RedHot Cyber

WWW.REDHOTCYBER.COM

La cybersecurity è condivisione.
Riconosci il rischio, combattilo,
condividi le tue esperienze ed
incentiva gli altri a fare meglio di te.

Dal Cybercrime al Cyber Organized Crime (COC)

Edited by Edoardo Faccioli

IL COLLETTIVO DARKLAB E' UN SOTTO GRUPPO DELLA COMMUNITY DI RED HOT CYBER SPECIALIZZATO AL MONITORAGGIO DELLE MINACCE INFORMATICHE.

Dark Lab nasce con l'obiettivo principale di diffondere la conoscenza sulle minacce informatiche per migliorare la consapevolezza e le difese digitali del paese.

INTRODUZIONE

Edoardo Faccioli

Il cybercrime rappresenta un universo in costante espansione, capace di attirare non solo l'interesse di singoli hacker esperti di informatica, ma anche di criminali tradizionali e organizzazioni ben strutturate, con obiettivi complessi e su larga scala.

Ho deciso di redigere questo report per fornire una panoramica dettagliata sullo stato attuale del cybercrime, analizzando come anche il crimine organizzato e le mafie sfruttino questo contesto per accrescere il proprio potere ed espandere i confini delle proprie attività, sia a livello territoriale che virtuale.

Nella prima parte esamineremo l'ambiente underground del web, dove si trovano molteplici attività illecite: dallo spaccio di farmaci e stupefacenti alla pedopornografia, fino alle truffe di vario tipo. Nella seconda parte, ci concentreremo sul fenomeno del Cyber Organized Crime (COC), analizzando i gruppi che hanno attirato maggiore attenzione da parte delle forze dell'ordine. Concluderemo esplorando come i social network rappresentino uno strumento potente per le mafie, consentendo loro di costruire consenso, soprattutto tra i più giovani.

INDEX OF CONTENTS

PREFAZIONE

La crescente presenza di Internet nelle nostre vite ha favorito lo sviluppo di azioni criminali che si sono adattate e perfezionate grazie alle nuove tecnologie.

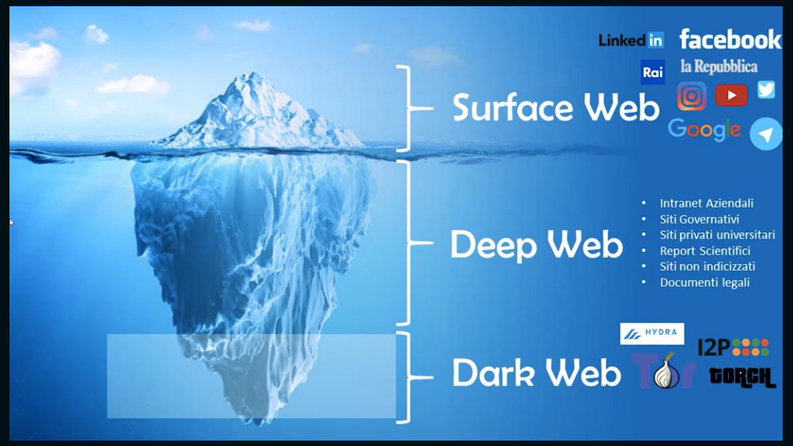
Sicuramente tutti, almeno una volta, abbiamo sentito parlare di Deep Web e Dark Web, ma cosa sono esattamente queste due realtà, e cosa si nasconde all'interno di queste sezioni più "nascoste" e "segrete" del web?

Il Deep Web rappresenta la parte di Internet in cui gli URL o gli indirizzi dei siti non sono indicizzati dai comuni motori di ricerca, come Google o Bing. Nonostante ciò, è facilmente accessibile tramite i browser più comuni, a patto di conoscere gli indirizzi esatti.

Il Dark Web, invece, costituisce una sezione ancora più oscura, accessibile esclusivamente attraverso strumenti specifici come TOR o I2P. Questa parte del web è stata progettata per garantire anonimato e privacy. Anche qui, per accedere ai portali web, è necessario conoscere gli indirizzi corretti.

L'aumento dei black market nel web, insieme alla crescente diffusione di strumenti per l'utilizzo e l'investimento in criptovalute, ha attirato l'interesse della criminalità organizzata, sia italiana che internazionale.

Di seguito presentiamo un'immagine che illustra quanto possano essere vaste queste due realtà, spesso inesplorate, del web.



È proprio in questa oscurità, in particolare sul Dark Web, progettato per garantire riservatezza e anonimato, che prendono forma molte delle principali attività criminali. Tra queste vi sono frodi, truffe (di natura romantica o finanziaria), furti, la vendita di materiali illegali (informazioni sensibili e personali, carte di credito, droga e armi) e la diffusione di materiale pedopornografico. Queste attività spesso richiedono operazioni di riciclaggio di denaro e fanno largo uso di criptovalute, un settore in continua espansione.

Già dal secondo semestre del 2022, la DIA (Direzione Investigativa Antimafia), nei suoi rapporti semestrali, ha evidenziato i legami tra il cybercrime e le mafie. Queste ultime, da sempre abili nell'adattarsi e nello sfruttare nuove tecnologie per aumentare i propri profitti, hanno trovato nel Dark Web e nella possibilità di effettuare pagamenti in criptovalute – senza limiti geografici e con controlli ridotti – un'opportunità ideale per espandersi, collaborare con altri gruppi criminali e incrementare significativamente i propri guadagni.

Un fenomeno da non sottovalutare è quello del ransomware, in costante crescita, che genera profitti sempre maggiori grazie alle richieste di riscatto. Le recenti operazioni delle forze dell'ordine internazionali, come la celebre Operazione Cronos, hanno messo in luce la sofisticata organizzazione di queste reti criminali, capaci di gestire enormi flussi di denaro con grande efficienza.

Questo scenario evidenzia come l'evoluzione tecnologica rappresenti non solo una risorsa, ma anche una sfida significativa per la sicurezza globale. E' importante comprendere che i criminali informatici, sempre più spesso, non agiscono da soli, ma vengono reclutati o diventano collaboratori di organizzazioni vaste e ben strutturate che hanno obiettivi criminali di ampia portata.

LA CONO D'OMBRA

Come Viene Sfruttata Dal Crimine Informatico

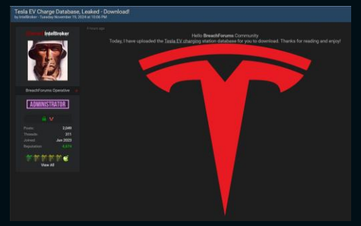
All’interno del Deep Web, e in particolare del Dark Web, si trovano numerosi portali web dedicati alla compravendita di materiale illecito. L’utilizzo delle criptovalute, che permette di superare i confini nazionali per il commercio di beni e servizi senza intermediari finanziari, unito al sistema TOR, progettato per garantire privacy e anonimato, ha senza dubbio favorito la crescita di questi mercati illegali. Ma vediamo più nello specifico cosa i criminali possono trovare o mettere in vendita su questi portali web.

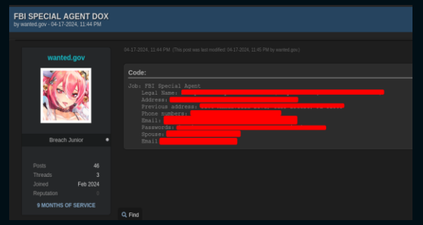
Dalle ricerche effettuate, emerge che la criminalità cyber è sostanzialmente una trasposizione della criminalità tradizionale nel dominio cibernetico. I mercati illegali di cui parleremo spaziano dal furto di identità alla vendita di materiale illegale, come armi non registrate, documenti falsi, carte di credito rubate, attività di hacking ed estorsione, frodi finanziarie, materiale pedopornografico, gioco d’azzardo clandestino e, ultimo ma non meno importante, riciclaggio di denaro.
E’ bene ricordare che comunque in questa zona “ombra” del Web non esistono garanzie o sicurezze pertanto tutto quello che si trova o si legge va sempre visionato con molta attenzione e pensiero critico.

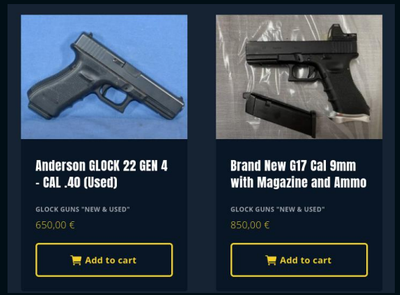
Quando si accede per la prima volta al Dark Web, la prima cosa che solitamente si esplora sono i **forum**. Molti di questi sono accessibili liberamente, mentre altri, più di nicchia, dove il materiale e le discussioni risultano decisamente più “black” e “underground”, richiedono il pagamento di una quota di iscrizione, che può variare dai 100 ai 500 dollari. In alternativa, l’accesso può essere concesso attraverso una “raccomandazione” o una “garanzia” da parte di un membro già iscritto e ben inserito nella comunità.

I forum, nella loro struttura, si somigliano molto tra loro. Di solito presentano una chat generale e una sezione dedicata agli argomenti di carattere generale, che spaziano dalle notizie del giorno ai fumetti, come anime e musica, fino a temi tecnologici come la programmazione. Un’altra sezione è riservata ai cosiddetti “Leaks”, dove si trovano post contenenti dati di vario genere, come account, database, log di varia natura e persino casi di *doxing*, ovvero la condivisione di informazioni private su persone o aziende.

Molte di queste piattaforme, inoltre, offrono servizi di *Escrow* o sezioni dedicate alla compravendita dei dati menzionati in precedenza, facilitando lo scambio di denaro e materiale tra i membri.







I Darknet Market, invece, vanno oltre la vendita di informazioni, tipica delle sezioni "Leaks", proponendo un'ampia gamma di materiali illegali, tra cui droga, armi, carte di credito rubate e documenti falsi..

I pagamenti avvengono quasi esclusivamente in criptovalute, come Bitcoin, Ethereum o Monero, per garantire maggiore anonimato e sicurezza nelle transazioni. A differenza dei forum, dove gli utenti possono pubblicare post liberamente, nei Darknet Market le inserzioni sono pubblicate direttamente dal market stesso, mantenendo un controllo centralizzato sul contenuto e sulle operazioni.

Forum e Darknet Market generano un mercato proficuo e in continua crescita. Secondo il report effettuato da Chainalysis i movimenti di criptovalute collegate alla compravendita di servizi offerti dai Darknet Markets ha raggiunto nel 2023 l'1.7 Miliardi di dollari segnale di crescita rispetto al 2022 anno in cui ha chiuso il famigerato hydra market.

All'interno dei Darknet Market si sta sviluppando rapidamente il fenomeno del **carding**, ovvero la compravendita di carte di credito rubate e clonate. I criminali ottengono i dati delle carte tramite tecniche tradizionali o di hacking, come phishing, malware o il furto di database, e li rivendono sul dark web. Queste carte possono essere utilizzate per transazioni online o per prelievi di denaro, richiedendo anche la spedizione della carta fisica.

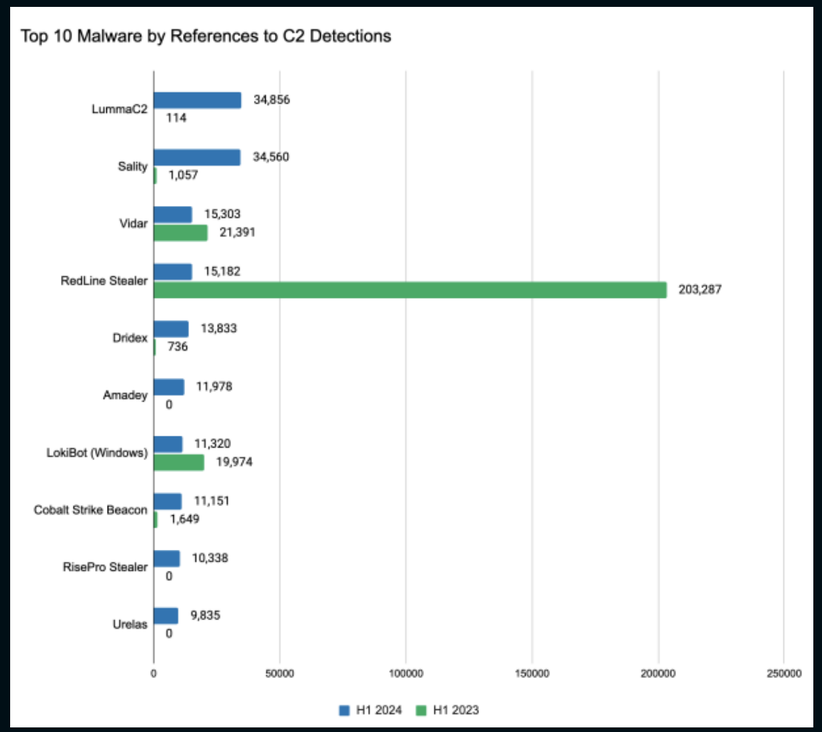
Secondo un report di NordVPN del 2023, che ha analizzato 6 milioni di carte rubate, il prezzo medio di vendita per una carta rubata è di **$10,08**. Le carte più costose sono quelle danesi, con un prezzo medio di $11,54, mentre quelle italiane si trovano al terzultimo posto, con un valore medio di $8,98.

Come per altre attività criminali sul dark web, anche il carding sfrutta metodi di pagamento in criptovalute, rendendo estremamente difficile il tracciamento delle transazioni.

Malware, Ransomware e Infostealer

All'interno del dark web si sta diffondendo sempre più la compravendita di informazioni sensibili e dati rubati dai dispositivi elettronici delle vittime tramite malware noti come **Infostealer**. Questi software malevoli, una volta installati sul dispositivo target, estraggono il maggior numero possibile di informazioni, che vengono inviate sotto forma di log a un server di Command and Control (C2). Da lì, i dati vengono distribuiti su portali dedicati o canali Telegram accessibili ai criminali, previo pagamento di un abbonamento mensile o annuale, con costi di alcune centinaia di dollari che possono variare in base al tipo di servizio richiesto. Questo modello operativo è noto come MaaS (Malware as a Service).

Secondo un recente report di Recorded Future sull'andamento dei malware, nella prima metà del 2024 (H1 2024), LummaC2 ha superato RedLine per diffusione di server C2 rilevati, conquistando il primo posto tra i malware di questo tipo.



Top 10 malware (Fonte Recorded Future)

La facilità di utilizzo e l'accessibilità di questi strumenti consentono anche ai criminali meno esperti in ambito tecnologico di rubare informazioni sensibili da numerose vittime, per poi utilizzarle per differenti scopi illeciti.

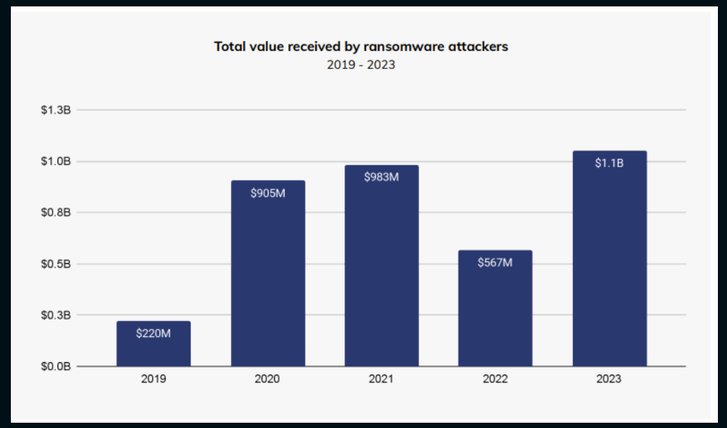
Le *Ransom Gang* stanno ottenendo un notevole successo nella diffusione dei ransomware, raggiungendo risultati significativi. Le vittime di un attacco ransomware possono appartenere a qualsiasi settore: istituti finanziari, ospedali, università e molte altre organizzazioni. Queste comunità criminali sono spesso ben organizzate e strutturate, con numerosi affiliati che eseguono materialmente gli attacchi.

Quando una vittima viene colpita da un ransomware, si ritrova con i propri sistemi tecnologici criptati, rendendo inutilizzabili i dati al loro interno. L'obiettivo del criminale è costringere la vittima a pagare un riscatto per ottenere la chiave di decriptazione necessaria a ripristinare l'accesso ai dati e ai sistemi. Tuttavia, molti attacchi includono una fase di esfiltrazione dei dati prima della crittografia, consentendo agli attaccanti di effettuare una doppia estorsione: oltre al riscatto per la decriptazione, possono richiedere un ulteriore pagamento per evitare la diffusione pubblica o la vendita dei dati sensibili rubati.

Questa strategia rende gli attacchi ransomware particolarmente devastanti, sia per l'impatto operativo che per le implicazioni legali e reputazionali delle organizzazioni colpite

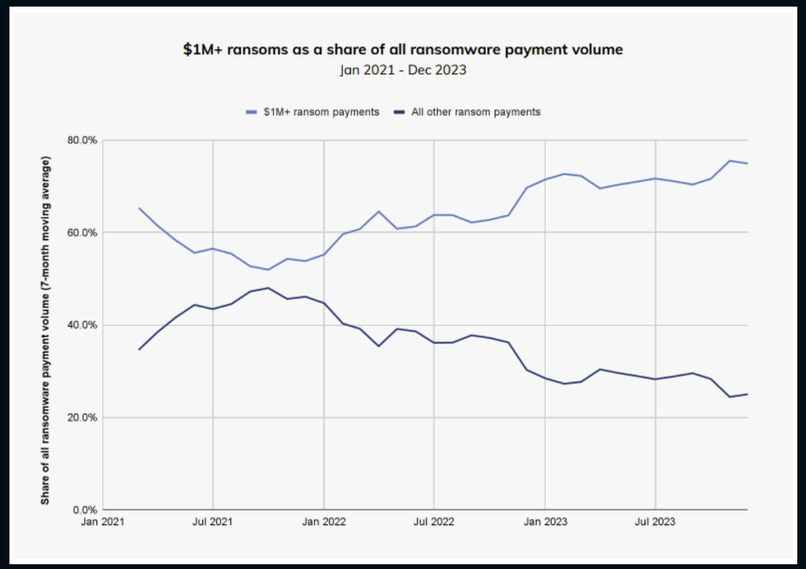
Il fenomeno dei ransomware rappresenta una delle aree del cybercrime più redditizie e problematiche, caratterizzato da un impatto immediato e tangibile a causa della sua natura e delle modalità con cui si diffonde e colpisce le vittime. Le richieste di riscatto generano un forte stress e, negli ultimi tempi, stanno diventando sempre più elevate. Questo avviene perché i gruppi attaccanti si informano accuratamente e spesso adattano l'importo richiesto in base al fatturato dell'azienda presa di mira.

Secondo l'ultimo report annuale di Chainalysis, che analizza il fenomeno dei ransomware nel 2023 e negli anni precedenti, si osserva una tendenza in crescita, con volumi economici che hanno superato il miliardo di dollari.



Il valore dei riscatti ottenuti dalle cybergang ransomware (fonte chainalysis)

Un tale volume di denaro è stato reso possibile anche grazie alla strategia di attaccare aziende di grandi dimensioni e con fatturati elevati, permettendo agli aggressori di chiedere riscatti che spesso superano il milione di dollari.



fonte chainalysis

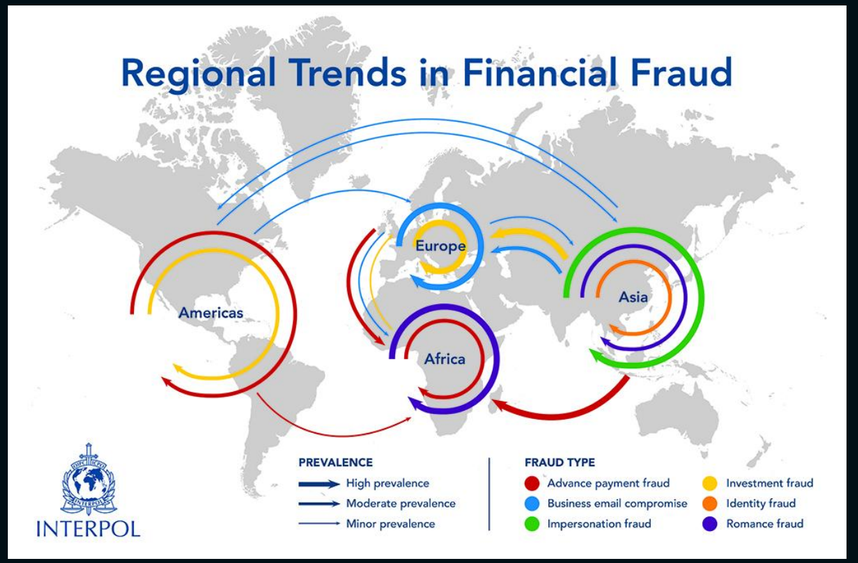
OLTRE L'UNDERGROUND

SCAM, Tratta di esseri umani e sfruttamento, CSAM (Child Sexual Abuse Material) - Pedopornografia

L'esposizione a Internet e la facilità con cui tutti noi possiamo accedervi e utilizzarlo hanno facilitato l'espansione e la crescita delle truffe online, comunemente conosciute come **SCAM**.

Queste truffe possono assumere forme molto diverse, e ogni giorno i criminali ideano nuove tecniche per ingannare le proprie vittime. Il settore delle truffe è in continua espansione, favorito dall'aumento dei furti di identità, che consentono ai truffatori di raccogliere numerose informazioni sulle vittime prima di mettere in atto la loro strategia. Inoltre, sul dark web sono disponibili vere e proprie guide e tutorial che spiegano come realizzare scam con successo.

Secondo il report di Chainalysis, il valore economico totale di questo mercato criminale ha superato i 4 miliardi di dollari nel 2023. Tra le tipologie di truffe in maggiore crescita si segnalano quelle romantiche e finanziarie, sia nell'ambito della finanza tradizionale sia in quella basata su blockchain. Inoltre, continuano a essere diffuse truffe più comuni, come quelle legate agli acquisti online di beni, alle false offerte di lavoro, ricatti e tutte quelle legate a tecniche di social engineering attuabili anche telefonicamente.



Fonte Europol

Il legame tra le truffe online, in particolare le false offerte di lavoro e le truffe romantiche, e il traffico di esseri umani è diventato sempre più evidente, con un aumento significativo di questo tipo di crimine.

Secondo l'Interpol, già nel 2023 è stato emesso un avvertimento globale sulla sicurezza a causa della rapida crescita di questo fenomeno. Sempre più persone, attratte da offerte di lavoro apparentemente vantaggiose, accettano di trasferirsi in altri Paesi con viaggi pagati, alloggi garantiti e la falsa promessa di un futuro migliore. Tuttavia, una volta giunti a destinazione, si ritrovano intrappolati e costretti a lavorare in centri tecnologici dedicati a truffe online e telefoniche.

Fonte Europol

I trafficanti utilizzano strumenti tecnologici come social network, siti di incontri e portali di offerte di lavoro per adescare le vittime, favorendo la diffusione del fenomeno noto come e-trafficking. Le persone che cadono in queste trappole non finiscono solo in hub dedicati alle truffe, ma spesso, una volta arrivate nel Paese indicato dai criminali, vengono obbligate a ripagare il presunto debito contratto per le spese di viaggio. Questo debito diventa il pretesto per costringerle a lavorare in condizioni di schiavitù o, in molti casi, a prostituirsi.

Uno dei reati più diffusi che le forze dell'ordine italiane cercano quotidianamente di contrastare è quello legato ai crimini pedopornografici, molto presenti sul web.

Secondo l'Europol, i materiali pedopornografici possono essere classificati principalmente in due categorie:

1. **Materiali presenti su reti che favoriscono privacy e anonimato**, come la rete TOR. In queste piattaforme si trovano numerosi siti e forum dedicati allo scambio di materiale CSAM (Child Sexual Abuse Material), spesso distribuito gratuitamente o tramite pagamenti in criptovalute come Bitcoin o Monero. Sono frequenti anche gruppi su Telegram utilizzati per la condivisione di questo materiale.
2. **Live streaming di abusi su minori**, in cui le vittime, spesso adescate online, vengono costrette a passare molto tempo davanti a una telecamera per svolgere attività su richiesta o imposte dai loro sfruttatori.

Per ottenere questo tipo di materiale e poterlo vendere, i criminali utilizzano una pratica chiamata ***grooming*** online. Questa consiste in un processo di seduzione e adescamento del minore, che prevede:

- La selezione della vittima;
- La costruzione di un rapporto di fiducia attraverso amicizia apparente e manipolazione;
- La raccolta di quante più informazioni possibili sulla vittima, sia online che offline, per poterla ingannare.

L'obiettivo finale è ottenere materiale pedopornografico attraverso scambi diretti online o, nei casi peggiori, incontrare la vittima fisicamente per abusarne sessualmente.

L'economia legata al CSAM (Child Sexual Abuse Material) non è facile da analizzare, poiché si basa prevalentemente sullo scambio di materiale piuttosto che sul pagamento diretto. Tuttavia, anche in questo ambito è stato rilevato un crescente utilizzo delle criptovalute, che garantiscono un elevato livello di privacy nelle transazioni, rendendo sempre più complessa l'attività investigativa delle forze dell'ordine.

Secondo analisi condotte da Chainalysis e IWF (Internet Watch Foundation), i prezzi per l'acquisto di materiale pedopornografico variano generalmente da 10 a oltre 70 dollari. La tendenza evidenzia un maggiore utilizzo di materiale a basso costo, accompagnato però da un aumento della quantità complessiva di contenuti disponibili.

Nel 2023 sono stati segnalati oltre 275.000 URL contenenti materiale di abusi su minori, con un incremento dell'8% rispetto al 2022. Questo dato sottolinea la continua crescita del fenomeno, richiedendo sforzi sempre maggiori per contrastare la diffusione e garantire la protezione delle vittime.

VERSO IL COC

Espansione nel cyberspazio del Cyber Organized Crime

Le organizzazioni mafiose sono in continua evoluzione e si adattano efficacemente al contesto in cui operano. Oggi le mafie hanno modificato profondamente il loro modo di agire, cercando di infiltrarsi nel tessuto sociale in maniera sempre più silenziosa ma altrettanto efficace, perseguendo i propri interessi economici e di potere.
Per integrarsi nel tessuto imprenditoriale del Paese, le organizzazioni criminali utilizzano i capitali ottenuti attraverso attività illecite tradizionali o più moderne, come quelle legate al cybercrime. Questa evoluzione ha favorito una crescente interazione tra il crimine organizzato e le nuove tecnologie.

Mafie Italiane, narcotraffico e gioco d'azzardo

Secondo le relazioni della DEA, già nel 2023 era emerso che le organizzazioni mafiose sfruttavano le nuove tecnologie per lo smercio di stupefacenti, che continua a rappresentare il principale business in termini di introiti per queste realtà criminali. In questo scenario, le mafie italiane potrebbero ampliare ulteriormente la loro rete internazionale di narcotraffico, già molto estesa grazie alla presenza di numerosi affiliati nei Paesi di produzione e transito di sostanze stupefacenti. In particolare, si è registrato un aumento dei traffici provenienti dai Paesi dell'Africa occidentale.

Inoltre, i guadagni elevatissimi derivanti dal narcotraffico richiedono un espansione dei sistemi di riciclaggio di denaro. Per questo motivo, un'attività sempre più utilizzata dalle organizzazioni criminali è il **gioco d'azzardo online** non regolamentato e illecito. Questa pratica è favorita dalla possibilità di costituire aziende "cartiere" con sedi legali in paradisi fiscali, che consentono sia il riciclaggio di denaro sia ulteriori guadagni illeciti.

Già nel 2018, la Direzione Distrettuale Antimafia aveva coordinato un'operazione condotta dalla Polizia di Stato, nota come "Operazione "Bruno", che aveva portato all'arresto di 13 individui sia in Italia che in Romania accusati di reati che andavano dall'associazione a delinquere all'accesso abusivo a sistemi informatici, fino al riciclaggio di proventi derivanti da massicce campagne di phishing. Questa operazione ha evidenziato come anche la 'ndrangheta stesse iniziando a muoversi nel campo del crimine informatico.

Truffe Online e Crimine Organizzato Albanese

Anche la mafia albanese ha come principale attività criminale il traffico di stupefacenti. Si tratta di organizzazioni ben attrezzate e strutturate, che basano la loro forza su legami di fiducia e parentela. Queste mafie dispongono di referenti sia in Italia che all'estero, il che consente loro di espandersi rapidamente anche al di fuori del Paese d'origine. Sono state segnalate, inoltre, attività criminali nel campo dell'immigrazione e delle tratte di esseri umani. Tuttavia, l'aspetto che ha maggiormente avvicinato la mafia albanese al cybercrime riguarda le **truffe online e telefoniche**.

Nel 2023 si è conclusa un'operazione denominata "Dream Earnings", coordinata tra la polizia italiana e quella albanese, che ha smantellato un'organizzazione criminale composta da oltre 50 persone. La truffa consisteva nel contattare telefonicamente le vittime tramite call center situato a Tirana, in Albania, e convincerle a investire somme di denaro in proposte finanziarie fraudolente, promettendo guadagni rapidi.

I criminali, inoltre, erano molto abili nell'utilizzo di tecniche di social engineering, che permettevano loro di entrare in sintonia con le vittime e guadagnarne la fiducia. In alcuni casi, riuscivano persino a lavorare da remoto sui computer delle persone prese di mira, aumentando l'efficacia delle loro frodi e amplificando i danni economici. I criminali inoltre convertivano il denaro della vittima in criptovalute così da poter non essere facilmente tracciati e facilitare i trasferimenti da diversi wallet. Si stima che il valore totale delle cifre movimentate sia intorno ad alcune decine di milioni di euro.

BLACK AXE e il cybercrime

Anche la mafia nigeriana si è avvicinata al crimine informatico, stabilendosi in diversi contesti europei e extraeuropei. Oltre a condurre le classiche attività illecite tipiche delle organizzazioni mafiose, come il traffico di stupefacenti, il contrabbando, le estorsioni, la prostituzione e i rapimenti, questa mafia riesce a generare ingenti profitti attraverso le **truffe online**. Queste frodi spaziano da quelle finanziarie più comuni a sofisticate truffe sentimentali, spesso realizzate tramite piattaforme di incontri.

Proprio perché le loro truffe non sono limitate da confini geografici, l'Interpol ha identificato il gruppo Black Axe come uno dei principali attori criminali responsabili di frodi informatiche e altre attività legate al cybercrime. Per comprendere l'estensione e l'influenza di questo gruppo, si può fare riferimento all'operazione Jackal III, condotta dall'Interpol: una campagna che ha coinvolto 21 Paesi distribuiti su 5 continenti, portando a 300 arresti, all'identificazione di 400 sospetti e al blocco di oltre 720 conti bancari utilizzati per le attività criminali.

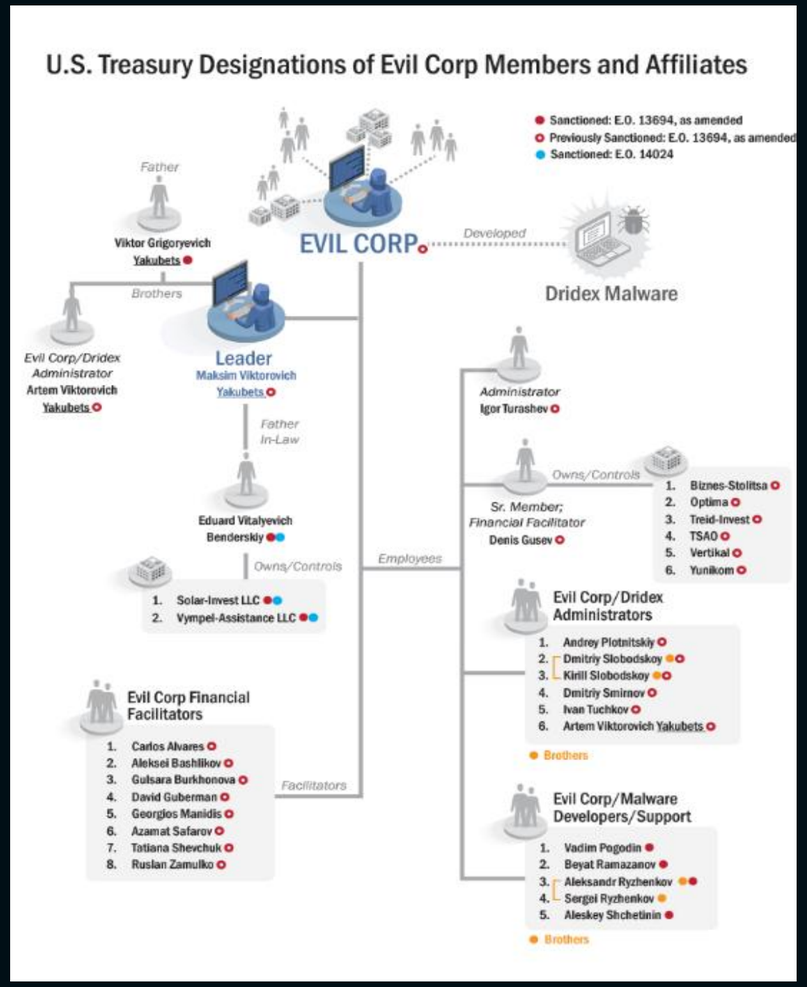
Il volume delle frodi online provenienti dall'Africa occidentale è in costante aumento. Queste organizzazioni riescono a riciclare ingenti somme di denaro grazie a una rete sofisticata di riciclaggio, che include numerosi Money Mule distribuiti in vari Paesi del mondo. I Money Mule, aprendo conti bancari a loro nome, consentono il trasferimento di fondi senza destare sospetti né alle vittime né agli istituti di credito.

Le tecniche utilizzate per spostare il denaro riciclato includono l'acquisto di beni di valore, come automobili, e il crescente utilizzo delle criptovalute, che offrono anonimato e difficoltà di tracciamento.

Ransomware Gang & Threat Actor

Anche i gruppi ransomware e le organizzazioni specializzate esclusivamente in cybercrime stanno diventando sempre più vaste e sofisticate. Questi gruppi, pur non condividendo le caratteristiche tipiche delle mafie tradizionali, operano con una struttura simile a quella aziendale, puntando a massimizzare i loro "profitti". Possiedono una gerarchia ben definita e sofisticati portali web che permettono di comunicare con affiliati, fornire strumenti tecnologici avanzati e gestire in modo coordinato le operazioni criminali.

A far luce sul funzionamento interno di questi gruppi criminali è stata l'Operazione Cronos e le sanzioni applicate contro l'organizzazione nota come Evil Corp e il suo collegamento con Lockbit. Questi gruppi pianificano i loro attacchi con estrema attenzione, analizzando nel dettaglio i loro obiettivi e seguendo un approccio metodico in ogni fase dell'attacco.



source: U.S. Department of the treasury

Le loro strutture sono organizzate in modo da suddividere chiaramente i compiti: ci sono figure incaricate di gestire le comunità online, "mediatori" che facilitano il coordinamento con le vittime e con altre organizzazioni, sviluppatori altamente competenti che progettano e implementano i malware, e infine esperti di riciclaggio di denaro.

Il sistema di riciclaggio di questi gruppi si avvale di tecnologie avanzate nel campo della finanza decentralizzata (DeFi) e di strumenti come le criptovalute, ma sfrutta anche le tradizionali reti di Money Mule, che garantiscono la movimentazione dei fondi senza destare sospetti.

Social Media e Mafie

Le mafie, oltre a trasformare gli spazi in cui operano, stanno modificando radicalmente anche il modo in cui promuovono e reclutano nuovi membri. Attraverso i social network, queste organizzazioni criminali sfruttano strumenti potenti per raggiungere diversi obiettivi: reclutare nuovi affiliati, ostentare ricchezza e potere, intimidire avversari e, al contempo, alimentare un immaginario glamour che risulta particolarmente attraente per le nuove generazioni.

Piattaforme come **YouTube**, **Instagram**, **Facebook** e **TikTok**, ciascuna con le proprie peculiarità, permettono alle mafie di adattare i loro messaggi al pubblico e al contesto. Questi canali digitali diventano quindi veicoli strategici per:

Costruzione di un'identità digitale
Le organizzazioni criminali promuovono un'immagine di successo, ricchezza e potere attraverso la pubblicazione di contenuti che mettono in mostra denaro, lusso e stili di vita ambiti. Questo tipo di comunicazione mira a costruire una vera e propria "brand identity" digitale, capace di attrarre e sedurre i più giovani.

source: Fondazione Magna Grecia "Le mafie nell'era digitale"

1. **Reclutamento e senso di appartenenza**
   La condivisione di contenuti che esibiscono successo e potere ha l'obiettivo di suscitare un senso di appartenenza negli spettatori, facilitando il reclutamento e il processo di affiliazione.
2. **Propaganda intimidatoria e controllo del potere**
   Attraverso i social network, le mafie possono diffondere messaggi intimidatori e rafforzare la percezione del loro controllo sul territorio, unendo il mondo virtuale a quello reale. Questa convergenza tra vita online e offline contribuisce a consolidare la loro autorità e il loro prestigio.

L'uso strategico delle nuove tecnologie permette quindi alle mafie di amplificare il loro potere e la loro influenza, creando un ecosistema digitale che le supporta nelle loro attività illecite e nel controllo sociale.

BIBLIOGRAFIA

- Relazioni Semestrali DIA: https://direzioneinvestigativaantimafia.interno.gov.it/relazioni-semestrali/
- Report Crypto Crime 2024: https://go.chainalysis.com/crypto-crime-2024.html
- Report NordVPN: https://s1.nordcdn.com/nord/misc/0.71.0/vpn/brand/research-lab/payment-card-details-theft/Payment-card-research-report.pdf
- Report Recorded Future: https://www.recordedfuture.com/research/h1-2024-malware-and-vulnerability-trends-report
- Interpol SCAM: https://www.interpol.int/News-and-Events/News/2024/INTERPOL-Financial-Fraud-assessment-A-global-threat-boosted-by-technology
- Interpol Human Trafficking: https://www.interpol.int/News-and-Events/News/2023/INTERPOL-issues-global-warning-on-human-trafficking-fueled-fraud
- CSAM Europol: https://www.europol.europa.eu/crime-areas/child-sexual-exploitation
- IWF: https://www.iwf.org.uk/annual-report-2023/trends-and-data/reports-analysis/
- DEA 2023: https://direzioneinvestigativaantimafia.interno.gov.it/wp-content/uploads/2024/06/Rel-Sem-I-2023.pdf
- Operazione Bruno: https://www.poliziadistato.it/articolo/15265ac487b649954752027145
- Operazione Dream Earnings: https://questure.poliziadistato.it/it/Pordenone/articolo/85264c241cb62df8327157748
- Interpol Jackal III: https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-operation-strikes-major-blow-against-West-African-financial-crime
- Operazione Cronos: https://www.nationalcrimeagency.gov.uk/the-nca-announces-the-disruption-of-lockbit-with-operation-cronos
- Sanzioni Evil Corp: https://www.nationalcrimeagency.gov.uk/the-nca-announces-the-disruption-of-lockbit-with-operation-cronos
- Fondazione magna grecia Le mafie nell'era digitale: https://fondazionemagnagrecia.it/wp-content/uploads/2023/10/12000.31Ravvedutoebook.pdf