MEF Dipartimento del Tesoro

Newsletter

Frauds: some facts

DIREZIONE V:
Prevenzione dell'Utilizzo del Sistema Finanziario per Fini Illegali

UFFICIO VI

Newsletter n° 20 — Aprile 2019

In questo numero:

CONTRAFFAZIONE DELL'EURO, PUBBLICATO IL RAPPORTO MEF

Buone notizie su sequestri e lotta alla contraffazione monetaria

Buone notizie dalla lotta al falso monetario in base al trend registrato nel 2017 e confermato nel 2018. Progressivo è stato infatti il contenimento del fenomeno della contraffazione di monete e banconote (Figure A e B), come risulta dall'ultimo Rapporto sulla falsificazione dell'euro, curato dall' Ufficio Centrale Antifrode dei Mezzi di Pagamento (UCAMP) del Dipartimento del Tesoro.
Le incidenze dei sospetti di frode sono in calo per valore, sia rispetto alla popolazione italiana (-3%) sia rispetto all'ammontare di banconote totali circolanti in Italia (-7%).

Stato della circolazione	5 Euro	10 Euro	20 Euro	50 Euro	100 Euro	200 Euro	500 Euro	Totale
Prima della circolazione	0	0	592	0	0	0	0	592
Durante la circolazione	1.506	4.464	69.168	71.699	14.046	835	804	162.522
Totale	**1.506**	**4.464**	**69.760**	**71.699**	**14.046**	**835**	**804**	**163.114**

	10 centesimi	20 centesimi	50 centesimi	1 euro	2 euro	Totale
Prima della circolazione	0	0	0	0	27.982	27.982
Durante la circolazione	7	45	13.884	15.564	34.709	64.209
Totale	**7**	**45**	**13.884**	**15.564**	**62.691**	**92.191**

Figure A e B —Banconote e Monete per taglio/conio. Sospetti di falsità sequestrati prima e durante la circolazione - 2017 - valore in €

I dati del rapporto sono stati elaborati grazie al Sistema Monitoraggio Euro Carte (SIMEC), nel quale sono raccolte tutte le segnalazioni di sospetto falso provenienti dalle autorità competenti relativamente a monete e banconote.
Ottime notizie arrivano, però, anche dal capitolo sequestri. E' delle settimane scorse la notizia di un'operazione della Guardia di Finanza, nei pressi di Napoli, dove è stata sgominata una banda di falsari e sequestrato un ammontare complessivo di 36 milioni di euro di banconote false. Le indagini sono state coordinate dalla Procura della Repubblica di Napoli area Nord e l'operazione è stata gestita dalla Guardia di Finanza – Nucleo di Polizia Economico-Finanziaria di Napoli e Nucleo Speciale di

Polizia Valutaria di Roma. I falsari producevano migliaia di banconote da 50 euro al giorno in un immobile nella zona industriale di Pomigliano d'Arco, dove veniva trattata e commercializzata carne di suino. La fattura delle banconote false era pregevole al punto da poter tranquillamente ingannare gli ignari possessori e gran parte dei commercianti. Gli agenti hanno tenuto d'occhio il locale per settimane dopo aver notato l'arrivo di macchinari molto grandi, utilizzati per l'attività criminosa.

Di falsificazione monetaria, operazioni di polizia e attività di prevenzione amministrativa si era parlato anche durante il consueto seminario internazionale che l'Ufficio VI promuove nell'ambito del programma Pericles 2020, tenutosi lo scorso ottobre a Belgrado.

In quella sede, di particolare rilievo, furono la trattazione dei fenomeni del darknet e di quello dei cryptoassets e dello specifico legame tra questi e la contraffazione monetaria, con l'intervento di esperti della Commissione Europea, BCE, Eurojust ed Europol di fronte a una platea costituita dalle delegazioni provenienti da Bulgaria, Moldavia, Montenegro, Romania e Ucraina.

Per consultare la versione integrale del Rapporto sulla falsificazione dell'euro

http://www.dt.tesoro.it/export/sites/sitodt/modules/documenti_it/antifrode_mezzi_pagamento/antifrode_mezzi_pagamento/XXXI_Rapporto_-_1_gennaio_2017_-_31_dicembre_2017.pdf

Per maggiori dettagli sull'evento Pericles a Belgrado

http://www.dt.tesoro.it/it/attivita_istituzionali/antifrode_mezzi_pagamento/formazione_specialistica/seminari_pericles_2018.html

L'AZIONE DEL GIPAF TRA FRODI E CYBERATTACCHI

L'Italia è stato il Paese europeo e il decimo al mondo più colpito dai ransomware

Nel 2018 l'Italia è stato il Paese europeo e il decimo al mondo più colpito dai ransomware, attacchi informatici che bloccano i dispositivi e chiedono un riscatto per liberarli, stando a una ricerca di *Trend Micro Research*. Dei ransomware indirizzati agli Stati europei, il 12,92% ha colpito in Italia. Nella top 10, il nostro Paese è preceduto da Stati Uniti, Brasile, India, Vietnam, Messico, Turchia, Indonesia, Cina e Bangladesh.

Il rapporto "Catturati nella rete: Districare la matassa di minacce vecchie e nuove" parla inoltre di un numero totale di malware intercettati in Italia nel 2018 di 26,3 milioni. Enorme è anche il numero delle minacce arrivate via mail: 611,6 milioni. I malware rivolti verso le banche online sono stati 4.295 e le app maligne scaricate 25.128.

Il rapporto sottolinea come gli attacchi stiano cambiando. Le offensive sono più studiate e prendono di mira meno organizzazioni, ma più grandi e redditizie. Questo si riflette nell'aumento del 28% degli attacchi Bec (Business Email Compromise), che puntano alle reti aziendali.

Di frodi nel mondo dei pagamenti legate a crimini informatici si è parlato anche il 10 dicembre scorso, presso la "Sala Parlamentino" del Ministero dell'Economia e delle Finanze, dove si è tenuto il GIPAF, il Gruppo di Lavoro Interdisciplinare per la Prevenzione Amministrativa delle Frodi sulle Carte di Pagamento presieduto dal MEF. Tra i presenti, rappresentanti della Presidenza del Consiglio, di vari Ministeri, della Banca di Italia e delle forze di polizia, oltre che del mondo accademico e dell'industria finanziaria, che hanno avuto modo di confrontarsi su statistiche, prevenzione amministrativa, attività di repressione e ulteriori possibili soluzioni da porre in essere nella lotta alle frodi derivanti da crimini informatici.

MEF Dipartimento del Tesoro

GIPAF

Gruppo di Lavoro Interdisciplinare per la Prevenzione Amministrativa delle Frodi sulle Carte di Pagamento

Agenda dei Lavori - *Roma, 10 Dicembre 2018*
Ministero dell'Economia e delle Finanze – Via XX Settembre 97
Sala del Parlamentino

09:00	Registrazione dei partecipanti
10:00	*Apertura lavori* Antonio Adinolfi, Dirigente Ufficio VI
10:10	*Intervento introduttivo* Roberto Ciciani, Dirigente Generale
10:20	*Il nuovo framework di sicurezza definito dalla PSD2 per gli operatori del sistema dei pagamenti* Gino Giambelluca (Banca d'Italia)
10:40	*Il trend delle frodi Internet e Mobile banking in Italia* Romano Stasi (CERTFin)
11:00	Break
11:30	*L'evoluzione del rapporto statistico sulle frodi con carte di pagamento: possibili scenari* Stefano Grossi (SOGEI)
11:40	*Il contesto dei cryptoassets e del cash out alla luce della nuova direttiva europea 2018/843* Stefano Capaccioli (Università Statale di Milano)
12:00	*L'evoluzione delle frodi e i nuovi metodi investigativi* Riccardo Croce (Polizia Postale e delle Comunicazioni)
12:20	*Il crimine informatico su scala globale* Pierluigi Paganini (CSE Cybsec Enterprise SpA)
12:40	*Il SIMEC nella lotta alle frodi e al falso monetario: dati e statistiche* Col. Mauro ODORISIO (Guardia di Finanza)
13:00	*Varie ed eventuali*
13:10	*Chiusura dei lavori* Antonio Adinolfi

Ad aprire l'evento il Capo della Direzione V Ciciani che ha sottolineato come "*il*

Gipaf vuole continuare a rappresentare una sede di dibattito sulle più efficaci modalità di lotta alle frodi con mezzi di pagamento diversi dai contanti, perché le frodi rappresentano una minaccia per la sicurezza, spesso fonte di entrate per la criminalità organizzata, e in grado di favorire attività criminali come il terrorismo, il traffico di droga e la tratta di esseri umani".

Nel contesto GIPAF di particolare rilevanza è stato quindi l'intervento di Banca d'Italia sulla PSD2, spiegando "come la nuova Direttiva sui servizi di pagamento si inserisce in uno scenario evolutivo che vede l'affermarsi di nuovi operatori, tecnologie, modelli di business e connessi rischi emergenti, sottolineando la necessità che le autorità finanziarie adottino un approccio molto attento ai profili di sicurezza senza però ostacolare l'innovazione".

In questo contesto, da qualche anno si inserisce la partnership pubblico-privato nella lotta al crimine informatico e alle relative frodi, e che ha dato vita a interessanti esperienze quale quella della OF2CEN, una piattaforma in cui far confluire tutte le segnalazioni provenienti da banche e Forze di polizia su transazioni sospette che avvengono in Rete, in modo da poter analizzare e condividere in tempo reale ogni informazione e bloccare così le operazioni illegali. "Eu-of2cen" (European Union Online Fraud Cyber Centre Expert Network) è un progetto ideato dalla Polizia di Stato, gestito dalla Polizia postale e delle comunicazioni, e finanziato dall'Unione europea per il contrasto al cybercrime finanziario.

Il crimine informatico-finanziario, secondo la Polizia Postale e delle comunicazioni, ha fatto registrare nell'anno appena trascorso aumenti esponenziali, tanto nel numero (+318% rispetto al 2017) quanto nel valore complessivo dei reati (+170%).

Gli attacchi ai sistemi di home banking, più che alla violazione logica delle piattaforme operative, si dirigono verso la sottrazione e l'utilizzo illecito di codici di accesso. L'ambito del Card Not Present (addebito sulla carta di pagamento senza l'esibizione materiale della stessa) conosce infine un aumento sensibile, anche grazie ai furti massivi di codici personali conseguenti ad esfiltrazioni massive di dati, poi rivenduti sulle reti anonimizzate del Darkweb. Il phishing, finalizzato

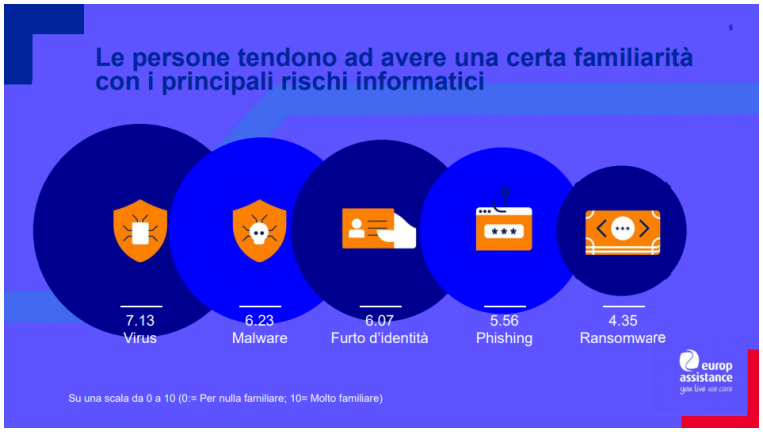
all'inoculazione di malware ed al furto di dati su larga scala, trova nuovi scenari di propagazione, con riferimento alla violazione dei sistemi di e-payment e mobile-payment.

Per maggiori info sul GIPAF:
http://www.dt.tesoro.it/it/attivita_istituzionali/antifrode_mezzi_pagamento/gipaf/

Approfondimenti & Statistiche

2018: anno horribilis tra cyber attacchi e furto di identità

Secondo il *Barometro 'Cyber & Digital Protection' di Europ Assistance,* meno di un italiano su due (48%) protegge il proprio smartphone da possibili virus o malware, eppure gli italiani sono tra i più consapevoli e preoccupati sui rischi dei crimini informatici: furto di identità, protezione di bambini e anziani, cyber bullismo sono riconosciuti come un reale problema. Secondo al ricerca, il 39% degli italiani si dichiara vulnerabile al pericolo di attacco, che arriva principalmente da e-mail, furto della carta di credito e virus contratti durante la navigazione online.



Uno dei temi centrali della ricerca è stato il furto di identità: l'attenzione degli italiani e la relativa preoccupazione di rimanere vittima di un furto d'identità è tra le più alte d'Europa (il 55% si dichiara da "abbastanza" a "molto preoccupato" di questa eventualità), +10 punti percentuali rispetto alla media Europea e seconda nel continente solo alle preoccupazioni degli spagnoli.

Il rapporto rileva infine che il 55% degli italiani, contro una media europea del 47%, è interessato ai nuovi sistemi per la protezione della propria impronta digitale. Un interesse che aumenta con la presenza di bambini e adolescenti in famiglia così come di anziani.

Dunque sia le famiglie sia le aziende non dormono sonni tranquilli.

Sempre in tema di cyber attacchi, è stata infatti Kaspersky Lab a segnalare nel marzo scorso una campagna di cybercrime "chirurgica", l'operazione ShadowHammer, che ha preso di mira gli utenti con Asus Live Update Utility, strumento di aggiornamento fornito dalla casa madre: hanno introdotto una backdoor all'interno, cioè una entrata di servizio, grazie alla quale hanno inserito un codice malevolo. L'operazione è durata "almeno

da giugno a novembre 2018".

E un approfondimento sul tema non può non menzionare gli outcomes del noto Rapporto Clusit. Negli ultimi dodici mesi, rilevano gli esperti del Clusit, la sanità ha subito l'incremento maggiore degli attacchi, pari al 99% rispetto al 2017. Nel 96% dei casi gli attacchi a questo settore hanno avuto finalità cyber criminali e di furto di dati personali.

Segue il settore pubblico, con il 41% degli attacchi in più rispetto ai dodici mesi precedenti e i cosiddetti "multiple targets" - i bersagli multipli - che nel 2018 risultano anche i maggiormente colpiti, con un quinto degli attacchi globali a loro danno, dato in crescita del 37% rispetto al 2017. Queste cifre rilevano che non solo ormai tutti sono diventati bersagli, ma anche che gli attaccanti sono diventati sempre più aggressivi e sono in grado di condurre operazioni su scala sempre maggiore, con una logica "industriale", che prescinde sia da vincoli territoriali che dalla tipologia delle vittime.

Nel 2018 sono stati presi di mira anche i settori della ricerca e formazione, che vede un incremento del 55% degli attacchi rispetto al 2017, dei servizi online e cloud e delle banche, con l'aumento degli attacchi rispettivamente in crescita del 36% e del 33%, sempre rispetto all'anno precedente.

Considerando la gravità dei singoli attacchi nei settori di riferimento, gli esperti Clusit evidenziano che la sanità e le infrastrutture critiche risultano essere i settori per i quali i rischi cyber sono cresciuti maggiormente nel 2018; pur avendo subito in assoluto un numero di attacchi maggiore, il settore pubblico e i "multiple targets" non mostrano invece peggioramenti significativi in termini di gravità.

©Ministero dell' Economia e delle Finanze, 2019
Dipartimento del Tesoro
Direzione V – Ufficio VI

Responsabile: Dott. Antonio Adinolfi
Dirigente Ufficio VI

Redazione: Dott. Augusto Santori
Funzionario Ufficio VI

Via XX Settembre, 97
00187 – Roma
Tel. 06 47610488
Web: http://www.dt.tesoro.it
E-mail: augusto.santori@mef.gov.it

Tutti i diritti riservati. E' consentita la riproduzione ai fini didattici e non commerciali, a condizione che venga citata la fonte.