

SEKTÖREL RAPOR 2023



YILIN İKİNCİ
YARISINDA
HAVACILIK
SEKTÖRÜNE
YÖNELİK
SALDIRILAR

 @echocti

 @echocti

 echocti.com

İçindekiler

Yönetici Özeti	2
Havacılık Sektöründe Siber Tehditler.....	3
Başlıca Siber Tehditler.....	3
Önemli Olaylar.....	4
En Aktif Tehdit Aktörleri	7
MuddyWater	7
APT-33	8
APT-27	9
APT-34	10
APT-28	11

Yönetici Özeti

Bu rapor, 2023 yılının ikinci yarısında gözlemlenen siber güvenlik alanındaki önemli gelişmeleri özetlemektedir. İlgili başlıklar altında raporlanan olaylar, belirli siber tehditler ve sektördeki önemli eğilimlerin analizini sunmaktadır.

Phishing, zararlı yazılım saldırıları ve fidye yazılımı saldırıları, bu dönemde öne çıkan siber tehditler arasında yer aldı. Kötü niyetli aktörler, kullanıcıları manipüle etmek ve hassas bilgilere erişmek için phishing saldırılarını arttırdılar. Benzer şekilde, zararlı yazılım ve fidye yazılımı saldırıları, kurumların faaliyetlerini olumsuz etkileyerek ciddi riskler oluşturdu.

2023 yılında, belirli siber tehdit aktörlerinin etkinlikleri gözlemlendi. Bu aktörler, karmaşık ve değişken saldırı teknikleri kullanarak kendilerini öne çıkardılar. Aynı zamanda, belirli ülkeler ve sektörler, saldırılara karşı daha fazla maruz kaldılar. Bu durum, siber güvenlik stratejilerinin özellikle sektörel ve coğrafi bazda daha özenli bir şekilde ele alınması gerektiğini vurgulamaktadır.

Önemli veri ihlalleri, kurumların hassas bilgilerini tehlikeye attı ve güvenlik açıklarının kritik olduğunu bir kez daha gösterdi. Bu ihlaller, siber savunma stratejilerinin güçlendirilmesi ve iyileştirilmesi gerekliliğini ortaya koydu.

Son olarak, keşfedilen önemli zafiyetler, sistemlerimizdeki açıkları açıkça gösterdi. Bu zafiyetlerin tespit edilmesi, düzeltilmesi ve gelecekteki saldırılara karşı daha güçlü bir savunma mekanizması oluşturulması kritik bir öncelik haline geldi.

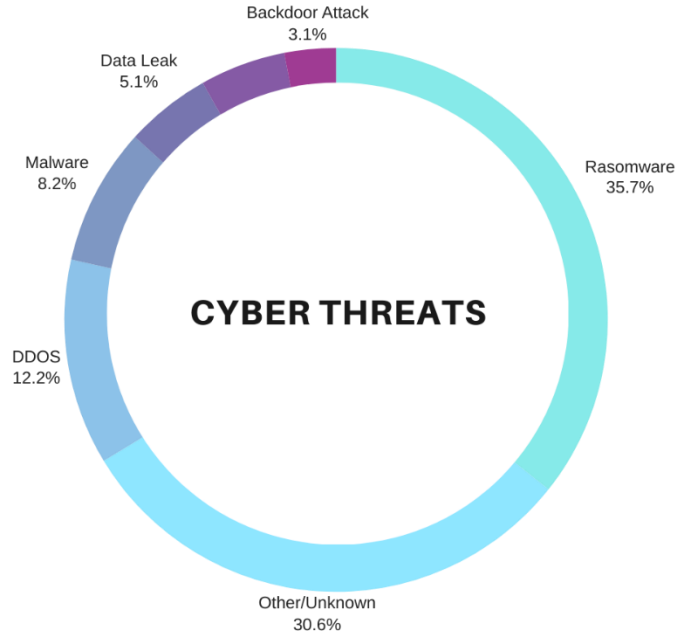
Siber güvenlik tehditleri sürekli olarak evrilmekte olup, kurum olarak güvenlik stratejilerimizi güncellemeye ve iyileştirmeye odaklanmaktayız. Bu rapor, 2023 yılının ikinci yarısını için önemli siber güvenlik trendlerini özetlemekte olup, gelecek yıl için daha sağlam bir güvenlik altyapısı oluşturmak adına yol gösterici olmayı hedeflemektedir.

Havacılık Sektöründe Siber Tehditler

Havacılık sektörü, teknolojinin hızla geliştiği, dijitalleşmenin yaygınlaştığı bir alan olarak siber tehditlere açık bir sektördür. Bu yazıda, havacılık endüstrisinde karşılaşılan siber tehditlerin doğası, etkileri ve sektördeki güvenlik önlemlerine odaklanacağız.

Havacılık sektörü, dijitalleşme sürecinde uçak sistemlerinden yer hizmetlerine kadar geniş bir yelpazede teknolojik altyapı kullanmaktadır. Ancak bu altyapının karmaşıklığı, sektörü siber tehditlere karşı savunmasız hale getirebilir. Siber tehditler, veri sızıntıları, hava trafik kontrol sistemlerine müdahale, uçuş sistemlerinin manipülasyonu gibi ciddi sonuçlara yol açabilir.

Başlıca Siber Tehditler



Yapılan araştırmalarda havacılık sektörünün en çok fidye yazılımı saldırıları ile hedef alındığı gözlemlenmiştir. Bu konu hakkında önceden hazırladığımız [2023 yılında Fidye Yazılımları](#) adlı raporumuzu inceleyebilirsiniz.

Önemli Olaylar

ABD havacılık şirketine yönelik siber saldırı tespit edildi

İranlı bilgisayar korsanlarının, ManageEngine ve Fortinet hatalarını kullanarak bir ABD havacılık kuruluşuna sızdıkları ortaya çıktı. Tehdit grupları henüz isimlendirilmedi, ancak USCYBERCOM, İran'ın istismar çabalarıyla ilişkilendirildiğini belirtti. İhlal, Zoho ManageEngine ServiceDesk Plus ve Fortinet güvenlik duvarı üzerindeki açıkların istismarıyla gerçekleşti. Saldırganların, Ocak ayından beri kurumun ağında bulundukları, ağa sızdıktan sonra da kalıcılık sağladıkları belirtildi. Saldırının, yamalanmamış güvenlik açıklarına sahip cihazlar kullanılarak gerçekleştirildiği tespit edildi.

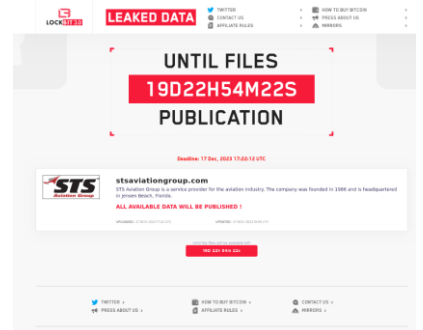


Kanada hükümeti veri ihlalini açıkladı

Ukrayna Savunma Bakanlığı'na bağlı istihbarat servisi, Rusya Federal Hava Taşımacılığı Ajansı olan Rosaviatsia'yı hacklediklerini iddia ediyor. Ukrayna, çalınan verilerin Rus havacılık sektörünün sorunlu durumunu ortaya çıkardığını söylüyor. Rosaviatsia ise henüz konuyla ilgili bir açıklama yapmadı.

LockBit fidye yazılımı grubu STS Aviation Group şirketini kurban listesine ekledi.

STS Aviation Group, 1986 yılında kurulan havacılık endüstrisi için bir hizmet sağlayıcısıdır. 27 Kasım 2023 tarihinde LockBit 3.0 fidye yazılımı grubu, söz konusu kurumun fidye yazılımına maruz kaldığını ve fidye ödenmemesi durumunda verilerin yayınlanacağını bildirdi.



Yingling Aviation, fidye yazılımı saldırısına maruz kaldı

Yingling Aviation

United States

www.yinglingaviation.com

views: 281

amount of data: ??? gb

added: 2023-10-28

publication date: 2023-11-03

information: Yingling Aviation is a full-service FBO/MRO and premier Textron Aviation affiliate located at Wichita's Dwight D. Eisenhower National Airport (KICT). Established in 1946 their range of services include airframe, engine, avionics, parts sales, propeller sales

comment: Private and personal confidential data, clients documents, IDs, payroll, tax, HR, insurance, finance information and etc.

1946 yılından beri uçak gövdesi, motor, aviyonik, parça satışı, pervane satışı gibi birçok alanda hizmet veren Yingling Aviation şirketi Play fidye yazılımı saldırısına maruz kaldı. 28 Ekim 2023 tarihinde Play fidye yazılımı grubu, söz konusu kuruma fidye yazılımı bulaştırdıklarını ve bazı özel bilgileri çaldıklarını açıkladı. Bu bilgiler: özel ve kişisel gizli veriler, müşteri belgeleri, kimlikler, bordro, vergi, İK, sigorta, finans bilgileri vb.

<p>AHS Aviation Handling Services GmbH</p> <p>The AHS Group is the market leader in Germany among independent providers of airline passenger handling and operations.</p> <table border="1"> <thead> <tr> <th>Website</th> <th>Revenue</th> <th>Employees</th> </tr> </thead> <tbody> <tr> <td>https://www.ahs-de.com</td> <td>\$658M</td> <td>3255</td> </tr> </tbody> </table>	Website	Revenue	Employees	https://www.ahs-de.com	\$658M	3255	<p>Encrypted 16/04/2022</p> <p>Downloaded more than 4Tb</p> <p>Status: DISCLOSED 389928 16/04/2022</p>	<p>Share</p> <p>f</p> <p>t</p> <p>Contact us</p> <p>✉</p>
Website	Revenue	Employees						
https://www.ahs-de.com	\$658M	3255						
<p>Evidence packs: Download</p> <p>Password: x5CLG6aPE1YtC3UzuwpX</p> <p>FULL DATA DUMP: Download</p> <p>One more thing to note everyone tends to forget: one of AHS's subsidiary companies, Aviova (www.aviova.com), is also down like their own infrastructure.</p> <p>Interesting articles on the whole situation: Aerotelegraph.com Airliners.de</p>								


AHS Aviation Handling Services Fidye Yazılımı Saldırısına Maruz kaldı

Almanya'da Pazar lideri durumunda bulunan AHS Grubun, 18 Ağustos 2023 günü RansomHouse fidye yazılımı saldırısına maruz kaldığı duyuruldu. Fidye yazılımı grubu, 4TB'den büyük veri çalındığını iddia etti.

Boeing LockBit 3.0 fidye yazılımına maruz kaldı

UNTIL FILES
5D19H54M22S
PUBLICATION

Deadline: 02 Nov, 2023 13:25:39 UTC

**boeing.com**

Boeing, the 60 billion Company, together with its subsidiaries, designs, develops, manufactures, sells, services, and supports commercial jetliners, military aircraft, satellites, missile defense, human space flight, and launch systems and services worldwide.

A tremendous amount of sensitive data was exfiltrated and ready to be published if Boeing do not contact within the deadline!

For now we will not send lists or samples to protect the company BUT we will not keep it like that until the deadline.

ALL AVAILABLE DATA WILL BE PUBLISHED !

UPLOADED: 27 OCT. 2023 17:27 UTC UPDATED: 27 OCT. 2023 18:29 UTC

Until the files will be available left
5D 19h 54m 22s

Ticari uçaklar, savunma ürünleri ve uzay sistemleri geliştiren, üreten ve hizmet veren Boeing şirketi, 27 Ekim 2023 tarihinde LockBit 3.0 fidye yazılımı saldırısına maruz kaldı. LockBit 3.0 fidye yazılımı grubu 40GB boyutunda veri çalındığını iddia etti.

En Aktif Tehdit Aktörleri

Ekibimiz tarafından yapılan incelemeler sonucunda, bazı APT gruplarının bu yılın ikinci yarısında havacılık sektörünü hedef aldığı tespit edilmiştir. Raporun bilgilendirme amacı doğrultusunda söz konusu APT gruplarına ait bilgilere aşağıda yer verilmiştir.

MuddyWater



MuddyWater APT grubu, çeşitli ulusal ve uluslararası hedeflere karşı saldırılar gerçekleştiren bir gelişmiş kalıcı tehdit (APT) grubudur.

Bu grup, ilk olarak 2017 yılında tespit edilen ve genellikle Orta Doğu ve Asya ülkelerindeki kamu kurumları, telekomünikasyon şirketleri, üniversiteler ve diğer sektörlerle yönelik saldırılarında aktif olduğu bilinen bir grup olarak bilinir.

MuddyWater'ın saldırıları genellikle gelişmiş sosyal mühendislik teknikleri, karmaşık malware saldırıları ve hedeflenmiş phishing kampanyaları içerir. Bu grup, sahte belgeler, Word veya Excel dosyaları gibi güvenilir görünen iletiler aracılığıyla hedef sistemlere sızma girişiminde bulunur. Saldırılarında, gelişmiş gizlilik ve gizlenme tekniklerini kullanarak tespit edilmeyi önlemeye çalışır.

MuddyWater'ın hedeflediği amaçlar arasında bilgi toplama, casusluk, bilgi sızdırma ve ağların kontrolünü ele geçirme gibi faaliyetler bulunabilir. Bu grup, karmaşık saldırıları gerçekleştirme yeteneğine sahip olan uzman bir aktör olduğu bilinir ve sürekli olarak taktiklerini ve tekniklerini geliştirmeye devam eder.

MuddyWater APT grubu, bilgi güvenliği uzmanları ve siber güvenlik ekipleri tarafından yakından takip edilmekte ve analiz edilmektedir. Bu sayede yeni saldırı eğilimleri ve yöntemleri hakkında bilgi edinilerek savunma stratejileri oluşturulmaya çalışılmaktadır.

APT-33



APT33, bilinen diğer adıyla Cozy Bear, Rusya'ya bağlı bir Advanced Persistent Threat (APT) grubudur.

Bu grup, genellikle devlet destekli siber casusluk ve çeşitli ülkelerin hükümetleri, savunma endüstrisi ve enerji sektörü gibi stratejik hedeflere yönelik saldırılarıyla tanınır.

Başlıca Özellikleri

- Devlet Destekli Operasyonlar:** APT33, Rus hükümetiyle bağlantılı olduğuna inanılan bir grup olarak bilinir. Bu nedenle, faaliyetleri genellikle Rus devletinin stratejik çıkarları doğrultusunda gerçekleşir.
- Sofistike Siber Operasyonlar:** Grup, gelişmiş ve sofistike siber operasyonlar gerçekleştirme kabiliyetine sahiptir. Hedef sistemlere sızma, casusluk faaliyetleri ve uzun vadeli saldırı stratejileri kullanma konusunda uzmandır.
- Hedef Çeşitliliği:** APT33, geniş bir hedef yelpazesi üzerinde faaliyet gösterir. Bu hedefler arasında devlet kurumları, savunma endüstrisi, enerji sektörü ve diğer stratejik sektörler bulunur.

Bilinen Saldırıları:

Politikacılara ve Devlet Kurumlarına Karşı Saldırıları: APT33, çeşitli ülkelerin politikacılarına ve devlet kurumlarına karşı gerçekleştirilen sofistike phishing kampanyaları ve casusluk operasyonlarıyla bilinir.

Enerji Sektörü Hedefleri: Grup, enerji tesisleri ve altyapılarına yönelik saldırılar gerçekleştirir. Bu saldırılar, uzun vadeli etkiler bırakacak şekilde planlanmıştır.

Amaç ve Hedefleri:

APT33, genellikle Rus hükümetinin stratejik çıkarlarını desteklemek amacıyla faaliyet gösterir. Grup, siber casusluk ve çeşitli sektörlerle yönelik saldırılarla, politik, askeri ve ekonomik bilgileri toplamayı hedefler. Aynı zamanda, uzun vadeli etkiler yaratmak amacıyla devlet destekli siber operasyonlar yürüterek düşman ülkelerin savunma yeteneklerini zayıflatmayı amaçlar.

APT-27



APT27, bilinen diğer adıyla Emissary Panda veya Threat Group-3390, Çin merkezli bir gelişmiş kalıcı tehdit (APT) grubudur. Grup, stratejik web kompromisleri kullanarak kurbanlarını hedefleyen bir tehdit aktörüdür.

En az 2010 yılından beri faal olan bu grup, havacılık, hükümet, savunma, teknoloji, enerji, üretim ve kumar/bahis sektörlerinde faaliyet gösteren kuruluşları hedef almıştır.

Başlıca Özellikleri

1. **Stratejik Web Kompromisleri:** APT27, kurbanlarını hedef almak için yaygın bir şekilde stratejik web kompromisleri kullanır. Bu, hedef organizasyonların web tabanlı güvenlik açıklarını kullanarak sızma yeteneklerini artırır.
2. **Uzun Süreli Faaliyet:** Grup, en az 2010 yılından beri faal olup uzun vadeli siber saldırı stratejilerini benimsemiştir. Bu, sürekli olarak hedeflere yönelik faaliyetlerini sürdürme eğilimindedir.
3. **Çeşitli Sektörlere Yönelik Saldırıları:** APT27, havacılık, hükümet, savunma, teknoloji, enerji, üretim ve kumar/bahis gibi geniş bir sektör yelpazesine yönelik saldırılar gerçekleştirebilen bir grup olarak bilinir.
4. **Diğer APT Grupları ile İlişkiler:** Emissary Panda, Turbine Panda, APT 26, Shell Crew, WebMasters, KungFu Kittens ve muhtemelen UNC215 gibi diğer APT gruplarıyla örtüşen özelliklere sahiptir. Ayrıca, Operation StealthyTrident adlı operasyonda TA428 ile işbirliği yapmıştır.

Bilinen Saldırıları:

APT27'nin hedefleri arasında yabancı elçilikler bulunur ve bu kuruluşlardan veri toplama amacı güder. Bu saldırılar genellikle hükümet, savunma ve teknoloji sektörlerine yöneliktir.

Amaç ve Hedefleri:

APT27'nin ana amaçları arasında yabancı hükümetlerden ve kuruluşlardan stratejik bilgileri toplamak, özellikle de hükümet, savunma ve teknoloji sektörlerinde faaliyet gösteren organizasyonların güvenliğini zayıflatmak yer alır. Çin merkezli bir aktör olarak, bu grup, ulusal çıkarları koruma amacı taşır ve siber casusluk faaliyetleri yürütür.

APT-34



APT34, yani bilinen adıyla OILRIG, İran merkezli bir gelişmiş kalıcı tehdit (APT) grubudur.

Bu grup, İran'ın stratejik çıkarlarını desteklemek amacıyla siber casusluk ve siber saldırıları gerçekleştiren bir istihbarat birimi olarak kabul edilir.

APT34, çeşitli sektörlerle yönelik siber saldırılar yapma yeteneğine sahiptir ve İran hükümeti tarafından desteklenmektedir.

Başlıca Özellikleri:

1. İran Hükümeti Bağlantısı: APT34, İran hükümeti ile yakından ilişkilendirilen bir siber casusluk grubudur. Grup, İran'ın stratejik çıkarlarını desteklemek amacıyla faaliyet gösterir.
2. Hedef Çeşitliliği: APT34, enerji, savunma, telekomünikasyon, finans ve hükümet gibi bir dizi sektöre yönelik saldırılar gerçekleştirir. Hedefler arasında genellikle yabancı hükümetler, şirketler ve düşman ülkelerin stratejik pozisyonları bulunur.
3. Sosyal Mühendislik Yetenekleri: Grup, hedeflerine sızmak için sosyal mühendislik taktiklerini kullanır. Bu, kurbanların güvenini kazanmak ve kötü amaçlı yazılımları yaymak için manipülasyon ve dolandırıcılık içerebilir.
4. Zararlı Yazılımlar: APT34, kötü amaçlı yazılım kullanımında uzmandır. Özellikle, çeşitli türde zararlı yazılımları hedeflerine sızmak için kullanır.

Bilinen Saldırıları:

APT34'nin en dikkat çekici saldırılarından biri, dünya çapında çok sayıda hükümet ve özel sektör kuruluşuna karşı gerçekleştirilen Phosphorus kampanyasıdır. Bu kampanya, hedeflere yönelik siber casusluk ve bilgi toplama operasyonlarını içerir.

Amaç ve Hedef:

APT34, İran hükümetinin stratejik çıkarlarını korumak ve ileriye taşımak amacıyla faaliyet gösterir. Hedefleri arasında yabancı hükümetler, enerji sektörü, askeri savunma ve stratejik bilgi bulunur.

IoC için [tıklayın](#).

APT-28



APT28, diğer adıyla Fancy Bear veya Sofacy olarak da bilinen bir tehdit grubudur ve Temmuz 2018'de ABD Adalet Bakanlığı tarafından yayınlanan bir iddiaya göre, Rusya'nın Genelkurmay İstihbarat Dairesi'ne (GRU) bağlı bir grup olarak tanımlanmıştır.

Bu grup, 2016 yılında Amerika Birleşik Devletleri başkanlık seçimlerine müdahale etmek amacıyla Hillary Clinton kampanyası, Demokrat Ulusal Komitesi ve Demokrat Kongre Kampanya Komitesi'ni hedef aldığı belirtilmiştir. APT28, en az Ocak 2007'den beri faaldir.

Başlıca Özellikleri:

1. **Rusya'ya Bağlantı:** APT28, Rusya'nın Genelkurmay İstihbarat Dairesi'ne bağlı olduğuna inanılan bir tehdit grubudur. ABD Adalet Bakanlığı'nın 2018 iddianamesine göre, bu grup Rus hükümetinin bilgileri toplamak ve müdahale etmek amacıyla faaliyet gösterir.
2. **Amerikan Seçimlerine Müdahale:** 2016 ABD başkanlık seçimlerine müdahale iddialarıyla ün kazanan APT28, Hillary Clinton kampanyası, Demokrat Ulusal Komitesi ve Demokrat Kongre Kampanya Komitesi'ni hedef almıştır.
3. **Doğu Avrupa ve Gürcistan Odaklı Faaliyetler:** FireEye analizine göre, APT28, Gürcistan'ın güvenlik ve politik dinamikleri hakkında bilgi toplamaya çalışarak Gürcistan'ın İçişleri ve Savunma Bakanlıkları'nda çalışan yetkililere odaklanmıştır.
4. **Doğu Avrupa ve Avrupa Güvenlik Organizasyonlarına Yönelik Saldırıları:** Grup, Doğu Avrupa hükümetleri ve güvenlik kuruluşlarına olan ilgisini sürdürmüş, bu şekilde Rus hükümetine politika yapıcı niyetleri öngörme ve kamuoyunu etkileme yeteneği sağlamıştır.

Bilinen Saldırıları:

2016 ABD Başkanlık Seçimleri: APT28, Amerika Birleşik Devletleri başkanlık seçimlerine müdahale etmek amacıyla Hillary Clinton kampanyası, Demokrat Ulusal Komitesi ve Demokrat Kongre Kampanya Komitesi'ni hedef almıştır.

Doping Ajanslarına Karşı Saldırıları: 2018'de ABD, APT28 ile ilişkilendirilen beş GRU Unit 26165 subayını, Dünya Anti-Doping Ajansı (WADA), ABD Anti-Doping Ajansı, ABD nükleer tesisi, Kimyasal Silahların Yasaklanması Örgütü (OPCW), Spiez İsviçre Kimyasal Laboratuvarı ve diğer kuruluşlara yönelik 2014-2018 arasında gerçekleştirilen siber operasyonlarla suçlamıştır.

Amaç ve Hedef:

APT28'nin ana amaçları, Rus hükümetinin çıkarları doğrultusunda stratejik bilgileri toplamak ve uluslararası politika üzerinde etki sağlamaktır. Doğu Avrupa, Gürcistan ve Amerika Birleşik Devletleri gibi bölgelerdeki hedefleri aracılığıyla, grup bilgi sızdırma ve manipülasyon yoluyla Rusya'nın politik etkisini artırmayı amaçlar.

IoC için [tıklayın](#).



ECHO

CYBER THREAT INTELLIGENCE