Polizia di Stato

CYBER SECURITY:
PREVENZIONE E REPRESSIONE DELLA CRIMINALITÀ INFORMATICA

Milano 23 gennaio 2020

Polizia di Stato

POLIZIA POSTALE E DELLE COMUNICAZIONI

Dai reati Postali a quelli legati al mondo ICT

Servizio Centrale

CNAIPIC e CNCPO

20 *Compartimenti regionali*

80 *Sezioni provinciali*

Competenze (DM 15 agosto 2017):

- Pedopornografia online
- Cyberterrorismo
- Financial cybercrime
- Protezione infrastrutture critiche
- Intrusioni informatiche

Polizia di Stato

REATI INFORMATICI PROPRI E A MEZZO INFORMATICO

- I reati di specialità
  1. Pedopornografia e tutela minori
  2. Cyberterrorismo(propaganda terroristica ed eversiva)
  3. Protezione Infrastrutture Critiche
  4. Financial cybercrime (frodi di organizzazioni criminali)
  5. Tutela "Poste"
  6. "Diritto d'autore"

Polizia di Stato

POLIZIA POSTALE E PREVENZIONE

Non solo repressione ma anche **prevenzione**

Rivolta a:

- Studenti scuole primarie e secondarie
  - Alunni, Genitori e Docenti
- Aziende (management e dipendenti)

Polizia di Stato

PROTOCOLLI DI INTESA

Assolombarda

Confcommercio

Regione Lombardia - Welfare

Obiettivi

- Elaborare e proporre standard comuni per migliorare la protezione delle infrastrutture
- Individuare ed arginare i fattori di rischio (anche umano/comportamentali)
- Supportare la formazione al personale e partecipare ad incontri di sensibilizzazione

Piattaforma di scambio informativo bidirezionale (fenomeni, antivirus,nuove vulnerabilità)

Polizia di Stato

SICUREZZA E CYBERSICUREZZA

Sicurezza fisica e sicurezza ***cyber*** - **percezione** diversa del rischio

«La cybersecurity è qualcosa che non mi riguarda»

Siamo tutti possibili bersagli !

Il crimine organizzato si sposta sul mondo virtuale e mira a:

- Denaro
- Dati : informazioni riservate: piani aziendali, brevetti, elenco clienti - foto
- Reputazione /Immagine
- Sentimenti

Polizia di Stato

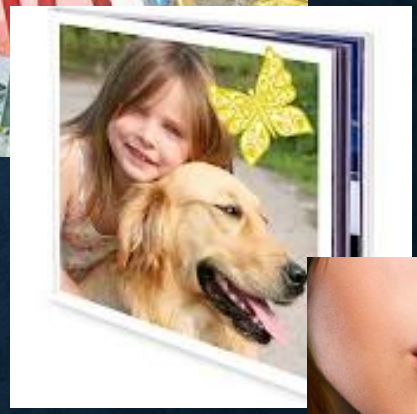
PILLOLE DI CYBERSECURITY

Gli attori: attaccanti, obiettivi e vittime

- i nuovi hacker
- denaro – dati – reputazione - sentimenti
- Istituzioni- aziende – privati cittadini

Perché così poca sicurezza

- Diffusione capillare e nuovi interessi criminali
- Vulnerabilità tecniche
  - bug nelle applicazioni / S.O.
  - manca la «security by design» su primi servizi Internet
- Fattore umano
  - evoluzione tecnologica esponenziale *(storage – banda - miniaturizzazione)*
  - scarsa consapevolezza del rischio *(sicurezza ≠ cybersecurity)*



Polizia di Stato

RAPIDA EVOLUZIONE TECNOLOGICA

Storage – Banda - Miniaturizzazione

- Dal Commodore 64K alla SD 64G (6 ordini di grandezza:1 milione di volte più capace)
- 1986 Internet Italia – velocità di pochi KB oggi Fibra 1 Gb
- Potenza di calcolo raddoppia ogni 18 mesi (Moore)
- Numero dei dispositivi connessi: da IPv4 a IPv6
  - da 4 miliardi a circa 3,4 × 10^38 indirizzi;
  - per ogni metro quadrato di superficie terrestre, ci sono 655.571 miliardi di miliardi di IPv6 ma solo 7 IPv4 ogni milione di metri quadrati.
  - Per dare un'idea delle grandezze in uso, se si paragona l'indirizzo singolo ad un quark (grandezza nell'ordine di 1 attometro), con IPv4 si raggiungerebbe il diametro dell'elica del DNA (di pochi nanometri), mentre con IPv6 si raggiungerebbe il centro della Via lattea dalla Terra (tre decine di millenni-luce). (Wikipedia)


NINTENDO 2DS


SONY


SAMSUNG


Nikon


55
Via Delle Terme Di Diocleziano


CASIO
WORLD TIME


AGENDA


GlobeCast

Polizia di Stato

PRINCIPALI MINACCE CYBER - AZIENDE

- Social engineering (anche telefonico) come attività propedeutica
- Malware generico per bornet /keylogger
- Ransomware
- False mail aziendali / CEO Fraud / IBAN modificati
- Distribuited Denial of Service

Il principale vettore utilizzato per l'attacco resta la mail

(con allegato eseguibile o link su pagina per download o furto credenziali)

Polizia di Stato

PRINCIPALI MINACCE CYBER - PRIVATI

- Malware generico per bornet /keylogger
- Ransomware
- Sostituzione di persona
- Sex extortion
  - su foto/video intime copiate dal pc oppure registrate tramite un adescamento via chat
- Truffa su acquisti di beni, case vacanza, lotterie
- Frodi su investimenti/trading

Il principale vettore utilizzato per l'attacco resta la mail

(con allegato eseguibile o link su pagina per download o furto credenziali)

LA SICUREZZA

- **Tecnologia**
- **Fattore umano**: Leggi/Regole e Comportamenti
- La sicurezza è scomoda (cinture di sicurezza, caschi, password lunghe e diverse)

… ma è questione di abitudine

Polizia di Stato

CASI

CASO: MAN IN THE MIDDLE

Obiettivo: fare effettuare un bonifico verso IBAN estero dei truffatori

- Due tipologie differenti:
  1. Accesso abusivo a casella di posta elettronica
     - notaio – direttrice di banca
     - fornitore – ditta
     - (password deboli/brute force – ricerca di parole chiave su migliaia di email)

Polizia di Stato

CEO FRAUD

1. Mail con Mittente fasullo – dal capo del capo (sistema banale ma funziona ancora – sarebbe sufficiente un Reply To)
2. Destinatario mirato (abilitato a disporre bonifici)
3. Importante acquisizione societaria con massima **urgenza** e **riservatezza**
4. Passaggio a contatti su email privata e non aziendale
5. Contatti da intermediatore (avvocato/notaio di «Ginevra»)
6. Velate promesse di promozione
7. Istruzioni per il bonifico su file …**cifrato!**

Polizia di Stato

TRADING E INVESTIMENTI

Primi contatti da call center o via skype

Piattaforme ben fatte con assistenza telefonica

Secondo contatto da abili promotori finanziari

Assistenza da remoto *(es. TeamViewer)*

Piccole somme iniziali

Guadagni significativi

Bonifici di ritorno

Polizia di Stato

HOW DO YOU BECOME THE BEST TRADER?

Trade with Sigma4trade – the Industry's Leading Forex Brokerage.

READ MORE

LEARN AS YOU GO

Sigma4trade provides rich learning materials that teach clients the ins-and-outs trading

LEARN MORE

MINIMUM DEPOSIT	TRADING ASSETS	LEVERAGE	SPREAD FROM
$500	327	1:50	0.6

DOWNLOAD MT4

Polizia di Stato

POLIZIA DI STATO

COMPARTIMENTO POLIZIA POSTALE
E DELLE COMUNICAZIONI
LOMBARDIA

OGGETTO: Verbale di ricezione di Querela sporta da:
[redacted], nato a [redacted] il [redacted].08.1937 residente a Milano in Viale [redacted], identificato mediante Carta di identità elettronica numero [redacted] rilasciata da Comune di Milano in data [redacted] valida fino al [redacted], recapito telefonico [redacted].---------//

L'anno 2020, addì 10 del mese di Gennaio, alle ore [redacted], in Milano, presso gli Uffici del Compartimento Polizia Postale e delle Comunicazioni per la Lombardia siti in via Moisè Loria nr. 74, innanzi a noi sottoscritti Ufficiali ed Agenti di P.G. V.Isp. [redacted] ed Agt. Scelto [redacted]., in forza all'Ufficio in intestazione è presente il nominato in oggetto, il quale per ogni effetto di legge espone quanto segue----------//
"Premetto di essere titolare di un c/c cointestato con mia moglie [redacted] avente Iban IT[redacted] Banca [redacted].----------//

Polizia di Stato

Nel mese di Settembre 2019, venivo contattato da un certo Fabio [redacted] il quale spacciandosi per un bro ker di una società di investimenti tale CODEXFX.COM mi proponeva di investire con loro(0934592384;0226112400; 0734993973) .----------//

Dopo la firma di un contratto cominciavo ad investire con versamenti dalle mie carte di credito:

numero 5[redacted] valida fino al 09.2022[redacted]----------//

numero 5[redacted] valida fino al 04/2022[redacted]----------//

numero 5[redacted] valida fino al 08/2020[redacted]----------//

numero 5[redacted] valida fino al 01/2024[redacted]----------//

per un totale di euro 7.500,00 dal 24.09.2019 al 23.12.2019 in favore di CODEXFX.COM.---------//

tramite un addetto della società tale [redacted] Marco che come meglio specificato nell'allegato numero 1, mi convinceva ad effettuare dei bonifici.----------//

In data 25.09.2019 importo di 5.000,00 in favore di codexfx ltd sull'iban LT315510001581407581 dall'iban IT[redacted]----------//

In data 14.10.2019 importo di 2.002,00 in favore di Fx investment sull'iban LT315510001581407581 dall'iban IT[redacted]----------//

In data 14.10.2019 importo di 8.001,00 in favore di Fx investment sull'iban LT315510001581407581 dall'iban [redacted]----------//

In data 15.10.2019 importo di 9.980,00 in favore di Fx investment sull'iban LT315510001581407581 dall'iban [redacted]----------//

In data 08.11.2019 importo di 5.000,00 in favore di TECHVIEW OU sull'iban MT56PHPY270070TECHVIEW000000001 dall'iban [redacted] questo bonifico veniva effettuato a seguito di un bonifico in entrata di euro 5,000.00 da parte della società CodexFx.----------//

In data 22.11.2019 importo di 10.000,00 in favore di Maxiflex ltd sull'iban LT333880010100300749 dall'iban IT[redacted]----------//

Ufficio Denunce
Via Moisè Loria nr. 74 - 20144 Milano - Tel. 0243333011 - Fax 0243333067
compartimento.polposta.mi@pecps.poliziadistato.it

Polizia di Stato

In data 22.11.2019 importo di 40.000,00 in favore di MAXIFLEX LTD sull'iban LT3[redacted]3388001010030074 9 dall'iban IT[redacted].----------//
In data 02.12.2019 importo di 5.000,00 in favore di Techview OU sull'iban MT[redacted]6PHPY270070TECHVIEW000000001 dall'iban IT[redacted].--//
In data 04.12.2019 importo di 25.000,00 in favore di Maxiflex ltd sull'iban LT3[redacted]3388001010030074 9 dall'iban IT[redacted].----------//
In data 05.12.2019 importo di 5.000,00 in favore di Goldencrypto OU sull'iban LT403880010100301884 dall'iban IT[redacted].----------//
In data 10.12.2019 importo di 3.000,00 in favore di Goldencrypto OU sull'iban MT[redacted]0PHPY270070PHOENIX0000253952 dall'iban IT[redacted].---//
In data 10.12.2019 importo di 5.000,00 in favore di Globalnetint sull'iban LT403880010100301884 dall'iban IT[redacted].----------//
In data 20.12.2019 importo di 23.000,00 in favore di globalnetint uab sull'iban LT403880010100301884 dall'iban IT[redacted].----------//
In data 09.01.2020 ricevevo una telefonata da +390289735055 da una persona che diceva di lavorare per la società CodexFx informandomi che il bonifico emesso da loro in mio favore di euro 271,893.00, era stato bloccato dalla società internazionale in quanto io avevo bloccato chiedendo il rientro di un bonifico di 5,000.00 euro(allegato a).----------//
Per quanto di cui sopra dichiaro che ignoti tramite artifizi e raggiri mi hanno truffato.----------//
Preciso che la somma che ho versato è di circa 173.680,00 euro----------//
Allegato tutta la documentazione in mio possesso.----------//
Con la presente QUERELA chiedo la punizione dei responsabili dei reati che l'A.G. vorrà ravvisare.----------//
Chiedo di essere avvisato in caso di archiviazione.----------//
Letto, confermato e sottoscritto in data ora e luogo di cui sopra, previo rilascio copia del presente atto all'interessato unitamente all'avviso alla persona offesa del reato art.90-bis c.p.p.----------//

Il Querelante

Gli Ufficiali e Agenti di P.G.

Polizia di Stato

POLIZIA DI STATO

COMPARTIMENTO POLIZIA POSTALE
E DELLE COMUNICAZIONI
LOMBARDIA

OGGETTO: Verbale di integrazione di Querela sporta da:
A [redacted], nato a [redacted] il [redacted], residente a Milano in Viale [redacted] 6, identificato mediante Carta di identità elettronica numero [redacted] rilasciata da Comune di Milano in data [redacted] valida fino al [redacted], recapito telefonico [redacted].---------//

L'anno 2020, addì [redacted] del mese di Gennaio, alle ore [redacted] in Milano, presso gli Uffici del Compartimento Polizia Postale e delle Comunicazioni per la Lombardia siti in via Moisè Loria nr. 74, innanzi a noi sottoscritti Ufficiali ed Agenti di P.G. Sov. [redacted] ed Agt. Scelto [redacted], in forza all'Ufficio in intestazione è presente il nominato in oggetto, il quale per ogni effetto di legge integra quanto segue:----------//
Integro documentazione inerente telefonata(0390289735055 e +447874961438) ricevuta in data 13.01.2020 da addetti della Codexfx i quali mi chiedevano di non bloccare o richiamare i bonifici perchè altrimenti non avrebbero "dato il consenso" al pagamento di 271893,00.----------//
Allego documentazione in mio possesso.----------//
Letto, confermato e sottoscritto in data ora e luogo di cui sopra, previo rilascio copia del presente atto all'interessato unitamente all'avviso alla persona offesa del reato art.90-bis c.p.p.----------//

Il Querelante

Gli Ufficiali e Agenti di P.G.

Polizia di Stato

English | Mappa | Contatti | Ufficio stampa | A A+ A++

CONSOB | COMMISSIONE NAZIONALE PER LE SOCIETA' E LA BORSA

Autorità italiana per la vigilanza dei mercati finanziari

La Consob | Regolamentazione | Soggetti e mercati | Prospetti e Documenti OPA | Pubblicazioni | Comunicazioni | Occhio alle truffe! | FinTech

Sei in: CONSOB / AREA PUBBLICA / OCCHIO ALLE TRUFFE!

OCCHIO ALLE TRUFFE!

- Imprese di investimento italiane - Sim
- Imprese Ue con succursale in Italia
- Imprese Ue senza succursale in Italia
- Società non autorizzate ad operare - avvisi ai risparmiatori
- Fiduciarie
- Consulenti finanziari
- Servizi per segnalare una truffa
- Telefono
- Associazioni dei consumatori

OCCHIO ALLE TRUFFE!

L'esercizio nei confronti del pubblico dei servizi e attività di investimento è riservato ai soggetti autorizzati dalla CONSOB.

Nella stragrande maggioranza dei casi l'operatività dei soggetti NON AUTORIZZATI, privi quindi dei requisiti, tra cui quelli patrimoniali e organizzativi, previsti dall'ordinamento, anche a tutela degli investitori, si sostanzia in vere e proprie TRUFFE.

Per saperne di più clicca qui

TRADING ONLINE

→ Come difendersi

→ Verifica se il soggetto è autorizzato

VEDI ANCHE

Avvisi della settimana a tutela dei risparmiatori

Area verde "Educazione finanziaria", "truffe e abusivismi"

PROVVEDIMENTI CONTRO SITI ABUSIVI

Interventi trimestrali Consob di contrasto all'attività abusiva ai sensi dell'art. 7-octies del TUF

Interventi Consob per l'oscuramento dei siti abusivi di trading on line - Nuovi poteri di vigilanza attribuiti dal "decreto crescita"

APPROFONDIMENTI

Rischi per i consumatori: valute virtuali e criptovalute

Avviso dell'Esma del 9 gennaio 2019: Initial Coin Offerings and Crypto-Assets

Comunicato della FINMA in merito agli «stable

Polizia di Stato

AVVISI SPECIFICI: SELICOIN

CONSOB | COMMISSIONE NAZIONALE PER LE SOCIETA' E LA BORSA

Autorità italiana per la vigilanza dei mercati finanziari

AVVISI AI RISP

Blueford Consul
Rising Speed In
Yulanta Busines
Kuvera LLC - Fa
Premium - Race
Monetix Service
Investing - Soft
Interstate Europ
criptovalute e st

Le autorità di vigil
Nacional del Merc
Quebec), Lussemb
Market Authority
autorizzazioni.

Segnalate dalla F

- **Blueford**
- **M. Succes**
- **Andreas**
- **Wagon Fi**
- **31FX** (htt
- **ASCO Inv**

Segnalate dalla S

- **www.asia**
- **Rising Sp**

Segnalate dalla C

- **Red Básica** (http://www.redbasica.com);
- **selinusinvestment.com, selicoin.io** (precedentemente segnalato dalla Cnmv, pubblicato in "*Consob Informa*" n. 24/2019 del 1° luglio 2919);
- **MMTIG** (https://mmtig.com);
- **FinRally / Algobit LTD** (www.finrally.com);

BaFin Federal Financial Supervisory Authority

16.08.2019 | Topic Unauthorised business

Identity fraud: selinusinvestment.com and selicoin.com (formerly selicoin.io)

The Federal Financial Supervisory Authority (Bundesanstalt für Finanzdienstleistungsaufsicht – BaFin) is issuing a warning that the operators of the websites selinusinvestment.com and selicoin.com (formerly selicoin.io) have no connection with the licensed companies Selinus Capital GmbH and Selinus Capital Advisors GmbH, both based in Frankfurt am Main, Germany.

The operators are advertising the distribution of financial products while fraudulently referring to the above-mentioned companies based in Frankfurt.

OF2CEN

ONLINE FRAUD CYBER CENTRE AND EXPERT NETWORK

- Progetto per il contrasto al fenomeno del Phishing
- Piattaforma di condivisione di informazioni tra le forze dell'ordine e le Banche
- Interventi tempestivi per congelamento di conti correnti e carte in frode
- Recupero somme frodate
- Inserimento in black list degli indirizzi IP e degli IBAN dei phisher
- Analisi del fenomeno

Polizia di Stato

SECONDO PASSAGGIO

→ Se hai investito

Ricorda che l'esercizio abusivo di servizi e attività di investimento è un **reato** punito con la reclusione fino ad un massimo di 8 anni (art. 166 del Testo unico della Finanza - Tuf).

→ Invia un esposto tramite il modulo esposti online.

→ denuncia il soggetto alle autorità di pubblica sicurezza

→ segnala il soggetto alla CONSOB

Diffida di soggetti che ti promettono il recupero del denaro investito.

Indici di allerta

- Alle tue domande il soggetto che ti ha contattato non ha fornito risposte chiare;
- Le risposte fornite non hanno trovato riscontro nel web e nei siti da te esaminati;

Grazie per l'attenzione

Polizia di Stato

MAIL ESTORSIVA 1/7

I do know angelo is your pass. Lets get right to the point. You do not know me and you're probably thinking why you're getting this e-mail? Not one person has paid me to check you.

MAIL ESTORSIVA 2/7

In fact, I setup a software on the adult video clips (pornography) web site and there's more, you visited this website to experience fun (you know what I mean). While you were viewing videos, your internet browser initiated functioning as a RDP having a key logger which provided me with accessibility to your screen as well as web cam

MAIL ESTORSIVA

after that, my software program obtained your entire contacts from your Messenger, FB, as well as e-mailaccount. After that I created a video. 1st part shows the video you were watching (you've got a good taste haha . . .), and next part displays the view of your webcam, yea its you.

MAIL ESTORSIVA

You got a pair of alternatives. Why dont we review each of these solutions in aspects:

1st solution is to skip this message. In such a case, I am going to send your video to every one of your contacts and then visualize about the awkwardness you feel. Furthermore if you happen to be in an intimate relationship, precisely how it will eventually affect?

MAIL ESTORSIVA

Latter solution is to give me $1000. We will regard it as a donation. In such a case, I most certainly will straight away delete your video recording. You could keep going your life like this never took place and you never will hear back again from me.

You'll make the payment via Bitcoin (if you do not know this, search for "how to buy bitcoin" in Google).

BTC Address: 1MN7jxLUteSmMCFVUFJL8sjyS9m217CDiW

[CASE-sensitive, copy & paste it]

MAIL ESTORSIVA

If you are making plans for going to the law, very well, this email cannot be traced back to me. I have taken care of my steps. I am not attempting to charge you a lot, I would like to be rewarded. You now have one day in order to pay. I have a unique pixel in this mail, and now I know that you have read this message.

MAIL ESTORSIVA

If I don't get the BitCoins, I will, no doubt send out your video recording to all of your contacts including family members, coworkers, and many others. Having said that, if I receive the payment, I will destroy the video immediately. This is the nonnegotiable offer, and so please do not waste mine time and yours by responding to this message. If you really want evidence, reply with Yeah and I will send your video to your 10 contacts.

Polizia di Stato

CONSIGLI

Polizia di Stato

GLI ERRORI PIU' COMUNI 1/2

1. **Password deboli e/o condivise**
2. **Stessa mail e stessa password (magari quelle dell'ufficio!) per tanti servizi on-line**
3. **No PIN / password sui dispositivi mobili e app in «*autologon*»**
4. **Postazione o smartphone senza blocco/screensaver**
5. **Antivirus non aggiornato**
6. **Software freeware/shareware da fonte non verificata**

Polizia di Stato

GLI ERRORI PIU' COMUNI 2/2

7. **Non controllare validità di mail** ed eseguire istruzioni per curiosità
8. **Collegarsi a qualsiasi rete *wifi free***
9. **Dispensare informazioni personali su qls sito** per download di software o documenti
10. **Pubblicare sui social la cronaca delle attività quotidiane**
11. **Non leggere informative e/o accordi di licenza**
12. **Copiare dati (anche riservati) su chiavetta USB non cifrata e non cancellarli mai** (tanto è attaccata al portachiavi che tengo nella stessa borsa dove ho riposto il telefono, quello con le app in autologon … e le chiavi dell'armadio aziendale)