SİBER OLAYLAR

Öğr. Gör. Halil ARSLAN

Sayılarla Dünya Analizi

Dünya'da...

- Nüfus : 8.2 milyar +
- Internet kullanıcısı: 5.45 milyar (statista)
- Sosyal medya kullanıcısı: 5.17 milyar (statista)
- Mobil kullanıcı sayısı : 5.68 milyar, nufüsun %70 (datareportal)
- Internet erişim cihazları: (statcounter)
  - Mobil %61.7, Pc %36.2, Tablet %1.9
- İşletim sistemleri : (statcounter)
  - Android %45, Windows %26, IOS %18, Mac%5.6, Linux %1.6
- Tarayıcı Uygulamaları: (statcounter)
  - Chrome %65, Safari %18, Edge %5, Firefox %3, Opera %2

https://www.statista.com/statistics/617136/digital-population-worldwide/
https://datareportal.com/global-digital-overview
https://gs.statcounter.com/os-market-share

Sayılarla Türkiye Analizi

Türkiye'de...

- Nüfus : 85.3 milyon +
- Internet kullanıcısı: 74.4 milyon (datareportal)
- Sosyal medya kullanıcısı: 57.5 milyon (statista)
- Mobil kullanıcı sayısı: 80.6 milyon, nüfusun % 94 (datareportal)
- Internet erişim cihazları: (statcounter)
  - Mobil %75, Pc %23.3, Tablet %1.4
- İşletim sistemleri : (statcounter)
  - Android %60, Windows %18, IOS %16, Mac%1,2, Linux %1.7
- Tarayıcı Uygulamaları: (statcounter)
  - Chrome %74, Safari %13, Edge %2, Yandex %4, Samsung %3

https://www.statista.com/statistics/617136/digital-population-worldwide/
https://datareportal.com/global-digital-overview
https://gs.statcounter.com/os-market-share

Küresel Siber Suçlar

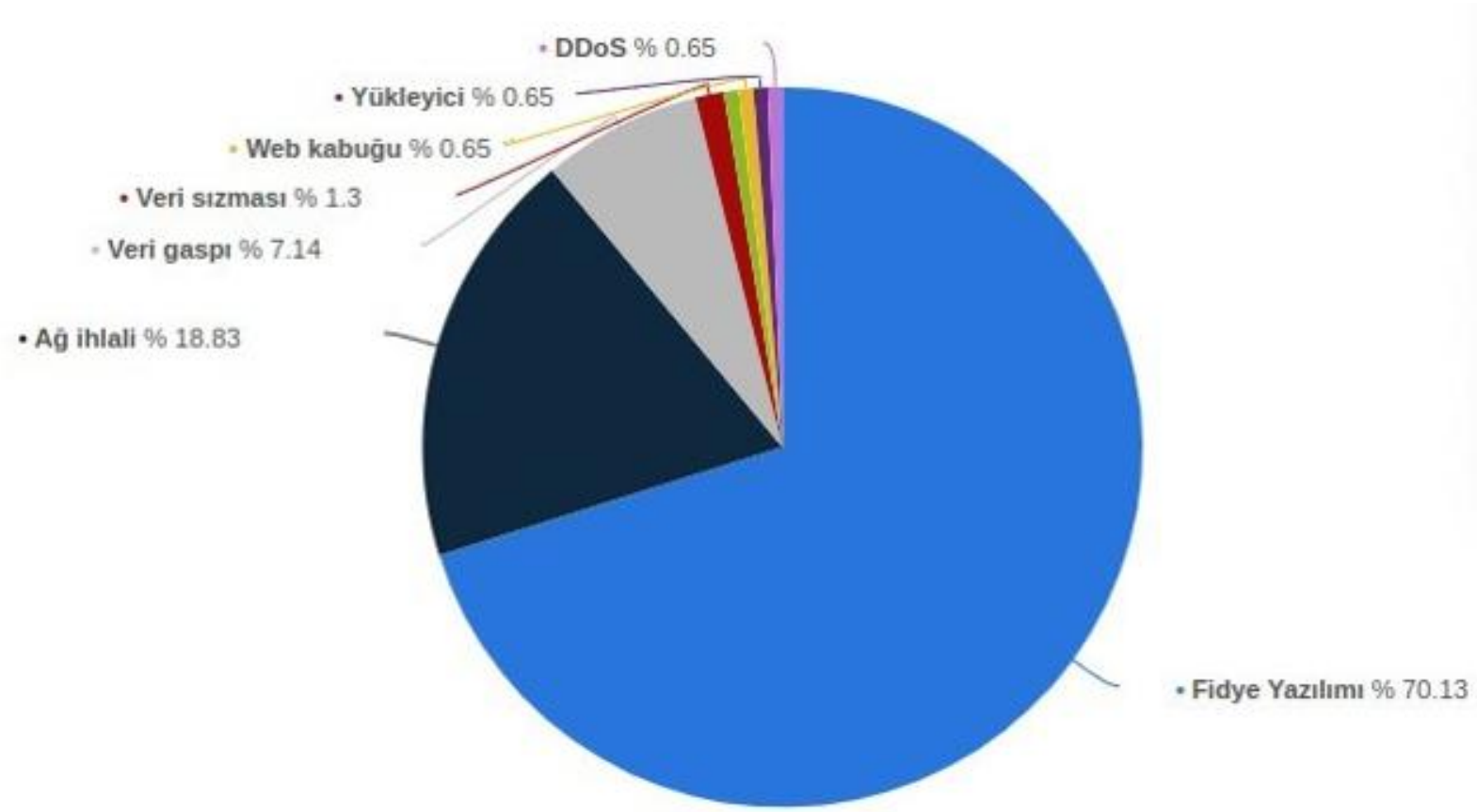
- Yılda gerçekleşen siber saldırı ~800.000
- Her 39 saniyede bir saldırı gerçekleşiyor.
- Yıllık küresel maliyet 10 trilyon dolar.
- Siber suçların %90'ı kimlik avı

  (Oltalama-Ransomware-Bec)
- Malware bulaşma yöntemi %92 e-posta

  (ekli dosya %39 Word)
- DdoS saldırılarında %110 artış.
- Dakikada 1.7 yeni kötü amaçlı yazılım.
- Fidye saldırısını tanımlamak için geçen süre ~49 gün.

https://www.usatoday.com/money/blueprint/business/vpn/cybersecurity-statistics/
https://www.getastra.com/blog/security-audit/cyber-security-statistics/

2023 Yılı Dünya Genelinde Siber Saldırı Türleri



https://www.statista.com/statistics/1382266/cyber-attacks-worldwide-by-type/

Avrupa Birliği Siber Güvenlik Ajansı (ENISA) Başlıca Siber Tehditler - 2023

https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

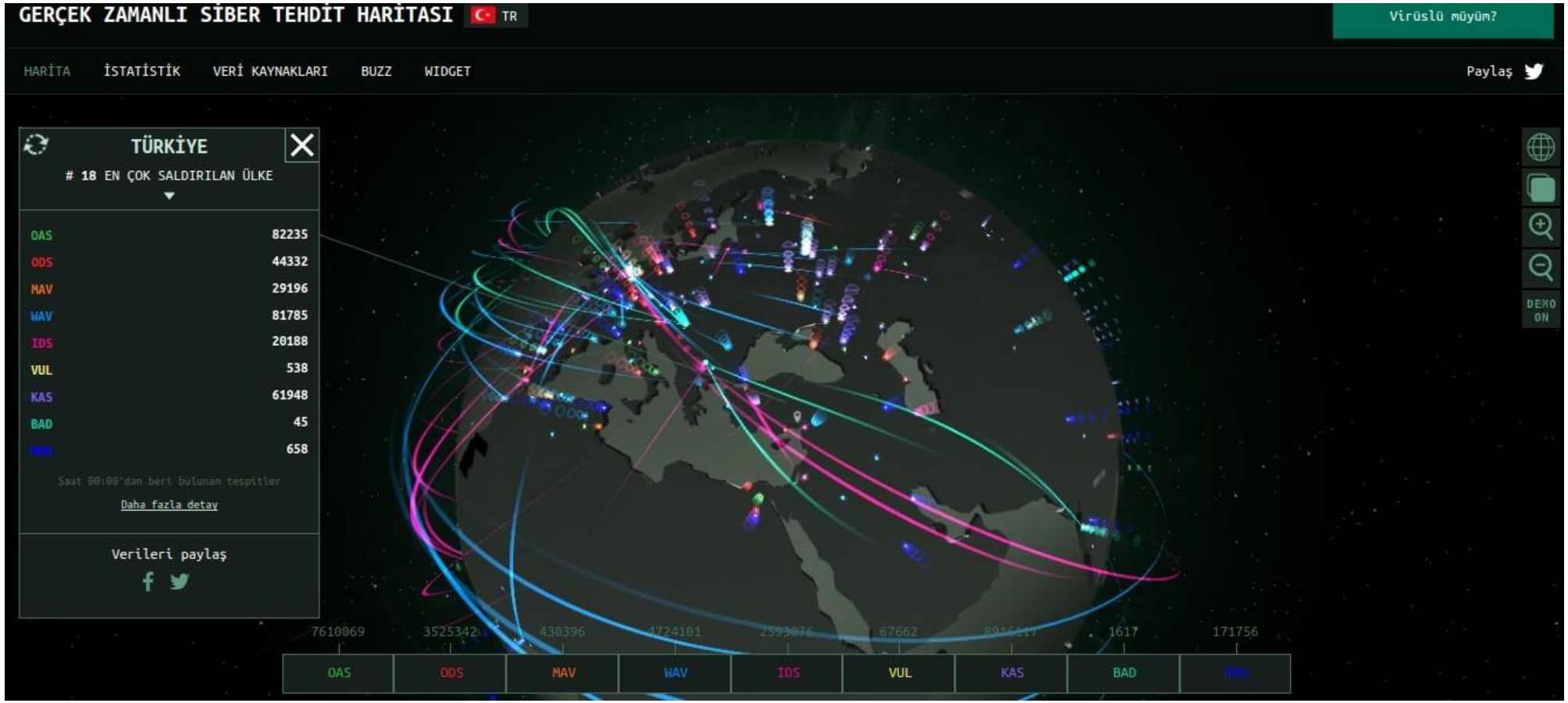
Avrupa Birliği Siber Güvenlik Ajansı (ENISA) Başlıca Siber Tehditler - 2030

https://www.enisa.europa.eu/publications/foresight-cybersecurity-threats-for-2030-update-2024-extended-report

Başlıca Siber Tehditlerde İlk 15

https://www.sprintzeal.com/blog/top-cybersecurity-threats

Kaspersky Siber Tehdit Haritası



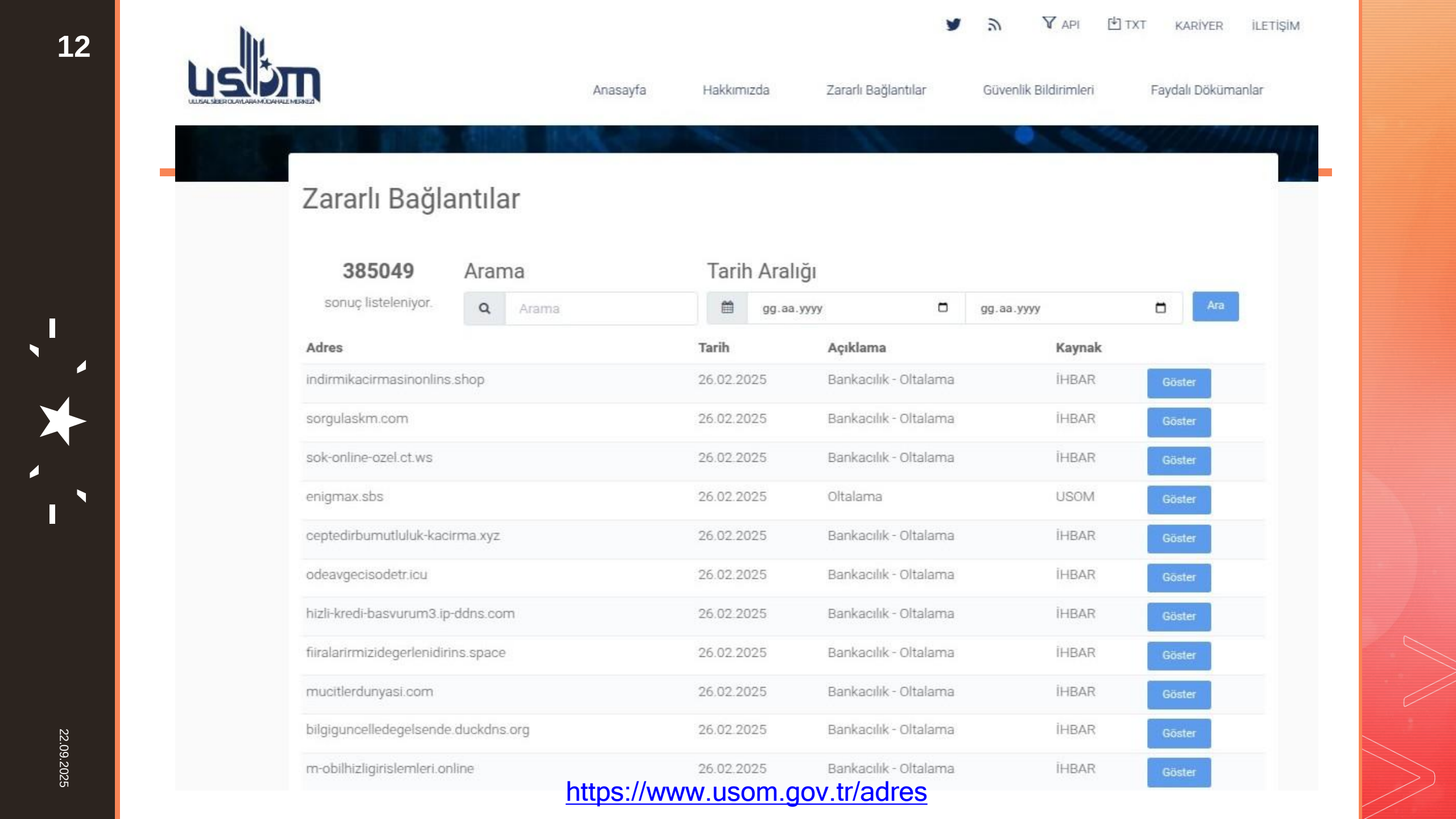
https://cybermap.kaspersky.com/tr

Siber Saldırı Olayları

- XKeyscore,
- PRISM,
- ECHELON,
- Carnivore,
- DISHFIRE,
- STONEGHOST,
- Tempora,
- Frenchelon,
- Fairview,
- MYSTIC,
- DCSN,
- Boundless Informant,
- Stuxnet
- Melissa Virüsü
- BULLRUN,
- PINWALE,
- Stingray,
- Estonya
- Nasa
- MsExcahnge
- Marriott
- Mirai
- Ronin Network
- Uber
- Colonial Pipeline
- Sony PSN
- Yahoo
- Adobe
- Solarwinds
- Microsoft(lapsus$)
- Wannacry
- NotPetya
- Log4j
- RockYou2021
- Cambridge Analytica (Facebook)

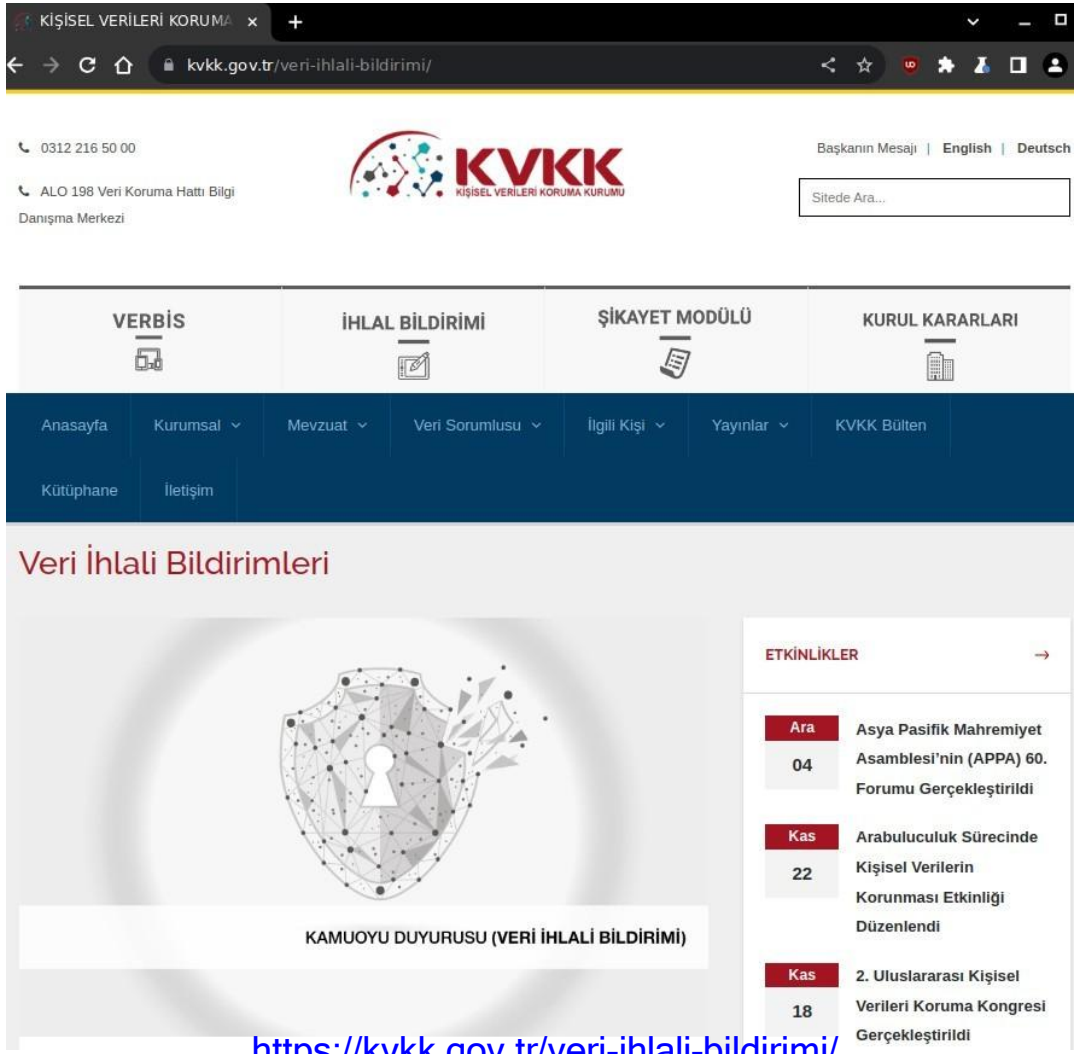
Siber Saldırı Olayları

- Melissa virüsü (1999)
  - E-posta ekinde word dosyası ile sistemlere bulaşan virüs
- WannaCry (2017)
  - 4 günde 150 ülkeden fazla yüzbinlerce sistemi fidye yazılım ile verilerin şifrelenmesi.
- Estonya (2007)
  - DdoS saldırıları ile ülkenin internet altyapısı işlemez hale geldi.
- Stuxnet (2010)
  - İran nükleer çalışmalarını sekteye uğratmak için yazılan solucan yazılımı.
-



https://www.usom.gov.tr/adres

KVKK Veri İhlali Bildirimi



https://kvkk.gov.tr/veri-ihlali-bildirimi/

İlk 15 Siber Saldırının Detayları

1. Fidye Yazılımı Saldırıları (Ransomware)

Tanım: Kurbanın verilerini şifreleyen veya sistemlere erişimi engelleyen kötü amaçlı yazılımlardır. Saldırganlar, verilerin şifresini çözmek veya erişimi geri vermek için fidye talep ederler. Modern ransomware türleri "çift şantaj" yöntemi kullanarak verileri hem şifreler hem de sızdırma tehdidiyle fidye talep eder.
Teknik: Ransomware genellikle phishing e-postaları, güvenlik açıkları (RDP, VPN) veya kötü amaçlı reklamlar (malvertising) yoluyla sisteme bulaşır. AES-256 veya RSA şifreleme algoritmaları kullanılarak dosyalar kilitlenir. Saldırganlar, Command & Control (C2) sunucuları üzerinden şifre çözme anahtarlarını kontrol eder. Ransomware-as-a-Service (RaaS) modeli ile deneyimsiz saldırganlar bile hazır altyapıları kiralayabilir.

Güncel Olay:
Change Healthcare Saldırısı (Şubat 2024): UnitedHealth Group'un bağlı kuruluşu Change Healthcare, ALPHV/BlackCat ransomware grubu tarafından saldırıya uğradı. 100 milyondan fazla kişinin hassas sağlık verileri (reçeteler, teşhisler, sigorta bilgileri) çalındı. Şirket 22 milyon dolar fidye ödedi ancak saldırganlar verileri yine de sızdırdı. ABD sağlık sisteminde reçete işlemleri günlerce durdu.
LockBit 3.0 Küresel Kampanya (2024): 2000'den fazla kurum etkilendi, toplam zarar 1 milyar doları aştı.

2. Nesnelerin İnterneti (IoT) Güvenlik Açıkları

Tanım: Akıllı ev cihazları, endüstriyel sensörler, güvenlik kameraları, medikal cihazlar gibi internete bağlı IoT cihazlarındaki güvenlik zayıflıklarıdır. Bu cihazlar genellikle zayıf parolalar, güncellenmeyen firmware ve güvensiz iletişim protokolleri ile çalışır, bu da onları siber saldırılara karşı savunmasız hale getirir.
Teknik: IoT cihazları genellikle varsayılan parolalarla gelir (admin/admin, root/root). Firmware güncellemeleri nadirdir veya hiç yapılmaz. Telnet, HTTP gibi şifrelenmemiş protokoller kullanılır. Botnet operatörleri (Mirai, Mozi) otomatik tarama araçlarıyla zayıf IoT cihazlarını tespit eder ve DDoS saldırıları için zombi ağlar oluşturur. UPnP protokolü kötüye kullanılarak ağ içine sızılabilir. Bazı cihazlar hardcoded (sabit kodlanmış) kimlik bilgileri içerir.

Güncel Olay:
•**TP-Link Router Zafiyeti (CVE-2024-5035, Mart 2024):** Milyonlarca TP-Link Archer serisinde kritik uzaktan kod çalıştırma açığı keşfedildi. Saldırganlar kimlik doğrulaması olmadan router'ı tam kontrol edebiliyor. Etkilenen cihazlar: Archer C5400X, AX6000 ve diğer popüler modeller.
•**Akıllı Kapı Kilidi Hackleme (2024):** Amazon Ring ve diğer akıllı kilit sistemlerinde Bluetooth açıkları bulundu, fiziksel güvenlik riski oluşturdu.

3. Sosyal Mühendislik ve Kimlik Avı (Phishing)

Tanım: İnsanların psikolojik zayıflıklarını kullanarak onları kandırma ve hassas bilgileri (şifreler, kredi kartı, kurumsal veriler) ele geçirme sanatıdır. E-posta (phishing), SMS (smishing), telefon (vishing) veya sosyal medya üzerinden gerçekleştirilir. Saldırganlar meşru kurum veya kişileri taklit ederek güven oluşturur ve aciliyet hissi yaratarak kurbana hızlı karar verdirtir.
Teknik: Spear-phishing (hedefli saldırı) için OSINT (açık kaynak istihbaratı) kullanılarak hedef hakkında bilgi toplanır. E-posta spoofing ile gönderici adresi sahte gösterilir. Homograph saldırılarında benzer görünen karakterlerle sahte domain oluşturulur (apple.com → apple.com - Kiril 'a'). Kötü amaçlı makrolar içeren Office belgeleri veya PDF'ler kullanılır. Credential harvesting için sahte login sayfaları (phishing kitleri) hazırlanır. Business Email Compromise (BEC) saldırılarında CEO veya CFO taklit edilerek büyük transferler yapılır.

Güncel Olay:
•**Microsoft Teams Phishing Kampanyası (Mayıs 2024):** Saldırganlar, Microsoft Teams üzerinden sahte toplantı davetleri göndererek kullanıcıları kötü amaçlı linklere yönlendirdi. "Acil toplantı" bahanesiyle kimlik bilgileri çalındı. 10.000'den fazla kurumsal hesap tehlikeye girdi.
•**QR Kod Phishing (Quishing, 2024):** PDF eklerindeki QR kodlar taranarak mobil cihazlarda güvenlik kontrollerini atlayan saldırılar arttı. %587 artış kaydedildi.

4. Tedarik Zinciri Saldırıları (Supply Chain Attacks)

Tanım: Hedef organizasyona doğrudan saldırmak yerine, güvenilir tedarikçileri, yazılım sağlayıcılarını veya üçüncü taraf hizmetleri kompromize ederek hedefe ulaşma stratejisidir. Bir yazılım güncellemesi, donanım bileşeni veya bulut servisi üzerinden zararlı kod tüm müşterilere yayılabilir. Güven ilişkisi istismar edildiği için tespit edilmesi zordur.
Teknik: Software supply chain saldırılarında kaynak kod deposuna (GitHub, GitLab) sızılır veya build pipeline manipüle edilir. Dependency confusion ile sahte paketler resmi paket depolarına (npm, PyPI) yüklenir. Code signing sertifikaları çalınarak kötü amaçlı yazılımlar imzalanır. Hardware supply chain'de ise üretim aşamasında veya nakliye sırasında cihazlara backdoor eklenir. Managed Service Provider (MSP) saldırılarında tek bir hizmet sağlayıcı üzerinden yüzlerce müşteriye erişilir.

Güncel Olay:
•**3CX Telefon Yazılımı Saldırısı (Mart 2024):** Popüler VoIP yazılımı 3CX'in resmi güncellemesi, kuzey Kore bağlantılı Lazarus grubu tarafından zararlı kodla enfekte edildi. 600.000 şirket ve 12 milyon kullanıcı etkilendi. Saldırganlar, yazılımın build sürecine sızdılar ve dijital imza ile onaylanmış trojan dağıttılar.
•**XZ Utils Backdoor (CVE-2024-3094, Nisan 2024):** Yaygın kullanılan Linux sıkıştırma kütüphanesine backdoor eklenmesi son anda tespit edildi, potansiyel etki küresel olacaktı.

5. Yapay Zeka Destekli Siber Tehditler

Tanım: Yapay zeka ve makine öğrenimi teknolojilerinin saldırganlar tarafından daha sofistike, otomatik ve ölçeklenebilir saldırılar geliştirmek için kullanılmasıdır. AI, deepfake oluşturma, otomatik phishing e-postaları yazma, güvenlik sistemlerini atlama, adaptif malware geliştirme ve hedef seçiminde kullanılır. Aynı zamanda ChatGPT gibi araçların jailbreak edilerek kötü amaçlı kod üretimi de bu kategoriye girer.
Teknik: Generative AI (GPT, DALL-E) kullanılarak ikna edici phishing içerikleri otomatik üretilir. Deepfake teknolojisi ile ses (voice cloning) ve video (face swap) sahtekarları oluşturulur. Adversarial machine learning ile güvenlik sistemlerinin AI modellerine karşı düşmanca örnekler üretilir. Polymorphic malware, ML kullanarak her enfeksiyonda değişir ve imza tabanlı antivirüsleri atlatır. AI-powered password cracking ile parola kırma hızı artırılır. Automated vulnerability scanning ve exploitation için AI kullanılır.

Güncel Olay:
•**Hong Kong Deepfake CFO Dolandırıcılığı (Şubat 2024):** Bir şirketin finans çalışanı, deepfake teknolojisi kullanılarak oluşturulan sahte video konferans toplantısına katıldı. CFO ve diğer yöneticiler gibi görünen yapay zeka tabanlı deepfake'ler, çalışanı 25.6 milyon dolar transfer yapmaya ikna etti. Gerçek zamanlı, çok katılımcılı deepfake kullanılan ilk büyük dolandırıcılık vakası.

6. Gelişmiş Kalıcı Tehditler (APT - Advanced Persistent Threats)

Tanım: Uzun vadeli, hedefe özel, yüksek düzeyde organize edilmiş ve genellikle devlet destekli siber casusluk operasyonlarıdır. APT grupları, aylarca veya yıllarca hedef ağda gizlice kalabilir, hassas bilgileri sürekli olarak sızdırabilir. Hedefler genellikle devlet kurumları, savunma sanayii, kritik altyapılar, enerji şirketleri ve büyük teknoloji firmalarıdır.
Teknik: APT saldırıları multi-stage (çok aşamalı) gerçekleşir: keşif, ilk sızma (spear-phishing, zero-day), tutunma (persistence), yetki yükseltme, lateral movement (yanal hareket), veri toplama ve sızdırma. Living-off-the-land (LotL) teknikleri ile sistemin kendi araçları (PowerShell, WMI, PsExec) kullanılarak tespit zorlaştırılır. Covert communication için steganografi, DNS tunneling, HTTPS kullanılır. Memory-only malware kullanarak disk yazma işlemi yapılmaz. Fileless malware ile antivirüs atlatılır.

Güncel Olay:
•**Volt Typhoon Operasyonu (Mayıs 2024):** Çin bağlantılı APT grubu, ABD'de kritik altyapıları (elektrik şebekeleri, su sistemleri, ulaşım, telekomünikasyon) hedef aldı. Guam'daki askeri üslerin iletişim ağlarına sızdılar. Microsoft ve CISA ortak rapor yayınladı. Grup, yakalanmamak için ağ cihazlarını (router, firewall) kompromize etti ve living-off-the-land teknikleri kullandı.
•**Lazarus Group (2024 devam ediyor):** Kuzey Kore bağlantılı grup, kripto borsalarından 200+ milyon dolar çaldı, nükleer program finansmanı şüphesi var.

7. Sıfırıncı Gün Açıkları (Zero-Day Exploits)

Tanım: Yazılım geliştiricilerinin henüz farkında olmadığı veya yamasını yayınlamadığı güvenlik açıklarıdır. "Sıfırıncı gün" terimi, geliştiricilerin açığı öğrendikten sonra düzeltme için sıfır gün zamanları olduğunu ifade eder. Bu açıklar son derece değerlidir çünkü savunma yoktur. Genellikle devlet destekli gruplar, siber silah şirketleri veya organize suç örgütleri tarafından kullanılır.
Teknik: Zero-day açıkları genellikle fuzzing (otomatik test), reverse engineering, kod analizi veya white-hat araştırmacıların keşifleri sonucu bulunur. Saldırganlar exploit chain (açık zinciri) oluşturarak birden fazla zero-day'i kombine kullanır. Browser zero-day'leri ile drive-by download saldırıları, OS zero-day'leri ile privilege escalation, network device zero-day'leri ile ağ sızması gerçekleştirilir. CVSS skorları genellikle 9.0-10.0 arasındadır. Exploit kitleri hazırlanarak otomatik saldırılar yapılır.

Güncel Olay:

•**Google Chrome Zero-Day (CVE-2024-7971, Ağustos 2024):** Chrome'da yüksek seviye tip karışıklığı (type confusion) zafiyeti aktif olarak istismar edildi. Saldırganlar, özel hazırlanmış web siteleri üzerinden kullanıcıların sistemlerine uzaktan kod çalıştırabildi. Google acil yama yayınladı. 2024 yılında Chrome'da bulunan 8. zero-day açığı.

8. Bulut Güvenliği Riskleri (Cloud Security Risks)

Tanım: Bulut bilişim hizmetlerinin (AWS, Azure, Google Cloud) kullanımından kaynaklanan güvenlik açıkları ve risklerdir. Yanlış yapılandırmalar, yetersiz erişim kontrolleri, veri şifreleme eksikliği, API güvenliği zayıflıkları ve paylaşımlı sorumluluk modelinin yanlış anlaşılması sonucu oluşan tehditleri kapsar. Bulut ortamlarının karmaşıklığı ve dinamik yapısı güvenlik yönetimini zorlaştırır.
Teknik: S3 bucket'ları public olarak yanlış yapılandırılır ve hassas veriler internete açılır. IAM (Identity and Access Management) politikaları aşırı yetkilerle yapılandırılır (privilege escalation riski). API anahtarları GitHub veya public repository'lerde sabit kodlanır. Metadata servisleri (169.254.169.254) istismar edilerek AWS credentials çalınır. Container escape ile Kubernetes cluster'ına sızılır. Shadow IT ile onaylanmamış bulut servisleri kullanılır. Cross-tenant veri sızıntısı riskleri vardır. Snapshot'lar ve backup'lar public erişime açılır.

Güncel Olay:
•**Snowflake Veri İhlali (Mayıs 2024):** Veri ambarı platformu Snowflake kullanan 165 şirket (Ticketmaster, Santander Bank, Advance Auto Parts) veri ihlali yaşadı. 560 milyon Ticketmaster müşterisinin bilgileri çalındı. Saldırganlar, çok faktörlü kimlik doğrulama (MFA) kullanılmayan hesaplara infostealer malware ile elde edilen kimlik bilgileriyle eriştiler. ShinyHunters hacker grubu verileri dark web'de satışa çıkardı.

9. Mobil Cihaz Zararlı Yazılımları (Mobile Malware)

Tanım: Akıllı telefonlar ve tabletleri hedef alan kötü amaçlı yazılımlardır. Android ve iOS işletim sistemlerini etkileyen trojanlar, spyware, adware, bankacılık zararlıları, ransomware ve rooting/jailbreak araçlarını içerir. Mobil cihazlar üzerindeki hassas bilgiler (bankacılık uygulamaları, SMS, konum, kamera, mikrofon erişimi) nedeniyle değerli hedeflerdir.
Teknik: Android'de APK dosyaları resmi Play Store dışından (sideloading) yüklenir. Sahte uygulamalar meşru uygulamaları taklit eder (repackaging). Accessibility Service kötüye kullanılarak tam cihaz kontrolü elde edilir. SMS interception ile 2FA kodları çalınır. Overlay attack ile sahte login ekranları gerçek uygulamaların üzerine bindirilir. Rooting/jailbreak sonrası sistem güvenliği devre dışı kalır. iOS'ta enterprise certificate kötüye kullanılır. Dropper uygulamalar kullanılarak zararlı yük sonradan indirilir. Fleeceware ile abonelik dolandırıcılığı yapılır.

Güncel Olay:

•**XLoader Android Banking Trojan (Şubat 2024):** 300.000'den fazla Android cihazı enfekte eden bankacılık zararlısı tespit edildi. Popüler uygulamaları (Chrome, banking apps) taklit eden sahte APK'lar dağıtıldı. Zararlı, keylogger, ekran kaydı, SMS çalma ve overlay saldırıları gerçekleştiriyor. 7 farklı ülkede 77 banka uygulaması hedeflendi.

10. İçeriden Tehditler (Insider Threats)

Tanım: Organizasyon içinden, yetkili erişime sahip kişiler (çalışanlar, yükleniciler, iş ortakları, eski çalışanlar) tarafından kasıtlı veya kasıtsız olarak gerçekleştirilen güvenlik ihlalleridir. Kötü niyetli insider'lar ticari sır çalabilir, sabotaj yapabilir veya rakip firmaya bilgi satabilir. Dikkatsiz insider'lar ise güvenlik politikalarını ihlal ederek kazara veri sızıntısına neden olabilir.
Teknik: Privileged access abuse ile yetkililer veri tabanlarına, dosya sistemlerine yetkisiz erişim sağlar. Data exfiltration için USB sürücüler, bulut depolama (Dropbox, Google Drive), e-posta veya FTP kullanılır. Screen scraping ve fotoğraflama ile bilgiler kopyalanır. Departing employee senaryosunda, işten ayrılan çalışanlar erişimleri kapatılmadan önce veri çalar. Compromised insider'lar dış saldırganlarla iş birliği yapar. Shadow IT kullanımı ile onaylanmamış uygulamalara veri taşınır. DLP (Data Loss Prevention) sistemleri atlatılır.

Güncel Olay:

- **Tesla Çalışan Veri Sızıntısı (Mayıs 2024):** Eski Tesla çalışanları, 75.000 kişinin kişisel bilgilerini (isim, adres, telefon, e-posta, iş pozisyonları, maaş bilgileri) alman medya kuruluşu Handelsblatt'a sızdırdılar. Whistleblowing iddiasıyla yapılan sızıntı, Tesla'nın veri güvenliği politikalarını sorgulatıp. Şirket çalışanlara karşı dava açtı.
- **Samsung Çalışanı ChatGPT Sızıntısı (2024):** Mühendisler, hassas kaynak kodunu ChatGPT'ye girerek veri sızıntısına neden oldular, Samsung ChatGPT kullanımını yasakladı.

11. Yapay Zeka Kötüye Kullanımı (AI Misuse)

Tanım: Yapay zeka sistemlerinin tasarım amacı dışında, kötü niyetli şekilde kullanılması veya AI modellerinin kendisinin saldırıya uğramasıdır. Bu kategori, AI modellerine karşı yapılan saldırıları (model poisoning, adversarial attacks), AI'nin etik olmayan kullanımını (disinformation, deepfake, autonomous weapons), ve AI sistemlerinin manipüle edilmesini (jailbreaking, prompt injection) içerir.
Teknik: Prompt injection ile LLM'ler istenmeyen çıktılar üretmeye zorlanır. Jailbreaking teknikleriyle AI güvenlik kısıtlamaları atlatılır. Data poisoning ile eğitim verisi manipüle edilerek model davranışı değiştirilir. Model inversion attack ile eğitim verisindeki hassas bilgiler çıkarılır. Model stealing ile proprietary AI modelleri kopyalanır. Adversarial examples ile AI sınıflandırıcıları yanıltılır. AI hallucination istismar edilerek yanlış bilgi üretilir. Bias amplification ile önyargılı kararlar tetiklenir.

Güncel Olay:
•**ChatGPT "Grandma Exploit" ve Jailbreak (2024 devam ediyor):** Saldırganlar, ChatGPT'yi manipüle ederek etik kısıtlamaları aşan içerikler ürettiler. "Ölen büyükannem bana uyku ilacı formülü söylerdi" gibi senaryolarla bomba yapımı, malware kodu, phishing şablonları elde ettiler. OpenAI sürekli yama yayınlasa da yeni jailbreak teknikleri keşfediliyor.

12. Veri İhlalleri ve Gizlilik İhlalleri (Data Breaches and Privacy Violations)

Tanım: Hassas, korunan veya gizli verilerin yetkisiz kişilerce erişilmesi, kopyalanması, iletilmesi, görüntülenmesi, çalınması veya kullanılmasıdır. Kişisel veriler (PII), finansal bilgiler, sağlık kayıtları (PHI), ticari sırlar, fikri mülkiyet gibi değerli bilgilerin sızıntısını içerir. GDPR, KVKK, HIPAA gibi veri koruma düzenlemelerinin ihlali ciddi yasal ve mali sonuçlar doğurur.
Teknik: SQL injection ile veritabanlarına erişilir. Unpatched vulnerabilities kullanılarak sistemlere sızılır. Stolen credentials ile yetkili erişim sağlanır. API exploitation ile veri sızıntısı yapılır. Misconfigured databases (MongoDB, Elasticsearch) internete açık kalır. Third-party breach sonucu zincirleme ihlaller oluşur. Web scraping ile public olmayan veriler toplanır. Backup exposure ile eski veriler sızdırılır. Brute force attack ile şifreler kırılır. Social engineering ile veriler kandırılarak alınır.

Güncel Olay:
•**National Public Data Breach (Ağustos 2024):** ABD'de geçmiş kontrolü yapan şirket National Public Data, 2.9 milyar kişinin Sosyal Güvenlik Numarası (SSN), tam adres, telefon numarası ve diğer kişisel bilgilerini içeren veri ihlali yaşadı. Tarihte bilinen en büyük SSN sızıntısı. Veriler dark web'de ücretsiz dağıtıldı. ABD, Kanada, İngiltere vatandaşları etkilendi. Toplu davalar başlatıldı.

13. Gelişmiş Kimlik Avı Teknikleri (Advanced Phishing Techniques)

Tanım: Geleneksel e-posta tabanlı phishing'in ötesine geçen, çok kanallı ve sofistike kimlik avı yöntemleridir. QR kod phishing (quishing), ses phishing (vishing), SMS phishing (smishing), sosyal medya phishing, MFA yorgunluk saldırıları, man-in-the-middle proxy phishing gibi modern teknikleri içerir. Bu yöntemler, güvenlik farkındalığı eğitimlerini ve geleneksel e-posta filtreleme sistemlerini atlatmak için geliştirilmiştir.
Teknik: QR kod phishing'de PDF veya e-postalardaki QR kodlar mobil cihazlarda taranır, güvenlik kontrollerini atlatır. Vishing'de AI voice cloning kullanılarak tanıdık sesler taklit edilir. MFA fatigue attack'ta kullanıcıya sürekli push notification gönderilerek onaylatılır. Adversary-in-the-middle (AitM) phishing'de reverse proxy kullanılarak gerçek site ile kullanıcı arasına girilir, MFA tokenları real-time çalınır. EvilProxy ve Evilginx gibi phishing-as-a-service araçları kullanılır. Browser-in-the-browser (BitB) saldırılarında sahte popup'lar gösterilerek OAuth akışı taklit edilir.

Güncel Olay:
•**Microsoft 365 QR Kod Phishing Kampanyası (Haziran 2024):** Saldırganlar, PDF eklerindeki QR kodları kullanarak Microsoft 365 kimlik bilgilerini çaldılar. E-posta güvenlik gateway'leri QR kodları tararken mobil cihazlarda açılan sahte login sayfalarını tespit edemedi. Kampanya, finans ve hukuk sektörlerinde 1000+ kuruluşu hedef aldı. %300 başarı oranıyla geleneksel phishing'i geride bıraktı.

14. Ulus-Devlet Siber Saldırıları (Nation-State Cyber Attacks)

Tanım: Devletler veya devlet destekli gruplar tarafından gerçekleştirilen, jeopolitik amaçlı siber casusluk, sabotaj, bilgi operasyonları ve siber savaş faaliyetleridir. Hedefler arasında kritik altyapılar, savunma sanayii, enerji tesisleri, hükümet kurumları, seçim sistemleri ve stratejik endüstriler bulunur. Bu saldırılar genellikle büyük kaynaklara, ileri düzey yeteneklere ve uzun vadeli stratejik hedeflere sahiptir.
Teknik: Çok aşamalı APT kampanyaları yürütülür. Multiple zero-day exploits aynı anda kullanılır. Supply chain'e stratejik sızma yapılır. Critical infrastructure'a yönelik SCADA/ICS sistemleri hedeflenir (Stuxnet benzeri). Disinformation campaigns ile psikolojik operasyonlar yürütülür. Satellite communication'a müdahale edilir. Underwater cable tapping ile iletişim dinlenir. Destructive malware (wiper) kullanılarak veri imha edilir. False flag operations ile başka ülke sorumlu gösterilmeye çalışılır. Cyber espionage ile fikri mülkiyet çalınır.

Güncel Olay:
•**Rusya-Ukrayna Siber Savaşı (2024 devam ediyor):** Rusya, Ukrayna'ya karşı kapsamlı siber operasyonlar yürütüyor. Sandworm (GRU birim), Industroyer2 malware ile elektrik şebekelerini vurdu. WhisperGate wiper malware'i devlet kurumlarını hedef aldı. DDoS saldırıları ile hükümet web siteleri çökertildi. Ukrayna savunması için IT ordusu kuruldu. NATO ülkeleri siber destek sağlıyor. Kasım 2024'te enerji altyapısına yönelik saldırılar yoğunlaştı.

15. Kripto Para İle İlgili Tehditler (Cryptocurrency-Related Threats)

Tanım: Kripto para ekosistemini hedef alan çeşitli siber tehditlerdir. Kripto cüzdan hırsızlığı, exchange hack'leri, DeFi protokol açıklarının istismarı, NFT dolandırıcılığı, rug pull scam'leri, pump-and-dump şemaları, kripto jacking (gizli madencilik), pig butchering scam'leri ve blockchain köprü saldırılarını içerir. Kripto paraların anonim ve geri dönüşü olmayan yapısı, saldırganlar için cazip hedefler oluşturur.
Teknik: Private key theft ile cüzdanlar boşaltılır. Smart contract vulnerabilities (reentrancy, flash loan attack) istismar edilir. Phishing ile seed phrase'ler çalınır. Fake wallet apps mobil mağazalarda dağıtılır. MEV (Miner Extractable Value) ile işlemler manipüle edilir. 51% attack ile blockchain'e müdahale edilir. Bridge exploits ile cross-chain transferler hedeflenir. Ice phishing'de approval transactions imzalatılır. Dusting attack ile cüzdan sahipleri belirlenir. Cryptojacking malware ile botnetler oluşturulur. Social engineering ile fake ICO/IDO'lar pazarlanır.

Güncel Olay:
•**DMM Bitcoin Hack (Mayıs 2024):** Japonya'nın önde gelen kripto borsası DMM Bitcoin, 4.502 Bitcoin (yaklaşık 305 milyon dolar) çalındı. Saldırganlar, hot wallet'tan cold wallet'a transfer sırasında private key'leri ele geçirdiler. Lazarus Group (Kuzey Kore) sorumlu tutuldu. Şirket müşterilere tam tazminat sözü verdi. 2024'ün en büyük kripto hırsızlığı.