EUROPEAN CYBERCRIME CENTRE

EC3

EUROPOL

EC3
European Cybercrime Center

10TH AICOM Compliance Meeting , 25 June 2014

Paul Gillen
Head of Operation
EC3

European Cyber Crime Centre EC3

2013

Gennaio

1

EC3 é operativo

Aree Mandato dell' EC3

Reati informatici commessi da Gruppi Criminali Organizzati, con particolare attenzione ai delitti che generano ingenti profitti illeciti (es.Frodi online)

Delitti informatici che arrecano un grave danno alle vittime degli stessi (es. Pedopornografia, sfruttamento sessuale di minori on line)

Crimini informatici (compresi i c.d. cyber-attacks) che colpiscono le strutture critiche ed informatiche nei Paesi Membri e dell' Unione Europea.

Joint Cyber Crime Action task Force (J-CAT)

I reati informatici sono caratterizzati da modus operandi particolarmente efficaci e flessibili, possono colpire piú giurisdizioni contemporaneamente. Frontiere e norme giuridiche non rappresentano un ostacolo alla loro diffusione.

Le finalitá del J-CAT sono:

- Condurre in modo proattivo attivitá coordinate nei confronti di specifiche minacce informatiche e target di elevato livello;
- Potenziare lo scambio di intelligence;
- Evitare la duplicazione e sovrapposizione di misure investigative e cautelari;
- Individuare e condividere le prioritá;
- Indicare ed affrontare in modo congiunto ed armonico le forme di reato con il piú forte impatto criminale che affliggono piú paesi dell'UE;
- Ottimizzare le risorse investigative disponibili all'interno delle unitá Cybercrime nei Paesi Membri dell' Únione.

EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

AIRLINE ACTION DAY

Premesse:

11% delle frodi con carte di credito deriva dall'acquisto fraudolento di biglietti aerei;

Le singole Forze di Polizia non hanno una visione completa del fenomeno tanto da poter contrastare adeguatamente la minaccia;

Mancanza di coordinazione tra settore privato (Comp.Aeree) e Forze di Polizia.

Risultati :

- **2** giorni di Azione;
- **68** aeroporti interessati;
- **24** paesi dell'UE unitamente a Stati Uniti, Svizzera, Norvegia, Islanda, Colombia, Ucraina, Brasile e Peru;

  70 persone arrestate;
- **117** persone denunciate in stato di libertá;
- supporto tecnico di Visa, Mastercard ed American Express;
- Collegamento con altre forme di reato: frode, immigrazione illegale, traffico di esseri umani e sostanze stupefacenti, terrorismo, pedofilia.
- Consolidato rapporto di cooperazione tra FF.PP e compagnie aeree.

EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

OPERAZIONE "GO NO GO""

Indagine condotta dall'FBI nei confronti della rete Botnet peer to peer Game over Zeus (GOZ)

GOZ é la rete Botnet piú attiva che affligge il settore banking a livello mondiale

Durante i 3 giorni di Azione:
L'infrastruttura portante di GOZ é stata smantellata in Europa, USA, Giappone, Nuova Zelanda, Ucraina e Canada
1Milione di Botnet neutralizzati

L'intera rete di Botnet é stata disarticolata e resa incapace di comunicare

La struttura ospite del ransomware Cryptolocker smantellata nei Paesi Bassi

EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

OPERAZIONE DOWN FALL

Indagine dell' FBI nei confronti di Freedom Hosting e le sue attivitá criminali connesse all' abuso di minori sulla rete internet;

Servers ubicati nei Paesi Bassi;

EC3 sulla base delle direttive ricevute dalla Procura Olandese ha coordinato l'operazione che ha visto coinvolti ben **13** paesi dell Unione

11 arresti e perquisizioni domiciliari

85 collegamenti con casi aperti

20 collegamenti con nuovi potenziali casi

EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

Strategia di EC3

- Condurre attivitá coordinate nei confronti di specifiche minacce informatiche di elevato livello;
- Potenziare lo scambio di intelligence;
- Evitare la duplicazione e sovrapposizione di misure investigative;
- Individuare e condividere le prioritá;
- Condivisione delle responsabilitá circa le azioni/iniziative intraprese;
- Cooperazine con il Settore privato, Istituzioni ed Universitá.

Grazie

paul.gillen@europol.europa.eu