I Cybercrimes e le sue Vittime

analisi dei fenomeni in ascesa

Agenda

Introduzione

Caso I: Cybercrime in ambito relazionale e a sfondo sessuale

Caso II: Cybercrime in ambito economico e finanziario

Gen AI: 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.

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)

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

REVENGE PORN
condivisione per finalità di vendetta

SEXTORTION
condivisione per finalità estorsiva

IMAGE-BASED SEXUAL ABUSE
condivisione non consensuale di materiale intimo – c.p. 612-ter

PEDOPORNOGRAFIA
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 le seguenti motivazioni:

- Anonimato delle Rete
- Utilizzo di false identità digitali
- Manipolazione delle evidenze
- Creazione di artefatti digitali
- Uso di app o siti non attendibili
- Sexting «fraudolento»
- Furto di dati
- Condivisione di terze parti volontaria o involontaria
- Condivisione sul Dark Web

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, in particolare:

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

È possibile segnalare le immagini o i video diffusi
senza il consenso nei database NCII
al fine di 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 e Etichettatura del target
- Estrazione di informazioni personali
- Profilazione del target (investitore, manager, imprenditore, 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

Gestione del conto di 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 del conto di 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
- ✓ Il contatto inizia dall'attaccante
- ✓ Proposta di guadagni straordinari
- ✓ Scadenza a breve termine dell'offerta
- ✓ Insistenza da parte dell'attaccante
- ✓ Bonifici su conti off-shore o acquisto di criptovalute
- ✓ Documentazione palesemente fake
- ✓ Poca trasparenza e riluttanza a dare informazioni

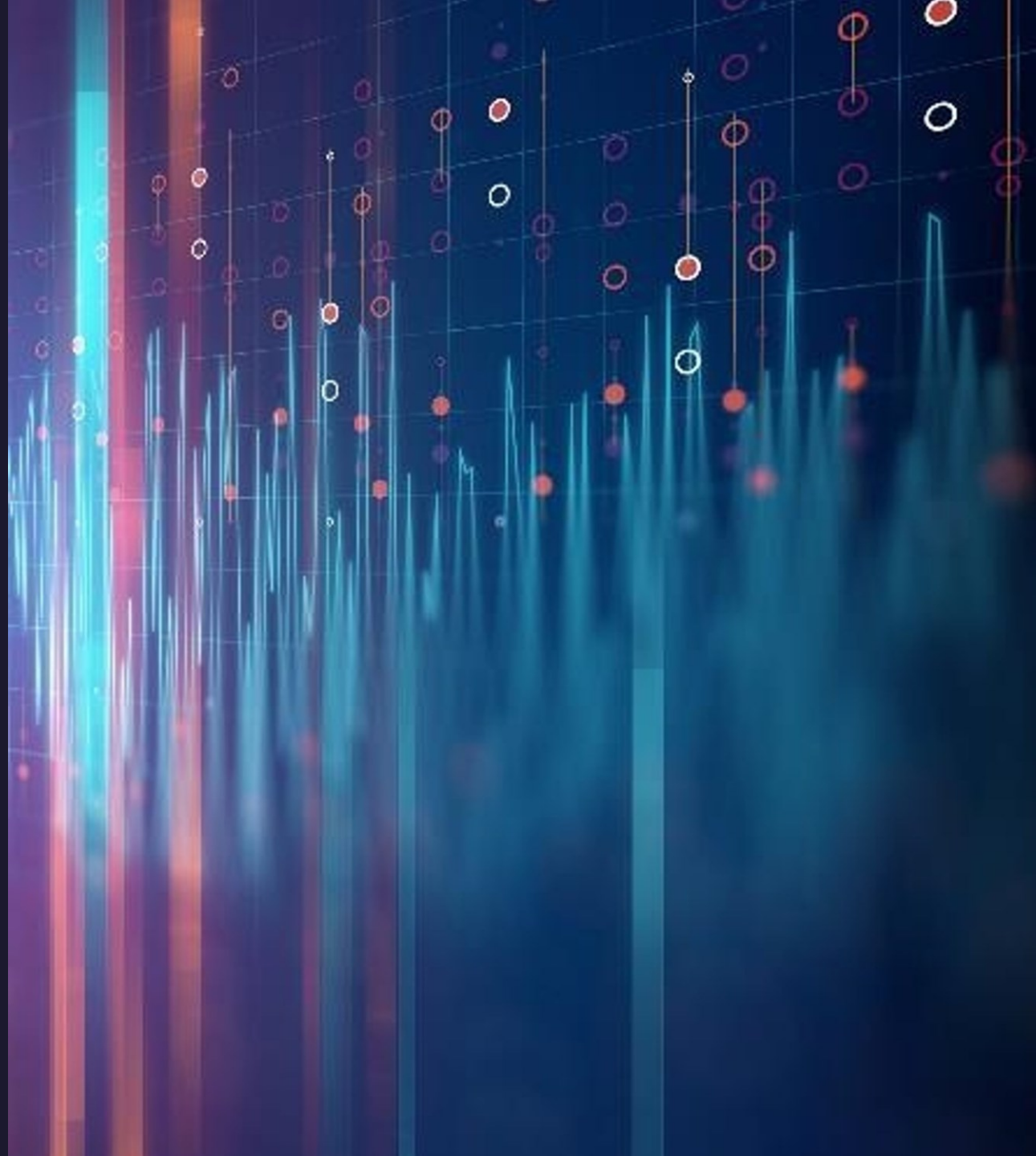
- ✓ Modificare le password degli account (mail e social), e i metodi autorizzativi dei conti correnti personali (controllare anche i sistemi di recupero credenziali)
- ✓ Analizzare le comunicazione pregresse
- ✓ Effettuare una copia/estrazione forense di:
  - Dispositivi utilizzati
  - Comunicazioni ricevute e inviate
  - Transazioni bancarie e criptomonete
  - Operazioni di trading
  - Documentazione ricevuta
- ✓ Presentare tempestivamente la denuncia

Dark web

Sul dark web è possibile acquisire **gli strumenti** oppure **il servizio** *(CaaS - Crime as a service)* per realizzare ogni singola fase.

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

Il **dark web** e le **criptovalute** offrono un ottimo schermo per le operazioni delittuose.



Intelligenza artificale generativa (GenAI)

L'intelligenza artificiale generativa amplifica le capacità cognitive e creative.

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

Nel contesto del cybercrime, è paragonabile ad una sorta di **superpotere**

La GenAI è una **risorsa** dual use si può utilizzare 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
Violazione dei codici captcha e delle password	Capacità di risolvere 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