CERTFin

Scenario Italiano Cyber nel settore finanziario

Romano Stasi

Direttore Operativo CERTFin

Il CERTFin – la mission

Facilitare il **tempestivo** scambio di informazioni all'interno del settore

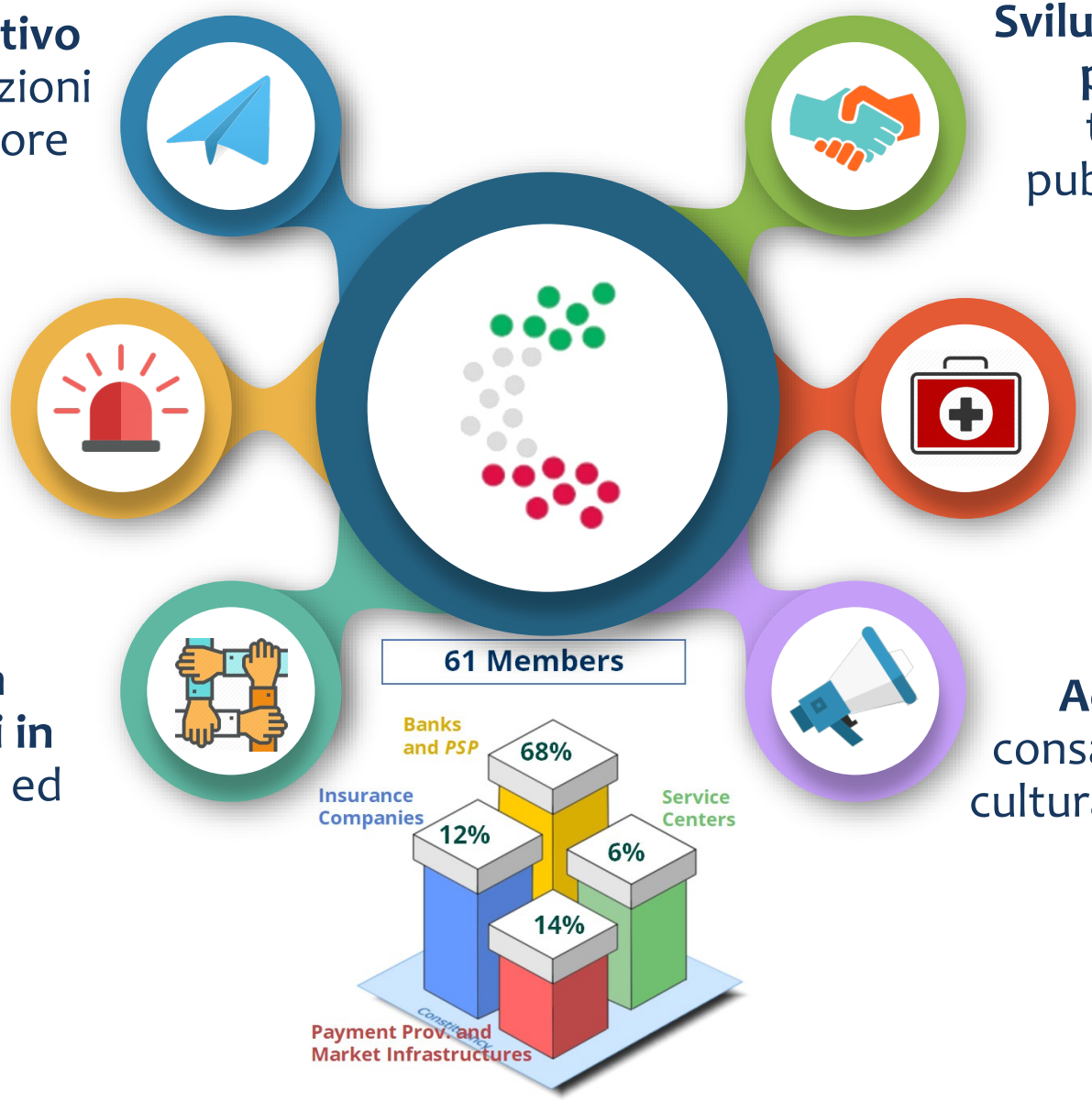
Facilitare la risposta del settore al verificarsi di cyber-incidenti su larga scala

Cooperare con strutture similari in ambito nazionale ed internazionale

Sviluppare logiche di partenariato tra il settore pubblico e privato

Supportare la risposta agli incidenti e il processo di gestione delle crisi

Accrescere la consapevolezza e la cultura della sicurezza



Recenti attività del CERTFin

- Realizzazione di una Sperimentazione **anti-SIM swap;**
- Supporto alla Realizzazione **infrastruttura MISP** del CERTFin a livello europeo (EPC);
- Diffusione di un Nuovo **Protocollo di Collaborazione interbancario** in materia di Frodi;
- Promozione e realizzazione di esercizi di RED TEAMING e simulazioni TABLE TOP con le banche nel 2020 nell'ambito del progetto europeo **REDFin;**
- Pubblicazione del **Threat Landscape Scenario** 2020;
- Crescita della rete di collaborazione con altri CERT-ISAC Finanziari (es. F-ISAC Japan, Tunisian Financial CERT, TB-CERT Thailand)
- Contributo alla diffusione del **Framework Nazionale CyberSecurity** in ambito finanziario;
- **NUOVO REPORT 2021 SICUREZZA E FRODI INFORMATICHE IN BANCA.**

Sintesi operatività

CERTFin Frodi informatiche: le dinamiche del 2020/21

- Nel contesto ormai pienamente digitale di oggi si registra un **deciso aumento dei tentativi di frode**, cresciuti di circa otto volte rispetto al 2019. Oltre al numero di eventi, il 2020 è stato un anno in cui sono cresciuti anche gli **importi economici** associati alle transazioni fraudolente;

- La capacità del settore finanziario di reagire agli attacchi rimane elevata, **la quota di tentativi di frode bloccati si mantiene al 83%;**

- Le tecniche di attacco si sono spostate verso **soluzioni maggiormente sofisticate** (c.d. «miste» 65%) , più complesse da intercettare che prevedono sempre modalità di manipolazione dell'utente per acquisire dati sensibili; sempre più sottile distinzione degli attacchi tra i canali di utilizzo dei servizi bancari (PC&Mobile);

- Si conferma il trend che vede la **clientela Retail la più colpita**, in 4 casi su 5: il frodatore è consapevole che il cliente è l'anello vulnerabile della catena;

- Si accresce la potenza di fuoco degli **attacchi RDDOS** finalizzati ad interrompere il servizio di singole banche (il 57% degli operatori intervistati è stato interessato).

Key messages

- Ponendosi come «barriere» agli attacchi, la sicurezza dei servizi finanziarie è influenzata anche dalle **vulnerabilità di altri settori come ad esempio il settore TLC** (es. sim swap); è opportuno **rafforzare il coinvolgimento dei diversi stakeholders di mercato**, per innalzare la capacità di costruire soluzioni di sicurezza che diano risposte integrate;

- Il **contesto regolamentare è in continua evoluzione e presenta** sovrapposizioni tra le diverse normative. La nuova direttiva europea DORA, la normativa NIS e sul Perimetro Cibernetico presentano divergenze e ridondanze rispetto alla robusta normativa bancaria già in essere; dobbiamo **stabilizzare i processi operativi a livello italiano**, non limitandosi a costruire processi di governance regolamentati ma **logiche di collaborazione intersettoriale pubblico / privato**;

- È **necessario accrescere l'interazione** di risposta **con le forze dell'ordine**, finalizzata ad evolvere nel continuo le modalità, robuste e coordinate, per incidere «proattivamente» sugli attacchi;

- Il processo di prevenzione e contrasto delle frodi deve partire dal **cliente**, che va reso maggiormente consapevole delle evoluzioni dei pattern di attacco: **l'awareness dell'utente finale deve, quindi, divenire sempre più prioritaria.**