



**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**



**POLIZIA DI STATO**  
**Compartimento Polizia Postale e delle Comunicazioni**  
**“Piemonte-Valle d’Aosta”**

---



**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.



**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"

---

**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»*



**POLIZIA DI STATO**  
**Compartimento Polizia Postale e delle Comunicazioni**  
**“Piemonte-Valle d’Aosta”**

---

## **L’humus per le Nuove Organizzazioni Criminali**

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





**POLIZIA DI STATO**  
**Compartimento Polizia Postale e delle Comunicazioni**  
**“Piemonte-Valle d’Aosta”**

## **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**





**POLIZIA DI STATO**  
**Compartimento Polizia Postale e delle Comunicazioni**  
**“Piemonte-Valle d’Aosta”**

---

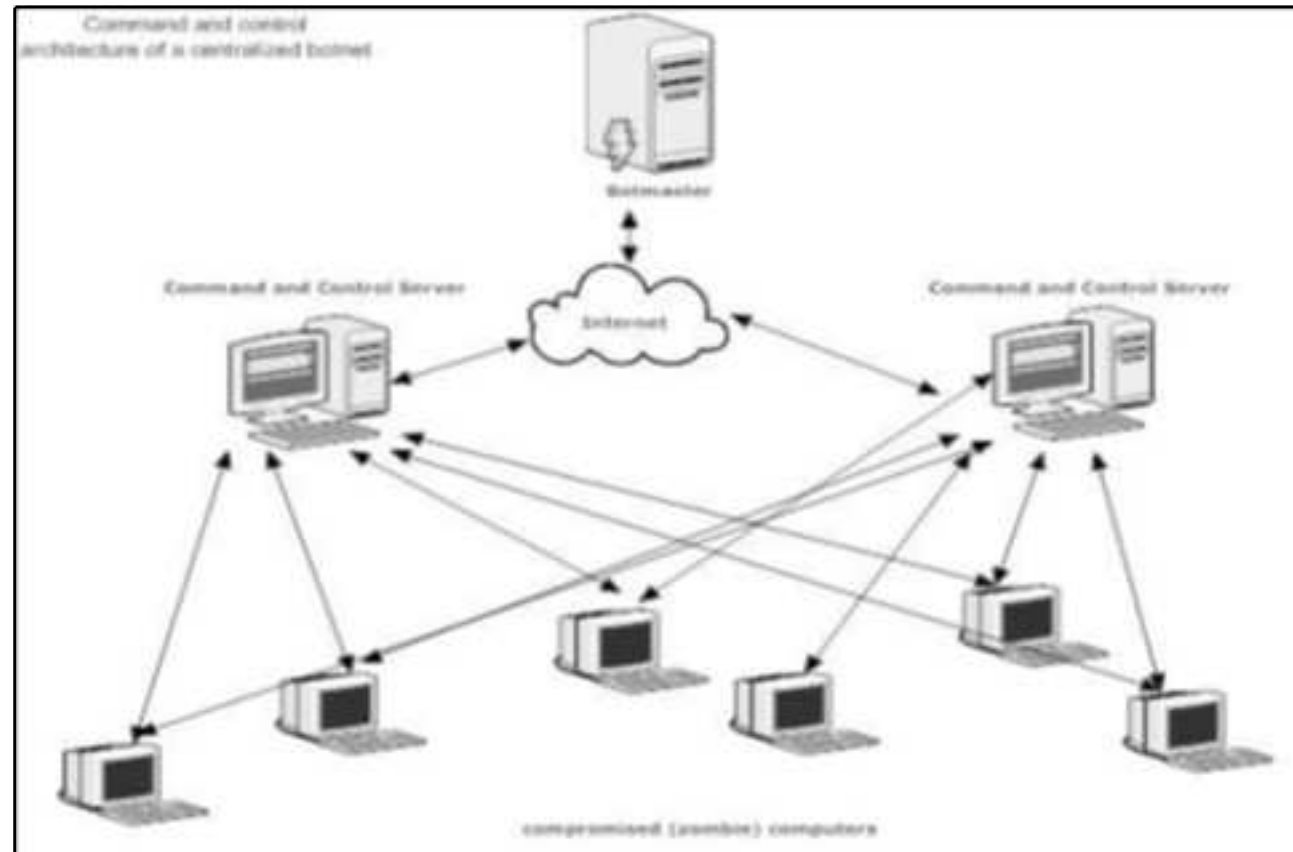
# **Video: Mappa Interattiva Attacchi**





**POLIZIA DI STATO**  
**Compartimento Polizia Postale e delle Comunicazioni**  
**“Piemonte-Valle d’Aosta”**

# 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”

SHODAN

admin 1234

Search





**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 Heathrow.

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 è scaduta, sono passati più di 90 giorni da quando la sua password non è stata cambiata.

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

È possibile creare una nuova password seguendo i passaggi successivi.

La procedura è molto semplice:

- 1 - Cliccare sul link qui sotto per aprire una finestra del browser.
- 2 - Confermare i dati richiesti e seguire le istruzioni.

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

Cordiali saluti,  
INTESA SAN PAOLO



**POLIZIA DI STATO**  
**Compartimento Polizia Postale e delle Comunicazioni**  
**“Piemonte-Valle d’Aosta”**

---



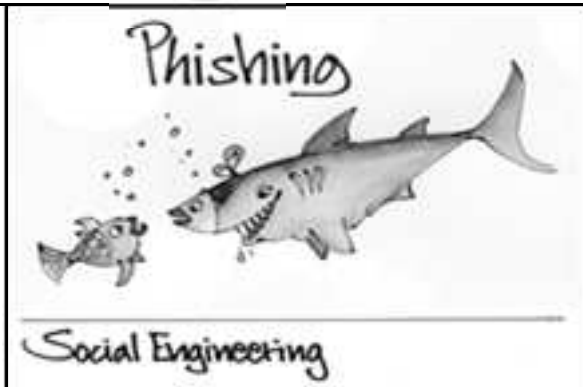
## **Test: 19mila utenti di 144 Paesi con un Phishing Quiz**

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

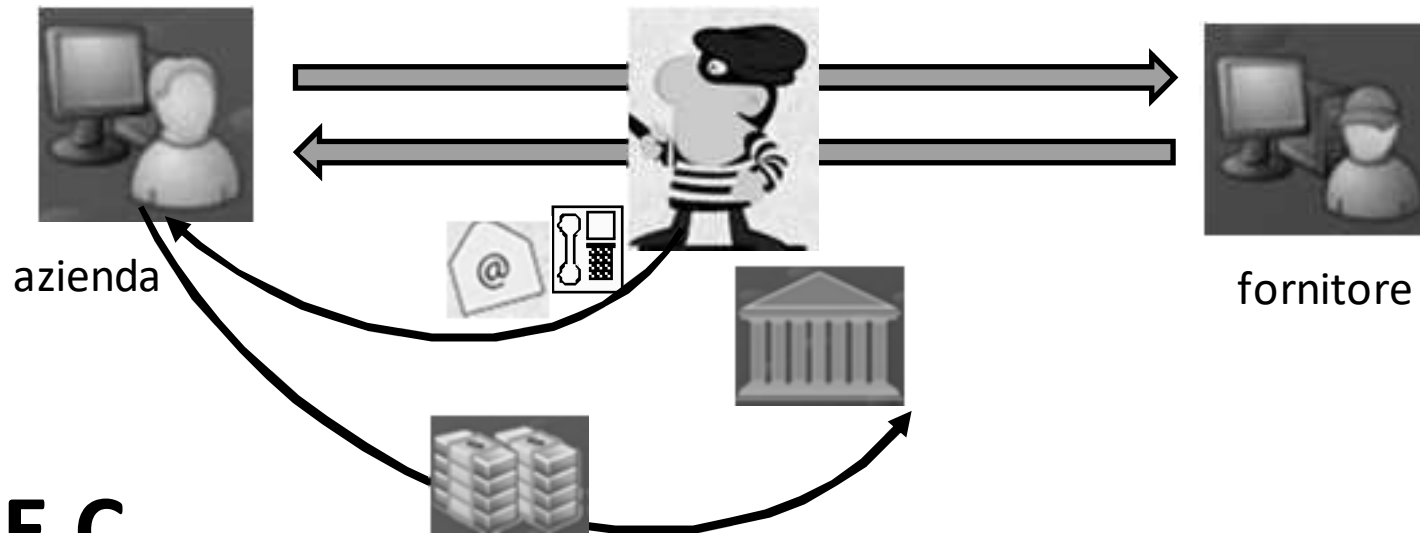
Sistema di truffa attuato tramite la compromissione di e-mail con l'obiettivo di ingannare i dipendenti aziendali ovvero clienti ad effettuare un trasferimento di fondi a beneficio dei truffatori.

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



**POLIZIA DI STATO**  
**Compartimento Polizia Postale e delle Comunicazioni**  
**“Piemonte-Valle d’Aosta”**



## **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



**GSM Modem Pool 8 ports for Wavecom Q2303 Module USB AT Commands Dual Frequency**

**\$198.99**  
Buy It Now  
Free Shipping  
7 watching · **9 sold**

[View Details](#)

Condition: **New**  
Time left: **9h 3m**  
Item location: **China**  
Sold by: **nikolastm (4409\*)**

(GSM Modem with industrial-grade Wavecom Q2303 module. Wavecom Module Q2303 Q2403 Q2406 Q2406B Q24 plus. 8 Ports GSM Modem USB interface 900/1500 MHz. P lease refer to the GSM World Coverage Map ) Co...

# VISHING







**POLIZIA DI STATO**  
**Compartimento Polizia Postale e delle Comunicazioni**  
**“Piemonte-Valle d’Aosta”**



# Ransomware le prime versioni



**POLIZIA DI STATO**  
**UNITÀ DI ANALISI SUL CRIMINE INFORMATICO**

È STATA RIVELATA UN'AUTENTICA TELECOMETE. IL SISTEMA OPERATIVO È STATA BLOCCATA PER UNA VIOLAZIONE DELLE LEGGI DELLA REPUBBLICA ITALIANA!  
È STATA FISSATA UNA SEGUENTE VIOLAZIONE: DAL TUO INDIRIZZO IP "93.32.108.140" ERA ESECUITO UN ACCESSO ALLE WEB-PAGINE CONTENENTI LA PORNOGRAFIA, LA PORNOGRAFIA MINORILE, ZOOFILIA, NOME CHE LA VIOLAZIONE DEI BAMBINI.

ANNO: 2012 | GIORNO: 31 | MESE: 05 | ALLE ORE: 19.44

INDIRIZZO IP: [ ] LOCALIZZAZIONE: MILAN REATO / CRIMINE: CRIMINE INFORMATICO DEL BROWSER: IE9

LE VIOLAZIONI DELLE NORME INTERNAZIONALI DI FUNZIONAMENTO DI INTERNET: ITC-B2XCCDD/FF

Nel tuo computer sono stati trovati video file contenenti violenza e la pornografia minorile.  
Dalla posta elettronica era effettuato anche la distribuzione della spams con un senso ricolando terrorismo.  
Il bloccaggio di computer serve per troncane l'attività illegale dalla parte tua.

Per togliere il bloccaggio devi pagare una multa di 100-euro.  
Hai due seguenti varianti di pagamento:  
1) Effettuare il pagamento tramite l'Ukash.  
Per questo inserisci il numero ricevuto nella colonna di pagamento, dopodiché premi "Pagare una multa" (se hai più numeri, allora inseriscili uno dopo l'altro, dopodiché premi "Pagare una multa")  
2) Effettuare il pagamento tramite il Paysafecard.  
Per questo inserisci il numero ricevuto nella colonna di pagamento, dopodiché premi "Pagare una multa" (se hai più numeri, allora inseriscili uno dopo l'altro, dopodiché premi "Pagare una multa")

Ukash or paysafecard

Puoi richiedere e ottenere Ukash presso migliaia di punti vendita, edicole, stazioni di servizio, bar e tabacchi e negozi di telefonia mobile dotati di terminale Epay, EpiPoll.  
Paysafecard è disponibile in tutta sicurezza vicino a te in Italia, ad esempio presso numerose edicole, bar, tabaccai anche nei negozi Sisa e Penny.

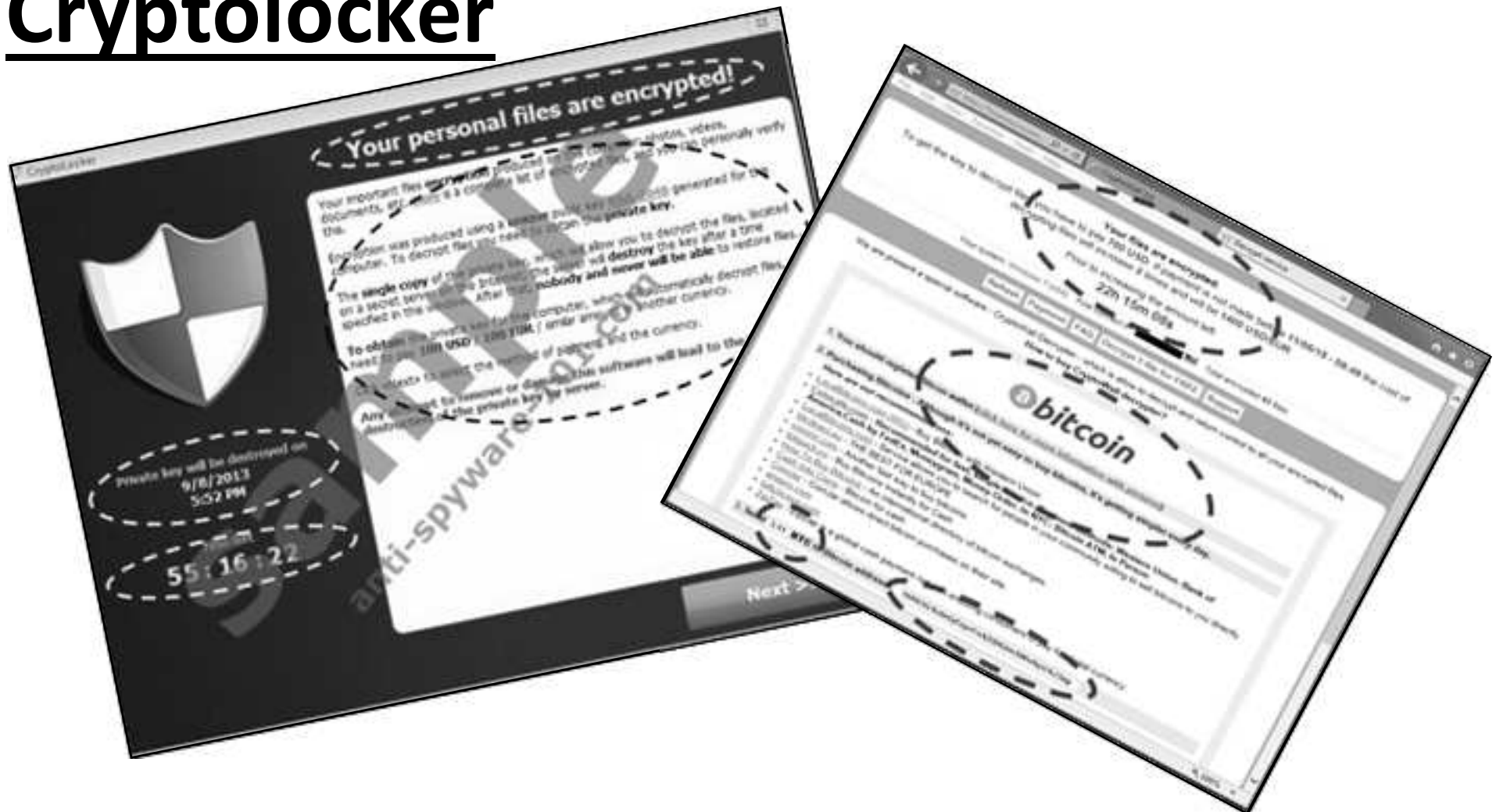
Logos: epony, PayMat, Bitcard, epipoll, Norton, Pagine Gialle

UNITÀ DI ANALISI SUL CRIMINE INFORMATICO, Piazza del Vittorino n. 1 - 00184 Roma



**POLIZIA DI STATO**  
**Compartimento Polizia Postale e delle Comunicazioni**  
**“Piemonte-Valle d’Aosta”**

# Cryptolocker





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

[www.virustotal.org](http://www.virustotal.org)

The screenshot displays the VirusTotal website interface. At the top, the VirusTotal logo is visible, consisting of a stylized 'V' icon and the text 'VirusTotal'. Below the logo, a descriptive sentence reads: 'Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community.' The main navigation area features three buttons: 'File', 'URL', and 'Search', each enclosed in a hand-drawn circle. Below these buttons is a large, light-colored rectangular area for file upload. In the center of this area is a document icon with a fingerprint symbol, and below it is a button labeled 'Choose file'. At the bottom of the page, a small disclaimer states: 'By submitting your file to VirusTotal you are asking VirusTotal to share your submission with the security community and agree to our [Terms of Service](#) and [Privacy Policy](#). [Learn more](#).'



**POLIZIA DI STATO**  
**Compartimento Polizia Postale e delle Comunicazioni**  
**“Piemonte-Valle d’Aosta”**

**www.nomoreransom.org**

**NO MORE RANSOM!**

★ Italiano

[Crypto Sheriff](#) [Ransomware G&A](#) [Contagi sulla Prevenzione](#) [Strumenti di Decrittazione](#) [Denunciare un Reato](#) [Partners](#) [Informazioni sul Progetto](#)



## INFORMAZIONI SUL PROGETTO

Le forze dell'ordine e le agenzie di sicurezza informatica hanno unito le loro forze per smantellare le attività criminali connesse al ransomware.

Il sito web "No More Ransom" è un'iniziativa intrapresa dal National High Tech Crime Unit della polizia olandese, dall'European Cybercrime Centre dell'Europol e McAfee, con l'obiettivo di aiutare le vittime del ransomware a recuperare i loro dati criptati, senza dover pagare i criminali.

Certo che è molto più semplice evitare la minaccia piuttosto che combatterla una volta che il sistema è stato infettato, il progetto ha anche l'intento di educare gli utenti su come funziona il ransomware, e quali contromisure si possono adottare per prevenire attivamente l'infezione. Più soggetti supporteranno questo progetto, migliori potranno essere i risultati. Questa iniziativa è aperta ad altre parti, sia pubbliche che private.

È il principio di quello di non pagare i ricatti. Se invece il vostro denaro ai criminali deve contribuire al finanziamento del ransomware e non vi è la garanzia di ricevere le chiavi per decrittare



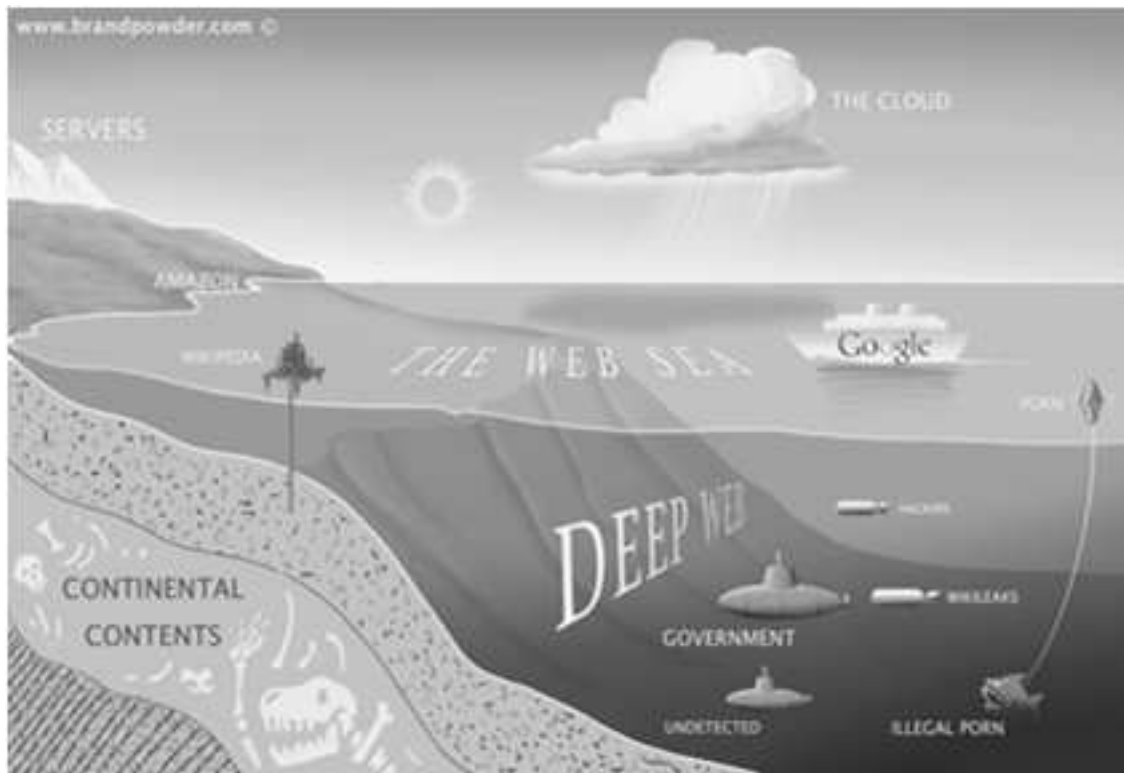
**POLITIE**





**POLIZIA DI STATO**  
**Compartimento Polizia Postale e delle Comunicazioni**  
**“Piemonte-Valle d’Aosta”**

## II DEEP WEB

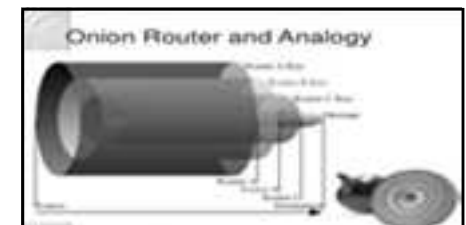


La rete internet è come immenso oceano, il browser, associato ad un motore di ricerca, sarà come una barca.

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**

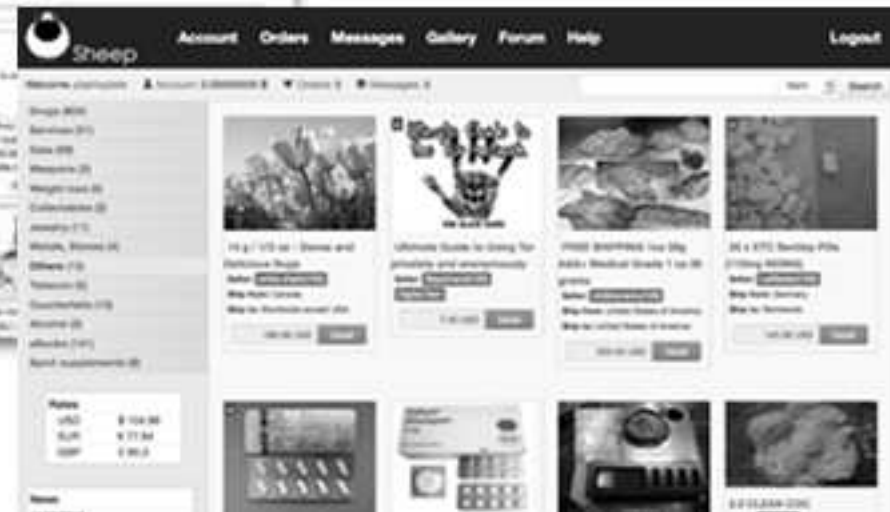
*Es: Rete TOR*





**POLIZIA DI STATO**  
**Compartimento Polizia Postale e delle Comunicazioni**  
**“Piemonte-Valle d’Aosta”**

# BLACK MARKET





**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”**

## **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)*





**POLIZIA DI STATO**  
**Compartimento Polizia Postale e delle Comunicazioni**  
**“Piemonte-Valle d’Aosta”**

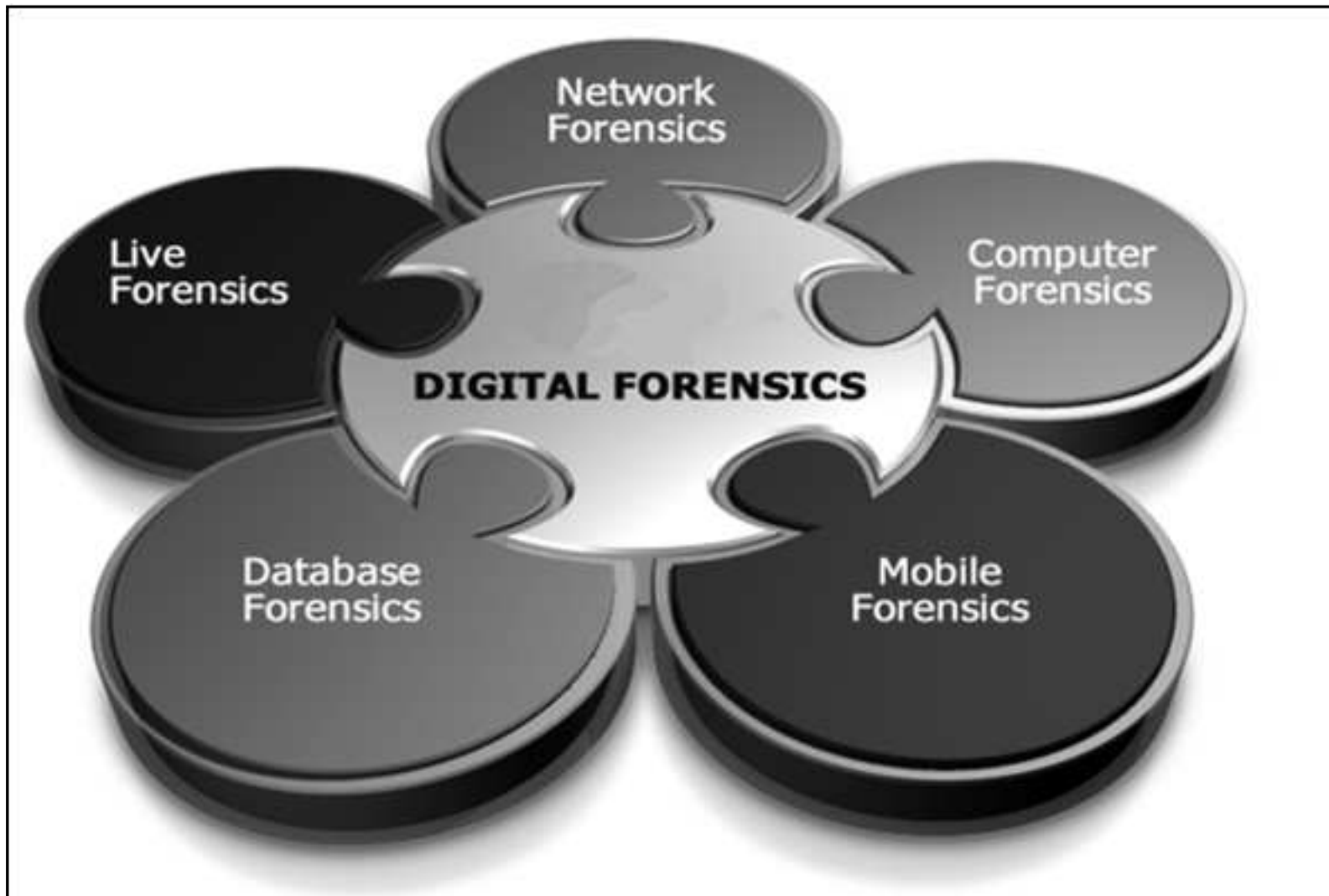
## ***INDIRIZZO IP, LOG FILES***

- *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.*





**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”**

---

**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**



**POLIZIA DI STATO**  
**Compartimento Polizia Postale e delle Comunicazioni**  
**“Piemonte-Valle d’Aosta”**

---



**È necessario implementare tecniche di OSINT e  
tecniche di Big Data analysis**



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

---

# **GRAZIE PER L'ATTENZIONE**

[www.poliziadistato.it](http://www.poliziadistato.it)

[www.commissariatodips.it](http://www.commissariatodips.it)

<https://it-it.facebook.com/AgenteLisa>

[it-it.facebook.com/unavitadasocial](https://it-it.facebook.com/unavitadasocial)

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

[compartimento.polposta.to@pecps.poliziadistato.it](mailto:compartimento.polposta.to@pecps.poliziadistato.it)

Tel. 011/3014611