nuove tecniche di indagine a contrasto del fenomeno del phishing, attraverso metodologie oSint.

« open source intelligence»

Relatori

Antonio Broi Pallotta

Esperto Computer Forensic e Data Analysis

Programmatore Osint-ProActive

Francesco Crocetti

Esperto Computer Forensic e Data Analysis

Breve definizione del fenomeno

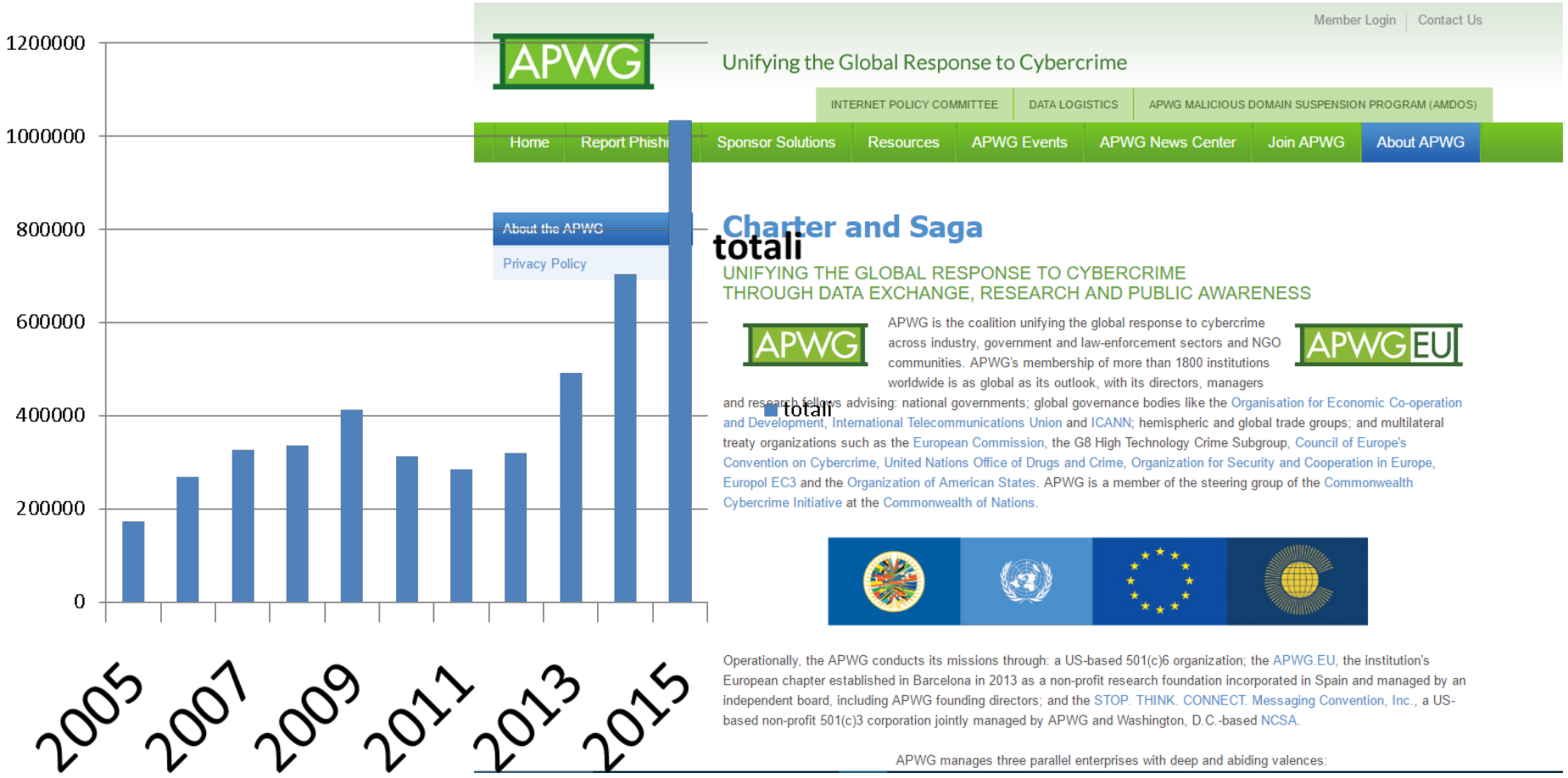
- **FONTE https://www.commissariatodips.itapprofondimentiphishing.html**
- E’ una particolare tipologia di truffa realizzata sulla rete Internet attraverso l’inganno degli utenti. Si concretizza principalmente attraverso messaggi di posta elettronica ingannevoli:
- Attraverso una e-mail, solo apparentemente proveniente da istituti finanziari (banche o società emittenti di carte di credito) o da siti web che richiedono l'accesso previa registrazione (web-mail, e-commerce ecc.). Il messaggio invita, riferendo problemi di registrazione o di altra natura, a fornire i propri riservati dati di accesso al servizio. Solitamente nel messaggio, per rassicurare falsamente l'utente, è indicato un collegamento (link) che rimanda **solo apparentemente** al sito web dell'istituto di credito o del servizio a cui si è registrati. In realtà il sito a cui ci si collega è stato artatamente allestito identico a quello originale. Qualora l'utente inserisca i propri dati riservati, questi saranno nella disponibilità dei criminali.
- Con la stessa finalità di carpire dati di accesso a servizi finanziari on-line o altri che richiedono una registrazione, un pericolo più subdolo arriva dall’utilizzo dei virus informatici. Le modalità di infezione sono diverse. La più diffusa è sempre il classico allegato al messaggio di posta elettronica; oltre i file con estensione **.exe**, i virus si diffondono celati da false fatture, contravvenzioni, avvisi di consegna pacchi, che giungono in formato **.doc .pdf** . Nel caso si tratti di un c.d. “financial malware” o di un “trojan banking”, il virus si attiverà per carpire dati finanziari. Altri tipi di virus si attivano allorquando sulla tastiera vengono inseriti “userid e password”, c.d. “keylogging”, in questo caso i criminali sono in possesso delle chiavi di accesso ai vostri account di posta elettronica o di e-commerce.

Come rilevare un attacco ????

- **FONTE** **http://it.norton.com/security_response/phishing.jsp**
- Il phishing è essenzialmente una truffa on-line e coloro che la attuano, indicati come phisher, non sono altro che truffatori e ladri di informazioni personali con competenze tecniche.
- Utilizzano lo SPAMMING, siti Web ingannevoli, e-mail e messaggi istantanei per indurre le persone a divulgare informazioni riservate, come ad esempio dettagli sul conto corrente bancario e sulle carte di credito.
- **Come rilevare un attacco**
- I phisher, fingendo di essere aziende legittime, possono utilizzare l'e-mail per richiedere informazioni personali e indurre i destinatari a rispondere per mezzo di siti Web nocivi
- **I phisher tendono a utilizzare linguaggio emozionale** che fa uso di tattiche intimidatorie e pressanti per indurre i destinatari a rispondere
- I siti di phishing possono sembrare autentici perché tendono a utilizzare immagini che riportano il copyright dei siti legittimi
- Le richieste di informazioni riservate tramite e-mail o messaggi istantanei non sono generalmente legittime
- Spesso i messaggi fraudolenti non sono personalizzati e possono condividere proprietà simili, come i dettagli nell'intestazione e nel piè di pagina

Qualche dato statistico

© 2016 Anti-Phishing Working Group, Inc.



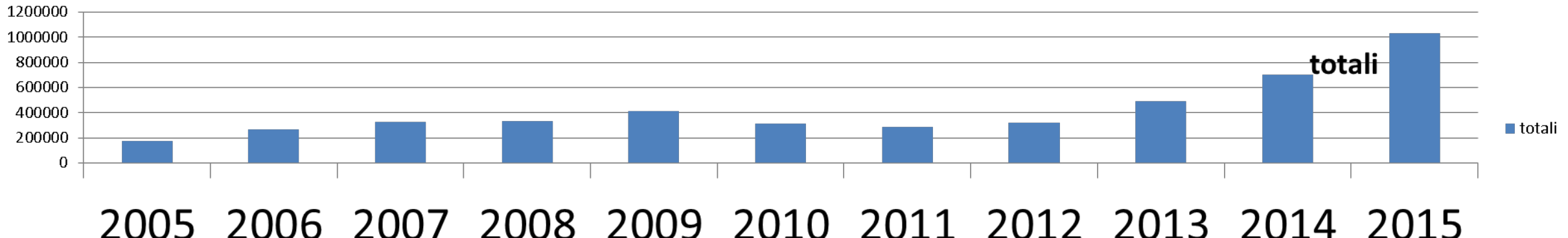
MANIFESTAZIONE STATISTICA DEGLI ATTACCHI.

http://www.antiphishing.org/resources/apwg-reports/

Total number of unique phishing reports (campaigns) received[10]

Year	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
2005	12845	13468	12883	14411	14987	15050	14135	13776	13562	15820	16882	15244
2006	17877	17163	18480	17490	20109	28571	23670	26150	22136	26877	25816	23787
2007	29930	23610	24853	23656	23415	28888	23917	25624	38514	31650	28074	25683
2008	29284	30716	25630	24924	23762	28151	24007	33928	33261	34758	24357	23187
2009	34588	31298	30125	35287	37165	35918	34683	40621	40066	33254	30490	28897
2010	29499	26909	30577	24664	26781	33617	26353	25273	22188	23619	23017	21020
2011	23535	25018	26402	20908	22195	22273	24129	23327	18388	19606	25685	32979
2012	25444	30237	29762	25850	33464	24811	30955	21751	21684	23365	24563	28195
2013	28850	25385	19892	20086	18297	38100	61453	61792	56767	55241	53047	52489
2014	53984	56883	60925	57733	60809	53259	55282	54390	53661	68270	66217	62765
2015	49608	55795	115808	142099	149616	125757	142155	146439	106421			

	totali
2005	**173.063**
2006	**268.126**
2007	**327.814**
2008	**335.965**
2009	**412.392**
2010	**313.517**
2011	**284.445**
2012	**320.081**
2013	**491.399**
2014	**704.178**
2015	**1.033.698**



LE CONNESSIONI AVVENGONO SEMPRE PIU' SPESSO DAI DISPOSITIVI 'MOBILE'.

Gli utenti sono sempre piu' predisposti all'accettazione di qualsiasi input in modo distratto !
Specialmente in luoghi ed orari particolari!

ASPETTI OPERATIVI

- **Fasi informatiche-operative del Phishing.**

La costruzione del meccanismo informatico di phishing è un'operazione abbastanza semplice da realizzare.

Si compone di diverse fasi:

1. Creazione di un sito Web 'malevolo ' , da parte dell'organizzazione criminale, atto a registrare le password degli utenti 'vittime';
2. Invio dell'email esca, da parte dell'organizzazione criminale, con link al sito Web appositamente creato ;
3. Compimento di atti criminosi, da parte dell'organizzazione Criminale, utilizzando le credenziali degli utenti 'vittime';

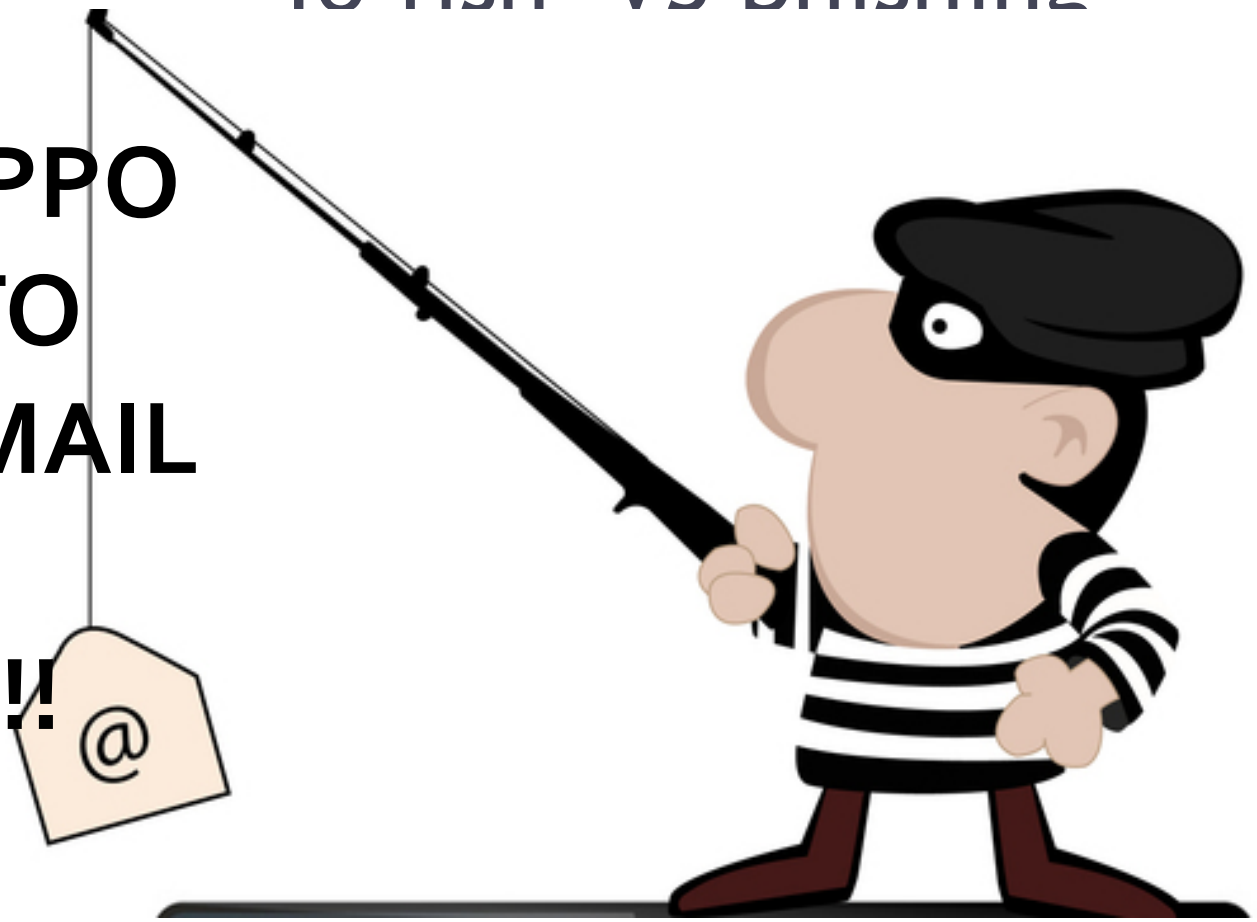
Creazione di una pagina ‘fake’ posta in un sito gestito dall’organizzazione criminale, atto a registrare le password degli utenti ‘vittime’;

- L’ipotetico malintenzionato o l’organizzazione criminale innanzitutto si occupa della costruzione della pagina web html dinamica, atta alla raccolta dei dati sensibili , quindi dell’individuazione ed analisi anche tramite attività di Osint dei o i bersagli; per poter in seguito effettuare phishing anche massivo tramite sistemi massivi «BEEF DOCET»;
- copia il codice sorgente della pagina Web Originale dove è presente il login del vero sito e, lasciando invariata la grafica, si adopera per modificarla in modo che invii i dati inseriti dall’utente, tramite uno script PHP (programmazione lato Server-Side).
- Tale programma di scripting (di solito PHP E MYSQL) si occupa di leggere e registrare, attraverso DUE variabili ottenute con HTTP POST o HTTP GET, le credenziali dei malcapitati in un file di log o in sistemi database, e anche inviandole eventualmente (in real-time) ad un indirizzo di posta elettronica dell’ipotizzata organizzazione criminale;

Inizia la stagione di pesca?

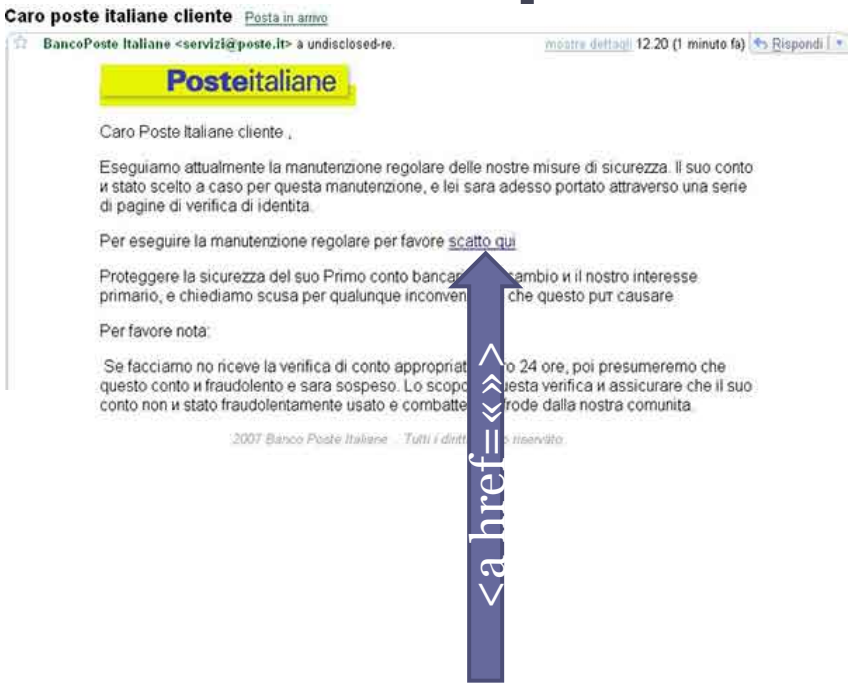
To fish VS phishing

PURTROPPO L'ASPETTO DELLE EMAIL NON è QUESTO !!



Forse questo !!??

Real @mail Example



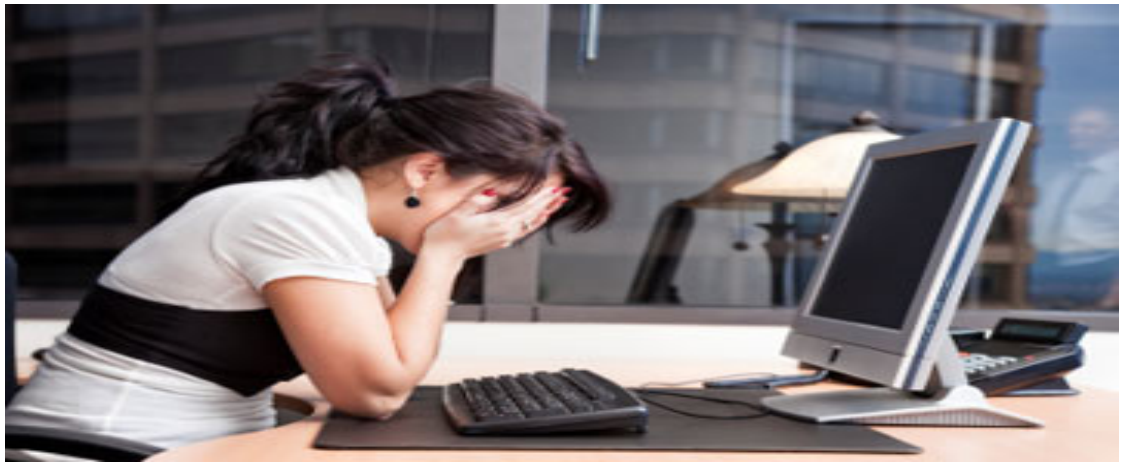
Invio dell'email esca con link camuffato «a href='hacker.banca.it'»vera.banca.it «a/»

- A questo punto, costruita la pagina html, l'organizzazione dovrà pubblicare la stessa, "fittiziamente" creata, in un web-server online di sua proprietà o appositamente «defaciato» (cioè espropriato del contenuto al proprietario della pagina);
- successivamente inviare le email costruite ad arte, per invitare le ignare vittime a cliccare sul link "fittizio" , il quale nasconde nel semplice codice sorgente HTML o comunque lato web Javascript/Php etc. , dietro un'apparenza ingannevole, (<a href="hacker.banca.it"> banca.it<a/>), il link alla pagina effettivamente creata; quest'ultima tramite il form HTML, costituito graficamente da due caselle di INPUT-TEXT con richiesta di nome utente e password, appena veranno riempite con i dati, e riceveranno l'input dell'apposito pulsante (submit o botton), inviera i dati ad un file server su base dbase (php /msql o altri linguaggi) , per poter essere utilizzati dall'organizzazione criminale.
- nel medesimo istante spesso le pagine sono scritte, per non sollevare sospetti immediati nei malcapitati, con una immediata deviazione (al premere del BUTTON o SUBMIT) verso una pagina dove risulterà la correttezza dei dati immessi, o ancora peggio in una pagina dove si vedrà una scritta del tipo "hai effettuato l'operazione correttamente ora verrai indirizzato al login per controllo di sicurezza", oppure direttamente indirizzati nella home page con "login" della vera pagina web;
- **CLICK E POI……**

Il vero Momento fatale !!??

Ora zero !!!
Momento della cessione delle credenziali !

Utilizzo dei dati sensibili acquisiti dall'organizzazione criminale – FACCIAMOCI ALCUNE DOMANDE??



1. LA TRUFFA POSTA IN ESSERE DA SINGOLI ORGANIZZAZIONI CRIMINALI O ALTRO??
2. Utilizzo immediato o vendita nel DARK WEB ? (TOR WEB);
1. EVIDENTE SCOSTAMENTO NEL TEMPO TRA MOMENTO DEL FURTO DI INFORMAZIONI SENSIBILI ED UTILIZZO DEGLI STESSI PER EFFETTUARE ACQUISTI;

Analisi delle fasi investigative sui reati denunciati di phishing.

- L’analisi investigativa giudiziaria di un reato di phishing è composta da diverse fasi :
- La raccolta della denuncia presentata dalla persona vittima del reato e l’immediata raccolta di tutti i dati informatici relativi alle comunicazioni (email log pagine web connessioni di rete etc. etc.);
- Analisi dell’headers(intestazione) dell’email cioè del codice sorgente della stessa, analisi di tutti gli snodi a ritroso di invio della posta elettronica e individuazione e sviluppo del primo server di uscita della posta elettronica;
- Analisi del codice sorgente del testo del messaggio di posta elettronica ed individuazione del link nascosto nel codice (di solito semplice HREF=”sitophishing.ru”);
- Individuazione di tutti gli elementi di prova (compreso Osint) e compilazione della relativa Notitia Criminis all’A.G.;

CASO REALE «SVOLGIMENTO INDAGINE»

1) Il Sig. Y si presentava presso gli uffici giudiziari per svolgere denuncia penale su un caso di phishing essendosi accorto di prelievi sulla sua carta di credito xxxx xx con nr. xxx xxx (caso classico di denuncia);
2) All'atto della denuncia il sig. Y dichiarava inoltre di aver ricevuto qualche giorno addietro una strana email proveniente dal suo istituto di Credito dove addirittura avrebbe vinto un fantomatico premio fedeltà consistente in punti per l'acquisto di un bene super scontato; unica richiesta per poter usufruire di tali benefici l'inserimento delle sue credenziali della carta; d'altronde l'email proveniva dal suo Istituto di Credito (situazione rassicurante), inoltre nella stessa email appariva il chiaro tenore frettoloso e quasi intimidatorio (pressione psicologica);
3) Quindi, gli ufficiali di p.g. operanti con la piena collaborazione della parte acquisivano la email , dalla quale dall'analisi dell ' headers dell'email si risaliva ad un server di invio email anonimizzato ma nel codice della email vi era invece un chiaro collegamento ad un dominio /IP «a href=sitophishing.it» la mia banca «a/»;
4) Il successivo sviluppo del dominio/ip riportava ad uno spazio freee di un noto Provvider italiano, il quale grazie alla attenta attività di analisi e rispondendo prontamente alle richieste dell'A.G. inoltrate tramite P.G. operante, faceva risalire all'autore materiale di tale sito trappola di phishing;
5) La successiva perquisizione/identificazione/sequestro /analisi con modalità secondo i dettami della Legge 48/2000 best practice «Digital Forensic» del Sig. X portava alla precisa ricostruzione delle prove che univocamente riconducevano all'autore del reato;
6) Veniva in particolare trovato il movimento fraudolento di denaro dal conto del truffato verso un conto xx xxx del truffatore;

NOTA TECNICA SU CASO REALE

1) Il semplice sviluppo dell'headers della email incriminata «rimandava ad un sito di invio email anonimizzato» QUINDI FALSA PISTA;

2) Ilcodice sorgente dell'email riportava un chiaro HREF, riconducibile ad uno spazio free di un noto provider;

3) Grazie all aprecisa indicazione dello spazio free occupato della data ora dell'occupazione di tale spazio, il provvider è stato in grado di fornire l'IP della persona che aveva pubblicato la pagina;

4) L'attività di P.G. ha permesso di individuare tutte le prove compreso il flusso di denaro e di restituire anche il maltolto.

5) Questo caso senz'altro denota un carattere di semplicità è di facile risoluzione tecnica, oggi purtroppo il carattere sempre piu' associativo delle «bande specializzate di phishing» unite alle problematiche di estraterritorialità e di normative non omogeneizzate comporta la non facile risoluzione di molti casi.
6) Per questo motivo nuovi strumenti di indagine moderna debbono essere messi in campo «Osint vs ProActive».

Caso reale «il tribunale condanna»

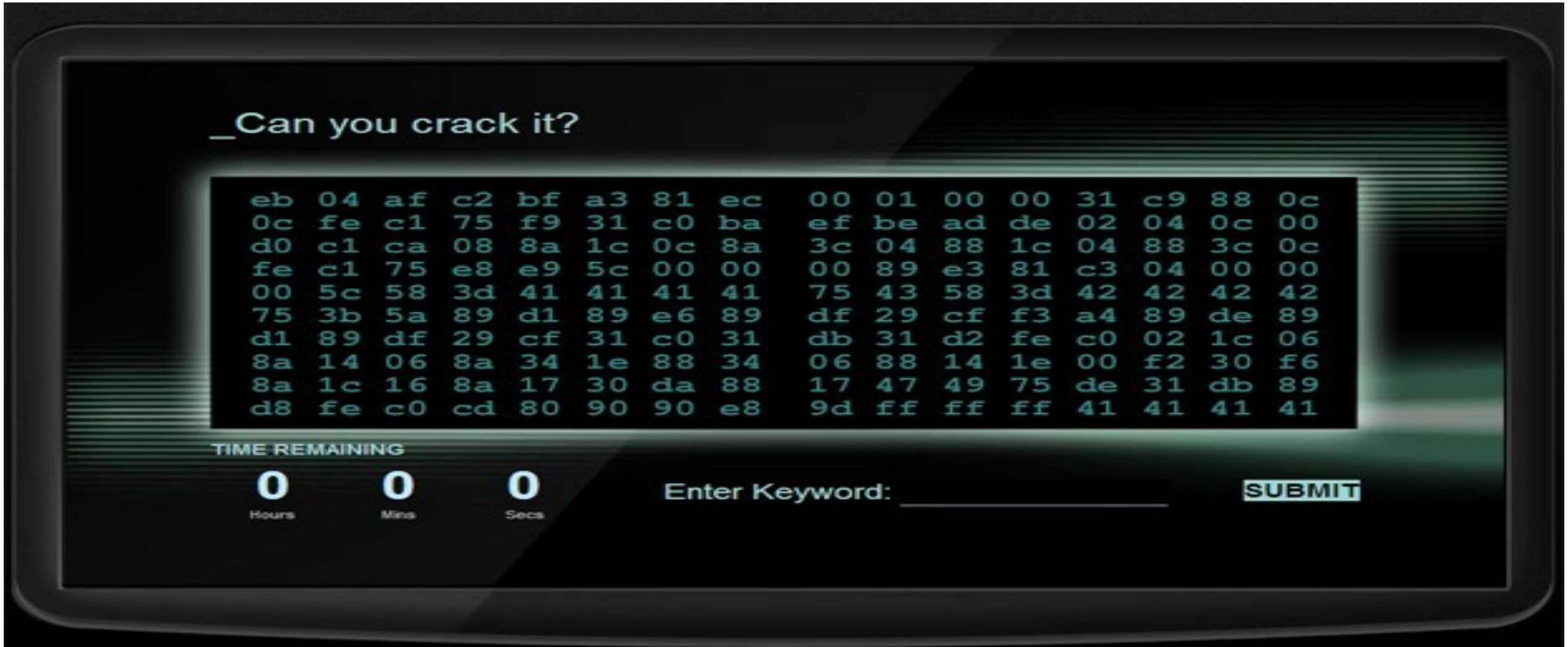
P.Q.M.

Visti gli artt. Di legge 533 e 535 c.p.p.,
Dichiara l'imputato xxx xxx colpevole del reato ascritto (640 ter CP) e, lo condanna alla pena di 6 mesi di reclusione e €. 400,00 dimulta oltra al pagamento delle spese processuali . Pena sospesa.

IMPUTAZIONE

1) Condanna del delitto p. e p. dall'art. 640 ter CP. Perché mediante artifizi e raggiri, consistiti nell'inoltro di una e-mail emulando il sito internet di XXXX XXXXXX – il cui contenuto vantava la vincita di un bonus premio fedeltà, per ottenere ilq uale era neccessario fornire i dati sia personali che della Carta Xxx –xxxx nr. xxxx – xxx –xxx ; in tale modo il Sig. xxx xxxx intervenendo senza diritto sui dati e sulle informazioni contenute in un sistema informatico, riusciva a prelevare dalla carta di yyy yyyyy l'importo di € 8.683,00 ricaricando la sua carta xxxx xxx nr. xxx xxxx e si procurava l'ingiusto profitto di € 8.683,00 con conseguente danno pari danno per il Sig. yyy yyyy .

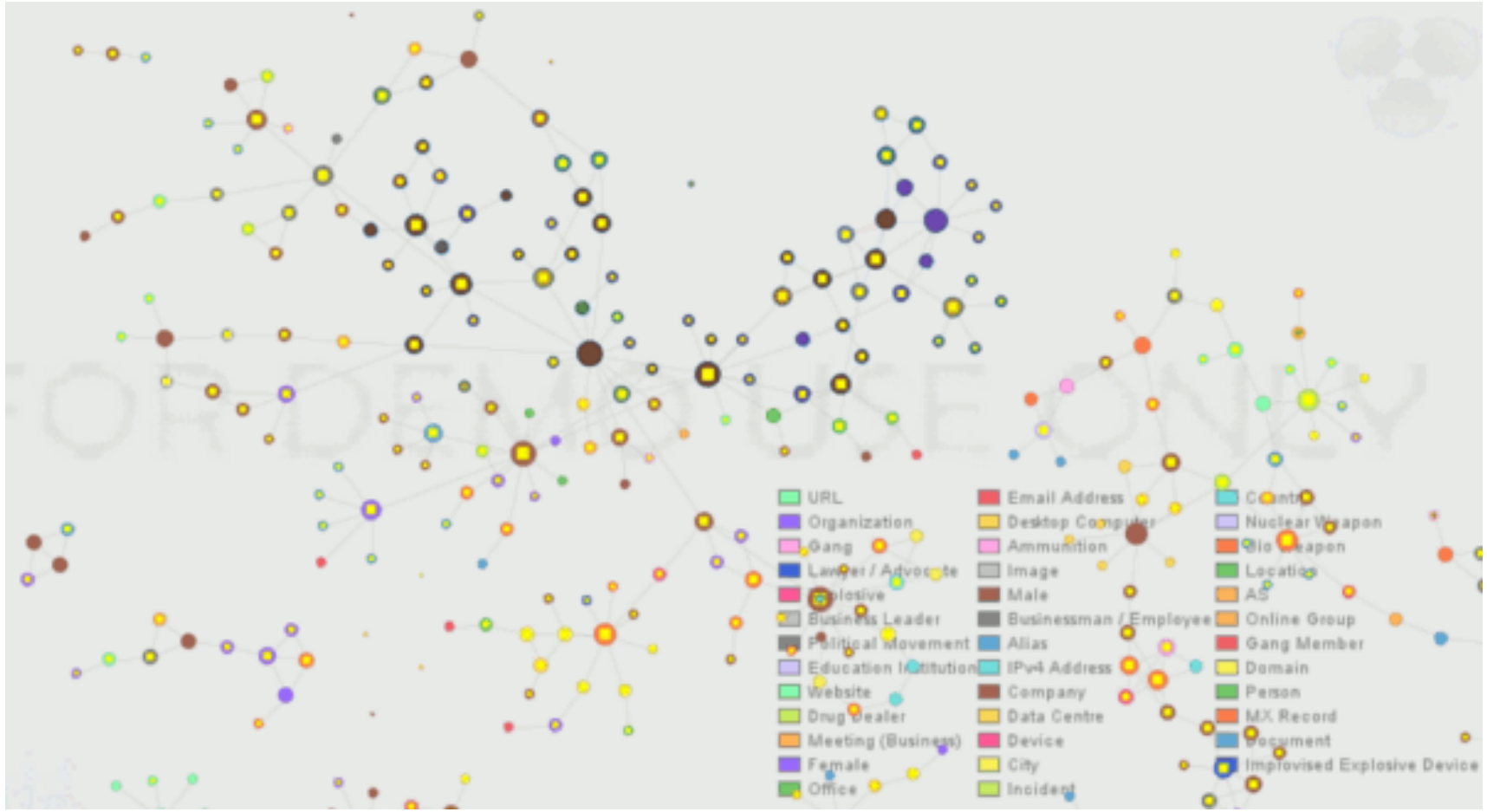
Investigatori hacker?



Un valido aiuto «osint» Open source intelligence.

- L’ausilio dell’attività di Osint (open source intelligence, da non confondere con il software Open Source), unito all’utilizzo delle banche dati in dotazioni alle FF.PP, in una attività (parallelamente ad altre) che sempre di piu’ si svolge su campi di battaglia virtuali (internet) assimetrici.
- TERRITORIALITA’;
- GIURISDIZIONALITA;
- EFFICACIA DELL’AZIONE PENALE;
- STRUMENTI INVESTIGATIVI CLASSICI / OSINT /PROACTIVE;

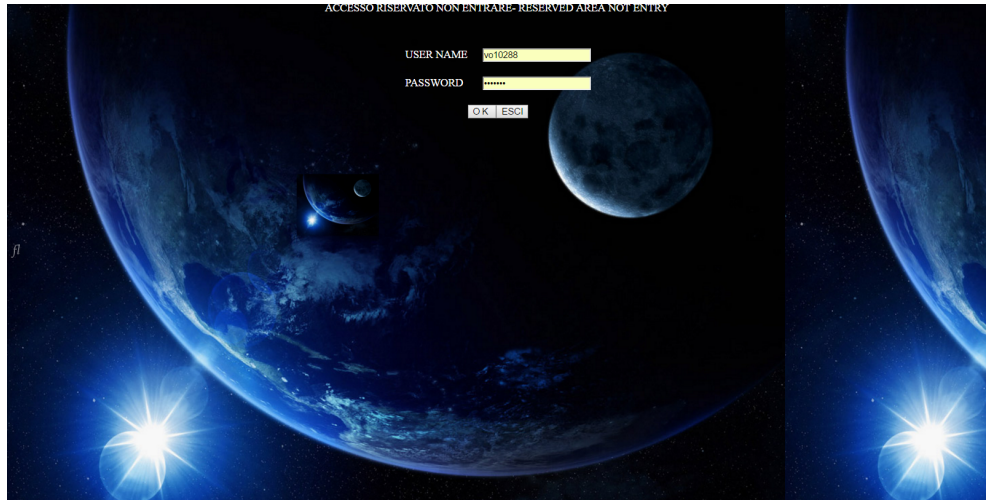
Strumenti CLASSICI di analisi osint



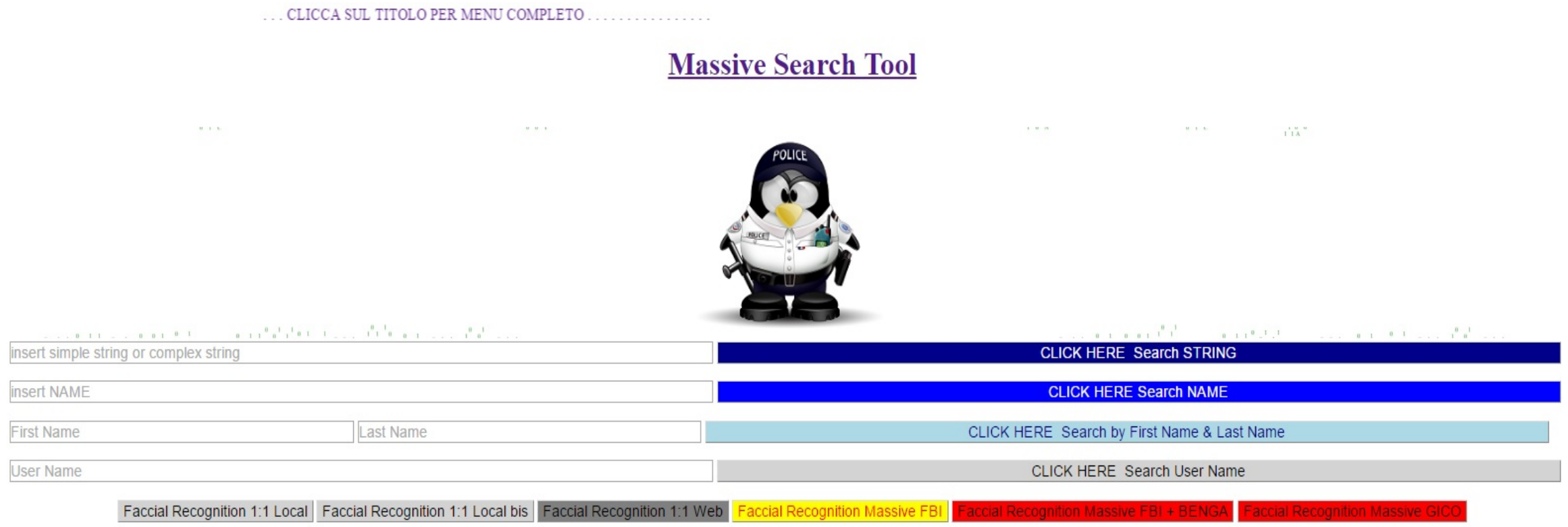
Attività di analisi anche tramite attività di Osint (Open Source Intelligence) e delle relative relazioni sociali per poter risalire ai veri autori ed alle organizzazioni;

Strumenti dedicati per l'analisi delle reti sociali fonti Aperte /chiuse (Archivi FF.PP.).

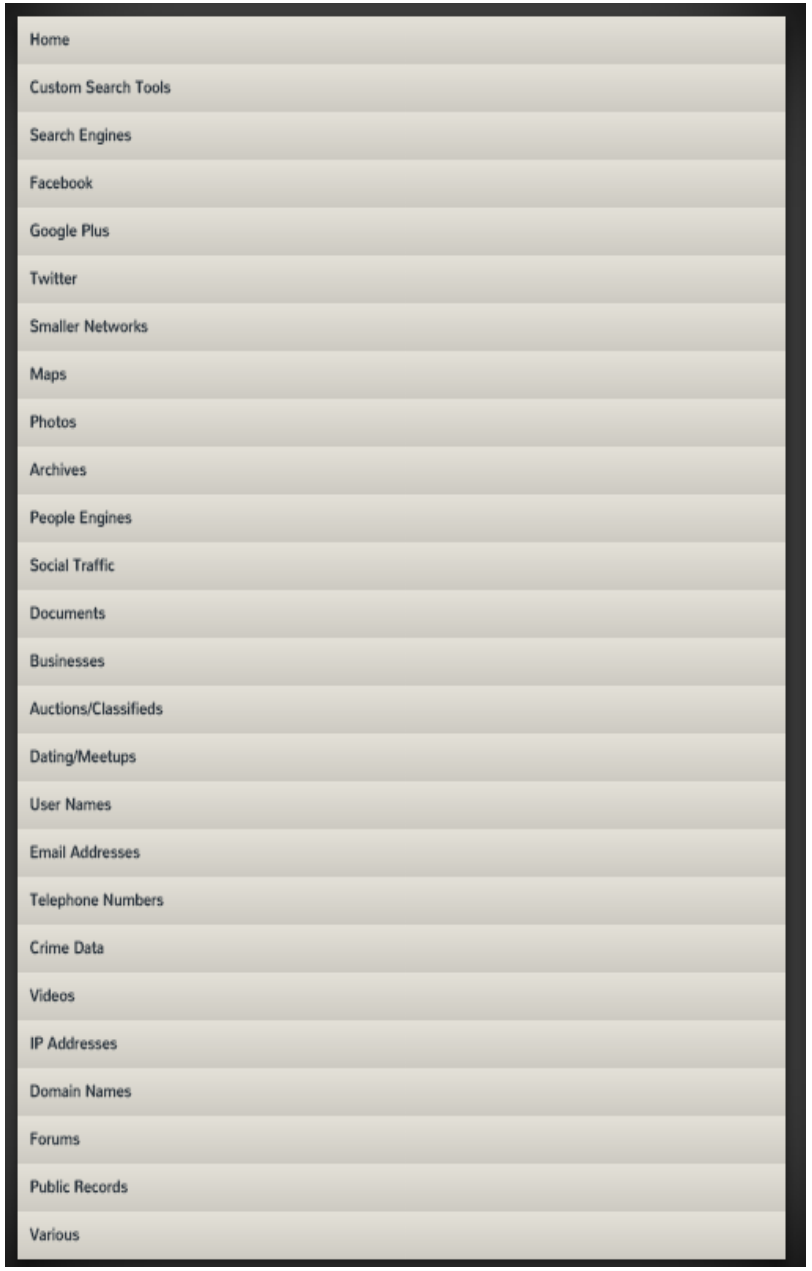
Vecchia piattaforma oSint

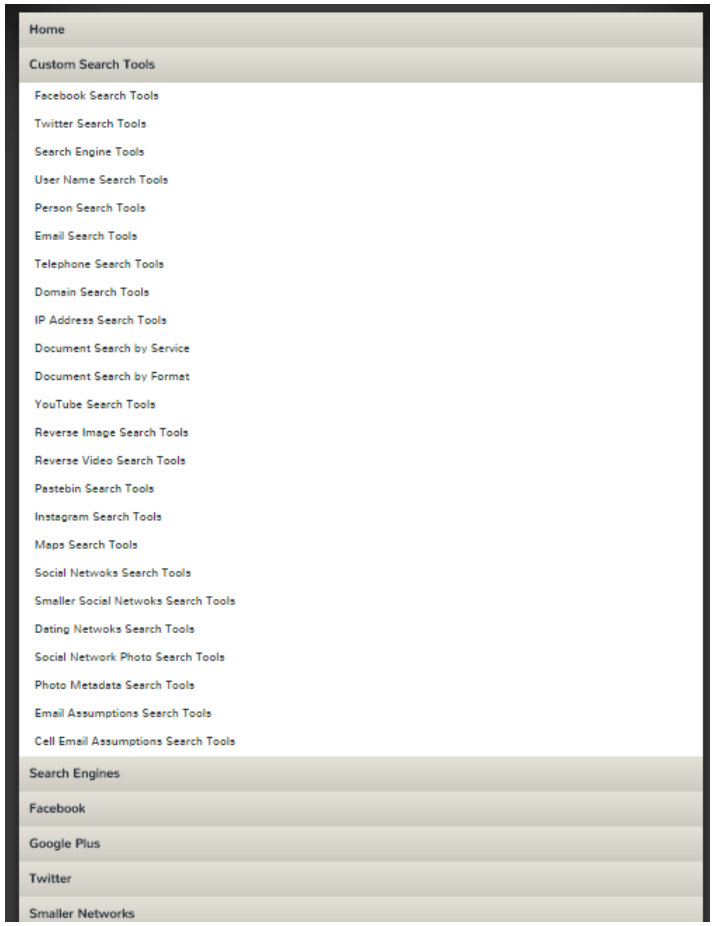


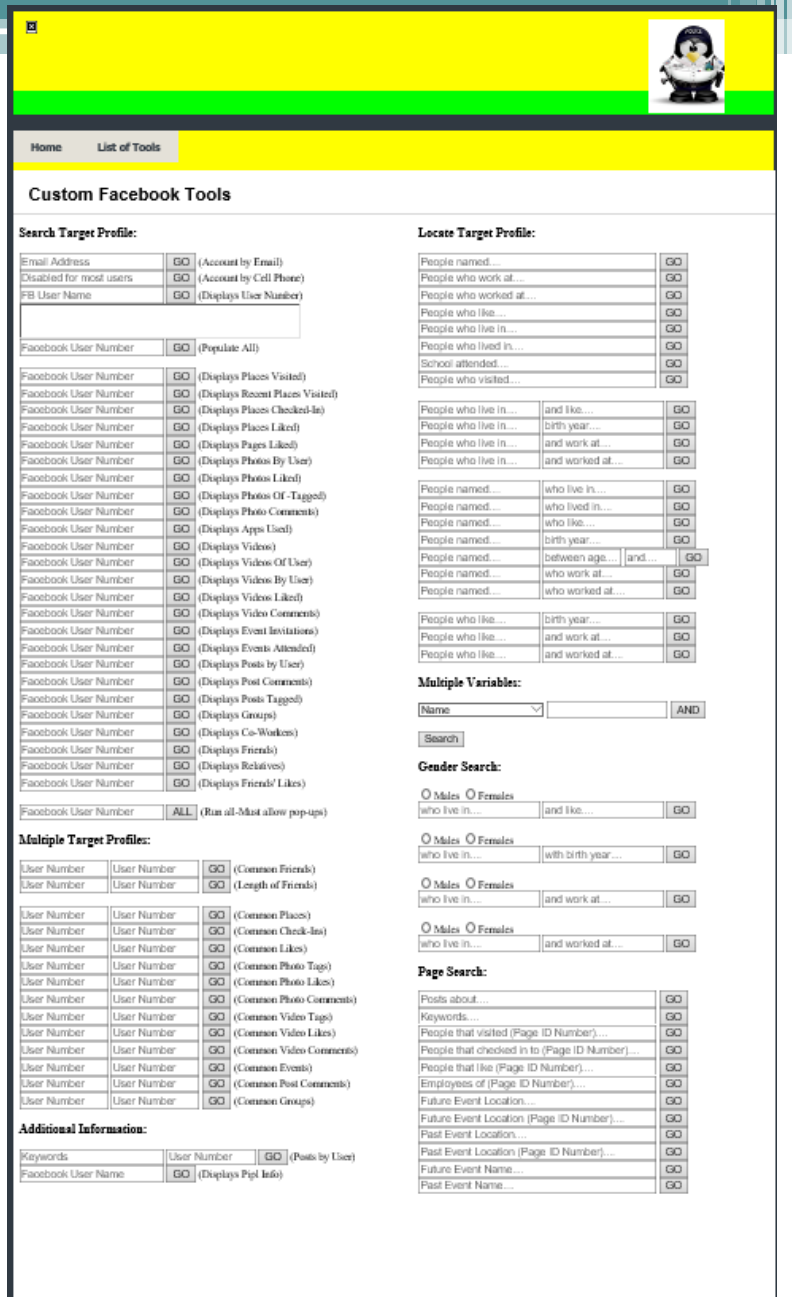
ALCUNE ATTIVITA' CLASSICHE DI INVESTIGAZIONE SUI REATI DI PHISHING QUALI INDAGINI ASSIMETRICHE DA FONTI APERTE – analogamente ad altre tipologie di reato ANCHE TRAMITE SVILUPPO E CREAZIONE DI SOFTWARE .



Menu completo

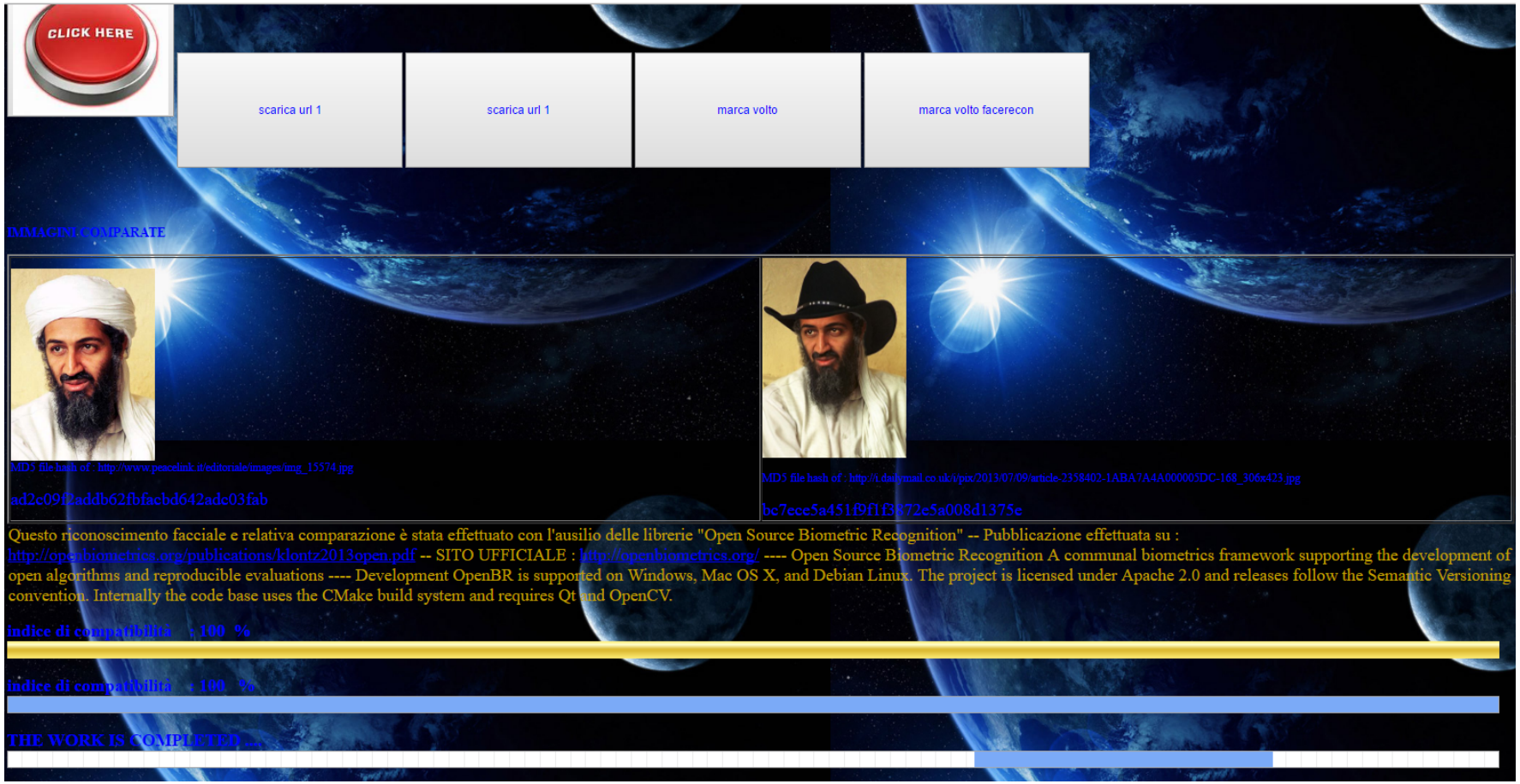




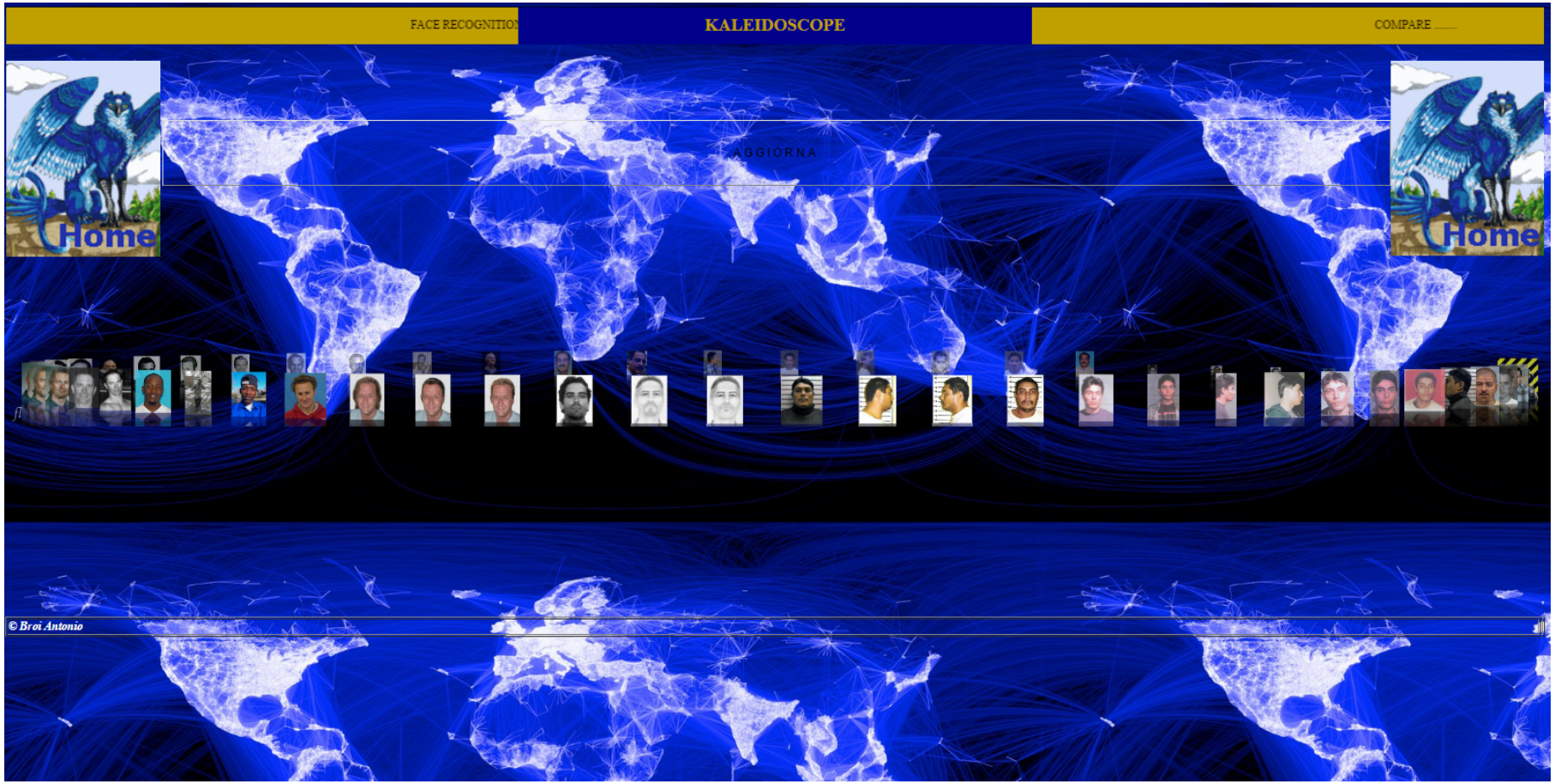


ABBIAMO SEMPRE I DATI DA INCROCIARE??
E' POSSIBILE FARE OSINT ANCHE NEL FACIAL-RECOGNITION & COMPARE MASSIVO? ..... ABBIAMO CREATO UN PICCOLO STRUMENTO (solo d.b.m.s. niente dati raccolti in database !!!!!!!!)

Facial recognition 1 1 web – fonti aperte



Kaleidoscope show circle – fonti aperte



Strumenti proactive

- Eventuale attività piu' incisiva di ProActive intelligence (tracciamenenti sulle email perquisizioni in remoto spyware etc.) **solo previa autorizzazione della A.G.;**
- con unico fine di individuare la territorialità dell'organizzazione criminale e procedere in seguito tramite anche rogatorie internazionali all'attività d'indagine «PROBANTE» con organi collaterali e Forze di Polizia estera all'indagine arresto e raccolta di prove, anche tramite sequestro ed analisi di tutti i dispositivi elettronici dell'organizzazione (server pc cellulari etc.etc.) .
- Per la formalizzazione probatoria della prova.

TECNICHE AVANZATE DI PHISHING - PHARMING

- La tecnica del cosiddetto Phishing, purtroppo viene sempre più usata per il furto di credenziali per operazioni bancarie anche tramite la avanzata tecnica di Pharming (tecnica ancora piu' pericolosa in quanto c'è una manipolazione dei server DNS e l'utente crede davvero di trovarsi nel sito ufficiale), soprattutto per il furto d'identità nei Social Network ma anche per leggere le email altrui, fenomeno questo, molto più grave e di difficile individuazione.
- L'utente ha solo una modalità per difendersi da queste truffe e cioè verificando sempre l'indirizzo del sito (URL), che deve corrispondere all'effettivo registrato e non a server strani.

Alcuni consigli pratici ai naviganti

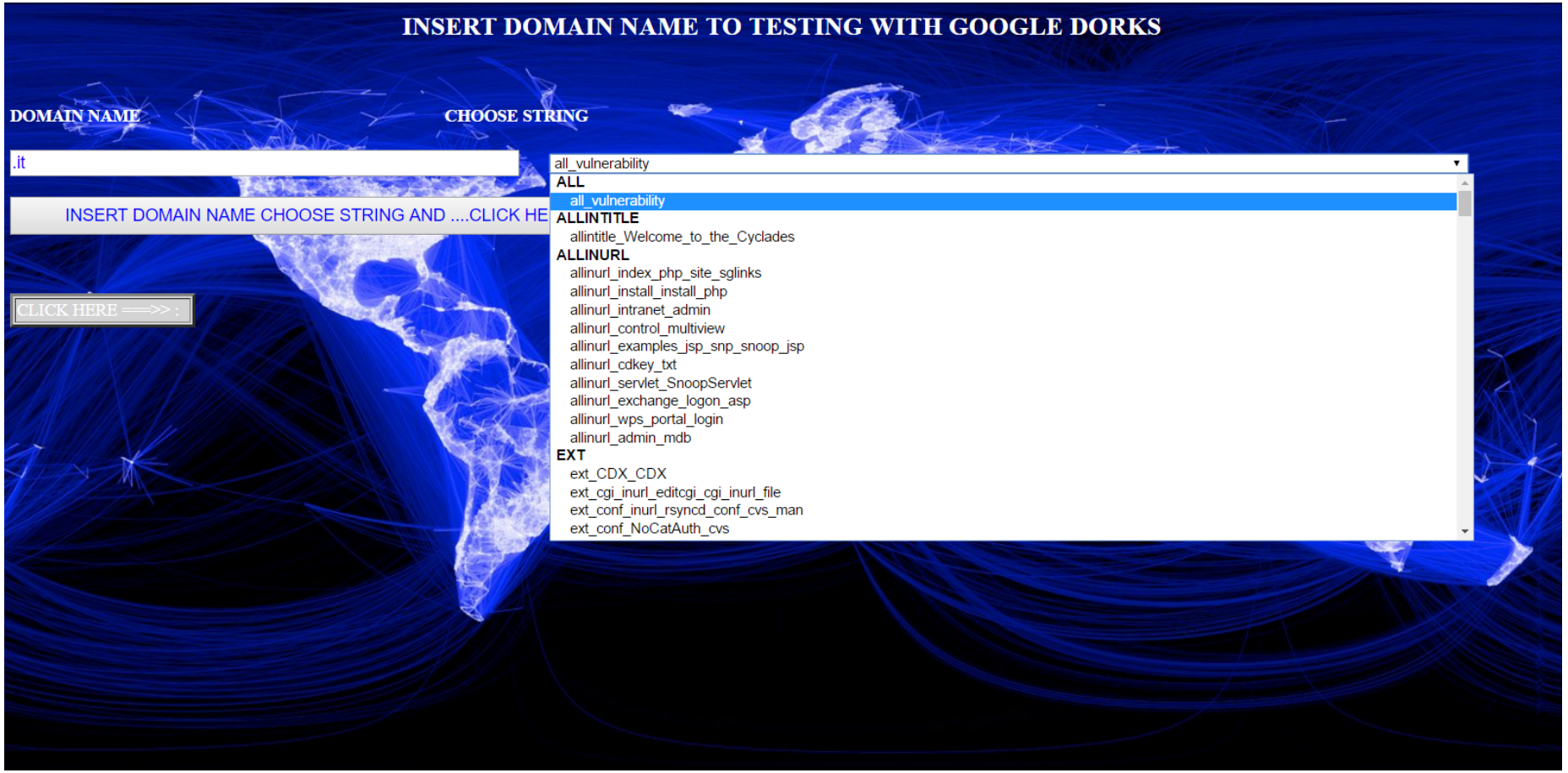
- Si raccomanda sempre di preferire, per le connessioni di navigazione internet riguardanti tutte le transazioni bancarie, le connessioni da reti di nostra proprieta e quindi PRIVATE, rispetto a reti diconnessione PUBBLICHE (la rete cellulare GSM è considerata sicura, ad eccezione di rare forme di intercettazioni abusive cellulare illegale -- poco diffuso, ed attacco illegale da software spia cosiddetti spyware) .
- Nelle connessioni wifi private in particolare possono essere loro stesse degli snodi di «sniffing» o possono avere qualche utente logato alla stessa rete, il quale tramite tecniche di MAN-IN-THE-MIDDLE sniffare tutte le credenziali dei malcapitati, anche le connessioni SSL https con scambio di un certificato creato ad hoc e falsificato);

- SOCIAL ENGINEERING ➔> Inoltre altra raccomandazione ai naviganti e quella di non credere a tutte le email che arrivano sulla posta elettronica (vi ricordate la fiaba del Lupo Cattivo di Cappuccetto Rosso) e portare tanta attenzione all'apertura di allegati delle email ed all'inserimento di credenziali in siti (URL) non verificati almeno a vista e corrispondenti al vero sito Web.
- Gli allegati dannosi non sono soltanto i file .exe ma bensi anche pdf jpg ed altre tipologie!!

Punto di vista dei relatori

- Gli istitui bancari e finanziari e la loro clientela rappresentano i veri target di queste organizzazioni criminali e sono le vittime di queste attacchi criminali spesso su vasta scala (bot-net), veri fenomeni sempre piu' caratterizzati dallo stampo organizzativo-malavitoso ed associativo, dai quali è sempre piu' difficile difendersi.
- Per questo motivo nuovi strumenti debbono essere messi in campo ad arricchimento della difesa del sistema paese.
- Insieme ad una buona e pressante prevenzione divulgativa si potrebbe estendere il campo di prevenzione, effettuando una prevenzione informatico pro-activa e quindi di ricerca di vulnerabilità non solo sulle infrastrutture fisiche ma anche sulle indicizzazioni logiche – ABBIAMO UN PICCOLO PROGRAMMA ANCHE PER QUESTO!.
- Conosciamo meglio le armi del nemico impariamo ad usarle addestrandoci ad usarle per una migliore prevenzione PEN-TESTING –FISICO -LOGICO.

Vulnerability search
cioè ricerca di vulnerabilità logiche – solo per gli addetti ai lavori!!!!!



GRAZIE PER L'ATTENZIONE

Antonio Broi Francesco Crocetti Pallotta