

OdinEye®



2025
BLACKSHRANTAC:
RANSOMWARE THREAT ANALYSIS

İçindekiler

Giriş	3
Genel Bakış	4
Hedef ve Kurban Analizi	7
Teknik Analiz	9
Vaka İncelemeleri	13
Teknik Göstergeler	25
Sonuç ve Öneriler	26
Kaynakça	29

Giriş

Siber tehdit dünyası, geleneksel fidye yazılımlarının (ransomware) sadece dosya şifrelemeye odaklandığı dönemden, çok daha karmaşık ve tespiti zor olan "veri odaklı şantaj" (data extortion) modellerine doğru evrilmektedir. Bu dönüşümün en güncel ve agresif örneklerinden biri olan **BlackShrantac**, 2025 yılının son çeyreğinde siber tehdit sahnesine çıkararak özellikle kritik altyapı, üretim ve teknoloji sektörlerini hedef alan küresel bir risk unsuru haline gelmiştir. 17 Eylül 2025 tarihinde ilk faaliyetleri tespit edilen ve kısa süre içerisinde Amerika Birleşik Devletleri, Hindistan ve Türkiye başta olmak üzere dünya genelinde 35 doğrulanmış saldırıyla imza atan grup, operasyonel hız ve etkinlik açısından dikkat çekici bir profil çizmektedir. Klasik fidye yazılımı gruplarının aksine, BlackShrantac operasyonlarında dosya şifreleme adımını büyük ölçüde devre dışı bırakarak kaynaklarını doğrudan terabaytlarca hassas verinin ağ dışına sızdırılmasına (exfiltration) odaklamaktadır; bu durum, grubun temel motivasyonunun sistemleri çalışmaz hale getirmekten ziyade, kurumsal verinin gizliliğini ihlal ederek şantaj yoluyla finansal kazanç sağlamak olduğunu göstermektedir.

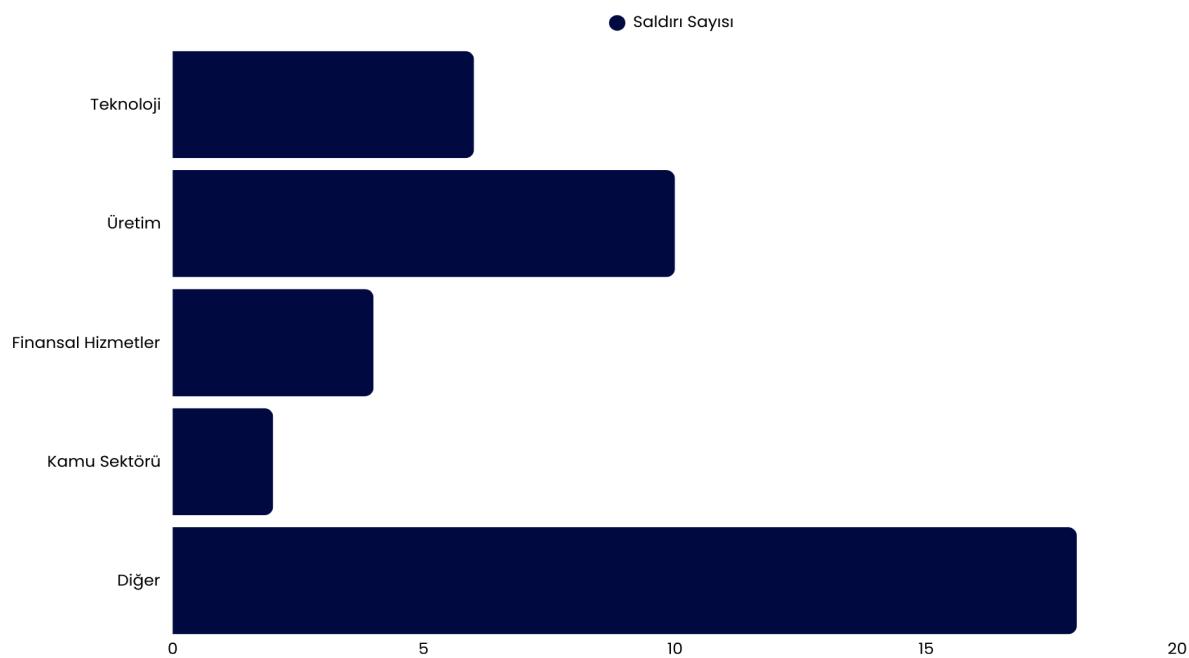
Bu rapor; BlackShrantac tehdit grubunun taktik, teknik ve prosedürlerini (TTP), hedef profillerini ve operasyonel kapasitesini kapsamlı bir şekilde analiz ederek, kurumların güvenlik ekiplerine (SOC/CSIRT) ve üst düzey yöneticilerine (CISO) eyleme geçirilebilir istihbarat sağlamak amacıyla hazırlanmıştır. Raporun hazırlanmasında kullanılan metodoloji, çok katmanlı bir veri doğrulama sürecine dayanmaktadır. Analizler; açık kaynak istihbaratı (OSINT), teknik analiz raporları ve en önemlisi **tehdit aktörlerine ait ifşa platformlarından (Dark Web) elde edilen birincil verilerin** incelenmesiyle oluşturulmuştur. Özellikle grubun jeopolitik sınır tanımaksızın Rusya Federasyonu dahil olmak üzere geniş bir coğrafayı hedef alması ve Türkiye'nin küresel ölçekte en çok saldırıyla uğrayan üçüncü ülke konumunda bulunması, bu raporu yerel kuruluşlar ve kritik altyapı işletmecileri için hayatı bir savunma kaynağı haline getirmektedir. Bu doküman, tehdidin sadece tanımını yapmakla kalmayıp, tespit edilen zararlı yazılım imzaları, ağ altyapısı ve saldırı vektörleri üzerinden somut savunma stratejileri sunmayı hedeflemektedir.

Genel Bakış

BlackShrantac, 17 Eylül 2025 tarihinde siber tehdit sahnesine çıkan ve finansal motivasyonla hareket eden yeni nesil bir siber suç örgütüdür. Grub, 2025 yılının son çeyreğinde agresif bir büyümeye stratejisi izlemiştir; Eylül ayında başlayan operasyonlarını Ekim ayında zirve noktasına taşıyarak kısa sürede küresel çapta tanınırlık kazanmıştır.

Aralık 2025 itibarıyla grup tarafından gerçekleştirildiği doğrulanın **35 başarılı saldırı** bulunmaktadır. BlackShrantac, hedef seçiminde "Büyük Av" (Big Game Hunting) stratejisine benzer bir yol izlese de, kurban profilini sadece Fortune 500 şirketleriyle sınırlı tutmayıp; verisi kritik olan KOBİ'leri, hukuk bürolarını ve üretim tesislerini de fırsatçı bir yaklaşımla hedef almaktadır. Grubun operasyonel durumu şu an itibarıyla **Aktif (Active)** statüsündedir.

Grubun kurban profili incelendiğinde, rastgele saldırılar yerine **Teknoloji** ve **Üretim** gibi katma değeri yüksek sektörlerde odaklandığı görülmektedir. Aşağıdaki grafik, saldırıların sektörel yoğunluğunu özetlemektedir:



Şekil 1: BlackShrantac Saldırılarının Doğrulanmış Sektörel Dağılımı (2025)

1. Tehdit Profili ve Motivasyon

BlackShrantac, kendisini "karanlık, kapüşonlu bir avatar" ile görselleştirmekte ve siber yeraltı dünyasında korku unsuru yaratmaya çalışmaktadır. Grubun hedef kitlesi incelemişinde, geleneksel fidye yazılımı gruplarının aksine (Örn: REvil, DarkSide) politik veya coğrafi "kırmızı çizgileri" olmadığı görülmektedir.

Özellikle Bağımsız Devletler Topluluğu (CIS) ülkelerine saldırmama kuralını ihlal ederek **Rusya Federasyonu**'ndaki kurumları hedef almaları, grubun devlet destekli (State-Sponsored) bir yapıdan ziyade, tamamen finansal kazanç odaklı, bağımsız ve kuralsız bir "Paralı Asker" (Mercenary) yapısında olduğunu göstermektedir. Küresel saldırı trafiğinde **Amerika Birleşik Devletleri (7 saldırı)** ve **Hindistan (6 saldırı)** başı çekerken, **Türkiye (4 saldırı)** grubun en yoğun faaliyet gösterdiği üçüncü ülke konumundadır.

2. Operasyonel Model: Şifrelenmesiz Gasp (Non-Encryption Extortion)

BlackShrantac'ı günümüz tehdit ortamında (Threat Landscape) farklı kılan en kritik özellik, saldırının zincirindeki (Kill Chain) **dosya şifreleme adımını atlama** eğilimidir. Grup, kurbanın sistemlerini kilitleyip operasyonu durdurmak yerine; ağ içerisinde sessizce ilerleyerek (Lateral Movement) Terabayt (TB) boyutlarına varan hassas veriyi dışarı sızdırarak ve "Veri İfşası" üzerinden şantaj yapmaktadır.

Bu "Saf Veri Gaspi" (Pure Data Extortion) modelinin kanıtları, Türkiye'deki saldırılarda net bir şekilde görülmektedir:

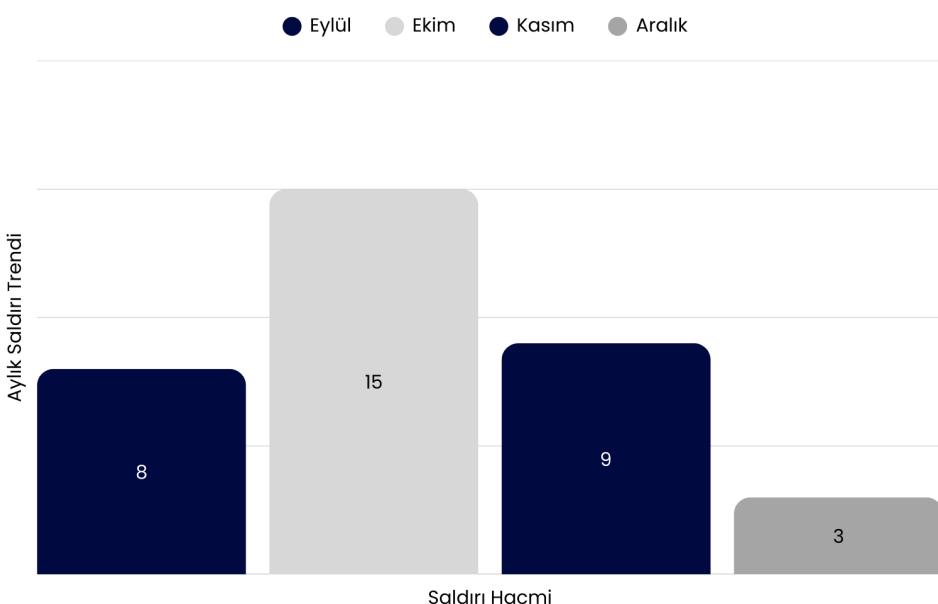
- **Dem İlaç:** 1 TB boyutunda AR-GE ve formül verisi sızdırılmıştır.
- **Rasen İnşaat:** 400 GB boyutunda stratejik şirket verisi ve çalışan bilgileri ele geçirilmiştir.
- **Şimşek A.Ş.:** 200 GB boyutunda lojistik ve dağıtım ağı verisi sızdırılmıştır.

Bu yöntem, grubun güvenlik yazılımlarının (Antivirüs/EDR) "fidye yazılımı davranışlarını" (dosya şifreleme vb.) tespit etmesini zorlaştırmakta ve saldırının fark edilme süresini (Dwell Time) uzatmaktadır.

Analist Notu : "Saf Veri Gaspi" (Pure Data Extortion), tehdit aktörlerinin kurbanın dosyalarını şifreleyerek erişimi engellemek yerine, veriyi çalıp ifşa etmekle tehdit ettiği bir siber suç taktigidir. Bu modelde birincil risk "Veri Kaybı" (Data Loss) değil, "**Veri Gizliliği İhlali**"dir (**Confidentiality Breach**). Dolayısıyla, kurumların güvendiği geleneksel "Yedekleme" (Backup) stratejileri, veriler kilitlenmediği ancak çalındığı için bu senaryoda bir pazarlık kozu olmaktan çıkar.

3. Operasyonel Büyüme ve Saldırı Hızı

Grup, 2025 yılının son çeyreğinde agresif bir büyümeye stratejisi izlemiştir. Eylül ayında başlayan keşif ve ilk saldırı dalgası, Ekim ve Kasım aylarında zirve noktasına ulaşmıştır. Aşağıdaki grafik, grubun aylar bazında artan saldırı hacmini özetlemektedir:



Şekil 2: BlackShrantac Aylık Saldırı Trendi (Eylül – Aralık 2025)

Grafikte görülen Ekim ayındaki ani artış, grubun altyapısını tamamlayıp "toplu saldırı" (mass exploitation) aşamasına geçtiğini işaret etmektedir. Aralık 2025 itibarıyla toplam **35 doğrulanmış kurban** bulunmaktadır ve grup "Aktif" statüsünü korumaktadır.

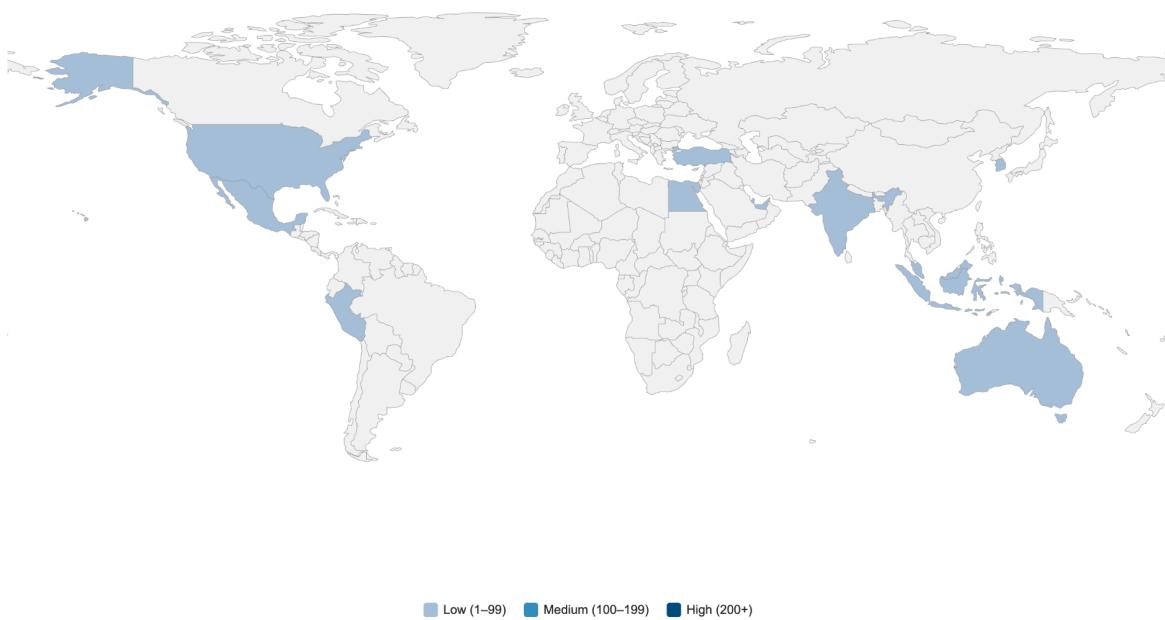
Hedef ve Kurban Analizi

BlackShrantac grubunun operasyonel verileri, grubun sadece mevcut kurbanları değil, gelecekteki hedef hacmini de gözler önüne sermektedir. Bu bölüm, grubun küresel erişimini ve sizıntı platformu üzerindeki iddialarının gerçek boyutunu analiz etmektedir.

1. Jeopolitik Hedefleme ve Küresel Erişim

Grubun coğrafi dağılımı, jeopolitik sınır tanımayan bir yapıya sahip olduğunu kanıtlamaktadır.

- Kritik Bölgeler:** En yüksek saldırı hacmi **ABD (7)** ve **Hindistan (6)** üzerinde yoğunlaşıırken, **Türkiye (4)** grubun en çok hedef aldığı üçüncü ülke konumundadır.
- Geniş Menzil:** Doğrulanmış kurban listesinde Meksika, Peru, Endonezya, Güney Kore, BAE, Katar, Malezya, Mısır ve Avustralya gibi stratejik ülkeler yer almaktadır.
- Sınır Tanımayan Tehdit:** Grubun **Rusya Federasyonu**'ndaki kurumları hedef listesine dahil etmesi, bölgesel koruma kurallarına uymadığını ve tamamen finansal odaklı olduğunu göstermektedir.

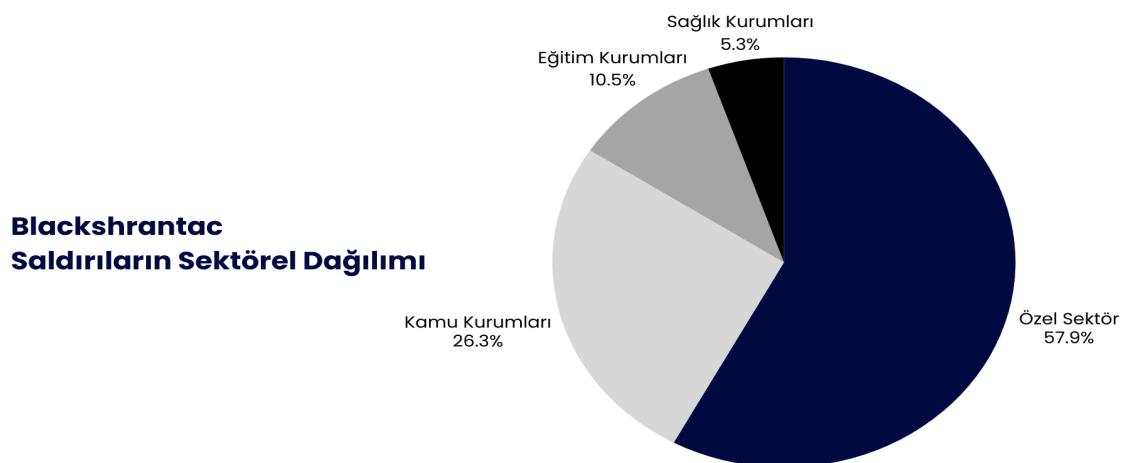


Şekil 3: Black Shrantac Operasyonlarının Dünya Genelindeki Etki Alanı

2. Operasyonel Ölçek: Doğrulanmış ve İddia Edilen Saldırılar

Grubun sizıntı paneli verilerine göre, gerçekleşen operasyonlar ile iddia edilen hacim arasında büyük bir fark bulunmaktadır. Bu durum grubun "tehdit enflasyonu" yaratarak kurbanlar üzerinde psikolojik baskı kurduğunu göstermektedir.

- Genel Tehdit Hacmi:** Grup tarafından gerçekleştirildiği kesinleşen **38 doğrulanmış (verified)** saldırısı bulunurken; panellerinde henüz kanıtlanmamış **621 doğrulanmamış (unverified)** saldırısı kaydı yer almaktadır.
- Doğrulama Oranı:** Toplam iddiaların sadece yaklaşık **%5.7**'si doğrulanmış durumdadır.



Şekil 4: BlackShrantac Saldırılarının Sektörel Dağılımı

3. Sektörel Dağılım ve Gerçek Yüzdeler

38 doğrulanmış saldırının kurumsal sınıflara göre dağılımı, grubun hedefleme stratejisinin gerçek yüzünü yansımaktadır:

- Özel Sektör (Businesses):** Doğrulanmış saldırıların **%57.9'u (22 saldırısı)** doğrudan özel şirketleri hedef almaktadır.
- Kamu Kurumları (Public Institutions):** Saldırıların **%26.3'ü (10 saldırısı)** kamu yönetimlerini hedef almıştır.
- Eğitim Kurumları (Educational Institutions):** Toplam payı **%10.5'tir (4 saldırısı)**.
- Sağlık Kurumları (Healthcare Institutions):** En düşük pay ile **%5.3 (2 saldırısı)** oranında hedeflenmiştir.

4. Kritik Sektörel Dikey Hedefler

Grup, bu ana sınıflar içerisinde özellikle şu dikey sektörlerle odaklanmaktadır:

- Sanayi ve Teknoloji:** Teknoloji (6), Üretim (5) ve Bilgisayar Tasarım Hizmetleri.
- Kritik Altyapı ve Hizmetler:** Enerji, İnşaat, Tekstil Üretimi ve Hukuk Büroları.
- Tarım:** Bitkisel Üretim (Crop Production) ve Tarım/Ormancılık faaliyetleri.

Teknik Analiz

Bu bölüm, Black Shrantac grubunun operasyonel altyapısını, saldırı döngüsünü ve grubun "Saf Veri Gaspi" (Pure Data Extortion) modelini nasıl yürüttüğünü teknik detaylarıyla ele almaktadır. Analizimiz, aktörün kullandığı yöntemlerin tespiti ve etkisiz hale getirilmesi için kritik bilgiler içermektedir.

1. Grubun Operasyonel Geçmişi ve Aktivite Analizi

Black Shrantac grubuna dair ilk teknik bulgular 2025 yılının başında gözlemlenmiştir. Grubun aktivite grafiği, standart fidye yazılımı gruplarından farklı olarak belirgin dalgalanmalar göstermektedir:

- Erken Dönem Faaliyetleri:** Grup, Ocak 2025'te 7 doğrulanmış saldırı ile sahneye çıkmış, Şubat ayında ise saldırı hacmini 15'e çıkararak ilk büyük zirvesini yaşamıştır.
- Yeniden Yapılanması ve İkinci Dalga:** Mart ve Ağustos ayları arasında saldırı hacmi düşüş gösterse de, grup Eylül ayı itibarıyla yeniden aktifleşmiştir.
- Mevcut Durum:** 17 Eylül 2025 tarihinde "Aktif" olarak sınıflandırılan grup, Ekim 2025'te tekrar 15 saldırılık bir zirveye ulaşarak operasyonel kapasitesini kanıtlamıştır.

2. Black Shrantac Saldırı Yaşam Döngüsü (Attack Kill Chain)

Grubun teknik operasyonları, verinin gizliliğini ihlal etmeye yönelik çok aşamalı bir süreçten oluşmaktadır.

- **Keşif ve İlk Erişim:** Saldırganlar, hedef ağlardaki zafiyetleri tespit ederek ilk sızmayı gerçekleştirir.
- **Veri Toplama ve Hazırlama:** Sızma sonrası; finansal belgeler, İK kayıtları, AR-GE verileri ve iç yazışmalar gibi kritik veriler "staging" alanlarında toplanır.
- **Yüksek Hacimli Veri Sızıntısı:** Grubun teknik becerisinin en somut kanıtı, TB boyutundaki verileri (Örn: Dem İlaç - 1 TB, Rasen İnşaat - 400 GB) ağdan dışarı aktarma (exfiltration) kapasitesidir.
- **Dwell Time (Ağda Kalma Süresi):** Şifreleme adının atlanması veya sona bırakılması, güvenlik yazılımlarının (EDR/AV) "fidye yazılımı" alarmlarını tetiklemesini engelleyerek saldırıcıların ağda daha uzun süre kalmasını sağlar.



Şekil 5: Black Shrantac Saldırı Zinciri

3. Veri Gasabı ve Şantaj Metodolojisi

Black Shrantic, teknik olarak "şifrelemesiz fidye" (encryptionless ransomware) taktığıne ağırlık vermektedir.

- Kurban Utandırma (Victim Shaming):** Black Shrantic, kurbanları ödemeye zorlamak için çalınan verileri sizıntı platformlarında yayinallyarak sosyal baskı ve taktiksel bir güç kullanmaktadır.
- Genişletilmiş Şantaj:** Grup, sadece verileri yayılmamakla tehdit etmekle kalmaz; aynı zamanda iş ortaklarına e-posta göndererek saldırıya dikkat çekme ve kurumsal itibarı sarsma yoluna gider.
- Ifşa Edilen Veri Tipleri:** Yapılan incelemeler; pasaportlar, sigorta belgeleri, bilanço tabloları, ürün AR-GE verileri ve stratejik iç yazışmaların hedeflendiğini göstermektedir.

Analist Notu: Victim Shaming (Kurban Utandırma), kurban kuruluşları fidye taleplerini yerine getirmeye zorlamak için uygulanan taktiksel bir sosyal baskı yöntemidir. Black Shrantic'in bu yöntemi agresif kullanması, savunma ekiplerinin sadece "erişilebilirlik" değil, "veri gizliliği" odaklı savunma kurgulaması gerektiğini kanıtlamaktadır.

4. Altyapı ve Panel Yönetimi

Grup, saldırılarını koordine etmek ve kurban verilerini yönetmek için merkezi olmayan ve anonim bir altyapı kullanmaktadır.

- Yönetim Portalları:** Operatörler ve iştirakler (affiliates), kurbanlarla pazarlık yapmak ve sizıntı listelerini güncellemek için özel olarak tasarlanmış TOR tabanlı yönetim panellerine erişim sağlarlar.
- Operasyonel Güvenlik (OPSEC):** Saldırganlar, gerçek IP adreslerini gizlemek ve takip edilmeyi önlemek için TOR ağının derinliklerinde barınan birden fazla katmanı kullanmaktadır.

5. Operasyonel Strateji ve Taktikler (TTPs)

Black Shrantic, geleneksel fidye yazılımı gruplarından farklı olarak "Pure Data Extortion" (Saf Veri Gasrı) modelini teknik bir ustalıkla uygulamaktadır. Grubun kullandığı temel MITRE ATT&CK teknikleri şunlardır:

İlk Erişim (Initial Access - T1566):	Grup, ağa sızmak için ağırlıklı olarak mızraklı kimlik avı (Spear-phishing) ve dışa açık zayıf barındıran servislerin istismarını kullanmaktadır.
Veri Toplama ve Hazırlama (Collection - T1074):	Saldırganlar, sızma sonrası ağda yayılıarak (Lateral Movement) finansal verileri, İK kayıtlarını ve AR-GE dökümanlarını tespit edip merkezi bir konumda toplar (staging).
Veri Sızdırma (Exfiltration - T1041):	Grubun en belirgin imzası, saptanan verileri şifreleme aşamasına geçmeden önce kendi kontrolündeki sunuculara transfer etmesidir. Dem ilaç (1 TB) ve Rasen İnşaat (400 GB) vakaları, grubun devasa boyuttaki verileri tespit edilmeden dışarı çıkarma konusundaki teknik kabiliyetini kanıtlamaktadır.

Vaka İncelemeleri

Black Shrantic grubunun sizıntı sitesi (leak site) üzerinde yaptığı paylaşımlar, grubun hedef aldığı kurumların en mahrem verilerine ulaştığını kanıtlamaktadır. Aşağıdaki vakalar, grubun "Saf Veri Gaspi" modelinin yıkıcı etkilerini göstermektedir.

1. Dem İlaç (demilac, Inc) – Türkiye

İlaç sektöründe faaliyet gösteren Dem İlaç, grubun en büyük çaplı veri hırsızlığı vakalarından biridir.

- Sızıntı Boyutu:** 1 TB.
- İçerik Analizi:** Çalınan veriler arasında pasaport ve sigorta belgelerini içeren İnsan Kaynakları verileri, AR-GE çalışmaları, ürün verileri ve finansal tablolar (Bilanço, Nakit Akış Tabloları) yer almaktadır.
- Kritiklik:** AR-GE verilerinin "Satılık" (For Sale) olarak etiketlenmesi, grubun veriyi sadece şantaj için değil, ticari casusluk pazarında da kullandığını göstermektedir.

Black Shrantic

Contact Email: BlackShranticSupport@onionmail.org
Contact Tox: EFE1A6E5C8AF91FB1EA3A170823F5E69A85F866CF33A4370EC467474916941042E29C2EA4930

 demilac, Inc 7,912

 Turkey

 demilac.com.tr

Dem İlaç is a prominent pharmaceutical company in Turkey focused on research and development to produce medications that enhance human health. The company adheres to international standards of Good Manufacturing Practices (GMP) and offers a diverse portfolio of products, including anesthetics, serum, antibiotics, and biotechnology-based products. Targeting various therapeutic areas, Dem İlaç exports its products to 25 countries across six regions, including Canada, Poland, and Thailand. With a commitment to reliability, quality, and innovation, Dem İlaç continuously strives to address contemporary health needs.

DATASIZE: 1TB

1) Personal Information(private human resource include passport , insurance documents)
 2) Business Management Documents
 - Legal and Governance Documents
 - Financial Documents(Tax Documents , Balance Sheet, Profit & Loss Statement, Cash Flow Statement)
 - Marketing and Sales Documents(Customer Relationship Management , Marketing Plan)
 - R&D Data and Product Data
 - Human Resource(Passport, Personal Private, and so on)

Şekil 6: Dem İlaç Veri Sızıntısına Ait Kanıt Dökümanları



Şekil 7: Dem İlaç Çalışanlarına Ait Hassas Kişisel Veriler

2. Rasen İnşaat ve Yatırım Ticaret A.Ş. – Türkiye

İnşaat sektöründeki bu vakada, grubun kurumsal iç işleyişe ne kadar derin nüfuz ettiği görülmektedir.

Sızıntı Boyutu: 400 GB veri sızdırılmıştır.

Kritik Bulgular:

- Dahili İletişim Veritabanı:** Şirket içi e-posta trafiği ve strateji tartışmaları ele geçirilmiştir.
- Çalışan Verileri:** Maaş bilgileri, bonus yapıları, vize başvuru formları ve tazminat dökümleri sızdırılmıştır.
- İş Ortakları:** Müşteri sözleşmeleri ve yatırımcı detayları gibi üçüncü taraf bilgilerine de erişilmiştir.

Durum: Grubun panelinde verilerin yakında tamamen yayınlanacağına dair "Company data will be Publish soon" uyarısı yer almaktadır.

Black Shrantic Login

Contact Email: BlackShrantacSupport@onionmail.org
 Contact Tox: EFE1A6E5C8AF91FB1EA3A170823F5E69A85F866CF33A4370EC467474916941042E29C2EA4930

Rasen Insaat Ve Yatirim Ticaret A.S. 21,901

Turkey www.rasen.com.tr

Rasen Insaat Ve Yatirim Ticaret A.S. is a company in Turkiye, with a head office in Istanbul. It operates in the Nonresidential Building Construction industry. It was incorporated on May 11, 2006.

DATA SIZE: 400 GB

1. Financial Data (Bank account details, Transaction History, Revenue, profits, and detailed financial performance, etc)
 2. Client and Partner Information(Client contracts, Investor details, etc)
 3. Employee Data (Personal employee details, Salaries, bonuses, and compensation structures, Visa Application Form, etc)
 4. Internal Communication Database(Mail, Company strategy discussions)

Company data will be Publish soon.

Şekil 8: Rasen İnşaat Veri İhlalinin Teknik Özeti



Şekil 9: Rasen İnşaat'a Ait Hassas Şirket Verileri

3. Şimşek A.Ş. (simsekas, Inc) – Türkiye

Coca-Cola distribütörü olan Şimşek A.Ş. vakası, grubun lojistik ve dağıtım ağı verileri üzerindeki hakimiyetini göstermektedir.

- **Sızıntı Boyutu: 200 GB** veri ele geçirilmiştir.
- **Hedeflenen İçerikler:** İş sürekliliği planları, gizlilik sözleşmeleri, kurumsal yazışmalar (Business Letters) ve pazarlama-satış stratejileri.
- **Analiz:** Bu verilerin ifşası, şirketin ticari rekabet gücüne ve tedarik zinciri güvenliğine doğrudan zarar verme potansiyeli taşımaktadır.

The screenshot shows a dark-themed user interface for a ransomware attack. At the top, it says "Black Shrantac" and has a "Login" button. Below that, there's contact information: "Contact Email: BlackShrantacSupport@onionmail.org" and "Contact Tox: EFE1A6E5C8AF91FB1EA3A170823F5E69A85F866CF33A4370EC467474916941042E29C2EA4930". The main area displays a list of files with the following details:

File Name	Type	Last Modified
simsekas, Inc	Document	33,510
Turkey	Image	
simsekas.com.tr	Link	

Below the file list, there is a paragraph of text about Şimşek A.Ş. followed by a section titled "DATA SIZE: 200GB" and a list of document types.

Şimşek A.Ş. has been a Coca-Cola distributor since 1977, serving the regions of İzmir and Antalya, including the Kemer district. The company focuses on providing distribution services for Coca-Cola products. Their intended clients include businesses and consumers in the specified regions. Şimşek A.Ş. is committed to addressing any complaints or requests related to Coca-Cola products.

DATA SIZE: 200GB

Personal Information (private human resource include passport, insurance documents)
Business Management Documents
- Legal and Governance Documents
- Financial Documents(Tax Documents , Balance Sheet, Profit & Loss Statement, Cash Flow Statement)
- Marketing and Sales Documents(Customer Relationship Management , Marketing Plan)
- Operational and Administrative Documents(Business Continuity Plan and so on)
- Miscellaneous Documents (Business Letters , Confidentiality Agreements and so on)

Şekil 10: Şimşek A.Ş. Veri İhlalinin Teknik Özeti



Şekil 11: Şimşek A.Ş.ye Ait Hassas Kurumsal Veriler



Şekil 12: Şimşek A.Ş. Çalışanlarına Ait Hassas Kişisel Veriler

4. Altaş Temizlik – Türkiye

Şehir temizliği ve katı atık yönetimi sektöründe Türkiye'nin önde gelen kuruluşlarından biri olarak tanımlanan Altaş Temizlik, Black Shrantac grubunun sizıntı platformunda en çok dikkat çeken kurbanlardan biridir. Grubun panelindeki verilere göre, bu vaka **52.440** üzerinde görüntülenme alarak yüksek bir ifşa trafiğine ulaşmıştır.

Sızdırılan Hassas Veri Kategorileri:

Grup, kurumun hem operasyonel maliyetlerini hem de çalışanlarının en mahrem bilgilerini içeren iki ana veri setini ifşa etmiştir:

- **1. Finansal Veriler (Finance Info):**

- Şirketin üretim maliyetleri ve detaylı fatura kayıtları.
- Banka ekstreleri, ödeme listeleri ve kurumsal beyannameler.
- Özellikle sizıntı görsellerinde yer alan "**Ağustos 2023 Ödeme Planı**" ve "**Ticari Krediler**" dökümleri, şirketin nakit akışının ve borçlanma yapısının tamamen deşifre edildiğini göstermektedir.
- Çalışanlara ait maaş bordroları (payrolls) ve yan hak dökümleri.

- **2. İnsan Kaynakları Verileri (HR Information):**

- Çalışanlarla yapılan iş sözleşmeleri ve özlük dosyaları.
- Sürücü belgesi (DL) fotokopileri.
- En kritik bulgu olarak, çalışanların **Sosyal Güvenlik Numaraları (SSN)** ve kimlik bilgileri.

Black Shrantaç

Contact Email: BlackShrantaçSupport@onionmail.org
Contact Tox: EFE1A6E5C8AF91FB1EA3A170823F5E69A85F866CF33A4370EC467474916941042E29C2EA4930

Altaş Temizlik

52,440

Turkey

altastemizlik.com.tr

Altaş Cleaning company is one of the leading companies in the Urban Cleaning sector.

1. Finance info such as production costs, bills, invoices, statements, payrolls, etc;
2. HR information about employers, contracts, DL, SSNs, etc

The screenshot shows a dark-themed web application. At the top, there's a navigation bar with a logo, a search bar, and a 'Login' button. Below the header, contact information is listed. The main content area has a title 'Altaş Temizlik' with a small icon. It includes a 'Turkey' section with a flag icon and a URL. A descriptive paragraph follows. Below that are two numbered lists. The bottom half of the page contains several tables and a summary table. On the right side, there's a sidebar with a 'Disclosure' link.

	fon+vergi	toplam tutar	aylık ıks tutarı
3.00	3.00	2946.803.00	80.390.00
43.92	43.92	544.887.47	13.042.531.09
49.62	49.62	644.887.47	17.39.52
30.985.440.09	30.985.440.09	887.039.92	

Şekil 13: Altas Temizlik Hassas Kurumsal Veri Sızıntısı

Şekil 14: Altas Temizlik Ait Hassas Kurumsal Veriler

5. Küresel Perspektif (Global Victims)

Black Shrantac grubunun operasyonel menzili, Türkiye sınırlarının çok ötesine uzanarak beş farklı kıtaya yayılmış durumdadır. Grubun sizıntı platformu incelendiğinde, Batı dünyasından Asya-Pasifik bölgесine kadar geniş bir coğrafyada "Saf Veri Gaspi" modelini başarıyla uyguladığı görülmektedir.

Aşağıda, grubun küresel ölçekte gerçekleştirdiği en kritik veri ihlallerinin detaylı analizi yer almaktadır:

A. Okyanusya ve Asya Operasyonları

- Netstar Australia PTY Ltd (Avustralya):** Grubun küresel ölçekteki en büyük kurbanlarından biridir. Teknoloji ve navigasyon çözümleri sunan firmadan tam **800 GB** boyutunda veri sizdirilmiştir. Bu verilerin Netstar'ın kurumsal sistemlerine ve müşteri veri tabanlarına ait olduğu değerlendirilmektedir.
- VFM Systems & Services (P) Ltd (Hindistan):** Hindistan, grubun en çok hedef aldığı ikinci ülke konumundadır. VFM Systems vakasında **70 GB** boyutunda veri sizdirilarak kurumun IT ve sistem entegrasyonu dökümanları ifşa edilmiştir.
- Badan Pengelola Keuangan Haji (Endonezya):** Kamu finansmanı ve hac fonu yönetimi yapan bu kritik kurumdan **200 GB** veri çalınmıştır. Kamu kurumlarına yönelik bu saldırı, grubun sadece özel sektörü değil, devlet destekli finansal yapıları da hedeflediğini kanıtlamaktadır.

B. Kuzey ve Güney Amerika Hedefleri

- MultistateTax Inc (Amerika Birleşik Devletleri):** ABD, grubun **7 doğrulanmış saldırısı** ile dünya genelinde en çok hedef aldığı ülkedir. Bu vakada **50 GB** boyutunda hassas vergi ve finans danışmanlığı verisi sizdirilmiştir.
- Cabinets 2000, LLC (Amerika Birleşik Devletleri):** ABD merkezli bir diğer kurban olan bu işletme, grubun "Businesses" odaklı saldırısı stratejisinin bir parçasıdır.
- Superintendencia Nacional de Fiscalización Laboral (Peru):** Güney Amerika operasyonları kapsamında Peru'daki bu denetleyici kamu kurumu hedef alınarak resmi dökümanlar ifşa edilmiştir.

C. Avrupa ve Diğer Bölgeler

- **M&BM, Inc (Bulgaristan):** Doğu Avrupa'da faaliyet gösteren bu lojistik ve servis firması, grubun Avrupa pazarındaki etkinliğini göstermektedir.
- **Geniş Coğrafi Yelpaze:** Doğrulanmış kurban listeleri; Meksika, Rusya Federasyonu, Güney Kore, Birleşik Arap Emirlikleri, Katar, Malezya ve Mısır gibi ülkelerdeki kurumların da Black Shrantac tarafından aktif olarak izlendiğini ve sizildiğini kanıtlamaktadır.

Black Shrantac

Contact Email: BlackShrantacSupport@onionmail.org
 Contact Tox: EFE1A6E5C8AF91FB1EA3A170823F5E69A85F866CF33A4370EC467474916941042E29C2EA4930

 Agricola Cerro Prieto  5,734  Peru 🔗 https://www.acpagro.com DATA SIZE: 250GB	 Netstar Australia PTY Ltd  10,350  Australia 🔗 www.netstaraustralia.com.au DATA SIZE: 800 GB	 VFM Systems & Services (P) Ltd  12,123  India 🔗 https://vfmindia.biz DATA SIZE: 70 GB
 demilac, Inc  13,363  Turkey 🔗 demilac.com.tr DATASIZE: 1TB For Sale	 Rasen Insaat Ve Yatirim Ticaret A.S.  26,909  Turkey 🔗 www.rasen.com.tr DATA SIZE: 400 GB	 MultistateTax Inc  27,013  United States 🔗 multistatetax.net DATA SIZE : 50 GB

Badan Pengelola Keuangan Haji  27,092 Indonesia bpkh.go.id DATA SIZE: 200 GB	Superintendencia Nacional de Fiscalización Laboral  32,229 Peru www.sunafil.gob.pe DATA SIZE: 200 GB	Cabinets 2000, LLC  37,348 United States www.cabinets2000.com DATA SIZE : 850GB IMAGE UPDATED
Carvimsa  38,236 Peru www.carvimsa.com DATA SIZE: 250 GB	simsekas, Inc  38,239 Turkey simsekas.com.tr DATA SIZE: 200GB	M&BM, Inc  38,241 Bulgaria mbm-bg.com DATA SIZE: 900 GB
Newgen Digitalwork  38,249 India newgendigital.com DATA SIZE: 5 GB	libertyshoes, Inc  38,251 India libertyshoes.com DATA SIZE: 50GB	The Matlusky Firm LLC  44,930 United States thematluskyfirm.com DATA SIZE: 100 GB
Eligibility Tracking Calculators  44,971 United States eligibilitytrackingcalculators.com DATA SIZE: 110GB IMAGE UPDATED	TENAX Law Group PC  44,989 United States tenaxlawgroup.com DATA SIZE: 150GB	CCI Tax Pros, Inc  45,404 United States www.ccitaxpros.com DATA SIZE: 80GB IMAGE UPDATED
CyPark Resources Berhad  45,412 Malaysia www.cypark.com DATA SIZE : 450GB IMAGE UPDATED	Falco Electronics  48,127 Mexico falco.com DATA SIZE : 8 TB	Gulf Warranties LLC  48,136 UAE www.gulfwarranties.com DATA SIZE : 300 GB
Al Ahly Leasing & Factoring Company  48,207 Egypt alc.com.eg DATA SIZE : 6TB	Standard Fiber  51,568 United States standardfiber.com DATA SIZE : 2TB FIRST DISCLOSURE: 1GB	General Directorate of Taxes and Estates  53,495 Senegal dgid.sn DATA SIZE : 1TB Our Message
KlingInberg india pvt ltd  57,029 India KlingInberg.in DATA SIZE: 2TB SECOND DISCLOSURE: 3GB	Altas Temizlik  57,059 Turkey altastemizlik.com.tr DATA SIZE : 600GB SECOND DISCLOSURE: 3GB	SK shieldus  77,377 South Korea www.skshieldus.com DATA SIZE : 24 GB IMAGES UPDATED (2)

Şekil 15: Black Shrantac Ait Hassas Kurumsal Veriler

Teknik Göstergeler (INDICATORS OF COMPROMISE – IOCs)

Bu bölüm, savunma ekiplerinin (SOC, Incident Response) Black Shrantic saldırularını tespit etmek, engellemek ve ağ ortamında geriye dönük tarama (threat hunting) yapabilmesi için gerekli olan teknik verileri içermektedir. Aşağıdaki göstergeler, grubun operasyonel altyapısına ve kullandığı zararlı yazılım örneklerine aittir. Black Shrantic aktörleri, tespit edilmekten kaçınmak için anonim iletişim kanallarını ve gizli servisleri birincil operasyon üssü olarak kullanmaktadır.

URL:	http://b2ykcy2gcug4gnccm6hnrb5xapnresmyjjqgvhafaypppwgo4feixwyd.onion/login
	http://jvkpexgkuaw5toiph7fbgucycvnafaqmfvakymfh5pdxepvahw3xryqd.onion/login
E-POSTA:	BlackShrantacSupport@onionmail.org
TOX ID:	EEF1A6E5C8AF91FB1EA3A170823F5E69A85F866CF33A4370EC467474916941042E29C2EA4930
MD5:	f89aab69e01d21b2c8ce2b8ee9909d25
	42b9f136abd20fce07cd08a9b1631ea8
	e46f155df70c8a8c4506a2a42425c1a6
	17794ab9e93297365519f0db1c6a8a6d97b7a2c449ee51c4ae4723cf1d18a71e
	b5f90df776e6f57a7fec03f9e325ccf9debe4ddbcc8c385f0bb3edd91ef71927

Analist Notu: Black Shrantic'in küresel vaka profili, grubun "Sektörel Agnostik" (sektör ayırt etmeksiz) ancak "Veri Odaklı" bir yaklaşımı sahip olduğunu göstermektedir. Avustralya'da navigasyon verilerine, Endonezya'da kamu fonlarına, Türkiye'de ise ilaç AR-GE verilerine odaklanması; aktörün girdiği her ağda o kuruma en büyük zararı verecek (veya fidyeye zorlayacak) "en değerli veri setini" tespit edip çırarma konusundaki teknik uzmanlığını kanıtlamaktadır.

Sonuç ve Öneriler

Black Shrantic, 2025 yılı boyunca Türkiye ve küresel ölçekte gerçekleştirdiği operasyonlarla, geleneksel fidye yazılımı savunma mekanizmalarını aşabilen sofistike bir tehdit olduğunu kanıtlamıştır. Grubun dosya şifrelemek yerine doğrudan "**Veri Gizliliğini**" hedef alması ve "Victim Shaming" taktiklerini agresif bir şekilde kullanması, kurumların sadece yedekleme stratejilerine değil, kapsamlı bir veri koruma mimarisine ihtiyaç duyduğunu göstermektedir.

1. Genel Değerlendirme

Analiz edilen vakalar (Dem İlaç, Rasen İnşaat, Şimşek A.Ş., Altaş Temizlik), aktörün girdiği her ağda en yüksek fidyeyi koparabilecek "kritik veri setlerini" (AR-GE formülleri, finansal bilançolar, pasaportlar) tespit etme konusunda uzmanlaşlığını ortaya koymaktadır. Black Shrantic'in özellikle Türkiye'deki sanayi ve teknoloji kurbanlarında TB boyutunda veriyi dışı sızdırması, ağ içi görünürlük ve veri sızıntısı önleme (DLP) konusundaki eksiklikleri istismar ettiğini kanıtlar niteliktedir.

2. Stratejik ve Taktiksel Öneriler

Kuruluşların Black Shrantac ve benzeri "Saf Veri Gaspi" gruplarına karşı direnç kazanması için aşağıdaki adımları atması önerilir:

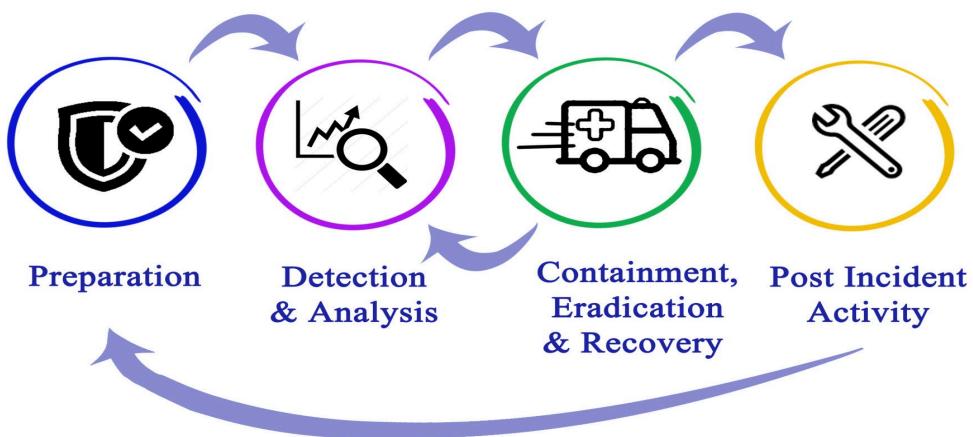
Taktiksel Önlemler (SOC ve IT Ekipleri İçin):

- IOC Bloklama:** Bölüm 6'da belirtilen MD5 hash değerleri, e-posta adresleri ve `.onion` uzantılı alan adları tüm güvenlik duvarlarında ve EDR sistemlerinde ivedilikle engellenmelidir.
- Ağ Trafiği Analizi:** Şirket ağından dışarıya (outbound) yönelik yüksek hacimli veri transferleri (özellikle mesai saatleri dışındaki upload aktiviteleri) anlık alarm üretecek şekilde konfigüre edilmelidir.
- Ayrıcalıklı Hesap Denetimi:** Grup, yanal hareket (Lateral Movement) için ele geçirilmiş kimlik bilgilerini kullandığından, Admin hesaplarında MFA (Çok Faktörlü Kimlik Doğrulama) kullanımı zorunlu hale getirilmeli ve şüpheli oturum açma aktiviteleri izlenmelidir.

Stratejik Önlemler (Yönetim ve Güvenlik Liderleri İçin):

- DLP Entegrasyonu:** Hassas verilerin (PII, AR-GE dökümanları, pasaportlar) ağ dışına çıkışını engelleyecek Veri Sızıntı Önleme (DLP) kuralları uygulanmalıdır.
- Tedarik Zinciri Güvenliği:** Shimşek A.Ş. örneğinde olduğu gibi, distribütörler ve iş ortakları üzerinden gelebilecek dolaylı saldırılara karşı üçüncü taraf güvenlik denetimleri artırılmalıdır.
- Çalışan Bilinçlendirme:** Grubun ilk erişim için kullandığı mızraklı kimlik avi (Spear-phishing) saldırılara karşı personelin düzenli olarak eğitilmesi ve simülasyonlarının yapılması elzemdirdir.

Incident Response Planning



Şekil 16: Black Shrantic Tehditine Karşı Önerilen Olay Müdahale (Incident Response) Planlaması Döngüsü

Black Shrantic, kurbanları üzerinde oluşturduğu sosyal baskı (Victim Shaming) ve sizdirdiği kritik verileri rakiplere satma tehdidiyle siber suç ekosisteminde yıkıcı bir oyuncu olmaya devam edecektir. Savunma ekiplerinin bu raporu temel alarak proaktif bir duruş sergilemesi, olası veri ihlallerinin etkisini minimize edecektir.

Kaynakça (References)

- [1] Ransomlook.io. BlackShrantac Fidye Yazılımı Grubu Profili ve İzleme. url: <https://www.ransomlook.io/group/blackshrantac>. (Erişim: 30.12.2025).
- [2] Ransomware.live. Fidye Yazılımı Gruplarının Faaliyetleri ve Sızıntı Sitesi Gerçek Zamanlı İzleme. Url:<https://www.ransomware.live/>. (Erişim: 30.12.2025).
- [3] Hookphish. Fidye yazılımı grubu BlackShrantac, Altas Temizlik'i (Türkiye) vurdu. url:<https://www.hookphish.com/blog/ransomware-group-blackshrantac-hits-altas-temizlik/>. (Erişim: 30.12.2025).
- [4] Dr. Disk Lab. *BlackShrantac Ransomware Grubu Teknik Analiz ve Profilleme*. url: <https://drdisklab.com/ransomware-gruplari/blackshrantac>. (Erişim: 30.12.2025).
- [5] BlackFog. Siber Güvenlik 101: BlackShrantac Fidye Yazılımı Operasyonlarını Anlamak. url: <https://www.blackfog.com/cybersecurity-101/blackshrantac/>. (Erişim: 30.12.2025).
- [6] SOCRadar. Siber Tehdit İstihbaratı ve Karanlık Web İzleme Platformu. url: <https://socradar.io/>. (Erişim: 30.12.2025).

Z111 [83322]
69.07

OdinEye



odineyecti.com



contact@odineyecti.com