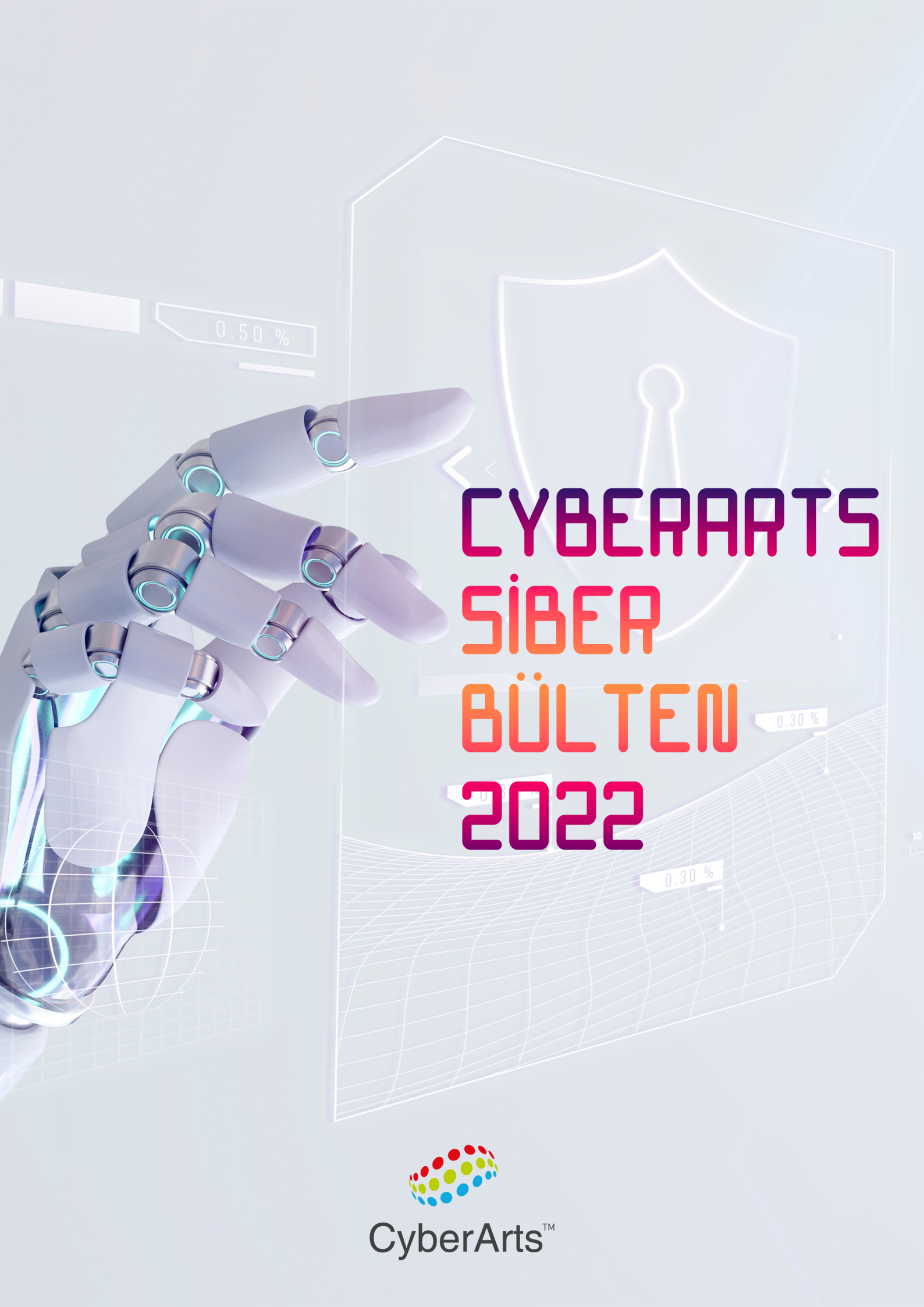


CYBERARTS SİBER BÜLTEN 2022

CyberArts™

CYBERARTS FELSEFESİ

Söz konusu siber hizmetler olduğunda, tüm kurumlar her şeyin en iyisini talep eder ve her şeyin en iyisini de hak eder. Siber dünyadaki tecrübelerimizi, sanatçı hassasiyeti ve titizliği ile çalışan diğer kurum ve kişilerle bir araya gelerek, sıradanlık değil sanat talep eden kurumların hizmetine sunuyoruz. Her ne yaparsak yapalım içinde "sanat" hep var olacak. CyberArts olarak bu bizim sözümüz.

HAKKIMIZDA

CyberArts olarak finans, telekom, lojistik, e-ticaret, üretim, inşaat, teknoloji, hizmet ve kamu gibi farklı sektörlerden büyük yerli ve uluslararası kurumlara bilgi güvenliği ve siber güvenlik hizmetleri sunuyoruz.

Danışmanlık verdiğimiz kurumlarda bir karar alırken bu kararın diğer iş süreçlerinde yaratacağı etkiyi ve sürdürülebilirliği ilk baştan hesaba katıyoruz. Uluslararası deneyime sahip siber sanatçılarımız sayesinde, büyük resmi görüp; insan kaynakları, süreçler ve teknolojileri kapsayacak bir stratejiyi birlikte inşa ediyor; hukuk, yönetişim ve siber güvenlik disiplinlerini bir araya getiriyoruz. Projeleri bir orkestra şefi gibi yürütüyor, tüm işlerimizi bir sanatçı hassasiyetiyle yapıyor ve büyük kurumların dijital dönüşüm yolculuklarında güvendikleri yol arkadaşları haline geliyoruz.

Diğer taraftan Türkiye Siber Güvenlik Kümelenmesinin kurucu üyelerinden biri olarak; mümkün olan tüm projelerimizde olgunluğunu ispat etmiş ve global vizyona sahip yerli siber güvenlik teknolojilerine öncelik vererek başarı hikayelerine imza atıyor ve yerli siber güvenlik ekosisteminin büyümesine katkı sağlıyoruz.

Giriş:

Bu yazımızda 2022 yılında yapılmış siber saldırıları inceledik. En çok kullanılan atak vektörlerini, sıklıkla siber saldırı alan ülkeleri ve aynı zamanda en çok siber saldırı yapan ülkeleri sizin için listeledik.

Saldırıların Nedenleri:

Saldırıların nedenleri arasında siber suçluların maddi kazanç sağlamak için saldırı düzenlemesi, devletlerin birbirleriyle veya ülkelerindeki muhalif gruplara karşı siber saldırılar düzenlemesi, siber güvenlik açıklarından faydalanma, çalışanların hataları veya kötü niyetli davranışları yer alabilir.

Etkileri ve Sonuçları:

2022 yılında gerçekleşen siber saldırıların etkileri ve sonuçları oldukça geniş kapsamlıydı. Saldırıların şirketlerin iş sürekliliğini bozması, kişisel verilerin çalınması, finansal kayıplar, müşteri güveninin sarsılması, kamu hizmetlerinin kesintiye uğraması ve daha birçok olumsuz sonuçları olabilir.

Siber Güvenlik Önlemleri:

Siber saldırıların önlenmesi ve siber güvenliğin artırılması için birçok önlem alınabilir. Bunlar arasında daha güçlü şifreleme yöntemleri kullanmak, güvenlik açıklarını tespit etmek ve kapatmak, çalışanların siber güvenlik konusunda eğitilmesi, siber güvenlik stratejilerinin güncellenmesi gibi yöntemler alabilir.

2022 YILINDA EN ÇOK GERÇEKLEŞTİRİLEN SİBER SALDIRILAR

En çok kullanılan atak vektörleri:

1. Compromised Credentials (Güvenliği İhlal Edilmiş Kimlik Bilgileri)

Kullanıcı adları ve parolalar hâlâ en yaygın erişim kimlik bilgisi türleridir ve veri sızıntılarına, kimlik avı dolandırıcılıklarına ve kötü amaçlı yazılımlara maruz kalmaya devam etmektedir. Kimlik bilgileri kaybolduğunda, çalındığında veya açığa çıktığında saldırganlara sınırsız erişim sağlar. Kuruluşların veri ifşalarını ve sızdırılmış kimlik bilgilerini sürekli olarak izlemek için araçlara yatırım yapmasının nedeni budur. Parola yöneticileri, iki faktörlü kimlik doğrulama (2FA), çok faktörlü kimlik doğrulama (MFA) ve biyometri, bir güvenlik olayıyla sonuçlanan kimlik bilgilerinin sızması riskini azaltabilir.

2. Weak Credentials (Zayıf Kimlik Bilgileri)

Zayıf parolalar ve yeniden kullanılan parolalar, bir veri ihlalinin çok daha fazlasına yol açabileceği anlamına gelir. Kuruluşunuza güvenli bir parola oluşturmayı, bir parola yöneticisine veya çoklu oturum açma aracına yatırım yapmayı ve personeli bunların avantajları konusunda eğitmeyi öğretin.

3. Insider Threats (Kurum İçi Tehditler)

Canı sıkılan çalışanlar veya kötü niyetli kişiler özel bilgileri ifşa edebilir veya şirkete özgü güvenlik açıkları hakkında bilgi sağlayabilir.

4. Missing or Poor Encryption (Yanlış veya Düşük Şifreleme)

SSL sertifikaları ve DNSSEC gibi yaygın veri şifreleme yöntemleri, ortadaki adam saldırılarını önleyebilir ve iletilen verilerin gizliliğini koruyabilir. Bekleyen veriler için

eksik veya zayıf şifreleme, bir veri ihlali veya veri sızıntısı durumunda hassas verilerin,kimlik bilgilerinin açığa çıkması anlamına gelebilir.

5. Misconfiguration (Hatalı Konfigürasyon)

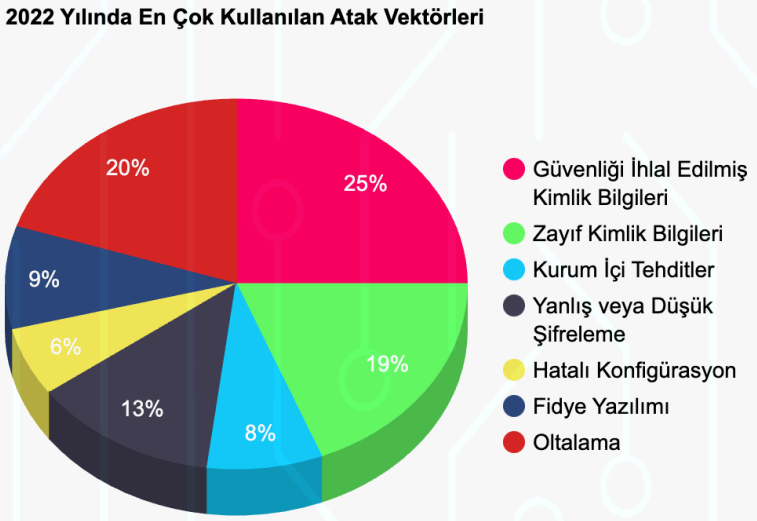
Kurum içinde kullanılan 3.parti yazılımların yine kurum içinde kullanılan yazılımlar ile beraber entegre çalışması gerekmektedir. Sonradan eklenen yazılımların eklendikten sonra entegrasyon testinin yapılması gerekmektedir.

6. Ransomware (Fidye Yazılımı)

Fidye yazılımı, WannaCry gibi bir fidye ödenmedikçe verilerin silindiği veya şifrelendiği bir gasp biçimidir. Sistemlerinize yama uygulamak ve önemli verileri yedeklemek de dahil olmak üzere bir savunma planı uygulayarak fidye yazılımı saldırılarının etkisini en aza indirin.

7. Phishing (Oltalama)

Kimlik avı saldırıları, hedefle e-posta, telefon veya kısa mesaj yoluyla, bir meslektaş veya kurum gibi davranan birinin onları hassas veriler, kimlik bilgileri veya kişisel olarak tanımlanabilir bilgiler sağlamaları için kandırmak üzere iletişim kurduğu sosyal mühendislik saldırılarıdır. Sahte mesajlar, kullanıcıları virüsler veya kötü amaçlı yazılım içeren kötü amaçlı web sitelerine gönderebilir.



2022'DEN SİBER HABERLER

PrivateLoader Hizmeti RisePro Kötü Amaçlı Yazılımını Dağıtırken Bulundu

PrivateLoader olarak bilinen kötü amaçlı yazılım yayma hizmeti, RisePro adında daha önce belgelenmiş ve bilgi çalan kötü amaçlı yazılımı dağıtmak için kullanılıyor. En son 13 Aralık 2022 tarihinde FlashPoint radarına takılan son aktivite toplanan bilgilerin, birkaç veri seti halinde 'Russian Market' adındaki illegal siber suç pazarında yayınlandığı tespit edildi. Detaylar için tıklayınız.

Okta'nın Github Hesabı Saldırıya Uğradı

Kimlik Doğrulama Hizmeti ve Kimlik Erişim Yönetimi (IAM) çözümlerinin lider üreticisi olan Okta, özel GitHub hesaplarının bu ay saldırıya uğradığını açıkladı. Okta tarafından gönderilen gizli e-postaya göre, güvenlik olayı Okta'nın kaynak kodlarını çalma potansiyeli olan atak vektörlerini içeriyor. Okta kaynak kodu çalındı fakat müşteri verileri etkilenmedi. Detaylar için tıklayınız.

Yeni Python Zararlısı Uzaktan Erişimler İçin Wmware ESXİ Backdoor'ları Kullanıyor!

Wmware ESXİ sunucularını hedef alan, daha önce belgelenmemiş bir python backdoor tespit edildi ve bu zafiyete maruz kalan sistemde zafiyet uzaktan kod çalıştırılmasına olanak sağladı. Detaylar için tıklayınız.

Rusya'nın En Büyük Bankalarından VTB Bank DDoS Saldırısına Uğradı:

Rusya'nın en büyük ikinci finans kurumu olan VTB Bank, tarihindeki en büyük DDoS saldırısıyla karşı karşıya olduğunu açıkladı. Bankaya yönelik yapılan DDOS saldırısını hacktivist bir grup üstlendi. Kasım ayında hacktivist grup Telegram kanalında saldırıyı duyurdu. Saldırı, bankanın web sitesine ve mobil uygulamasına müşterilerin erişimini engelliyor ve büyük bir soruna neden oluyor. Banka yapılan saldırı sonucunda müşterileri verilerinin tehlikeye atılmadığını bildirdi. Detaylar için tıklayınız.

Spotify'ın Backstage Yazılım Kataloğu ve Geliştirici Platformunda Uzaktan Kod Yürütme Hatası Bildirildi!

Spotify'ın Backstage projesinde kimliği doğrulanmamış RCE Güvenlik açığı keşfedildi. Güvenlik açığı (CVSS puanı:9,8) geçen aylarda çıkan JavaScript sanal alan kitaplığı (Sandbreak) olan vm2'de kritik bir sanal alan sızıntısından yararlanıyor. Detaylar için tıklayınız.

Anahtarsız Giriş Teknolojisini Kullanarak Arabaları Hackleyen Saldırganlar Yakalandı

Europol bu hafta, İspanyol ve Letonyalı yetkililerin desteğiyle, bir araba hırsızlığı çetesini başarıyla dağıttı. Anahtarsız araçları çalmak için saldırı tekniği geliştiren ve kullanan saldırganlara yönelik gerçekleştirdiği baskında 31 kişiyi tutukladığını açıkladı. Tutuklanan kişiler arasında yazılım geliştiricileri, satıcılar ve sahte yazılım kullanan saldırganlar bulunuyor. Europol'ün basın açıklamasına göre, saldırganlar

araç çalmak için sahte yazılımlar kullandı. Çetenin aracı çalmak için fiziksel anahtarlara bile ihtiyacı yoktu. Detaylar için tıklayınız.

Binance Hacklendi!

Kripto para borsası Binance'e siber saldırı gerçekleştirildi. Tahmini olarak 110 milyon dolarlık kripto para çalındığı söyleniyor fakat kapsam olarak daha büyük olduğu da söylenenler arasında. Resmî açıklamalar BNB Chain sosyal medya hesaplarından "Düzensiz faaliyet nedeniyle Binance Akıllı Zincir'i (BSC) geçici olarak duraklatıyoruz" şeklinde yapıldı. İkinci açıklamada ise saldırıyı duyuran yetkililer, fonların güvenliğinden yana bir güven sorunu olmadığını belirttiler. Detaylar için tıklayınız.

Uber Saldırıya Uğradı!

Uber 16 Eylül Perşembe günü yaptığı açıklamada sistemlerinin hacklendiğini doğruladı. Şirket, Twitter üzerinden "Şu anda bir siber güvenlik olayıyla karşı karşıyayız. Güvenlik birimleriyle iletişim halindeyiz, yeni bilgiler geldikçe burada yayınlayacağız." açıklamasını yaptı. Detaylar için tıklayınız.

Akasa Air, Yolcularının Kişisel Bilgilerini Sızdırdı

Hindistan'ın en yeni ticari havayolu şirketi olan Akasa Air, teknik bir yapılandırma hatası sonucu müşterilerine ait kişisel verileri ifşa etti. Siber güvenlik araştırmacısı olan Ashutosh Barot'a göre hesapların kayıt sürecinde gerçekleşen bir sorun olduğunu ve bu sorunun isim, cinsiyet, e-posta, telefon numaraları gibi bilgilerin görünebilmesine imkân sağlıyordu. Araştırmacılar, 7 Ağustos'ta firma faaliyetlerine başladığı gün zafiyet tespit etti. Detaylar için tıklayınız.

LastPass Saldırıya Uğradı

Kaynak Kodu Ele Geçirildi. Parola yönetim uygulaması olan LastPass, geçen hafta gerçekleşen hack olayını doğruladı. Güvenlik ihlalinin iki hafta önce meydana geldiği ve geliştirme ortamını hedef aldığı söyleniyor. Hiçbir müşteri verisine veya şifreli parolaya erişilmediği de iddialar arasında. Detaylar için tıklayınız.

Cellebrite'a Ait 4 TB Veri Sızıntısı İddiası

Digital Forensic alanında dünyanın önde gelen markalarından olan Cellebrite, 2007 yılından beri dünya çapında kolluk kuvvetleri başta olmak üzere kriminal laboratuvarlar, özel denetim şirketleri ve adli bilişim hizmeti veren pek çok özel kuruluşa çözüm sağlamaktadır. Cellebrite bir İsrail firmasıdır ve dijital verileri toplamak, incelemek, analiz etmek, yönetmek gibi hizmetler sunmaktadır. İsimsiz bir kaynak, Cellebrite'a ait yaklaşık 4 TB'lık verinin sızdırıldığını iddia etti. Sızdırılan verinin büyük çoğunluğu (3,6 TB) Cellebrite Mobilogy'den (şirketin amiral gemisi ürünü) sızdırıldı. Cellebrite Team Foundation sunucusundan ise 430 GB büyüklüğünde veri sızdırıldı. Detaylar için tıklayınız.

Hackerlar, Bitcoin ATM'lerinden Kripto Çaldı

Bitcoin ATM üreticisi General Bytes, 18 Ağustos'ta kullanıcılarından kripto paraları elde edebilmek için yazılım eski sürümlerinden gelen bir zero day saldırısına kurban oldu. Bu güvenlik açığı CAS yazılımında 2020-12-08 sürümünden beri mevcuttur. Detaylar için tıklayınız.

Cisco, Hacklendiğini Doğruladı!

Cisco, 10.08.2022 Çarşamba günü, Yanluowang Ransomware grubunun dosyalarının yayınlayacağını iddia etmesinden ve çalınan bilgilerin ekran görüntülerini dark web'de yayınlamasından kısa bir süre sonra çalışanı üzerinden hack vakası gerçekleştirildiğini onayladı. Olayda birçok ransomware grubunun ismi geçmesine rağmen (UNC2447, Lapsus$, Yanluowang) dosya ekran

görüntülerini paylaşan grup Yanluowang ransomware grubudur. Detaylar için tıklayınız.

Facebook'ta Gösterilen Reklam İçerikleri Ne Kadar Güvenilir?

Android cihazlar için sistem temizleyiciler ve optimize ediciler olarak, Google Play Store'da yer alan uygulamaların Facebook'ta tanıtılmasıyla hatırı sayılır sayıda kullanıcı bu uygulamaları güvenliğini sorgulamadan indiriyor. Detaylar için tıklayınız.

Microsoft, Windows 11'e RDP 'Brute Force' Saldırılarına Karşı Varsayılan Koruma Ekliyor

Microsoft, gelişen tehdit ortamını karşılamak için güvenlik potansiyelini yükseltmek amacıyla Windows 11 işletim sisteminin en son sürümünün bir parçası olan Uzak Masaüstü Protokolü (RDP), Brute Force saldırılarını önlemek için adımlar atıyor. Microsoft'un işletim sistemi güvenliği ve kurumsal başkan yardımcısı David Weston, "Windows 11 derlemelerinin artık RDP ve diğer Brute Force parola vektörlerini azaltmak için bir varsayılan hesap kilitleme politikası var" dedi. Bu teknik, insan tarafından çalıştırılan fidye yazılımlarında ve diğer saldırılarda Windows işletim sistemine sahip bilgisayarlara izinsiz erişim sağlamak için kullanılan en popüler yöntemlerden biri olmuştur. Detaylar için tıklayınız.

Dolandırıcıların Yeni Hedefi Microsoft Kripto Yatırımcıları Metamask Phishing

Cyber Watchdog Armorblox tarafından Microsoft 365 savunmasını atlamak için popüler kripto cüzdanı MetaMask'i taklit eden bir kimlik avı saldırısı tespit edildi. Araştırmacılar, kullanıcıların kripto para birimlerini depolamasına ve takas etmesine, blok zinciri ile etkileşime girmesine ve blok zinciri dağıtılmış bir defter tarafından desteklenen merkezi olmayan bir ağ üzerinde inşa edilen App'lere ev sahipliği yapmasına olanak tanıyan en yaygın kullanılan kripto uygulamalarından biri olan MetaMask taklit eden bir kimlik avı saldırısı tespit etti. Detaylar için tıklayınız.

Reddit'te CSRF Açığı!

Bir sosyal tartışma ve haber sitesi olan Reddit'te CSRF (Cross- Site Forgery) güvenlik açığı; yalnız yetişkinlerin erişebileceği içerikleri yetişkin olmayan kullanıcılarında görüntülemesine zorladı. Orta önem derecesine sahip güvenlik hatası, belirli ayarları devre dışı bıraktı. Bu, kötü niyetli ajanların, yetişkin olmayan kullanıcıları içeriğe yönlendirebileceği ihtimalini ortaya çıkardı. Detaylar için tıklayınız.

Microsoft Zero-Day Açığı!

Haziran ayının başlarında nao_sec ekibindeki araştırmacılar, Windows makinelerde uzaktan kod çalıştırmayı sağlayan Follina zero-day zafiyetini bulmuşlardır. Detaylar için tıklayınız.

Çinli Bilgisayar Korsanları Ağ Trafiğini Gözetlemek İçin Telekomünikasyon Sistemlerini İhlal Etti!

Çin destekli tehdit aktörlerinin kimlik bilgilerini çalmak ve verileri toplamak için büyük telekomünikasyon şirketlerini ve ağ hizmeti sağlayıcılarını hedef aldığını ve tehlikeye attığını açıkladı. Detaylar için tıklayınız.

Bilgisayar Korsanları Windows Olay Günlükleri Kategori 0x4142 Kötü Amaçlı Yazılımları Gizliyor!

Yeni Kaos Fidye Yazılımı Oluşturucu Varyantı "Yashma" Vahşi Doğada Keşfedildi. Siber güvenlik araştırmacıları, Yashma olarak adlandırılan Chaos fidye yazılımı serisinin en son sürümünün ayrıntılarını açıkladı. Detaylar için tıklayınız.

Allianz 'Risk Barometresi 2022' Sonuçlarını Yayımladı

Almanya'nın Münih kentinde bulunan dünyanın en büyük sigorta ve finansal yatırım şirketlerinden birisi olan Allianz Global Corporate & Specialty (AGCS) tarafından her yıl düzenli olarak gerçekleştirilen iş dünyası riskleri anketi 'Allianz Risk Barometresi 2022' sonuçları açıklandı. 2022 yılında 11'incisi yayımlanan yıllık küresel iş dünyası riskleri anketi: Allianz Risk Barometresi 89 ülke ve bölgeden 2 bin 650 kişilik; risk yöneticileri, brokerler, CEO'lar ve sigorta uzmanlarının da aralarında bulunduğu bir topluluğun görüşleri sonucu oluşturuldu. Detaylar için tıklayınız.

Siber Tehdit Aktörleri 850 WordPress Sitesini Ele Geçirdiğini İddia Etti

CyberArts siber güvenlik ekibi dark webde, birçok WordPress kullanıcısının wp-admin login bilgilerini sattığını iddia eden bir tehdit aktörü tespit etmiştir. Siber tehdit aktörü ile iletişime geçen siber istihbarat birimimiz örnek bilgileri almayı başarmıştır. Detaylar için tıklayınız.

Logo Yazılım Sanayi ve Ticaret A.Ş. Veri İhlal Bildirimi

Bir şahsın, veri sorumlusuna bir e-posta göndererek, bir veri sızıntısı olayı ile ilgili görüşmek istediğini belirtiği, bunun üzerine ilgili şahıs ile çevrimiçi bir görüşme gerçekleştirildiği, ilgili şahıs tarafından sızıntı olduğunun iddia edilen verilerin veri sorumlusuna iletildiği belirtilmiştir. Detaylar için tıklayınız.

Türk E-Ticaret ve Kamu Kurumlarına Yönelik 0-Day Sattığını İddia Eden Bir Tehdit Aktörü Tespit Edildi

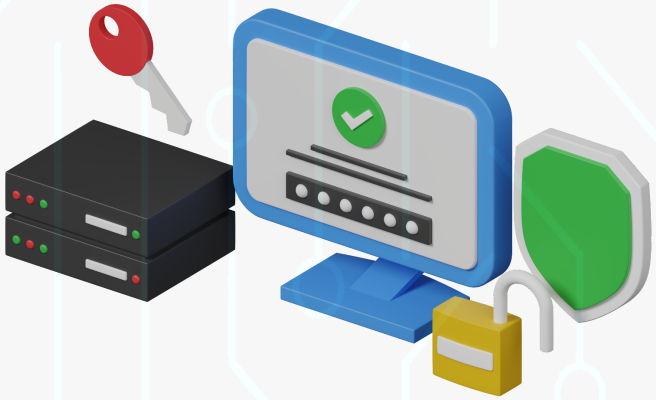
CyberArts siber güvenlik ekibi dark webde, birçok e-ticaret ve kamu kurumunda dosya yükleme alanı içinde uzaktan komut çalıştırılabilecekleri 0-Day sattığını iddia eden bir tehdit aktörü tespit etmiştir. Siber tehdit aktörü iddiasını kuvvetlendirmek adına yaptığı PoC'den ekran görüntüleri paylaşmıştır. Yaptığı

PoC kamu kurumlarından biri olduğu gözlenmiştir. PoC görüntülerinde ".gov" uzantısı dikkat çekmiştir. Detaylar için tıklayınız.

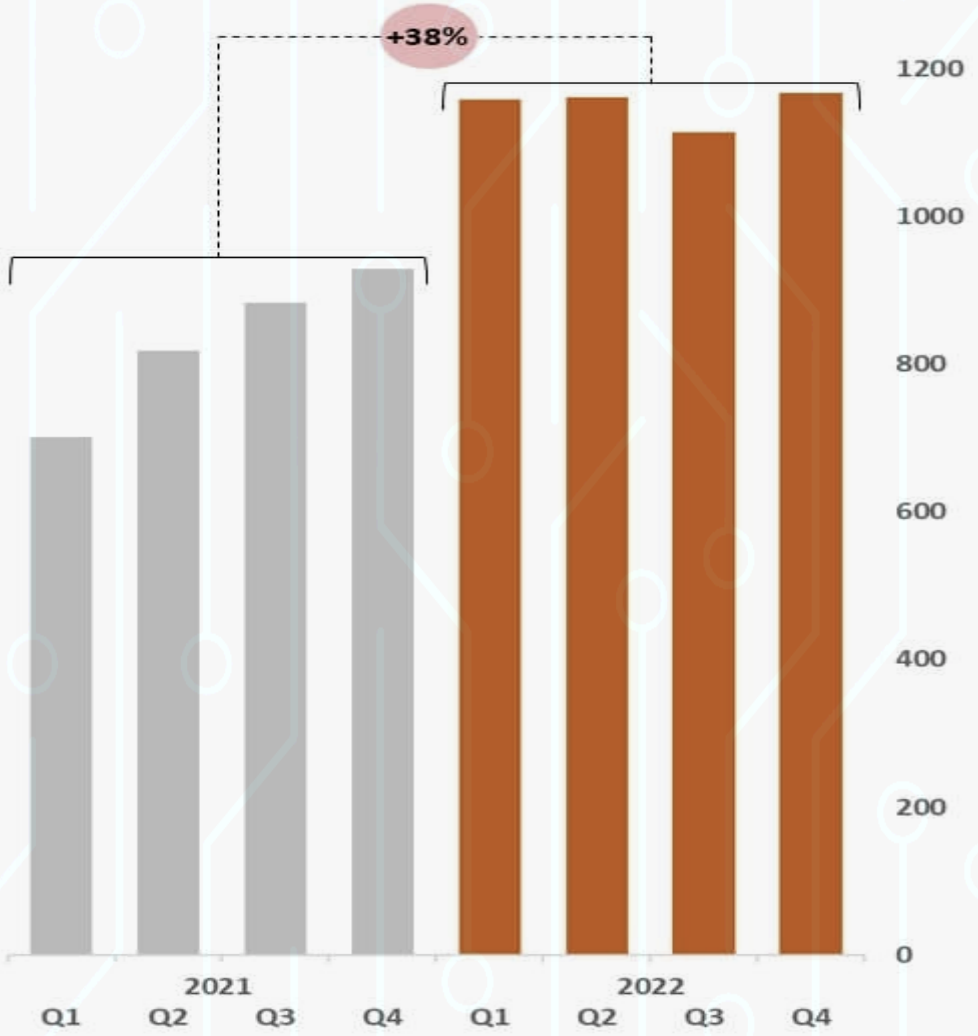
Sağlık Sektörünün Lideri Broward Health Veri İhlali Yaşadı!

Broward Health, Florida merkezli çok çeşitli tıbbi hizmetler sunan, otuzdan fazla lokasyona sahip bir sağlık sistemidir ve yılda 60.000'den fazla hasta kabul etmektedir. Detaylar için tıklayınız.

2022 SİBER GÜVENLİK İSTATİSTİKLERİ

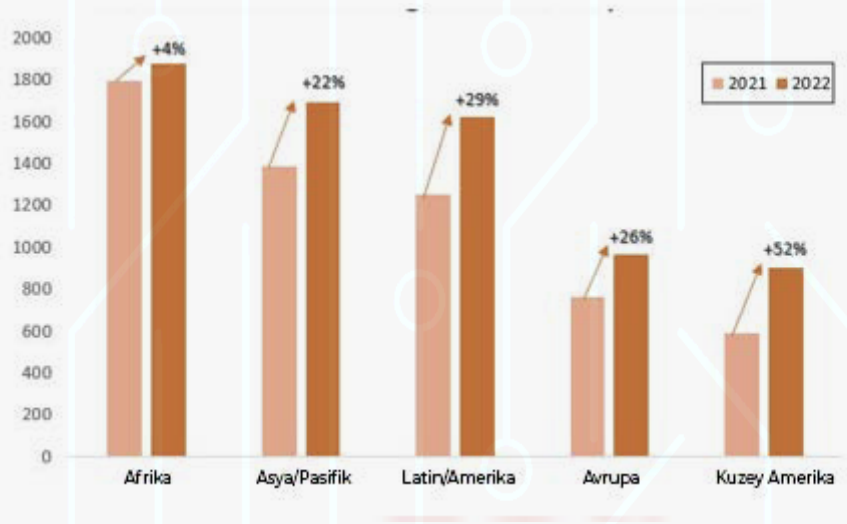


1. 2022'nin ilk yarısında dünya çapında yaklaşık 236,1 milyon fidye yazılımı saldırısı rapor edildi.
2. 2022 yılında ABD, Kanada, Birleşik Krallık, Avustralya ve Yeni Zelanda'yı kapsayan bir vaka çalışmasına katılanların %76'sı kuruluşlarının bu yıl en az 1 siber saldırıya maruz kaldığını belirtmiştir. Bu oran 2020'deki %55'lik orana göre büyük bir artış anlamına gelmektedir.
3. İşletme sahiplerinin %69'u başarılı bir siber saldırının KOBİ'lerini tamamen iflas ettirebileceğinden korkuyor.
4. 2022'de ihlallerin %82'si siber güvenlik farkındalığı düşük çalışan unsurunu içeriyordu.
5. İçeriden tehdit olayları son iki yılda %44 arttı ve olay başına maliyet üçte birden fazla artarak 15,38 milyon dolara ulaştı.
6. Tüm ihlallerin %43'ü kasıtlı ya da kasıtsız içeriden gelen tehditlerdir.
7. İçeriden gelen bir tehdit olayını kontrol altına alma süresi 77 günden 85 güne çıkmıştır.
8. Küçük, orta ve büyük ölçekli işletmeler BT ve siber güvenliklerini sırasıyla %58, %55 ve %60 oranlarında dış kaynak kullanımı ile yaptırmaktadır.
9. 2022 yılında Türkiye'de gerçekleşen kötü amaçlı yazılım saldırıları bir önceki yıla göre %61 oranında artış göstererek 1.015.810'a ulaştı.



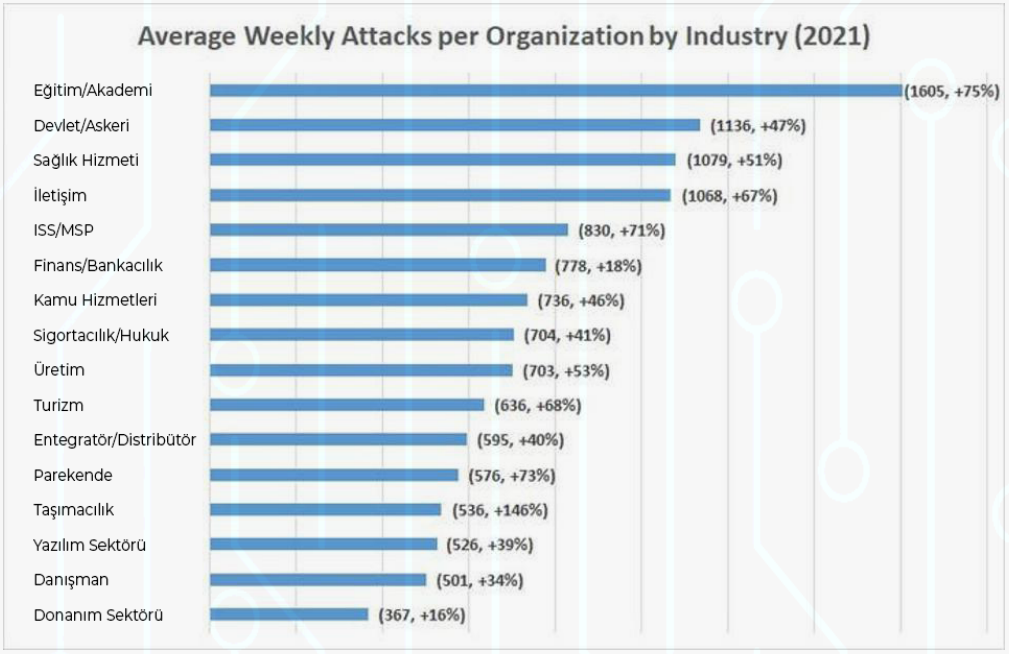
Şekil 1 - Yılların Çeyreklere Oranla Karşılaştırılması

Yukarıdaki istatistik 2021 ve 2022 yılları arasındaki çeyrekleri baz alarak (Dünya çapındaki) siber saldırı oranlarını kıyaslamıştır.



Şekil 2 - Kıtaların Yıllara Göre Karşılaştırılması

Yukarıdaki istatistik 2021 - 2022 yıllarını kıtalar baz alarak karşılaştırmaktadır.

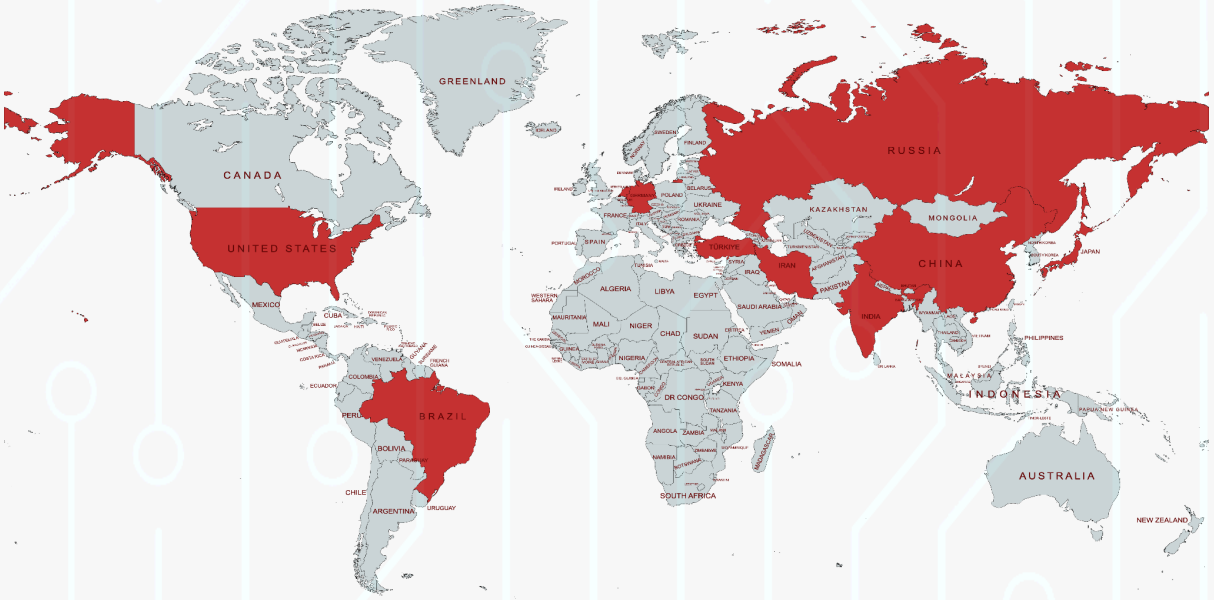


Şekil 3 - Sektörlerin Yıl Bazında Karşılaştırılması

Yukarıdaki istatistik 2021 – 2022 yıllarını sektörler baz alarak karşılaştırmaktadır. Grafiğin sonundaki değer 2021 yılındaki saldırını sayısını temsil etmektedir. Sağındaki artı (+) değer ise 2022 yılında ki artış oranını göstermektedir.

En Çok Siber Saldırı Yapan Ülkeler

En çok siber saldırı yapan ülkeler sırasıyla aşağıda listelenmiştir;



1- Hindistan

2- Amerika

3- Rusya

4- Çin

5- Türkiye

6- Almanya

7- Brezilya

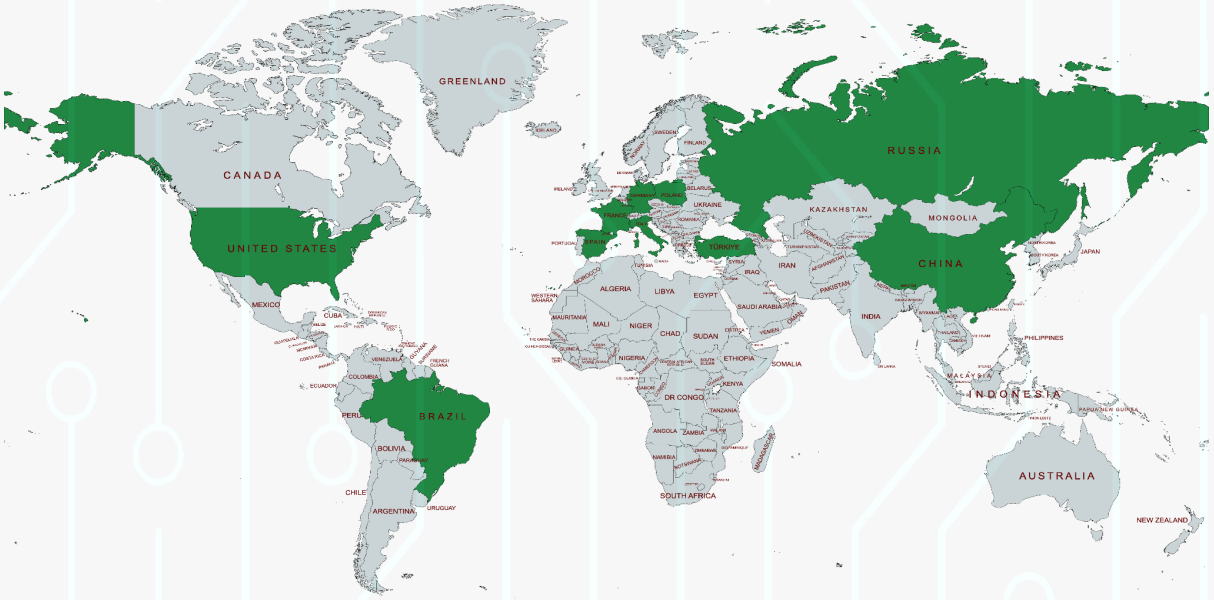
8- İran

9- Japonya

10- Hollanda

En Çok Siber Saldırı Yapılan Ülkeler

En çok siber saldırı yapılan ülkeler sırasıyla aşağıda listelenmiştir;



1- Çin

2- Amerika Birleşik Devletleri

3- Türkiye

4- Rusya

5- Almanya

6- Brezilya

7- İtalya

8- Fransa

9- İspanya

10- Polonya

Kaynakça / Referanslar:

1- https://cyberartspro.com

2-https://aag-it.com/the-latest-cyber-crime-statistics/#:~:text=Headline%20Cyber%20Crime%20Statistics&text=Data%20breaches%20cost%20businesses%20an,a%20cyber%20attack%20in%202022.

3- https://abnormalsecurity.com/blog/cybersecurity-stats-2022

4- https://insights.integrity360.com/2022-in-22-cyber-security-statistics

5- https://www.ninjaone.com/blog/smb-cybersecurity-statistics-2022/