmaktadır.[1] Yapılan değerlendirmelerde grubun ransomware-as-a-service modeliyle çalıştığı, yani fidye yazılımı altyapısını farklı saldırganlara kullandırdığı belirtilmektedir. Bu modelde çekirdek grup yazılım, sızıntı sitesi, ödeme kanalları ve pazarlık altyapısını sağlarken; saldırganlar ilk erişim, yatay hareket ve saldırının fiilen icrası aşamalarında rol oynayabilmektedir.

Grubun motivasyonu ideolojik veya siyasi olmaktan çok finansaldır. Eylem modeli, mağdurun iş sürekliliğini bozmak, veri gizliliğini tehdit etmek ve itibar baskısı yaratmak üzerine kuruludur. Bu nedenle Akira'yı sıradan bir zararlı yazılım ailesi olarak değil, teknik araçları olan bir ekonomik suç organizasyonu olarak ele almak daha isabetlidir.

## 1.2 Faaliyet Alanı ve Hedef Profili

Akira'nın hedefleri tek bir ülke veya sektörle sınırlı değildir. CISA ve FBI'nın ortak danışma metnine göre Akira, Kuzey Amerika, Avrupa ve Avustralya'daki birçok işletme ve kritik altyapı kuruluşunu etkilemiştir.[2] FortiGuard verileri, grubun otomotiv, enerji, eğitim, bilgi teknolojileri, finans, sağlık, kamu, üretim, telekomünikasyon, taşımacılık ve perakende gibi çok sayıda sektöre yöneldiğini göstermektedir.[3]

Bu tablo, Akira'nın belli bir ideolojik hedefin peşinde koşmadığını daha çok zayıf halka neredeyse oraya yöneldiğini göstermektedir. Güvenlik açığı, zayıf kimlik doğrulama, açık uzaktan erişim servisi ve ödeme kapasitesi gibi fırsat unsurlarına göre hareket ettiğini düşündürmektedir. Başka bir ifadeyle Akira'nın mağdur seçimi, çoğu zaman mağdurun kim olduğundan çok, sistemin ne kadar erişilebilir ve saldırıdan sonra ne kadar ödeme baskısına açık olduğuyla ilgilidir.

## 1.3 Eylem Türleri

### 1.3.1 İlk Erişim

Akira olaylarında ilk erişim için en sık görülen kanallardan biri, çok faktörlü kimlik doğrulama kullanılmayan VPN servisleridir. FBI ve siber güvenlik araştırmacıları, bazı olaylarda Cisco ürünlerine ilişkin bilinen zafiyetlerin ve tek faktörlü uzak erişim mekanizmalarının istismar

---

[1] FortiGuard Labs, "Akira Ransomware - Threat Actor", https://www.fortiguard.com/threat-actor/6049/akira-ransomware

[2] FBI, CISA, EC3 ve NCSC-NL, "#StopRansomware: Akira Ransomware", Product ID: AA24-109A, 18.04.2024, https://www.ic3.gov/CSA/2024/240418.pdf

[3] FortiGuard Labs, "Akira Ransomware - Threat Actor", https://www.fortiguard.com/threat-actor/6049/akira-ransomware

edildiğini belirtmektedir.[4] Bunun yanında RDP gibi dışa açık servisler, kimlik bilgisin kötüye kullanımı ve hedefli oltalama yöntemleri de saldırı zincirinde yer alabilmektedir.

Bu aşamadaki hukuki sorun, yetkisiz erişim fiilinin çoğu hukuk sisteminde başlı başına suç teşkil etmesidir. Türk hukuku bakımından bu fiil, somut olaya göre TCK m.243'teki bilişim sistemine girme veya orada kalmaya devam etme suçunu gündeme getirebilir. Eğer sistemdeki veriler bozulmuş, yok edilmiş, değiştirilmiş veya erişilemez hale getirilmişse TCK m.244 de devreye girebilir.

### 1.3.2 Kalıcılık, Keşif ve Yetki Yükseltme

İlk erişimin ardından saldırganların ağ içinde kalıcılık sağlamaya ve yetkilerini artırmaya çalıştığı görülmektedir. Ortak danışma metninde Akira aktörlerinin alan adı denetleyicileri üzerinde yeni hesaplar oluşturduğu, LSASS bellek alanı gibi kaynaklardan kimlik bilgisi toplamaya çalıştığı, Mimikatz ve LaZagne gibi araçları kullandığı ve ağ keşfi için SoftPerfect, Advanced IP Scanner ve Windows komutlarından yararlandığı belirtilmektedir.[5]

Bu aşama, saldırının yalnızca tek bir kullanıcı hesabını ele geçirmekten ibaret olmadığını gösterir. Asıl amaç, kurum ağı içinde daha geniş yetkiler elde etmek, kritik sunuculara erişmek, yedekleri bulmak ve daha sonra gerçekleştirilecek şifreleme ile veri sızdırma aşamalarının etkisini artırmaktır.

### 1.3.3 Veri Dışarı Aktarma ve Çift Yönlü Şantaj

Akira'nın en belirgin yönü çift yönlü şantaj modelidir. Bu modelde veriler şifrelenmeden önce dışarı aktarılır. Daha sonra mağdur hem sistemlerine erişememe hem de verilerinin yayımlanması riskiyle karşı karşıya bırakılır. Ortak danışma metni, Akira aktörlerinin FileZilla, WinRAR, WinSCP ve RClone gibi araçlarla veri dışarı aktardığını; AnyDesk, MobaXterm, RustDesk, Ngrok ve Cloudflare Tunnel gibi araçları komuta kontrol veya dışarı aktarma aşamasında kullandığını belirtmektedir.[6]

Çift yönlü şantaj, ransomware olaylarının hukuki niteliğini ağırlaştırmaktadır. Çünkü şirketler açısından sorun yalnızca iş sürekliliği kaybı değildir; kişisel verilerin ifşası, ticari sırların kaybı, müşteri güveninin zedelenmesi, düzenleyici kurum bildirimleri, idari para cezaları ve özel hukuk sorumluluğu gibi sonuçlar da doğmaktadır.

### 1.3.4 Şifreleme ve İş Sürekliliğinin Bozulması

Akira, Windows sistemlerinin yanı sıra Linux ve sanallaştırma altyapılarını da hedef alabilmektedir. MITRE, Akira'nın C++ ile yazılmış varyantlarının yanı sıra ESXi sistemlerini hedef alan varyantlarına işaret etmektedir.[7] 2025 tarihli güncellenmiş danışma metninde ise Akira'nın Nutanix

---

[4] FBI, CISA, EC3 ve NCSC-NL, "#StopRansomware: Akira Ransomware", Product ID: AA24-109A, 18.04.2024, https://www.ic3.gov/CSA/2024/240418.pdf

[5] FBI, CISA, EC3 ve NCSC-NL, "#StopRansomware: Akira Ransomware"

[6] FBI, CISA, EC3 ve NCSC-NL, "#StopRansomware: Akira Ransomware"

[7] MITRE ATT&CK, "Akira, Software S1129", https://attack.mitre.org/software/S1129/

AHV sanal makine disk dosyalarını da şifrelediği ve kabiliyetini VMware ESXi ile Hyper-V dışına taşıdığı belirtilmiştir.[8]

Sanallaştırma altyapısının hedeflenmesi, saldırının etkisini büyütür. Çünkü tek bir fiziksel ana sistem üzerindeki birden çok sanal sunucu aynı anda etkilenebilir. Bu durum özellikle finans, sağlık, kamu hizmetleri ve üretim gibi kesintiye tahammülü düşük sektörlerde ciddi operasyonel risk yaratır.

## 1.4 Bilinen Olaylar ve Mağdurlar

Aşağıdaki tablo, Akira ile ilişkilendirilen bazı olayları özetlemektedir. Bu liste tüm olayları kapsamamaktadır; amaç, grubun hedef yelpazesini ve hukuki etkilerini somutlaştırmaktır.

| Tarih | Olay veya Şirket Adı | Kısa açıklama | Hukuki önem |
|---|---|---|---|
| 2023 | Stanford University olayı | Stanford Department of Public Safety ağına yetkisiz erişim iddiası ve veri sızıntısı açıklamaları kamuya yansımıştır.[9] | Eğitim kurumu verileri, kişisel veri ve güvenlik verisi riski |
| Aralık 2023 | Nissan Australia ve Nissan Financial Services | Avustralya ve Yeni Zelanda'daki yerel sunuculara yetkisiz erişim sonucunda yaklaşık 100.000 kişinin etkilenebileceği açıklanmıştır.[10] | Kimlik belgeleri, finansal bilgiler, bildirim yükümlülüğü ve itibar zararı |
| Ocak 2024 | Tietoevry İsveç veri merkezi | Tietoevry, İsveç'teki bir veri merkezinin Akira ransomware saldırısına maruz kaldığını ve bazı müşteri hizmetlerinin | Tedarik zinciri, bulut hizmetleri ve kritik hizmet sürekliliği sorunu |

[8] FBI, CISA, DC3, HHS ve diğer kurumlar, "#StopRansomware: Akira Ransomware", güncellenmiş danışma metni, 13.11.2025, https://www.ic3.gov/CSA/2025/251113.pdf, erişim tarihi: 26.05.2026.

[9] EdScoop, "Stanford failed to detect fall cyberattack for 4 months", 14.03.2024, https://edscoop.com/stanford-university-akira-cyberattack-ransomware-2024/, erişim tarihi: 26.05.2026.

[10] NSW Government, ID Support NSW, "Nissan Motor Corporation and Nissan Financial Services data breach", 15.03.2024, https://www.nsw.gov.au/departments-and-agencies/id-support-nsw/learn/data-breaches/data-breach-announcements/nissan-data-breach, erişim tarihi: 26.05.2026.

| | | | |
|---|---|---|---|
| | | etkilendiğini duyurmuştur.[11] | |
| Nisan 2024 | Ortak kamu danışma metni | FBI, CISA, EC3 ve NCSC-NL Akira'ya ilişkin teknik ayrıntıları ve önlemleri yayımlamıştır.[12] | Kamu otoritelerinin ortak tehdit istihbaratı ve savunma tavsiyesi |
| Kasım 2025 | Güncellenmiş danışma metni | Akira'nın sanallaştırma altyapılarına yönelik kabiliyetinin genişlediği belirtilmiştir.[13] | Sanallaştırma, yedekleme ve iş sürekliliği risklerinin artması |

Bu örnekler, Akira'nın yalnızca teknoloji şirketlerini hedef almadığını göstermektedir. Bir otomotiv finans şirketi, bir üniversite, bir veri merkezi veya bir kamu hizmeti tedarikçisi aynı saldırı modelinden etkilenebilir. Dolayısıyla Akira'nın önemi teknik karmaşıklığından kadar, farklı sektörlerde zincirleme hukuki sonuç üretme kapasitesinden de kaynaklanmaktadır.

## 1.5 Akira'nın Siber Suç Ekonomisindeki Yeri

Ransomware faaliyetleri artık tek bir kişinin geliştirdiği ve rastgele gönderdiği zararlı yazılımlar olmaktan çıkmıştır. Akira örneğinde görüldüğü üzere, modern ransomware grupları pazarlık kanalı, sızıntı sitesi, kripto varlıkla ödeme alma, bağlı saldırgan ağı, teknik destek ve veri yayımlama tehdidi gibi işlevleri olan bir organizasyon gibi çalışmaktadır. TRM Labs, Akira'nın 2025 yılında yüksek fidye geliri elde eden gruplar arasında öne çıktığını ve 2025 yılı itibarıyla yüzlerce mağdurun sızıntı sitesinde yer aldığını belirtmektedir.[14]

Bu durum, hukuki mücadelenin yalnızca zararlı yazılım dosyasını tespit etmekle çözülemeyeceğini gösterir. Kripto varlık akışlarının izlenmesi, kara para aklama bağlantıları, fidye ödemelerinin yaptırım hukukuyla ilişkisi, uluslararası adli yardımlaşma, delil muhafazası ve mağdur bildirim süreçleri aynı dosyanın parçası haline gelir.

---

[11] Tietoevry, "Tietoevry: Ransomware attack in Sweden - restoration work progressing", 22.01.2024, https://www.tietoevry.com/en/newsroom/all-news-and-releases/press-releases/2024/01/tietoevry-ransomware-attack-in-sweden–restoration-work-progressing/, erişim tarihi: 26.05.2026.

[12] FBI, CISA, EC3 ve NCSC-NL, "#StopRansomware: Akira Ransomware", Product ID: AA24-109A, 18.04.2024, https://www.ic3.gov/CSA/2024/240418.pdf, erişim tarihi: 26.05.2026.

[13] FBI, CISA, DC3, HHS ve diğer kurumlar, "#StopRansomware: Akira Ransomware", güncellenmiş danışma metni, 13.11.2025, https://www.ic3.gov/CSA/2025/251113.pdf, erişim tarihi: 26.05.2026.

[14] TRM Labs, "Akira Ransomware Group: Threat Profile and TTPs", 20.03.2026, https://www.trmlabs.com/resources/intel-library/akira, erişim tarihi: 26.05.2026.

## 1.6 Akira'nın Doğurduğu Hukuki Sorunlar

### 1.6.1 Bilişim Sistemine Yetkisiz Erişim ve Sistemin İşleyişinin Bozulması

Akira saldırılarında ilk aşamada sisteme yetkisiz erişim sağlanmaktadır. Türk hukuku açısından bu aşama TCK m.243 kapsamında değerlendirilebilir. Saldırı sonucunda sistem verileri bozulur, yok edilir, değiştirilir veya erişilemez hale getirilirse TCK m.244 gündeme gelir. Ransomware olaylarında şifreleme, çoğu kez verilerin teknik olarak silinmemesine rağmen mağdur bakımından erişilemez hale gelmesi sonucunu doğurur. Bu nedenle TCK m.244 bakımından "erişilebilirliğin ortadan kaldırılması" yönü özellikle önemlidir.

### 1.6.2 Kişisel Verilerin Hukuka Aykırı Olarak Ele Geçirilmesi ve Yayılması

Ransomware olaylarında kişisel veriler saldırı zincirinin merkezine yerleşmiştir. Bir mağdur kuruluşun müşteri kayıtları, çalışan bilgileri, kimlik belgeleri, finansal verileri veya sağlık verileri dışarı aktarılabilir. Bu durumda TCK m.136'daki kişisel verileri hukuka aykırı olarak verme, yayma veya ele geçirme suçu gündeme gelebilir. KVKK bakımından ise veri sorumlusunun güvenlik tedbirleri, ihlal bildirimi ve ilgili kişileri bilgilendirme yükümlülükleri tartışılır.

7545 sayılı Kanun m.16/4 ise bu noktada daha özel bir sorun alanını hedeflemektedir. Sızıntı nedeniyle siber uzayda yer alan kişisel veya kritik kamu hizmeti kapsamındaki kurumsal verilerin izinsiz şekilde erişime açılması, paylaşılması ya da satışa çıkarılması. Akira'nın sızıntı sitesi üzerinden veri yayımlama tehdidi, bu hükmün pratik karşılığını açık biçimde gösterir.[15]

### 1.6.3 Şantaj, Yağma ve Dolandırıcılık Tartışmaları

Ransomware olaylarında saldırgan, mağdura fiilen "ödeme yapmazsan verini yayımlar ve sistemlerini çalışamaz halde bırakırım" mesajı vermektedir. Bu davranış, farklı hukuk sistemlerinde şantaj, gasp, haraç alma, bilgisayar suçları veya dolandırıcılık başlıkları altında ele alınabilmektedir. Türk hukuku bakımından somut olayın özelliklerine göre TCK'daki şantaj hükümleri, nitelikli dolandırıcılık veya bilişim suçlarıyla birlikte değerlendirme yapılması gerekebilir. Ancak ransomware olaylarının kendine özgü niteliği, mevcut klasik suç tiplerinin her zaman yeterli açıklığı sağlamadığını göstermektedir.

### 1.6.4 Fidye Ödemesi ve Yaptırım Hukuku

Fidye ödemesi yapmak mağdur açısından kısa vadede sistemi kurtarma aracı gibi görülebilir ancak ödeme, saldırgan ekosistemini finanse eder. Ayrıca bazı ülkelerde ödeme yapılan kişi veya grubun yaptırım listelerinde bulunması, mağdurun ek hukuki risklerle karşılaşmasına neden olabilir. Akira bakımından açık kaynaklar farklı değerlendirmeler içerse de genel ransomware literatürü, fidye ödemelerinin yaptırım ve kara para aklama hukuku bakımından dikkatle değerlendirilmesi gerektiğini göstermektedir.

---

[15] 7545 sayılı Siber Güvenlik Kanunu, m.16/4, Resmi Gazete, 19.03.2025, sayı 32846.

### 1.6.5 Sınır Aşan Delil ve Yetki Sorunu

Akira gibi gruplar bir ülkedeki mağdura, başka ülkelerdeki sunucular, kripto varlık cüzdanları, VPN altyapıları ve forum hesapları üzerinden saldırabilir. Bu nedenle soruşturma bakımından ülkesel yetki, delilin bulunduğu yer, log kayıtlarının saklanması, uluslararası adli yardımlaşma ve özel sektör siber güvenlik şirketlerinden bilgi alınması gibi konular kritik hale gelir.

### 1.6.6 Sigorta, Sözleşme ve Tedarik Zinciri Sorumluluğu

Tietoevry örneği, saldırının yalnızca doğrudan mağduru değil, mağdurun hizmet verdiği müşterileri de etkileyebileceğini göstermektedir.[16] Bu tür olaylarda hizmet seviyesi taahhütleri, veri işleyen ve veri sorumlusu ilişkisi, bulut hizmet sağlayıcısının güvenlik taahhüdü, dış hizmet sözleşmeleri, mücbir sebep savunması ve siber sigorta poliçeleri birlikte değerlendirilmelidir.

## 1.7 Sonuç

Akira örneği, modern ransomware gruplarının yalnızca teknik bir tehdit olmadığını göstermektedir. Yetkisiz erişim, veri dışarı aktarma, şifreleme, fidye talebi, veri yayımlama tehdidi, kripto varlıkla ödeme alma ve uluslararası gizlenme davranışları tek bir operasyon zinciri içinde birleşmektedir. Bu nedenle Akira'nın faaliyetleri bilişim ceza hukuku, kişisel verilerin korunması hukuku, siber güvenlik mevzuatı, özel hukuk sorumluluğu ve uluslararası ceza iş birliği alanlarını aynı anda ilgilendirmektedir.

[16] Tietoevry, "Tietoevry: Ransomware attack in Sweden - restoration work progressing", 22.01.2024, https://www.tietoevry.com/en/newsroom/all-news-and-releases/press-releases/2024/01/tietoevry-ransomware-attack-in-sweden–restoration-work-progressing/

# 2 Kaynakça


- 7545 sayılı Siber Güvenlik Kanunu, Resmi Gazete, 19.03.2025, sayı 32846.
- FBI, CISA, EC3 ve NCSC-NL, “#StopRansomware: Akira Ransomware”, Product ID: AA24-109A, 18.04.2024.
- FBI, CISA, DC3, HHS ve diğer kurumlar, “#StopRansomware: Akira Ransomware”, güncellenmiş danışma metni, 13.11.2025.
- FortiGuard Labs, “Akira Ransomware - Threat Actor”.
- MITRE ATT&CK, “Akira, GOLD SAHARA, PUNK SPIDER, Howling Scorpius, Storm-1567, Group G1024”.
- MITRE ATT&CK, “Akira, Software S1129”.
- EdScoop, “Stanford failed to detect fall cyberattack for 4 months”, 14.03.2024.
- NSW Government, ID Support NSW, “Nissan Motor Corporation and Nissan Financial Services data breach”, 15.03.2024.
- Tietoevry, “Tietoevry: Ransomware attack in Sweden - restoration work progressing”, 22.01.2024.
- TRM Labs, “Akira Ransomware Group: Threat Profile and TTPs”, 20.03.2026.