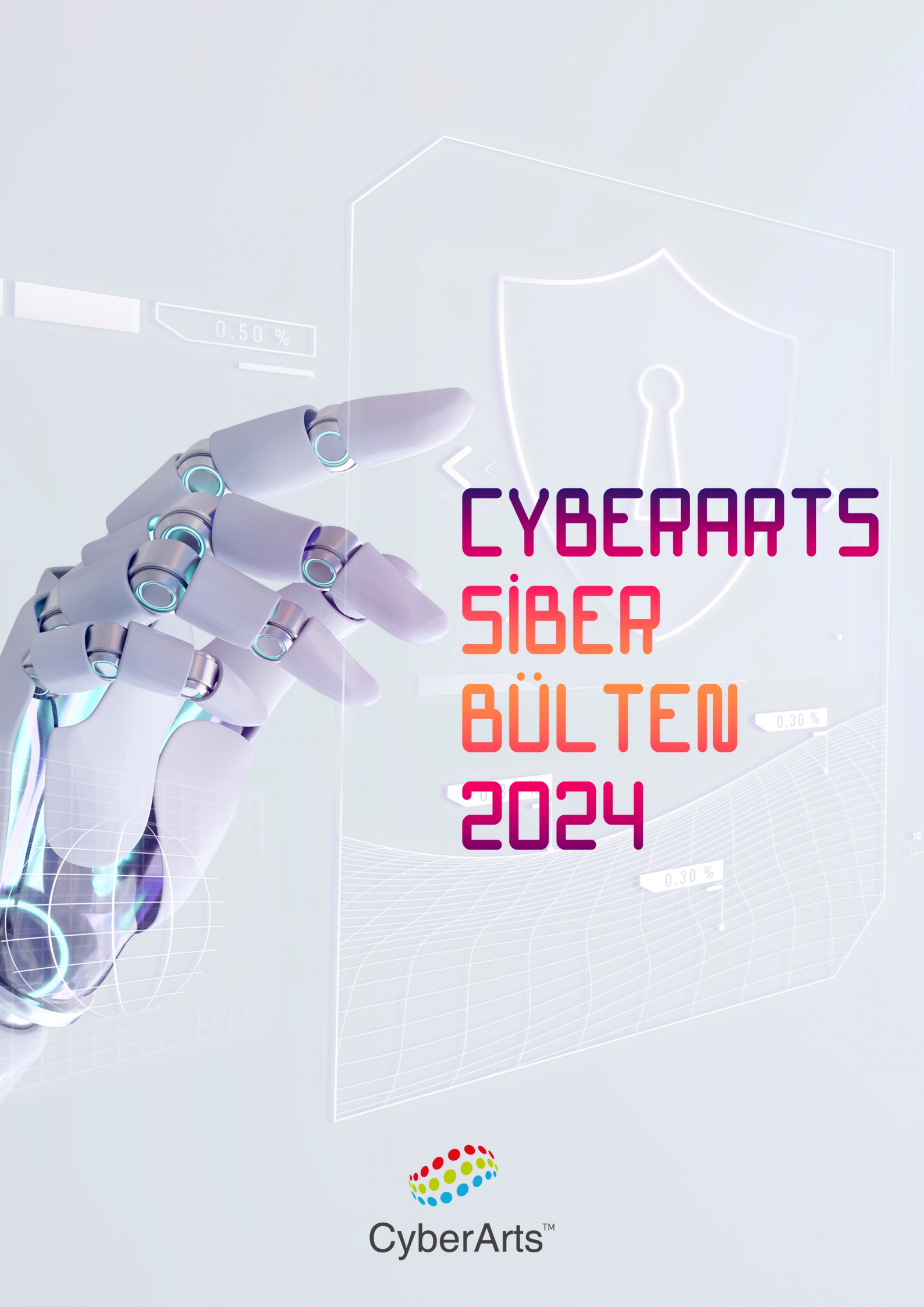


CYBERARTS SİBER BÜLTEN 2024

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.

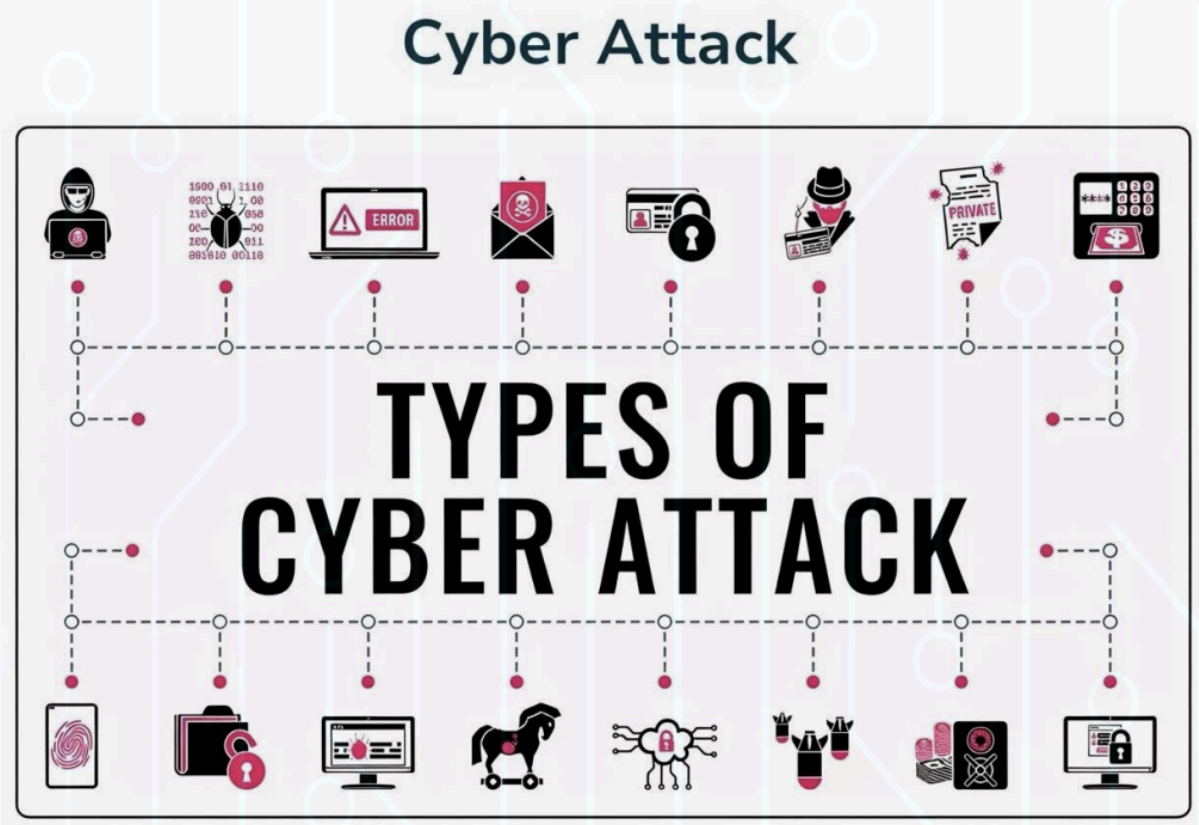
Danışmanlık verdiğimiz kurumlarda bir karar alırken bu kararın diğer iş süreçlerinde yaratacağı etkiyi ve sürdürülebilirliği ilk baştan hesaba katıyoruz. Uluslararası deneyime sahip siber sanatçılarımız sayesinde, büyük resmi görüp; insan kaynakları, süreçler ve teknolojileri kapsayacak bir stratejiyi 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 2024 yılında yapılmış siber olayları inceledik. En önemlisiber güvenlik haberlerini, trendlerini, saldıran tarafları ve bir sonraki siber salgının önlenmesi için öneriler sizin için derledik.

2024'ün En Çok Kullanılan 10 Atak Vektörü



1. Advanced Persistent Threats (APT): Uzun süreli, karmaşık hedefli saldırılar.

2. Zero-Day Açıkları: Daha önce bilinmeyen güvenlik açıklarının hızlısömürülmesi.

3. Supply Chain Attacks (Tedarik Zinciri Saldırıları): Güvenilir üçüncü tarafların hedef alınması.

4. Phishing (Oltalama): Kimlik avı saldırılarıyla hassas bilgilerin ele geçirilmesi.

5. Ransomware (Fidye Yazılımı): Sistemleri kilitleyerek fidye talep etme.

6. Insider Threats (Kurum İçi Tehditler): İçeriden gelen tehditler.

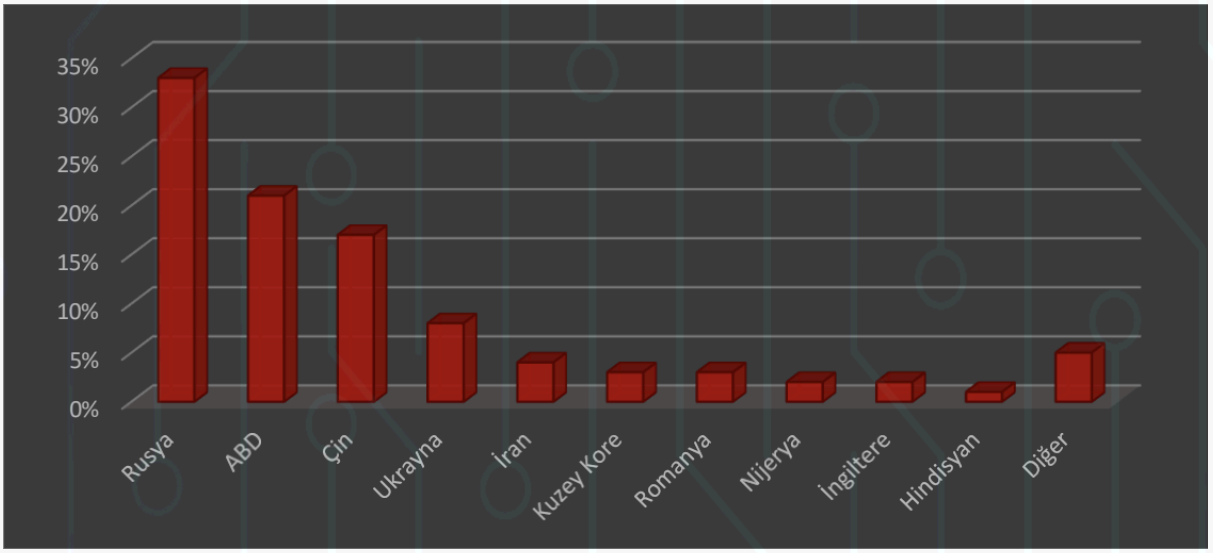
7. Weak Credentials(Zayıf Kimlik Bilgileri): Zayıf ve tekrar kullanılan parolaların istismarı.

8. Misconfiguration (Hatalı Konfigürasyon): Yanlış yapılandırmaların kötüye kullanılması.

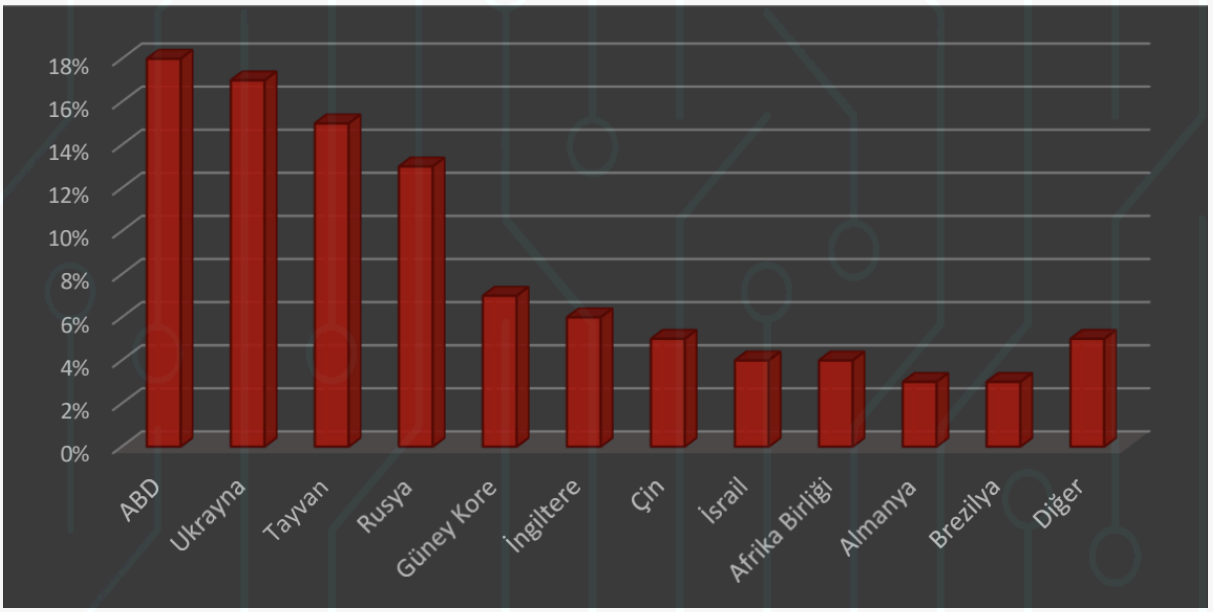
9. Missing or Poor Encryption (Yanlış veya Düşük Şifreleme): Yetersiz şifreleme yöntemlerinin kullanılması.

10. Malware (Kötü Amaçlı Yazılımlar): Casus yazılım, truva atları ve rootkitlerin yaygın kullanımı.

En Çok Siber Saldırı Yapan Ülkeler



En Çok Siber Saldırıya Uğrayan Ülkeler



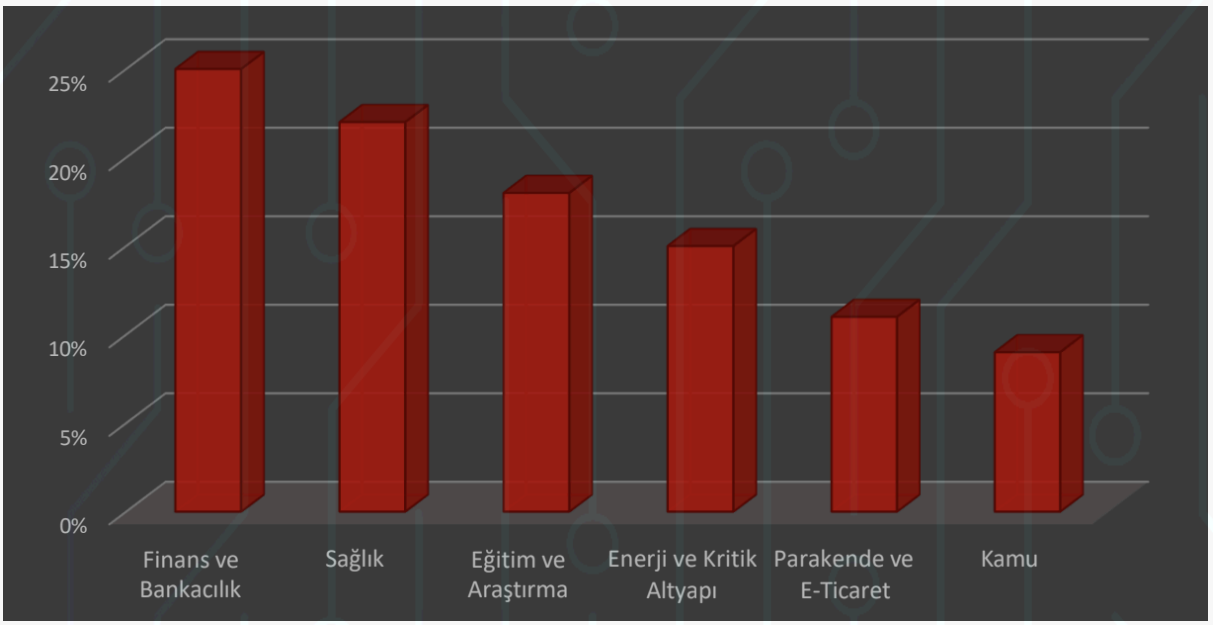
Rusya ve Çin gibi ülkelerin, özellikle devlet destekli siber saldırılarda aktif rol oynadığı bilinirken, ABD ve Avrupa ülkeleri ise savunma sistemlerini güçlendirmeye odaklanmıştır. Ukrayna örneğinde olduğu gibi, çatışma bölgelerinde siber saldırılar, fiziksel savaşın bir uzantısı haline gelmiştir. Bunun yanında, Tayvan gibi teknoloji merkezleri de ekonomik casusluk ve veri hırsızlığına yönelik saldırıların ana hedeflerinden biri olmuştur.

En Çok Siber Saldırı Alan Sektörler

2024 yılında bu tablo, siber saldırıların hedeflerini sektörler bazında nasıl çeşitlendiğini ve derinleştiğini gözler önüne sermektedir. Eğitim sektörünün en çok saldırıya maruz kalan alanlardan biri olması, özellikle uzaktan eğitim platformları ve öğrenci veritabanlarına yönelik tehditlerin arttığını göstermektedir.

Bu durum, eğitimin dijitalleşmesiyle birlikte güvenlik açıklarının daha sık kullanılabileceğini işaret etmektedir.

Sağlık ve finans sektörlerinin, yüksek hassasiyette veriler barındırmaları nedeniyle siber saldırganların birincil hedefleri olmaya devam ettiği görülmektedir. Sağlıkta hasta bilgilerinin çalınması veya fidye yazılımı saldırıları, finans sektöründe ise banka sistemlerine ve ödeme ağlarına yapılan saldırılar 2024'te öne çıkan tehditler arasında yer almıştır.



2024 Yılında Gerçekleşen En Yüksek Veri Sızıntıları

1. MOAB (Mother of All Breaches)

Ocak 2024'te tespit edilen bu veri sızıntısı, 26 milyar veri kaydının ihlal edilmesiyle dikkat çekmiştir. Sızdırılan veriler arasında Twitter, Reddit ve Wattpad gibi popüler platformlarda yer alan 1.5 milyar insana ait bilgiler bulunmaktadır. Bu büyük veri sızıntısı, kişisel bilgilerin kötüye kullanımına yol açarak küresel çapta ciddi güvenlik tehditleri yaratmıştır. Sızıntı boyutu yaklaşık 12 Terabayt (TB) olarak hesaplanmıştır.

2. RockYou2024

Temmuz 2024'te gerçekleşen bu verisızıntısı, yaklaşık 10 milyar benzersizşifreyi içermektedir. Bu sızıntı, eski ve yeni veri ihlallerinden derlenen şifrelerin bir

koleksiyonudur. Bu kadar büyük bir şifre sızıntısı, dünya çapında çok sayıda hesap için güvenlik risklerini artırır ve siber suçlular için büyük bir fırsat oluşturur.

3. Ubisoft Veri Sızıntısı

2024 yılında oyun ve eğlence devi Ubisoft, sunucularına yapılan bir siber saldırı sonucu büyük bir veri sızıntısı yaşadı. Milyonlarca kullanıcıya ait kişisel bilgiler, oyun hesapları ve ödeme bilgileri sızdırıldı. Sızıntı boyutu yaklaşık 5 Terabayt (TB) olarak hesaplandı. Bu tür bir sızıntı, kullanıcıların finansal güvenliğini tehdit eder ve kimlik avı gibi siber saldırıların artmasına yol açabilir.

4. Hindistan Mobil Ağ Veri Sızıntısı

Hindistan'da 750 milyon vatandaşın kişisel verileri, bir yeraltı forumunda satışa sunulmuştur. Bu sızıntı, kimlik hırsızlığı ve dolandırıcılık gibi suçlar için ciddi bir fırsat yaratmaktadır. Ancak verilerin çoğu anonim kalmakla birlikte, kişisel güvenlik tehditleri hala mevcuttur. Sızıntının boyutu oldukça büyük olmakla birlikte, daha spesifik ve doğrudan bir güvenlik tehdidi oluşturmamaktadır.

5. Planeta Araştırma Merkezi Saldırısı

2024 yılında Rusya'nın Planeta araştırma merkezine yapılan bir siber saldırı sonucu, 2 petabayt veri silindi. Bu saldırı, kişisel verilerin sızdırılmasından ziyade, verilerin kaybına yol açmıştır. Ancak yine de bu olay, önemli verilerin kaybına yol açarak büyük bir güvenlik ihlali teşkil etmektedir. Bu tür saldırılar, siber güvenlik açısından kritik altyapıların tehdit altında olduğunu göstermektedir.

En Tehlikeli APT Grupları

APT41 (Double Dragon): Çin devlet destekli bir grup olup hem casusluk hem de finansal motivasyonlu operasyonlar gerçekleştirmekte ve küresel ölçekte çeşitli sektörleri hedef almaktadır.

Sandworm: Rusya istihbaratıyla bağlantılı bu grup, kritik altyapıyı hedef alan casusluk ve yıkıcı saldırılarla tanınmaktadır.

APT29 (Cozy Bear): Rusya istihbaratına bağlı olan APT29, özellikle hükümet ve siyasi varlıkları hedef alan çok sayıda casusluk kampanyasında yer almıştır.

APT10 (Red Apollo): Çin merkezli bu grup, yönetilen BT hizmet sağlayıcılarını hedef alarak çeşitli endüstrilerdeki hassas verilere erişimi sağlamasıyla bilinir.

Lazarus Group: Kuzey Kore devlet destekli bu grup, finansal hırsızlık ve yıkıcı saldırılar gibi çeşitli siber operasyonlara katılmaktadır.

APT28 (Fancy Bear): Rus askeri istihbaratıyla bağlantılı olan bu grup, özellikle siyasi bağlamda casusluk ve etki operasyonlarıyla öne çıkmaktadır.

Hafnium: Çin destekli bir grup olan Hafnium, özellikle Microsoft Exchange Server'daki güvenlik açıklarını istismar ederek ABD'deki kuruluşları hedef almıştır.

APT32 (OceanLotus): Vietnam merkezli bu grup, Güneydoğu Asya'da siyasi ve özel sektör organizasyonlarını hedef alan casusluk faaliyetleriyle bilinir.

APT33 (Elfin): İran kaynaklı bu grup, havacılık ve enerjisektörlerini hedef alan casusluk ve yıkıcı saldırılar gerçekleştirmektedir.

APT35 (Charming Kitten): İran devlet destekli bir grup olan APT35, sosyal mühendislik yöntemlerini kullanarak bireyleri ve kuruluşları hedef alan casusluk faaliyetleri yürütmektedir.

En Tehlikeli Tehdit Aktörleri

RansomHub: Gelişmiş şifreleme yöntemleri ve yüksek fidye talepleriyle tanınan, çeşitli sektörlerde sayısız saldırıya imza atan bir fidye yazılımı grubu.

Qilin Ransomware: Çift taraflı şantaj tekniklerini kullanarak farklı endüstrileri hedef alan gelişmiş bir fidye yazılımı grubu.

Dark Angels: Agresif taktikleri ve geniş çaplı saldırılarıyla bilinen, ciddi operasyonel kesintilere neden olan bir fidye yazılımı grubu.

LockBit: Sürekli olarak kötü amaçlı yazılımlarını ve stratejilerini geliştiren, yüksek aktivite seviyesiyle dikkat çeken bir fidye yazılımı grubu.

WhiteWarlock: Çeşitli sektörlerde hassas bilgileri hedef alan karmaşık siber casusluk faaliyetleriyle tanınan yeni bir tehdit aktörü.

IntelBroker: Küresel ölçekte çok sayıda kuruluşu etkileyen veri ihlalleri ve çalınan bilgilerin satışı konusunda uzmanlaşmış bir siber suç grubu.

Cyber Army of Russia Reborn: Özellikle politik ve devlet hedeflerine yönelik siber saldırılar gerçekleştiren, Rusya yanlısı bir hacktivist grup.

NoName057(16): Politik görüşlerine karşı olan kuruluşlara dağıtık hizmet engelleme (DDoS) saldırıları düzenleyen bir hacktivist grup.

Sandworm: Rus istihbaratına bağlı bir APT grubu olup, kritik altyapıyı hedef alan yıkıcı saldırılar ve casusluk faaliyetleriyle tanınır.

Scattered Spider: Gelişmişsosyal mühendislik taktikleriyle çeşitli sektörlerde hedeflenen saldırılar düzenleyen yeni bir tehdit aktörü.

En Tehlikeli CVE'ler

CVE-2024-47575: FortiManager'da kritik bir fonksiyon için eksik kimlik doğrulama nedeniyle uzaktan kod yürütülmesine olanak sağlayan bir güvenlik açığı.

CVE-2024-21260: Oracle WebLogic Server'da, T3 veya IIOP protokolleri üzerinden kimlik doğrulama gerekmeksizin uzaktan kod yürütülmesine yol açan bir açık.

CVE-2024-43625: Microsoft Windows VMSwitch'te ayrıcalık yükseltme güvenlik açığı, saldırganların sistem üzerinde daha yüksek yetkiler elde etmesine izin verebilir.

CVE-2024-35250: Microsoft Windows Kernel-Mode Driver'da güvenilmeyen bir işaretçi kullanımı, yerel saldırganların yetki artırmasına olanak tanıyor.

CVE-2024-49138: Microsoft Windows Common Log File System (CLFS) sürücüsünde yığın tabanlı bellek taşması, yerel saldırganların yetki artırmasına izin veriyor.

CVE-2024-51378: CyberPanel'de yanlış varsayılan izinler nedeniyle kimlik doğrulama atlatma ve rastgele komut çalıştırma mümkün oluyor.

CVE-2024-11680: ProjectSend uygulamasında uygunsuz kimlik doğrulama güvenlik açığı, özel HTTP istekleriyle uygulama yapılandırmasının yetkisiz bir şekilde değiştirilmesine izin veriyor.

CVE-2024-11667: Zyxel marka birçok güvenlik duvarının web yönetim arayüzünde dizin geçişi güvenlik açığı, saldırganların hazırlanmış URL'ler ile dosya indirip yüklemesine olanak tanıyor.

CVE-2024-43573: Microsoft HTML (MSHTML) platformunda yer alan bir sahtecilik güvenlik açığı, saldırganların web sitelerini veya uygulamaları taklit etmesine olanak tanıyor ve bu durum kimlik avı saldırılarına neden olabilir.

CVE-2024-28461: Array Networks AG ve vxAG ArrayOS'ta kritik bir fonksiyon için eksik kimlik doğrulama, saldırganların SSL VPN ağ geçidinde yerel dosyaları okumasına ve kod yürütmesine olanak tanıyor.

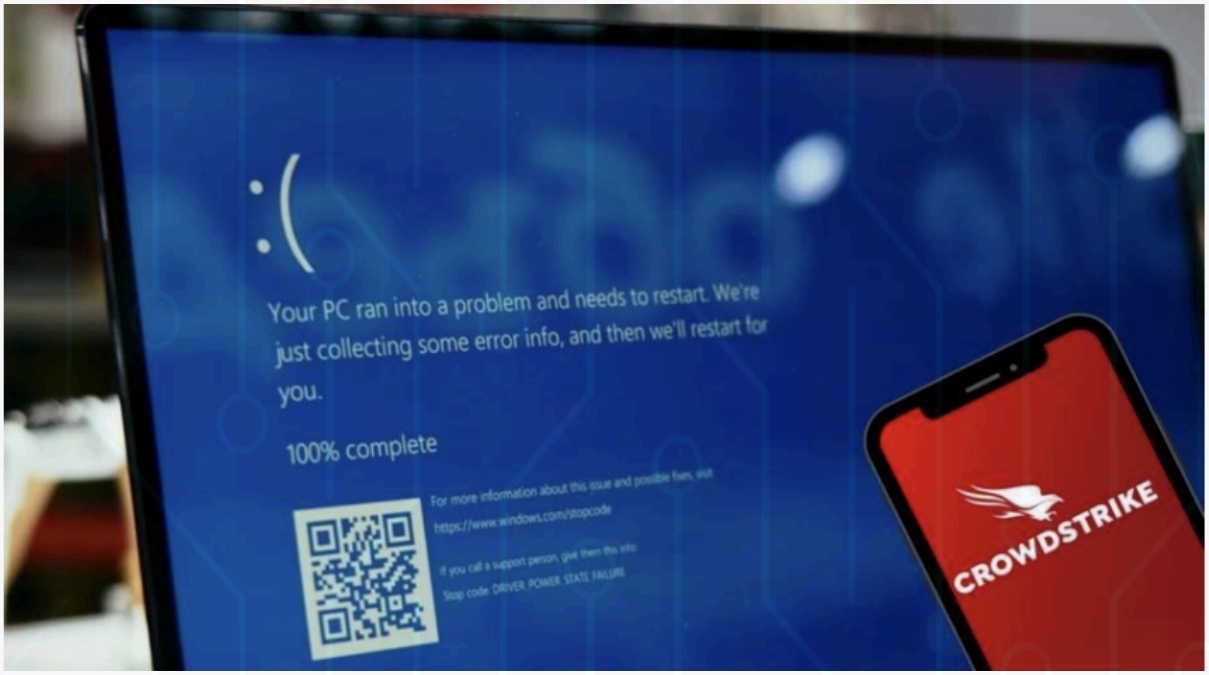
2024 Yılının Siber Güvenlik Alanında En Unutulmaz Olayları

İsrail'den Lübnan'a Siber Saldırı Çağrı Cihazları Bombaya Dönüştü

İsrail'in Lübnan'daki Hizbullah üyelerine yönelik gerçekleştirdiği saldırı, tarihin en sıra dışı ve en kanlı siber operasyonlarından biri olarak kayıtlara geçti. Bu saldırıda, Hizbullah tarafından kullanılan şifreli çağrı cihazları, bir dizi teknik müdahaleyle uzaktan aktive edilerek bombaya dönüştürüldü. Patlamalar sonucunda 9 kişi hayatını kaybetti, yaklaşık 3.000 kişi ise yaralandı. Detaylar için tıklayınız.

CrowdStrike Mavi Ekran Sorunu

Crowdstrike güncellemesi, Windows 10 kullanılan bilgisayarların çökmesine neden oldu. Sorunun kaynağı CrowdStrike update'i olup, geçici çözüm için Güvenli Mod veya Windows Kurtarma Ortamında problemli dosyanın silinmesi önerilmektedir. Detaylar için tıklayınız.



Cloudflare, 3,8 Tbpsile Şimdiye Kadarki En Büyük DDoS Saldırısını Püskürttü

Cloudflare, 3,8 Tbps zirvesine ulaşan ve 65 saniye süren rekor düzeyde bir DDoS saldırısını engellediğini açıkladı. Şirket, Eylül 2024'ün başından itibaren finansal hizmetler, internet ve telekomünikasyon sektörlerini hedef alan 100'den fazla hiper-hacimli DDoS saldırısını durdurduğunu belirtti. Detaylar için tıklayınız.

AnyDesk Hacklendi: Milyonlarca Kullanıcı Risk Altında

AnyDesk, 2024'ün ilk aylarında siber saldırıya uğrayarak kaynak kodu ve özel kod imzalama anahtarlarını kaybetti. Bu olay, milyonlarca kullanıcının güvenliğini tehlikeye attı. Detaylar için tıklayınız.

INTERPOL'dan Siber Suçlara Büyük Darbe: 1.006 Tutuklama, 134.089 Kötü Amaçlı Ağ Çökertildi

INTERPOL liderliğinde gerçekleştirilen bir operasyon, Afrika kıtasında siber suçları engellemek amacıyla düzenlenen koordineli bir çaba sonucunda 19 Afrika ülkesinde 1.006 şüphelinin tutuklanması ve 134.089 kötü amaçlı altyapı ve ağın çökertilmesiyle sonuçlandı. Detaylar için tıklayınız.

HGS Sistemine Siber Saldırı

Hızlı Geçiş Sistemi'nin (HGS) iPhone mobil uygulaması ciddi bir siber saldırıya maruz kaldı. Dolandırıcılar, uygulamanın güvenlik açıklarını kullanarak kullanıcı hesaplarına erişim sağladı ve bu süreçte birçok kişinin kişisel bilgilerini ve ödeme detaylarını ele geçirdi. Detaylar için tıklayınız.

Kaynakça / Referanslar:

1. National Vulnerability Database (NVD)

- Erişim adresi: https://nvd.nist.gov/
- Açıklama: NVD, yazılımların güvenlik açıklarını kataloglayan ulusal bir veri tabanıdır.

2. Cloudflare

- Erişim adresi: https://www.cloudflare.com/
- Açıklama: Cloudflare, DDoS koruması, web güvenliği ve performans iyileştirme alanlarında hizmet sunan bir şirket.

3. STM

- Erişim adresi: https://www.stm.com.tr/tr
- Açıklama: STM, savunma sanayi ve siber güvenlik alanında yenilikçi çözümler sunan Türk bir şirket.

4. Fortinet

- Erişim adresi: https://www.fortinet.com/
- Açıklama: Fortinet, kurumsal güvenlik çözümleri ve siber tehdit koruma hizmetleri sunmaktadır.

5. MITRE ATT&CK

- Erişim adresi: https://attack.mitre.org/
- Açıklama: MITRE ATT&CK, siber tehdit aktörlerinin tekniklerini ve taktikerini belgeleyen kapsamla bir bilgi tabanı.

6. CrowdStrike

- Erişim adresi: https://www.crowdstrike.com/
- Açıklama: CrowdStrike, siber tehdit avcılığı, analiz ve endpoint koruma hizmetleri sunan bir firma.

7. CyberArts Haber

- Erişim adresi: https://cyberartspro.com
- CyberArts, 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 sunmaktadır.