Sicurezza e pagamenti: lo stato dell'arte

Milano, 24 novembre 2017

Giorgio Orlandi

Cyber Security and Fraud Analyst

TLP GREEN

What keeps us up at night?

Un'appropriata **gestione della cybersecurity** è al centro dei piani strategici non solo di singole aziende ma di tutto il Paese per:

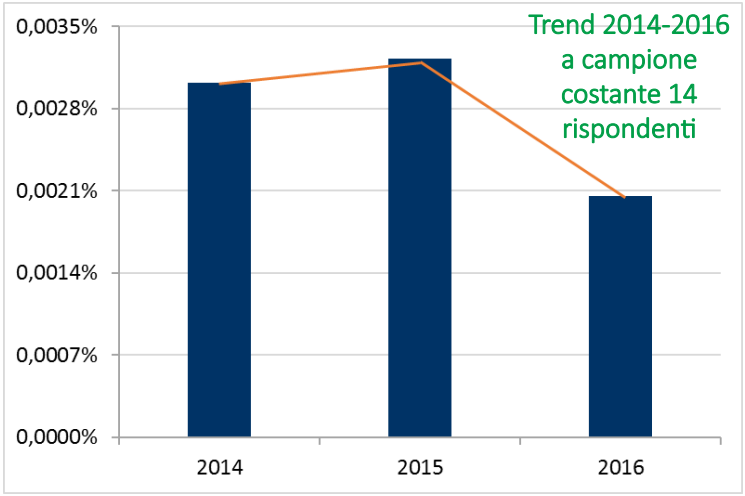
- Far fronte alle **minacce cyber** in **continua evoluzione**
- Garantire un equilibrio tra **innovazione** dei servizi digitali e **sicurezza** di dati, reti e informazioni
- Mantenere elevata la **fiducia** dell'utente nei confronti dei servizi digitali
- Essere **compliant** alle normative nazionali e internazionali

Furto di credenziali e danno economico
Clientela Retail e Corporate

CERTFin
CERT Finanziario Italiano

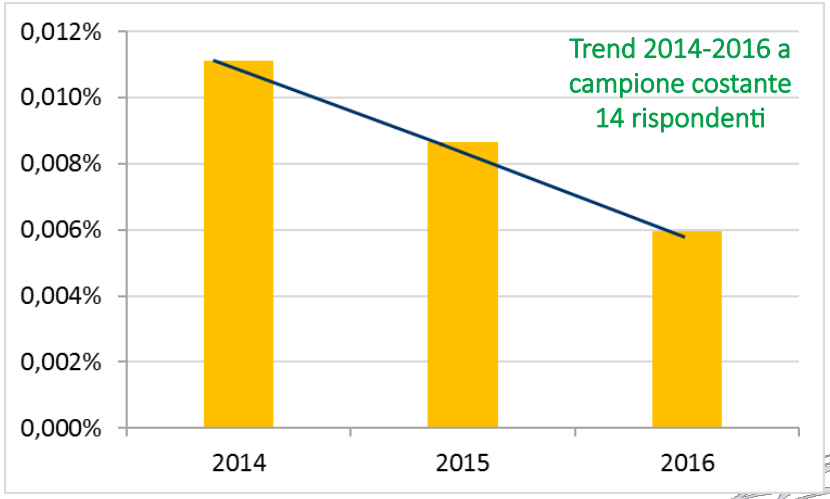
- ✓ Nel 2016, la percentuale di clienti attivi **Retail** che hanno subito un **furto di credenziali** è cresciuta rispetto al 2015, passando dallo 0,108% allo 0,204%. Per il comparto **Corporate**, si registra un trend in diminuzione (dall'1,532% allo 0,67%).
- ✓ Considerando **tutta la clientela***, nel 2016 lo 0,45% degli utenti attivi ha subito un furto di credenziali.

Percentuale di clienti attivi Retail che hanno perso denaro



- Nel 2016 la percentuale di clienti Retail che ha perso denaro è diminuita rispetto all'anno precedente ed è pari allo **0,002%.**

Percentuale di clienti attivi Corporate che hanno perso denaro



- Lo **0,0059%** del segmento Corporate ha perso denaro nel 2016, in diminuzione rispetto al 2015.

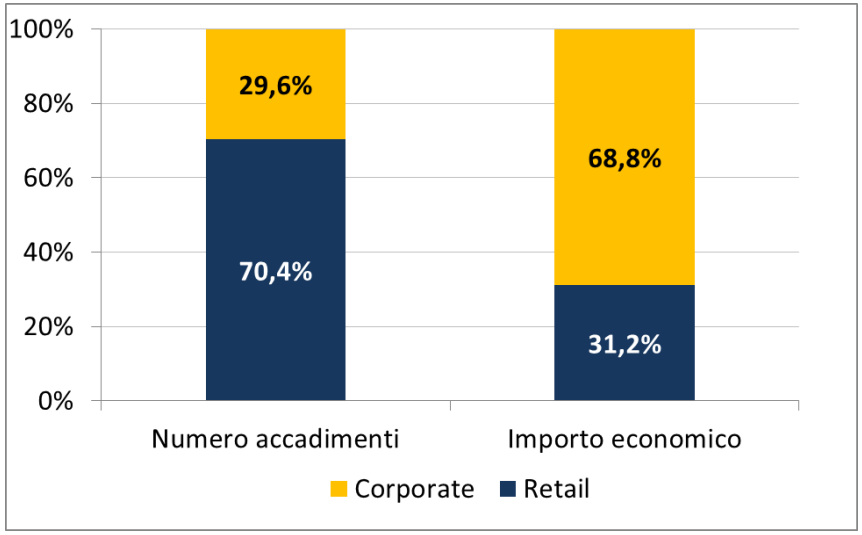
ANALISI SU TUTTA LA CLIENTELA*: nel 2016 lo **0,013%** dei clienti attivi ha subito una **perdita di denaro**

Fonte: CERTFin, Osservatorio Cyber Knowledge and Security Awareness, Survey Frodi Internet e Mobile Banking, 2017 (*Campione: 28 rispondenti)

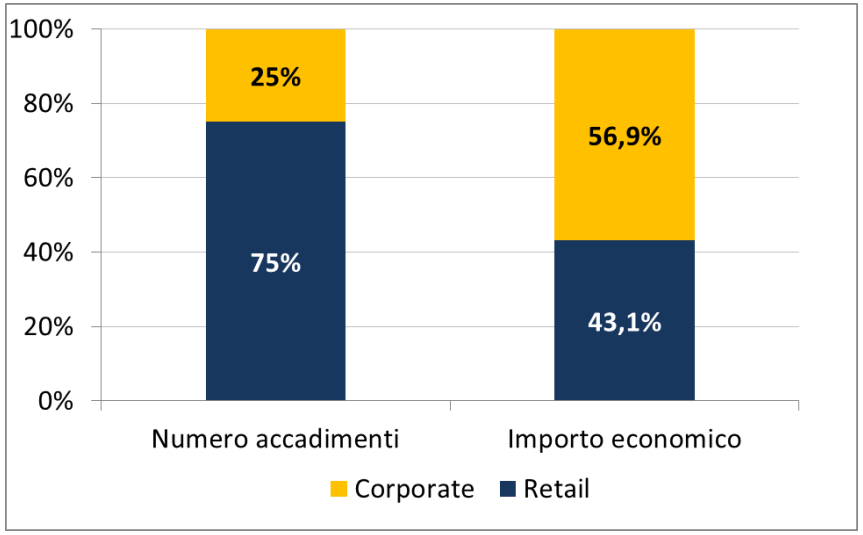
Scenario complessivo transazioni anomale
Confronto Retail e Corporate

CERTFin
CERT Finanziario Italiano

Transazioni anomale (bloccate, recuperate ed effettive) – confronto Retail e Corporate per numero accadimenti e importo economico*



Transazioni fraudolente effettive – confronto Retail e Corporate per numero accadimenti e importo economico*



- Per entrambi i segmenti di clientela, circa il **95% degli importi** associati alle transazioni anomale è stato **bloccato/recuperato**
- Verso il segmento **Retail** si registra la numerosità più elevata di **attacchi**
- Con riferimento, invece, agli **importi** associati alle transazioni fraudolente, è la clientela Corporate cui si associano le **perdite maggiori**, seppur in diminuzione rispetto al 2015

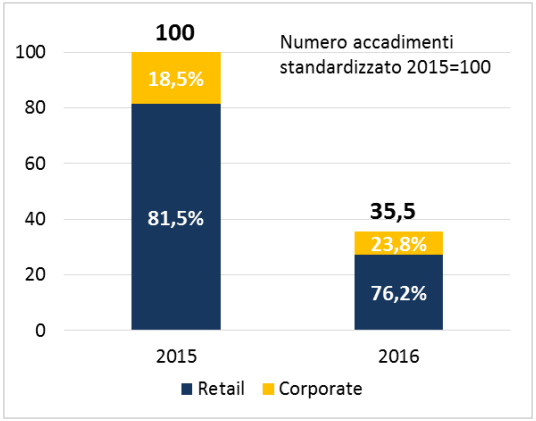
Permane una certa differenziazione nelle modalità e nelle finalità di un attacco rispetto alla clientela

Fonte: CERTFin, Osservatorio Cyber Knowledge and Security Awareness, Survey Frodi Internet e Mobile Banking, 2017 (*Campione: 22 rispondenti)

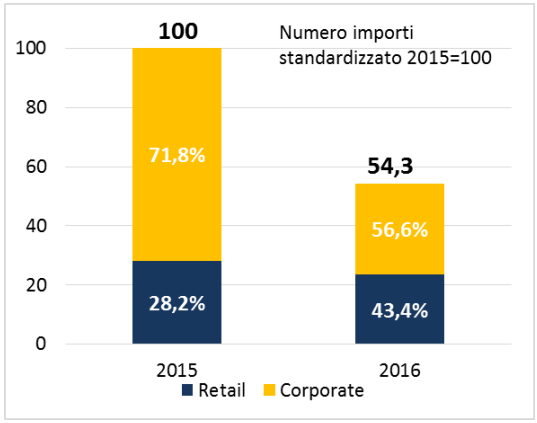
Trend transazioni fraudolente effettive

Rispetto al 2015, nel **2016** si è registrata una **consistente diminuzione** del totale delle **transazioni fraudolente effettive**, in termini sia di **numero di accadimenti (-64,5%)** sia di **importi (-45,7%)**

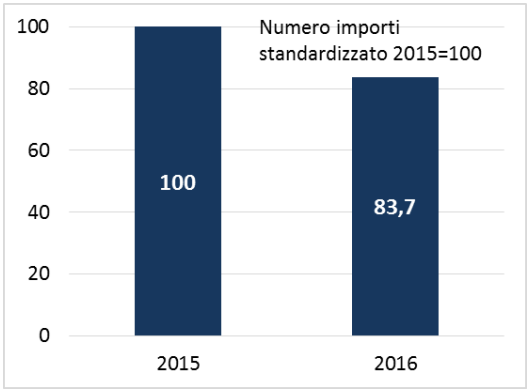
Totale transazioni fraudolente effettive – ripartizione percentuale numero accadimenti tra Retail e Corporate – Trend standardizzato 2015-2016



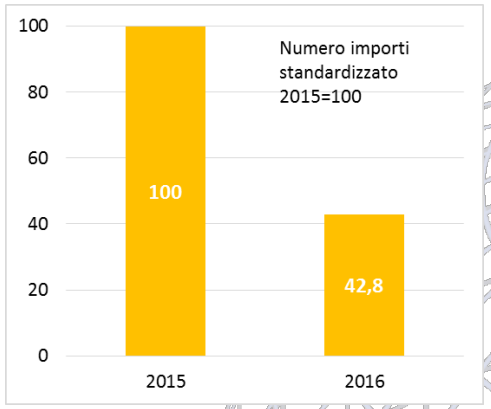
Totale transazioni fraudolente effettive – ripartizione percentuale importo transato tra Retail e Corporate – Trend standardizzato 2015-2016



Valore standardizzato degli importi delle transazioni fraudolente effettive in danno alla clientela Retail - Trend 2015-2016



Valore standardizzato degli importi delle transazioni fraudolente effettive in danno alla clientela Corporate - Trend 2015-2016

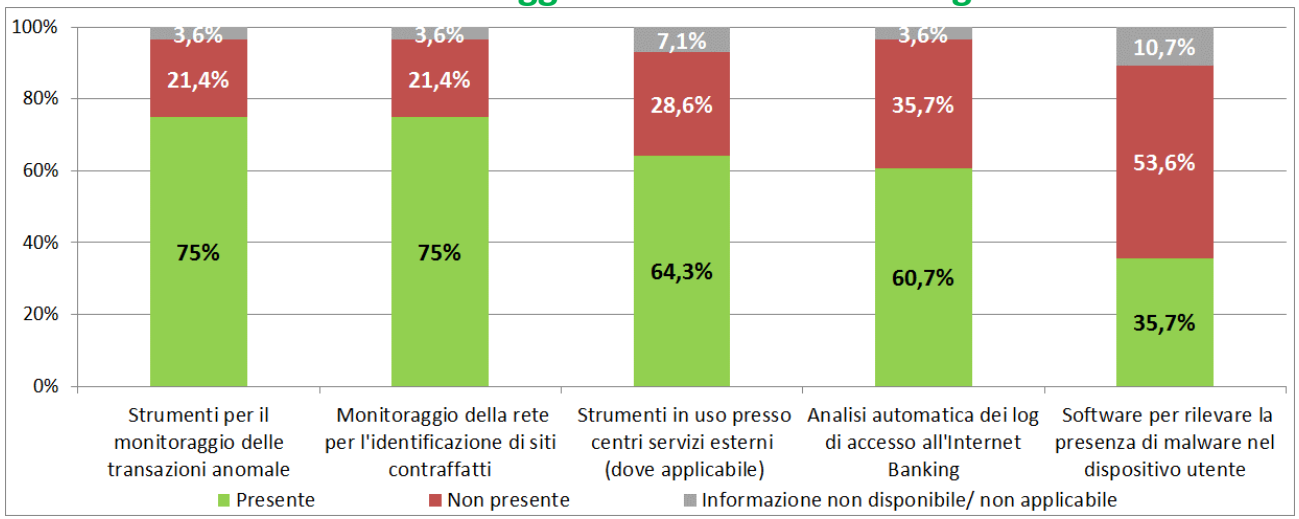


Fonte: CERTFin, Osservatorio Cyber Knowledge and Security Awareness, Survey Frodi Internet e Mobile Banking, 2017
*Ripartizione percentuale sul totale di transazioni fornite da un campione costante di 17 rispondenti)

Le azioni di contrasto interne della banca

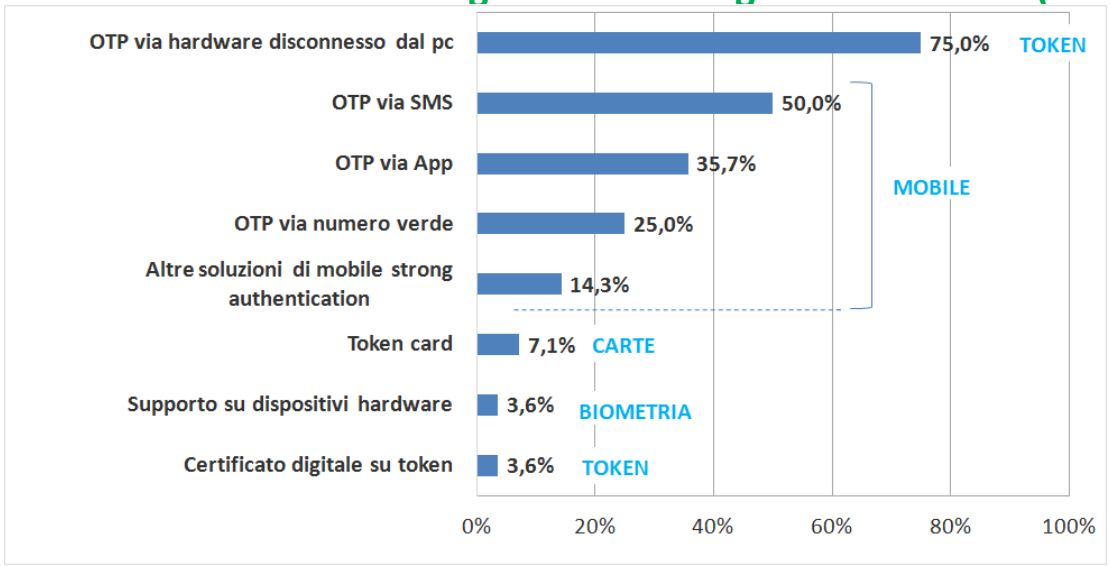
CERTFin
CERT Finanziario Italiano

Attività di monitoraggio e dotazione tecnologica*



- Il **monitoraggio** è uno dei requisiti principali delle regole di attuazione della **PSD2** per gli aspetti di **sicurezza** e per il **regime di esenzione** dell'applicazione della **SCA**

Strumenti di secondo fattore grafico di strong authentication (comparto Retail)*



Dynamic linking:

- Adottato nel 2016 dal **4,2%** delle realtà del segmento Retail e dall'**8,3%** del comparto Corporate**
- Adozione prevista nel 2017 per il **25%** del campione Retail e il **16,7%** del segmento Corporate**

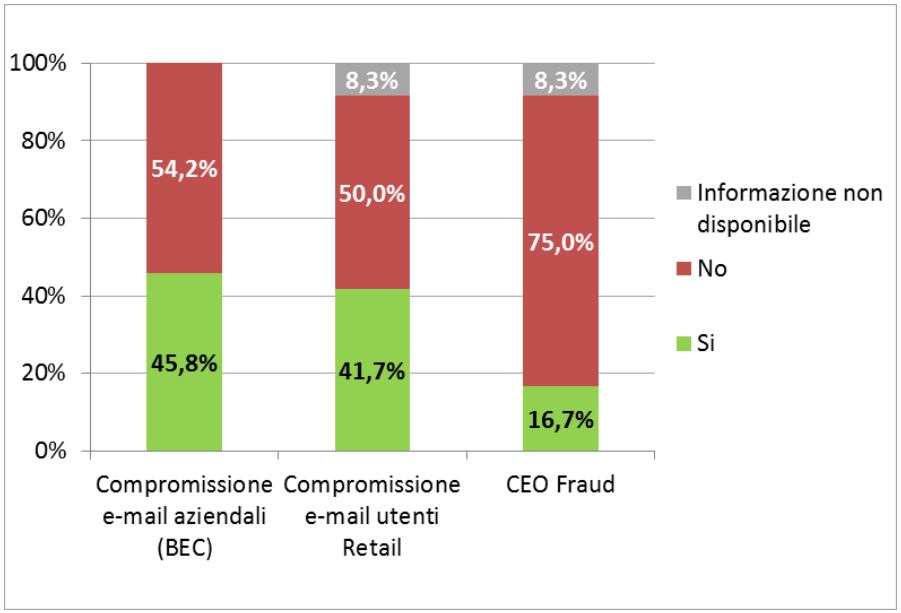
Fonte: CERTFin, Osservatorio Cyber Knowledge and Security Awareness, Survey Frodi Internet e Mobile Banking, 2017 (*Campione: 28 rispondenti; ** Campione Ratail e Corporate: 24 rispondenti)

Modalità di realizzazione dell'attacco
Focus social engineering

CERTFin
CERT Finanziario Italiano

- ✓ L'obiettivo dei frodatori è **carpire dati per disporre transazioni** → si mira a **raggirare l'utente** inducendolo a eseguire operazioni verso i frodatori, senza che questi ultimi violino necessariamente le credenziali di accesso e autorizzative dei servizi di Internet Banking.
- ✓ Non sfruttano vulnerabilità tecnologiche, ma puntano sulle relazioni della «vittima»; per tale motivo, sono **difficili da rilevare tempestivamente**, anche da parte della banca.

Rilevazione di meccanismi di attacco basati su tecniche di social engineering*



- Per la categoria **BEC** si sono registrati **14 frodi effettive** (7 rispondenti) su un totale di **71 tentativi** (8 rispondenti)
- **25 frodi** andate «a buon fine» (su 5 rispondenti) sono stati segnalati in relazione alla **compromissione** di **email di utenti Retail**, su un totale di **81 tentativi** (6 rispondenti)
- La tecnica di **CEO Fraud** ha registrato una percentuale media di efficacia delle **frodi** pari a circa il **30% dei tentativi** (totale 27 tentativi, 3 rispondenti)

È fondamentale la sensibilizzazione dell'utente rispetto ai nuovi schemi di attacco e a un uso attento della posta elettronica

Fonte: CERTFin, Osservatorio Cyber Knowledge and Security Awareness, Survey Frodi Internet e Mobile Banking, 2017 (*Analisi su tutta la clientela: 24 rispondenti)

Modalità di realizzazione dell'attacco
Confronto segmenti di clientela

CERTFin
CERT Finanziario Italiano

Vettori di attacco e modalità di esecuzione della frode

SEGMENTO RETAIL

- Il **90,3%** del totale dei casi di furto di identità rilevati è associato ad attacchi di **phishing***
- **4 realtà** hanno rilevato casi di **vishing**
- **81,1%** delle transazioni eseguite da una **sessione di log-in aperta dal frodatore** a seguito del furto di credenziali***

SEGMENTO CORPORATE

- È il **crimeware** il vettore più utilizzato dai frodatori per realizzare un attacco (**48,9%**), seguito dal pishing (44,2%) e da tecniche miste (6,9%)**
- **Nessun** caso di **vishing**
- Il **61,5%** degli attacchi è eseguito dalla **sessione legittima** dell'utente***

❖ Nel **2016** sono stati **19.526** i siti clone rilevati da 18 banche e tempestivamente **bloccati**

Focus device mobili

Gli attacchi (limitati) che hanno coinvolto device mobili si caratterizzano per **due principali step,** ma presentano **discreta variabilità** in termini di **impatto**:

➢ **Sottrazione dei codici di accesso statici** al portale di Internet Banking attraverso tecniche di **social engineering** (phishing, Smishing, etc.)

➢ **Intercettazione dei codici autorizzativi** delle transazioni disposte via Internet, attraverso **SIM Swap** o, in un numero limitato di casi, **malware**

SEGMENTO RETAIL (14 rispondenti)

- Fenomeni di **SIM swap** e **malware** segnalati, rispettivamente, da 4 e 2 banche

SEGMENTO CORPORATE (13 rispondenti)

- Nel **2016** sono stati registrati per la **prima volta** casi di attacco tramite **device mobili** (3 realtà coinvolte)

Fonte: CERTFin, Osservatorio Cyber Knowledge and Security Awareness, Survey Frodi Internet e Mobile Banking, 2017 (Campione: *17 rispondenti; **16 rispondenti;***Andamento medio su 14 rispondenti)

CERTFin – CERT Finanziario Italiano
Overview

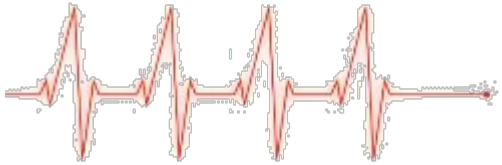
CERTFin
CERT Finanziario Italiano

FILONI OPERATIVI

FINANCIAL INFO SHARING AND ANALYSIS CENTER (FinISAC)

CYBER KNOWLEDGE AND SECURITY AWARENESS

CENTRALE OPERATIVA DI GESTIONE DELLE EMERGENZE CYBER



Parlano di noi:

Banca d'Italia – *"Relazione annuale sul 2016 - Considerazioni finali del Governatore":*
https://www.bancaditalia.it/pubblicazioni/interventi-governatore/integov2017/cf_2016.pdf

DIS - "*Relazione sulla politica dell'informazione per la sicurezza - 2016*":
https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/02/relazione-2016.pdf

ADESIONI

39 soggetti aderenti al CERTFin
9 partecipanti al Team Virtuale

www.certfin.it
info@certfin.it

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

CERTFin
CERT Finanziario Italiano

CERT di settore / Entità europee di cybersecurity

Nordic CERT
NCSC-UK
CERT Israele…

CERT nazionali di altri Paesi

CERT Austria
CERT Lussemburgo
CERT Polonia
CERT Svizzera…

Istituti nazionali e centri di competenza

CERT Nazionale/ CERT-PA
MEF
Università
Cyber Advisor
…

Forze dell'ordine

polizia delle comunicazioni
EUROPEAN CYBERCRIME CENTRE EC3 EUROPOL
C.N.A.I.P.I.C

Telco Provider

CERTFin
CERT Finanziario Italiano

Organizzazioni europee

SWIFT
FINANCIAL SERVICES ISAC
European FI-ISAC

…attraverso ABI Lab

Constituency

COMING SOON!

Banche e operatori finanziari

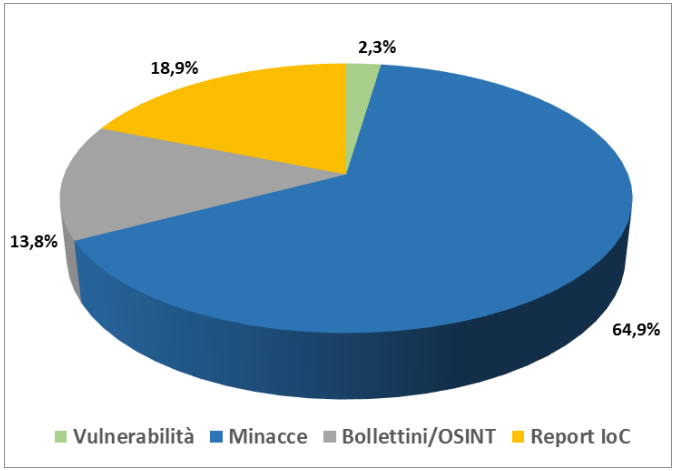
Team virtuale

Assicurazioni e altri operatori

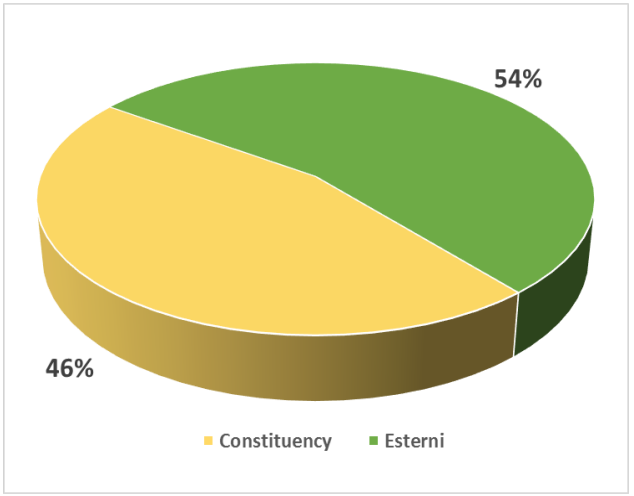
Resoconto attività CERTFin 1 gen – 23 nov 2017
Information Sharing - FinISAC

CERTFin
CERT Finanziario Italiano

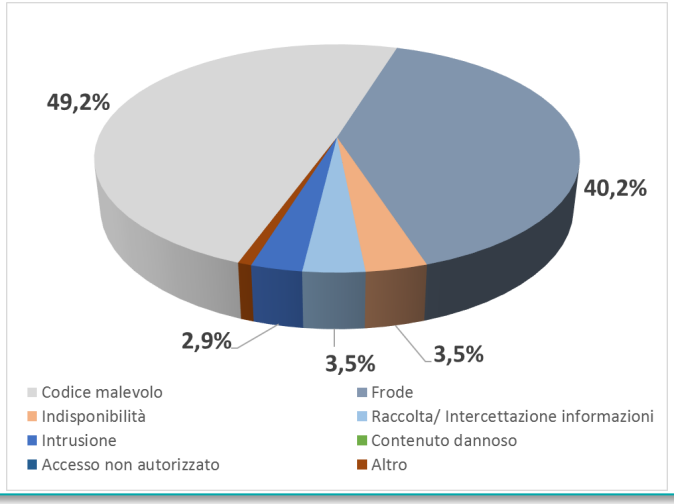
TIPOLOGIE SEGNALAZIONI



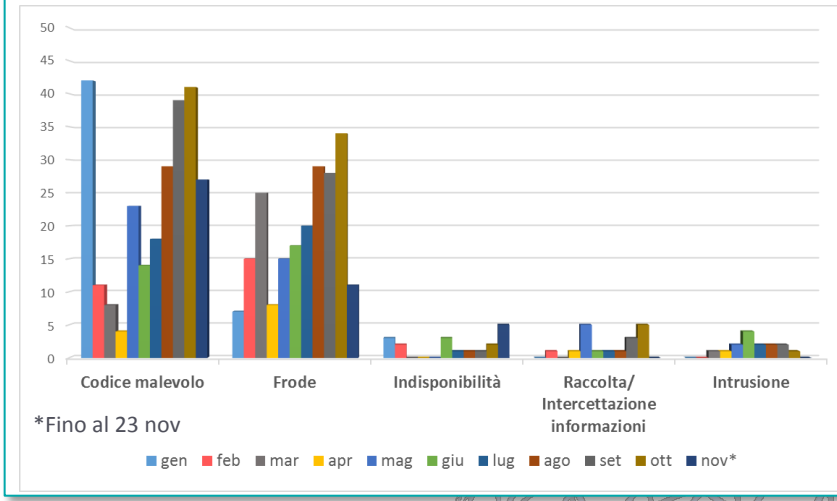
DETTAGLIO FONTI SEGNALAZIONI



DETTAGLIO MINACCE SEGNALATE



DETTAGLIO MINACCE SEGNALATE - TREND



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

Resoconto attività CERTFin 1 gen – 23 nov 2017
Information Sharing - FinISAC

CERTFin
CERT Finanziario Italiano

CLASSI DI MINACCE / EVENTI CYBER ANALIZZATI – gennaio / novembre 2017

Frodi informatiche
- Nuovi fenomeni di SIM swap e di abilitazione fraudolenta device
- Nuove casistiche di avvio trasferimento fondi con malware
- 206 IBAN e 108 IP fraudolenti

Attacchi a dati e informazioni
- Attacchi in Ucraina e Russia
- WIFI Key Reinstallation Attacks (KRACK)
- Compromissione SW Ccleaner
- Ukraine Independence Day threat
- Petya/Not Petya Malware
- Minacce Eye Pyramid/ WannaCry
- Campagne SPAM/CEO Fraud da PEC
- Breach ai danni di un gruppo bancario italiano

Attacchi alla disponibilità di servizi/asset IT
- Tentativi di DDoS
- Attività massiva di port-scan (spesso propedeutica ad attacchi DoS-DDoS)

LESSONS LEARNED

Frodi informatiche
- Vulnerabilità protocollo SS7 - evidenza debolezze del canale SMS
- Esigenza di rafforzare le azioni di contrasto e prevenzione con I Telco provider

Attacchi a dati e informazioni
- Aumento della frequenza del processo di aggiornamento SW
- Rafforzamento training / awareness su tematiche di cybersecurity
- Rafforzamento e aggiornamento delle policy di sicurezza su user / terze parti esterni in grado di accedere (anche tramite extranet) agli applicativi della banca e ai dati dei clienti

Attacchi alla disponibilità di servizi/ asset IT
- Capacità di attacco in aumento e in evoluzione grazie allo sfruttamento di vulnerabilità tecnologiche che compromettono la disponibilità di network e sistemi
- Attivazione di filtri e indirizzamento verso il traffico web in entrata per contrastare attacchi DDoS

GRAZIE PER L'ATTENZIONE