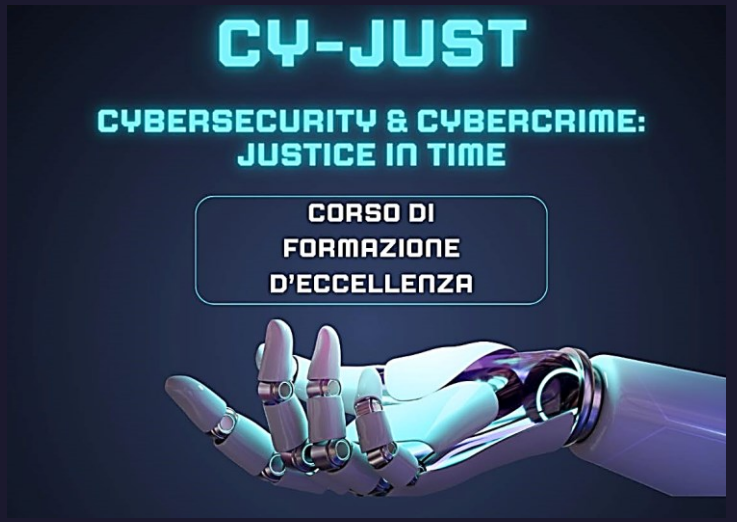
I Cybercrimes e le sue Vittime

analisi dei fenomeni in ascesa



Salerno, 26 ottobre 2024

Agenda

Introduzione

Caso I: Cybercrime in ambito relazionale e a sfondo sessuale

Caso II: Cybercrime in ambito economico e finanziario

Il Dark Web e l’Intelligenza Artificiale Generativa

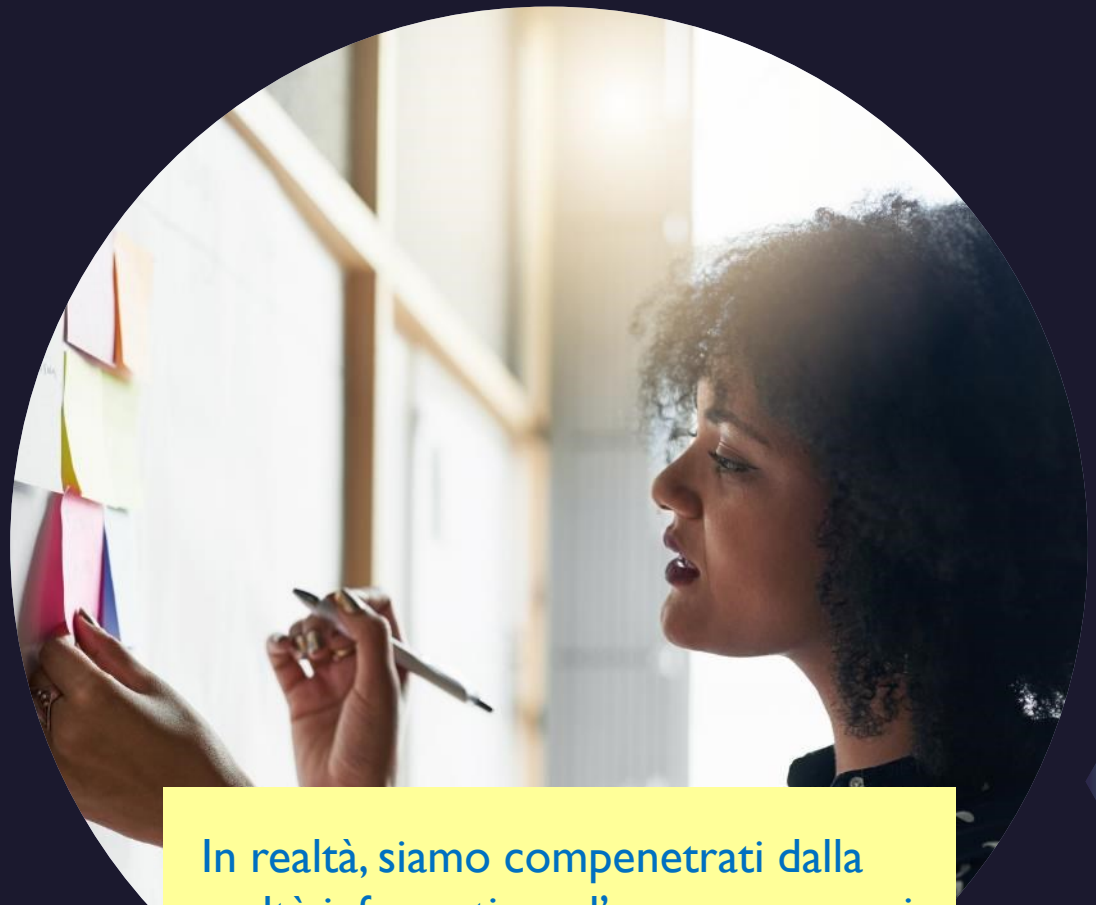
Viviamo nell'era digitale

La maggior parte degli individui vive immerso in un mondo digitale, un mondo in cui i confini tra la vita online e quella offline si dissolvono all'ombra della iper-connettività.

cit. Luciano Floridi

Cybercrime

Reato nel quale la condotta o l'oggetto materiale del crimine sono correlati a un sistema informatico o telematico, ovvero perpetrato utilizzando un tale sistema (computer as a tool) o colpendolo (computer as a target)



In realtà, siamo compenetrati dalla realtà informatica e l'essere connessi è diventato parte integrante della nostra quotidianità, tanto che si parla di vite condotte ***onlife***, per cui è difficile distinguere i reati classici da quelli del modo cyber.

Caso I
Diffusione illecita di immagini o video sessualmente espliciti

Cybercrime in ambito relazionale a sfondo sessuale

Diffusione illecita di immagini o video sessualmente espliciti (c.p. 612 ter)

REVENGE PORN
condivisione per finalità di vendetta

SEXTORTION
condivisione per finalità estorsiva

SEXTING SECONDARIO ovvero IMAGE-BASED SEXUAL ABUSE
condivisione non consensuale di materiale intimo

PORNOGRAFIA MINORILE
condivisione di materiale pornografico di minori – c.p. 600 ter

PORNOGRAFIA VIRTUALE
materiale pornografico virtuale utilizzando immagini di minori - c.p. 600 quater 1

La casistica è articolata e in continua evoluzione, soprattutto tra gli **adolescenti**, per i seguenti motivi:

- Anonimato delle Rete
- Mancanza di consapevolezza
- Utilizzo di false identità digitali
- Manipolazione delle evidenze
- Creazione di artefatti digitali (A.I.)
- Furto o sottrazione di dati
- Uso di app o siti «*insicuri*»
- Sexting «*fraudolento*»
- Condivisione di terze parti volontaria o involontaria
- Condivisione sul Dark Web

Spesso questi reati sono perpetrati in associazione ad altri: **atti persecutori** (stalking o cyberbullismo), **molestie**, lesioni, omicidio preterintenzionale, istigazione al suicidio, estorsione, diffamazione, detenzione materiale pornografico

Attività investigativa

Acquisire l'intera catena di distribuzione,
sia **dispositivi fisici** che **profili virtuali**,
in **tempi brevi** e nei **limiti consentiti dalle legge**

Analizzare il materiale acquisito, in particolare:

- **tutti profili virtuali** (OSINT)
- **le ricerche sul web e sui social network**
- **le app installate** (social network, dating, gaming, app di messaggistica, app di incontri, browser tor, software di vpn, editing image e video, ecc.)

È possibile segnalare ai database di ***«NCII»***
le immagini o i video diffusi senza il consenso
per interrompere la catena di distribuzione

Caso II
Truffa del Trading Online

Cybercrime in ambito economico e finanziario

Fasi della Truffa del Trading online

Raccolta delle informazioni

- Selezione ed Etichettatura dei potenziali target
- Estrazione delle informazioni personali
- Profilazione dei target acquisiti (investitore, manager, imprenditore, risparmiatore, ecc.)

Primo contatto con il target

- Adescamento del target sui social network oppure telefonicamente
- Creazione di una relazione empatica (condivisione degli stessi problemi oppure elargizione di consigli)
- Raccolta di informazioni confidenziali

Ottenimento della fiducia

- Primo contatto con il broker inglese
- Esibizione di documenti a riprova della serietà e affidabilità
- Proposta di un piccolo investimento
- Restituzione dell'utile maturato

Gestione del conto trading

- Apertura di un conto virtuale
- Installazione di un app di trading (in realtà è un RAT o keylogger)
- Acquisto di criptomonete o effettuazione di bonifici verso conti offshore per alimentare il conto virtuale
- Assistenza telefonica per gli investimenti e le acquisizioni

Chiusura canale e conto trading

- Cliente decide di prelevare la somma guadagnata
- Richiesta di ulteriori pagamenti per tasse e provvigioni
- Inibizione dell'accesso al portale e al conto
- Chiusura canale comunicazione

Peculiarità e Attività investigativa

- ✓ Anonimato della Rete
- ✓ Utilizzo di piattaforme non convenzionali «*insicure*»
- ✓ Il contatto inizia dall'attaccante
- ✓ Proposta di guadagni straordinari in poco tempo
- ✓ Scadenza a breve termine dell'offerta
- ✓ Insistenza da parte dell'attaccante
- ✓ Bonifici su conti off-shore o acquisto di criptovalute
- ✓ Volatilità/provvisorietà dei contatti e delle transazioni
- ✓ Documentazione palesemente fake
- ✓ Poca trasparenza e riluttanza a dare informazioni

- ✓ Modificare le password degli account (mail e social), e i metodi autorizzativi dei conti correnti personali (controllare anche i sistemi di recupero credenziali)
- ✓ Effettuare una copia/estrazione forense dei:
  - dispositivi utilizzati
  - comunicazioni ricevute e inviate (mail, msg, social)
  - transazioni bancarie e cripto monete
  - operazioni di trading
  - documentazione ricevuta
- ✓ Presentare tempestivamente la denuncia
- ✓ Analizzare tutte le comunicazione pregresse
- ✓ Evitare di interrompere il canale di comunicazione

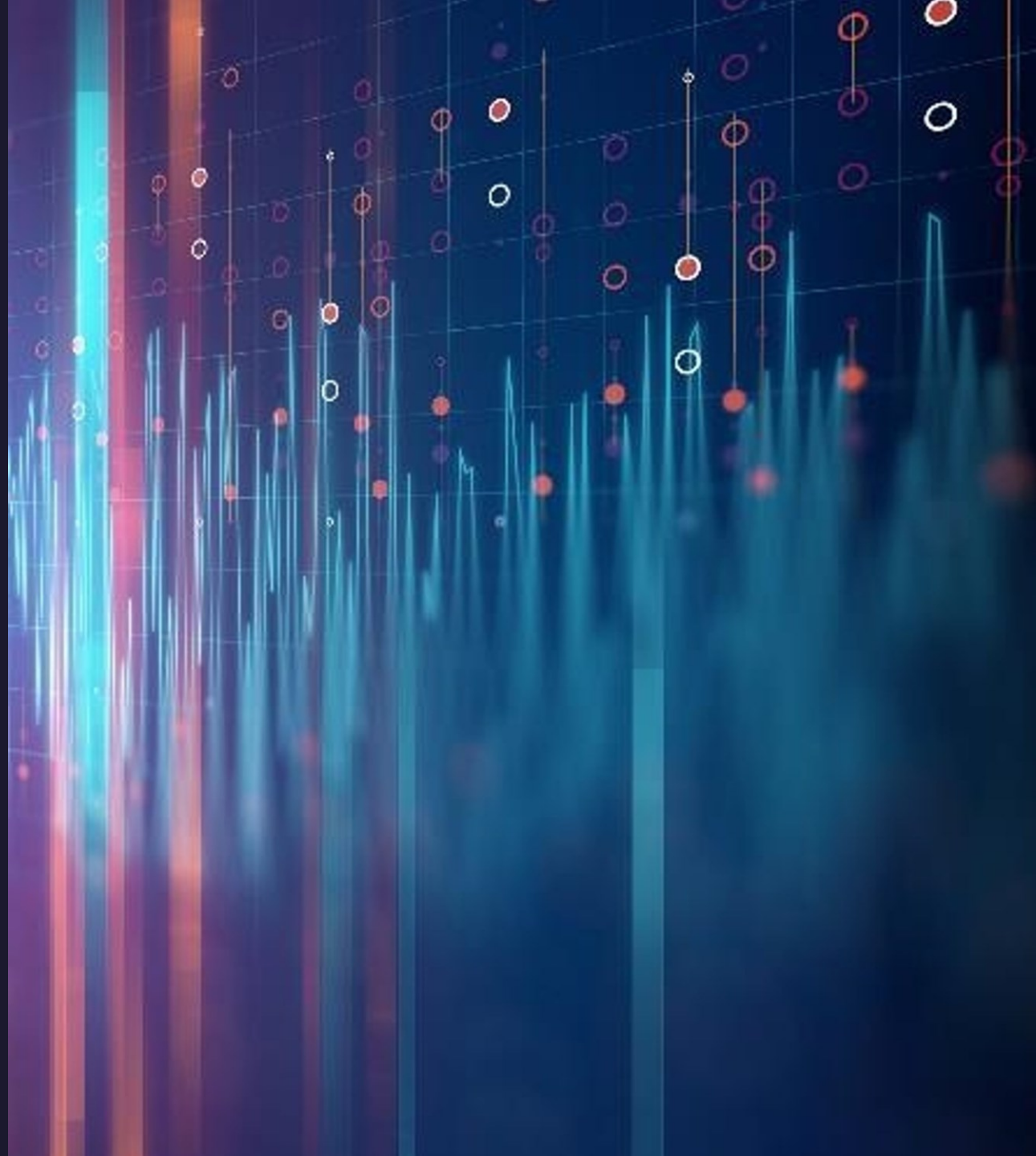
Dark Web

Il dark web si basa sull'uso intensivo dei protocolli crittografici e delle tecniche di anonimizzazione

Pertanto, l'**anonimato** e le **criptovalute** offrono un'ottima schermatura per le operazioni delittuose

Inoltre, sul Dark Web si possono acquisire gli **strumenti** *(software e dati)* oppure i **servizi** *(CaaS - Crime as a service)* per realizzare qualsiasi attività illegale

La criminalità organizzata **investe** nel dark web per finanziare le organizzazioni criminali dedite alla truffe o agli attacchi informatici



Intelligenza Artificale Generativa

L'**Intelligenza Artificiale Generativa** amplifica le capacità cognitive e creative

L'allarmante uso dell'GenAI ha avuto un considerevole impatto sull'entità, sulla velocità e sulla portata dei reati

Nel contesto del cybercrime è paragonabile ad una sorta di **super-potere**

La GenAI è una **risorsa** dual use può essere utilizzata per migliorare il contrasto e le investigazioni digitali

Ambito	Capacità
Social engineering	Raccolta, elaborazione e sintesi delle informazioni
Spamming, Phishing e Spear Phishing	Generazione di artefatti testuali, audio e video
Spoofing e Impersonation	Generazione di artefatti testuali, audio e video
Ransomware, Trojan, Spyware e gli altri tipi di malware	Generazione di software malevolo
Violazione dei codici captcha e delle password	Capacità di risolvere i problemi velocemente
Vulnerability discovery	Elaborazione di tecniche di hacking e cracking
Bot e Automazione	Elaborazione automatizzata delle risposte

Grazie

Vincenzo Calabrò

33 875 19 875

info@vincenzocalabro.it

www.vincenzocalabro.it

vincenzocalabro