POLIZIA DI STATO
Compartimento Polizia Postale e delle Comunicazioni
"Piemonte-Valle d'Aosta"

Il Cybercrime: l'evoluzione e le indagini di polizia giudiziaria

UNIONE INDUSTRIALE TORINO
Torino – 14 Novembre 2018

***Dott. Ing. Giuseppe ZUFFANTI**, Direttore Tecnico Principale della Polizia di Stato*
compartimento.polposta.to@pecps.poliziadistato.it Tel. 011/3014611

Cos'è il Cyber-Crime?

- Un crimine come tutti gli altri, ma con l'aggiunta della componente informatica, che può essere il mezzo e/o il fine del crimine.


Technology as Instrument
Technology as Target
Mass Marketing Fraud
Money Laundering
Hacking for Criminal Purposes
Identity Theft
Child Exploitation
Cybercrime
Criminal Botnet Operations
Intellectual Property infringements
Cyberbullying
Malware Threats
Internet-based Drug Trafficking
Distributed Denial of Service
National Security offences

Catturare soldi e catturare informazioni

INFORMAZIONI = SOLDI

⇩

POSSEDERE DATI = AVERE POTERE

«Per controllare un popolo non serve invaderlo, basta avere accesso ai dati dei cittadini e saperli usare per orientare decisioni e scelte»

L'humus per le Nuove Organizzazioni Criminali

- Largo uso di nuovi sistemi di pagamento
- Velocità di realizzo
- Vulnerabilità della rete (sicurezza informatica)
- Anonimato
- Trasnazionalità

Tutti Siamo Potenziali Bersagli

- Il **Cybercrime** (sottrarre informazioni/denaro) → **prima causa di attacchi gravi a livello mondiale** con il 76% degli attacchi complessivi, in crescita del 14% rispetto al 2016.

- In aumento gli attacchi sferrati con finalità di **Information Warfare** +24% e il **Cyber Espionage** +46%.

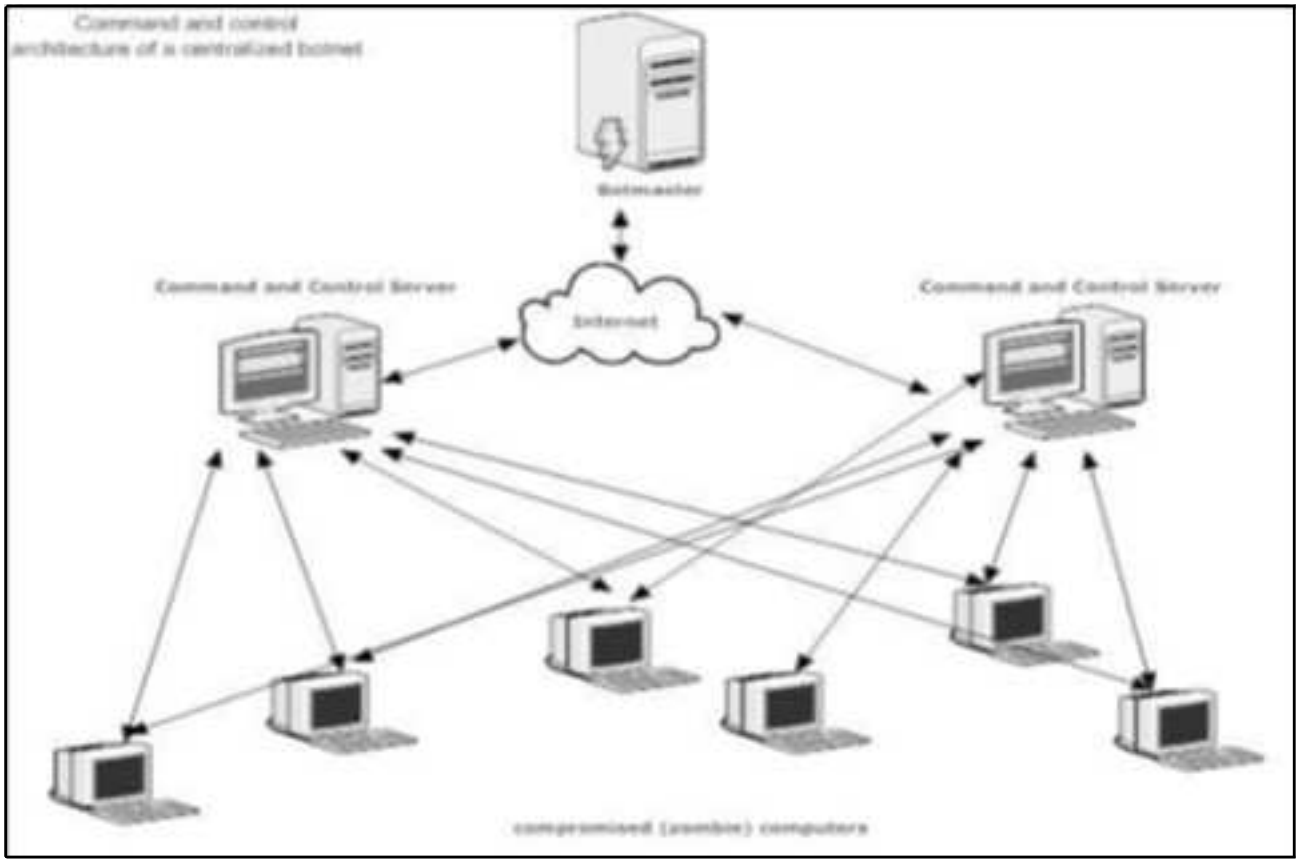
- Costi generati globalmente dalle sole attività del **Cybercrime** quintuplicati, stimati **500 miliardi $ nel 2017**.

- **180 miliardi $** la perdita stimata per truffe, estorsioni, furti di denaro e dati personali.

  - Il **Malware** è l'arma più utilizzata
  - **MultipleThreats/APT**
  - **Phishing/Social Engineering/Spear Phishing/BEC**

Video: Mappa Interattiva Attacchi

Esempio di Distributed Denial-of-Service (**DdoS**) le **BOTNET**



POLIZIA DI STATO
Compartimento Polizia Postale e delle Comunicazioni
"Piemonte-Valle d'Aosta"

!!! Internet of Things !!!

POLIZIA DI STATO
Compartimento Polizia Postale e delle Comunicazioni
"Piemonte-Valle d'Aosta"

POLIZIA DI STATO
Compartimento Polizia Postale e delle Comunicazioni
"Piemonte-Valle d'Aosta"

LONDRA : Heathrow Airport Fined £120,000 Over Lost USB Drive (October 8, 2018)

L'UK Information Commissioner's Office ha sanzionato Heathrow Airport con una multa di circa $157,000 USD per la perdita di una USB pendrive che conteneva dati sensibili riguardanti la sicurezza dell'aeroporto.

I dati contenevano, ad esempio, i percorsi di sicurezza delle pattuglie di polizia, i posizionamenti delle telecamere di sicurezza a circuito chiuso nonché molte altre informazioni relative alla sicurezza aeroportuale di Heatrhow.

La USB stick è stata trovata da un privato cittadino nell'Ottobre 2017.

Il contenuto è stato visualizzato all'interno di una biblioteca e poi la chiavetta usb è stata consegnata ad un giornale che si è fatto propria copia delle informazioni ed ha restituito la pen drive all'aeroporto londinese.

La chiavetta USB era priva di qualsiasi sistema di criptazione dei dati e di protezione con password.

POLIZIA DI STATO
Compartimento Polizia Postale e delle Comunicazioni
"Piemonte-Valle d'Aosta"

PHISHING

INTESA SANPAOLO IL GRUPPO CORPORATE BANCHE ESTERE

Gentile cliente,

La sua password e scaduta, sono pasati piu di 90 giorni da quando la sua password non e stata cambiata.

Per motivi di sicurezza, e pregato di cambiare subito la sua password, altrimenti la sua carta diventa inativa.

E possibile creare una nuova password seguendo i passaggi successivi.

La procedura e molto semplice:
1 - Cliccare sul link qui sotto per aprire una finestra del browser.
2 - Confermare i dati richesti e segui le istruzioni.

https://www.intesasanpaolo.com/script/ServiceLogin/ib/login

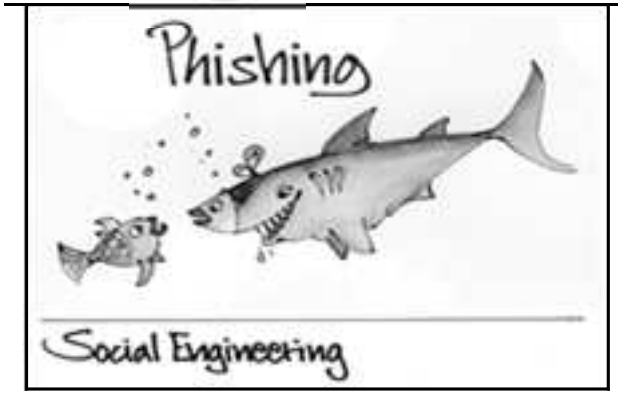
Cordiali saluti,
INTESA SAN PAOLO

Test: 19mila utenti di 144 Paesi con un Phishing Quiz

I risultati sono preoccupanti:

- davanti a 10 email solo il 3% degli interpellati è riuscito a distinguere quelle "autentiche" da quelle di phishing
- mentre l'80% non ha identificato almeno una email di phishing, condizione sufficiente per cadere vittima di un attacco.

POLIZIA DI STATO
Compartimento Polizia Postale e delle Comunicazioni
"Piemonte-Valle d'Aosta"

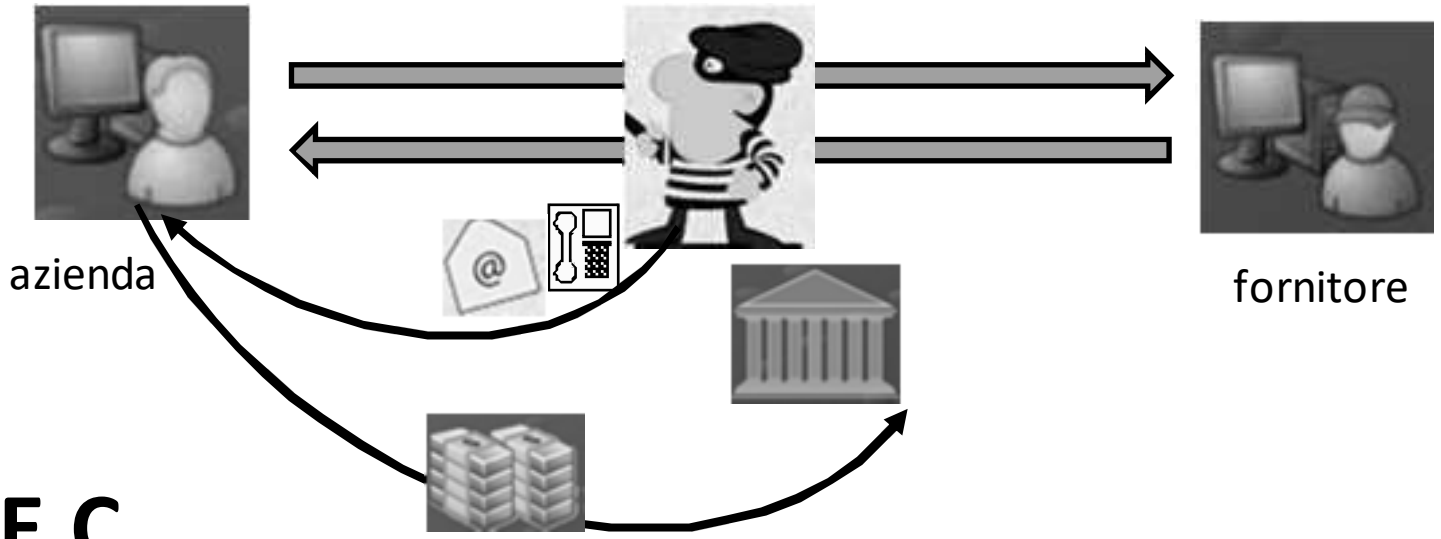


Business Email Compromise e CEO Fraud

Sistema di truffa attuato tramite la compromissione di e-mail con l'obiettivo di ingannare i dipendenti aziendali ovvero clienti ad effettuare un trasferimento di fondi a beneficio dei truffatori.

Le frodi di tipo BEC si rivolgono principalmente alle aziende che svolgono regolarmente bonifici con fornitori/terze parti estere.

Ecco alcune modalità con cui è realizzata la truffa BEC



B.E.C.

Es: Ad una azienda che ha un rapporto con un fornitore da diverso tempo viene chiesto di pagare una fattura mediante bonifico. La richiesta viene effettuata via telefono, fax o e-mail.

Se effettuata via e-mail verrà utilizzato un indirizzo molto simile a quello del fornitore.

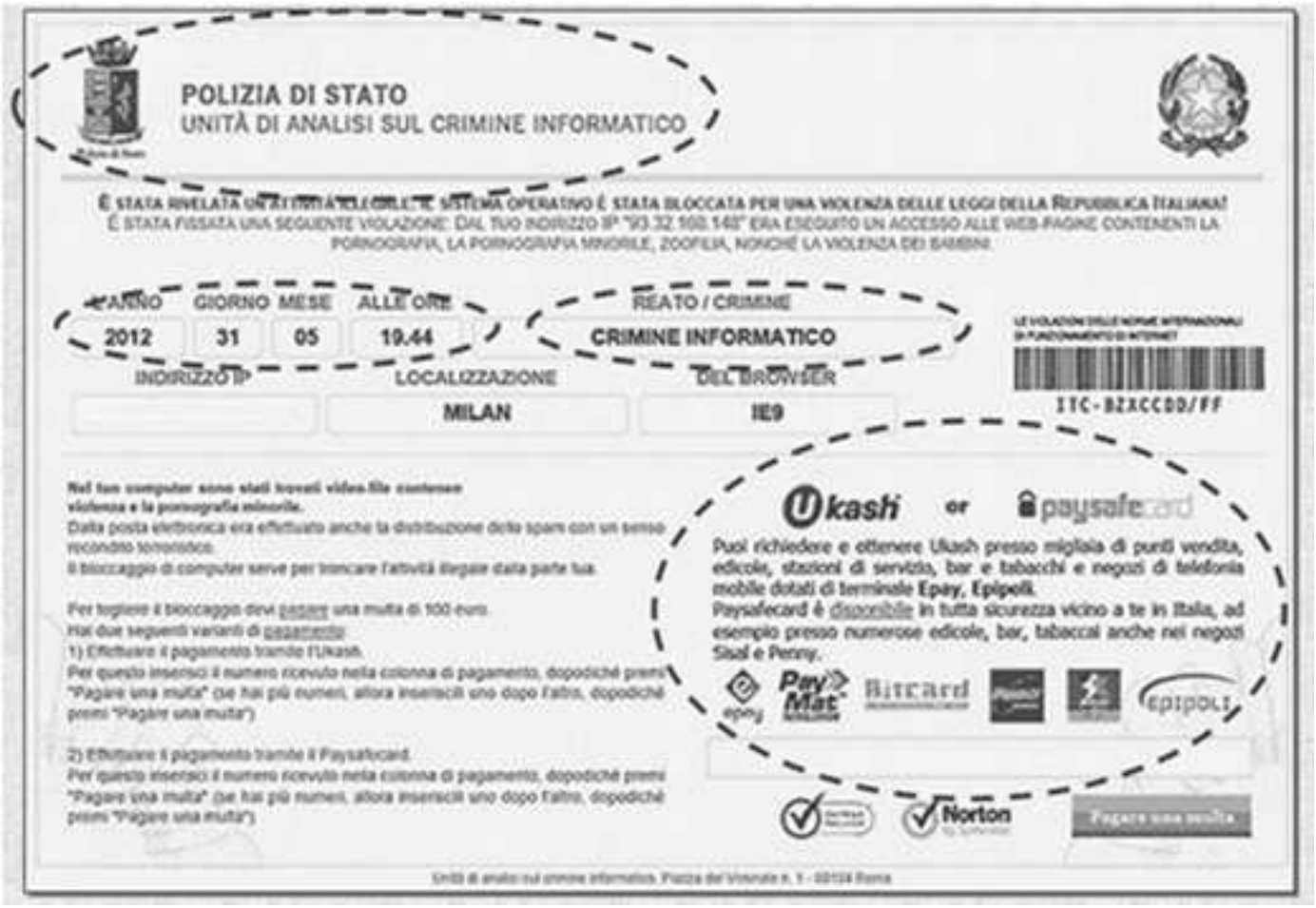
POLIZIA DI STATO
Compartimento Polizia Postale e delle Comunicazioni
"Piemonte-Valle d'Aosta"

SMISHING

VISHING

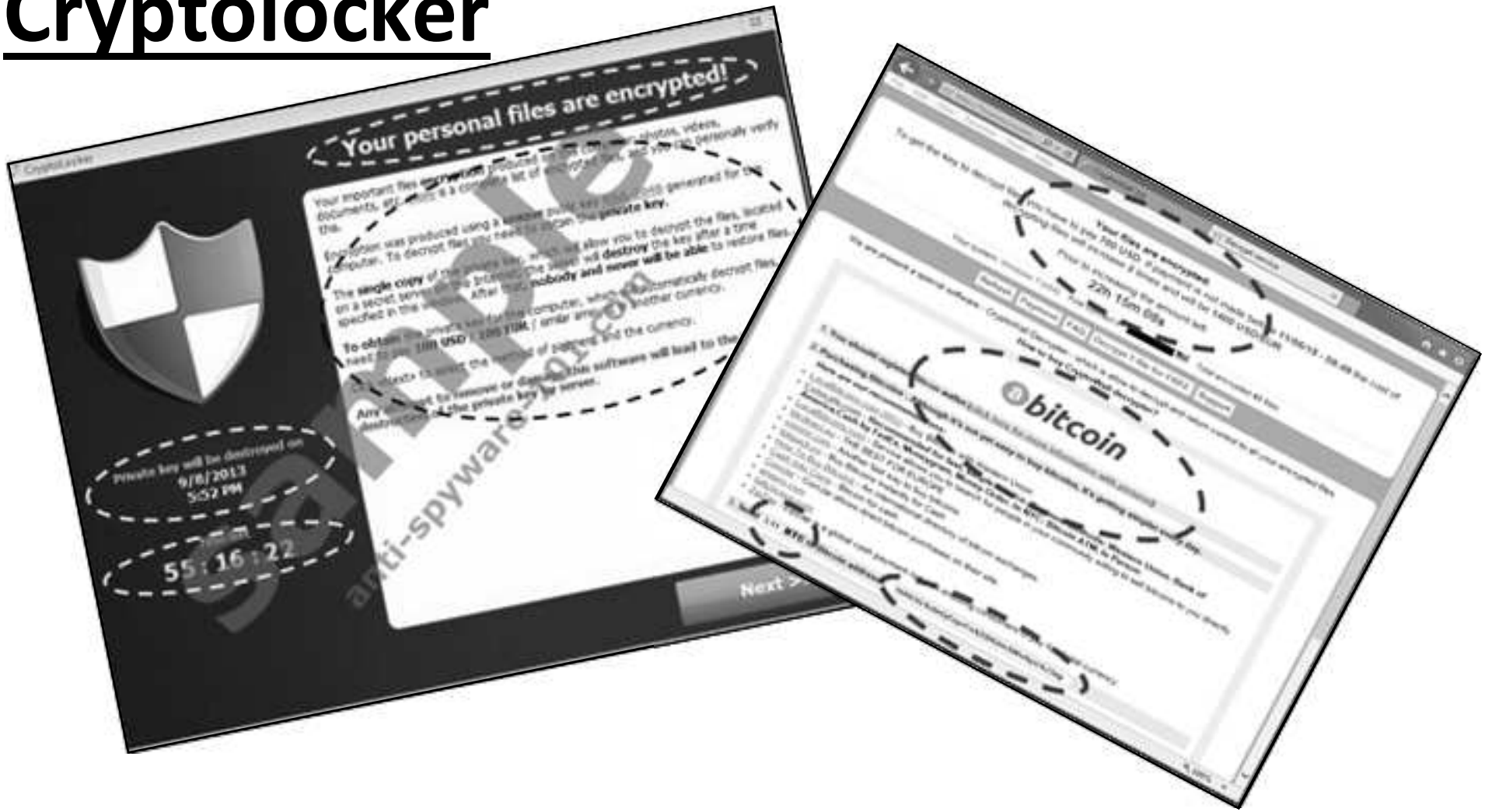
POLIZIA DI STATO
Compartimento Polizia Postale e delle Comunicazioni
"Piemonte-Valle d'Aosta"

Ransomware le prime versioni

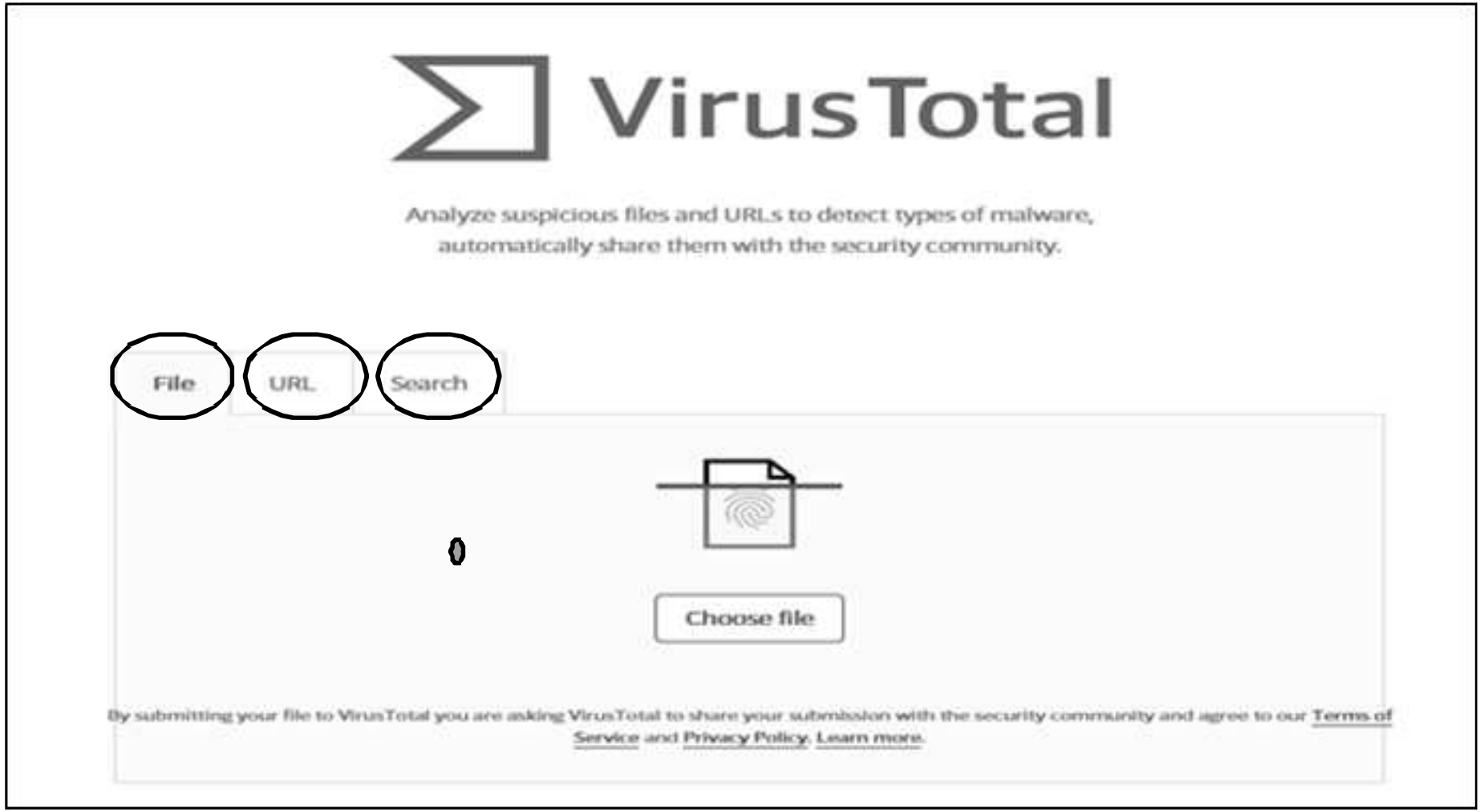


POLIZIA DI STATO
Compartimento Polizia Postale e delle Comunicazioni
"Piemonte-Valle d'Aosta"

Cryptolocker



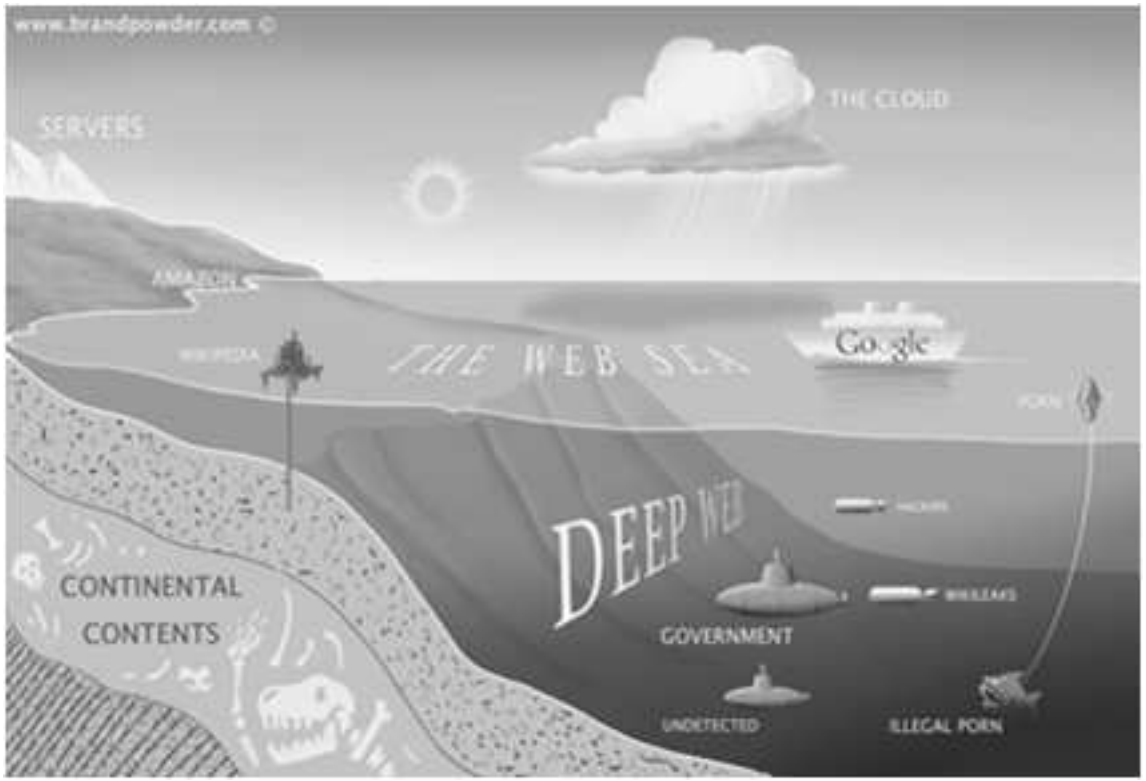
www.virustotal.org



POLIZIA DI STATO
Compartimento Polizia Postale e delle Comunicazioni
"Piemonte-Valle d'Aosta"

www.nomoreransom.org

Il DEEP WEB

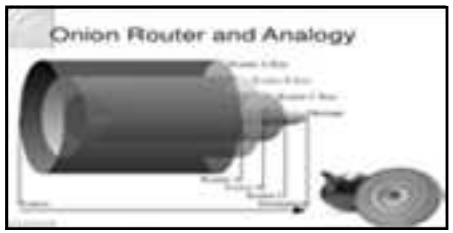


La rete internet è come immenso oceano, il browser, associato ad un motore di ricerca, sarà come una barca.

Questi mezzi permettono di navigare in superficie, ma esiste un intero mondo al disotto di più di 200 volte maggiore di quello che i normali motori di ricerca, come google, yahoo, msn search e bing, riescono a fornire.

Reti Anonimizzatrici

Es: Rete TOR



BLACK MARKET

POLIZIA DI STATO
Compartimento Polizia Postale e delle Comunicazioni
"Piemonte-Valle d'Aosta"

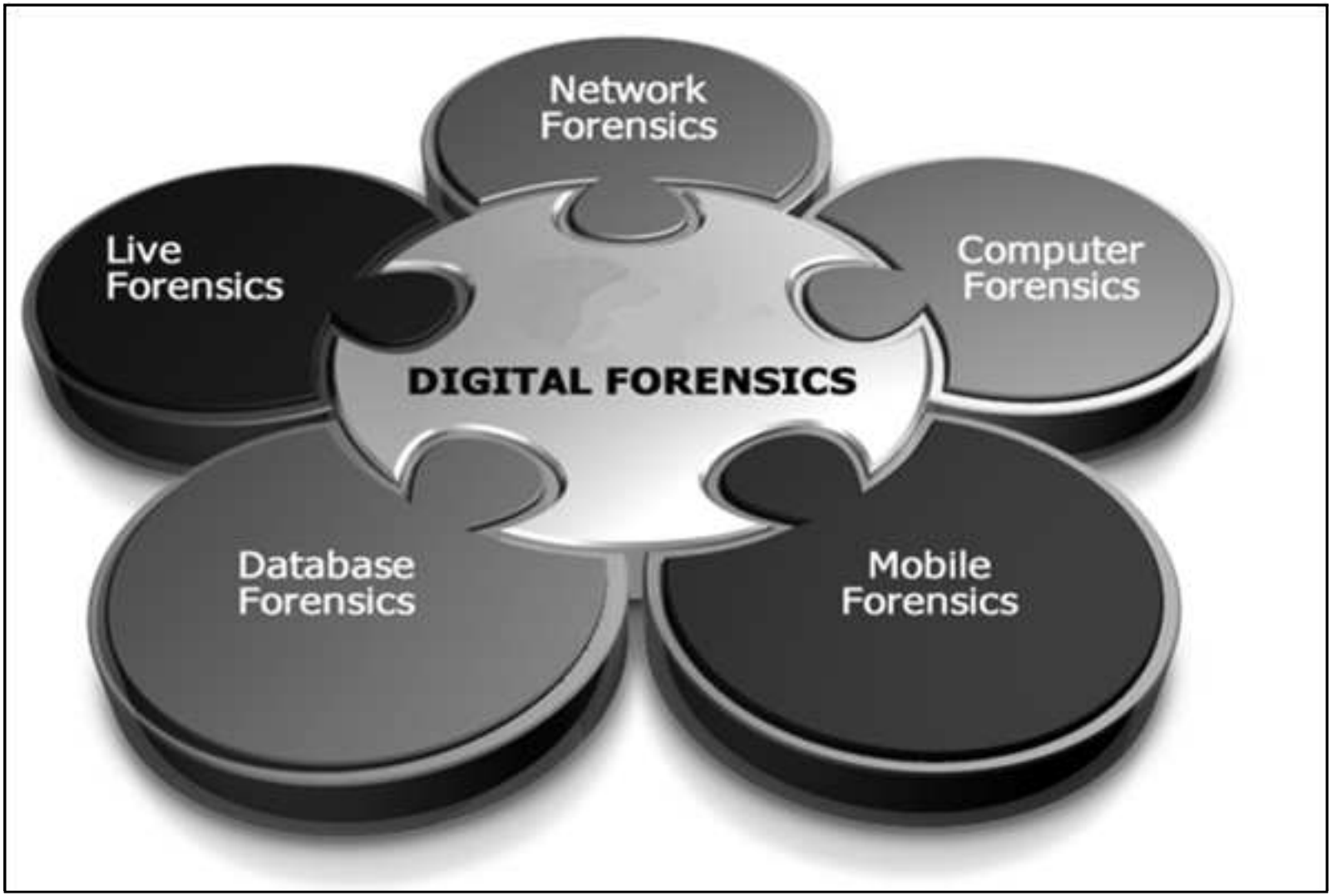
L'Indagine Informatica

- *Ricerca di elementi riferiti ad un **reato on line**;*
  Indirizzi IP, nickname e identità chat, indirizzi e-mail, tabulati telefonici, log, cloud, ecc….

- *Ricerca di elementi all'interno di **dispositivi informatici**;*
  nickname e identità chat, indirizzi e-mail, contatti, connessioni, utilizzatori, cronologia, file temporanei, file pedopornografici, fonti di prova, ecc.. (anche nello spazio di memoria non allocato)

INDIRIZZO IP, LOG FILES

- *Quando un utente si "collega" ad un Internet Service Provider (ISP) la sua connessione ad Internet sarà "loggata"*
- *All'utente riconosciuto dal sistema viene assegnato un **numero di IP dinamico** (se non è attivo un abbonamento internet con IP statico) che seguirà la sua navigazione e che identificherà il dispositivo collegato in rete.*


Network Forensics
Live Forensics
Computer Forensics
DIGITAL FORENSICS
Database Forensics
Mobile Forensics

Reati Informatici (alcuni esempi)

- ***Art. 640 ter c.p.*** *- **Frode informatica** alterare un sistema informatico allo scopo di procurarsi un ingiusto profitto «**[…]** è punito con la RECLUSIONE da 6 mesi a 3 anni e con la multa da euro 516 a euro 1032. La pena è della reclusione da 1 a 5 anni e della multa da euro 309 a euro 1549 se […] se il fatto è commesso con abuso della qualità di operatore del sistema. […]".*
- ***Art. 615 ter c.p. - Accesso abusivo** ad un sistema informatico o telematico […] è punito con la reclusione fino a tre anni*
- ***Art. 615 quater c.p. - Detenzione e diffusione abusiva di codici di accesso** a sistemi informatici e telematici*
- ***Art. 615 quinquies c.p.*** *- **Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere** un sistema informatico o telematico […] è punito con la reclusione sino a due anni*
- ***Art. 617 quinquies c.p - Chi installa apparecchiature dirette ad intercettare, interrompere o impedire comunicazioni** informatiche è punito con la reclusione da uno a quattro anni […]*
- ***Art. 617 sexies c.p** Chi falsifica, altera o sopprime o falsifica la comunicazione informatica acquisita mediante l'intercettazione*
- ***Art. 635 bis c.p. Chi distrugge, deteriora, cancella, dati, informazioni o programmi informatici***
- ***Art. 493 ter c.p. Indebito utilizzo e falsificazione di carte di credito e di pagamento***

È necessario implementare tecniche di OSINT e

tecniche di Big Data analysis

GRAZIE PER L'ATTENZIONE

www.poliziadistato.it
www.commissariatodips.it
https://it-it.facebook.com/AgenteLisa
it-it.facebook.com/unavitadasocial

***Dott. Ing. Giuseppe ZUFFANTI**, Direttore Tecnico Principale della Polizia di Stato*

compartimento.polposta.to@pecps.poliziadistato.it
Tel. 011/3014611