



**ATTACCHI INFORMATICI:
RIFLESSIONI ANDAMENTO ANNO 2017**

CYBER SECURITY SUMMIT
Milano, 31 maggio 2018



PRINCIPALI AREE DI COMPETENZA

PEDO PORNOGRAFIA ONLINE

FINANCIAL HACKING

INFRASTRUTTURE CRITICHE

FRODI INFORMATICHE SU LARGA SCALA

HACKING

CYBER-TERRORISMO



Funzioni Principali

«Cultura» del Web Sicuro



Prevenzione mirata



Contrasto operativo



Metodologia

Programmi nazionali per le scuole

Progetti e Servizi avanzati

Tecniche speciali di investigazione



Progetti e Servizi Avanzati

**CHILDE ABUSE/PORNOGRAPHY
ADVANCED WEB
MONITORING AND FILTERING**

**WEB MONITORING FOR
ANTITERRORISM PURPOSES**

**G8 - INTERNATIONAL POINT OF
CONTACT FOR CYBERCRIME**

**PROTECTION OF STRATEGIC
CRITICAL INFRASTRUCTURES**

**ONLINE FRAUDS AND CYBER CRIME
EXPERT NETWORK (OF2CEN)**



CENTRO NAZIONALE ANTICRIMINE INFORMATICO PER LA PROTEZIONE DELLE INFRASTRUTTURE CRITICHE



CNAIPIC - Anno 2017

Diramati **31524** *Alert* alle infrastrutture critiche nazionali (cinque volte rispetto al 2016)

Gestiti:

1032 attacchi informatici nei confronti di servizi internet relativi a siti istituzionali e infrastrutture critiche informatizzate di interesse nazionale;

83 richieste di cooperazione nell'ambito del circuito "High Tech Crime Emergency".

72 indagini per un totale di **34** persone denunciate e **2** arrestate.



CENTRO NAZIONALE ANTICRIMINE INFORMATICO PER LA PROTEZIONE DELLE INFRASTRUTTURE CRITICHE



CNAIPIC - 1° Trimestre 2018

ATTACCHI	GEN	FEB	MAR	APR
ACCESSI ABUSIVI/DUMP	41	4	14	24
DEFACEMENT	24	6	4	39
DDOS	0	0	7	3
ALTRI ATTACCHI	5	12	3	3
TOTALE RILEVATI	70	22	28	69
TOTALE ALERT	116	178	94	119

VULNERABILITA' E MINACCE	GEN	FEB	MAR	APR
VULNERABILITA' RILEVATE	16	50	25	3
MINACCE	71	66	82	73
TOTALE RILEVATE	87	116	107	76
SEGNALAZIONI	3434	4364	5555	4804
<i>Vulnerabilità + Minacce</i>				
TOTALE SEGNALAZIONI	3550	4542	5649	4923



accounts



Intermediate accounts



Online gaming

Destination accounts



Cash withdrawal Online Purchases Recharge Cards

Illegal Profits



*Data Breach
Privacy
Identity Theft
Fraud*

*Impersonation
Hacking
Fraud
Self-Money Laundering*

*Fake ID
Credit Card Frauds
Stolen merchandise
Self-Money Laundering
Money Laundering*



OF2CEN
ONLINE FRAUDS CYBER CENTRE AND EXPERT CENTER

ONLINE FRAUD CYBER CENTRE

Partenariato pubblico-privato che ha portato alla stipula di convenzioni intercorse mediante ABI con gran parte del mondo bancario.

Consente di intervenire in tempo quasi reale sulla segnalazione bloccando la somma prima che venga polverizzata in vari rivoli di prestanome

Polizia Postale e delle Comunicazioni

Dato Nazionale Frodi Anno 2017:

Denunce ricevute **1009**
per importi frodati **15.673.027,00 €**
Persone denunciate **151**

Dato Nazionale Frodi 1° Trim. 2018:

Denunce ricevute **201**
per importi frodati **1.845.557,00 €**
Persone denunciate **10**
Persone Arrestate **12**

Piattaforma OF2CEN anno 2017:

Importo inserito **26.717.865,97 €**
Importo bloccato **22.365.232,14 €**
 (84%)

Importo perso **4.352.633,83 €**
Importo stornato **900.000,00 €**



BEC e CEO Fraud anno 2017 in danno del settore bancario/finanziario e industriale

Settore merceologico	tipologia di frode	Importo frode	Consumato	Tentato	Descrizione
Bancario	B.E.C.	€ 5.000.000,00	X		(1)
Bancario	C.E.O.	€ 480.000,00	X		(2)
Bancario	C.E.O.	€ 480.000,00		X	(3)
Industriale	C.E.O.	€ 480.000,00		X	(4)
Industriale	C.E.O.	€ 700.000,00		X	(5)
Industriale	C.E.O.	€ 6.000.000,00	X		(6)
Industriale	C.E.O.	€ 480.000,00	X		(7)

(1)

Ignoti tramite e-mail si sono sostituiti ad un fornitore di servizi di un istituto di credito italiano inducendo quest'ultimo a saldare una fattura regolarmente emessa dirottando il relativo bonifico su un c/c bancario sotto il controllo del sodalizio criminale.

(2)-(3)-(4)-(5)-(6)

Ignoti tramite e-mail si sono sostituiti al C.E.O., inducendo in errore il dipendente addetto ai pagamenti, ordinandogli di disporre bonifici, a fronte di non meglio specificate operazioni finanziarie, in favore di c/c bancari sotto il controllo del sodalizio criminale.



FATTORI DI RISCHIO

**DISPOSITIVI ACCESI/SPENTI
«SEMPRE CONNESSO»
PASSWORD
(DIS)ABILITAZIONI UTENTE
CRITTOGRAFIA**

**USO PROMISCO
ACCOUNT UNICO
VISIBILITA' (DISPOSITIVO E DATI)
CONNESSIONI NON SICURE
SOCIALIZZAZIONE ONLINE**

**TEMPI DI ESECUZIONE
PROCESSI SENSIBILI INDIVIDUALIZZATI
SOTTOVALUTAZIONE CONTENZIOSO
DANNO REPUTAZIONALE
RUOLO FUNZIONE DI SECURITY**

**COMPARTIMENTAZIONE
FIREWALL AGGIORNATI
TRACCIAMENTO IP
CUSTODIA FILES DI LOG
AMMINISTRAZIONE RETE
AGGIORNAMENTI**



CONDIZIONE 1:
SEPARAZIONE TRA DISPOSITIVI
AZIENDALI E PERSONALI
TRA RETE SVILUPPO E COMMERCIALE
(ISOLAMENTO)

CONDIZIONE 2:
POLICY DI SICUREZZA
ORGANIZZATIVA E INFORMATICA
COLLEGIALITA' OPERATIVA
(COMPORTAMENTO)

CONDIZIONE 3:
SISTEMI DI SICUREZZA
HARDWARE E SOFTWARE
(PROTEZIONE)

CONDIZIONE 4:
MONITORAGGIO
DELLA SICUREZZA
(CONTROLLO)



Funzioni Principali

«Cultura» del Web Sicuro



Prevenzione mirata



Contrasto operativo



Metodologia

Programmi nazionali per le scuole

Progetti e Servizi avanzati

Tecniche speciali di investigazione



INCONTRI DI «PROSSIMITA'» E PROGETTO «UNA VITA DA SOCIAL»

Manifestazione itinerante nelle città del Paese per incontrare giovani, scolaresche e famiglie e dialogare con loro su come prevenire i principali rischi derivanti dall'uso dei servizi della Retet. Legato ai programmi di insegnamento nelle scuole, in un ampio partenariato pubblico-privato, il progetto punta a prevenire l'adescamento di minori, il cyberbullismo, le condotte contro la privacy, il copyright e il download di materiali inappropriati.

Dato Nazionale Progetto:

Studenti incontrati: 1.300.000

Insegnanti incontrati: 82.500

Scuole coinvolte: 10.750

Città: 190

Altri incontri educativi:

250.000 studenti

2500 Istituti Scolastici

APP «YOU POL»



Grazie per l'attenzione
salvatore.labarbera@interno.it