


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


**LE INDAGINI TECNOLOGICHE :
 GLI STRUMENTI INVESTIGATIVI
 ED I LORO LIMITI.**

**PALAZZO DI GIUSTIZIA
 Torino – 21 Novembre 2019**
Dott. Ing. Giuseppe ZUFFANTI, Commissario Capo Tecnico 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"

- 1 Servizio Centrale
- 20 Compartimenti
- 80 Sezioni

Contrasto

- Pedopornografia
- Financial Cybercrime
- Hacking
- Protezione delle infrastrutture critiche del Paese
- Cyberterrorismo
- Crimini informatici
- Perquisizioni, perquisizioni informatiche

Prevenzione

- Monitoraggio rete Internet
- Formazione/Sensibilizzazione
- Progetto scuole Incontri con studenti/genitori/Insegnanti
- Protocolli d'intesa

Digital Forensics




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"

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"



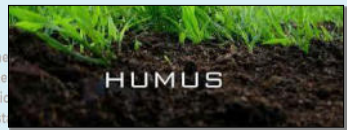
"C'è una guerra là fuori, amico mio. Una guerra mondiale. E non ha la minima importanza chi ha più pallottole, ha importanza chi controlla le informazioni. Ciò che si vede, si sente, come lavoriamo, cosa pensiamo, si basa tutto sull'informazione!"

UN LATITANTE, UNO SCASSINATORE, UN DELINQUENTE, UNA SPIA E UN LADRO... E QUESTI SONO I BUONI!


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

- Nel 2018 il Cybercrime (*sottrarre informazioni e/o denaro*) → **prima causa di attacchi gravi a livello mondiale** con il 76% degli attacchi complessivi, in crescita del 14%
- **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, **~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**
- **Multiple Threats/APT**
- **Phishing/Social Engineering/Spear Phishing/BEC**


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** ai 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"

CNCPO
 Centro Nazionale per il Contrasto
 alla Pedo-Pornografia su Internet

- L.155/2005 art.7- CNAIPIIC → DM 9/1/2008
- Funge da centrale operativa a cui le IC convenzionali possono indirizzare H.24 allarmi informatici di attacchi o segnalare attività sospette.
- Attività di intelligence
- Raccolta informazioni
- Attività investigativa, monitoraggio e studio
- Coordinamento attività con i Compartimenti sul territorio e organismi polizia internazionale



Compartimento Polizia Postale e delle Comunicazioni Piemonte e Valle d'Aosta

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

A chi interessa il mio Computer?

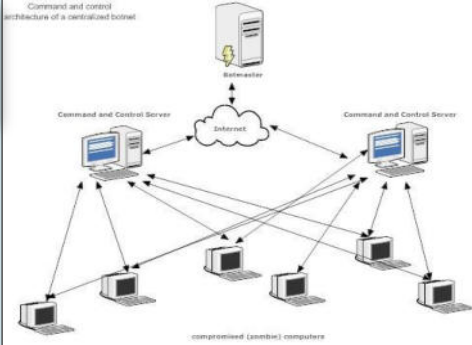
- Ladri di identità
- Nemici/Avversari/Invidiosi
- Stalkers
- Hackers/Crackers in genere
- Pedofili
- Gestori di Botnet



Compartimento Polizia Postale e delle Comunicazioni Piemonte e Valle d'Aosta

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

Esempio: DDoS (Distributed Denial-of-Service)



Command and control architecture of a centralized botnet

Botmaster
 Command and Control Server
 Botnet
 Command and Control Server
 compromised (zombie) computers

Compartimento Polizia Postale e delle Comunicazioni Piemonte e Valle d'Aosta

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

....I.O.T



Smart City
 Industry 4.0
 I.O.T

Compartimento Polizia Postale e delle Comunicazioni Piemonte e Valle d'Aosta

Polizia di Stato
Compartimento Polizia Postale e delle Comunicazioni
"Piemonte-Valle d'Aosta"

Tecnologia
In Virginia partono le consegne online con i droni



In Christenburgh gli abitanti di vecchia "resistenza" i prodotti acquistati sul territorio di casa, in nel centro, anche in quanto relativi dal momento dell'ordine alla garanzia di servizio di un servizio Agave e Conigli, la Strig.

NEW YORK. Gli aerei senza pilota arrivano dal cielo. In particolare hanno a loro favore impiegate antiche. Perché in Virginia sono state usate ufficialmente le droni per consegnare a un gruppo di anziani un pacchetto di medicine. Un progetto di assistenza a lungo termine di consegna a domicilio di farmaci, che ha permesso di evitare che gli anziani si recassero nei negozi di farmacia. Il progetto è stato avviato da un'azienda di droni, la Strig. Strig è un'azienda di droni che ha sviluppato un sistema di consegna a domicilio di farmaci, che ha permesso di evitare che gli anziani si recassero nei negozi di farmacia. Il progetto è stato avviato da un'azienda di droni, la Strig.

Compartimento Polizia Postale e delle Comunicazioni Piemonte e Valle d'Aosta

Polizia di Stato
Compartimento Polizia Postale e delle Comunicazioni
"Piemonte-Valle d'Aosta"

SHODAN Admin: 1234 Search



Compartimento Polizia Postale e delle Comunicazioni Piemonte e Valle d'Aosta

Polizia di Stato
Compartimento Polizia Postale e delle Comunicazioni
"Piemonte-Valle d'Aosta"

Surfing Web
Google
Reddit
OMG
talking

Deep Web
Dark Web

96% of content on the Web is hidden

ENGINES OF ORGANISED CRIME



Compartimento Polizia Postale e delle Comunicazioni Piemonte e Valle d'Aosta

Polizia di Stato
Compartimento Polizia Postale e delle Comunicazioni
"Piemonte-Valle d'Aosta"

Possedere Dati = Petrolio dell'Infosfera

Cyber-Furti al posto di rapine

L'80% delle aziende italiane sotto attacco inconsapevole

Un attacco si compra nel Dark Market con una normale transazione (50\$ in bitcoin)

Compartimento Polizia Postale e delle Comunicazioni Piemonte e Valle d'Aosta


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

CRIPCOCURENCY



Sono una commodity
 • creata da un fenomeno innovativo di rete sociale
 • che si basa su un protocollo di scambio garantito fra sconosciuti
 • definito da una tecnologia open-source non vincolabile a controlli centrali
 • semplice da usare.

Oltre ai bitcoin ci sono altre valute alternative, per numero e volumi degli scambi attuali es: ripple e litecoin.
 Sono dette anche criptovalute, valute matematiche, valute virtuali, ecc.
 Fra i non addetti ai lavori è comune usare il termine bitcoin per intendere qualsiasi criptovaluta.


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



Bitcoin Value: Tick by tick, real time updates. All data is indicative.
 Change: 024.90%
9320.300


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



CryptoMiner sfrutta vulnerabilità Microsoft

Microsoft è in grado di entrare nelle reti locali e sfruttare le capacità di calcolo degli host infetti per generare nuove monete della crypto-valuta Monero.

Hacking, società italiana nei servizi di cyber security, sta informando i propri clienti dell'avvio di una pericolosa campagna di cyber-crime guidata da motivazioni finanziarie, mirata alla propagazione di un malware (Worm), CryptoMiner.

Si tratta di una minaccia in grado di entrare nelle reti locali e sfruttare le capacità di calcolo degli host infetti per "minare", ovvero generare nuove monete della crypto-valuta Monero, una moneta digitale cifrata, che consente di effettuare pagamenti online in maniera sicura e anonima il cui utilizzo si sta diffondendo rapidamente.

I campioni analizzati utilizzano codice reperibile in strumenti di sicurezza open-source per propagare all'interno delle reti locali e utilizzano tecniche di propagazione automatica basate su noduli di rete per sistemi Microsoft e tecniche di esecuzione remota basate sulla tecnologia WMI (Windows Management Instrumentation).

Hacking consiglia di mantenere alto il livello di attenzione all'interno delle aziende, monitorare potenziali rischi di sicurezza, mantenere signature e sandbox aggiornate e verificare periodicamente la sicurezza degli apparati di rete.

Inoltre, suggerisce di rafforzare la consapevolezza degli utenti, condividendo regolarmente informazioni sulle minacce in corso e fare ricorso a team di esperti per salvaguardare la sicurezza del perimetro "cyber".


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



L'Indagine Informatica

Compartimento Polizia Postale e delle Comunicazioni Piemonte e Valle d'Aosta

Ricerca di elementi riferiti ad un reato on line:
 Indirizzi IP, nickname e identità chat, indirizzi e-mail, tabulati telefonici, log, cloud, ecc.... Problemi del NAT, dell'anonimizzazione, 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)

Compartimento Polizia Postale e delle Comunicazioni Piemonte e Valle d'Aosta

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"**

IP e CALLER ID

- INDIRIZZO IP:** 4 NUMERI DA 0 a 255 separati da punti (Es. 111.111.111.111)
- Conoscendo l'indirizzo IP e giorno e ora esatta della connessione è possibile sapere **PREVIO DECRETO DELL'A.G.** la **linea di comunicazione utilizzata per la connessione (CALLER ID)**
- IL NAT**
- La rete TOR e la catena di indirizzi IP --- LE BOTNET**
- RISORSE UTILI:** whois.com - <https://mxtoolbox.com/DNSLookup.aspx>
DNS LOOKUP → attenzione: i dati personali potrebbero non essere veritieri
IP: Ripe.net (ci dice a quale ISP appartiene un determinato indirizzo IP).
Domini: Ican.org (lista dei diversi enti che gestiscono i diversi domini nel mondo).

Polizia di Stato
**Compartimento Polizia Postale e delle Comunicazioni
 "Piemonte-Valle d'Aosta"**

EMAIL HEADER

Polizia di Stato
**Compartimento Polizia Postale e delle Comunicazioni
 "Piemonte-Valle d'Aosta"**

www.facebook.com/records




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

Reti Anonimizzatrici

- Le reti anonimizzatrici sono strumenti nati appositamente per consentire ad un utente di:
 - Navigare in Internet**
 - Offrire servizi**
 - Condividere file**
 - Comunicare con altri utenti in modo "anonimo".
- L'anonimità è ottenuta creando automaticamente delle catene di nodi che agiscono come proxy
- Tipicamente le reti anonimizzatrici offrono ulteriori garanzie di integrità e riservatezza dei dati mediante crittografia




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

ALCUNI ESEMPI DI INDAGINI


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

Operazione «BABYLON»

Tra i mercati virtuali → Spazio riservato al materiale pedopornografico

In Italia la Polizia Postale con l'operazione "**Babylon**" dopo una lunga attività sottocopertura si è arrivati ad un **hidden service** (Servizio web anonimizzato) all'interno della rete TOR, gestito da italiani ove le comunità pedofile scambiavano informazioni per reperire il materiale "di nuova produzione" (furono sequestrati i wallet per ricostruire il volume d'affari) materiale **autoprodotta**, **tecniche di adescamento on-line** a volte **vendite di bambini**, naturalmente il tutto nella più totale **privacy** della realtà virtuale.


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

Operazione "Babylon": la Postale scopre un mercato illecito nella darknet



È il primo sequestro in Europa e il secondo al mondo: la **Polizia postale** ha individuato un vero e proprio mercato virtuale nascosto nella darknet e ha sequestrato circa 14 mila wallet (carte elettroniche) di criptovalute per un valore di circa un milione di euro. Si poteva acquistare di tutto, armi, sesso, documenti, droghe e qualsiasi altro materiale a servizio illecito attraverso il pagamento con la moneta virtuale conosciuta con il nome di Bitcoin.



Durante le indagini è stato scoperto il sito "Babylon", un grande mercato dove s'incontra l'offerta e la domanda degli utenti che vanno alla ricerca di cose "particolari". L'indagine (Video) ha individuato un italiano, gestore del più gettonato market place di traffico illecito nella darknet.

31/07/2015

<https://www.poliziadistato.it/articolo/39585>

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

Operazione «INFRAUD» Deanonimizzazione della rete attraverso una cooperazione internazionale - 2018

La dimostrazione la recente attività «Infraud» Operazione congiunta in 16 paesi nel mondo anche in Italia con la Polizia Postale che ha permesso l'arresto e l'individuazione di 14 membri di una organizzazione criminale operante nel dark web.

L'attività illecita era focalizzata sulla compravendita di migliaia di carte di credito clonate, codice di accesso all'home banking, dati personali di migliaia di vittime; il sito **Infraud** era di fatto un negozio di riferimento per i cyber criminali di tutto il mondo.

Obiettivo del fondatore era diventare il punto di riferimento nel "carding" ovvero agevolare l'acquisto dei beni on line tramite carte di credito e codici rubati.

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

Carte clonate e codici bancari nel dark web, arrestati 13 cybercriminali



Il suo nickname era "Dennylogor" e faceva parte di un'organizzazione criminale internazionale specializzata nella compravendita di carte di credito rubate e clonate, di codici di verifica per l'utilizzo delle carte online, codici di accesso a servizi di home banking e dati personali, appartenenti a migliaia di vittime in tutto il mondo.

L'uomo, un italiano destinatario di un mandato di arresto internazionale, è stato arrestato dagli uomini della sezione "Financial cybercrime" del Servizio polizia postale e del Compartimento polizia postale Campania, al termine dell'operazione "Infraud" (Valle). Grazie ai traffici illeciti l'organizzazione criminale ha accumulato un bottino di oltre 530 milioni di dollari.

L'attività investigativa è stata condotta in 16 Paesi del mondo in collaborazione con l'Interpol e la National Security Agency (NSA), dipartimento degli Stati Uniti che tra i suoi compiti ha anche quello di proteggere il territorio americano da attacchi terroristici e di contrastare le organizzazioni criminali che sfruttano legalmente i sistemi di viaggio, commerciali, finanziari e di immigrazione.

Nell'ambito della stessa operazione sono state arrestate altre 12 persone, mentre la settimana scorsa era finito in carcere anche il presunto capo dell'organizzazione, un uomo di nazionalità coreana, fermato in Thailandia.

Per la compravendita delle informazioni i cybercriminali utilizzavano il dark web e "Liberty reserve" una piattaforma di scambio di criptovalute virtuali impiegata per il riciclaggio di denaro e chiusa nel 2015 dagli Stati Uniti.

Valle d'Aosta Valle d'Aosta

07/02/2018
<https://www.poliziadistato.it/articolo/1654763487a075275262878>

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

Dark Web subisce un duro colpo da Europol, chiuso uno dei "supermercati" di droga e materiali illeciti



Una struttura coordinata da Europol e dalla polizia di diverse Stati membri dell'UE, alla guida dell'italiano Alessandro, ha portato alla chiusura di uno dei maggiori siti europei del Dark Web, all'interno dei quali si vendono e si acquistano ingenti somme di contanti.

Per chi non ne avesse mai sentito parlare, Valhalla è uno dei siti commerciali illegali più antichi e consistenti a livello internazionale, su cui era possibile acquistare **mercerie e altri beni illeciti**. Dopo la chiusura del sito principale da parte delle autorità, alcuni dei componenti FishMarket di Valhalla hanno trasferito le proprie attività su altri siti illegali, tra cui appunto Wall Street Market.

Il successo dell'operazione è stato possibile grazie all'apporto coordinato di Europol e di organismi di polizia di diversi Stati membri dell'UE e di partner come Enxopiq. Per contrastare la criminalità sul Dark Web, Europol ha istituito un team dedicato che collabora con i partner dell'UE e le forze dell'ordine in tutto il mondo per ridurre le dimensioni di questa economia clandestina illegale. L'operazione coordinata include la condivisione delle informazioni, il supporto operativo e delle competenze le diverse aree del crimine, lo sviluppo di strumenti, tattiche e tecniche per condurre indagini sul Dark Web, l'identificazione di vittime e obiettivi.

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

LA STAMPA

La Polizia postale di Torino smaschera una rete di pedofili attivi in rete

Due arresti e 7 denunce: in alcuni casi i soggetti incriminati si scambiarono materiale pedopornografico realizzato anche in ambito sfruttamento di minori addeposti sul web.



la Repubblica

Pedopornografia, scoperta a Torino una community online: due arresti, 7 denunce

Il materiale realizzato anche con lo sfruttamento di minori

Una persona arreolata e altre sette denunce. Il titolare di un'attività commerciale con la pedopornografia in rete scoperta dalla polizia postale di Torino che ha permesso di ingenerare una rete di persone che, servendosi di canali internazionali, commerciavano materiale pedopornografico, venduto in Italia con anche banche di abbattimento del sito. Nel corso dell'indagine, diretta dalla Procura di Torino, è risultato dal Centro Nazionale di Crimine alle Pedopornografie (Cenac) del Servizio Polizia Postale di Roma che ha individuato, oltre il territorio nazionale, otto altri importanti nodi di rete.

Un'indagine è scaturita dal monitoraggio di canali web che commercializzano materiale pedopornografico. Il titolare di un'attività commerciale, conosciuta come "Dark Web", è stato arrestato, così come il titolare di un'altra attività commerciale, conosciuta come "Dark Web".

Offerta di lavoro del servizio clienti, in attesa di essere addeposti sul sito, con un contratto di lavoro a tempo pieno che viene richiesto per il cliente, e un contratto di lavoro a tempo pieno, non recente, e un contratto di lavoro a tempo pieno, non recente, e un contratto di lavoro a tempo pieno, non recente.

Compartmento Polizia Postale e delle Comunicazioni Piemonte e Valle d'Aosta

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

ESEGUITE DALLA POLIZIA DI STATO 2 MISURE DI CUSTODIA IN CARCERE PER SOGGETTI RITENUTI RESPONSABILI DI RICICLAGGIO DI DENARO PROVENTO DI FRODI INFORMATICHE

Commissariato di P.S. online
Sportello per la sicurezza degli utenti del web

Il Compartimento Polizia Postale e delle Comunicazioni Piemonte e Val d'Aosta sotto la direzione della Procura della Repubblica presso il Tribunale di Torino ha compiuto negli ultimi mesi una complessiva attività di primo gradimento finalizzata al controllo del riciclaggio nell'ambito del più ampio contesto del Financial Cybercrime. Preparazione ha condotto all'arresto di parte dell'A.S. di Torino di due persone considerate in quanto nei confronti di altrettanti soggetti, un cittadino originario già noto alle forze dell'Ordine con esecutori alleati ed una donna di origini tedesche residenti nel capoluogo piemontese.

Le responsabilità relative ai riciclaggi commessi bancari e/o postali, ingenti somme di denaro immediatamente prelevate e distratte verso altri conti al fine di far perdere le tracce. Degli accertamenti fatti è evidente che gli operatori finanziari sono a conoscenza banche operanti.

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

LE FRODI RELATIVE ALLE CARTE DI PAGAMENTO

FRODE IN AMBIENTE "CARD NO PRESENT"

Questo tipo di crimine consiste nel furto di dettagli relativi alla carta quali il nome del titolare, il numero, la data di scadenza ecc.

FRODE IN AMBIENTE "CARD PRESENT"

Presuppone il possesso materiale del supporto

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

ID THEFT AND PAYMENT CARD FRAUD

STEP 1
A fraudulent user malware and social engineering to access your computer

STEP 2
Your login credentials, bank account details, credit card numbers and other personal information are stolen

STEP 3
Your data is sold on the Darknet

STEP 4
Criminals use your compromised ID and financial data to hijack their criminal activities

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

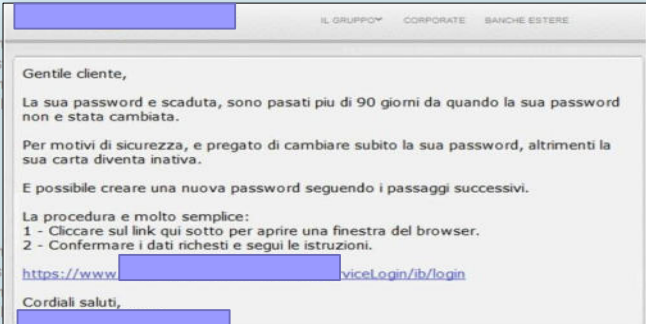
Test: 19mila utenti di 144 Paesi con un Phishing Quiz

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"

DAL PHISHING ALLO SPEARPHISHING



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 un esempio

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



B.E.C.

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

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

mario.rossi@azienda.it → mario.rossi@azienda.it
mario.rossi@azienda.it → mario.rossi@gmail.com

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"

ATM ATTACKS

- **Card Skimming:** customer's card information and PIN are captured at an ATM → used to produce counterfeit cards.
- **Card Trapping:** customer inserts their card into an ATM → card is physically captured at the ATM
- **Cash Trapping:** attaching the ATM that will trap any cash that the ATM tries to dispense.




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

VIDEO

VIDEO : SKIMMER POSTAMAT

VIDEO : SEQUESTRO CLONAZIONE CARTE

VIDEO : SKIMMER MICROCAMERA


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



Placchetta adesiva con foro telecamera


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



Placchetta adesiva con foro telecamera **Sovrapposizione all'originale**




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

CASH TRAPPING



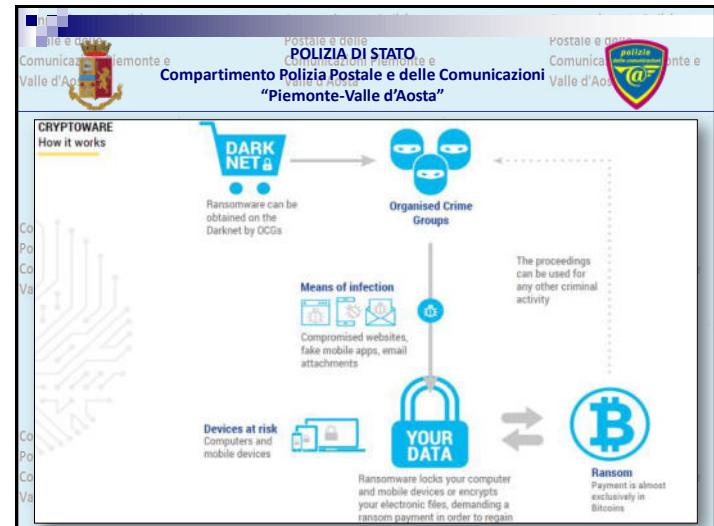


POLIZIA DI STATO
 Compartimento Polizia Postale e delle Comunicazioni
 "Piemonte-Valle d'Aosta"

ESEMPIO: ARRESTI ESEGUITI




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"

Ransomware delle prime versioni

CRIMINE INFORMATICO
2012 11 05 19:44
MILAN

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

Cryptolocker

Your personal files are encrypted!
Bitcoin

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

Sei vittima di cryptolocker? → www.nomoreransom.org

NO MORE RANSOM!
CRYPTO SHERIFF
Selezionate un primo file criptato
Selezionate un secondo file cript...
VIA!

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

www.nomoreransom.org

STRUMENTI DI DECRIPTAZIONE

IMPORTANTE! Prima di scaricare e avviare la soluzione, leggete le istruzioni guida. Accertatevi di rimuovere prima il malware dal sistema, altrimenti continuerà ad operare, bloccandolo nuovamente, o criptandone i file. Qualsiasi soluzione antivirus affidabile può fare questo per voi.

Quick Search...

Tutto Ransom (ordine alfabetico):
 ▼ 777 Ransom
 Trend Micro Ransomware e progettato per decriptare file criptati da 777
 Per maggiori informazioni si prega vedere questo [guida come fare](#)

> AES_NI Ransom
 > Agent.ih Ransom
 > Alcatraz Ransom

DOWNLOAD


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




Tecniche di Polizia Giudiziaria Standard, Tecniche di OSINT
Tecniche di Big Data Analysis


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

Investigare nella rete – *Contenuti*

- Discriminare le tipologie di informazione
- Individuare le sorgenti informative
- Determinare le tecniche (utilizzabili e in quali condizioni) per l'acquisizione di informazioni
- Organizzare i contenuti di interesse
- Raccogliere i contenuti di interesse


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

Esempi di tecniche di acquisizione

- Wardriving
- Password cracking
- Sniffing di rete
- Information gathering
- Fingerprinting
- Malware injection, SQL injection
- Google cache
- Motore di ricerca (non solo Google)
- API di social network
- Whois – RIPE
- Honeypotting
- Data harvesting
- Data mining
- Social engineering (phishing, pharming)
- Man in the middle
- Intercettazione (metadati, contenuti)
- Fingerprinting documento, foto, video
- Osservazioni


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

OPEN SOURCE INTELLIGENCE

- Individuare ed analizzare le informazioni proveniente da ogni sorgente pubblicamente disponibile
- Evoluzione tecnologica
- Prima dell'era Internet, l'OSINT consisteva in attività di analisi delle informazioni sui giornali, sui magazine, alla radio e TV provenienti da tutto il mondo



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

INFORMATION GATHERING

- People
- Groups of people
- Companies
- Organizations
- Web sites
- Internet infrastructure
- Phrases
- Affiliations
- Documents and files



Individuazione del "network della persona"
L'indagine sul singolo individuo → punto di partenza dell'indagine
Individuare rete di relazioni sociali
Estendere le indagini. Relazioni indirette (A → B; B → C; A → C?)

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

Who IS, DomainTools, Maxmind, Whoisology, Reverse Who IS, etc..



Legend:
 ■ AfrNIC
 ■ APNIC
 ■ ARIN
 ■ LACNIC
 ■ RIPE NCC

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




Evoluzione dei motori di ricerca - 2002

LEGEND
 Search Engines - Red Lines Primary Search Engines
 Search Engines - Blue Lines Secondary Search Engines
 Search Engines - Green Lines Tertiary Search Engines
 Search Engines - Yellow Lines Paid Services

Click On a Logo for Search Engine Information
 Click Here to Select a Different Chart

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



Evoluzione dei motori di ricerca - 2011

LEGEND
 Search Engines - Red Lines Primary Search Engines
 Search Engines - Blue Lines Secondary Search Engines
 Search Engines - Green Lines Tertiary Search Engines
 Search Engines - Yellow Lines Paid Services

Click On a Logo for Search Engine Information
 Click Here to Select a Different Chart

Comunicazione Piemonte e Valle d'Aosta
POLIZIA DI STATO
Comunicazione Piemonte e Valle d'Aosta

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

Comunicazione Piemonte e Valle d'Aosta
POLIZIA DI STATO
Comunicazione Piemonte e Valle d'Aosta

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

Comunicazione Piemonte e Valle d'Aosta
POLIZIA DI STATO
Comunicazione Piemonte e Valle d'Aosta

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

Finì diversi

- Search engines:
 - General search engines
 - Multi search engines
 - Country based search engines
 - Clustering search engines
 - Image search engines
 - People search engines
 - Social media search engines
 - Scientific & computational search engines
 - Privacy friendly search engines
 - Deep web search tools
- Information resources
 - Wiki's
 - Directories

Comunicazione Piemonte e Valle d'Aosta
POLIZIA DI STATO
Comunicazione Piemonte e Valle d'Aosta

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

Multi Search Engine

Compartimento Polizia Postale e delle Comunicazioni Piemonte e Valle d'Aosta	Compartimento Polizia Postale e delle Comunicazioni Piemonte e Valle d'Aosta	Compartimento Polizia Postale e delle Comunicazioni Piemonte e Valle d'Aosta
Compartimento Polizia Postale e delle Comunicazioni Piemonte e Valle d'Aosta	Compartimento Polizia Postale e delle Comunicazioni Piemonte e Valle d'Aosta	Compartimento Polizia Postale e delle Comunicazioni Piemonte e Valle d'Aosta


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

Country based Search Engine

<http://www.whitelines.net/>

Compartimento Polizia Postale e delle Comunicazioni Piemonte e Valle d'Aosta	Compartimento Polizia Postale e delle Comunicazioni Piemonte e Valle d'Aosta	Compartimento Polizia Postale e delle Comunicazioni Piemonte e Valle d'Aosta
Compartimento Polizia Postale e delle Comunicazioni Piemonte e Valle d'Aosta	Compartimento Polizia Postale e delle Comunicazioni Piemonte e Valle d'Aosta	Compartimento Polizia Postale e delle Comunicazioni Piemonte e Valle d'Aosta


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

Clustering Search Engines

Compartimento Polizia Postale e delle Comunicazioni Piemonte e Valle d'Aosta	Compartimento Polizia Postale e delle Comunicazioni Piemonte e Valle d'Aosta	Compartimento Polizia Postale e delle Comunicazioni Piemonte e Valle d'Aosta
Compartimento Polizia Postale e delle Comunicazioni Piemonte e Valle d'Aosta	Compartimento Polizia Postale e delle Comunicazioni Piemonte e Valle d'Aosta	Compartimento Polizia Postale e delle Comunicazioni Piemonte e Valle d'Aosta


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

Image Search Engines

Compartimento Polizia Postale e delle Comunicazioni Piemonte e Valle d'Aosta	Compartimento Polizia Postale e delle Comunicazioni Piemonte e Valle d'Aosta	Compartimento Polizia Postale e delle Comunicazioni Piemonte e Valle d'Aosta
Compartimento Polizia Postale e delle Comunicazioni Piemonte e Valle d'Aosta	Compartimento Polizia Postale e delle Comunicazioni Piemonte e Valle d'Aosta	Compartimento Polizia Postale e delle Comunicazioni Piemonte e Valle d'Aosta


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

People Search Engines

Compartimento Polizia Postale e delle Comunicazioni Piemonte e Valle d'Aosta	Compartimento Polizia Postale e delle Comunicazioni Piemonte e Valle d'Aosta	Compartimento Polizia Postale e delle Comunicazioni Piemonte e Valle d'Aosta
Compartimento Polizia Postale e delle Comunicazioni Piemonte e Valle d'Aosta	Compartimento Polizia Postale e delle Comunicazioni Piemonte e Valle d'Aosta	Compartimento Polizia Postale e delle Comunicazioni Piemonte e Valle d'Aosta

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

Information Gathering with Maltego

Compartimento Polizia Postale e delle Comunicazioni Piemonte e Valle d'Aosta	Compartimento Polizia Postale e delle Comunicazioni Piemonte e Valle d'Aosta	Compartimento Polizia Postale e delle Comunicazioni Piemonte e Valle d'Aosta
Compartimento Polizia Postale e delle Comunicazioni Piemonte e Valle d'Aosta	Compartimento Polizia Postale e delle Comunicazioni Piemonte e Valle d'Aosta	Compartimento Polizia Postale e delle Comunicazioni Piemonte e Valle d'Aosta

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

BROWSER UNIQUENESS

Variable	Source	Remarks
User Agent	Transmitted by HTTP, logged by server	Contains Browser micro-version, OS version, language, toolbars and sometimes other info.
HTTP ACCEPT headers	Transmitted by HTTP, logged by server	
Cookies enabled?	Inferred in HTTP, logged by server	
Screen resolution	JavaScript AJAX post	
Timezone	JavaScript AJAX post	
Browser plugins, plugin versions and MIME types	JavaScript AJAX post	Sorted before collection. Microsoft Internet Explorer offers no way to enumerate plugins; we used the PluginDetect JavaScript library to check for 8 common plugins on that platform, plus extra code to estimate the Adobe Acrobat Reader version.
System fonts	Flash applet or Java applet, collected by JavaScript/AJAX	Not sorted; see Section 6.4.
Partial supercookie test	JavaScript AJAX post	We did not implement tests for Flash LSO cookies, Silverlight cookies, HTML5 databases, or DOM globalStorage.

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



DIGITAL FORENSICS

- Individuazione
- Conservazione
- Protezione
- Estrazione
- Documentazione

e studia ogni altra forma di trattamento del dato informatico per essere valutato in un processo giuridico e studia ai fini probatori, le tecniche e gli strumenti per l'esame metodologico dei sistemi informatici.

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



- ...attraverso le modifiche introdotte dalla L. 18 marzo 2008, n.48 il legislatore ha regolamentato anche le operazioni di **PERQUISIZIONE E SEQUESTRO IN AMBITI INFORMATICI-TELEMATICI**, chiedendo agli ufficiali/agenti di p.g., di assicurare, la conservazione e l'inalterabilità dei dati originali mediante l'adozione di idonee misure tecniche.
- Corrette procedure da utilizzare per l'accesso, l'acquisizione, la duplicazione e certificazione dell'evidenza digitale.



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

Art. 359 cpp - Consulenti tecnici del pubblico ministero

1. Il pubblico ministero, quando procede ad accertamenti, rilievi segnaletici, descrittivi o fotografici e ad ogni altra operazione tecnica per cui sono necessarie specifiche competenze, può nominare e avvalersi di consulenti (233; 73 att.), che non possono rifiutare la loro opera.
2. Il consulente può essere autorizzato dal pubblico ministero ad assistere a singoli atti di indagine.

Art. 360 cpp - Accertamenti tecnici NON RIPETIBILI

1. Quando gli accertamenti previsti dall'art. 359 riguardano persone, cose o luoghi il cui stato è soggetto a modificazione (116, 117 att.), il pubblico ministero avvisa, senza ritardo, la persona sottoposta alle indagini, la persona offesa dal reato e i difensori del giorno, dell'ora e del luogo fissati per il conferimento dell'incarico e della facoltà di nominare consulenti tecnici (233).
2. Si applicano le disposizioni dell'art. 364 comma 2.
3. I difensori nonché i consulenti tecnici eventualmente nominati hanno diritto di assistere al conferimento dell'incarico, di partecipare agli accertamenti e di formulare osservazioni e riserve.
4. Qualora, prima del conferimento dell'incarico, la persona sottoposta alle indagini formuli riserva di promuovere incidente probatorio (392 s.), il pubblico ministero dispone che non si proceda agli accertamenti salvo che questi, se differiti, non possano più essere utilemente compiuti.
5. Se il pubblico ministero, malgrado l'espressa riserva formulata dalla persona sottoposta alle indagini e pur non sussistendo le condizioni indicate nell'ultima parte del comma 4, ha ugualmente disposto di procedere agli accertamenti, i relativi risultati non possono essere utilizzati nel dibattimento.

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

COMMISSARIATO ONLINE <https://www.commissariatodips.it/>

COMPARTIMENTO POLIZIA POSTALE E DELLE COMUNICAZIONI PIEMONTE E VALLE D'AOSTA

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

#UNAVITADASOCIAL

COMPARTIMENTO POLIZIA POSTALE E DELLE COMUNICAZIONI PIEMONTE E VALLE D'AOSTA


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

GRAZIE PER L'ATTENZIONE

www.poliziadistato.it
www.commissariatodips.it
it-it.facebook.com/unavitadasocial

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