T.C.
İSTANBUL ÜNİVERSİTESİ-CERRAHPAŞA
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

DİJİTAL AYAK İZİ ÖGELERİNİN SİBER SALDIRILARDA KULLANIM SENARYOLARININ İNCELENMESİ

Alper KENDİRLİ

DANIŞMAN
Dr. Öğr. Üyesi Özgür Can TURNA

Bilgisayar Mühendisliği Anabilim Dalı

Bilgisayar Mühendisliği, Tezli Yüksek Lisans Programı

Mayıs, 2024

TEZ KABUL VE ONAYI

Alper KENDİRLİ tarafından, **Dr. Öğr. Üyesi Özgür Can TURNA** danışmanlığında hazırlanan **"DİJİTAL AYAK İZİ ÖGELERİNİN SİBER SALDIRILARDA KULLANIM SENARYOLARININ İNCELENMESİ"** başlıklı bu çalışma, jürimiz tarafından **01/05/2021** tarihinde yapılan sınav sonucunda **oy birliği** ile başarılı bulunarak **Yüksek Lisans Tezi** olarak kabul edilmiştir.

Tez Jürisi

		İmza	**Sonuç**
DANIŞMAN	Dr. Öğr. Üyesi Özgür Can TURNA İstanbul Üniversitesi - Cerrahpaşa Bilgisayar Mühendisliği Anabilim Dalı		☒ Kabul ☐ Ret
ÜYE	Doç. Dr. Muhammed Ali AYDIN İstanbul Üniversitesi - Cerrahpaşa Bilgisayar Mühendisliği Anabilim Dalı		☒ Kabul ☐ Ret
ÜYE	Dr. Öğr. Üyesi Serpil ÜSTEBAY İstanbul Medeniyet Üniversitesi Bilgisayar Mühendisliği Anabilim Dalı		☒ Kabul ☐ Ret

Annem, babam ve kardeşime ithaf ediyorum…

BÜTÇE DESTEKLERİ

DİJİTAL AYAK İZİ ÖGELERİNİN SİBER SALDIRILARDA KULLANIM SENARYOLARININ İNCELENMESİ

Bu tez çalışması için herhangi bir kurumdan bütçe desteği alınmamıştır.

TEŞEKKÜR

Çalışma boyunca gösterdiği her türlü destek ve yardımlarından dolayı Dr. Öğr. Üyesi Özgür Can TURNA'ya, arkadaşlarıma ve tüm hayatım boyunca yanımda olan aileme bu süreçteki desteklerinden dolayı en içten dileklerimle teşekkür ediyorum.

Mayıs 2024 **Alper KENDİRLİ**

İÇİNDEKİLER

Sayfa No

ŞEKİL LİSTESİ

Sayfa No

TABLO LİSTESİ

Sayfa No

SİMGE VE KISALTMA LİSTESİ

Kısaltmalar **Açıklama**

ABD : Amerika Birleşik Devletleri

CAPTCHA : İnsan ve Bilgisayar Ayrımı Amaçlı Tam Otomatik Genel Turing Testi (Completely Automated Public Turing test to tell Computers and Humans Apart)

CTI : Cyber Threat Intelligence (Siber Tehdit İstihbaratı)

CVSS : Commen Vulnerability Scoring System (Genel Zafiyet Puanlama Sistemi)

DNS : Domain Name System (Alan Adı İsimlendirme Sistemi)

GDPR : General Data Protection Regulation (Genel Veri Koruma Regülasyonu)

ICANN : Internet Corporation for Assigned Names and Numbers (İnternet Tahsisli Sayılar ve İsimler Kurumu)

IoT : Internet of Things (Nesnelerin İnterneti)

IP : Internet Protocol (İnternet Protokolü)

ISP : Internet Service Provider (İnternet Servis Sağlayıcı)

MITRE : Massachusetts Institute of Technology Research and Engineering (Massachusetts Teknoloji araştırma ve mühendislik enstitüsü)

NVD : National Institute of Standarts and Technology **(**Standartlar ve Teknoloji Ulusal Enstitüsü)

OSINT : Open Source Intelligence (Açık Kaynak İstihbaratı)

QR-kod : Quik Response (Hızlı etkileşim kodu)

SMS: : Short messaging Service (Kısa Mesajlaşma Servisi)

SOCMINT : Social Media Intelligence (Sosyal Medya İstihbaratı)

SQL : Structured Query Language (Yapılandırılmış Sorgu Dili)

SSL : Secure Sockets Layer (Güvenli Giriş Katmanı)

TCKN : Türkiye Cumhuriyeti Kimlik Numarası

XSS : Cross-Site Scripting (Siteler Arası Betik Çalıştırma)

ÖZET

[YÜKSEK LİSANS TEZİ]

[DİJİTAL AYAK İZİ ÖGELERİNİN SİBER SALDIRILARDA KULLANIM SENARYOLARININ İNCELENMESİ]

[Alper KENDİRLİ]

İstanbul Üniversitesi-Cerrahpaşa

Lisansüstü Eğitim Enstitüsü

Bilgisayar Mühendisliği Anabilim Dalı

Bilgisayar Mühendisliği, Tezli Yüksek Lisans Programı

[Danışman : Dr. Öğr. Üyesi Özgür Can TURNA]

[Teknolojinin hızlı gelişimi ve internet ağının herkes tarafından kullanılabilir durumda olması dijital ayak izine sahip varlıkların sayısında artışa neden olmuştur. Teknolojide yaşanılan bu gelişim ile birlikte kötücül amaç barındıran tehdit aktörü sayısında da artış meydana gelmiştir. Tehdit aktörleri, belirledikleri hedefe siber saldırı gerçekleştirmeden önce hedef hakkında bilgi toplamaları gerekmektedir. Toplanacak olan bu veriler açık kaynak istihbaratı yöntemleri ile toplanmaktadır. İlgili tez çalışması kapsamında açık kaynak istihbaratı yöntemi ile toplanabilecek verilerin türü ve toplanan verilerin hangi siber saldırılarda kullanılabileceği tespit edilmeye çalışılmıştır.]

Mayıs 2016 , [92] sayfa.

Anahtar kelimeler: [Siber Tehdit İstihbaratı, Dijital Ayak İzi, Atak Yüzeyi, Siber Saldırı]

ABSTRACT

[M.Sc. THESIS]

[ANALYSING DIGITAL FOOTPRINT ELEMENTS IN CYBER-ATTACK SCENARIOS]

[Alper KENDİRLİ]

İstanbul University-Cerrahpaşa

Institute of Graduate Studies

Department of Computer Engineering

Computer Engineering, Thesis Master's Program

[Supervisor : Assoc. Prof. Dr. Özgür Can TURNA]

[The rapid development of technology and the availability of the internet network to everyone have led to an increase in the number of entities with digital footprints. With this development in technology, the number of threat actors has also increased. Threat actors need to gather information about the target before executing a cyber attack on the intended target. The data that's need for the cyber attack is mostly collected with open-source intelligence methods. Within the scope of this thesis study, the type of data that can be collected with open-source intelligence will be determined and will be correlated with the cyber attacks were the collected data can be used.]

May 2024, [92] pages.

Keywords: [Cyber Threat Intelligence, Digital Footprint, Attack Surface, Cyber Attack]

1. GİRİŞ

Uluslararası kamuoyunda kabul edilmiş olan Cyber Kill Chain (Türkçe karşılığı ile siber ölüm zinciri) metodolojisine göre Tehdit aktörleri belirledikleri hedefe yönelik siber saldırı gerçekleştirmeden önce hedefe yönelik keşif çalışması gerçekleştirmesi gerekmektedir [1]. Keşif aşamasında tehdit aktörünün hedef ile henüz herhangi bir iletişim kurmamış olması sebebiyle bu aşama tamamıyla açık kaynak istihbaratı metodolojisi kullanılarak ilerletilmektedir. Tehdit aktörü, keşif aşaması ile birlikte hedefe erişeceği noktayı ve hedefe erişirken kullanacağı verileri tespit etmeye çalışmaktadır.

İnternet ortamında bulunan her türlü varlık arkasında bir iz bırakmaktadır. Bu izlere dijital ayak izi adı verilmektedir. Kişiler (gerçek veya tüzel) veya teknolojik altyapı fark etmeksizin internet ortamında bulunduğu takdirde bir dijital ayak izi oluşmaktadır. Dijital ayak izleri, internet ortamına bağlı varlığı tanımlayan veri parçacıkları olarak tanımlanabilmektedir [2]. Dijital ayak izi ögelerini oluşturan verilerin bir araya gelmesi ile birlikte ise atak yüzeyi oluşmaktadır.

Tehdit aktörleri, açık kaynak istihbaratı yaklaşımları ile hedefe ait atak yüzeyini belirledikten sonra Cyber Kill Chain'de bir sonraki faz olan silahlandırma fazına geçmektedir. Tehdit aktörü bu fazda keşif aşamasında elde ettiği veriler doğrultusunda gerçekleştireceği siber saldırıyı belirleyerek, gerçekleştirdiği siber saldırıya uygun hazırlık yapmaktadır.

Tehdit aktörleri gerçekleştirdikleri bu siber saldırılarda temel motivasyon kaynağı olarak; gelir elde etmek, espiyonaj, zarar verme, manipülasyon, ego tatmini ve itibar kazancı elde etmeyi amaçlamaktadır.

İlgili tez çalışması kapsamında açık kaynak istihbaratı yaklaşımı ile elde edilebilecek dijital ayak izi ögelerinin tespiti ve bunların hangi siber saldırılarda kullanılabileceği incelenecektir.

Sosyal medya platformları üzerinden elde edilebilecek dijital ayak izi ögelerinin tespiti aşamasında literatürde yer alan platformlarda kullanıcılar oluşturulmuş olup, platformun bize sunduğu her veri giriş alanı doldurulmuş ve herkese açık görüntülenebilecek şekilde yapılandırılmıştır. Oluşturulan hesaplar sonrasında üçüncü bir göz olarak, tehdit aktörü bakış

açısı ile farklı bir hesap ile tekrar incelenmiş ve elde edilebilecek dijital ayak izi ögeleri tespit edilmiştir. Elde edilen verilerin tamamı tablolaştırılarak tez çalışması içerisinde sunulmuştur.

Elde edilen dijital ayak izi ögelerinin kullanılabileceği siber saldırıları tespit etmek üzere siber saldırılara yönelik literatür taraması gerçekleştirilmiştir. Gerçekleştirilen literatür taramasında keşif aşamasında dijital ayak izi ögelerine ihtiyaç duyulan siber saldırılar incelenmiştir. Gerçekleştirilen incelemeler sonucunda, ilgili siber saldırıda hangi dijital ayak izi ögesinin kullanılabileceği belirlenmiş ve dijital ayak izi ögesi ile siber saldırı arasında korelasyon tablosu oluşturulmuştur.

Tez çalışmasındaki motivasyon, internet üzerinde bıraktığımız dijital ayak izimizin hangi siber saldırılarda kullanılabileceğinin tespit edilmesidir.

Bununla birlikte elde edilen dijital ayak izi ögelerinin oluşturacağı siber güvenlik stresi ve risk derecelendirmesinin hesaplanması amaçlanmıştır.

Elde edilen tüm bulgular doğrultusunda dijital ayak izi ögelerimizi kullanan siber saldırılardan korunmanın yöntemlerinden tez kapsamında bahsedilmiştir.

2. KAVRAMSAL ÇERÇEVE

Gerçekleştirilen tez çalışması kapsamında siber tehdit istihbarat çalışmalarının bir parçası olan açık kaynak istihbarat metodolojileri ile gerçek ve tüzel kişilerin atak yüzeyi üzerinde tespit edilen dijital ayak izi ögelerini kullanılarak tehdit aktörleri tarafından gerçekleştirilebilecek olası siber saldırı yöntemlerinin belirlenmesi ve bunların önlenmesine yönelik alınabilecek aksiyonların tespit edilmesi amaçlanmaktadır. Tez çalışması boyunca kullanılan terimlerin ve kavramların anlaşılabilir olması amacıyla teorik bilgilere ve konu ile alakalı benzeri örneklere "Kavramsal Çerçeve" başlığı altında yer verilmiştir.

2.1. Sosyal Medya Platformu

Sosyal medya oluşumu itibari ile gerçek ve tüzel kişilerin birbirleriyle iletişimini amaçlayan yüz yüze iletişimin yerine geçen çevrim içi ortamlardır [3]. Sosyal medya, literatür ve tanımı

doğrultusunda; iletişim disiplini, halka ilişkiler disiplini ve bilgi teknolojileri disiplinlerinin ortak çalışması olarak değerlendirilmektedir [4].

Sosyal medya platformları temel olarak iletişimi amaçlamakla birlikte çeşitli sosyal medya platformları spesifik iletişim kaynaklarının paylaşılmasına odaklanmıştır ve sosyal medya platformları böylelikle içerik türü olarak ayrışmaktadır [5].

Günümüzde aktif olan her bir sosyal medya platformu, kullanıcılar tarafından spesifik iletişim materyaline takip etmek ve yayınlamak üzere kullanılmaktadır. Çalışma kapsamında; Facebook, Twitter, Instagram ve LinkedIn olmak üzere en yaygın olan 4 sosyal medya platformu üzerinde yer alan kullanıcıya ait dijital ayak izini oluşturan paylaşımlar ve tehdit aktörü tarafından siber saldırılarda kullanılmak üzere elde edilebilecek veri türleri incelenecek olup, aşağıda yer alan tablo içerisinde sosyal medya platformlara ilişkin; içerik türleri, amaçları ve kullanıcı motivasyonu yer almaktadır [6].

Tablo 1. Sosyal Medya Platformları ve Gerçekleştirilebilen Paylaşım İçeriği Türü.

Sosyal Medya / Özellikler	Facebook	Twitter	Instagram	LinkedIn
İçerik Temeli	Metin ve görsel	Metin	Görsel	Metin ve görsel
Amaç	Tanıdık kişilerle iletişim kurma	İnsanlarla ve topluluklara ulaşma	İnsanlara ve topluluklara görsel içerik sunmak	Kariyer doğrultusunda topluluklarla iletişim kurma
Kullanıcı Motivasyonu	Eğlence	Örgütlenme/ haber alma	Eğlence/ örgütleme	Kariyer/ örgütleme

2.2. Siber Tehdit İstihbaratı

İstihbarat (intelligence) kelime anlamı itibari ile bilgi edinme, haber alma anlamına gelmektedir. İstihbarat çalışmaları, elde edilmiş bilgilerin istihbarat yaklaşımlarını kullanılarak analiz edilmesi sonucunda olası tehditlerden kaçınılmasını ve bertaraf edilmesini amaçlamaktadır.

Siber tehdit istihbaratı (İngilizce karşılığı Cyber Threat Intelligence - CTI) ise istihbarat yaklaşımlarının siber uzay üzerinde gerçekleştirilmesi sonucunda tehdit oluşturabilecek;

kişilerin, yapılanmaların, zararlı yazılımların ve aktivitelerin tespit edilmeye çalışılmaktadır. Gerçekleştirilen tespitler neticesinde tehdit modellemesi çalışmaları gerçekleştirerek tehdit olabilecek unsurun detaylandırılmasını ve çalışma sonucunda elde edilen bulgular doğrultusunda önlem almayı amaçlamaktadır. [7]

Tehditlerin vakaya dönüşmesi durumunda mevcut durumu telafi etmek olası bir vaka gerçekleşmeden önce tehdidin tespit edilerek bertaraf edilmesine kıyasla daha fazla efor ve maliyet getirmektedir.

2.3. Açık Kaynak Tehdit İstihbaratı

İstihbarat çalışmalarında kullanılan çeşitli veri elde etme yöntemleri (yaklaşımları) bulunmaktadır. Herkes tarafından erişilebilen, halka açık şekilde sunulan verilerin geliştirilen metodolojiler doğrultusunda toplanarak analiz edilmesi "Açık Kaynak İstihbaratı" (İngilizce karşılığı olarak Open Source Intelligence - OSINT) olarak adlandırılmaktadır.

OSINT çalışmaları kapsamında gerçek veya tüzel kişilerin; sosyal medya hesapları, yazılı ve görsel haber ajansları, kurum ve kuruluşlara ait bilgi bankaları, blog yazıları, televizyon yayını kayıtları, bulut depolama araçları, kod geliştirme ve benzeri paylaşım ortamları incelenerek hedef olabilecek kişilere karşı kullanılabilecek ögelerin tespit edilmesi amaçlanmaktadır.[8]

2.4. Sosyal Medya İstihbaratı

İstihbarat yaklaşımlarından biri olan sosyal medya istihbaratı (SOCMINT), sosyal medya platformları aracılığı ile elde edilebilecek veriler ve verilerin ilişkilendirilmesi sonucunda elde edilen bilginin işlenmesini ve istihbarat bilgisi olarak kullanmayı amaçlamaktadır [9].

Sanal iletişim ve etkileşimin günümüzde sosyal medya platformları aracılığı ile yapılması sebebiyle çeşitli platformlar popülerlik kazanmıştır. Mevcut durumda; Instagram, Twitter (X), Facebook, LinkedIn, Snapchat ve Youtube başlıca yaygın olarak kullanılan sosyal medya platformları arasında yer almaktadır[10].

2.5. Siber Tehdit Aktörleri

Siber uzayda kötücül faaliyet gerçekleştirmeyi amaçlayan; kişiler, gruplar, otomatize ağlar ve zararlı yazılımlar siber tehdit aktörü veya tehdit aktörü olarak anılmaktadır.

Tehdit aktörleri devlet destekli yapılanmalar olabilecekleri gibi , çeşitli aktivist gruplardan veya bağımsız hacker gruplarından veya bu gruplar tarafından yönetilen zararlı yazılımlar ve otomatize ağlardan da oluşabilmektedir.

Siber tehdit aktörleri siber faaliyetlerini gerçekleştirirken; espiyonaj, maddi kazanç, zarar verme, ego tatmini, sosyo-politik etki yaratma gibi temel motivasyon kaynakları bulunmaktadır[11].

2.6. Dijital Ayak İzi

Dijital ayak izi; gerçek, tüzel veya otomatize varlıkların internet kullanımından sonra arkada bıraktıkları her türlü veri parçasına verilen isimdir. Dijital ayak izi, varlıklara ait kişisel bilgilerden oluşabileceği gibi sistemlere ait teknik bilgilerden de oluşabilmektedir. Tehdit aktörleri ise açık kaynak yöntemler ile elde ettikleri dijital ayak izi ögelerini kullanarak hedeflerine siber saldırılar gerçekleştirebilmektedirler. Dijital ayak izi ögeleri incelenirken ögeler arasında bulunan ilişkileri tespit etmek üzere iki farklı başlık altında incelenmektedir. Bunlar sırasıyla; kişilere (gerçek veya tüzel kişiler) ait dijital ayak izi ögeleri ve teknolojik alt yapı varlıklarına ait dijital ayak izi ögeleridir. Her iki başlık için aşağıda yer alan dijital ayak izi ögeleri örnekleri verilebilmektedir [12].

Kişilere (gerçek veya tüzel) ait dijital ayak izi ögeleri;

- Kişisel veriler.
    - Ad/soyadı bilgisi.
    - Doğum tarihi.
    - Kimlik numaraları.
    - Aile/akraba/arkadaş bilgisi.
    - Eğitim bilgisi.
    - Kariyer bilgisi.
- Sosyal medya hesapları.

    - Sosyal medya paylaşımları.
    - Sosyal medya üzerinde gerçekleştirilen beğeniler ve yorumlar.
- İletişim bilgileri.
    - Telefon numarası.
    - E-posta adresi.
    - Açık adres.
- Dahil olunan dernekler, siyasi partiler, spor kulüpler, sivil toplum örgütleri.
- Resmi kayıtlar.
    - Ticari sicil kayıtları.
    - Açık ihale bilgileri.
    - Herkese açık paylaşılan resmi dokümanlar.

Teknolojik altyapılara ait dijital ayak izi ögeleri;

- Alan adı bilgisi.
    - WhoIS kayıtları.
    - Alan adı.
    - Alt alan adı.
- Ağ altyapı bilgileri.
    - IP bilgisi.
    - Açık port bilgisi.
    - Çalıştırılan servis bilgisi.
    - Ağ bağlantı bilgileri.

- İnternet servis sağlayıcısı (ISP) bilgisi.

- Dokümanlar ve dosyalar
  - Doküman içerikleri.
  - Doküman üst verileri (Metadata).

2.7. Siber Atak Yüzeyi

Siber atak yüzeyi, dijital ayak izlerinin birleşmesi ile oluşan ve tehdit aktörleri tarafından ilk temasın gerçekleştiği noktalar olarak belirtilmektedir. [13]

Tehdit aktörleri siber saldırı gerçekleştirecekleri durumda, hedefe fark ettirmeden gerçekleştirdikleri OSINT çalışmaları ile gerçek kişilerin, tüzel kişilerin ve teknolojik alt yapıların siber atak yüzeyini çıkartmaktadır. Çıkartılan atak yüzeyi doğrultusunda hedefe yönelik saldırılar planlanmaktadır.

Siber atak yüzeyleri, kişiler (gerçek veya tüzel) ve teknolojik alt yapılar için farklılık gösterebilmektedir. Farklılıklar kişiler ve teknolojik alt yapıların sahip oldukları dijital ayak izinin farklılıklarından dolayı kaynaklanmaktadır.[14]

2.7.1. Gerçek Kişilere Ait Atak Yüzeyi

Gerçek kişiler sahip olabilecekleri sosyal medya hesapları ile tehdit aktörlerine daha fazla dijital ayak izi ve dolayısıyla da daha geniş bir atak yüzeyi sunmaktadır. Yalnızca sosyal medya değil, internete açık resmi kaynaklar ve daha önceden yaşanmış olan çeşitli veri sızıntıları ile de atak yüzeyleri genişlemektedir.

Gerçek kişiliklere ait atak yüzeyleri dijital ayak izi ile birlikte aşağıdaki ögeleri de kapsayabilmektedir [15];

- Doğum tarihi.
- Desteklenen spor kulüpleri/siyasi partiler/dernekler ve benzeri oluşumlar.
- Evcil hayvan bilgileri.
- Aile/akraba bilgileri.

- Telefon numarası.
- E-posta adresi.
- Çeşitli kaynaklarca sızdırılmış olan şifreler ve şifre şablonu.
- Alışveriş geçmişi.
- Abone olunan forumlar ve bültenler.
- Kullanılan cihazlara ilişkin veriler.

2.7.2. Teknolojik Altyapılara Ait Atak Yüzeyi

Tehdit aktörleri, teknolojik altyapıların bünyelerinde barındırdığı sistemleri ele geçirme, veri sızdırma, hizmet kesintisine uğratma ve botnet ağına dahil etme gibi kötücül amaçlar güderek teknolojik altyapılara siber saldırılar düzenleyebilmektedir. Tehdit aktörleri hedefe siber saldırı düzenlemeden önce hedefin atak yüzeyini keşfederek dijital ayak izi ögelerini elde etmeye çalışmaktadır. Elde ettiği dijital ayak izi ögeleri doğrultusunda ise siber saldırılarını gerçekleştirebilmektedir. Teknolojik altyapıların atak yüzeyinde bulunan dijital ayak izi ögelerine aşağıda yer alan maddeler örnek verilebilmektedir [12];

- Alan adı bilgisi.
- IP adresi bilgisi.
- Açık port bilgisi.
- WhoIS kayıtları.
- DNS bilgisi.
- Doküman ve dosyalar.
- Üst veri bilgisi.
- Servis bilgisi.

2.8. Sosyal Mühendislik ve Oltalama Saldırısı

Hedefin zafiyetlerini bilerek veya benzer zafiyete sahip kişileri hedef alarak, çeşitli gerçek veya tüzel kişileri; taklit ederek, yanıltıcı içerik üreterek veya toplumsal hareketi tetikleyerek hedefi manipüle etme bilimine sosyal mühendislik denmektedir. [16]

Tehdit aktörleri tarafından geliştirilen, orijinal içeriklere benzeyen, içerisinde zararlı yazılım barındıran veya kullanıcı verilerini saklayan; SMS, e-posta, QR-kodu, bağlantı (link) ve benzeri yollarla yayılım gösteren, yanıltıcı ve sahte içeriklerin kullanılmasına dayanan siber saldırılara oltalama denmektedir. [17]

Günümüzde karşımıza çıkan en yaygın oltalama şekilleri;

- Sahte Microsoft Outlook giriş ekranı.
- Sahte bankacılık sistemleri.
- Devlet kurum ve kuruluşlara ait sahte giriş ekranları.
- SMS aracılığı ile iletilen sahte kurye mesajları.
- E-ticaret sitelerini taklit eden sahte indirim bildirimleri.

2.9. “Cyber Kill Chain” Yaklaşımı

Cyber Kill Chain Framework veya Türkçe karşılığı ile siber ölüm zinciri yaklaşımı, 2011 yılında askeri standartlar gözetilerek Lockeed Martin tarafından geliştirilmiştir. Yaklaşımın geliştirilmesindeki amaç siber saldırıları meydana gelme evrelerine göre sınıflandırmak ve bu doğrultuda önlem almaktır. Bu yaklaşım 7 fazdan oluşmaktadır [18];

1. Keşif (Reconnaissance): Tehdit aktörlerinin hedef hakkında bilgi topladıkları fazdır. Bu fazda başta açık kaynak tehdit istihbaratı olmak üzere çeşitli veri toplama yaklaşımları kullanılmaktadır.
2. Silahlandırma (Weaponization): bu fazda tehdit aktörleri keşif aşamasında elde ettikleri veriler doğrultusunda zararlı yazılımları veya kullanacakları zararlı ortamları hedefe uygun bir şekilde geliştirmektedirler.

3. Gönderim/iletim (Delivery): silahlandırma fazında geliştirilen zararlı yazılımlar ve zararlı ortamlar gönderim fazında hedefe iletilmektedir.

4. Sömürme (Exploitation): gönderilmiş olan zararlı yazılım veya zararlı ortamın hedef sistemlerinde çalıştırılması anlamına gelmektedir. Burada hedef sistemde bulunan güvenlik açıklarından veya zafiyetlerinden yararlanılır.

5. Kurulum (Installation): sömürme fazı sonrasında sisteme ilk erişimin sağlanması durumunda kalıcılık sağlayabilmek üzere çeşitli mekanizmaların kurulmasını kapsamaktadır.

6. Komuta Kontrol (Command and Control): kalıcılık elde edilen hedef sistemlerin yönetiminin tamamen ele geçirilmesidir.

7. Eyleme geçme (Actions on Objectives): tamamen ele geçirilen hedef sistemlerde amaç doğrultusunda; veri çalma, silme, değiştirme ve benzeri işlemlerin gerçekleştirilmesidir.

2.10. Genel Zafiyet Puanlama Sistemi

ABD'de bulunan Ulusal Standartlar ve Teknoloji Enstitüsü (NVD) tarafından geliştirilen kısaltması CVSS (Common Vulnerability Scoring System) olan genel zafiyet puanlama sistemi, zafiyetlerin kritiklik derecesini belirleyen ve 0 ila 10 üzerinden puanlamanın gerçekleştirildiği puanlama yaklaşımıdır [19]. Tablo 2 içerisinde CVSS derecelendirmesine ilişkin tablo bulunmaktadır.

Tablo 2. CVSS Derecelendirme Tablosu

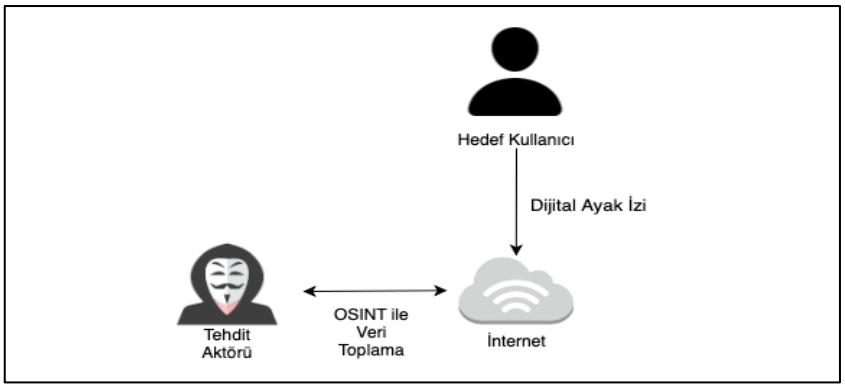
Derecelendirme	CVSS Puanı
Bulunmuyor	0,0
Düşük	0,1 - 3,9
Orta	4,0 - 6,9
Yüksek	7,0 - 8,9
Kritik	9,0 - 10,0

3. YÖNTEM

Teknolojinin hızlı gelişmesi ile birlikte gerçek ve tüzel kişiler tarafından gerçekleştirilen internet kullanımı artmış ve internet ortamında bulunan veriler de aynı doğrultuda artış göstermiştir. İnternetin yaygınlaşmaya başladığı dönemde kullanıcılar tarafından siber güvenlik farkındalığı bulunmaması sebebiyle her türlü veri ve bilgi açık bir şekilde çeşitli platformlar ile paylaşılmış olup, zaman içerisinde dijital ayak izinin büyümesine sebep olmuştur. Günümüzde ise siber güvenlik farkındalığı yine gerçek ve tüzel kişilerin bir kısmında yeterince oluşmamış olup, gerçekleştirilen veri paylaşımı ve yanlış yapılandırmalar sonucunda dijital ayak izleri ve dolayısıyla da atak yüzeyleri oldukça geniş olmaktadır.

Teknoloji ve internet kullanımının artması ile siber suçlular ve siber saldırılar da artmış bulunmaktadır. Siber saldırı gerçekleştirmek isteyen tehdit aktörleri hedefleri hakkında önceden bilgi edinerek saldırılarını bu doğrultuda planlamaktadırlar.

Saldırı planlama aşamasında olan tehdit aktörleri, hedefe mümkün olduğunca farkına vardırmadan açık kaynaklar üzerinden taramalarını gerçekleştirmeye çalışmakta ve veri toplamaktadır. Bu veri toplama aşamasında tehdit aktörleri OSINT tekniklerinden yararlanmaktadır. Şekil 1 içerisinde tehdit aktörünün hedefe ait verileri toplama şekline ilişkin diyagram yer almaktadır.



Şekil 1. Tehdit Aktörlerinin Dijital Ayak İzi Toplamasına İlişkin Diyagram.

Hedefin gerçek veya tüzel kişi olması, tehdit aktörü için OSINT taramasının seyrini etkileyen bir unsurdur. Gerçek kişilerin genellikle sabit IP adresinin bulunmaması ve sürekli çalışan sistemlerinin bulunmamasına karşın oltalama saldırısı esnasında kullanılabilecek veriler daha fazla önem arz edebilmektedir.

Açık kaynaklardan OSINT yöntemleri ile hedefe ait verilerin toplanmasının ardından saldırgan hedefe ait atak yüzeyini oluşturmaya başlamaktadır. Atak yüzeyi üzerinde yer alan

zafiyetler, yanlış yapılandırmalar ve oltama saldırısında kullanılabilecek veriler neticesinde saldırgan ilk temasını planlayabilmektedir.

Tez çalışmasının 3. bölümü olan yöntemler başlığı altında tehdit aktörlerinin dijital ayak izi ögelerini elde etme yöntemleri ve atak yüzeyinin nasıl elde edilebileceği ve tehdit aktörleri tarafından hangi saldırı yöntemleri ile birleştirilebileceği değerlendirilecektir.

3.1. Sosyal Medya Üzerinden Elde Edilebilen Dijital Ayak İzi Ögeleri

Modern çağda insanların sürekli iletişim ve bilgi edinme ihtiyacı beraberinde anlık durum bildirimi yapabildikleri, mesajlaşabildikleri ve çeşitli yöntemlerde iletişimi tamamlayabildikleri sosyal medya uygulamalarını da beraberinde getirmiştir. Temel iletişim ihtiyacını karşılayan ve gündelik olarak aktif kullanılan bu uygulamalar beraberinde çeşitli siber güvenlik risklerini de getirebilmektedir. Tehdit aktörleri, sosyal medya platformlarından elde ettikleri bilgiler doğrultusunda hem fiziksel zarar hem de sanal ortamda zarar verebilmektedir. [20]

Tez çalışması kapsamında tehdit aktörlerinin sosyal medya üzerinden elde edebilecekleri verilere ve bu elde edilen verilerin hangi senaryolar kapsamında değerlendirilebileceği incelenecektir.

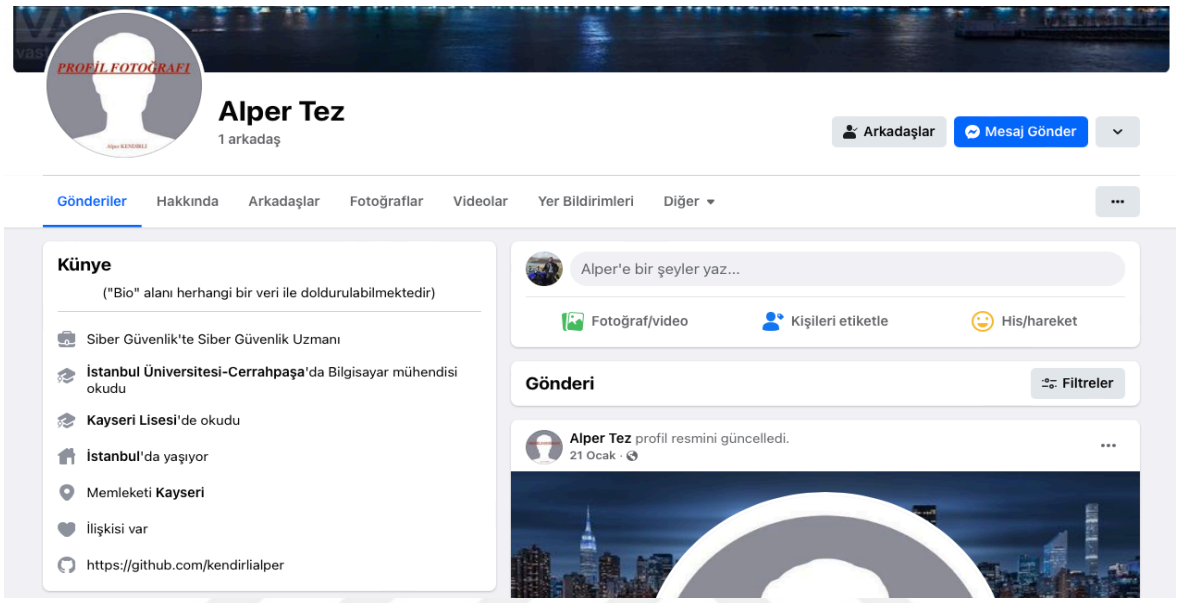
3.1.1. Facebook Üzerinde Elde Edilebilen Dijital Ayak İzi Ögeleri

2004 yılında kurulan ve günümüzde dahi aylık 2,9 milyar aktif kullanıcı sayısına sahip olan Facebook isimli sosyal medya sayfası 2004 yılında kurulmuş ve rekabet içerisinde bulunduğu çeşitli sosyal medya platformları olmasına rağmen hala aktif bir şekilde kullanılmaktadır. Kullanıcılar Facebook üzerinde hesap oluşturup diğer kullanıcılar ile platform içerisinde bulunan çeşitli iletişim araçları ile iletişim sağlayabilmektedir.[21]

Gerçek ve tüzel kişilerin hesap oluşturabildiği bu sosyal medya platformunda, kullanıcılar kişisel bilgilerini kendilerine ait profillerine ekleyerek platform üzerinde bulunan diğer kullanıcılar ile daha hızlı etkileşim sağlayabilmekte ve diğer kullanıcıların profil sahibi hakkında daha fazla bilgi edinmesine olanak sağlamaktadır.

Tez çalışması kapsamında Facebook sosyal medya platformu üzerinden tez özelinde “Alper Tez” kullanıcı adına sahip bir kullanıcı oluşturulmuş olup, kullanıcının profil içerisinde gerçekleştirebileceği paylaşımlar haricinde kullanıcı profiline ait “Hakkında” sekmesinden elde edilebilecek verilerin tespiti amaçlanmıştır.

İlgili tespit çalışmasında profil içerisinde “hakkında” başlığı altında yer alan tüm bilgi alanları doldurulmuş olup, tamamı “herkese açık” seçeneği seçilerek herkesin görüntüleyebileceği şekilde yapılandırılmıştır. Oluşturulan Facebook hesabına ilişkin ekran görüntüsü şekil 2 içerisinde yer almaktadır.

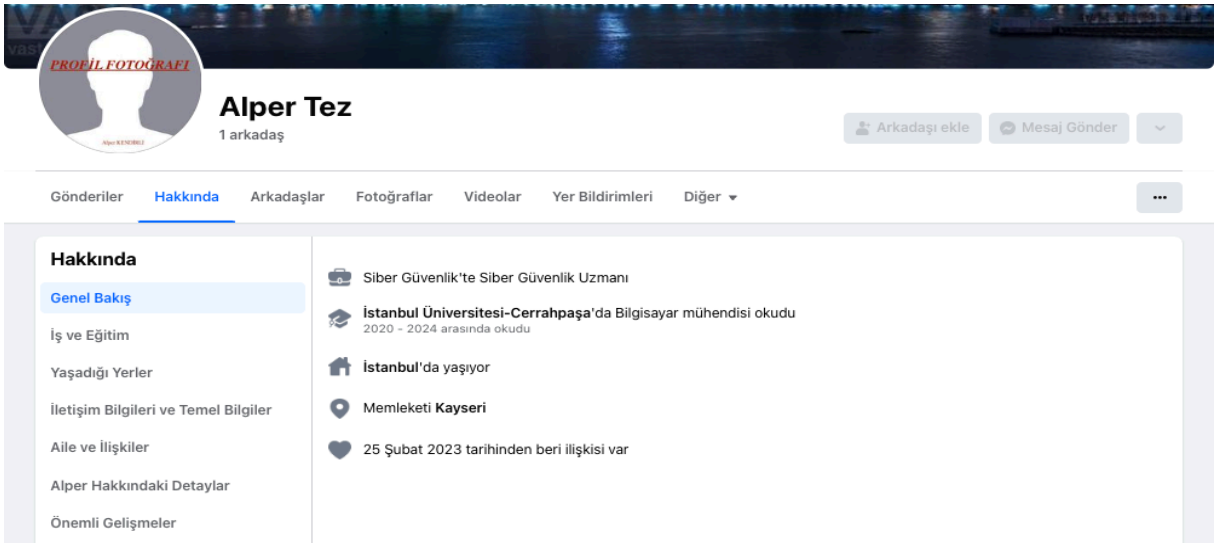


Şekil 2. Tez Çalışması Kapsamında Oluşturulan Facebook Hesabına İlişkin Ekran Görüntüsü.

Tez çalışması kapsamında oluşturulan “Alper Tez” hesabı, farklı bir hesap ile dışarıdan bir kişi olarak incelenmeye başlandığında; Gönderiler, Hakkında, Arkadaşlar, Fotoğraflar, Videolar, Yer Bildirimleri ve Diğer olmak üzere 7 sekmenin yer aldığı gözlemlenmiştir. İlgili sekmeler “sonsuz sayfa” şeklinde sayfa aşağı kaydırıldıkça peşi sıra gösterildiği gözlemlenmiştir.

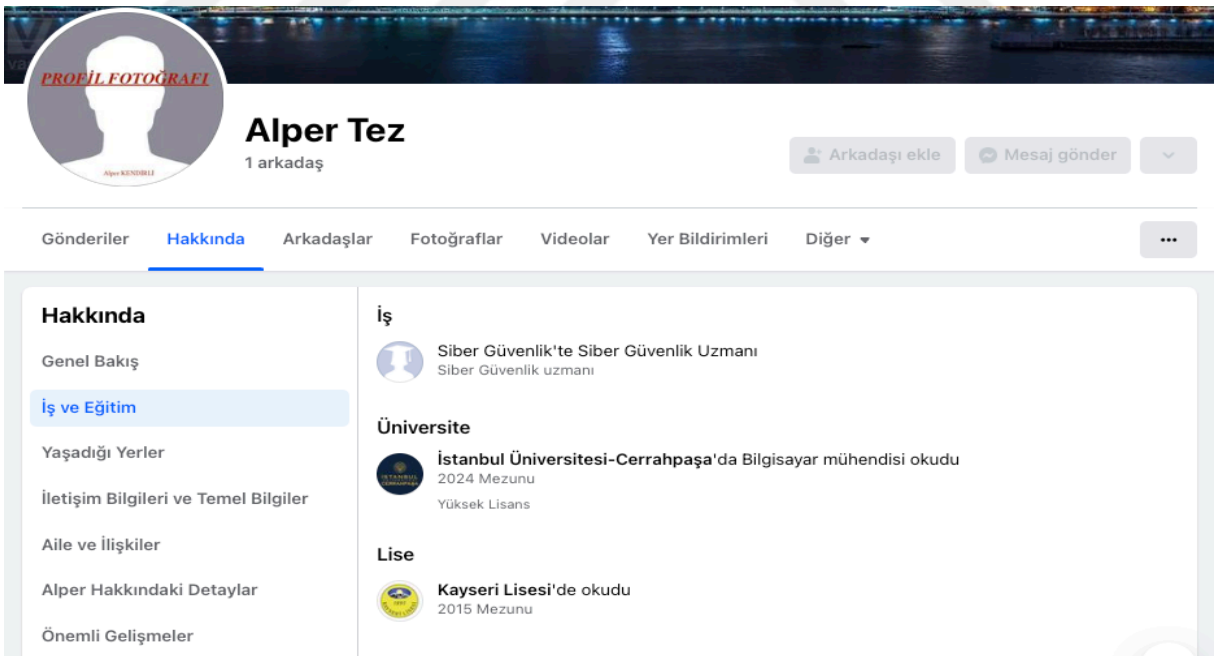
Facebook sosyal medya platformu tarafından sunulan kişisel bilgi alanlarını incelemek üzere “Hakkında” sekmesi içerisinde inceleme gerçekleştirilmiştir, “Hakkında” sekmesi altında; Genel Bakış, İş ve Eğitim, Yaşadığı Yerler, İletişim Bilgileri ve Temel Bilgiler, Aile ve İlişkiler, Alper Hakkındaki Detaylar, Önemli Gelişmeler olmak üzere 7 adet alt başlığın bulunduğu gözlemlenmiştir.

“Genel Bakış” alt başlığı altında yer alan veriler incelendiğinde sosyal medya hesabı sahibine ait; Kariyer bilgisi, eğitim bilgisi, ikamet bilgisi, memleket bilgisi ve ilişki bilgisinin yer aldığı gözlemlenmiştir. “Genel Bakış” sekmesine ilişkin ekran görüntüsü şekil 3 içerisinde yer almaktadır.



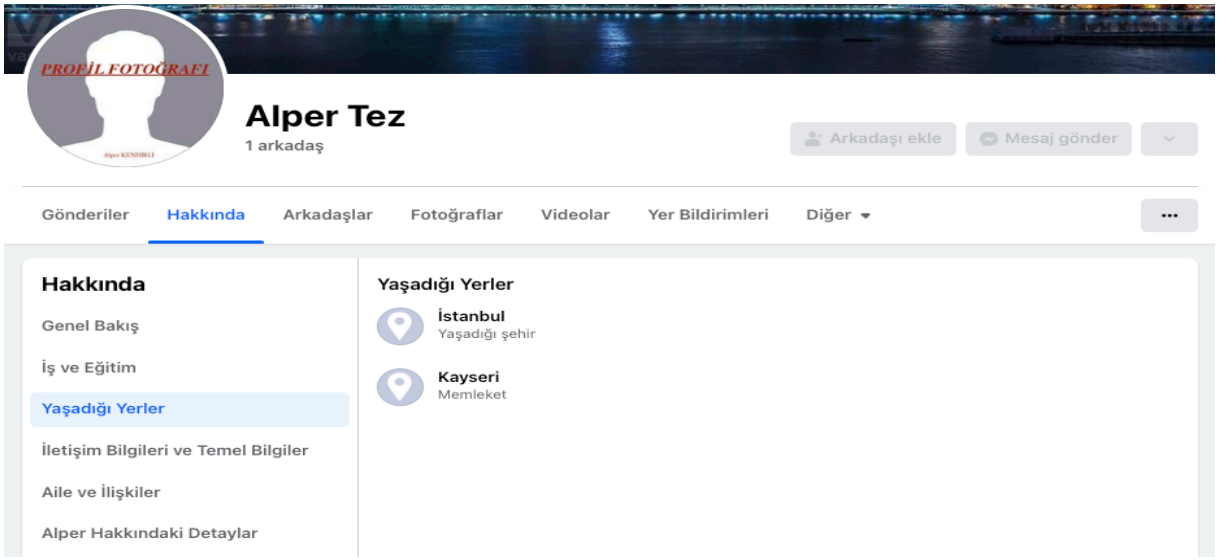
Şekil 3. Genel Bakış Sekmesine İlişkin Ekran Görüntüsü.

"İş ve Eğitim" alt başlığı altında yer alan veriler incelendiğinde sosyal medya hesabı sahibine ait; kariyer geçmişi ve eğitim geçmişi bilgilerinin daha ayrıntılı şekilde yer aldığı gözlemlenmiştir. "İş ve Eğitim" sekmesine ilişkin ekran görüntüsü şekil 4 içerisinde yer almaktadır.



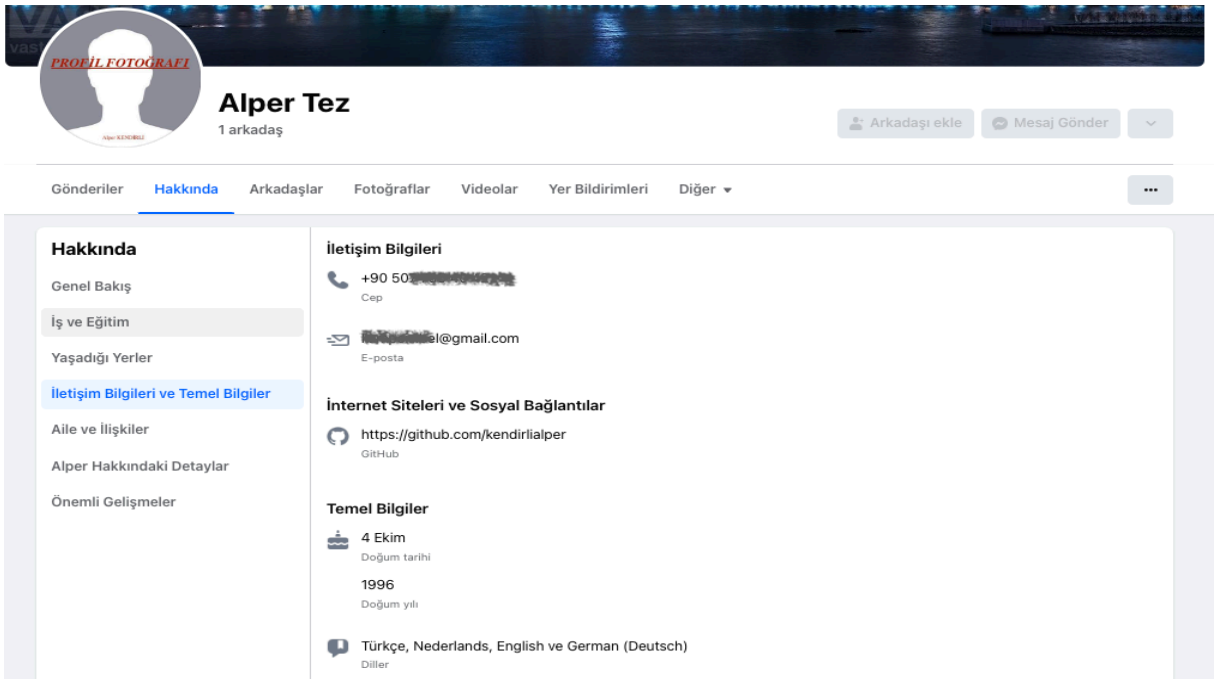
Şekil 4. İş ve Eğitim Sekmesine ilişkin Ekran Görüntüsü.

"Yaşadığı Yerler" alt başlığı altında yer alan veriler incelendiğinde sosyal medya hesabı sahibine ait ikamet bilgisi ve memleket bilgisinin yer aldığı gözlemlenmiştir. "Yaşadığı Yerler" sekmesine ilişkin ekran görüntüsü şekil 5 içerisinde yer almaktadır.



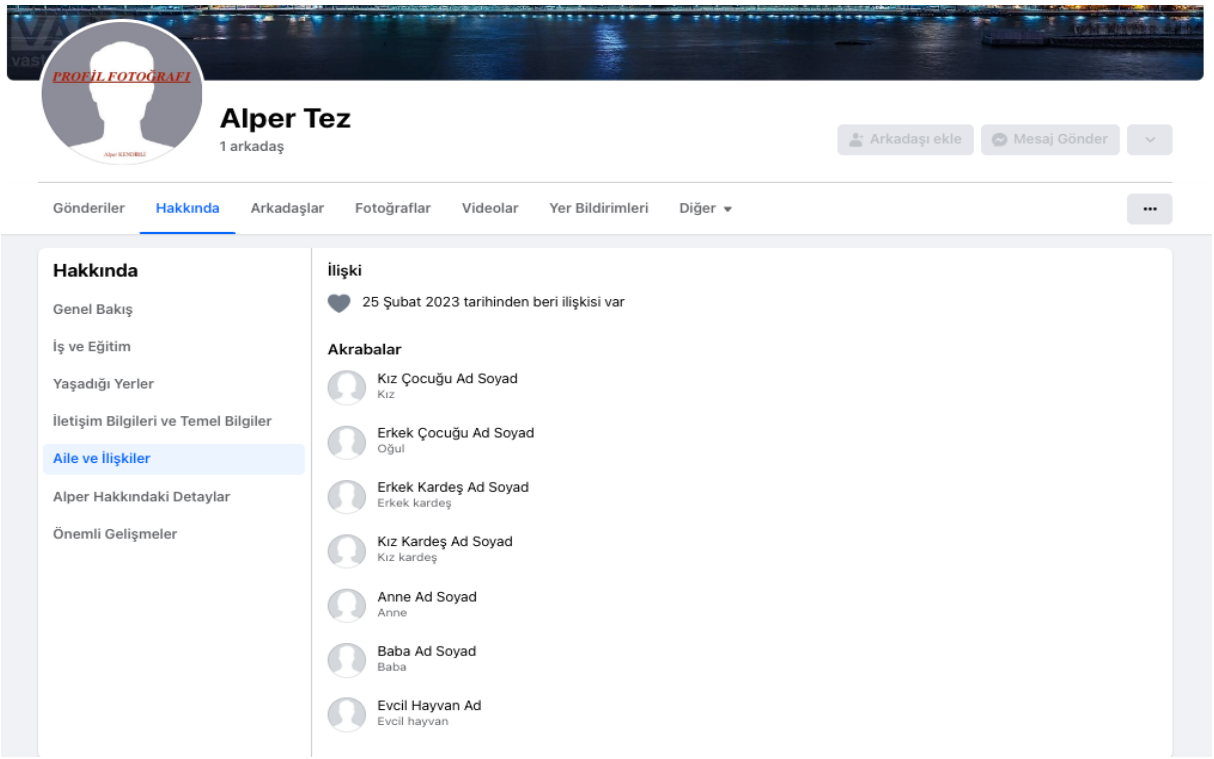
Şekil 5. Yaşadığı Yerler Sekmesine İlişkin Ekran Görüntüsü.

"İletişim Bilgileri ve Temel Bilgiler" alt başlığı altında yer alan veriler incelendiğinde sosyal medya hesabı sahibine ait telefon numarası bilgisi, e-posta adresi, web sitesi ve diğer sosyal bağlantı linkleri, doğum tarihi bilgisi, doğum yılı bilgisi ve kullanıcının bildiği dillere ilişkin verilerin bulunduğu gözlemlenmiştir. "İletişim Bilgileri ve Temel Bilgiler" sekmesine ilişkin ekran görüntüsü şekil 6 içerisinde yer almaktadır.



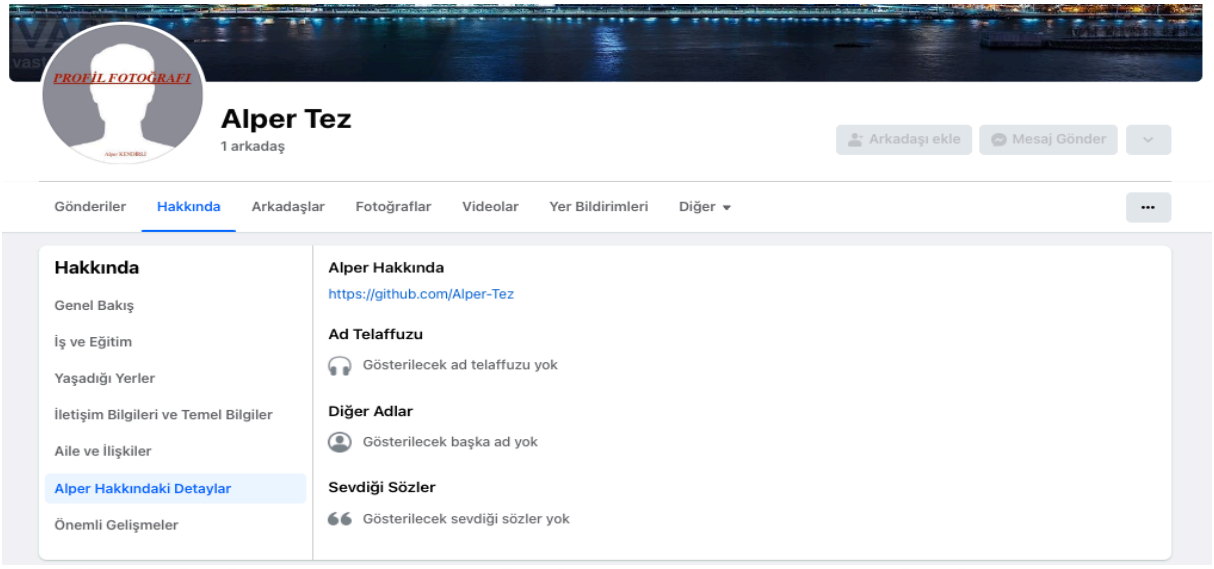
Şekil 6. İletişim Bilgileri ve Temel Bilgiler Sekmesine İlişkin Ekran Görüntüsü.

“Aile ve İlişkiler” alt başlığı altında yer alan veriler incelendiğinde sosyal medya hesabı sahibine ait medeni durum/ilişki bilgisi ve bu bilgiye ait başlangıç tarihi, diğer aile akraba ve evcil hayvana ait isim bilgisi yer almaktadır. Aile akraba ve evcil hayvan bilgisi kısmında ilgili kişinin Facebook hesabı da bağlanabildiği gözlemlenmiştir. “Aile ve İlişkiler” sekmesine ilişkin ekran görüntüsü şekil 7 içerisinde yer almaktadır.



Şekil 7. Aile ve İlişkiler Sekmesine İlişkin Ekran Görüntüsü.

“Alper Hakkındaki Detaylar” alt başlığı altında yer alan veriler incelendiğinde sosyal medya hesabı sahibine ait ismin telaffuzu, diğer ad bilgisi ve sevdiği sözlere ilişkin bilgi alanların bulunduğu gözlemlenmiştir. “Alper Hakkındaki Detaylar” sekmesine ilişkin ekran görüntüsü şekil 8 içerisinde yer almaktadır.

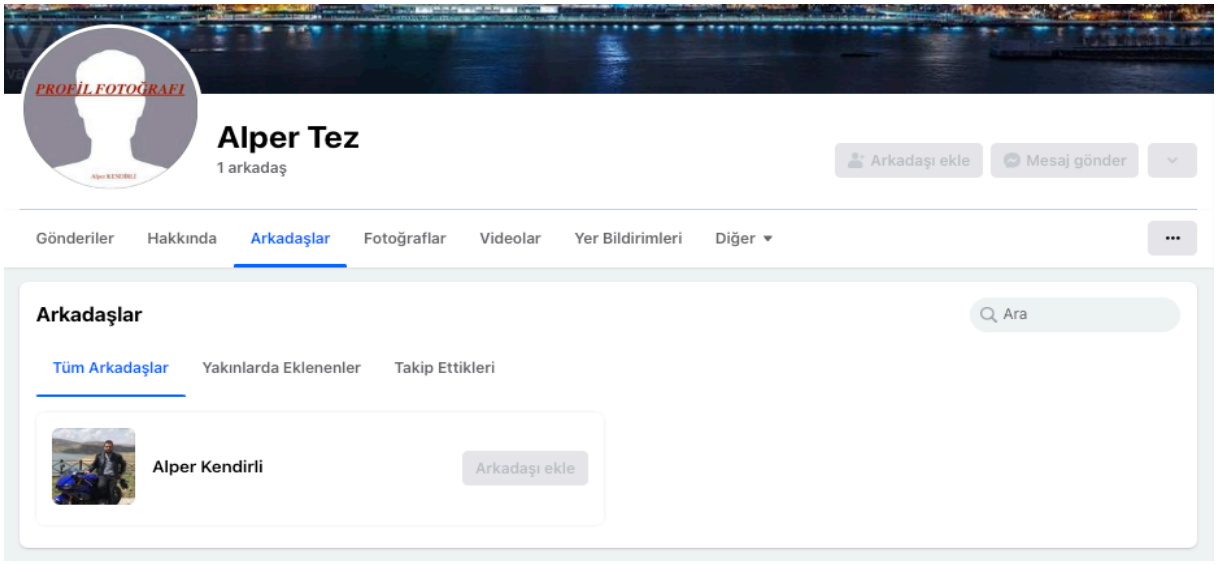


Şekil 8. Kullanıcı Hakkında Detaylar Sekmesine İlişkin Ekran Görüntüsü.

"Önemli Gelişmeler" alt başlığı altında yer alan veriler incelendiğinde sosyal medya hesabı sahibine ait diğer başlıklar altında girilen verilerin kronolojik olarak sıralandığı gözlemlenmiştir. "Önemli Gelişmeler" sekmesine ilişkin ekran görüntüsü şekil 9 içerisinde yer almaktadır.

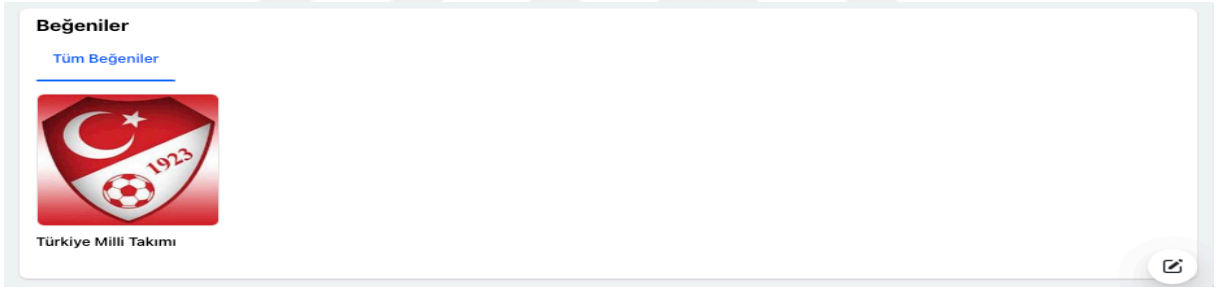
Şekil 9. Önemli Gelişmeler Sekmesine İlişkin Ekran Görüntüsü.

"Arkadaşlar" sekmesi incelediğinde profil sahibinin sosyal medya platformu aracılığı ile eklemiş olduğu ve takip ettiği kişilerin bilgisi yer aldığı gözlemlenmiştir. "Arkadaşlar" sekmesine ilişkin ekran görüntüsü şekil 10 içerisinde yer almaktadır.



Şekil 10. Arkadaşlar Sekmesine İlişkin Ekran Görüntüsü.

"Diğer" sekmesi altında profil sahibinin beğendiği sayfalara yönelik bilgi yer almaktadır. "Diğer" sekmesine ilişkin ekran görüntüsü şekil 11 içerisinde yer almaktadır.



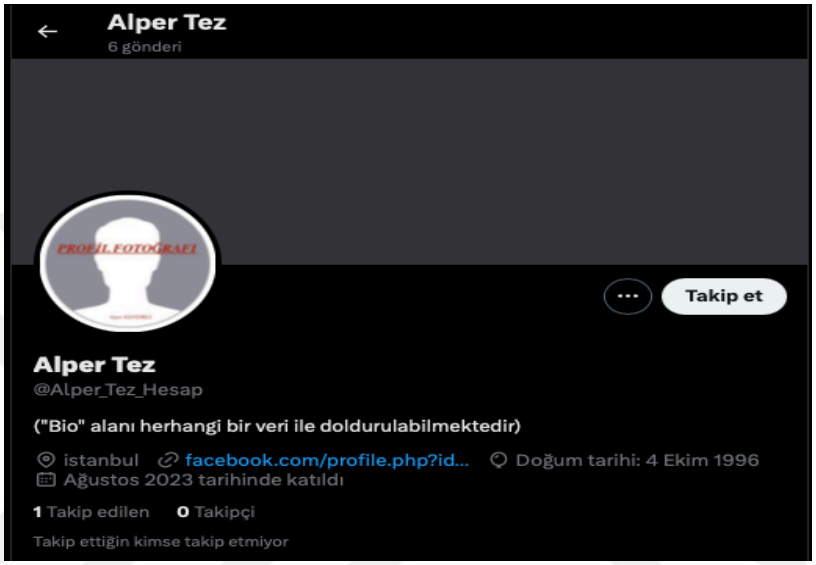
Şekil 11. Diğer Sekmesi Altında Yer Alan Beğeniler Sekmesine İlişkin Ekran Görüntüsü.

3.1.2. Twitter (X) Üzerinden Elde Edilebilen Dijital Ayak İzi Ögeleri

Twitter veya yani adı ile X, küresel çapta popüler olan ve yaygın olarak kullanılan sosyal medya platformudur. Çıkış itibariyle yalnızca yazılı iletişime olanak sağlayan bu platform zaman içerisinde görsel ve işitsel medyaya da yer vermeye başlamıştır [22].

Tez çalışması kapsamında Twitter sosyal medya platformu üzerinden elde edilebilecek dijital ayak izi ögelerini tespit etmek üzere "Alper Tez" isimli kullanıcı oluşturulmuş olup, profil herkese açık şekilde yapılandırılmıştır. Sosyal medya platformunun kullanıcı profilinde doldurmaya izin verdiği her bilgi alanı doldurulmuş olup, harici bir hesaptan oluşturulan hesap

gözlemlenmiştir. Oluşturulan hesaba yönelik ekran görüntüsü şekil 12 içerisinde yer almakta olup, profil incelendiğinde dijital ayak izi olarak; isim bilgisi, kullanıcı adı bilgisi, Konum bilgisi, doğum tarihi bilgisi, harici site bilgisi ve serbest biyografi alanının olduğu gözlemlenmiştir. Sosyal medya platformunun sunduğu veri alanları haricinde kullanıcı gerçekleştirdiği paylaşımlar ile de atak yüzeyini genişletebilmekte olup, herhangi bir sınırı bulunmadığı için tez çalışması kapsamında değerlendirmeye alınmamıştır.

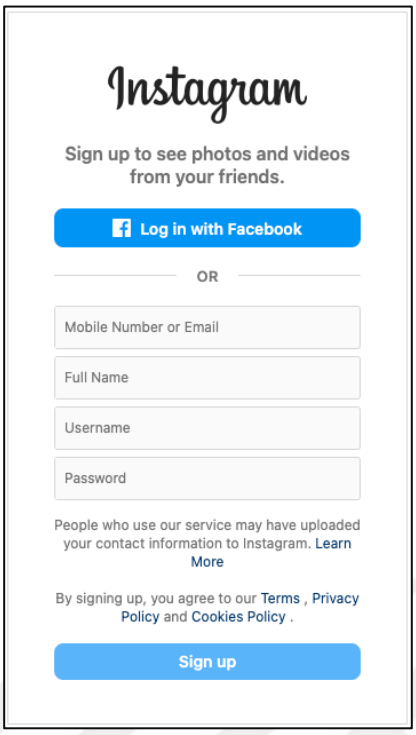


Şekil 12. Oluşturulan Twitter (X) Hesabına İlişkin Ekran Görüntüsü.

3.1.3. Instagram Üzerinden Elde Edilebilen Dijital Ayak İzi Ögeleri

Çeşitli sosyal medya platformlarının geliştirilmesi ve her bir sosyal medya platformunun belirli içerik türlerine odaklanmasından dolayı yalnızca görsel medyanın paylaşılabileceği bir sosyal medya platformu ihtiyacı doğmuştur. 2010 yılında bu ihtiyaca yönelik olarak "Instagram" platformu halka açık ücretsiz bir şekilde sunuldu. [23].

Instagram sosyal medya platformu üzerinde paylaşımları ve hesapları görüntüleyebilmek için kullanıcı oluşturmak gerekmektedir. Kullanıcı oluşturma aşamasında Facebook hesabınız ile kullanıcı oluşturulabileceği gibi mail adresiniz ile de kullanıcı oluşturulabilmektedir. Şekil 13 içerisinde kayıt ekranına ilişkin ekran görüntüsü yer almaktadır. Profesyonel veya işletme hesabı oluşturmak isteyen kullanıcıların aynı ekran aracılığı ile kayıt oluşturmaları ardından ayarlar sekmesi altından hesaplarının kullanım şekillerini değiştirmeleri gerekmektedir.

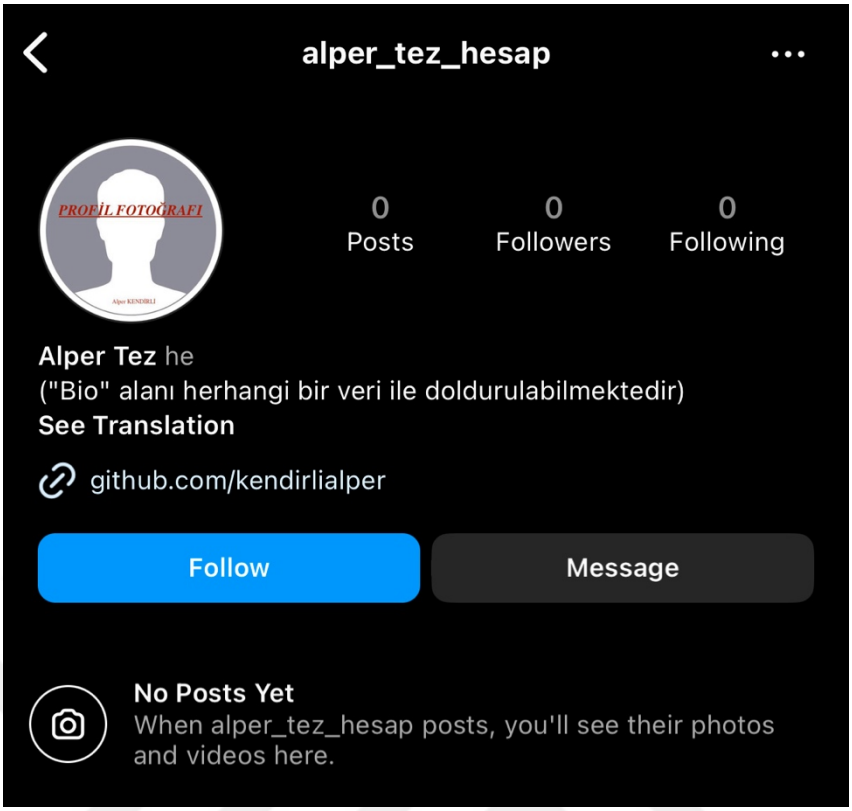


Şekil 13. Instagram Kayıt Olma Ekranına İlişkin Ekran Görüntüsü.

Tez çalışması kapsamında hem kişisel hesapların hem de tüzel kişilere ait hesapların oluşturduğu dijital ayak izini tespit etmek üzere "alper_tez_hesap" kullanıcı adına sahip hesap oluşturulmuştur.

İlgili sosyal medya platformu üzerinde gerçekleştirilecek inceleme iki aşamalı olup, ilk önce kişisel hesap oluşturulmuş ardından oluşturulan kişisel hesap işletme hesabına çevrilmiştir. Her iki hesap türünde sosyal medya platformunun bize sunduğu kişisel bilgi alanlarının tamamı doldurulmuş ve herkesin görüntüleyebileceği şekilde yapılandırılmıştır. Profil hakkında kısmında paylaşılan verinin oluşan dijital ayak izi üzerindeki yerini tespit etmek için harici bir hesaptan profil ziyaret edilmiş ve gözlemlenebilen veriler not alınmıştır. Bu aşamada tehdit aktörü bakış açısı ile elde edilebilecek verilerin tespiti amaçlanmıştır.

Oluşturulan ve kişisel verileri doldurulan hesap harici bir profilden incelendiğinde şekil 14'de yer alan ekran görüntüsündeki gibi gözükmektedir.

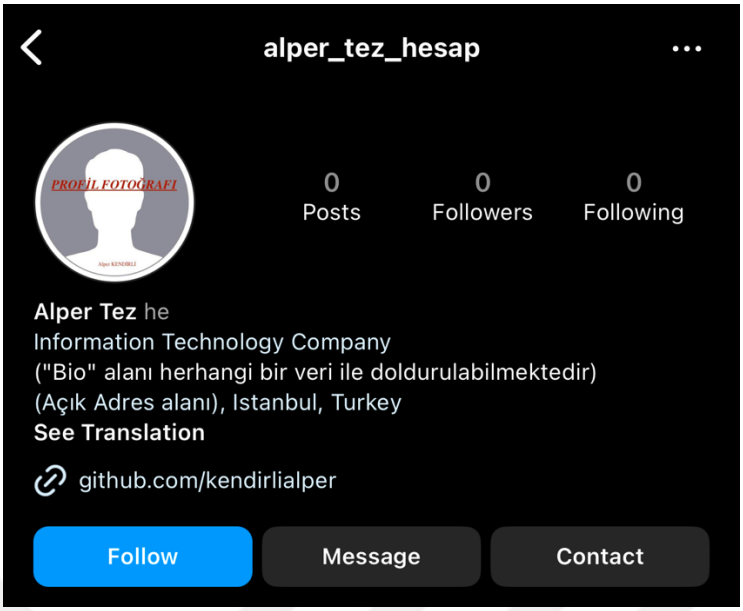


Şekil 14. Oluşturulan Kişisel Instagram Hesabına İlişkin Ekran Görüntüsü.

Her kişisel bilgi alanı doldurulmuş olan hesaptan; kullanıcı adı bilgisi, isim bilgisi, soyadı bilgisi, web sitesi bilgisi ve zamir (hitap) bilgisinin yer aldığı gözlemlenmiştir. Ayrıca kullanıcının kendi hakkında dilediği bilgiyi girebileceği biyografi alanı bulunmaktadır. Biyografi alanı kişiden kişiye değiştirilebilir olacağı ve paylaşılan veri konusunda sınırlama bulundurmadığı için içerik açısından tez kapsamında değerlendirilmemiştir.

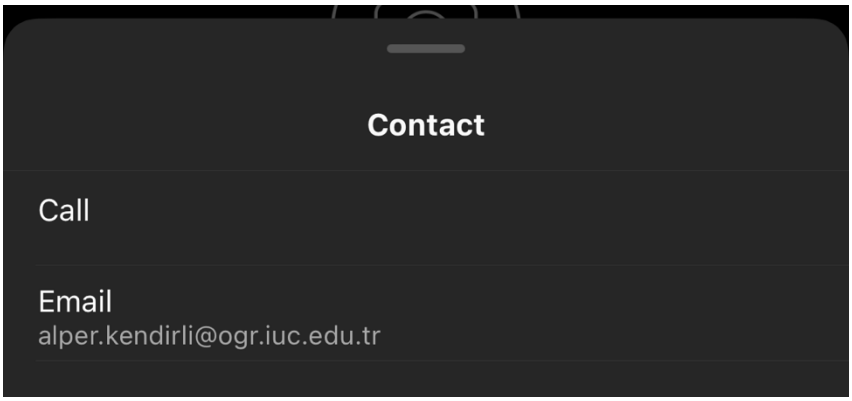
Instagram sosyal medya platformunun ikinci inceleme aşamasında ise mevcut hesap işletme hesabına çevrilmiş olup, yeni eklenen bilgi alanlarının tamamı doldurulmuştur. Doldurulan bilgilerin tamamı herkes tarafından görüntülenebilecek şekilde yapılandırılmıştır.

İşletme hesabına çevrilen ve verileri doldurulan hesap harici bir profilden incelenerek tehdit aktörü bakış açısı ile elde edilebilecek verilen tespiti amaçlanmaktadır. Şekil 15 içerisinde işletme hesabına ait ekran görüntüsü yer almaktadır.



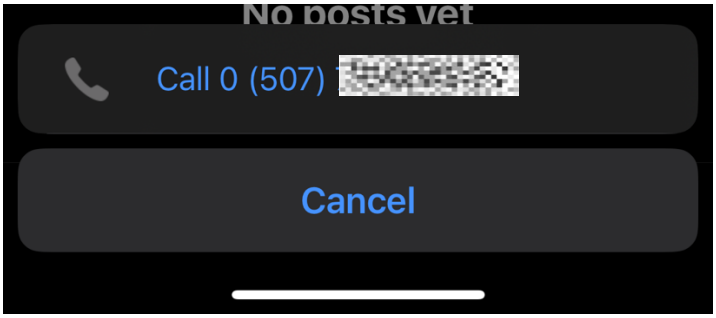
Şekil 15. Oluşturulan Instagram İşletme Hesabına İlişkin Ekran Görüntüsü.

Oluşturulan işletme hesabı incelendiğinde; kullanıcı adı bilgisi, isim bilgisi, soyadı bilgisi, web sitesi bilgisi, zamir (hitap) bilgisi, işletmenin bulunduğu sektör bilgisi, açık adres bilgisi alanların eklendiği gözlemlenmiştir. Buna ek olarak kişisel hesapta bulunmayan "Contact" veya Türkçe karşılığı ile "iletişim" butonunun belirdiği gözlemlenmiştir. Şekil 16'da yer alan ekran görüntüsü yer almakta olup, işletme hesabına ait elektronik posta adresinin açık bir şekilde sunulduğu gözlemlenmiştir.



Şekil 16. İletişim Bilgileri Ekranına İlişkin Ekran Görüntüsü.

"Call" veya Türkçe karşılığı ile arama butonuna tıkladığımızda telefonun işletim sistemi üzerinde açılır pencere şeklinde işletme hesabına ait telefon numarasının sunulduğu gözlemlenmiştir. İlgili dijital ayak izine yönelik ekran görüntüsü şekil 17 içerisinde yer almaktadır.

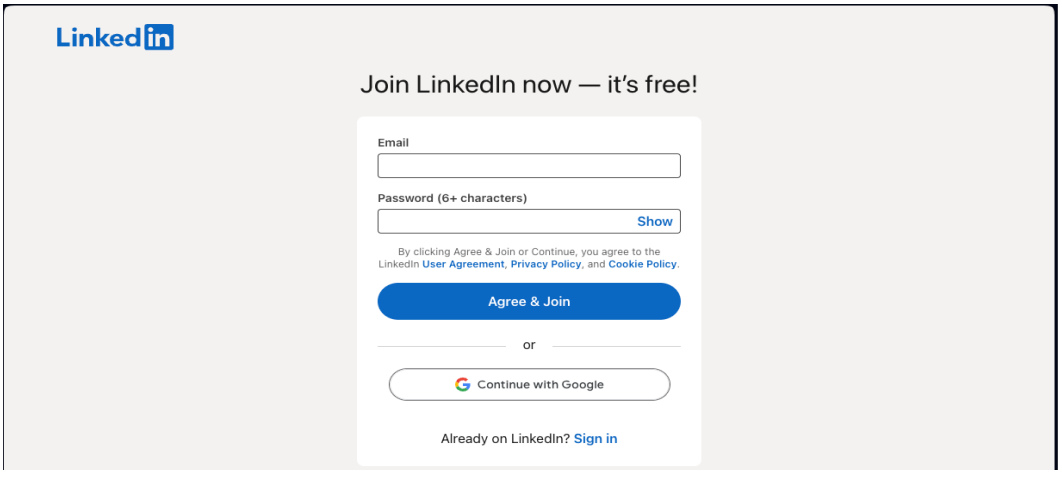


Şekil 17. Telefon Numarasına İlişkin Ekran Görüntüsü.

3.1.4. Linkedin Üzerinden Elde Edilebilen Dijital Ayak İzi Ögeleri

LinkedIn dünya çapında aktif bir şekilde kullanılan profesyonel kariyer odaklı en yaygın sosyal medya platformudur [24]. Kurum ve kuruluşlar açısından personel bulma, personel adayları tarafından ise iş bulmakta aracılık eden platform LinkedIn, özellikle kullanıcılar arasında mesajla iletişime olanak sağladığı, kullanıcıların çeşitli iletişim materyallerini paylaşmasına izin verdiği, paylaşımın türü içeriğinde ve içeriğinde sınırlama uygulamadığı, paylaşımlarda beğeni ve yorum özelliği bulunmasından dolayı sosyal medya platformu olarak değerlendirilmektedir [25].

Sosyal medya platformu LinkedIn'de kullanıcılara veya işverenlere ait profilleri ve iş ilanlarını görüntülemek üzere hesap oluşturma ihtiyacı bulunmamaktadır. Kullanıcılar ile etkileşim içine girmek ve iş ilanlarına başvurmak için kullanıcı oluşturmak gerekmektedir. Kullanıcı oluşturmak için iki seçenek bulunmaktadır. Bunlardan birincisi "Google" ile kullanıcı oluşturma diğeri ise e-posta adresi ile kullanıcı oluşturma. İlgili kullanıcı oluşturma ekranına ilişkin ekran görüntüsü şekil 18 içerisinde yer almaktadır.



Şekil 18. LinkedIn Kayıt Olma Ekranına İlişkin Ekran Görüntüsü.

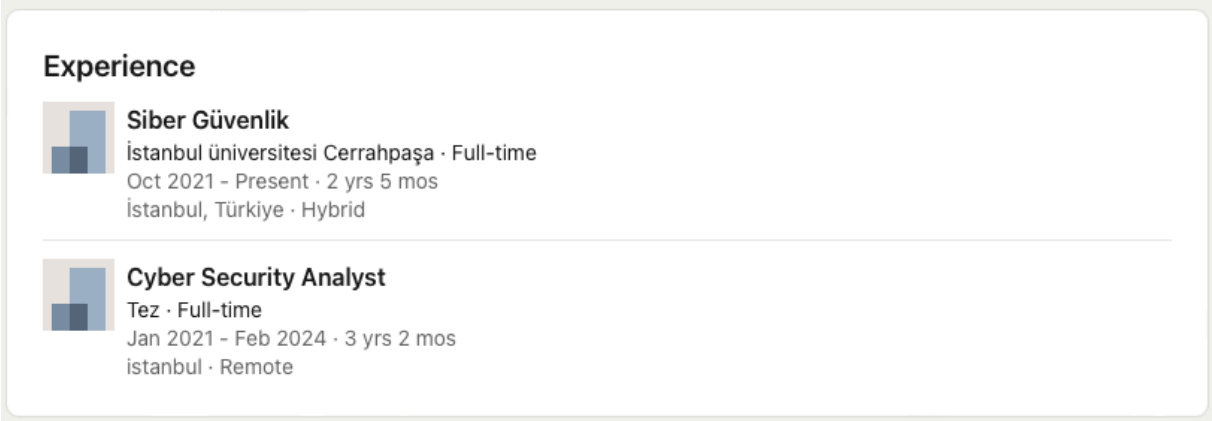
Tez çalışması kapsamında, LinkedIn sosyal medya platformundan elde edilebilecek dijital ayak izi ögelerini tespit etmek üzere “Alper Tez” isminde bireysel hesap ve “Alper - Tez - Tüzel Hesap” isminde iş veren hesabı olmak üzere iki farklı kullanıcı oluşturulmuştur. Hesapların oluşturulma aşamasında sosyal medya platformunun sunduğu her kişisel bilgi alanı doldurulmuştur. Oluşturulan bireysel hesaba yönelik ekran görüntüsü şekil 19 içerisinde yer almaktadır.

Şekil 19. Oluşturulan Kişisel LinkedIn Hesabına İlişkin Ekran Görüntüsü.

Kişisel bilgi alanları doldurulduktan sonra oluşturulan “Alper Tez” isimli hesap farklı bir tarayıcı ve farklı bir hesap ile görüntülenip, incelenmeye başlanmıştır.

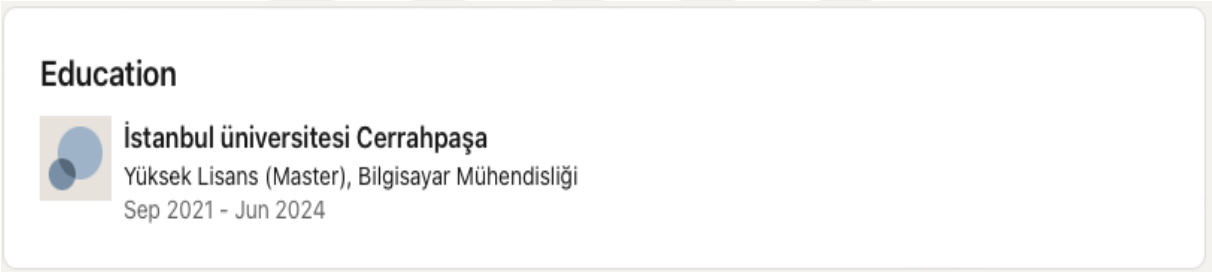
Gerçekleştirilen incelemelerde “Experience” veya Türkçe karşılığı ile “Deneyim” başlığı altında kullanıcıya ait çalışma geçmişinin yer aldığı gözlemlenmiştir.

Çalışma geçmişi detayında ise; Çalışılan kuruluş ismi, başlangıç ve ayrılış tarihi, çalışılan pozisyon ve istihdam türünün yer aldığı gözlemlenmiştir. Şekil 20 içerisinde deneyim başlığına ilişkin ekran görüntüsü yer almaktadır.



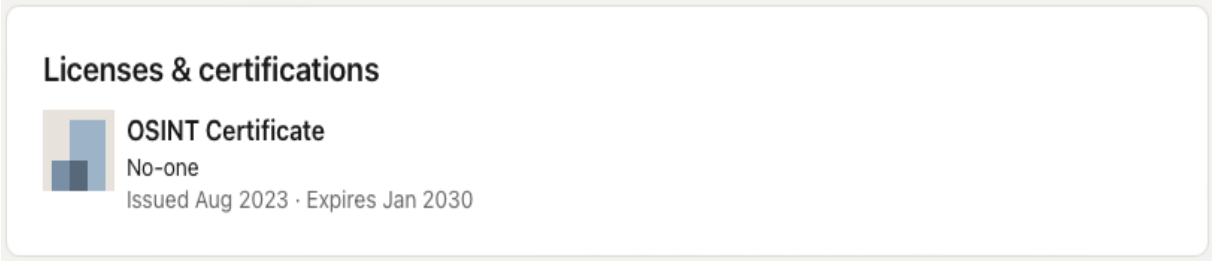
Şekil 20. Deneyim Başlığına İlişkin Ekran Görüntüsü.

Bir diğer başlık olan "Education" veya Türkçe karşılığı "Eğitim" olan başlığın altında kullanıcıya ait eğitim geçmişinin yer aldığı, eğitim detayında ise; Eğitim alının kurum, eğitimin türü, eğitimin dalı, başlangıç ve bitiş tarihlerinin yer aldığı gözlemlenmiştir. Şekil 21 içerisinde eğitim başlığına ilişkin ekran görüntüsü yer almaktadır.



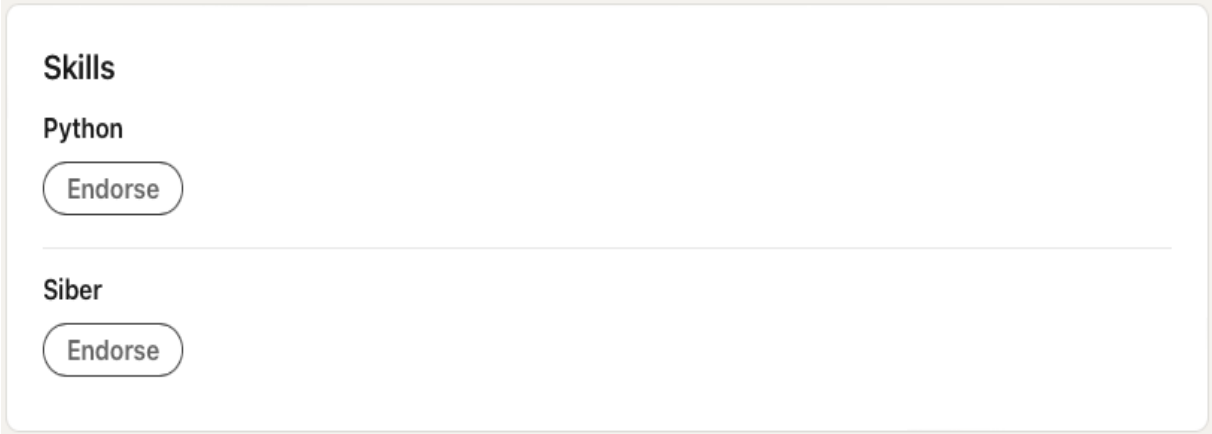
Şekil 21. Eğitim Başlığına İlişkin Ekran Görüntüsü.

Oluşturulan sosyal medya platformu içerisinde "Education" başlığı altında "Licences &certifications başlığı yer almaktadır. Türkçe karşılığı "lisanslar ve sertifikalar" olan bu başlık altında profil sahibi kullanıcı sahip olduğu lisans belgelerini ve sertifika belgelerini paylaşabilmektedir. Şekil 22 içerisinde lisanslar ve sertifikalar başlığına ilişkin ekran görüntüsü yer almaktadır.



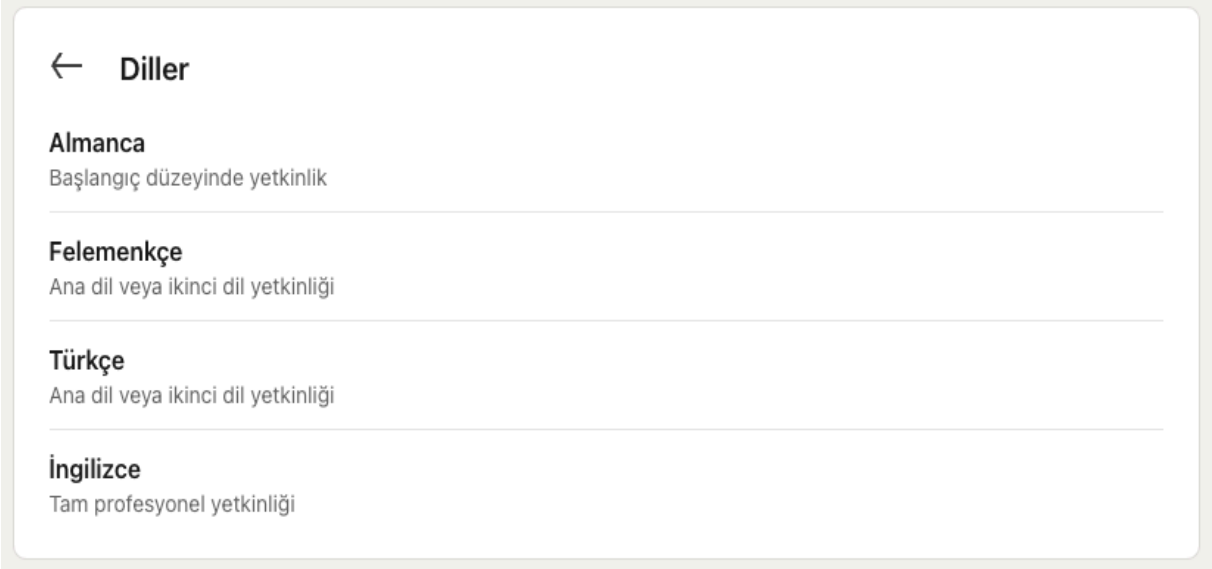
Şekil 22. Lisanslar ve Sertifikalar Başlığına İlişkin Ekran Görüntüsü.

LinkedIn profili sayfası içerisinde yer alan bir diğer başlık "Skills" başlığıdır. Türkçe karşılığı "yetenekler" olan bu başlığın altında profil sahibi, sahip olduğu yeteneklerini paylaşabilmekte ve diğer kullanıcılar tarafından bu yetenekler onaylanabilmektedir. Şekil 23 içerisinde yetenekler başlığına ilişkin ekran görüntüsü yer almaktadır.



Şekil 23. Yetenekler Başlığına İlişkin Ekran Görüntüsü.

LinkedIn profil sayfası içerisinde yer alan son başlık ise Diller başlığıdır. Burada profil sahibi hâkim olduğu yabancı dilleri ve bunlara ait bilgi düzeyini belirtebilmektedir. Şekil 24 içerisinde diller başlığına ilişkin ekran görüntüsü yer almaktadır.

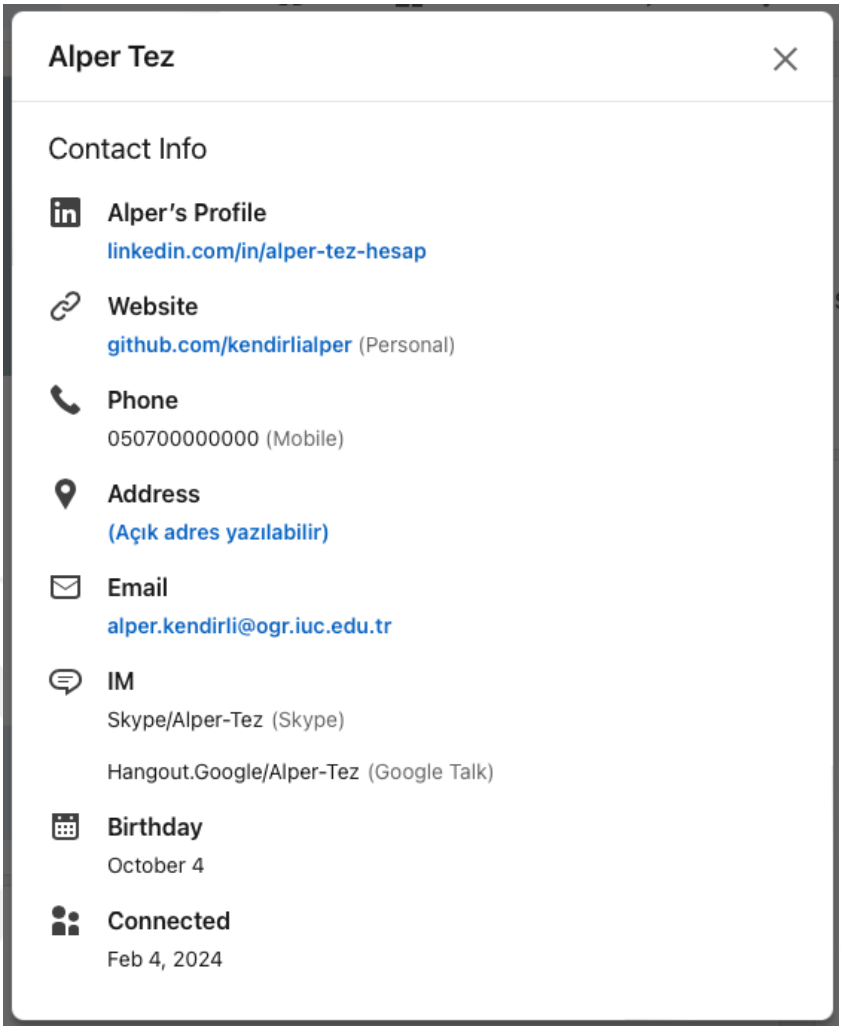


Şekil 24. Diller Başlığına İlişkin Ekran Görüntüsü.

Kullanıcı profilinde yer alan ve yukarıda bahsedilmiş olan verilerin dışında "More" veya Türkçe karşılığı ile "Daha Fazla" butonu altında da yine kullanıcı profiline ait kişisel veriler bulunmaktadır.

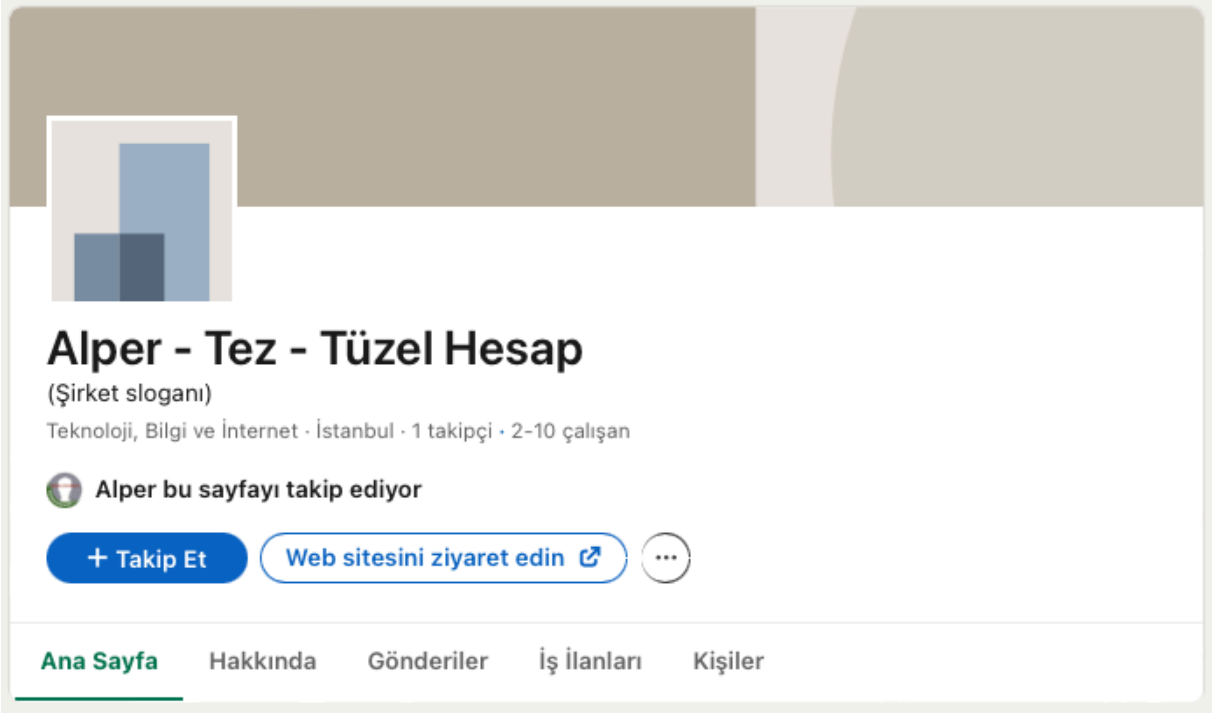
İlgili kişisel veriler yine LinkedIn sosyal medya platformunun sağladığı imkanlar neticesinde herhangi bir eksik alan bulunmadan doldurulmuş ve elde edilebilecek dijital ayak izine yönelik incelemeler gerçekleştirilmiştir.

İlgili butona tıklanması durumunda platform içerisinde bir pencere açıldığı gözlemlenmiş olup, profili incelenen kullanıcıya ait; kullanıcı adı bilgisi, web sitesi, telefon numarası, açık adres, eposta adresi, farklı mesajlaşma uygulamalarına ait kullanıcı adı bilgisi, doğum tarihi ve LinkedIn profilinin oluşturulma tarihinin yer aldığı gözlemlenmiştir. Şekil 25 içerisinde söz konusu pencereye ilişkin ekran görüntüsü yer almaktadır.



Şekil 25. Daha Fazla Başlığına İlişkin Ekran Görüntüsü.

LinkedIn üzerinde tüzel kişiler tarafından oluşturulan hesapların oluşturduğu dijital ayak izi ve buna bağlı atak yüzeyini incelemek üzere "Alper - Tez -Tüzel Hesap" isimli hesap oluşturulmuştur. Hesap oluşturulmasının ardından sosyal medya platformunun kullanıcıya sunduğu tüm bilgi alanları doldurulmuş ve herkese açık şekilde paylaşılmıştır. Oluşturulan tüzel hesaba yönelik ekran görüntüsü şekil 26 içerisinde yer almaktadır.

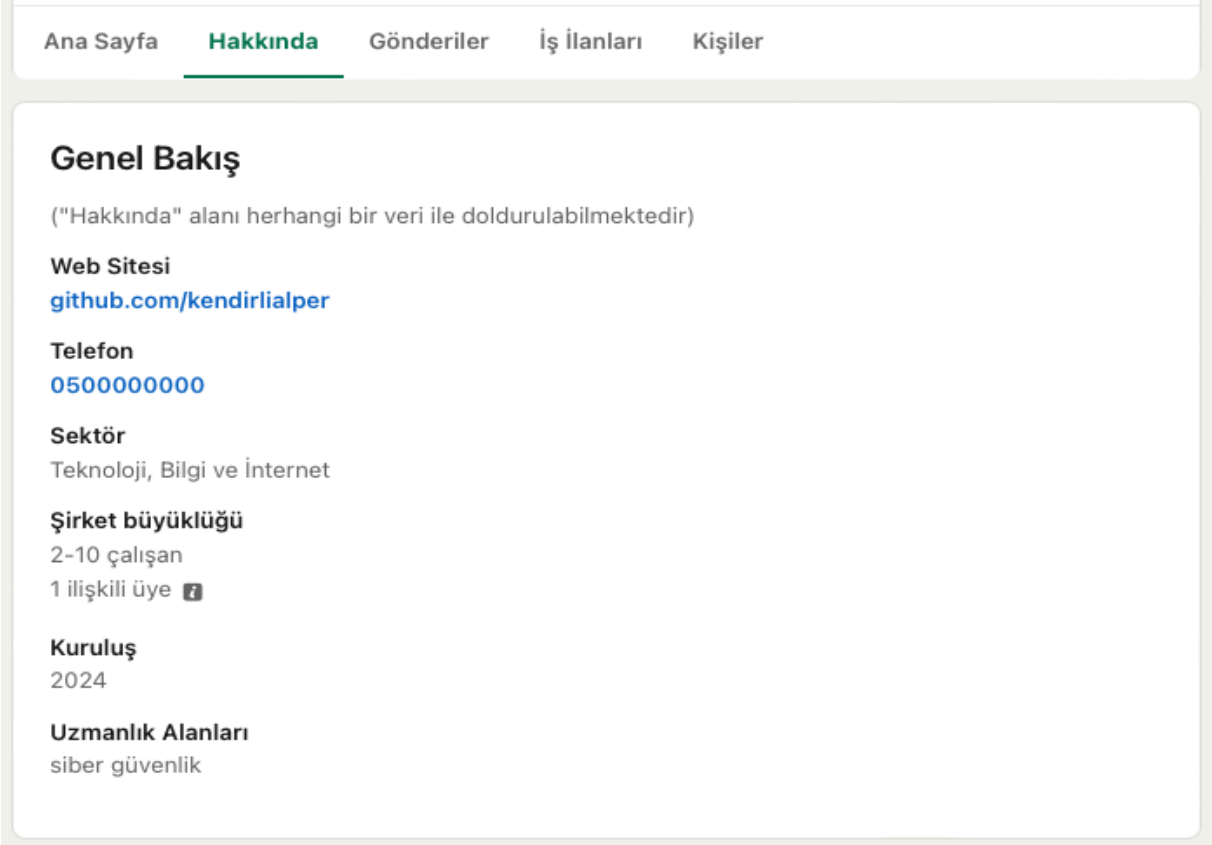


Şekil 26. LinkedIn Üzerinde Oluşturulan Tüzel Hesaba İlişkin Ekran Görüntüsü.

Oluşturulan tüzel hesaptan elde edilebilecek dijital ayak izlerini incelemek üzere oluşturulan hesap dışında harici bir hesap ile sosyal medya profili üzerinde inceleme sağlanmıştır. Profil sayfasında "Hakkında", "Gönderiler", "İş İlanları" ve "Kişiler" sekmeleri yer almakta olup, sosyal medya platformunun kullanıcıya doldurulmak üzere sunduğu bilgi alanlarını incelemek üzere "Hakkında", "İş İlanları" ve "Kişiler" sekmeleri incelemeye alınmıştır.

"Hakkında" sekmesi incelenmeye başlandığında "Genel Bakış", "Uzaktan Çalışma" ve "Konumlar" başlıklı bilgi alanları gözlemlenmiştir.

"Genel Bakış" bilgi alanında tüzel kişiye ait; herhangi bir veri ile doldurulabilen veri giriş alanı, web sitesi alanı, telefon numarası bilgisi, tüzel kişinin bulunduğu sektör, şirketin personel açısından büyüklüğü, kuruluş yılı ve uzmanlık alanlarına ilişkin doldurulabilir giriş alanlarının yer aldığı gözlemlenmiştir. Şekil 27 içerisinde ilgili bilgi alanına yönelik ekran görüntüsü yer almaktadır.

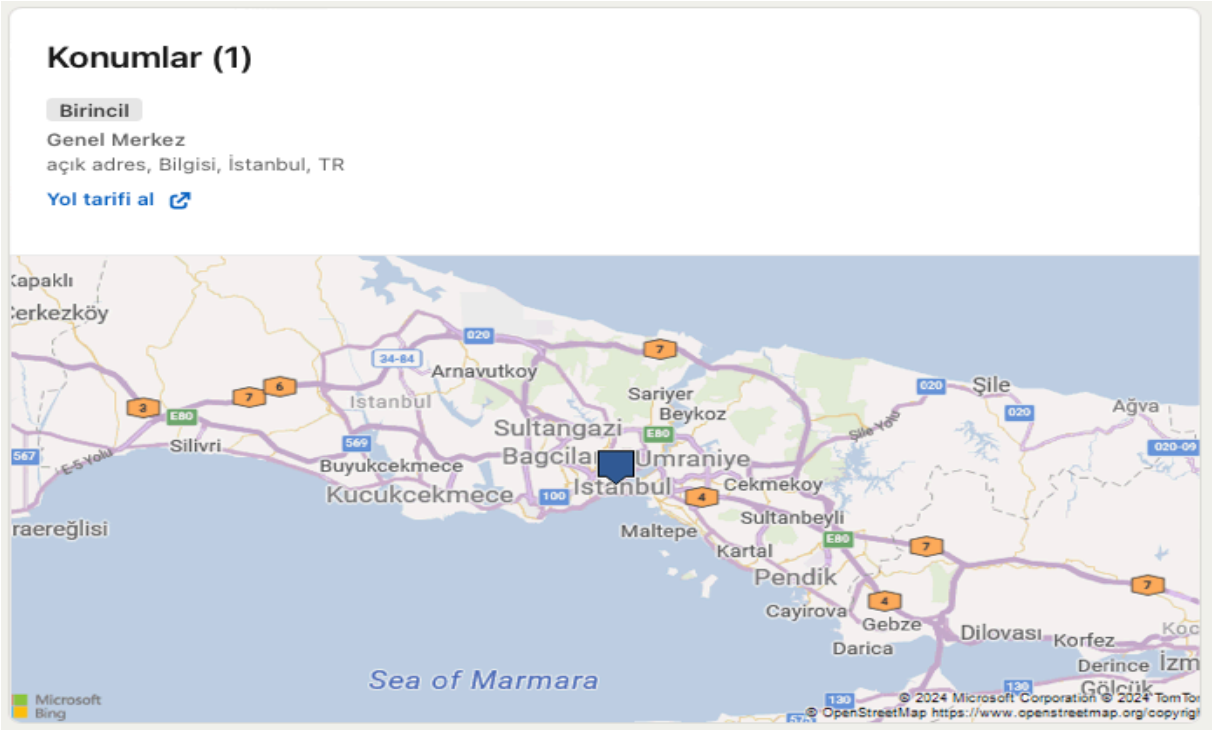


Şekil 27. Genel Bakış Sekmesine İlişkin Ekran Görüntüsü.

"Uzaktan çalışma" bilgi alanı incelendiğinde tüzel kişiye ait; işyeri politikası hakkında bilgi sağlamak için serbest veri giriş alanının, ödeme düzenleme bilgisi ve aşı politikası hakkında bilgi alanlarının bulunduğu gözlemlenmiştir. Şekil 28 içerisinde ilgili bilgi alanına yönelik ekran görüntüsü yer almaktadır.

Şekil 28. İşyeri Politikası Hakkında Bilgi Bölümüne İlişkin Ekran Görüntüsü.

Hakkında sekmesi altında yer alan son başlık ise “Konumlar” başlığıdır. Tüzel kişinin bulunduğu konuma ilişkin adres bilgisi açık adres şeklinde girilebilmektedir. Girilen açık adres doğrultusunda ise harita üzerinden otomatik konumlandırma yapılmaktadır. Şekil 29 içerisinde ilgili bilgi alanına yönelik ekran görüntüsü yer almaktadır.



Şekil 29. Konum ve Açık Adres Bilgisine İlişkin Ekran Görüntüsü.

3.2. Arama Motorları Üzerinden Elde Edilebilen Dijital Ayak İzi Ögeleri

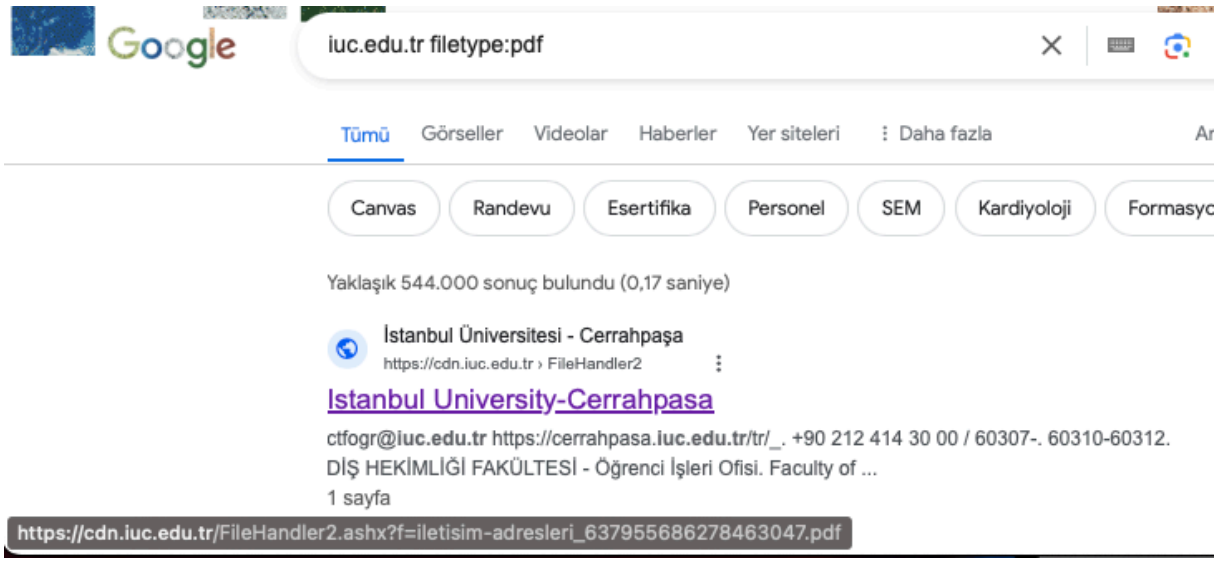
Arama motorları, internet ortamında herkese açık şekilde bulunan web sitelerini ve web sitesi içeriklerini endeksleyen, kullanıcının kullandığı arama kelimeleri doğrultusunda ilişkili olan sonuçları sunabilen yazılımlardır. Tehdit aktörleri bu yazılımlar aracılığı ile hedefe ait dijital ayak izlerini tespit ederek gerçekleştirecekleri siber saldırının hazırlıklarını yapabilmektedir. Tehdit aktörleri, topladıkları veri içerisinde hedefe ait hassas verileri ve hedefe ait teknolojik altyapıya yönelik bilgileri analiz ederken hedefe ait zayıf noktaları tespit etmeye çalışmaktadır [26].

3.2.1. Google Dorkıng Teknikleri İle Elde Edilebilen Dijital Ayak İzi Ögeleri

Açık kaynak istihbarat çalışmalarında kullanılan en temel tekniklerden biri ise “Google Dorking” olarak adlandırılan, arama motorlarını özelleştirmiş arama komutları ile istenilen

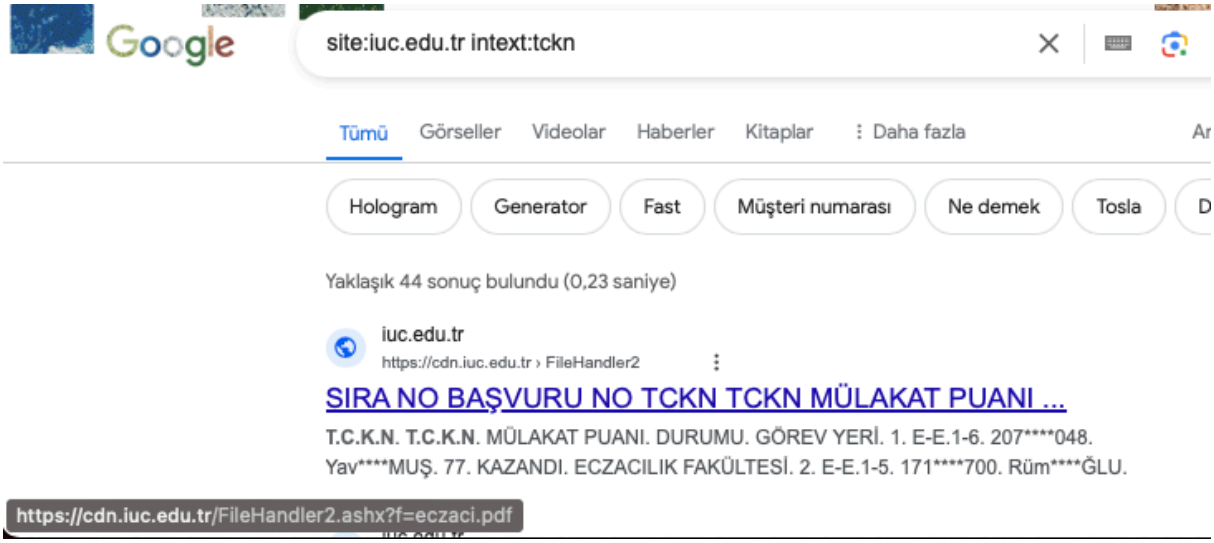
verileri elde etmeye yönelik kullanılan tekniktir. Arama motorlarında özelleştirilmiş arama komutlarını kullanarak herkese açık web sayfalarda bulunan ve indekslenen verileri elde etmek mümkündür [27].

Aşağıda yer alan örnek ekran alıntısında İstanbul Üniversitesi Cerrahpaşa'ya ait web sitesinde bulunan ".pdf" uzantılı dosyalara yönelik arama gerçekleştirilmiş olup, çıkan sonuçlarda ilgili alan adı altında bulunan tüm indekslenen ".pdf" uzantılı dosyaları getirdiği gözlemlenmiştir. Şekil 30 içerisinde ilgili sorguya ilişkin ekran görüntüsü yer almaktadır.



Şekil 30. iuc.edu.tr Web Sayfasında Yer Alan .Pdf Uzantılı Dosyalara İlişkin Sorgu.

Aynı teknik ile iuc.edu.tr adresinde bulunan ve içerisinde "tckn" ibaresi bulunan web sayfalarına yönelik araştırma gerçekleştirildiğinde ilgili web sayfasında paylaşılan ve "tckn" ibaresinin bulunduğu dosyaların getirildiği tespit edilmiştir. Şekil 31 içerisinde ilgili sorguya ilişkin ekran görüntüsü yer almaktadır.



Şekil 31. iuc.edu.tr web sayfasında yer alan ve içeriğinde TCKN ibaresi bulunan sonuçlara ilişkin Sorgu.

Google dorking tekniği ile tespit edilmesi hedeflenen anahtar kelimelere ve dosya türlerine yönelik arama gerçekleştirilebilmektedir. Elde edilebilecek veriler konusunda herhangi bir kısıtlama bulunmamakta olup, tespit edilebilecek veriler tamamen veriyi barındıran web sayfası ile ilişkilidir.

Tehdit aktörleri Google dorking teknikleriyle hedefe yönelik dijital ayak izi ögelerini tespit edebilmekte olup, gerçekleştirilmesi hedeflenen siber saldırıları bu doğrultuda gerçekleştirebilmektedirler [28].

3.2.2. Shodan Üzerinden Elde Edilebilen Dijital Ayak İzi Ögeleri

Shodan, ağlar ve ağ bağlı cihazlar hakkında arama gerçekleştirilebilen arama motorudur. Google, Bing, Yahoo benzeri arama motorları ile elde edilemeyecek tüzel kişilere ait ağ altyapısı ve ağ bağlı sistemler hakkındaki bilgi edinmeyi amaçlamaktadır. Sodan arama motoru aracılığı ile; IoT cihazları, ağ yönlendiricileri (Router), sunucular ve benzeri varlıkları inceleme imkanımız bulunmaktadır [29].

Shodan arama motoru internete bağlı varlığın; açık portları, üzerinde barındırdığı uygulama bilgisi, mevcut zafiyet bilgisi, sertifika bilgisi gibi çeşitli bilgileri sunabilmektedir [30].

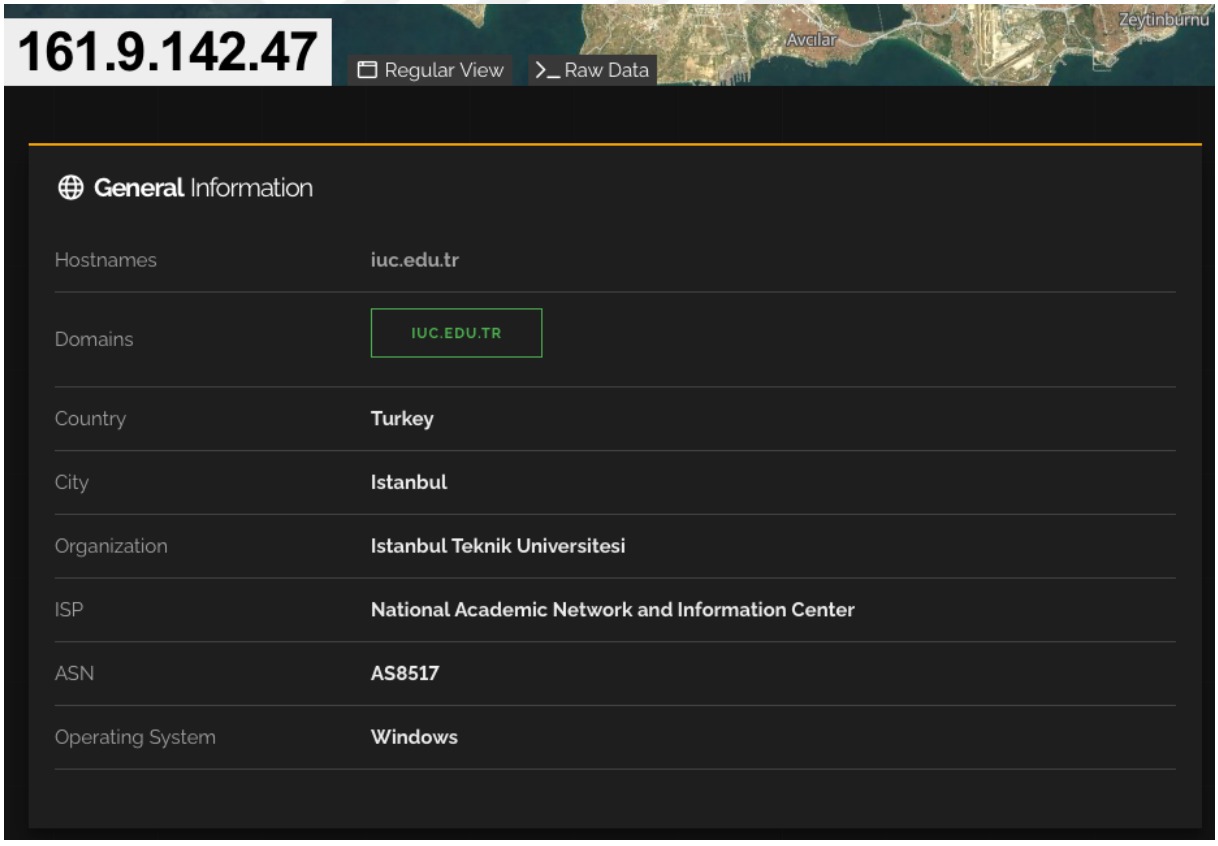
Tehdit aktörü bakış açısı ile Shodan arama motorunun yetkinliğini incelediğimizde MITRE ATT&CK çerçevesine göre tarama aşamasında kullanılabileceği değerlendirilmektedir. Shodan

arama motorunun çıktılarına göre tehdit aktörleri hedefe nereden erişim sağlayabileceği ve nasıl yöneteceği konusunda fikir verebilmektedir [31].

Tez çalışması kapsamında Shodan üzerinden elde edilebilecek veriler incelemek üzere rastgele teknolojik varlıklar incelenmiştir. Veriler incelenirken elde edilebilecek en fazla veriye ulaşılmak istenmiştir.

İncelemeye İstanbul Üniversitesi - Cerrahpaşa'ya ait web sayfası ile başlanmış olup, aramada yalnızca "iuc.edu.tr" ifadesi kullanılmıştır.

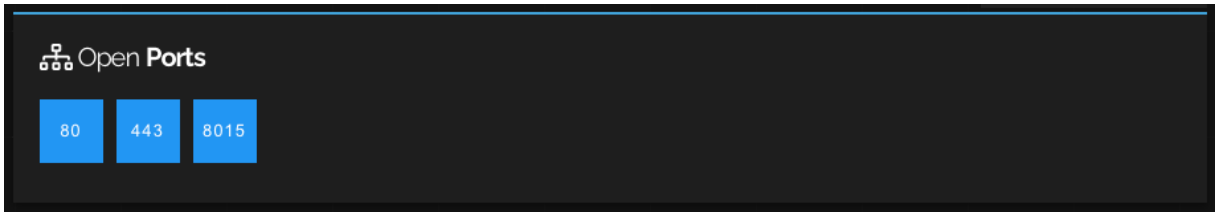
Shodan arama motoru bize ilgili web sayfasına ait genel bilgiler kısmında; IP adresi, alan adı bilgisi, Bulunduğu ülke ve şehir bilgisi, şirket adı, ISP (internet servis sağlayıcısı) bilgisi, ASN (Özerk Sistem Numarası) bilgisi ve işletim sistemi bilgisi yer almaktadır. Şekil 32 içerisinde genel bilgiler ekranına ait ekran görüntüsü yer almaktadır.



Şekil 32. iuc.edu.tr Sorgusuna İlişkin Genel Bilgiler.

Shodan arama motoru, incelenen varlığa ait açık port bilgisini de sunmaktadır. Mevcut örnekte 161.9.142.37 IP adresi üzerinde; 80, 443 ve 8015 portlarının açık ve internetten erişilebilir

durumda olduğu gözlemlenmiştir. Şekil 33 içerisinde yer alan ekran görüntüsünde incelenen varlığa ait açık port bilgisi yer almaktadır.



Şekil 33 iuc.edu.tr Alan Adının Üzerinde Açık Olan Portlara İlişkin Bilgiler.

İlgili örneğe ait 80 portu incelendiğinde Microsoft IIS ağ servisinin 10.0 sürümünün çalıştığı gözlemlenmiştir. Şekil 34 içerisinde çalışan ağ servisine yönelik ekran görüntüsü yer almaktadır.

Şekil 34. 80 Numaralı Port Üzerinde Açık Olan Servise İlişkin Bilgiler.

Yine aynı örnek IP'ye ilişkin 443 portu incelendiğinde yine Microsoft IIS ağ servisinin 10.0 sürümün yer aldığı gözlemlenmiş olup, ağ servisine ek olarak SSL sertifikasının da yer aldığı gözlemlenmiştir.

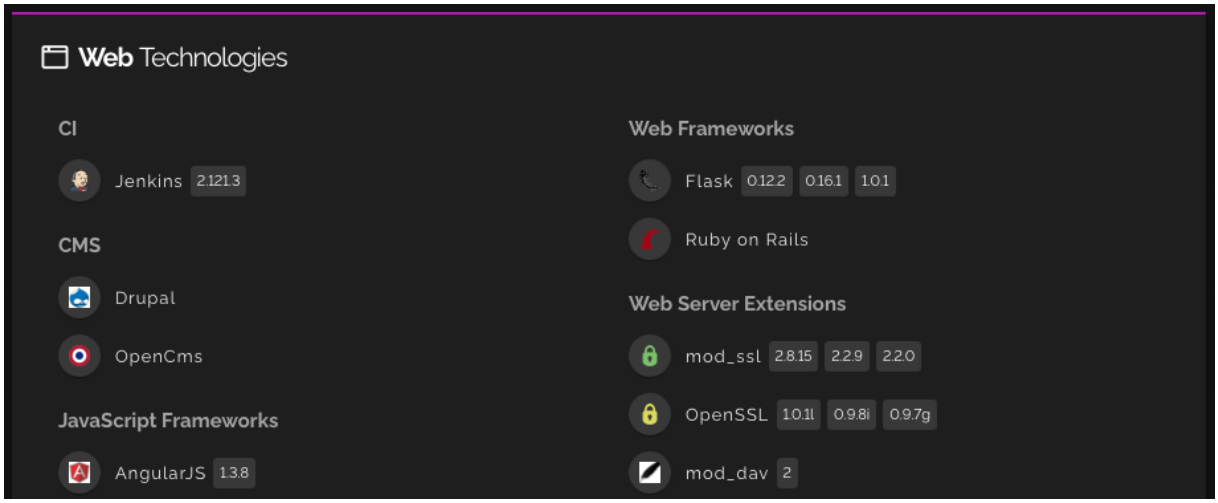
Sertifikaya ait bilgiler incelendiğinde "E-TUGRA EBG BILISIM TEKNOLOJILERI VE HIZMETLERI ANONIM SIRKETI" tarafından oluşturulduğu ve 28 Ocak 2025 tarihinde kullanım süresinin sona ereceği gözlemlenmiştir. Buna ek olarak kullanılan şifreleme algoritması bilgisi de yer almaktadır.

Şekil 35 içerisinde 443 port'u üzerinde çalışan servise ve barındırdığı sertifikaya yönelik ekran görüntüsü yer almaktadır.

Şekil 35. 443 Numaralı Port Üzerinde Açık Olan Servis ve Sahip Olduğu SSL Sertifikasına İlişkin Bilgiler.

Mevcut internet varlığı üzerinde incelenebilecek farklı bir öge bulunmamasından dolayı rastgele örnekler ile dijital ayak izlerinin tespitine devam edilmiştir. Rastgele bir internet varlığının seçilmesi ve incelenmesinin ardından ilgili varlıkta ağ teknolojileri başlığının varlığı gözlemlenmiştir. İlgili başlık altında varlığın üzerinde kurulu olan ve kullan; servislerin çerçevelerin ve uzantıların bulunduğu tespit edilmiştir.

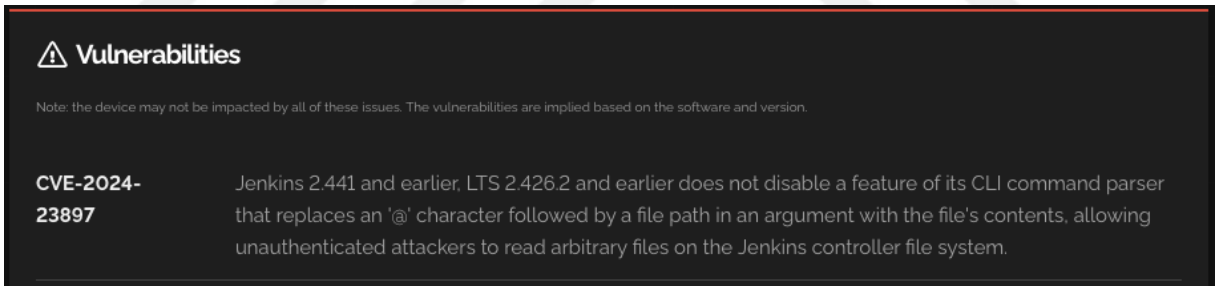
Şekil 36 içerisinde kullanılan web teknolojilerine ait ekran görüntüsü yer almaktadır.



Şekil 36. Shodan Aracılığı İle Tespit Edilebilen Web Teknolojileri Sekmesine İlişkin Ekran Görüntüsü.

Ağ teknolojilerinin incelendiği varlık üzerinde incelemeler devam ettirildiğinde zafiyetler başlığı tespit edilmiştir. İlgili başlık altında, varlık üzerindeki servislerinin barındırdıkları zafiyetlere yönelik bilgiler yer almaktadır.

Şekil 37 içerisinde zafiyetler başlığına yönelik ekran görüntüsü yer almaktadır.



Şekil 37. Shodan Aracılığı ile Tespit Edilebilen Zafiyetler Sekmesine İlişkin Ekran Görüntüsü.

3.3. Maltego Üzerinden Elde Edilebilen Dijital Ayak İzi Ögeleri

Maltego, OSINT süreçlerini ve yaklaşımlarını otomatize eden, dijital ayak izi incelenen kişilere (gerçek veya tüzel) ve teknolojik altyapılara ait tespit dijital ayak izi ögelerini ilişkilendiren, oluşturulan ilişkiler sonrasında görsel olarak diyagram sunan bir yazılımdır [12].

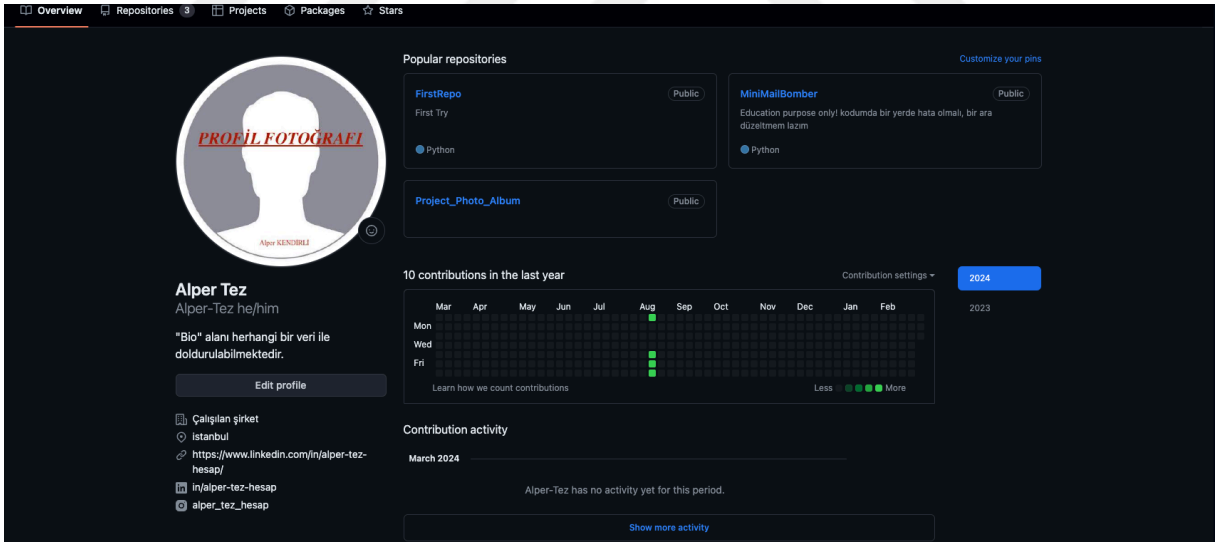
Maltego aracı sayesinde kişilere ait her türlü kişisel bilgi ile birlikte teknolojik altyapılara ait; alan adı, alt alan adı, IP adresi, açık portlar, zafiyetler, DNS kaydı, kullanılan servisler, sertifika bilgisi ve metadata bilgisine ulaşılabilmektedir[12].

3.4. Github Üzerinden Elde Edilebilen Dijital Ayak İzi Ögeleri

Kod geliştiricilerinin ve açık kaynak kodlu projelerin artması ile birlikte yazılım kodlarının herkese açık paylaşılabileceği, versiyon kontrolünün yapılabileceği, kişilerin yazdıkları proje kodlarını yayınlayabileceği bir platform ihtiyacı doğmuştur [32]. Mevzu bahis ihtiyaçlara yönelik sunulan çözümlerden biri olan kod paylaşım platformu GitHub üzerinde dijital ayak izine yönelik incelemeler gerçekleştirilmiştir.

Tez çalışması kapsamında GitHub üzerinde "Alper Tez" isminde bir kullanıcı oluşturulmuş olup, platformun kullanıcıya sunduğu her bilgi alanı doldurulmuş ve herkese açık görüntülenecek şekilde yapılandırılmıştır.

Oluşturulan hesaba üçüncü bir hesaptan kontrol edildiğinde sırasıyla; isim bilgisi, kullanıcı adı bilgisi, hitap/zamir bilgisi, serbest biyografi alanı, çalışılan şirket, konum bilgisi, harici web sayfası bilgisi, sosyal medya adresleri ve kişinin geliştirdiği projeler bilgisinin yer aldığı gözlemlenmiştir. Şekil 38 içerisinde oluşturulan hesaba yönelik ekran görüntüsü yer almaktadır.



Şekil 38. Oluşturulan GitHub Hesabına ilişkin Ekran Görüntüsü.

3.5. Whois Kayıtları Üzerinden Elde Edilebilen Dijital Ayak İzi Ögeleri

1980'li yılların başında; alan adları, kişiler ve kaynaklar hakkında temel bilgileri derlemek üzere oluşturulan WHOIS protokolü, 1982 yılında standardize edilerek günümüzde A.B.D. Bilgi Sistemleri Savunma Ajansı olarak bilinen kurum tarafından yönetilmeye başlanmıştır.

Oluşturulduğu tarih itibariyle 43 numaralı port üzerinden sağlanan verilerin herhangi bir sabit içeriği veya formatı bulunmamaktaydı. 1990'lı yılların sonuna doğru alan adlarının ticarileşmesi ile birlikte alan adı kayıtlarında bütünlük bozulmaya ve verilerde uyuşmazlıklar açığa çıkmıştır. Yaşanılan problemlerin ardından A.B.D. Bilgi Sistemleri Savunma Ajansı kayıtları ICANN (Internet Corporation for Assigned Names and Numbers) adı altında sabit formatta ve herkese açık şekilde sunulmaya başlanmıştır [33].

2018 yılında Avrupa Birliği'nin GDPR'ı (General Data Protection Regulation) tanıtmasının ardından veriler ICANN tarafından halka kısıtlı olarak, akreditasyona sahip kurumlara ise verinin tamamını sunmaya devam etmiştir [34].

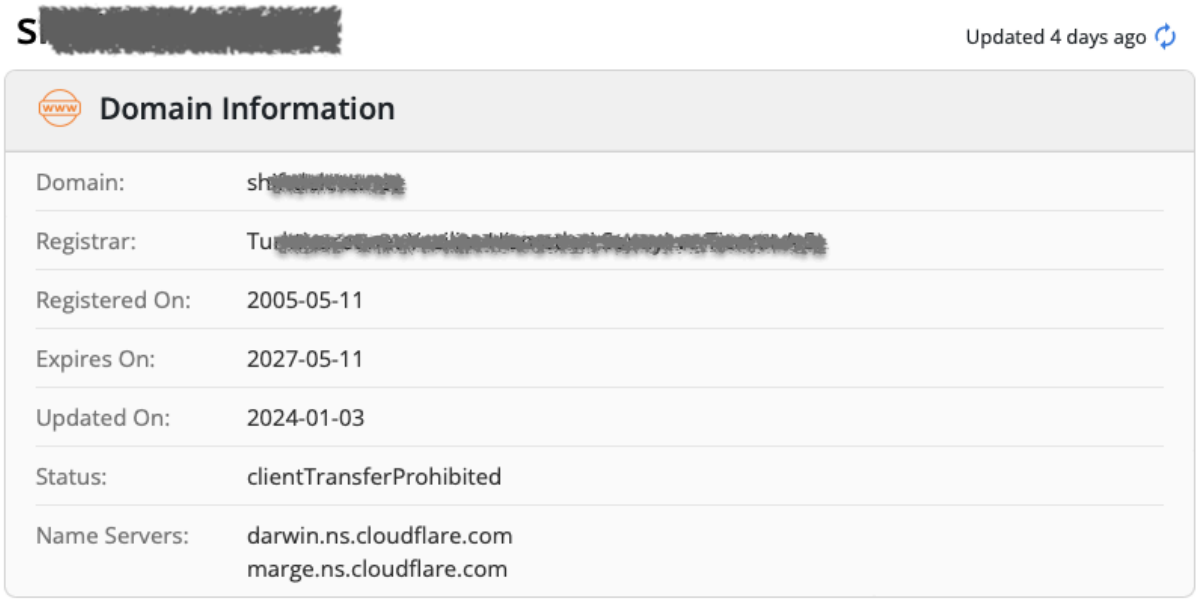
WHOIS kayıtları aracılığı ile hedefe yönelik kişisel verileri toplamak mümkündür, bu verilerin arasında; isim bilgisi, telefon numarası, adres bilgisi, mail adresi bilgisi tespit edilebilmektedir. Whois kayıtları aracılığı ile ayrıca hedef alan adının farklı alan adları ile ilişkisi tespit edilebilmektedir [35].

Tez çalışması kapsamında verinin içeriğinden ziyade elde edilebilecek verinin türü tespit edilmeye çalışılmakta olup, barındırdığı veri çeşidinin zenginliği ve GDPR kapsamında verilerin maskelenmiş olmasından ötürü yaygın olarak kullanılan bir alan adına ait WHOIS kayıtları incelenmiştir.

WHOIS kayıtlarını incelemeye yönelik çeşitli uygulamalar, araçlar ve web siteleri mevcut olup, çalışma kapsamında ICANN'in sorgulama arayüzü ve "www.whois.com" adresleri kullanılmıştır.

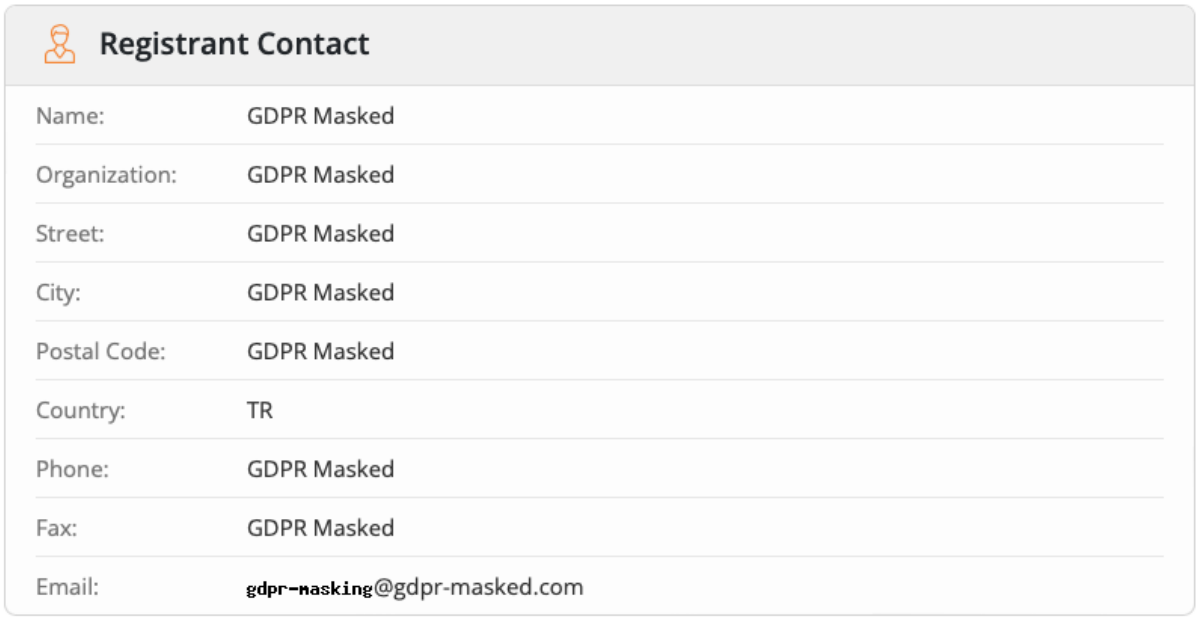
Alan adı sorgulandığında; "Alan Adı Bilgisi", "Kayıt Eden İletişim", "Yönetici İletişim" ve "Teknik İletişim" olmak üzere 4 farklı ana başlıkta veri sunmaktadır.

İlk başlık olan "Alan Adı Bilgisi" başlığı altında ; Alan adının kendisi, alan adını kayıt eden kuruluş ismi, ilk kayıt tarihi, güncelleme tarihi, bitiş tarihi, alan adının durumu ve alan adının bağlı olduğu DNS bilgisi yer almaktadır. Şekil 39 içerisinde ilgili başlığa yönelik ekran görüntüsü yer almaktadır.



Şekil 39. Alan Adı Bilgisine İlişkin Ekran Görüntüsü.

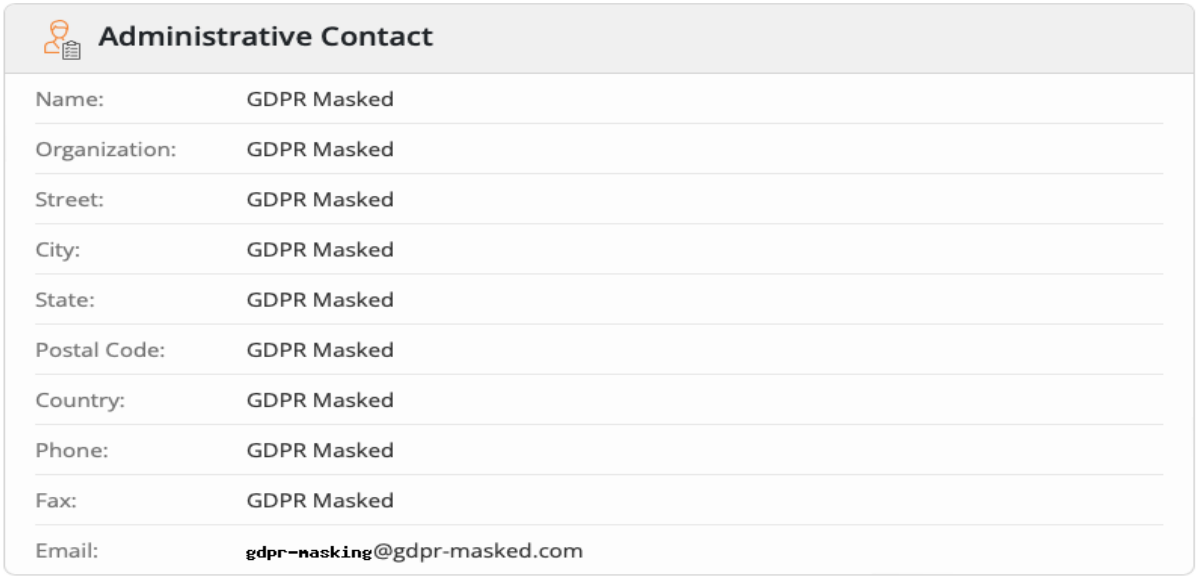
Kayıt eden kuruluşa ait bilgileri içeren başlık içeriğinde ise; kuruluşa ait isim bilgisi, açık adres bilgisi, telefon numarası, faks numarası ve e-posta adresi bilgileri yer almaktadır. Şekil 40 içerisinde ilgili başlığa yönelik ekran görüntüsü bulunmaktadır.



Şekil 40. Kayıt Eden Kuruluşa İlişkin Veriler.

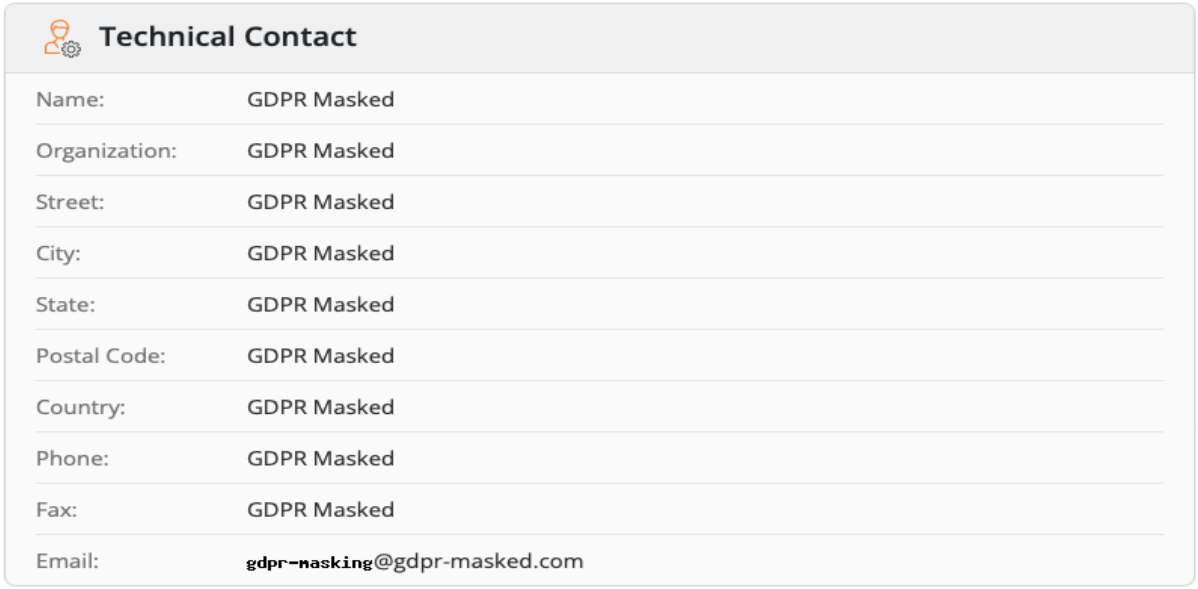
Yönetici iletişim bilgilerinin yer aldığı başlık altında alan adının yöneticiliğini gerçekleştiren gerçek veya tüzel kişiye ait iletişim bilgileri yer almaktadır. Mevcut iletişim bilgilerinin arasında; kuruluşa ait isim bilgisi, açık adres bilgisi, telefon numarası, faks numarası ve e-posta

adresi bilgileri yer almaktadır. Şekil 41 içerisinde ilgili başlığa yönelik ekran görüntüsü bulunmaktadır.



Şekil 41. Yönetici İletişim Bilgilerine Yönelik Verileri.

Teknik iletişim bilgilerinin yer aldığı başlık altında alan adının teknik olarak yöneticiliğini gerçekleştiren gerçek veya tüzel kişiye ait iletişim bilgileri yer almaktadır. Mevcut iletişim bilgilerinin arasında; kuruluşa ait isim bilgisi, açık adres bilgisi, telefon numarası, faks numarası ve e-posta adresi bilgileri yer almaktadır. Şekil 42. içerisinde ilgili başlığa yönelik ekran görüntüsü bulunmaktadır.



Şekil 42. Teknik iletişim bilgilerine yönelik veriler.

3.6. Veri Sızıntılarından Elde Edilebilen Dijital Ayak İzi Ögeleri

Teknolojinin ve amaca yönelik geliştirilmiş uygulamaların kullanımının artması ile birlikte her platform/uygulama kullanıcıya ait ve kullanıcının aktiviteleri sonucunda elde ettiği verileri saklamaktadır [36].

Uygulama ve platform sayısının artması ile birlikte herhangi bir uygulama veya platformun veri ihlaline maruz kalma ihtimali de artmaktadır. Kullanıcıların birden fazla uygulama veya platformda üyeliğinin bulunması olası bir veri ihlalinden etkilenme riskini de arttırmaktadır [37].

Uygulama veya platformun veri ihlaline uğraması sonucunda kullanıcılara ait; oturum açma bilgileri, kişisel veriler, çerezler (Cookies) ve diğer hassas veriler ele geçirilebilmektedir [36].

3.7. Dosya Üst Verilerinden (Metadata) Elde Edilebilecek Dijital Ayak İzi Ögeleri

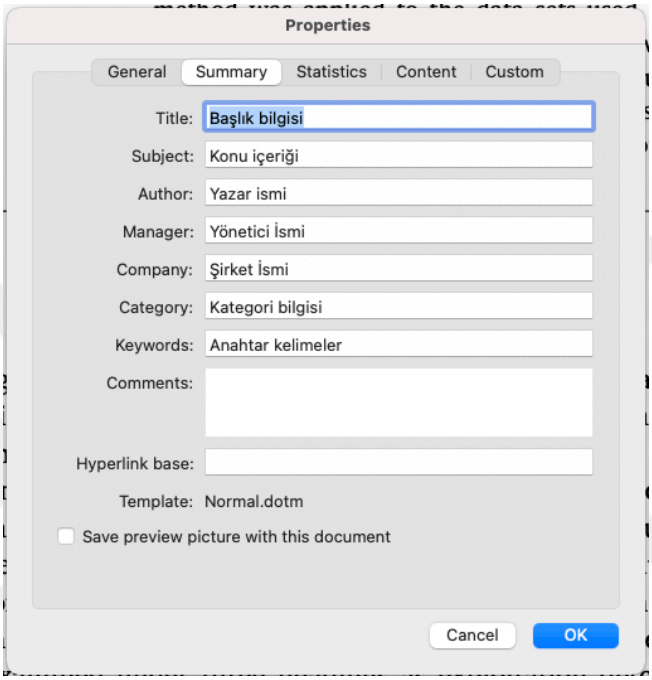
Üst veriler (Metadata), oluşturulan dosyaların özelliklerini tanımlamak için kullanılan dosya içerisinde barındırılan veriler bütünüdür [38].

Üst veriye yönelik gerçekleştirilen farklı bir çalışmada [39] 34 farklı dosya tipinin incelendiği belirtilmiş olup, tez çalışması kapsamında “.docx” ve “.JPG” uzantılı 2 farklı dosya incelenmiştir. Gerçekleştirilen inceleme esnasında oluşturulan dosyalarda doldurulabilecek tüm üst veri alanları doldurulmuştur.

JPG formatı bulunan bir dosya üzerinde inceleme yapıldığında; görseli oluşturan kişinin isim bilgisi, kullanılan fotoğraf makinesine ilişkin marka ve model bilgisi, kullanılan lense ilişkin marka ve model bilgisi, konum bilgisi telif hakkı bilgisi, kullanılan düzenleme yazılımına ilişkin bilgi ve açıklama kısmı yer almaktadır. Şekil 43 içerisinde JPG formatındaki dosyadan elde edilebilecek metadatalara ilişkin ekran görüntüsü yer almaktadır.

Şekil 43. JPG Formatında Bulunan Dosyaların Sahip Olabildiği Metadata Verileri.

Docx formatında bulunan dosya üzerinde inceleme yapıldığında; Başlık bilgisi, konu bilgisi, yazar ismi, yönetici ismi, şirket ismi, kategori bilgisi, anahtar kelimeler, yorum satırı ve bağlantı adresinin yer aldığı gözlemlenmiştir. Şekil 44 içerisinde docx formatındaki dosyadan elde edilebilecek metadatalara ilişkin ekran görüntüsü yer almaktadır.



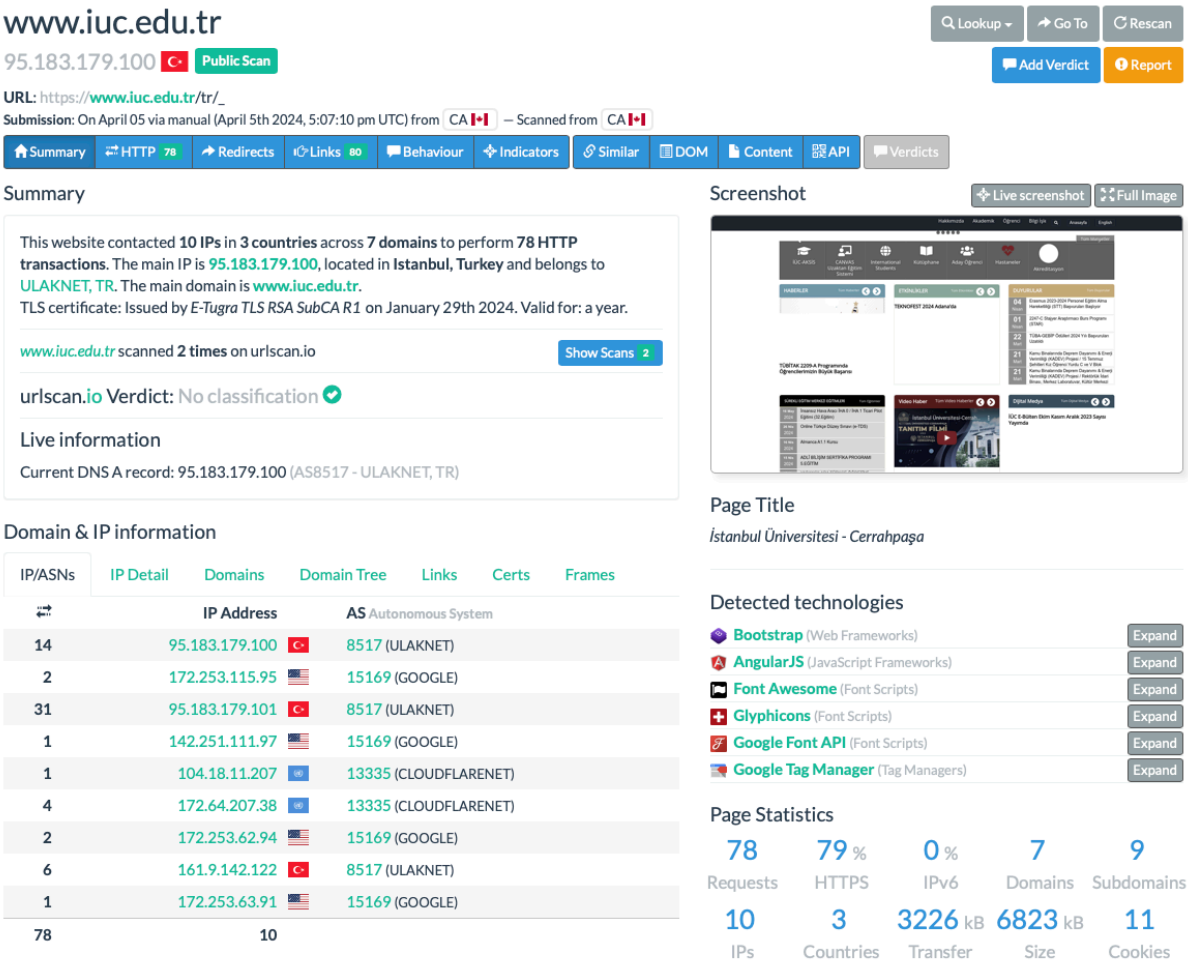
Şekil 44. Docx Formatında Bulunan Dosyaların Sahip Olabildiği Metadata Verileri.

3.8. Ağ Tarama Araçları

Ağ tarama araçları, ağ üzerinde bulunan veya belirlenen ağ ile bağlantılı olan tüm teknolojik altyapıların keşfi için kullanılmaktadır. Bu tarama araçları ile birlikte hedef ağa ait dijital ayak izi ögeleri elde edilebilir ve atak yüzeyi çıkartılabilmektedir. Ağ tarama araçları içerisinde en yaygın olarak kullanılanı NMAP'tir. NMAP tarama aracı temel olarak hedefe ait ağ yapılanmasını çıkartabilmekte, kullanılan servisleri ve açık olan portları tespit edebilmektedir. Bununla birlikte keşfedilen servislerde zafiyet taraması da yapabilmektedir. NMAP aracının dezavantajı ise taramalarını aktif yapmasıdır. Aktif tarama ile birlikte hedefe direkt olarak temas etmekte olup, hedefin tarama yapıldığını fark etmesine olanak sağlamaktadır [40].

3.9. Web Site Analiz Araçları

Web sitesi analiz araçları sayesinde hedef web sitesine ait teknolojik altyapı dijital ayak izi ögelerini elde etmek mümkündür. Web sitesi analiz araçları hedef web sitesinin alt alan adlarını, ip adreslerini, port bilgisini, DNS kayıtlarını, sertifika bilgisini ve metadata verilerini sunabilmektedir. Bu bilgileri açık kaynak araçlarla elde etmekle birlikte aktif tarama da gerçekleştirmektedir. Aktif taramada direkt olarak web sitesine ulaşıp, istenilen dosyaları hedef web sitesi üzerinden elde etmektedir. En popüler web sitesi analiz araçları arasında; Urlscan.io, pulsedive, SucuriSiteCheck bulunmaktadır. Şekil 45 içerisinde yer alan ekran görüntüsünde urlscan.io uygulamasından "www.iuc.edu.tr" adresine ait tarama sonucu yer almaktadır.



Şekil 45. Web Sitesi Analiz Aracı ile www.iuc.edu.tr Web Sayfasının Analiz Edilmesi.

3.10. Siber Saldırı Türleri ve İncelenmesi

Teknolojinin hızlı gelişimi beraberinde çeşitli riskleri de getirmiştir. Risklerden faydalanmak isteyen tehdit aktörleri çeşitli siber saldırı yöntemleri geliştirmiştir. Siber saldırıların çeşitliliğinden dolayı ortak bir sınıflandırma ve isimlendirme ihtiyacı doğmuştur[41].

Tez çalışması kapsamında dijital ayak izi ögelerinin kullanıldığı siber saldırılara yönelik inceleme gerçekleştirilmiştir [42]. İncelemeler esnasında pek çok siber saldırı türü gözlemlenmiş olup, mevcut durumda veri ihlali henüz gerçekleşmemiş ve siber saldırının keşif aşamasından sonraki ilk aşamada gerçekleştirilen siber saldırılar değerlendirilmiştir. Tespit edilen siber saldırı türleri aşağıda yer alan alt maddeler içerisinde incelenmiştir [43] [44].

3.10.1. Oltalama (Phishing) Saldırıları

Oltalama saldırıları, tehdit aktörlerinin hedefe yanıltıcı içeriklerle ulaşarak istenileni yaptırmaya yönelik geliştirilen siber saldırı türüdür. Siber saldırılar içerisinde en başarılı yöntem olarak tanımlanmakla birlikte aynı zamanda en yaygın siber saldırılardan biridir [45].

Tehdit aktörleri oltalama saldırısını gerçekleştirmeden önce hedeflerini seçmekle başlamaktadırlar. Bu seçim özel bir hedefe yönelik olabilmekle birlikte bir topluluk da hedef olabilmektedir. Tehdit aktörleri, çeşitli kaynaklardan elde ettikleri hedef bilgisi doğrultusunda siber saldırılarını planlamaktadırlar [46].

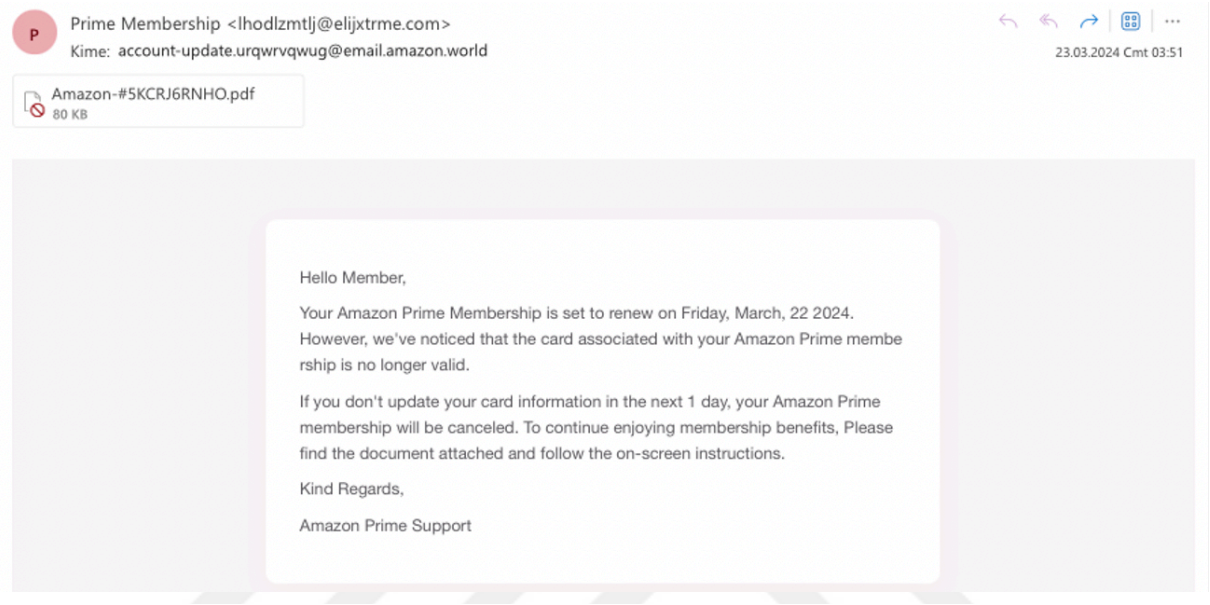
Hedefler, açık kaynak tehdit istihbarat yöntemleriyle belirlenebileceği gibi geçmiş dönemlerde yaşanılan çeşitli veri sızıntılarından yola çıkarak da belirlenebilmektedir.

Tehdit aktörleri hedef listesinin belirlenmesinin ardından hedefin veya hedeflerin ilgi alanları doğrultusunda sahte içerikli e-postalar, sms mesajları gönderebilmektedir. Bir senaryo çerçevesinde gerçekleşen bu siber saldırılarda tehdit aktörünün amacı hedefi yönlendirerek istenilen bilgiyi elde etmeye çalışmaktır.

2021 yılında Twitch yayın platformunun veri ihlaline maruz kalması sonucunda çeşitli kullanıcıların verileri sızdırılmıştı [47]. Tehdit aktörleri Twitch veri sızıntısından elde ettikleri verilerden yola çıkarak Twitch ve Twitch'in çatı şirketi olan Amazon'da hesabı bulunan kullanıcıları tespit edebilmektedir. Tehdit aktörleri ilgili hedeflerin tespitinin ardından kullanıcıları hedef alan yanıltıcı e-postalar gönderebilmektedir. E-posta içerisinde ise

kullanıcının verilerini elde etmeye yönelik veya cihazlarına zararlı yazılım yerleştirmeye yönelik içerik bulunmaktadır.

Şekil 46 içerisinde bulunan ekran görüntüsünde yer alan oltalama e-postası ilgili veri sızıntısı neticesinde sızdırılan e-posta adresinin hedef alınması ile meydana gelmiştir.



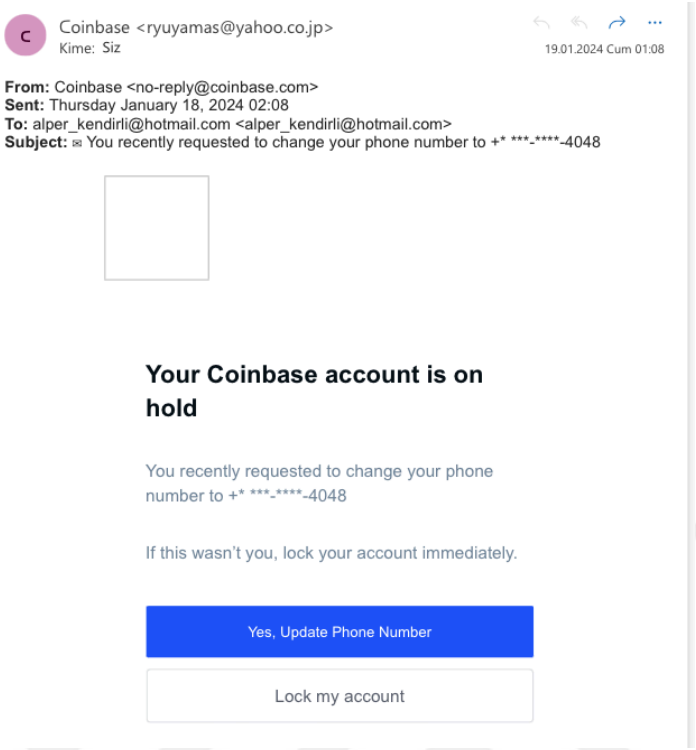
Şekil 46. Örnek Oltalama Saldırısı.

3.10.1.1. Hedef Odaklı Oltalama (Spear Phishing) Saldırısı

Spear phising saldırıları veya Türkçe karşılığı ile hedef odaklı oltalama saldırı temel olarak oltalama saldırıları ile aynı senaryoda kurgulanmaktadır. Hedef odaklı oltalama saldırıları ile normal oltalama saldırıları arasındaki tek fark gerçekleştirilen siber saldırılarda genel geçer bir oltalama içeriği yerine kişiye veya gruba yönelik özelleştirilmiş içeriklerin barındırmasıdır [48].

Tehdit aktörleri, hedef odaklı oltalama saldırılarında açık kaynak tehdit istihbaratı ile veya geçmiş dönemde yaşanan çeşitli veri sızıntılarından yararlanarak saldırılarını özelleştirmektedirler. Özelleştirilmiş olan bu siber saldırıların başarı oranı daha yüksek olmakla birlikte aynı zamanda tespiti de daha zor olmaktadır [49].

Şekil 47 içerisinde yer alan örnekte, tehdit aktörü hedefine oltalama e-postası gönderirken uyguladığı senaryoyu desteklemek adına hedefe ait telefon numarası bilgisini de eklemiştir. Eklediği telefon numarası ile inandırıcılığı arttırmakla birlikte hedefin istenileni yapma ihtimali artmış bulunmaktadır.



Şekil 47. Örnek Hedef Odaklı Oltalama Saldırısı.

3.10.1.2. Balina (Whaling) Oltalama Saldırısı

Whaling saldırısı, hedef odaklı oltalama saldırılarının hedef olarak daha kısıtlanmış halidir. Tehdit aktörleri bu oltalama saldırısı ile birlikte herhangi bir kişi veya grubu hedef almak yerine mevki, pozisyon ve varlık açısından daha seçkin kişileri tercih ederek siber saldırılarını gerçekleştirmektedirler. Whaling oltalama saldırıları teknik ve taktik açısından hedef odaklı oltalama saldırılarından herhangi bir farklı bulunmamaktadır[50].

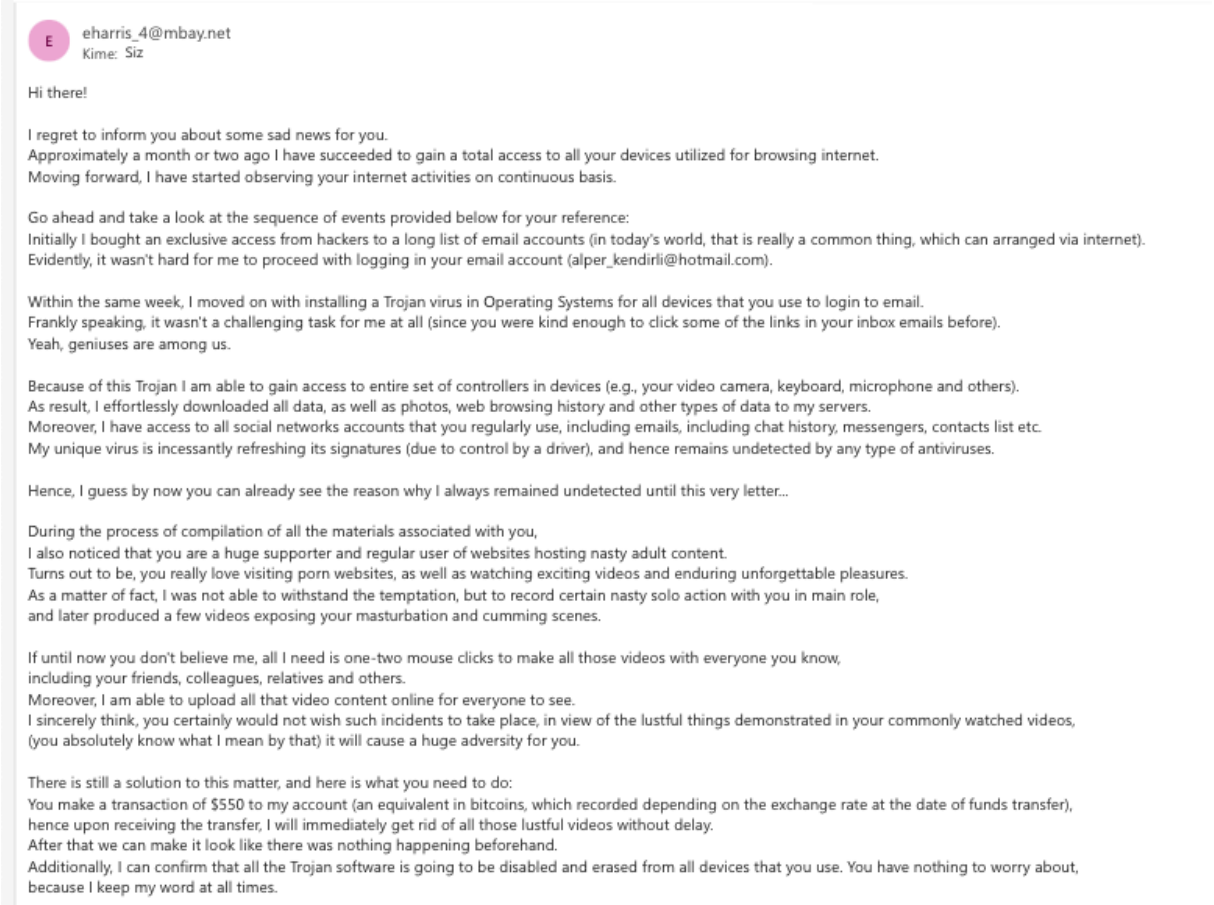
3.10.1.3. Scareware (Korkutucu) Oltalama Saldırısı

Scareware oltalama saldırıları, hedefin olası zafiyetlerinden yararlanarak, endişe ve korku ile istenileni yaptırmak üzere tasarlanmış oltalama saldırılarıdır. Tehdit aktörü açık kaynak tehdit istihbaratı veya geçmiş veri sızıntılarından elde ettiği veriler doğrultusunda hedefe yönelik oltalama saldırısı gerçekleştirmektedir [51].

Şekil 48 içerisinde yer alan ekran görüntüsünde tehdit aktörü e-posta aracılığı ile Scareware oltalama saldırısı gerçekleştirmiştir. Tehdit aktörü, hedefin cihazına erişim sağladığını ve tam yetki elde ederek; kamera, mikrofon, klavye ve benzeri çevre birimlerine erişim sağladığını, hedefin gerçekleştirdiği her işlemi elde ettiğini belirterek verilerin karşılığında para

istemektedir. İstenilen ücretin ödenmemesi durumunda ise verileri herkese açık şekilde paylaşmakla tehdit etmektedir.

İlgili e-postanın göndericisi olan tehdit aktörünün hedef üzerinde herhangi bir yetkisiz erişimi olmadığı bilinmekle birlikte, hedef üzerinde korku ve baskı oluşturarak istediğini yaptırmaya çalışmaktadır.



E eharris_4@mbay.net
Kime: Siz

Hi there!

I regret to inform you about some sad news for you.
Approximately a month or two ago I have succeeded to gain a total access to all your devices utilized for browsing internet.
Moving forward, I have started observing your internet activities on continuous basis.

Go ahead and take a look at the sequence of events provided below for your reference:
Initially I bought an exclusive access from hackers to a long list of email accounts (in today's world, that is really a common thing, which can arranged via internet).
Evidently, it wasn't hard for me to proceed with logging in your email account (alper_kendirli@hotmail.com).

Within the same week, I moved on with installing a Trojan virus in Operating Systems for all devices that you use to login to email.
Frankly speaking, it wasn't a challenging task for me at all (since you were kind enough to click some of the links in your inbox emails before).
Yeah, geniuses are among us.

Because of this Trojan I am able to gain access to entire set of controllers in devices (e.g., your video camera, keyboard, microphone and others).
As result, I effortlessly downloaded all data, as well as photos, web browsing history and other types of data to my servers.
Moreover, I have access to all social networks accounts that you regularly use, including emails, including chat history, messengers, contacts list etc.
My unique virus is incessantly refreshing its signatures (due to control by a driver), and hence remains undetected by any type of antiviruses.

Hence, I guess by now you can already see the reason why I always remained undetected until this very letter...

During the process of compilation of all the materials associated with you,
I also noticed that you are a huge supporter and regular user of websites hosting nasty adult content.
Turns out to be, you really love visiting porn websites, as well as watching exciting videos and enduring unforgettable pleasures.
As a matter of fact, I was not able to withstand the temptation, but to record certain nasty solo action with you in main role,
and later produced a few videos exposing your masturbation and cumming scenes.

If until now you don't believe me, all I need is one-two mouse clicks to make all those videos with everyone you know,
including your friends, colleagues, relatives and others.
Moreover, I am able to upload all that video content online for everyone to see.
I sincerely think, you certainly would not wish such incidents to take place, in view of the lustful things demonstrated in your commonly watched videos,
(you absolutely know what I mean by that) it will cause a huge adversity for you.

There is still a solution to this matter, and here is what you need to do:
You make a transaction of $550 to my account (an equivalent in bitcoins, which recorded depending on the exchange rate at the date of funds transfer),
hence upon receiving the transfer, I will immediately get rid of all those lustful videos without delay.
After that we can make it look like there was nothing happening beforehand.
Additionally, I can confirm that all the Trojan software is going to be disabled and erased from all devices that you use. You have nothing to worry about,
because I keep my word at all times.

Şekil 48. Örnek Scareware Saldırısı.

3.10.2. Fidye Yazılımı Saldırısı

Fidye yazılım saldırıları, tehdit aktörlerinin hedef sistemlere erişim elde etmesinin ardından tüm dosyaları şifreleyerek geçici olarak kullanılamaz hale getirmesi ve tekrardan dosyaların şifrelerinin çözülmesi için fidyenin istendiği siber saldırı türüdür. Tehdit aktörleri çeşitli yollarla sistemlere sızabilmekle birlikte temel olarak 2 farklı yöntem kullanmaktadırlar. Bunlardan birincisi kullanılacak zararlı yazılımın oltalama yöntemi ile iletilmesi ve oltalama saldırısının başarılı olması durumunda erişim sağlamasıdır. Diğer yöntem ise atak yüzeyinden

tespit edilen sistemlerde bulunan zafiyetlerin sömürülmesi ile sistemlere erişim sağlanmasıdır [52].

3.10.3. Parola Saldırıları

Parolalar teknoloji çağının en başından beri kullanılan bir kimlik doğrulama yöntemidir. Tehdit aktörleri hedeflerine ait parolaları ele geçirmek üzere çeşitli siber saldırı yöntemleri kullanmaktadırlar [53].

Parola oluşturma aşamasında insan faktörünün bulunduğu durumlarda, kullanıcıların şifreyi daha kolay hatırlamak üzere; aile bireylerin isimlerini, kişisel olarak önemli gördükleri tarihleri, destekledikleri spor takımlarını, bulundukları şehir veya memleketlerine ilişkin detayları, belirli motifleri içeren dizinler kullandıkları, pek çok durumda ise mevcut kullanıcı adı/parola bilgilerini farklı ortamlarda yeniden kullandıkları tespit edilmiştir [54].

3.10.3.1. Kaba Kuvvet (Brute-Force) Saldırıları

Kaba kuvvet saldırıları, tehdit aktörünün hedef oturum açma bilgilerine sahip olmadığı durumda, mümkün olan tüm oturum açma bilgilerinin kombinasyonlarını deneyerek kullanıcı adı ve/veya parolayı tespit etme çalışmasıdır [55].

Kaba kuvvet saldırılarını, bulunan ihtimallerin büyüklüğü sebebiyle oldukça yavaş sonuç verebilmektedir. Bu probleme çözüm olarak üretilecek dizinin uzunluğu, içereceği karakterler, oluşturulan dizinlerin içerisinde yer alacak karakter öbekleri şeklinde sınırlandırma yapılabilmektedir [56].

Tehdit aktörleri gerçekleştirdikleri açık kaynak istihbarat çalışmaları sonucunda hedef alınacak kişinin bilgilerine göre dizin üretme sürecini şekillendirebilmektedir.

3.10.3.2. Sözlük (Dictionary Attack) Saldırıları

Sözlük saldırıları uygulama aşamasında kaba kuvvet saldırılarıyla aynı yöntemi kullanmakla birlikte, sözlük saldırılarında olası tüm kombinasyonların denenmesi yerine denenecek olan kullanıcı adı/parola bilgisinin daha önceden belirlenerek yalnızca belirlenen dizinlerin denenmesi ile gerçekleşmektedir [57].

3.10.3.3. Oturum Açma Verisi İstifleme (Credential Stuffing)

Oturum açma verisi istifleme saldırıları (Credential Stuffing) saldırıları, uygulama aşamasında sözlük saldırıları ile aynı yöntemi kullanmakla birlikte, denenecek olan dizinler daha önceden

farklı veri ihlallerinden meydana gelen veri sızıntılarından elde edilen oturum açma verileri ile gerçekleştirilmektedir [58].

Tehdit aktörleri gerçekleştirecekleri oturum açma verisi istifleme saldırılarında, hedef üzerinde keşif incelemeleri yaparken hedefin geçmişte maruz kaldığı veri ihlalleri incelenir. İncelenen veriler sonucunda oturum açma verileri elde edilmeye çalışılmaktadır. Elde edilen oturum açma bilgileri denenerek yetkisiz erişim elde edilmeye çalışılmaktadır.

3.10.4. Kimliğe Bürünme (İmpersonation) Siber Saldırıları

Kimliğe bürünme (impersonation) saldırıları, tehdit aktörlerinin çeşitli yöntemler ile hedefe yönelik olarak olmadıkları kişi gibi davranması ve bu taklit davranışı sonrasında hedefe istenilen aksiyonların aldırılması ile sonuçlanan saldırılardır [59].

Sosyal medya platformları üzerinde gerçekleştirilen kimliğe bürünme saldırılarında tehdit aktörü, kimliğine bürüneceği kişinin dijital ayak izlerini toplamaktadır. Taklit edilecek kişi gerçek kişi ise temel olarak topladığı veriler arasında; adı/soyadı bilgisi, profil fotoğrafı, doğum tarihi, ikamet ettiği il, aile akraba bilgisi, iletişim bilgileri, desteklenen spor kulübü, desteklenen sivil toplum örgütü, desteklenen siyasi parti benzeri veriler bulunmaktadır. Eğer taklit edilecek kişi tüzel kişilik ise tehdit aktörleri; Tüzel kişiliğe ait isim bilgisi, konum bilgisi, logo/sembol bilgisi, tüzel kişinin hedef kitlesi ve personel bilgisi benzeri veriler yer almaktadır [60].

3.10.5. Zafiyet ve Yanlış Yapılandırmaya Dayalı Siber Saldırılar

Her ihtiyaç doğrultusunda çeşitli üreticiler tarafından teknolojik ürün geliştirilmesi sistemsel anlamda çeşitliliğe sebep olmuştur. Çeşitliliğin fazla olması sebebiyle sistem veya servis geliştiricilerinin sehven sebep oldukları zayıflıklar veya hatalar olarak tanımlanabilmektedir. Tehdit aktörleri hedef sistem üzerinde zafiyetleri tespit etmeye çalışırken hedefe ait; IP bilgisi, açık port bilgisi ve kullanılan servislere ait bilgileri elde ederek hedefte mevcut olan zafiyetleri tespit etmeye çalışmaktadır[61].

Tehdit aktörü, elde ettiği bilgiler doğrultusunda hedefte mevcut olan zafiyetleri sömürerek;

- Yetkisiz erişim sağlama
- Uzaktan yetkisiz komut çalıştırma
- Sistem üzerinde manipülatif işlem gerçekleştirme

- Zararlı yazılım kurma
- Arka kapı kurma
- Veri sızdırma
- Veri yok etme

İşlemlerini gerçekleştirebilmektedir.

Tehdit aktörleri tarafından sömürülecek zafiyetlerin de türleri bulunmaktadır. Aşağıda yer alan zafiyet türleri örnek olarak verilebilmektedir;

- Girdi kontrolünün hatalı yapılmasından kaynaklı zafiyetler.
- Yatayda veya dikeyde gerçekleştirilen kullanıcı geçişlerinde hatalı veya eksik kimlik doğrulamasından kaynaklı zafiyetler.
- Eksik veya hatalı kimlik doğrulamadan kaynaklı zafiyetler.
- Hatalı dizin izinlerinden kaynaklı zafiyetler.
- Bellek taşmasından kaynaklı zafiyetler.
- Siteler arası betik çalıştırma (XSS) zafiyetleri.
- SQL enjeksiyon zafiyetleri.

İlgili zafiyetlerin tamamında, zafiyetin bulunduğu sistemin IP adresi, port bilgisi ve zafiyetin barındıran sisteme yönelik bilgilerin edinilmesi gerekmektedir.

Hatalı yapılandırmalardan kaynaklı siber saldırılar ise; sistemlerin, sistem ayarlarının yanlış veya eksik olarak gerçekleştirilmesinden kaynaklanmaktadır. Bunlara örnek olarak;

- Varsayılan oturum açma bilgilerinin kullanılması.
- Hatalı kullanıcı yetkilendirmesi yapılmasından kaynaklı zafiyetler.
- Varsayılan güvenlik ayarlarının değiştirilmemesi.

- Mümkün olmasına rağmen SSL sertifikalarının kullanılmaması.
- Parola politikasının değiştirilebildiği durumlarda düşük korumalı politikaların belirlenmesi.
- Kullanılmayan portların kapatılmaması.
- Çoklu kimlik doğrulama mekanizmalarının aktif edilmemesi.

Başlıca örnekler arasında yer almaktadır [62].

3.10.6. Hizmet Kesintisi Saldırıları

Hizmet kesintisi saldırıları, tehdit aktörünün hedef teknoloji altyapısına; sahte, geçersiz ve yüksek miktarda istekte bulunması sonrasında hedef sistemin yanıt veremez duruma gelmesi olarak tanımlanmaktadır. Tehdit aktörleri hedefe yönelik hizmet kesintisi saldırısı düzenlemeden önce hedef alacakları IP adresi, portu ve üzerinde barındırdığı hizmeti bilmesi gerekmektedir. [63].

3.11. Siber Güvenlikte Risk Değerlendirmesi

Siber güvenlik alanında risk, bir siber saldırının gerçekleşme ihtimali ve siber saldırının gerçekleşmesi durumunda meydana gelen olası zararları tanımlamaktadır [64].

"Güvenlik Stresi" olarak tabir edilen ve Str ifadesi ile belirtilen terim, S varlığı üzerinde gerçekleştirilen siber güvenlik saldırılarının gelişmişlik seviyesini ve ne kadar sofistike olduğunu işaret etmektedir. 1 numaralı denklem içerisinde belirtilen V, hedef üzerinde mevcut dijital ayak izi ögelerini temsil etmekte olup, N ise toplam dijital ayak izi ögesi sayısını temsil etmektedir [65]. 2 numaralı denklemde ise varlığın sahip olduğu varlık sayısının sahip olabileceği varlık sayısına oranı hesaplanarak stres seviyesi elde edilmektedir [65].

$$(1) \qquad V = (V_n, n = 1, 2, \ldots, N)$$

$$(2) \qquad Str^s = \frac{Vn}{N}\ ,\ Str^s \in [0,1]$$

Siber saldırı riskinin hesaplanması için ise 3 numaralı denklemde yer aldığı üzere elde edilen güvenlik stresi miktarının zafiyete ait CVSS puanı ile çarpılmasından elde edilmektedir, zarar (harm) anlamına gelen h sembolü ile ifade edilir. Oltalama saldırıları ve Parola saldırıları

benzeri CVSS değerinin bulunmadığı ve insan faktörünün mevcut olduğu durumlarda risk hesaplaması h değişkeni ile yapılmaktadır [66]. Risk ($\mathcal{R}$) değeri hesaplanırken 4 numaralı denklemde yer aldığı üzere her bir Zafiyet için siber güvenlik riski ayrı ayrı hesaplanmakta olup, toplam mevcut olan zafiyet sayısına bölünmesi ile elde edilmektedir [66].

$$\mathcal{R} = Str^{s} . h \;\; ve \; h \in [0,1] \tag{3}$$

$$f(x) = \begin{cases} \mathcal{R} = Str^{s}.h\,, \; Vn \leq 1 \\ \mathcal{R} = \frac{\sum_{0}^{Vn} \mathcal{R}_{Vn}}{Vn}, \; Vn > 1 \end{cases} \tag{4}$$

4. BULGULAR

4.1. Kişilere Ait Çeşitli Platform ve Araçlardan Elde Edilebilecek Dijital Ayak İzi Ögeleri

Tez çalışması kapsamında, hedefin dijital ayak izi ve atak yüzeyi doğrultusunda tehdit aktörleri tarafından gerçekleştirilebilecek atak senaryolarını incelemek üzere hangi platformlardan hangi dijital ayak izi ögelerinin elde edilebileceği incelenmiştir.

Elde edilebilecek dijital ayak izleri literatüre uygun olarak 2 temel başlık altında incelenmiştir. Bunlar; kişilere (gerçek veya tüzel) ait dijital ayak izi ögeleri ve teknolojik altyapılara ait dijital ayak izi ögeleridir.

Kişilere ait dijital ayak izi ögeleri incelenirken ilgili tez çalışmasının "Yöntem" başlığı altında yer alan platformlardan (Facebook, Twitter, Instagram, LinkedIn, GitHub, WhoIS) yararlanılmıştır. Açık kaynak olan bu platformlarda hesap oluşturulup, platformun izin verdiği ölçüde tüm doldurulabilir kişisel bilgi alanları doldurulmuştur.

Oluşturulan hesaplar daha sonrasında farklı bir anonim hesap ile tekrar incelenmiş olup, farklı kullanıcıların hangi verileri elde edebileceği tespit edilmeye çalışılmıştır. Elde edilen her bir veri türü literatüre uygun olarak incelemeye alınmış olup, veriyi elde edebileceğimiz platformlar aşağıda yer alan tablo 3'e işlenmiştir

Tablo 3. Kişisel Verilerin Elde Edilebileceği Platformlar ve Elde Edilebilen Dijital Ayak İzi Ögeleri.

	Facebook (Kişisel Hesap)	Twitter (X)	Instagram (Kişisel Hesap)	Instagram (Tüzel Hesap)	Linkedin (Kişisel Hesap)	Linkedin (Tüzel Hesap)	GitHub (Kişisel Hesap)	WhoIS
Kullanıcı Adı		X	X	X			X	
Ad- Soyadı	X	X	X	X	X	X	X	X
E-posta adresi	X			X	X			X
Telefon numarası	X			X	X	X		X
Doğum Tarihi	X	X			X			
Doğum Yılı/Kuruluş Yılı	X	X				X		X
Zamir/hitap şekli			X				X	
Harici Website	X	X	X	X	X	X	X	X
İkamet yeri	X	X		X	X	X	X	X
Memleket/Doğum yeri	X							
İlişki durumu	X							
İlişki durumu Tarihi	X							
Aile/akraba Bilgisi	X							
Arkadaş Bilgisi	X	X	X	X	X			
Kariyer Bilgisi	X				X		X	
İş arayış durumu					X	X		
Personel bilgisi						X		
Eğitim Bilgisi	X				X			
Aldığı Eğitim/Sertifika					X			
Yetenekler/hobiler	X				X		X	
Bildiği Lisanslar/Diller	X				X			
Serbest Biyografi alanı	X	X	X	X	X	X	X	
Diğer Sosyal Medyalar	X	X	X	X			X	
Tüzel Kişi hakkında harici veriler						X		X

4.2. Teknolojik Altyapılara Ait Çeşitli Platform ve Araçlardan Elde Edilebilecek Dijital Ayak İzi Ögeleri

Teknolojik altyapıya ait dijital ayak izi ögeleri incelenirken literatüre uygun olan ayak izi ögeleri açık kaynak platformlar ve araçlar aracılığı ile tespit edilmeye çalışılmıştır. Platformlardan elde edilebilecek dijital ayak izi ögeleri tespit edilmiş olup, aşağıda yer alan tablo 4'te işlenmiştir.

Tablo 4. Teknolojik Altyapılara İlişkin Dijital Ayak İzi Ögelerinin Elde Edilebileceği Araçlar ve Elde Edilebilen Dijital Ayak İzi Ögeleri.

	Shodan	WhoIs	Google Dorking	Maltego	NMAP	Urlscan.io
Alan adı	X	X	X	X	X	X
Alt alan adı	X		X	X	X	X
Ip adresi	X	X	X	X	X	X
Açık port	X			X	X	X
Zafiyet	X			X	X	
Dns kaydı		X			X	X
Kullanılan servisler	X		X	X	X	X
Sertifika bilgisi	X		X	X	X	X
Metadata	X		X	X	X	

Tespit edilen platformlar haricinde veri sızıntılarından da kişiler (gerçek veya tüzel) ve teknolojik altyapılara ait dijital ayak izi ögeleri elde edilebilmektedir. Veri sızıntılarından elde edilebilecek verilerde herhangi bir sınırlama bulunmadığı için tablolaştırma çalışması gerçekleştirilmemiştir.

Kişiler (gerçek veya tüzel) ve teknolojik altyapılara ait dijital ayak izi ögeleri ve elde edilebilecek platformların tespitinin ardından literatürde yer alan siber saldırılar incelenmiştir. İncelemelerde "Cyber Kill Chain" metodolojisinde yer alan "Silahlandırma" ve "Dağıtım" aşamasında bulunan ve "keşif" aşamasında elde edilen dijital ayak izi ögelerinin kullanıldığı siber saldırılar temel alınmıştır.

Belirtilen siber saldırılara yönelik literatür çalışması gerçekleştirilmiş olup, ilgili siber saldırının hangi dijital ayak izlerinin mevcut olduğu durumda gerçekleştirilebildiği veya siber saldırı senaryosunu başlatmak üzere hangi verilere ihtiyaç duyulduğu tespit edilmeye çalışılmıştır.

Tez çalışması boyunca incelenen ve açık kaynak istihbaratı yaklaşımları ile elde edilebilen dijital ayak izi ögeleri ile siber saldırı türlerinin tamamını kapsayan tespitler tablo 5 içerisine eklenmiş olup, çeşitli siber saldırı senaryolarında kullanılan dijital ayak izi ögeleri ile ilişkilendirme sağlanmıştır.

Tablo 5. Dijital Ayak İzi Ögelerinin Kullanılabileceği Siber Saldırılara İlişkin Bağıntı Tablosu.

	Oltalama Saldırıları			Parola Saldırıları			Kimliğe Bürünme Saldırıları	Zafiyetlerden kaynaklı Saldırılar	Yapılandırma kaynaklı saldırılar	Hizmet kesintisi
	Hedef odaklı	Balina	Scareware	Kaba kuvvet	Sözlük	Istifleme				
Kullanıcı adı	X	X	X	X	X		X			
Ad- soyadı	X	X	X	X	X		X			
E-posta adresi	X	X	X	X	X		X			
Telefon numarası	X	X	X	X	X		X			
Doğum tarihi	X	X	X	X	X		X			
Doğum yılı/kuruluş yılı	X	X	X	X	X		X			
Zamir/hitap şekli	X	X	X				X			
Harici website	X	X	X				X			
İkamet yeri	X	X	X	X	X		X			
Memleket/Doğum yeri	X	X	X	X	X		X			
İlişki durumu	X	X	X	X	X		X			
İlişki durumu Tarihi	X	X	X	X	X		X			
Aile/akraba Bilgisi	X	X	X	X	X		X			
Arkadaş bilgisi	X	X	X				X			
Kariyer bilgisi	X	X	X				X			
İş arayış durumu	X	X	X				X			
Personel bilgisi	X	X	X				X			
Eğitim bilgisi	X	X	X				X			
Aldığı eğitim/sertifika	X	X	X				X			
Yetenek/hobiler	X	X	X	X	X		X			
Bildiği lisanslar/diller	X	X	X				X			
Serbest Biyografi alanı	X	X	X	X	X		X			
Diğer sosyal medyalar	X	X	X				X			
Tüzel Kişi hakkında harici veriler	X	X	X				X			

Alan adı	X	X	X				X	X	X	X
Alt alan adı	X	X	X				X	X	X	X
IP adresi	X	X	X				X	X	X	X
Açık port	X	X	X				X	X	X	X
DNS kaydı	X	X	X				X	X	X	X
Kullanılan servisler	X	X	X				X	X	X	X
Sertifika bilgisi	X	X	X				X	X	X	X
Metadata	X	X	X				X	X	X	X
Veri sızıntıları	X	X	X	X	X	X	X	X	X	X

Oluşturulan tablo 4 ve gerçekleştirilen ilişkilendirmeler sonucunda sosyal mühendislik saldırılarından olan oltalama saldırıları ve türevlerinde her türlü dijital ayak izi ögelerinin kullanılabildiği gözlemlenmiştir.

Kullanıcının siber saldırının hedefi olmadığı, doğrudan sistemin kendisini hedef alan siber saldırılarda ise kişilere ait (gerçek veya tüzel) dijital ayak izi ögelerinin kullanılmadığı, yalnızca teknolojik altyapılara ait dijital ayak izi ögelerinin kullanıldığı gözlemlenmiştir.

İlgili tespitler ve gerçekleştirilen korelasyonlar Cyber Kill Chain metodolojisi içerisinde değerlendirildiğinde dijital ayak izi ögelerinin kullanıldığı siber saldırı fazı tespit edilmektedir.

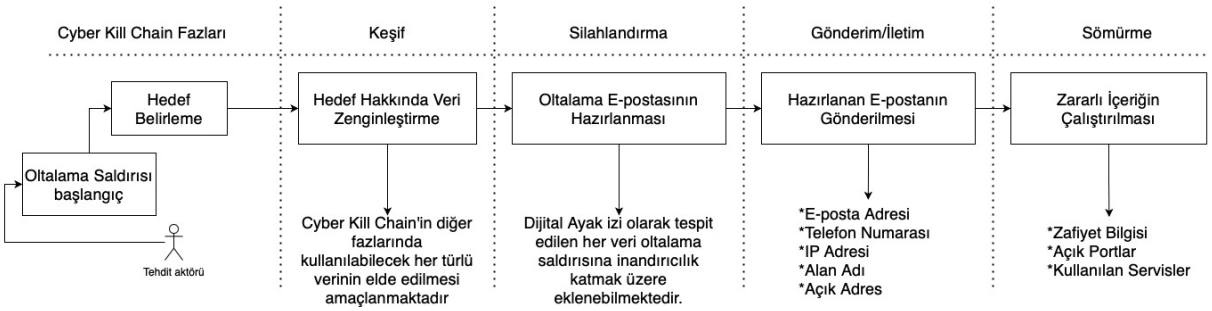
- Keşif (Reconnaissance): Hedefin belirlenmesi veya hedefi belirledikten sonra araştırmaları sürdürmek üzere hedef hakkında temel bilgilere sahip olunması gerekmektedir. Bu veriler doğrultusunda zenginleştirme çalışmaları yapılmaktadır.
    - Ad – soyadı bilgisi (Kimlik bilgisi)
    - Firma ismi
    - Kullanıcı adı
- Silahlandırma (Weaponization): Tehdit aktörü, gerçekleştireceği siber saldırıda hedefe uygun zararlı içerikler geliştirmesi gerekmektedir. Bu zararlı içerikler oltalama içerikleri olabileceği gibi zararlı yazılımlar da olabilmektedir.

- Oltalama e-postalarını zenginleştirecek her dijital ayak izi ögesi.
- Hedefin kullandığı servisler (Ağ tarama araçları, Google Dorking, sertifika bilgisi ve metadata'lardan elde edilebilmektedir.)
- Zafiyet bilgisi

- Gönderim/iletim (Delivery): Silahlandırma aşamasında geliştirilen zararlı içeriklerin iletimi için aşağıda yer alan maddelerden en az bir tanesine ihtiyaç duyulmaktadır
  - E-posta adresi
  - Telefon numarası
  - IP adresi
  - Alan Adı
  - Açık Adres
- Sömürme (Exploitation): Teslim edilen zararlı içeriğin faaliyete geçmesi durumudur. Aşağıda yer alan maddelerden en az bir tanesine ihtiyaç duyulmaktadır.
  - Zafiyet bilgisi
  - Açık port bilgisi
  - Hedefin kullandığı servisler

Cyber Kill Chain yaklaşımı içerisinde yer alan diğer fazlarda dijital ayak izi ögelerinin kullanımına ihtiyaç duyulmadığı için değerlendirmeye dahil edilmemiştir.

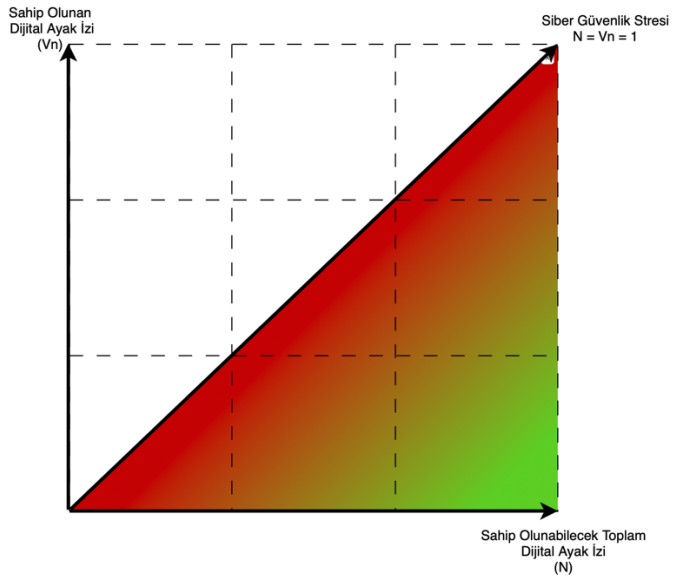
Oltalama Saldırısını Cyber Kill Chain yaklaşımı ile inceleyen bir çalışmayı baz alarak [67], tez kapsamında elde edilen bulgular ile birleştirildiğinde şekil 49 içerisinde yer alan diyagram oluşturulabilmektedir. İlgili diyagramda tehdit aktörünün oltalama saldırısı gerçekleştireceği durumda Cyber Kill Chain fazlarına uygun olarak hangi dijital ayak izi ögelerini kullanabileceğini görselleştirilmeye çalışılmıştır.



Şekil 49. Oltalama Saldırısının Cyber Kill Chain İçindeki Aşamaları ve Dijital Ayak İzi Ögelerinin Kullanımı.

4.3. Bulgulara Ait Risk Analizinin Gerçekleştirilmesi

Siber güvenlik stresi, sahip olunan ve sahip olunabilecek dijital ayak izi ögeleri arasındaki oranı temsil etmektedir. Sahip olunan dijital ayak izi ögelerinin sayısının sahip olunabilecek olan dijital ayak izi ögelerinin sayısına eşit olması durumunda siber güvenlik stresi derecemiz en üst derece olan 1 olmaktadır.



Şekil 50. Siber Güvenlik Stresi Diyagramı.

Herhangi bir sosyal medya platformunda sahip olunabilecek dijital ayak izi ögesi sayısı N olmak üzere, kullanıcının dijital ayak izi ögelerinin tamamına sahip olması durumunda $Vn = N$ olmaktadır, burada siber güvenlik stresi;

$$(5)\quad Vn = N \;\; ve \;\; Str^{s} \in [0,1] \; olmak \; \text{üzere}$$

(6) $Str^s = \frac{Vn}{N} = 1$

Oranı 1 olmaktadır, kullanıcının aynı platformda sahip olduğu dijital ayak izi ögelerinin sayısında azalma olması durumunda stres oranında azalma meydana gelecektir.

Herhangi bir sosyal medya platformunda sahip olunabilecek dijital ayak izi ögelerinin siber güvenlik stresi hesaplandıktan sonra risk değerlendirilmesi yapılmaktadır.

(7) $f(x) = \begin{cases} \mathcal{R} = Str^s.h\,,\ Vn \leq 1 \\ \mathcal{R} = \sum_0^{Vn} \mathcal{R}_{Vn}\,,\ Vn > 1 \end{cases}$ $olmak$ üzere,

Tek bir dijital ayak izi ögesinin bulunması durumunda risk değeri, $\mathcal{R} = Str^s.h$ olmaktadır. Birden fazla dijital ayak izi ögesinin bulunması durumunda;

(8) $\mathcal{R} = (Str_1^s\,.h_1) + (Str_2^s\,.h_2) + \ldots + (Str_n^s\,.h_n)$

Teknolojik altyapılarda bulunabilen zafiyetler gibi net bir kritiklik derecesine sahip olunan (CVSS benzeri) dijital ayak izi ögelerinin risk hesaplanmasında CVSS değeri h parametresine karşılık gelmektedir.

Küresel çapta yaygın olarak kullanılmış ve kullanılmakta olan Fortigate-600c güvenlik duvarının risk değerlendirilmesi yapılmak istendiğinde; NVD üzerinden gerçekleştirilen incelemeler sonucunda ilgili güvenlik duvarında CVE-2013-1414 ve CVE-2012-4948 olmak üzere iki zafiyetin mevcut olduğu gözlemlenmiştir [68].

CVE-2013-1414 zafiyetinin CVSS değeri incelendiğinde 5,1 olarak değerlendirildiği gözlemlenmiştir [69].

CVE-2012-4948 zafiyetinin CVSS değeri incelendiğinde ise 5,3 olarak değerlendirildiği gözlemlenmiştir [70].

Elde edilen veriler doğrultusunda, her iki zafiyetin de bulunduğu Fortigate-600c güvenlik duvarının kullanılması durumunda;

(9) $f(x) = \begin{cases} \mathcal{R} = Str^s.h\,,\ Vn \leq 1 \\ \mathcal{R} = \sum_0^{Vn} \mathcal{R}_{Vn}\,,\ Vn > 1 \end{cases}$ $olmak$ üzere,

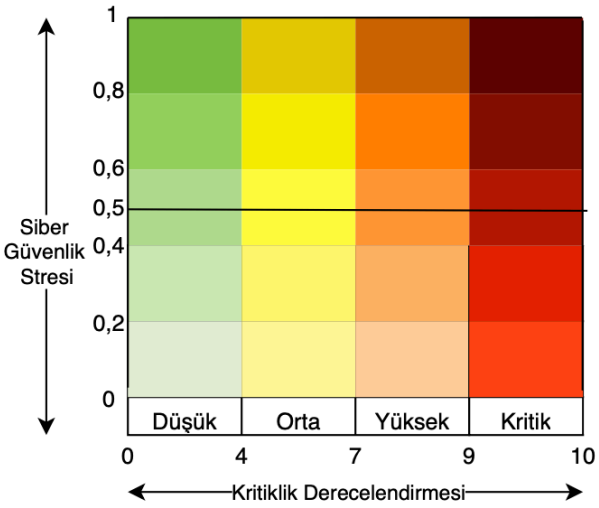
(10) $\mathcal{R} = (Str_1^s\,.h_1) + (Str_2^s\,.h_2)$

$$(11) \quad \mathcal{R} = \left(\frac{1}{2} \,.\, 5{,}1\right) + \left(\frac{1}{2} \,.\, 5{,}3\right)$$

$$(12) \quad \mathcal{R} = 5{,}2$$

Dijital ayak izini barındıran teknolojik altyapıda zafiyet sayısının artması siber güvenlik stresini arttırmakla birlikte zafiyetlerin derecelendirme puanlarının yüksekliği ise riski yükseltmektedir.

Aynı senaryo doğrultusunda mevcut olabilecek zafiyet sayısının yine iki olmasıyla birlikte bu zafiyetlerin yamalanmış olması zafiyetler açısında siber güvenlik stresini sıfıra düşürecektir.



Şekil 51. Zafiyet Derecelendirmesinin Bulunması Durumunda Risk Değerlendirmesi.

Belirtilen teknolojik altyapıda zafiyetin bulunmaması zafiyet özelinde siber güvenlik stresini sıfıra indirmekle birlikte teknolojik altyapı bir bütün olarak incelenip, teknolojik altyapının bütününe yönelik hesaplama gerçekleştirildiğinde siber güvenlik stresi açısından etkisi bulunmaktadır.

5. TARTIŞMA

Siber saldırılardan korunmanın en temel yolu korumamız gereken varlıkların ve internet ortamında bulunan, tehdit aktörleri tarafından kullanılabilecek verilerin farkında olmaktır. Tehdit aktörleri için toplayacakları dijital ayak izi ögeleri yüksek önem arz etmekte olup, dijital ayak izi ögelerinin tespit edilememesi durumunda siber saldırının da gerçekleştirilemeyeceği anlamına gelmektedir [71].

Tehdit aktörlerinin gerçekleştirecekleri siber saldırıların önüne geçmenin en temel yolu Cyber Kill Chain metodolojisinde yer alan keşif aşamasından silahlandırma aşamasına geçememeleri olacaktır. Bunu sağlamanın ise iki temel yolu vardır, bunlardan birincisi atak yüzeyini küçültmek diğeri ise atak yüzeyini aldatma teknolojileri ile genişletmektir.

5.1. Atak Yüzeyini Küçültmek

Tehdit aktörlerinin elde ettikleri dijital ayak izleri ile hedefe yönelik sofistikte siber saldırı gerçekleştirmeleri mümkündür. Tehdit aktörlerinin, dijital ayak izimize yönelik edinilen veriler ve bilgiler ile gerçekleştirilen siber saldırıların karmaşıklığı ve inandırıcılığı doğru orantılıdır. Tehdit aktörlerinin hedef hakkında daha az veriye ve bilgiye sahip olması gerçekleştirilen siber saldırının da sıradan ve tespit edilebilir olmasına neden olacaktır [72].

Tehdit aktörleri tarafından sofistike saldırıların hedefi olmamak ve gerçekleştirilecek olası siber saldırıların daha kolay tespit edilebilmesi için dijital ayak izinin ve atak yüzeyinin küçültülmesi önerilmektedir [72].

Dijital ayak izinin ve atak yüzeyinin küçültülmesi için yapılacak işlemler aşağıda sıralanmıştır.

- Sosyal medya hesaplarında mümkün olan en az verinin paylaşılmış olması.
- Sosyal medya hesaplarında, kullanıcıya ait kişisel veri olarak nitelendirilebilecek, dijital ayak izini oluşturan ve bunları ifşa edecek paylaşımların yapılmaması (Paylaşılan fotoğraflarda aile akraba bilgilerinin yer almaması, sahip olunan evcil hayvanlara yönelik bilgilerin yer almaması, sahip olunan eşyalara yönelik bilgilerin yer almaması,

desteklenen; siyasi parti, spor takımları, vakıf ve derneklere yönelik bilgileri içeren paylaşımların yapılmaması başlıca örnekleri oluşturmaktadır).

- Kişisel sosyal medya hesaplarının kapalı (gizli) olarak kullanılması.
- Kişisel sosyal medya hesaplarında arkadaşların düzenli olarak kontrol edilmesi, yabancı profiller tarafından takip edilmemiz durumunda yabancı profillerin çıkartılması veya engellenmesi.
- Verilerin gizlenebileceği noktalarda (WhoIs kayıtları, sosyal medya profilleri, Metadatalar ve benzeri) verilerin gizlenmesi.
- Oturum açma işlemlerinde farklı ve rastgele oluşturulmuş parolaların kullanılması.
- İnternete açık ortamların veya sistemlerin bulunması durumunda bunların düzenli olarak zafiyet kontrollerinin yapılması ve zafiyetlerin yamalanması.
- Herkese açık paylaşılan dosyalarda dosya bilgilerinin temizlenmesi.

Yukarıda belirtilen ve sıralanmış olarak yer alan yöntemler uygulanarak dijital ayak izi ve atak yüzeyi küçültülerek olası siber saldırıların sofistike olması ve daha inandırıcı olmasının önüne geçilebilmektedir.

5.2. Atak Yüzeyini Aldatma Teknolojileri ile Genişletmek

Tehdit aktörlerinin dijital ayak izlerinden yola çıkarak gerçekleştirdiği siber saldırılardan korunmanın bir diğer yolu ise aldatma yöntemlerini (Deception Framework) kullanmaktır. Burada amaç; "ekmek kırıntıları" (Breadcrumbs) olarak adlandırılan sahte dijital ayak izi ögelerini herkesin erişimine açık şekilde paylaşarak keşif aşamasında tehdit aktörünü yanlış yönlendirmeye çalışmaktadır [73].

Aldatma yöntemlerine örnek olarak;

- İnternete açık ortamlarda ve sistemlerde tehdit aktörünü yanıltacak ve tespit edilebilmesine imkan sağlayan zafiyetli cihazların veya sistemlerin bulunması.
- Kaydolunan web sitelerinde hatalı doğum tarihi kullanmak.

- Sosyal medya platformlarında paylaşımda bulunurken hatalı bilgi paylaşımında bulunmak (yanlış evcil hayvan ismi, sahte ilgi alanları, sahte hobiler, memleket bilgisinin yanlış paylaşılması ve benzeri).

Maddeleri örnek olarak verilebilmektedir. Tehdit aktörünü yanıltacak veriler paylaşarak hem olası siber saldırıların tespiti kolaylaşmaktadır hem de tehdit aktörlerinin başarı oranlarını düşürmektedir [74].

6. SONUÇ VE ÖNERİLER

Teknolojinin hızlı gelişimi ve zaman içerisinde azalan maliyetler teknolojiye ulaşan kişi sayısının artmasına ve teknolojik sistemlerin çeşitliliğine sebep olmuştur. Teknolojide yaşanan bu gelişim ile her kullanıcının ve her teknolojik varlığın bir dijital ayak izi oluşmaya başlamıştır.

Dijital ayak izleri; kişilerin (gerçek veya tüzel) veya teknolojik altyapı varlıklarının internet ortamında arkalarında bıraktığı ve varlığın kendisine ait özellikleri barındıran izler olarak nitelendirilmektedir.

Teknolojide yaşanan bu gelişme kötücül niyet barındıran ve tehdit aktörü olarak anılan siber saldırganların da ortaya çıkmasına sebep olmuştur. Tehdit aktörlerinin gerçekleştirdikleri kötücül faaliyetlerin arkasında temel motivasyon olarak; gelir eldesi, espiyonaj, ego tatmini, itibar kazancı ve zarar vermenin yer aldığı bilinmektedir.

"Cyber Kill Chain" metodolojisine göre tehdit aktörleri siber saldırı gerçekleştirmeden önce bir keşif aşamasından geçmeleri gerekmektedir. Bu aşamada ise hedefe ait dijital ayak izi ögeleri elde edilmeye çalışılmaktadır. Tehdit aktörleri keşif aşamasında elde ettikleri verinin zenginliği veya katma değeri doğrultusunda uygun olan siber saldırı senaryosunu gerçekleştirebilmektedir. Hedef hakkında bilgilere sahip olmayan tehdit aktörlerinin siber saldırıyı gerçekleştiremeyeceğinden ötürü keşif aşaması zorunlu bir aşamadır.

İlgili tez çalışması kapsamında açık kaynak tehdit istihbaratı yaklaşımlarını kullanarak elde edilebilecek dijital ayak izi ögeleri belirlenmiş ve literatürde yer alan siber saldırılardaki kullanımları ile ilişkilendirilmiştir.

Dijital ayak izi ve siber saldırıların ilişkilendirilmesi sonucunda bir tablo oluşturulmuş olup, varlıkların internet ortamında bıraktığı dijital ayak izi ögelerinin hangi siber saldırılarda kullanılabileceğinin tespit edilmesi amaçlanmıştır.

Gerçekleştirilen literatür çalışmasında tehdit aktörünün sahip olduğu veriler ile gerçekleştirilen siber saldırının sofistikeliğinin doğru orantılı olduğu tespit edilmiştir. Daha komplike ve daha

sofistike olan siber saldırıların başarı oranlarının basit ve genel siber saldırılara kıyasla daha başarılı olduğu tespit edilmiştir.

Atak yüzeyimizi küçülterek veya atak yüzeyimizi tehdit aktörlerini yanıltacak şekilde yapılandırarak tehdit aktörlerinin gerçekleştireceği siber saldırılardan korunmak mümkündür. Elinde yeterince veri bulunmayan veya elde ettiği veriler hatalı olan tehdit aktörlerinin gerçekleştireceği siber saldırıların da başarısız olması beklenmektedir.

Bu bilgiler doğrultusunda internet ortamında sahip olduğumuz dijital ayak izi ögelerinin farkında olmamız kritik önem arz etmektedir.

Gerçekleştirilen siber güvenlik stres hesaplaması ve risk analizi ile birlikte dijital ayak izi ögelerinin ne derece tehlike oluşturdukları ve hangi ölçüde siber saldırılarda kullanılabileceği tespit edilmek istenmiştir.

Dijital ayak izi ögelerinin sayısı artması siber güvenlik stresini arttırmakla birlikte, her bir stres faktörünün siber saldırıya maruz kalması durumunda oluşturabileceği zararın hesaplaması risk analizi ile gerçekleştirilmektedir.

KAYNAKLAR

[1] Y. Ahmed, A. T. Asyhari, and M. Arafatur Rahman, 'A Cyber Kill Chain Approach for Detecting Advanced Persistent Threats', *Computers, Materials & Continua*, vol. 67, no. 2, pp. 2497–2513, 2021, doi: 10.32604/cmc.2021.014223.

[2] L. V. Kapustina, 'Digital Footprint Analysis to Develop a Personal Digital Competency-Based Profile', 2021, pp. 591–596. doi: 10.1007/978-3-030-47458-4_68.

[3] J. A. Hall and D. Liu, 'Social media use, social displacement, and well-being', *Curr Opin Psychol*, vol. 46, p. 101339, Aug. 2022, doi: 10.1016/j.copsyc.2022.101339.

[4] A. M. Kaplan and M. Haenlein, 'Users of the world, unite! The challenges and opportunities of Social Media', *Bus Horiz*, vol. 53, no. 1, pp. 59–68, Jan. 2010, doi: 10.1016/j.bushor.2009.09.003.

[5] C. T. Carr and R. A. Hayes, 'Social Media: Defining, Developing, and Divining', *Atl J Commun*, vol. 23, no. 1, pp. 46–65, Jan. 2015, doi: 10.1080/15456870.2015.972282.

[6] D. Perea, E. Bonsón, and M. Bednárová, 'Citizen reactions to municipalities' Instagram communication', *Gov Inf Q*, vol. 38, no. 3, p. 101579, Jul. 2021, doi: 10.1016/j.giq.2021.101579.

[7] W. Tounsi, 'What is Cyber Threat Intelligence and How is it Evolving?', in *Cyber-Vigilance and Digital Trust*, Wiley, 2019, pp. 1–49. doi: 10.1002/9781119618393.ch1.

[8] J. R. G. Evangelista, R. J. Sassi, M. Romero, and D. Napolitano, 'Systematic Literature Review to Investigate the Application of Open Source Intelligence (OSINT) with Artificial Intelligence', *Journal of Applied Security Research*, vol. 16, no. 3, pp. 345–369, Jul. 2021, doi: 10.1080/19361610.2020.1761737.

[9] D. Omand, 'Social Media Intelligence (SOCMINT)', in *The Palgrave Handbook of Security, Risk and Intelligence*, London: Palgrave Macmillan UK, 2017, pp. 355–371. doi: 10.1057/978-1-137-53675-4_20.

[10] A. Teti, 'Social Media Intelligence as a Tool for Conducting Intelligence Activities', 2024, pp. 281–291. doi: 10.1007/978-3-031-48930-3_21.

[11] M. Sailio, O.-M. Latvala, and A. Szanto, 'Cyber Threat Actors for the Factory of the Future', *Applied Sciences*, vol. 10, no. 12, p. 4334, Jun. 2020, doi: 10.3390/app10124334.

[12] K. Schwarz and R. Creutzburg, 'Design of Professional Laboratory Exercises for Effective State-of-the-Art OSINT Investigation Tools - Part 3: Maltego', *Electronic Imaging*, vol. 33, no. 3, pp. 45-1-45–23, Jun. 2021, doi: 10.2352/ISSN.2470-1173.2021.3.MOBMU-045.

[13] P. K. Manadhata and J. M. Wing, ‘An attack surface metric’, *IEEE Transactions on Software Engineering*, vol. 37, no. 3, pp. 371–386, 2011, doi: 10.1109/TSE.2010.60.

[14] K.-L. Thomson, ‘CYBERSECURITY: REDUCING THE ATTACK SURFACE INAUGURAL LECTURE’, 2021.

[15] K. Schwarz and R. Creutzburg, ‘Design of Professional Laboratory Exercises for Effective State-of-the-Art OSINT Investigation Tools - Part 3: Maltego’, *Electronic Imaging*, vol. 33, no. 3, pp. 45-1-45–23, Jun. 2021, doi: 10.2352/ISSN.2470-1173.2021.3.MOBMU-045.

[16] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, ‘Advanced social engineering attacks’, *Journal of Information Security and Applications*, vol. 22, pp. 113–122, Jun. 2015, doi: 10.1016/j.jisa.2014.09.005.

[17] S. Gupta, A. Singhal, and A. Kapoor, ‘A literature survey on social engineering attacks: Phishing attack’, in *2016 International Conference on Computing, Communication and Automation (ICCCA)*, IEEE, Apr. 2016, pp. 537–540. doi: 10.1109/CCAA.2016.7813778.

[18] E. Karaarslan, ‘Siber Güvenlik Felsefesine Giriş (Introduction to Cyber Security Philosophy)’, *SSRN Electronic Journal*, 2022, doi: 10.2139/ssrn.4314352.

[19] S. Zhang, X. Ou, and D. Caragea, ‘Predicting Cyber Risks through National Vulnerability Database’, *Information Security Journal: A Global Perspective*, vol. 24, no. 4–6, pp. 194–206, Dec. 2015, doi: 10.1080/19393555.2015.1111961.

[20] S. Kumar and V. Somani, ‘Social Media Security Risks, Cyber Threats And Risks Prevention And Mitigation Techniques’, vol. 4, 2018, [Online]. Available: www.ijsart.com

[21] J. Breuer, Z. Kmetty, M. Haim, and S. Stier, ‘User-centric approaches for collecting Facebook data in the “post-API age”: experiences from two studies and recommendations for future research’, *Inf Commun Soc*, vol. 26, no. 14, pp. 2649–2668, Oct. 2023, doi: 10.1080/1369118X.2022.2097015.

[22] A. Karami, M. Lundy, F. Webb, and Y. K. Dwivedi, ‘Twitter and Research: A Systematic Literature Review Through Text Mining’, *IEEE Access*, vol. 8, pp. 67698–67717, 2020, doi: 10.1109/ACCESS.2020.2983656.

[23] Dr. D. D. Green and Dr. R. Martinez, ‘In a World of Social Media: A Case Study Analysis of Instagram’, *American Research Journal of Business and Management*, vol. 4, no. 1, Jul. 2018, doi: 10.21694/2379-1047.18012.

[24] J. Davis, H.-G. Wolff, M. L. Forret, and S. E. Sullivan, ‘Networking via LinkedIn: An examination of usage and career benefits’, *J Vocat Behav*, vol. 118, p. 103396, Apr. 2020, doi: 10.1016/j.jvb.2020.103396.

[25] S. A. Smith and B. Watkins, ‘Millennials’ Uses and Gratifications on LinkedIn: Implications for Recruitment and Retention’, *International Journal of Business*

Communication, vol. 60, no. 2, pp. 560–586, Apr. 2023, doi: 10.1177/2329488420973714.

[26] W. Mazurczyk and L. Caviglione, ‘Cyber reconnaissance techniques’, *Commun ACM*, vol. 64, no. 3, pp. 86–95, Mar. 2021, doi: 10.1145/3418293.

[27] Matthew Hickey and Jennifer Arcuri., ‘Open Source Intelligence Gathering’, in *Hands on Hacking*, Wiley, 2020, pp. 55–86. doi: 10.1002/9781119561507.ch4.

[28] V. R. Saraswathi, I. S. Ahmed, S. M. Reddy, S. Akshay, V. M. Reddy, and S. M. Reddy, ‘Automation of Recon Process for Ethical Hackers’, in *2022 International Conference for Advancement in Technology (ICONAT)*, IEEE, Jan. 2022, pp. 1–6. doi: 10.1109/ICONAT53423.2022.9726077.

[29] S. Mulero-Palencia and V. Monzon Baeza, ‘Detection of Vulnerabilities in Smart Buildings Using the Shodan Tool’, *Electronics (Basel)*, vol. 12, no. 23, p. 4815, Nov. 2023, doi: 10.3390/electronics12234815.

[30] T. M. Fernández-Caramés and P. Fraga-Lamas, ‘Teaching and Learning IoT Cybersecurity and Vulnerability Assessment with Shodan through Practical Use Cases’, *Sensors*, vol. 20, no. 11, p. 3048, May 2020, doi: 10.3390/s20113048.

[31] M. Bada and I. Pete, ‘An exploration of the cybercrime ecosystem around Shodan’, in *2020 7th International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*, IEEE, Dec. 2020, pp. 1–8. doi: 10.1109/IOTSMS52051.2020.9340224.

[32] J. Wachs, M. Nitecki, W. Schueller, and A. Polleres, ‘The Geography of Open Source Software: Evidence from GitHub’, *Technol Forecast Soc Change*, vol. 176, p. 121478, Mar. 2022, doi: 10.1016/j.techfore.2022.121478.

[33] S. Liu, I. Foster, S. Savage, G. M. Voelker, and L. K. Saul, ‘Who is .com?’, in *Proceedings of the 2015 Internet Measurement Conference*, New York, NY, USA: ACM, Oct. 2015, pp. 369–380. doi: 10.1145/2815675.2815693.

[34] C. Lu *et al.*, ‘From WHOIS to WHOWAS: A Large-Scale Measurement Study of Domain Registration Privacy under the GDPR’, in *Proceedings 2021 Network and Distributed System Security Symposium*, Reston, VA: Internet Society, 2021. doi: 10.14722/ndss.2021.23134.

[35] V. Troia, *Hunting Cyber Criminals*. Wiley, 2020. doi: 10.1002/9781119541004.

[36] N. Jamal and J. M. Zain, ‘A Review on Nature, Cybercrime and Best Practices of Digital Footprints’, in *2022 International Conference on Cyber Resilience (ICCR)*, IEEE, Oct. 2022, pp. 1–6. doi: 10.1109/ICCR56254.2022.9995834.

[37] K. Thomas *et al.*, ‘Data Breaches, Phishing, or Malware?’, in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, New York, NY, USA: ACM, Oct. 2017, pp. 1421–1434. doi: 10.1145/3133956.3134067.

[38] A. Dubettier, T. Gernot, E. Giguet, and C. Rosenberger, ‘File type identification tools for digital investigations’, *Forensic Science International: Digital Investigation*, vol. 46, p. 301574, Sep. 2023, doi: 10.1016/j.fsidi.2023.301574.

[39] S. Voida, W. K. Edwards, M. W. Newman, R. E. Grinter, and N. Ducheneaut, ‘Share and share alike’, in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, New York, NY, USA: ACM, Apr. 2006, pp. 221–230. doi: 10.1145/1124772.1124806.

[40] Y. Singh, ‘Footprinting Using Nmap Authors Yuvraj Singh’, *Journal of Informatics Electrical and Electronics Engineering (JIEEE)*, vol. 3, no. 2, pp. 1–15, 2022, doi: 10.54060/JIEEE/003.02.004.

[41] A. Chandra and M. J. Snowe, ‘A taxonomy of cybercrime: Theory and design’, *International Journal of Accounting Information Systems*, vol. 38, p. 100467, Sep. 2020, doi: 10.1016/j.accinf.2020.100467.

[42] H. Al-Mohannadi, Q. Mirza, A. Namanya, I. Awan, A. Cullen, and J. Disso, ‘Cyber-Attack Modeling Analysis Techniques: An Overview’, in *2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, IEEE, Aug. 2016, pp. 69–76. doi: 10.1109/W-FiCloud.2016.29.

[43] H. Ahmetoglu and R. Das, ‘A comprehensive review on detection of cyber-attacks: Data sets, methods, challenges, and future research directions’, *Internet of Things*, vol. 20, p. 100615, Nov. 2022, doi: 10.1016/j.iot.2022.100615.

[44] İ. AVCI, ‘Investigation of Cyber-Attack Methods and Measures in Smart Grids’, *Sakarya University Journal of Science*, vol. 25, no. 4, pp. 1049–1060, Aug. 2021, doi: 10.16984/saufenbilder.955914.

[45] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, ‘Phishing Attacks: A Recent Comprehensive Study and a New Anatomy’, *Front Comput Sci*, vol. 3, Mar. 2021, doi: 10.3389/fcomp.2021.563060.

[46] A. Diaz, A. T. Sherman, and A. Joshi, ‘Phishing in an academic community: A study of user susceptibility and behavior’, *Cryptologia*, vol. 44, no. 1, pp. 53–67, Jan. 2020, doi: 10.1080/01611194.2019.1623343.

[47] A. Houssard, F. Pilati, M. Tartari, P. L. Sacco, and R. Gallotti, ‘Monetization in online streaming platforms: an exploration of inequalities in Twitch.tv’, *Sci Rep*, vol. 13, no. 1, p. 1103, Jan. 2023, doi: 10.1038/s41598-022-26727-5.

[48] Y. Al-Hamar, H. Kolivand, M. Tajdini, T. Saba, and V. Ramachandran, ‘Enterprise Credential Spear-phishing attack detection’, *Computers & Electrical Engineering*, vol. 94, p. 107363, Sep. 2021, doi: 10.1016/j.compeleceng.2021.107363.

[49] T. Xu, K. Singh, and P. Rajivan, ‘Personalized persuasion: Quantifying susceptibility to information exploitation in spear-phishing attacks’, *Appl Ergon*, vol. 108, p. 103908, Apr. 2023, doi: 10.1016/j.apergo.2022.103908.

[50] G. Sonowal, ‘Types of Phishing’, in *Phishing and Communication Channels*, Berkeley, CA: Apress, 2022, pp. 25–50. doi: 10.1007/978-1-4842-7744-7_2.

[51] S. Bagui and H. Brock, ‘Machine Learning for Android Scareware Detection’, *Journal of Information Technology Research*, vol. 15, no. 1, pp. 1–15, Mar. 2022, doi: 10.4018/JITR.298326.

[52] Ekta and U. Bansal, ‘A Review on Ransomware Attack’, in *2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC)*, IEEE, May 2021, pp. 221–226. doi: 10.1109/ICSCCC51823.2021.9478148.

[53] U. Bodkhe, J. Chaklasiya, P. Shah, S. Tanwar, and M. Vora, ‘Markov Model for Password Attack Prevention’, 2020, pp. 831–843. doi: 10.1007/978-981-15-3369-3_61.

[54] A. Nosenko, Y. Cheng, and H. Chen, ‘Learning Password Modification Patterns with Recurrent Neural Networks’, 2022, pp. 110–129. doi: 10.1007/978-3-030-97532-6_7.

[55] I. Alkhwaja *et al.*, ‘Password Cracking with Brute Force Algorithm and Dictionary Attack Using Parallel Programming’, *Applied Sciences*, vol. 13, no. 10, p. 5979, May 2023, doi: 10.3390/app13105979.

[56] V. Grover, ‘An Efficient Brute Force Attack Handling Techniques for Server Virtualization’, *SSRN Electronic Journal*, 2020, doi: 10.2139/ssrn.3564447.

[57] S. R. Widianto, M. S. Maulana, E. B. Pratama, Y. Firmansyah, and Nurmalasari, ‘Python gmail dictionary attack using wordlist’, 2023, p. 030033. doi: 10.1063/5.0128464.

[58] M. H. Nguyen Ba, J. Bennett, M. Gallagher, and S. Bhunia, ‘A Case Study of Credential Stuffing Attack: Canva Data Breach’, in *2021 International Conference on Computational Science and Computational Intelligence (CSCI)*, IEEE, Dec. 2021, pp. 735–740. doi: 10.1109/CSCI54926.2021.00187.

[59] H. A. Kholidy, ‘Detecting impersonation attacks in cloud computing environments using a centric user profiling approach’, *Future Generation Computer Systems*, vol. 117, pp. 299–320, Apr. 2021, doi: 10.1016/j.future.2020.12.009.

[60] M. A Gharawi, A. Badawy, D. Elsayed Ramadan, and S. Elsayed, ‘SOCIAL MEDIA IMPERSONATION IN THE VIRTUAL WORLD’, *Al Hikmah International Journal of Islamic Studies and Human Sciences*, vol. 4, no. 1, pp. 57–65, Jan. 2021, doi: 10.46722/hkmh.4.1.21c.

[61] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, ‘A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions’, *Electronics (Basel)*, vol. 12, no. 6, p. 1333, Mar. 2023, doi: 10.3390/electronics12061333.

[62] S. Loureiro, ‘Security misconfigurations and how to prevent them’, *Network Security*, vol. 2021, no. 5, pp. 13–16, May 2021, doi: 10.1016/S1353-4858(21)00053-2.

[63] J. Galeano-Brajones, J. Carmona-Murillo, J. F. Valenzuela-Valdés, and F. Luna-Valero, ‘Detection and Mitigation of DoS and DDoS Attacks in IoT-Based Stateful

SDN: An Experimental Approach', *Sensors*, vol. 20, no. 3, p. 816, Feb. 2020, doi: 10.3390/s20030816.

[64] M. G. Cains, L. Flora, D. Taber, Z. King, and D. S. Henshel, 'Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation', *Risk Analysis*, vol. 42, no. 8, pp. 1643–1669, Aug. 2022, doi: 10.1111/risa.13687.

[65] F. Baiardi, F. Tonelli, A. Bertolini, and M. Montecucco, 'Metrics for Cyber Robustness'.

[66] J. L. Marble, W. F. Lawless, R. Mittu, J. Coyne, M. Abramson, and C. Sibley, 'The Human Factor in Cybersecurity: Robust & Intelligent Defense', 2015, pp. 173–206. doi: 10.1007/978-3-319-14039-1_9.

[67] F. Ali Garba, 'THE ANATOMY OF A CYBER ATTACK: DISSECTING THE CYBER KILL CHAIN (CKC)'.

[68] 'https://nvd.nist.gov/vuln/detail/'.

[69] 'https://nvd.nist.gov/vuln/detail/CVE-2013-1414'.

[70] 'https://nvd.nist.gov/vuln/detail/CVE-2012-4948'.

[71] M. M. Yamin, M. Ullah, H. Ullah, B. Katt, M. Hijji, and K. Muhammad, 'Mapping Tools for Open Source Intelligence with Cyber Kill Chain for Adversarial Aware Security', *Mathematics*, vol. 10, no. 12, p. 2054, Jun. 2022, doi: 10.3390/math10122054.

[72] F. Comunello, F. Martire, and L. Sabetta, 'Brushing Society Against the Grain: Digital Footprints, Scraps, Non-Human Acts, Crumbs, and Other Traces', *American Behavioral Scientist*, vol. 68, no. 5, pp. 623–639, May 2024, doi: 10.1177/00027642221144844.

[73] M. M. Islam and E. Al-Shaer, 'Active Deception Framework: An Extensible Development Environment for Adaptive Cyber Deception', in *2020 IEEE Secure Development (SecDev)*, IEEE, Sep. 2020, pp. 41–48. doi: 10.1109/SecDev45635.2020.00023.

[74] L. Zhang and Vrizlynn. L. L. Thing, 'Three decades of deception techniques in active cyber defense - Retrospect and outlook', *Comput Secur*, vol. 106, p. 102288, Jul. 2021, doi: 10.1016/j.cose.2021.102288.

İNTİHAL RAPORU İLK SAYFASI

Alper KENDİRLİ

ORİJİNALLİK RAPORU

%7	%6	%4	%5
BENZERLİK ENDEKSİ	İNTERNET KAYNAKLARI	YAYINLAR	ÖĞRENCİ ÖDEVLERİ

BİRİNCİL KAYNAKLAR

1	Submitted to The Scientific & Technological Research Council of Turkey (TUBITAK) Öğrenci Ödevi	%2
2	www.acarindex.com İnternet Kaynağı	%1
3	acikbilim.yok.gov.tr İnternet Kaynağı	%1
4	silo.tips İnternet Kaynağı	%1
5	edebiyat.medeniyet.edu.tr İnternet Kaynağı	<%1
6	doczz.biz.tr İnternet Kaynağı	<%1
7	Ceylan, Beril. "ogrenme Nesnelerinin ogretmen Adaylarinin Teknolojik Pedagojik Icerik Bilgisi Becerilerine Etkisinin Degerlendirilmesi", Anadolu University (Turkey), 2021 Yayın	<%1

KURUM İZNİ YAZILARI

Uyarı: Canlı ve cansız deneklerle yapılan tüm çalışmalar için kurum izin belgelerinin eklenmesi zorunludur. Gizlilik ve mahremiyet içeren durumlarda kurum adı kapatılmalıdır.

☐ **Kurum izni gerekmektedir.**

☒ **Kurum izni gerekmemektedir.**

Alper KENDİRLİ