SİBER İSTİHBARAT

Siber istihbarat, organizasyonların tehdit araştırmaları ve analiz süreçlerinin ortaya çıkarttığı önemli bir bilgi edinme faaliyetidir. Siber istihbarat söz konusu olduğunda, organizasyonlar ağlarındaki en güncel tehditlere odaklanarak gelebilecek tehditleri önceden tespit ederek önlem alırlar ve siber saldırılara karşı büyük bir avantaj sağlarlar. İnternet üzerinden siyasi partilere, hükümetlere, kurumlara ve askeri tesislere yapılan saldırıların korunması siber güvenlik, bu bilgilere siber saldırılar düzenleyerek erişilmesi siber istihbarat olarak adlandırılır.

Siber İstihbarat, hedef ülkenin siber uzaydaki altyapısını oluşturan aygıtlar, cihazlar, kablolar, internet servis sağlayıcıları, enerji üreticileri, sunucular vb. ile siber saldırıların gerçekleştirilebilmesi ya da saldırı olması durumunda ne gibi önlemlerin alınabileceğinin tespitini amaçlamaktadır.

Siber istihbarat, hedefin bilgisi ve rızası olmaksızın, siber uzaydaki ağlara, bilgisayara ve diğer cihazlara hacking saldırıları yaparak sızmak, hassas ve önemli verilerin toplanarak istihbarat çarkından geçirilmesi faaliyetlerini de kapsamaktadır. Bilgi toplama çalışmaları sadece teknik faaliyetlerle değil, aynı zamanda sosyal mühendislik, psikolojik harp ve diğer unsurlar da kullanılarak oluşturulabilmektedir.

HONEYPOT

Honeypot, bilgi sistemlerine yetkisiz erişen saldırganlar ya da kullanıcılar hakkında bilgi toplamaya yarayan tuzak sunuculardır. günümüz internet dünyasında en sık tercih edilen siber tehdit istihbaratı toplama sistemleri olarak kullanılmaktadır.

SİBER TEHDİT TÜRLERİ

- Malware – Zararlı yazılımlar
- Spyware – Casus yazılımlar
- Malvertising – Reklamlara gömülmüş zararlı yazılımla
- Man in the Middle (MITM) – Ortadaki Adam Saldırıları
- Wiper Attacks – Bulaştığı sistemde her şeyi silen zararlılar
- Distributed Denial of Service (DDoS) – Servis dışı bırakma saldırıları
- Ransomware – Fidye Zararlıları
- Botnets – Zombi Makineler
- Trojans – Truva Atları
- Phishing – Oltalama saldırıları

- Data Breaches – Veri sızıntıları
- Worms – Solucanlar
- Keyloggers – Klavye işlemlerini kaydeden programlar
- Backdoors – Arka kapılar
- Malvertising – Reklam zararlıları
- Advanced Persistent Threats – Hedef Odaklı Siber Saldırılar

OSINT(Açık Kaynak Kodlu İstihbarat)

Açılımı Open Source Intelligence olan OSINT, herhangi bir gizlilik gerektirmeyen, kamuoyuna açık, belirli bir amaç için toplanan bilgilerin, istihbarat niteliği taşıyıp taşımadığına karar veren bir süzgeçten geçirilmesiyle(analiz edilerek) elde edilen sonuçlardır.

OSINT ARAÇLARI

Maltego: Maltego konsol tabanlı olarak değil görsel olarak kullanılmaktadır ve topladığı bilgileri sınıflandırma işlemi yaparak görsel bir şekilde bizlere sunar.

Maltego neler yapabilir;

- Alan adları
- Whois bilgileri
- Ip adresi veya bir ağın tespiti
- E-posta adresi toplama
- Telefon, fax numaraları
- Sosyal paylaşım ağları
- İnsanların kişisel bilgileri
- Sosyal networkler
- Şirketler, web siteleri
- İnternet altyapısını kullarak domainleri,
- IP adreslerini, belgeleri ve dosyaları gibi birçok bilgiye ulaşabilir.

SHODAN: Shodan arama motoru temelde Google'dan çok farklı olmayan, interneti tarayıp internete açık olan sistemleri, cihazları, aygıtları tespit edip bunları bağlantı noktasına (port:"3389″), türüne (os:"Windows XP", coğrafi lokasyonuna (country:"TR" gibi) ve servis bilgisine (Anonymous user logged in) göre sınıflandırmaktadır. Bu bilgiler sayesinde de ülke bazında özel aramalar gerçekleştirilebilmektedir.

GOOGLE HACKİNG DATABASE: Özel arama operatörleri kullanarak hedef hakkında bilgi toplanabilir.

site: Belirttiğiniz adrese ait sayfaları listeler.
intitle: Belirttiğimiz kelimeyi ya da kelimeleri sayfa başlığında arar ve sonuçları listeler.
inurl: Belirttiğiniz kelime web sitelerinin URL' inde aranır. Site operatörüne benzer farkı; site operatörü host'a odaklanır inurl ise URL in herhangi bir yerinde (host,parametre,değer) bulunması yeterlidir.
inanchor: Belittiğiniz veri ile ilişkili olan bağlantıları listeler.
intext: Web sayfalarının içeriğinde arama yaparak aramaları kısıtlayabiliriz.
filetype: Filtrelediğimiz uzantıdaki dosyaları arayacaktır.
info: Belirttiğimiz web adresi ile alakalı web adreslerini listeler.
link: Tanımladığımız link'e ait sayfaları listeler.

The Harvester: Hedef siteye ait mail ve subdomainlerin saptanmasına yardımcı olan bir araçtır.

SOCMINT

SOCMINT Social Media & Intelligence kelimelerinin kısaltmasından türetilmiştir. Türkçede Sosyal medya İstihbaratı olarak tanımlanan SOCMINT istihbarat teşkilatlarının, kuruluşların veya devletlerin sosyal kanallarda yer alan konuşmaların izlenmesine, yanıt vermelerine ve sosyal veri odaklı konuşmaların incelenerek ihtiyaçlara göre ortaya çıkartılan analizler ve çözümler olarak tanımlanmaktadır. OSINT kaynaklarının artması ile birlikte SOCMINT ortaya çıkmıştır. Özellikle de insanların sosyal ağlardaki hareketleri, davranışları ve konuşmalarının incelenmesi, toplumsal olaylardaki verilen tepkilerin ölçülmesi, terör örgütlerinin veya siber saldırganların ortaya çıkarttıkları olaylar bu veri analizlerin önemini ortaya çıkarmıştır.