CERTFin

CERT Finanziario Italiano

La sfida tra hacker evoluti e nuove strategie di cyber security

Milano, 9 novembre 2018

Giorgio Orlandi

Cyber Security and Fraud Analyst

TLP GREEN

Un approccio cooperativo in risposta alle minacce cyber

Le minacce cyber hanno **caratteristiche** e generano **impatti molto simili**, indipendentemente dall'organizzazione coinvolta

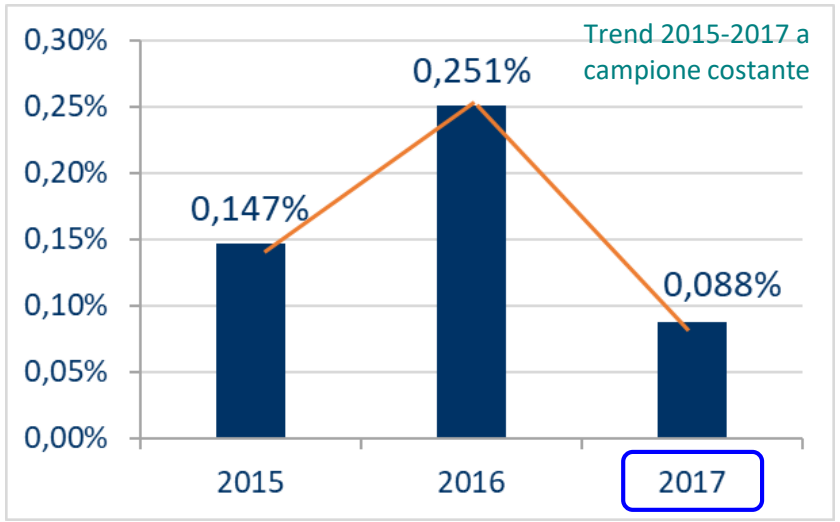
Soggetti con **intenzioni criminali,** possono attaccare **diversi obbiettivi con un singolo strumento** (sw o hw)

Le iniziative di settore consentono la cooperazione tra i diversi stakeholders ed incentivano nuove **sinergie di difesa**, come promosso dal piano nazionale in tema di cybersecurity

Furto di credenziali digitali e danno economico
Clientela Retail

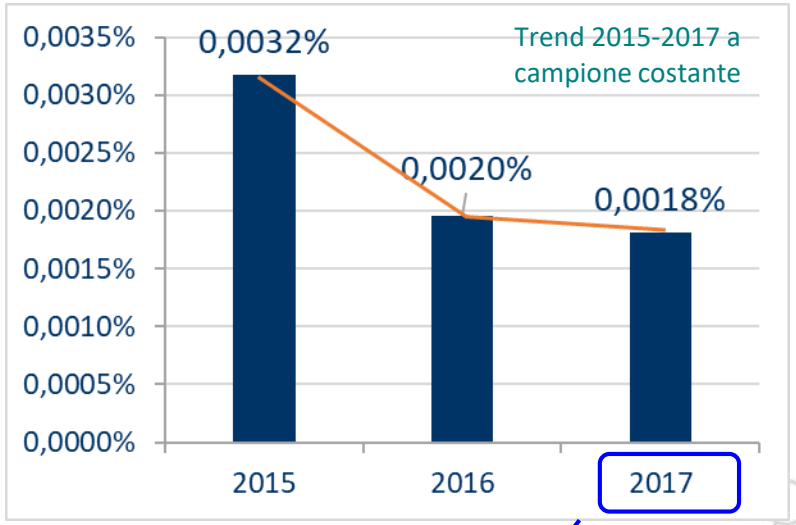
L'**81,5**% dei rispondenti ha registrato nel **2017** un **furto di credenziali di accesso** ai servizi di Internet / Mobile Banking ai danni della clientela Retail

Percentuale di clienti attivi Retail che hanno subito un furto di credenziali



Gli **attacchi di phishing** costituiscono il principale vettore di furto di identità (**91,1%**)

Percentuale di clienti attivi Retail che hanno perso denaro



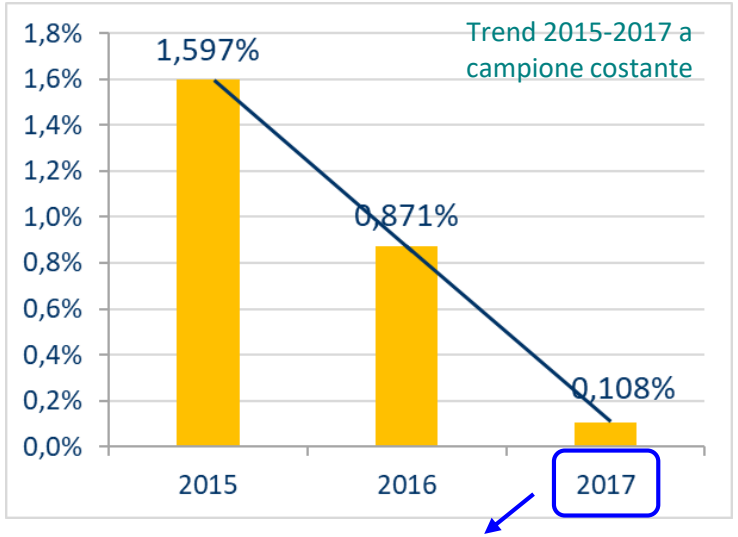
Trend in lieve **diminuzione** rispetto al 2016 → si rivelano efficaci gli strumenti e i processi messi in atto dalle banche: circa **1 ogni 55.500** utenti attivi ha subito un danno economico

Fonte: CERTFin, Osservatorio Cyber Knowledge and Security Awareness, Survey Information Security e Frodi Internet e Mobile Banking, 2018 (Campione complessivo: 29 rispondenti)

Furto di credenziali digitali e danno economico
Clientela Corporate

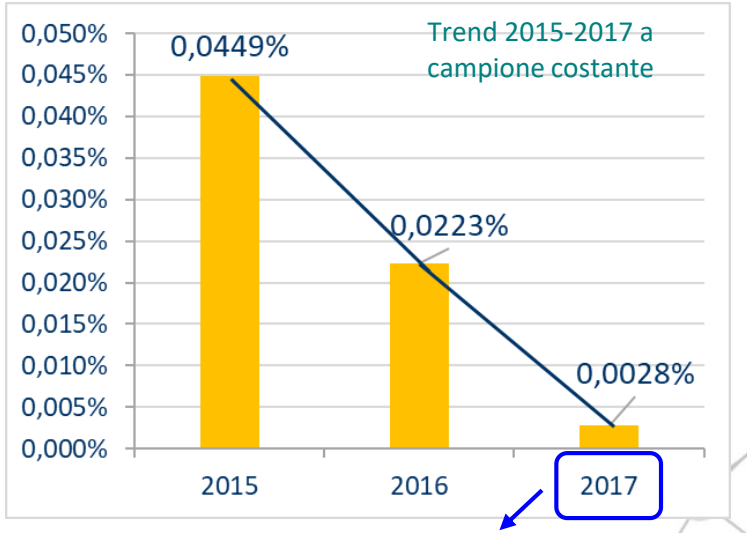
L'**84,6**% dei rispondenti ha registrato nel **2017** un **furto di credenziali di accesso** ai servizi di Internet / Mobile Banking ai danni della clientela Corporate

Percentuale di clienti attivi Corporate che hanno subito un furto di credenziali



Il **crimeware** è il vettore più utilizzato per la sottrazione delle credenziali e la realizzazione della frode (**71,8%**)

Percentuale di clienti attivi Corporate che hanno perso denaro



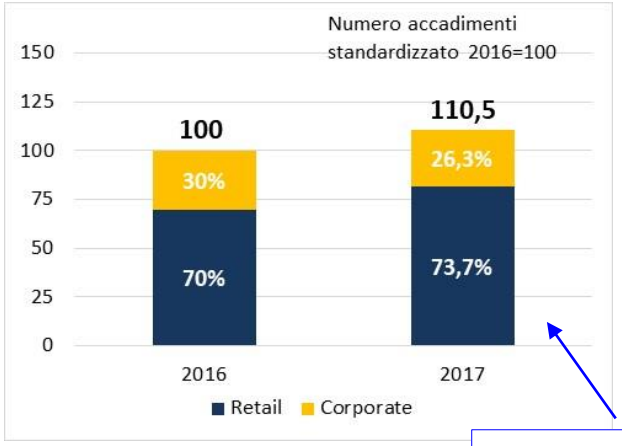
Trend di decrescita sui 3 anni molto marcato, pari a -**94%**

Anche a fronte di una netta diminuzione delle frodi basate sul furto di identità, si osserva un'evoluzione degli attacchi contro le imprese verso **nuovi modelli** finalizzati a «**manipolare**» l'utente, inducendolo ad eseguire transazioni – spesso di **importi economici ingenti** – a beneficio dei frodatori

Fonte: CERTFin, Osservatorio Cyber Knowledge and Security Awareness, Survey Information Security e Frodi Internet e Mobile Banking, 2018 (Campione complessivo: 29 rispondenti)

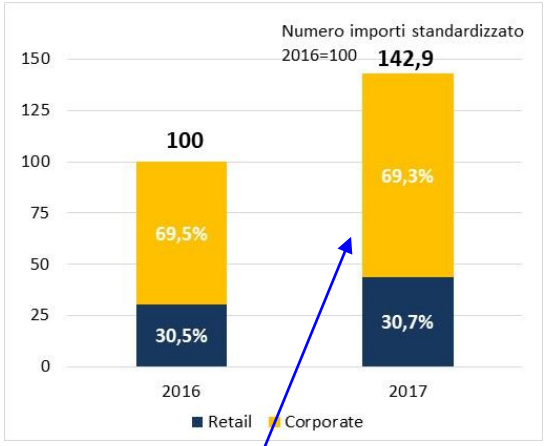
Trend 2016-2017 transazioni anomale ed effettive
Confronto Retail e Corporate

Transazioni **ANOMALE** (bloccate, recuperate ed effettive) – Ripartizione percentuale numero **ACCADIMENTI** tra **Retail e Corporate – Trend standardizzato 2016-2017**



Numero di tentativi e **accadimenti** più **elevato** per il **Retail**

Transazioni **ANOMALE** (bloccate, recuperate ed effettive) – Ripartizione percentuale **IMPORTI economici** transati tra **Retail e Corporate – Trend standardizzato 2016-2017**

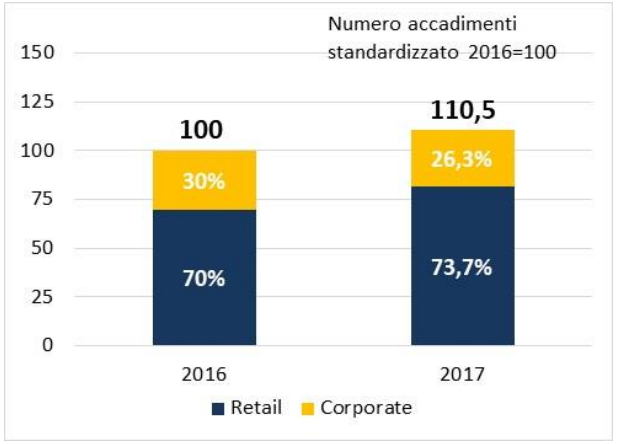


Importi economici più elevati per le frodi contro la clientela **Corporate**

Fonte: CERTFin, Osservatorio Cyber Knowledge and Security Awareness, Survey Information Security e Frodi Internet e Mobile Banking, 2018 (Campione complessivo: 29 rispondenti)

Trend 2016-2017 transazioni anomale ed effettive
Confronto Retail e Corporate

Transazioni **ANOMALE** (bloccate, recuperate ed effettive) – Ripartizione percentuale numero **ACCADIMENTI** tra **Retail e Corporate – Trend standardizzato 2016-2017**



Transazioni **ANOMALE** (bloccate, recuperate ed effettive) – Ripartizione percentuale **IMPORTI economici** transati tra **Retail e Corporate – Trend standardizzato 2016-2017**

Frodi **EFFETTIVE** – Ripartizione percentuale numero **ACCADIMENTI** tra **Retail e Corporate – Trend standardizzato 2016-2017**

Anche a fronte di maggiori tentativi, nel 2017 si riscontra una **diminuzione** delle **frodi** effettive in termini sia di **accadimenti** che di **importi**

Frodi **EFFETTIVE** – Ripartizione percentuale **IMPORTI economici** transati tra **Retail e Corporate – Trend standardizzato 2016-2017**

Fonte: CERTFin, Osservatorio Cyber Knowledge and Security Awareness, Survey Information Security e Frodi Internet e Mobile Banking, 2018 (Campione complessivo: 29 rispondenti)

Attacchi cyber e non solo

Attacchi alla confidenzialità

Data breach

- Pochi casi (solo 2 rilevati nel 2017), ma in 1 caso ha impattato 11.000 clienti

Attacchi alla disponibilità..

..del servizio (DoS-DDoS)

- Rilevati da 5 banche (in 3 hanno subito 6 attacchi)
- Nessun impatto significativo

..dei dati (ransomware)

Rilevati dal 46,2% del campione

Nessun impatto significativo

Nuovi fenomeni di social engineering – Manipolazione utente

- BEC – rilevati dal 40% delle banche
- CEO Fraud – rilevati dal 28% delle banche
- Numerosità dei casi esigua ma i volumi in gioco sono elevati

Altri casi di frode

- Attacchi a postazioni che hanno interessato i servizi SWIFT, non rilevati in Italia (in Bangladesh sottratti oltre 80 milioni di dollari)

Fonte: CERTFin - Osservatorio Cyber Knowledge and Security Awareness, 2018, 29 rispondenti

Attività di information sharing
Principali fenomeni rilevati e lesson learned (1/2)

Gennaio 2017 - Eye Pyramid

- Rilevato appena 5 giorni dopo la costituzione del CERTFin
- Il fenomeno ha rappresentato l'occasione per «testare» il punto di partenza in tema di collaborazione operativa e network creato negli anni del Presidio.Internet

Aprile 2017 – Blocco manuale bonifico disconosciuto

- Bloccato un bonifico fraudolento grazie alla collaborazione degli attori coinvolti
- È stato possibile impedire la fase di cash out bloccando la carta associata al mulo, con la cooperazione del CERTFin e la collaborazione della banca destinataria. Necessaria una maggior strutturazione nello scambio tempestivo di informazioni su operazioni fraudolente → EU OF2CEN

Maggio - Giugno 2017 – Wannacry & Petya/Not Petya

- Elevato impatto mediatico, cross-industry e cross-country
- Si è ritenuta necessaria un'attività di inforsharing coordinata almeno a livello italiano, avviando poco dopo i lavori per la definizione dell'architettura nazionale di information sharing

Frodi informatiche

Attacchi a dati/ informazioni

Attacchi alla disponibilità di servizi/ asset IT

Attività di information sharing
Principali fenomeni rilevati e lesson learned (2/2)

Agosto 2017 – Attacco in Ucraina

- Minacce di attacchi in concomitanza con festività nazionali (Independence day) e comunicati stampa della BCN
- Elevato livello di attenzione anche in Italia, primi contatti con il DIS per allineamento sullo stato dell'arte nel settore bancario → Opportunità di rafforzare la relazione

Gennaio 2018 – Attacchi DDoS in Olanda

- Attacco diffuso a diversi soggetti (banche e organizzazioni della PA)
- 4 delle principali banche olandesi sono state attaccate; impatti non gravi (indisponibilità di alcuni servizi per pochi minuti), ma il CERTFin si è subito attivato con il CERT Nazionale e i diversi network → E se succedesse in Italia? FOCUS

Aprile 2018 – SIM Swap #N

- Nuovi fenomeni di SIM swap, che hanno generato frodi
- Emergono nuovamente le necessità di rafforzare le iniziative di awareness verso la clientela e di cooperazione con i TELCO, anche individuando servizi e strumenti antifrode

Maggio 2018 – Frodi tramite PEC

- Nessun attacco alle banche, ma sfruttate vulnerabilità di processo di altri soggetti
- Importante rafforzare il livello dei controlli a livello di sistema Paese, le organizzazioni criminali sono sempre più attente a sfruttare anche la minima vulnerabilità

 **Frodi informatiche**

 **Attacchi a dati/ informazioni**

Attacchi alla disponibilità di servizi/ asset IT

Caso reale: attacco DDoS Olanda

29 Gennaio 2018: ING, ABN, Rabo, VolksBank e l'Agenzia per la fiscalità olandese hanno subito un attacco di tipo Distributed Denial of Service (DDoS).

L'attacco su tutti i soggetti è stato di tipo volumetrico e ha raggiunto picchi in alcuni casi di 100gbps.

Quali azioni ha intrapreso il CERTFin?

- **Analisi e studio del fenomeno,** in particolare focalizzandosi su aspetti tecnici come protocollo utilizzato dall'attaccante, portata, tempi di risposta;
- **Segnalazione tempestiva** e **condivisione** con i membri della constituency di tutte le informazioni raccolte;
- **Approfondimento** con il CERT Nazionale e analisi della modalità di attacco impiegata nella campagna, sulla base delle informazioni provenienti dal CERT olandese.

E se succedesse in Italia?

- **Condivisione tempestiva** dei dettagli dell'attacco a beneficio di tutta la constituency;
- **Attivazione** di tutti gli attori coinvolti a supporto della continuità del servizio;
- **Partecipazione attiva** nello scambio informativo dei soggetti direttamente o indirettamente interessati.

Il CERT Finanziario Italiano
Overview

OBIETTIVI PRINCIPALI

- **innalzare** la **capacità** del settore di **gestione dei rischi cyber**
- **coordinamento** centrale delle attività di contrasto e prevenzione degli attacchi

FILONI DI ATTIVITÀ

FINANCIAL INFO SHARING AND ANALYSIS CENTER (FinISAC)

CYBER KNOWLEDGE AND SECURITY AWARENESS

CENTRALE OPERATIVA DI GESTIONE DELLE EMERGENZE CYBER

COMMUNITY

TF-CSIRT Trusted Introducer

CERT IS A MARK OWNED BY CARNEGIE MELLON UNIVERSITY
CERT
AUTHORIZED TO USE CERT

ADESIONI

45 soggetti aderenti al CERTFin

10 partecipanti al **Team Virtuale**

Il CERT Finanziario Italiano come network di collaborazioni per rafforzare la sicurezza

CERT di settore / Entità europee di cybersecurity

Nordic Financial CERT

NCSC-UK

…

CERT nazionali di altri Paesi

CERT Austria

CERT Lussemburgo

CERT Polonia

CERT Svizzera…

Istituzioni e centri di competenza

DIS

CERT Nazionale/ CERT-PA

MEF

Università

…

Forze dell'ordine

Telco Provider

CERTFin

CERT Finanziario Italiano

Organizzazioni internazionali

…attraverso ABI Lab

Constituency

Banche e operatori finanziari

Team Virtuale

Imprese di assicurazione

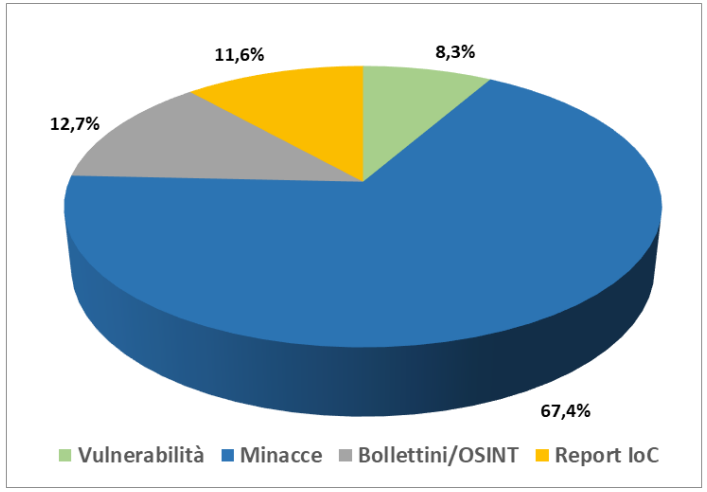
Altri operatori

COMING SOON

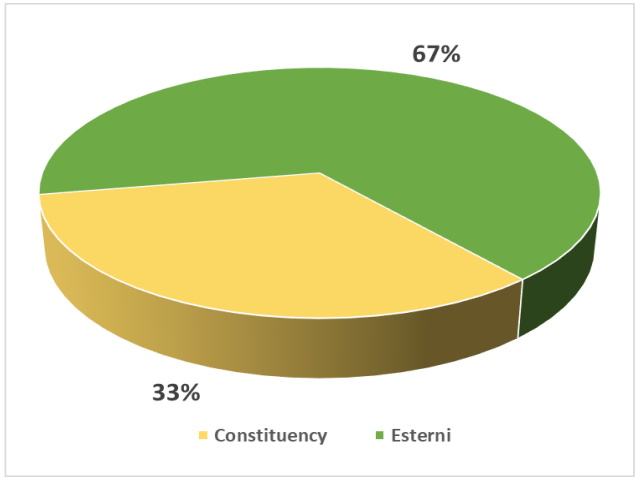
Resoconto attività CERTFin 1° gen – 7 set 2018
Information Sharing - FinISAC

*Elaborazione Tax. da https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/existing-taxonomies

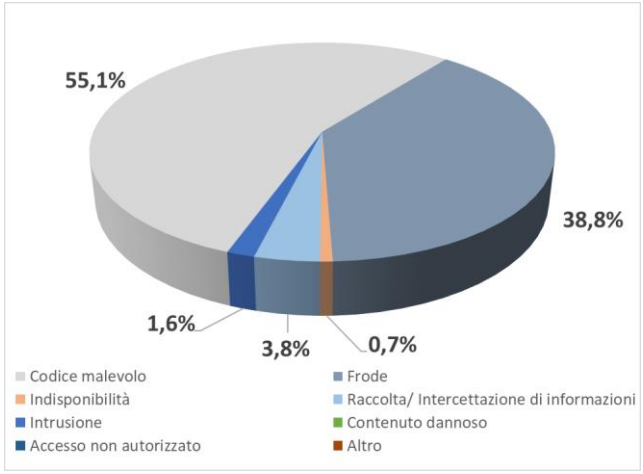
TIPOLOGIE SEGNALAZIONI



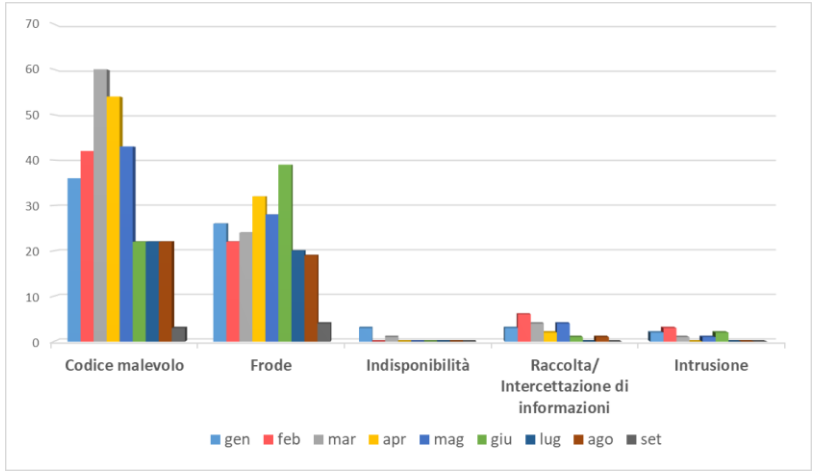
DETTAGLIO FONTI SEGNALAZIONI



DETTAGLIO MINACCE SEGNALATE



DETTAGLIO MINACCE SEGNALATE - TREND

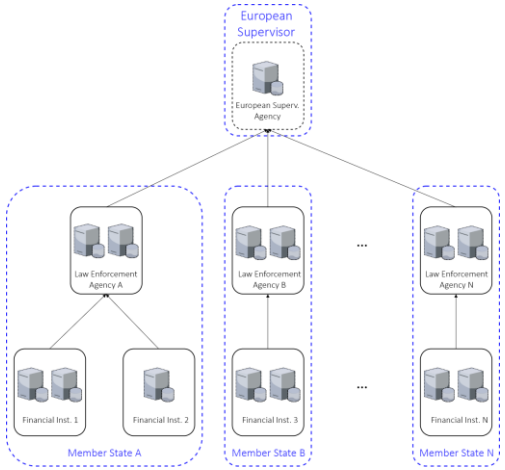


Piattaforme per la collaborazione e Information Sharing

Funded by the European Union

FULLY OPERATIONAL

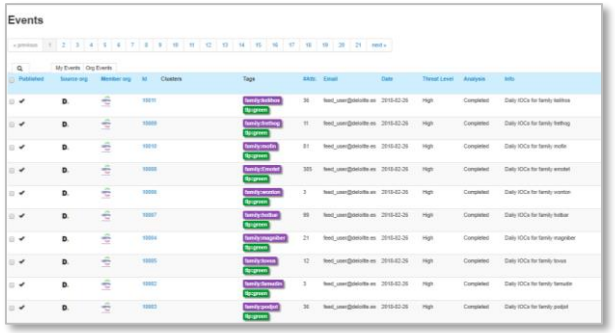
- **EU OF2CEN** mira a **definire una piattaforma di Information Sharing** basata sulla **collaborazione tra LEA e banche a livello Europeo**



- **Rende possibile il "network of networks"**, connettendo differenti Stati che scambiano informazioni secondo metodi e procedure conformi alle leggi europee

FULLY OPERATIONAL

- La **Malware Information Sharing Platform (MISP)** permette agli utenti di **ricevere informazioni sugli attacchi e sul fenomeno fraudolento** in maniera strutturata in formato machine readable (STIX)



- Accresce il **tempestivo e costante scambio di informazioni**, utile per **rilevare**, **prevenire** e **contrastare eventi** che impattano l'integrità, la disponibilità e la riservatezza delle informazioni

Il progetto REDFin - Readiness Enhancement to Defend Financial Sector

Il progetto **REDFin**, iniziato il 1° settembre e con una durata di 24 mesi, mira ad aumentare **la capacità** del settore bancario italiano **di rispondere agli attacchi cyber** e nel complesso di migliorare la sua **cyber resilience**.

Programme co-funded by the EUROPEAN UNION

OBIETTIVI PRINCPALI

- adottare una **metodologia avanzata** per **l'identificazione** degli **scenari di minaccia;**
- **definire** una **metodologia** per la conduzione degli **esercizi cyber table top e red teaming**, utilizzando come fonte principale il framework TIBER EU;
- **coordinare** l'esecuzione degli esercizi cyber table top e red teaming, per rilevare la **capacità di identificazione e contrasto degli attachi cyber;**
- **promuovere** l'information sharing e la condivisione dei risultati del progetto tra i principali stakeholders.

Coinvolgimento di numerosi **stakeholder**, sia nazionali (es. Banca d'Italia, MEF, CSIRT Italiano), che europei (es. ENISA, EBF, ECB, Europol, LEAs)

I fondi stanziati saranno dedicati a rafforzare le capacità del CERTFin nell'ambito dell'**identificazione** degli scenari di minaccia e delle attività di **intelligence testing**