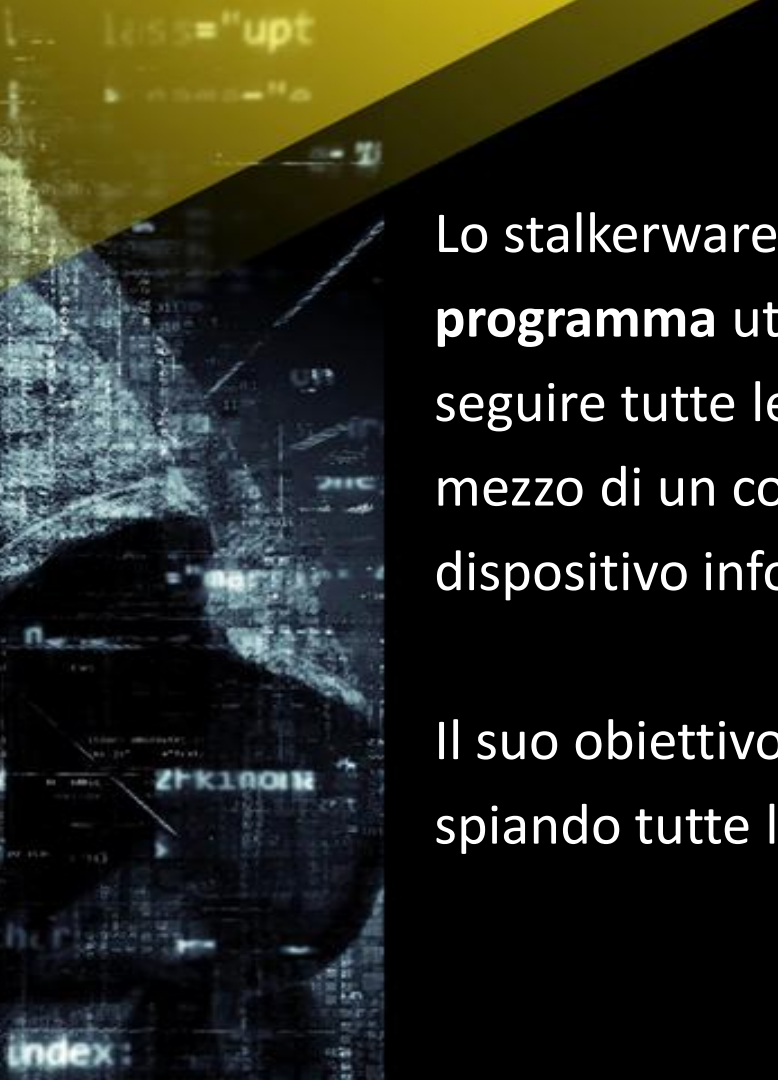
Presentazione di Interceptor

UN PO' DI STORIA:

Benvenuti nel paese in cui **due persone su quattro ritengono normale spiare il proprio partner senza il suo consenso.**

Consideriamo che, normalmente, l'**installazione di un software spia** avverrà su uno smartphone, un tablet o un computer perché attraverso questi dispositivi transita gran parte del nostro patrimonio di informazioni.



UN PO' DI STORIA:

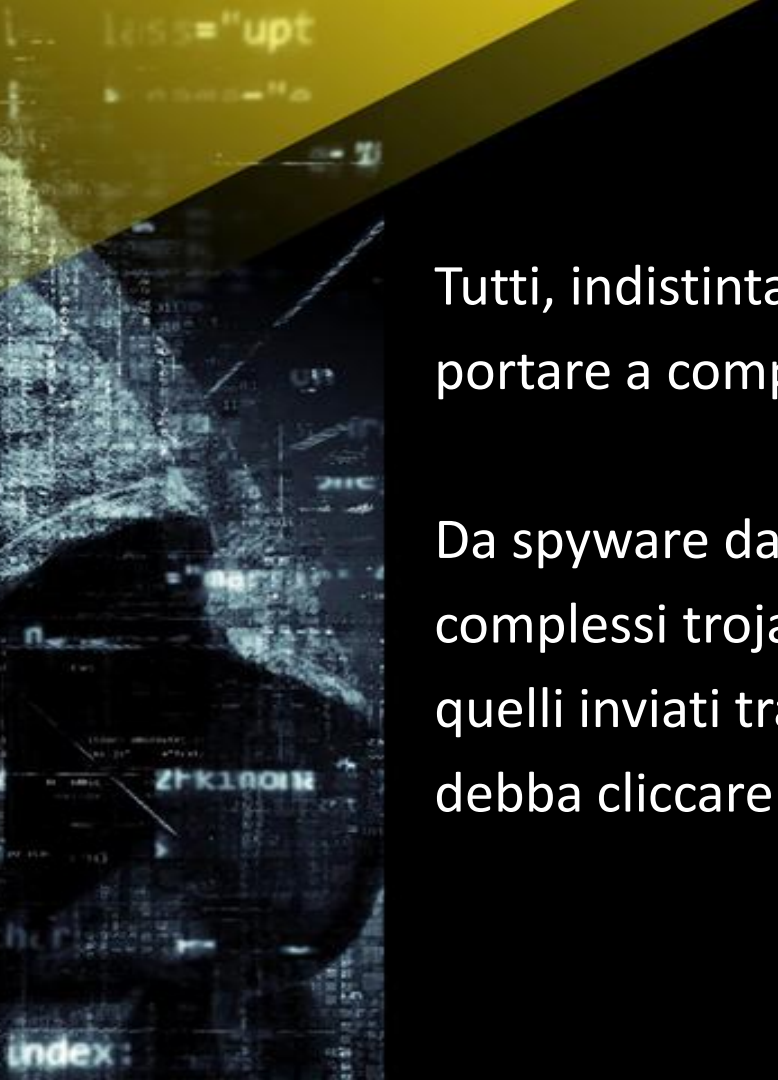
Lo stalkerware o **software spia o spyware è un programma** utilizzato per restare in ascolto, ovvero per seguire tutte le attività che vengono svolte da un'utente per mezzo di un computer, tablet, smartphone o qualsiasi altro dispositivo informatico.

Il suo obiettivo è quello di **violare la privacy** dell'utente, spiando tutte le azioni che quest'ultimo compie.

UN PO' DI STORIA:

Le vittime di questa violazione illecita della privacy sono:

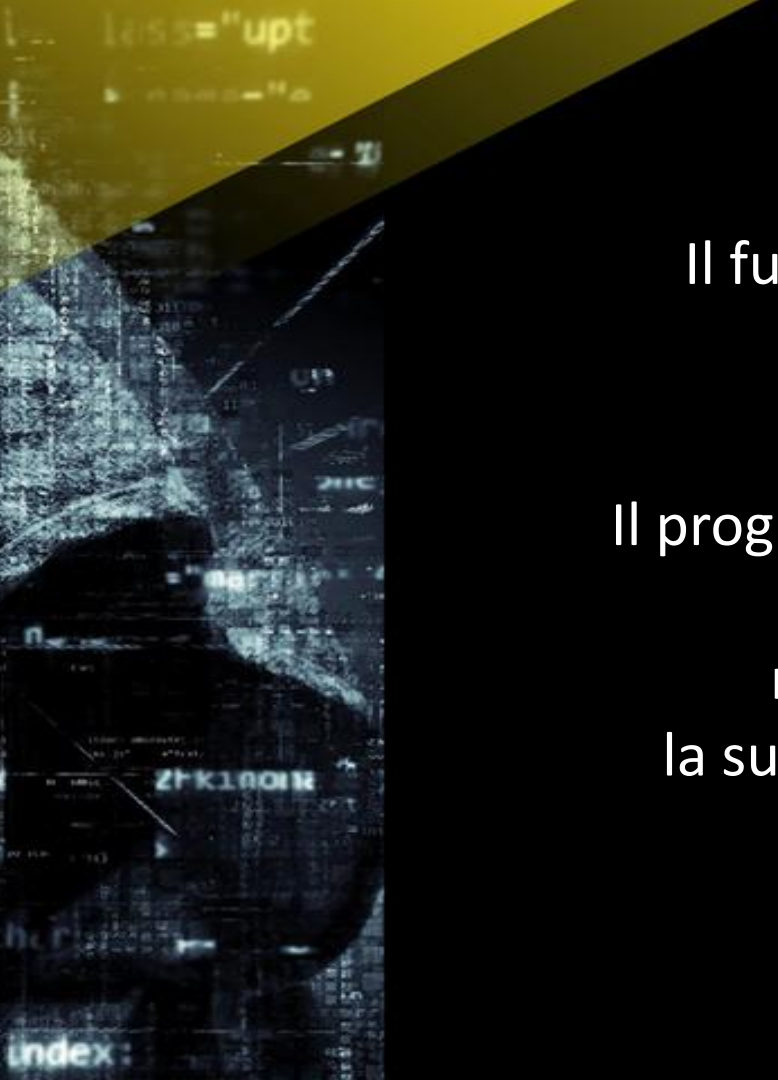
- mariti/mogli/compagni/compagne per sospetti tradimenti;
- mariti/mogli/compagni/compagne per stalking;
- professionisti/dirigenti/personalità/politici per spionaggio industriale.



FUNZIONAMENTO:

Tutti, indistintamente, utilizzano questo tipo di software per portare a compimento i loro obiettivi.

Da spyware da poche decine di euro all’anno fino a complessi trojan installati tramite exploit "zero clic", come quelli inviati tramite messaggi di testo senza che l’utente debba cliccare su qualcosa.



FUNZIONAMENTO:

Il funzionamento di **uno** stalkerware
è quasi elementare.

Il programma risiede nel dispositivo senza
dare segnali della sua attività:
non ci sono icone che segnalano
la sua presenza. Operano in background.

FUNZIONAMENTO:

Attraverso l'impiego di questo programma, l'attaccante riesce facilmente a:

- risalire alla posizione dell'utente tramite GPS;
- intercettare le comunicazioni telefoniche e testuali del dispositivo;
- monitorare tutto quello che viene digitato sulla tastiera del dispositivo: credenziali, password, codici;
- monitorare le notifiche e le attività dei social;
- visualizzare foto e video;
- accedere alla fotocamera o webcam ecc…

DIFFUSIONE:

Ma quanto è diffuso nel mondo il fenomeno degli spyware?


IMPRESSIONANTE VERO?
Pensate che l'Italia è al
2° posto per intrusioni di spyware
secondclonethetruthspy
exactspy fonetracker Trackplus
guestspy thespyapp innoaspy phonespying
TheWiSpy Traecar TrackMyPhonesTrackji
spytomobile Tracku Unisafe VIPTrack WebWatcher
WiseMo WtSpy XDSpy Xnore XploitSPY ZoeMob
bark iKeyMonitor iMonitorSpy jjspy jupi mSpytaly
etale uMobix spyfer surveillance enfants xHunter alltracker.org
.com calltruth.com
e.wondershare.jp h
nitor.com letmespy
ealth.com mspy.cor
ol-a.thetruthspy.co
onitoring.com spyfone.com spymasterpro.com
spy.com xnspy.com a.thd.cc cerberusapp.com
.com mspyonline.com hetruthspy.com
y.com i.minspy.com i.spvic.com i.spvier.com
.co sp.kuuvv.com a
keylogger.com apisp
net catwatchful.co
roidspy.com guest
ree.com i.neatspy.c
mobi netspy.net p
TheOneSpyTheTr
mobilespyfree
AndroidSpy
xoxospy
Accountable2y
childsafetytrackerapp BosSpy
spappmonitoring Cerberus
KidsControl EasyPhoneTrack Bulgok
KidsLox foxspy CallSMSTracker ultima
EspiaoAndroid android-monit
AbsoluTrack
ash ClevGuard
pyier.biz
spyic
cellphonetrackers
inspy
ISpy spyios8x FindMyPhone Curiosus smstra
highstermobile HelloSpy FamiShield CatWatchful
surepointspy spyhide GeoZilla FamiSafe Cocospy
tracerspy GPSTrackerLoki best-mobile-spy
Metasploit forever
MobileSpy MobileTool MobileTrackerFree MocoSpy MonitorUltra
MyCellSpy MzanziSpy NemoSpy NeoSpy NetSpy NexSpy Observer
OneLocator OneMonitar onespy OwnSpy mobileinnova webdetetive
veilstar PatanSpyApp PhoneMonitor PhoneSheriff retinax Apollo
Qustodio RastreadorDeNamorado RealtimeSpy spytech Spy24
Reptilicus Proteus SecretCamRecorder SentryPC SpyApp
ShadySpy SmartKeylogger awamisolution Snoopza
SpyAdvice SpyApp247 SpyAppGhazi SpyDroid
SpyKontr
SpyLive360
SpyMasterPro
SpyMug SpyNote
SpyPhoneApp SpySM
SpyTec SpyToApp Spyier
Spylix Spymie Spyzier SwiftM

DIFFUSIONE:

Pensate che le tecnologie di tracciamento sono state installate più di 500 milioni di volte

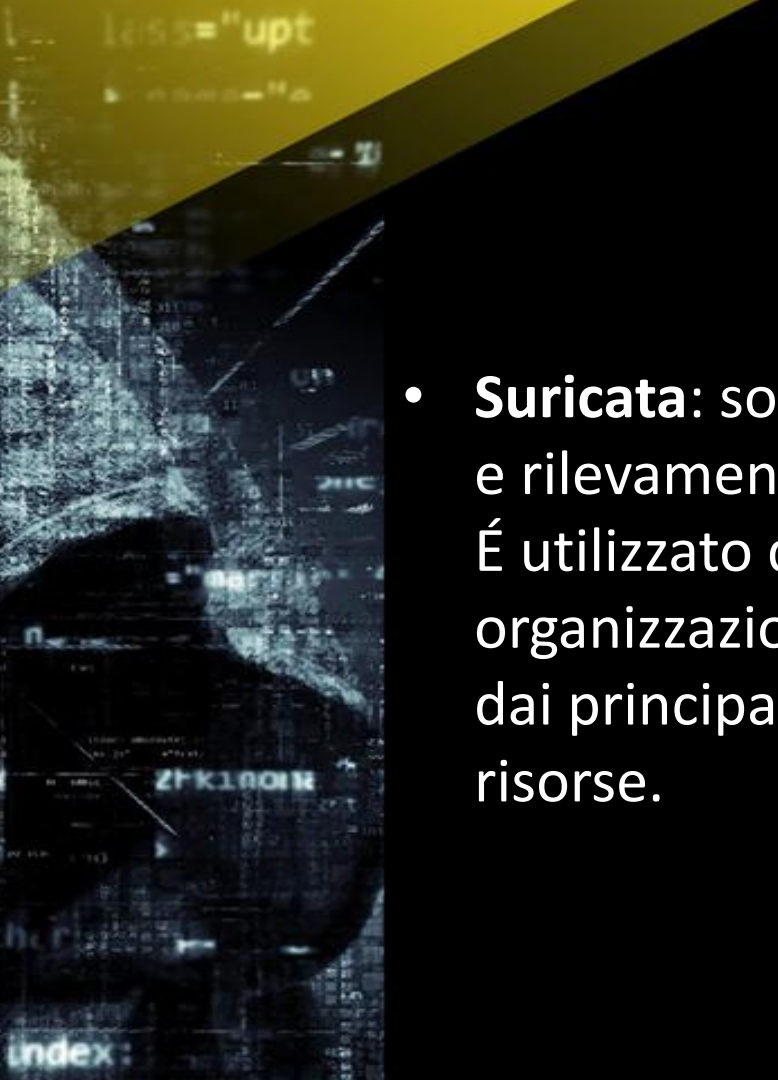
Inter cept r

INTERCEPTOR:

La nostra sfida è stata quella di scrivere un software che rilevasse qualsiasi tipo di intrusione anche operando da remoto.

INTERCEPTOR:

Interceptor attinge dal proprio database proprietario e anche da quelli disponibili in rete. Si avvale anche di sistemi IDS, ovvero Intrusion Detection System quali:



- **Suricata**: software open source di analisi di rete e rilevamento delle minacce ad alte prestazioni. É utilizzato dalla maggior parte delle organizzazioni, pubbliche e private, ed integrato dai principali fornitori per proteggere le proprie risorse.

zeek®

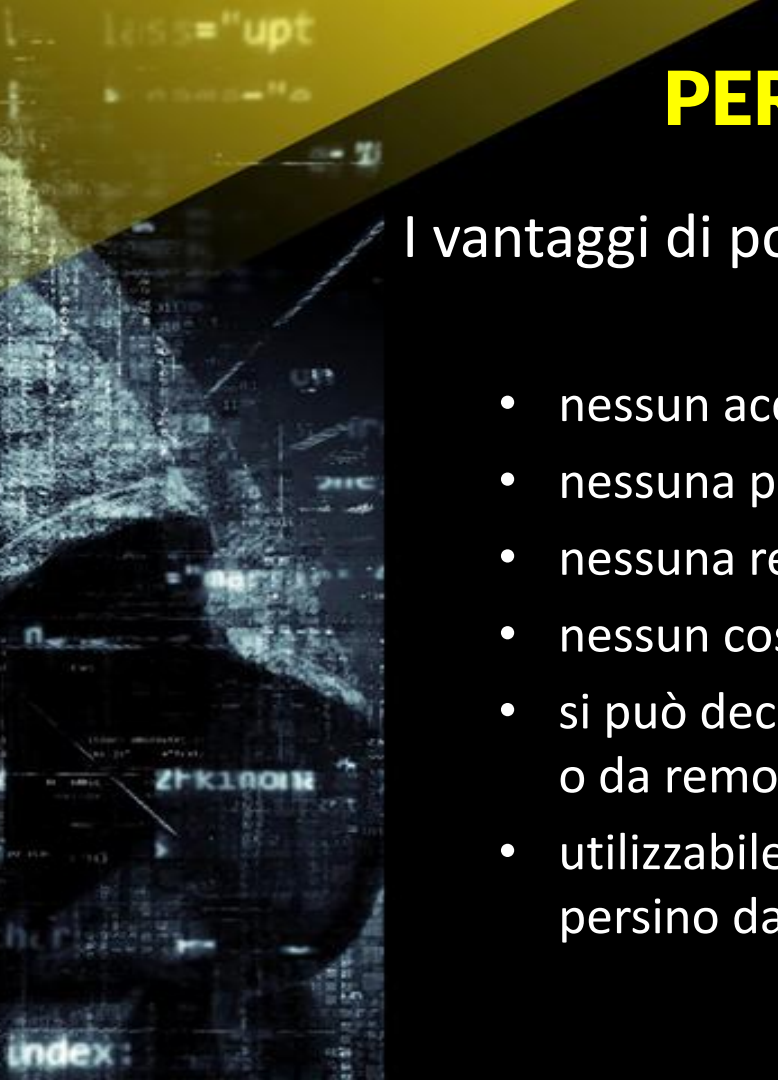
- Zeek: è un "sensore“ in cloud che osserva in modo silenzioso e discreto il traffico di rete.

Inter cept r

INTERCEPTOR:

Così é nato Interceptor,

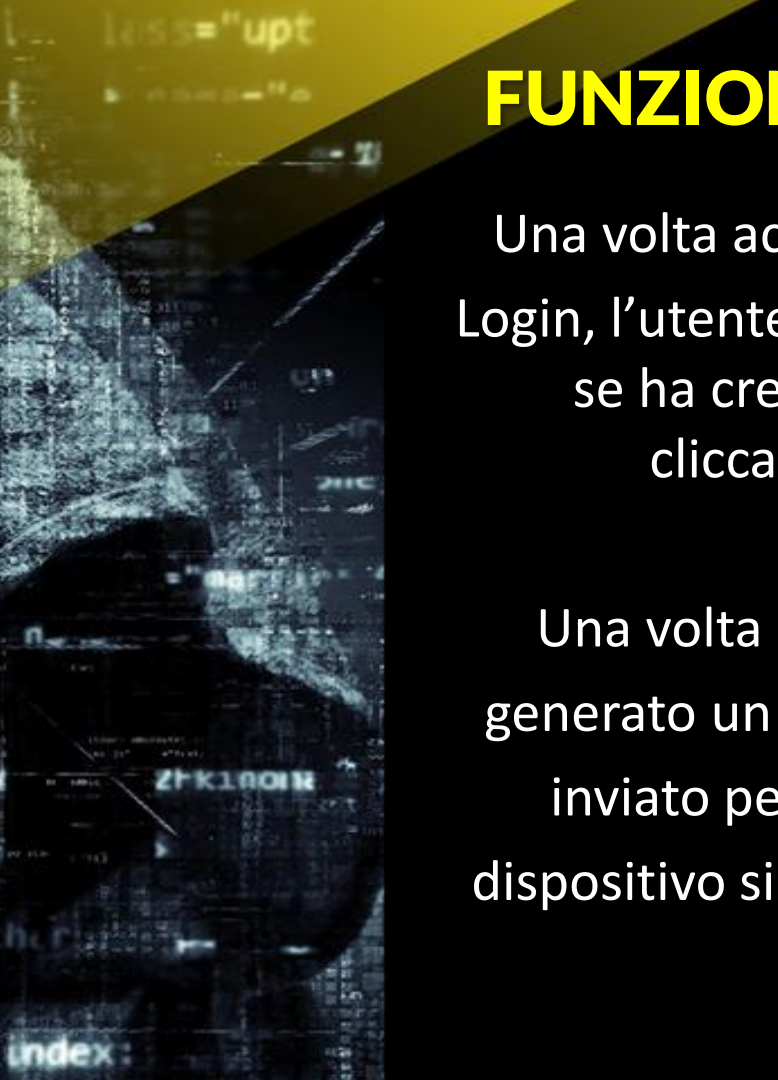
sul quale abbiamo costruito una piattaforma dove gestire gli utenti, le aziende e i gettoni prepagati.



PERCHE' INTERCEPTOR:

I vantaggi di poter operare da remoto:

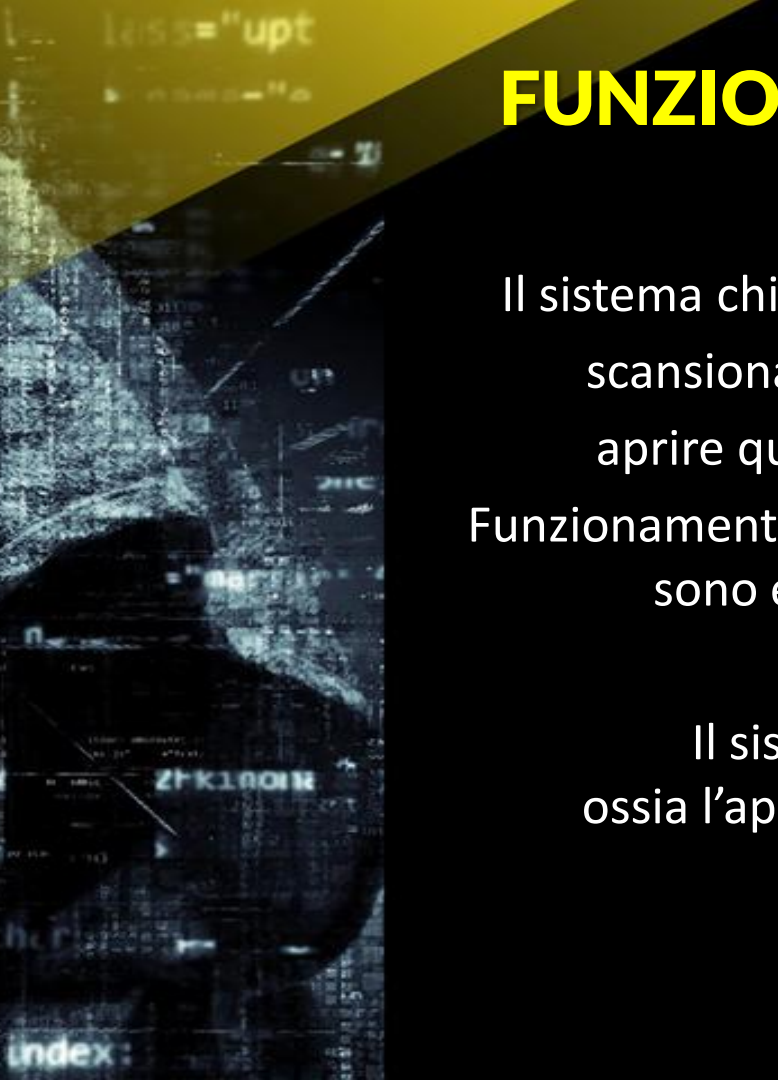
- nessun acquisto di hardware per essere operativi;
- nessuna possibilità di guasto, furto o danneggiamento;
- nessuna resilienza dell'hardware;
- nessun costoso aggiornamento periodico da fare;
- si può decidere di intervenire direttamente presso cliente o da remoto;
- utilizzabile da computer, notebook, tablet, persino da smartphone.



FUNZIONAMENTO INTERCEPTOR:

Una volta acceduto alla propria area privata tramite Login, l’utente può controllare lo storico delle analisi e, se ha crediti disponibili, può avviare altre analisi cliccando sul pulsante “nuova scansione”.

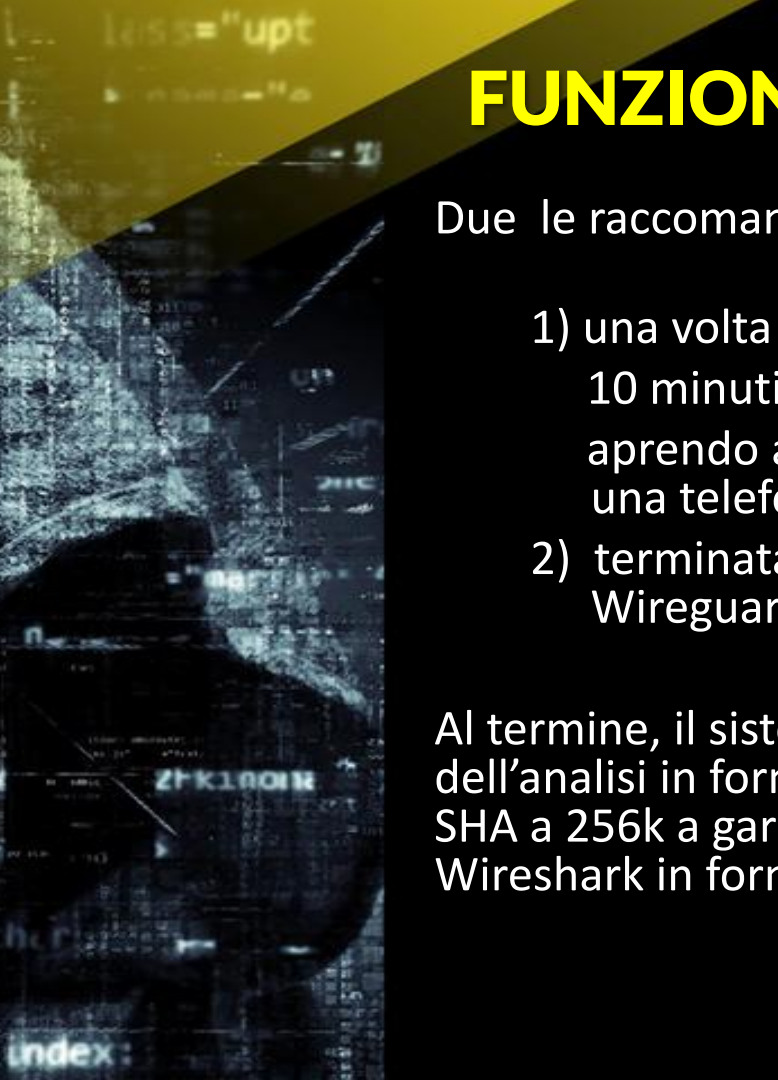
Una volta inserito il nome della scansione, verrà generato un QRcode, che dovrà essere fotografato o inviato per email al cliente, in base al fatto se il dispositivo sia nella vostra disponibilità fisica o meno.



FUNZIONAMENTO INTERCEPTOR:

Il sistema chiederà che tipo di dispositivo l'utente voglia scansionare (pc, smartphone, iPhone, ecc…) per aprire quindi, automaticamente, le istruzioni di Funzionamento ad esso relative. Le operazioni da eseguire sono estremamente semplici e ben descritte.

Il sistema si basa sulla app **Wireguard**,
ossia l'app gratuita di VPN più conosciuta al mondo.

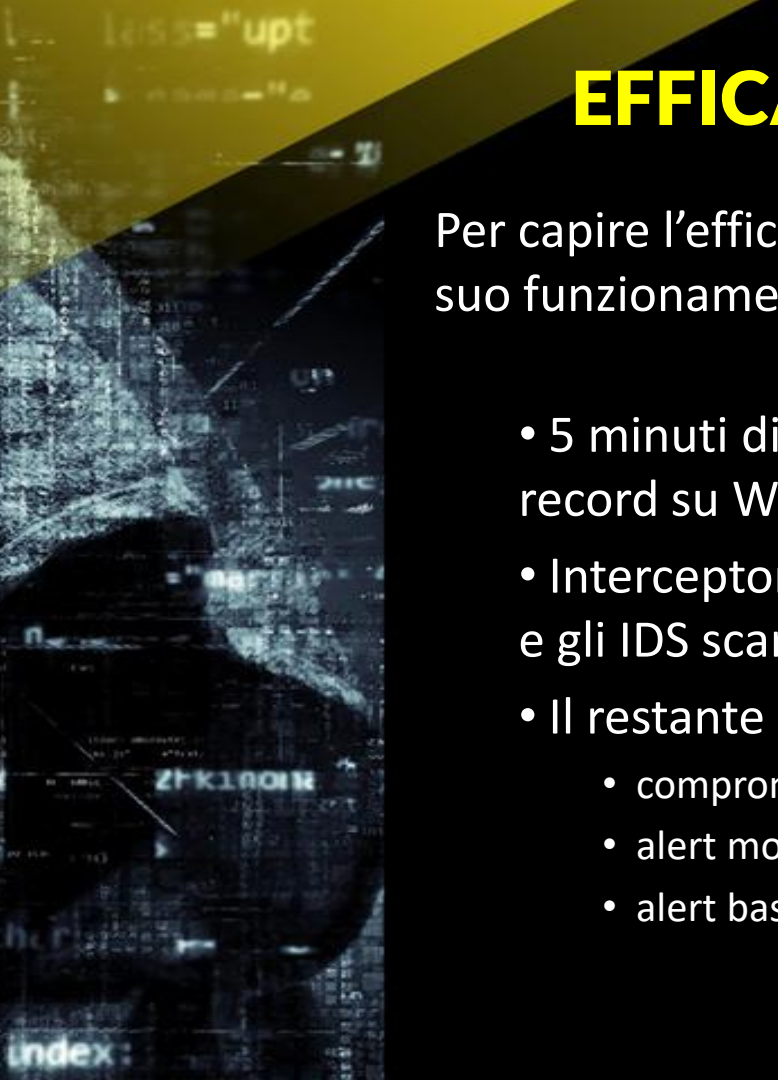


FUNZIONAMENTO INTERCEPTOR:

Due le raccomandazioni da fare al cliente:

1) una volta avviata l'analisi, deve "stressare" il telefono per 10 minuti inviando messaggi, chattando, navigando, aprendo app, inviando email e, per ultimo, effettuando una telefonata;
2) terminata l 'analisi, potrà eliminare il tunnel creato con Wireguard o disinstallare direttamente l'app.

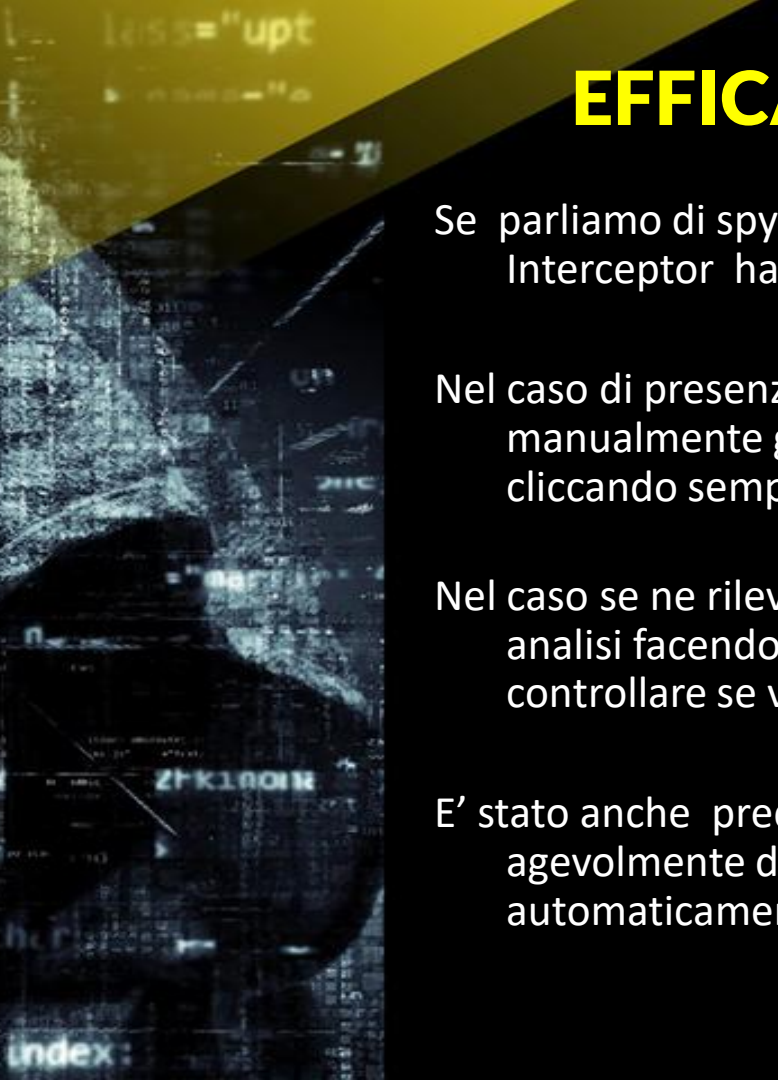
Al termine, il sistema consegnerà in area privata, il resoconto dell'analisi in formato PDF, un archivio ZIP contenente l'impronta SHA a 256k a garanzia forense, il report e il tracciato Wireshark in formato PCAP.



EFFICACIA DI INTERCEPTOR:

Per capire l'efficacia di Interceptor bisogna comprenderne il suo funzionamento:

- 5 minuti di uso di uno smartphone generano migliaia di record su Wireshark, con altrettante migliaia di DNS;
- Interceptor li valuta ad uno ad uno con l'analisi eurisitica e gli IDS scartandone il 99,5% perché ininfluenti;
- Il restante 0,5% verrà suddiviso in:
  - compromissione accertata: nulla da aggiungere;
  - alert moderati: si consiglia di procedere a verifica;
  - alert bassi: nessun problema.



EFFICACIA DI INTERCEPTOR:

Se parliamo di spyware, localizzatori, keylogger e trojan commerciali, Interceptor ha un efficacia assoluta.

Nel caso di presenza di “Troian di stato”, si consiglia di controllare manualmente gli avvisi moderati segnalati dal report di Interceptor cliccando semplicemente sopra l’indirizzo e verificandone la fonte.

Nel caso se ne rilevi uno sospetto è consigliabile ripetere l’operazione di analisi facendo effettuare al dispositivo soltanto una telefonata per controllare se vi sia ancora la presenza del DNS sospetto.

E’ stato anche predisposto un editor nella piattaforma per effettuare agevolmente delle ulteriori valutazioni che verranno automaticamente aggiunte al report.

PREZZI DI INTERCEPTOR:

Il meccanismo si basa su crediti prepagati

1 CREDITO = 1 ANALISI DI UN DISPOSITIVO

Ovviamente sono previste anche piattaforme
White Label e accordi distributivi in specifici settori.

GRAZIE A TUTTI PER L'ATTENZIONE!

info@interceptor.info