I criminali informatici stanno vincendo: è ora di passare al contrattacco

Pubblicato il 31 marzo 2025

Mobeen Tahir
Director, Research

Principali insegnamenti

- I criminali informatici stanno utilizzando l'IA e l'ingegneria sociale per lanciare attacchi più sofisticati.
- Un rilevamento rapido è fondamentale: alcune violazioni degenerano in meno di un minuto.
- Attacchi informatici di alto profilo stanno facendo emergere rischi geopolitici, dalle interferenze nelle elezioni alle violazioni a danno dei governi.
- Prodotti correlati WisdomTree Cybersecurity UCITS ETF – USD Acc Scopri di più

Recentemente ho creato un sito web, ma subito dopo averlo lanciato ho notato che non compariva nelle ricerche di Google. Mentre cercavo di capire come risolvere il problema, ho ricevuto un'e-mail con istruzioni dettagliate su cosa fare. Niente sembrava sospetto, nemmeno l'indirizzo del mittente. Ma quando ho usato l'intelligenza artificiale (IA) per verificarne l'autenticità, il messaggio è stato segnalato come sospetto.

Alcuni anni fa, le e-mail di phishing presentavano evidenti campanelli d'allarme: grammatica approssimativa, formattazione strana o link imprecisi. Ora che hanno a disposizione strumenti basati sull'IA, i criminali informatici sono molto più sofisticati. E se loro stanno diventando più intelligenti, la sicurezza informatica deve farsi ancora più furba.

Il costo insostenibile di una violazione dei dati

Nel 2024, il costo medio di una violazione dei dati è salito a quasi 5 milioni di dollari1. E questa è solo la media: molte violazioni hanno causato perdite molto maggiori. Nonostante siano anni che il numero cresce, nel 2024 si è registrato un brusco aumento, a dimostrazione di come l'adozione diffusa di strumenti avanzati di IA stia rendendo i criminali informatici più intelligenti e gli attacchi più costosi che mai.

"La velocità degli attacchi potrebbe aumentare fino a 100 volte grazie all'IA generativa" – Palo Alto Networks

In molti casi, il costo reale di una violazione dei dati va oltre i soldi: è incommensurabile. Cosa succede quando la fiducia dei clienti nella sicurezza di un'azienda va in frantumi? Il danno alla reputazione potrebbe essere irreversibile. E se la vittima è un ospedale e qualcuno perde la vita? La posta in gioco non potrebbe essere più elevata. Ecco perché la sicurezza informatica non è solo una priorità, ma una necessità. E il mondo se ne sta finalmente rendendo conto.

I criminali informatici stanno diventando sempre più intelligenti

Aumento del phishing vocale (vishing) nel secondo semestre rispetto al primo semestre del 2024

Attacchi privi di malware nel 2024 (in aumento rispetto al 40% del 2019)

51 seconds

Tempo di penetrazione più breve mai registrato nell'ambito di un attacco informatico

avversari rilevati, di cui 26 nuovi nel 2024

Fonte: "2025 Global Threat Report", CrowdStrike, marzo 2025.

Quando i criminali informatici colpiscono un obiettivo, la loro intenzione è quella di infiltrarsi nell'organizzazione attraverso un anello debole e penetrare sempre più in profondità nella rete. Il tempo di penetrazione di un attacco informatico si riferisce alla rapidità con cui si intensifica il controllo, passando dalla violazione iniziale ai sistemi critici, rubando dati, neutralizzando la sicurezza o distribuendo ransomware. Alcuni aggressori ci riescono in meno di un'ora, rendendo la rapidità di rilevamento e risposta cruciale. Nel 2024, il record di velocità registrato è stato di 51 secondi2.

Non sempre gli aggressori si affidano alle e-mail: spesso le telefonate moleste che riceviamo possono essere piuttosto nefaste. Gli attacchi di vishing (phishing vocale) sono perpetrati da criminali informatici che utilizzano telefonate per impersonare entità fidate, come banche, agenzie governative o fornitori di servizi, allo scopo di indurre le vittime a rivelare informazioni sensibili o a trasferire denaro. Queste truffe sono aumentate notevolmente, con il vishing che ha visto un incremento del 442% nel secondo semestre del 2024 rispetto al primo3, evidenziando come i criminali sfruttino la fiducia umana al telefono per aggirare le tradizionali difese della sicurezza informatica.

Qualche settimana fa ho visto un post su LinkedIn che ritraeva un uomo circondato da agenti di polizia. Stava raccontando di come si era introdotto fisicamente in un'organizzazione, superando i controlli di sicurezza, accedendo ad aree riservate e sfidando la sorte fino a quando non era stato scoperto. Ma non si trattava di un vero e proprio attacco, bensì di un penetration test, un esercizio di sicurezza controllato progettato per identificare le vulnerabilità prima che i criminali reali le sfruttino. Le organizzazioni conducono questi test perché gli hacker impiegano tecniche di ingegneria sociale sempre più sofisticate, manipolando le persone piuttosto che i sistemi, per aggirare la sicurezza e ottenere l'accesso. La minaccia è in crescita, dato che nel 2024 il 79% degli attacchi non utilizzava malware, rispetto al 40% del 20194; questo dimostra che, quando riescono a indurre gli esseri umani ad aprire la porta, i criminali informatici non hanno necessariamente bisogno di malware.

Gli attacchi di alto profilo sottolineano i rischi geopolitici

All'inizio del 2024, c'era molta preoccupazione per i rischi informatici nell'anno delle elezioni. Mentre molti paesi hanno superato il ciclo elettorale senza gravi incidenti noti, le elezioni presidenziali rumene di dicembre sono state annullate a causa di presunte interferenze russe. L'inaspettato vantaggio del

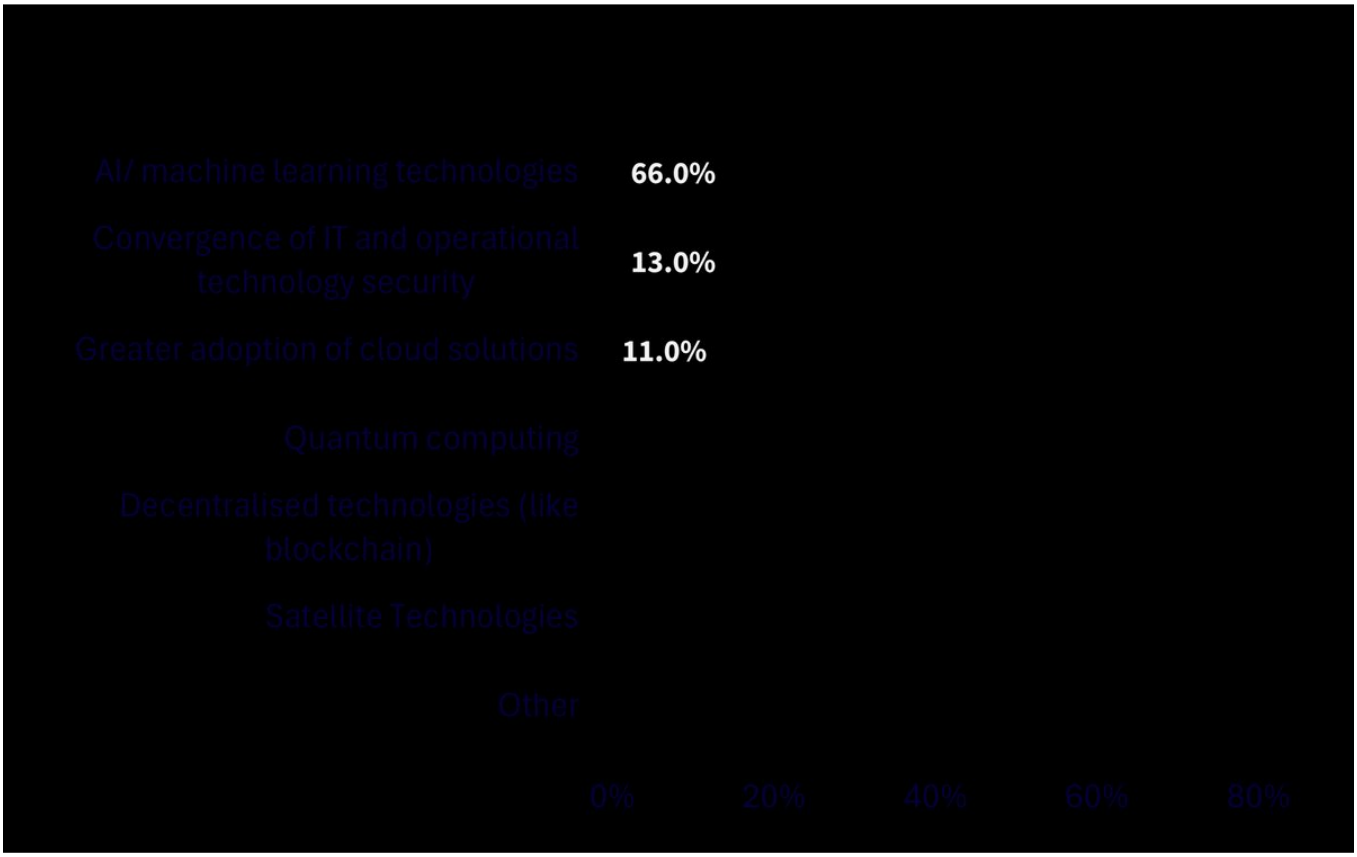
candidato di estrema destra Calin Georgescu al primo turno ha fatto scattare indagini che hanno rivelato una campagna online coordinata e attacchi informatici a sostegno della sua candidatura, portando i tribunali a invalidare le elezioni.

Nello stesso mese, il Dipartimento del Tesoro degli Stati Uniti ha riferito una violazione significativa della sicurezza informatica attribuita a hacker cinesi supportati dallo stato. Gli aggressori hanno sfruttato un fornitore di software terzo per accedere alle postazioni di lavoro del Dipartimento del Tesoro e a documenti non classificati. La violazione ha visto il furto di una chiave di sicurezza, che ha consentito l'accesso remoto ai sistemi. Sebbene il ministero degli esteri cinese abbia respinto le accuse, l'incidente sottolinea la crescente intersezione tra rischi geopolitici e minacce alla sicurezza informatica.

I dirigenti sono preoccupati per i rischi posti dall'IA

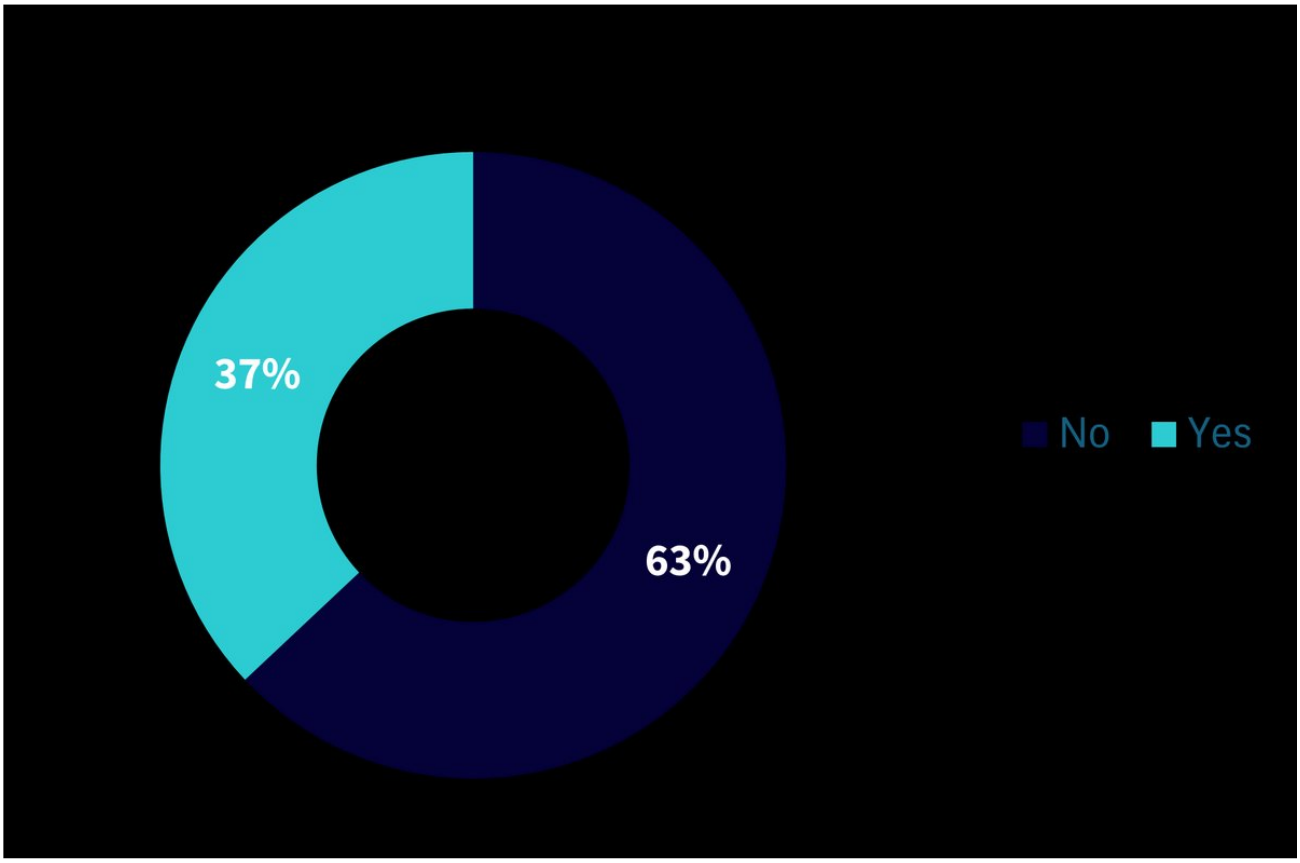
Un recente sondaggio tra i dirigenti condotto dal Forum economico mondiale5 ha rivelato che, secondo il 66%, ad avere l'impatto maggiore sulla sicurezza informatica nei prossimi 12 mesi saranno l'IA e l'apprendimento automatico. Eppure, il 63% ha ammesso che la propria organizzazione non dispone di processi per valutare la sicurezza degli strumenti di IA prima di distribuirli, evidenziando una lacuna critica tra innovazione e gestione del rischio.

Figura 1: Secondo lei, quale dei seguenti fattori avrà l’impatto più significativo sulla sicurezza informatica nei prossimi 12 mesi?



Fonte: Forum economico mondiale, “Global Cybersecurity Report 2025”.

Figura 2: La sua organizzazione ha in atto processi per valutare la sicurezza degli strumenti di IA prima di distribuirli?



Fonte: Forum economico mondiale, “Global Cybersecurity Report 2025”.

Un modo intelligente per sfruttare un tema in rapida crescita

Il WisdomTree Cybersecurity UCITS ETF (WCBR) è stato creato in collaborazione con gli esperti del settore di Team8. L'ETF (exchange-traded fund) identifica otto principali aree di interesse. Queste includono la sicurezza dei dati (poiché la nostra crescente impronta digitale deve essere protetta); la sicurezza dei dispositivi connessi (un aspetto fondamentale, con l’esplosione del numero di gadget dell'Internet of things - IoT); e quello che chiamiamo il “mondo senza confini” (dato che le organizzazioni non operano più entro i confini fisici).

L'ETF offre un portafoglio di aziende pure-play specializzate nella sicurezza informatica, con particolare attenzione a quelle i cui ricavi sono in rapido aumento e che abbracciano diversi temi legati alla stessa. Per gli investitori alla ricerca di un'esposizione intelligente a quest’area vitale, l'ETF può contribuire ad aggiungere potenziale di crescita al portafoglio.

La sicurezza informatica deve sempre essere un passo avanti

La sicurezza informatica deve rinnovarsi costantemente, sfruttando tecnologie all'avanguardia per essere sempre un passo avanti rispetto alle minacce in evoluzione. La corsa incessante tra difensori e aggressori è ciò che rende questo campo così entusiasmante e dinamico. I recenti titoli di giornale sull'informatica quantistica suggeriscono che l'era quantistica potrebbe essere più vicina di quanto si pensasse, lasciando presagire un futuro in cui un computer potrebbe riuscire a infrangere senza sforzo anche le più sofisticate tecniche di crittografia. Questo ridefinirebbe la sicurezza informatica che conosciamo. Che si tratti di informatica quantistica, IA o blockchain, ogni innovazione introduce nuove vulnerabilità e la relativa salvaguardia deve essere un'attività proattiva, non reattiva. Perché se aspettiamo che l'attacco avvenga, potrebbe essere ormai troppo tardi.

1 IBM, 2025.
2 Fonte: “2025 Global Threat Report”, CrowdStrike, marzo 2025.
3 Fonte: “2025 Global Threat Report”, CrowdStrike, marzo 2025.
4 Fonte: “2025 Global Threat Report”, CrowdStrike, marzo 2025.
5 Fonte: Forum economico mondiale, “Global Cybersecurity Report 2025”.

Important Risks Related to this Article

INFORMAZIONI IMPORTANTI

Comunicazioni di marketing emesse all¼interno dello Spazio economico europeo ("SEE")¦ Il presente documento è stato emesso e approvato da WisdomTree Ireland Limited, società autorizzata e regolamentata dalla Central Bank of Ireland.

Comunicazioni di marketing emesse in giurisdizioni non appartenenti al SEE: Il presente documento è stato emesso e approvato da WisdomTree UK Limited, società autorizzata e regolamentata dalla Financial Conduct Authority del Regno Unito.

Per fare riferimento a WisdomTree Ireland Limited e a WisdomTree UK Limited si utilizza per entrambe la denominazione "WisdomTree" (come applicabile). La nostra politica sui conflitti d¼interesse e il nostro inventario sono disponibili su richiesta.

Questa comunicazione di marketing è stata predisposta per investitori professionali; tuttavia, in alcune giurisdizioni i prodotti WisdomTree descritti in questo documento potrebbero essere disponibili per qualsiasi investitore, nel rispetto delle leggi e dei regolamenti applicabili. Poiché il prodotto potrebbe non essere autorizzato o la sua oerta potrebbe essere limitata in alcune giurisdizioni, spetta a ciascuna persona o entità accertarsi di agire in piena osservanza delle leggi e delle normative vigenti nella giurisdizione pertinente. Prima di eettuare una richiesta di sottoscrizione si consiglia agli investitori di ottenere tutta la consulenza legale, fiscale e di investimento necessaria in merito alle conseguenze di un investimento nei prodotti. I rendimenti ottenuti nel passato non sono un¼indicazione aidabile dei rendimenti futuri. I rendimenti storici ricompresi nel presente documento potrebbero essere basati sul back test, ossia la procedura di valutazione di una strategia d¼investimento, che viene applicata ai dati storici per simulare quali sarebbero stati i rendimenti di tale strategia. I rendimenti basati su back test sono puramente ipotetici e vengono forniti nel presente documento a soli fini informativi. I dati basati sul back test non rappresentano rendimenti eettivi e non devono intendersi come un¼indicazione di rendimenti eettivi o futuri. Il valore di un investimento potrebbe essere oggetto di oscillazioni dei tassi di cambio. Qualsiasi decisione d¼investimento deve essere basata sulle informazioni contenute nel Prospetto informativo di riferimento e deve essere presa dopo aver richiesto il parere di un consulente d¼investimento, fiscale e legale indipendente. I suddetti prodotti potrebbero non essere disponibili nel Suo mercato o adatti alle Sue esigenze. Il contenuto del presente documento non costituisce una consulenza in materia di investimenti, né un¼oerta di vendita o una sollecitazione di un¼oerta di acquisto di un prodotto o di sottoscrizione di un investimento.

Un investimento in exchange-traded product ("ETP") dipende dalla performance dell¼indice sottostante, sottratti i costi, ma diicilmente replicherà la performance dell¼indice con assoluta precisione. I prodotti ETP comportano numerosi rischi inclusi, tra gli altri, rischi generali di mercato correlati all¼indice sottostante di riferimento, rischi di credito riferiti al provider degli swap sull¼indice utilizzati nell¼ETP, rischi di cambio, rischi da tasso d¼interesse, rischi d¼inflazione, rischi di liquidità, rischi legali e normativi.

Le informazioni contenute nel presente documento non sono, e in nessun caso devono essere interpretate come, un annuncio pubblicitario o un altro strumento di promozione di un¼oerta pubblica di azioni negli Stati Uniti o in qualsiasi provincia o territorio degli stessi, laddove nessuno degli emittenti o dei relativi prodotti sia autorizzato o registrato per la distribuzione e laddove nessun prospetto di uno qualsiasi degli emittenti sia stato depositato presso una commissione di vigilanza o autorità di regolamentazione. Nessun documento, o informazione contenuta nel presente documento, deve essere estrapolato, trasmesso o distribuito (direttamente o indirettamente) negli Stati Uniti. Nessuno degli Emittenti né alcun titolo da essi emesso sono stati o saranno registrati ai sensi dello United States Securities Act del 1933 o dell¼Investment Company Act del 1940 o qualificati ai sensi di qualsiasi legge statale sui titoli applicabile.

Il presente documento può contenere commenti indipendenti sul mercato redatti da WisdomTree sulla base delle informazioni disponibili al pubblico. Benché WisdomTree si adoperi per garantire l¼esattezza del contenuto del presente documento, WisdomTree non garantisce né assicura la sua esattezza o correttezza. Qualsiasi terzo fornitore di dati di cui ci si avvalga per reperire le informazioni contenute nel presente documento non rilascia alcuna garanzia o dichiarazione di sorta in relazione ai suddetti dati. Laddove WisdomTree abbia espresso dei pareri relativamente al prodotto o all¼attività di mercato, si ricorda che tali pareri possono cambiare. Né WisdomTree, né alcuna consociata, né alcuno dei rispettivi funzionari, amministratori, partner o dipendenti, accetta alcuna responsabilità per qualsiasi perdita, diretta o indiretta, derivante

dall¼utilizzo del presente documento o del suo contenuto.

Il presente documento può contenere dichiarazioni previsionali, comprese dichiarazioni riguardanti le nostre convinzioni o le nostre attuali aspettative in relazione alla performance di determinate classi di attività e/o settori. Le dichiarazioni previsionali sono soggette a determinati rischi, incertezze e ipotesi. Non vi è alcuna garanzia che tali dichiarazioni siano esatte, e i risultati eettivi possano discostarsi significativamente da quelli previsti in dette dichiarazioni. WisdomTree raccomanda vivamente di non fare indebito aidamento sulle summenzionate dichiarazioni previsionali.

WisdomTree Issuer ICAV

I prodotti trattati nel presente documento sono emessi da WisdomTree Issuer ICAV ("WT Issuer"). WT Issuer è una società d'investimento multicomparto a capitale variabile con separazione patrimoniale tra i comparti, costituita ai sensi del diritto irlandese in forma di Veicolo di gestione patrimoniale collettivo irlandese e autorizzata dalla Central Bank of Ireland ("CBI"). WT Issuer è costituita in forma di Organismo di Investimento Collettivo in Valori Mobiliari ("OICVM") di diritto irlandese ed emette una classe di azioni separata ("Azioni") rappresentativa di ogni fondo.

Il Fondo è descritto in un Documento contenente le informazioni chiave (KID) o Documento contenente le informazioni chiave per gli investitori (KIID) destinato agli investitori del Regno Unito, nonché nel prospetto di WT Issuer ("Prospetto WT"). Una copia del Prospetto WT e del KID/KIID in lingua inglese è disponibile, esclusivamente per il SEE/Regno Unito, su www.wisdomtree.eu. Laddove previsto dalla normativa nazionale, il KID sarà disponibile anche nella lingua locale dello Stato membro del SEE

interessato. Per maggiori dettagli sui rischi associati a un investimento nelle Azioni, si invitano gli investitori a leggere il Prospetto WT prima di eettuare l'investimento e a consultare la sezione del Prospetto WT intitolata "Risk Factors".

La descrizione sintetica dei diritti degli investitori associati a un investimento nel fondo è disponibile in lingua inglese sul sito web di WisdomTree Europe. WisdomTree Management Limited può decidere di risolvere gli accordi relativi alla commercializzazione dei suoi organismi di investimento collettivo. In simili circostanze, gli azionisti situati nello Stato membro del SEE interessato riceveranno la comunicazione di tale decisione e avranno la possibilità di chiedere il rimborso della propria partecipazione nel fondo a titolo gratuito o senza alcuna detrazione per almeno 30 giorni lavorativi dalla data della suddetta notifica.

Per gli Investitori in Svizzera – Invesitori Qualificati

Questo documento costituisce una pubblicità dei prodotti finanziari qui menzionati.

Il prospetto e i documenti di informazioni chiave per gli investitori (KIID) sono disponibili sul sito Web di WisdomTree: https://www.wisdomtree.eu/it-ch/resource-library/prospectus-and-regulatory-reports

Alcuni comparti di cui al presente documento potrebbero non essere stati registrati presso l¼Autorità federale di vigilanza sui mercati finanziari (“FINMA”). In Svizzera, i comparti che non sono stati registrati presso la FINMA saranno distribuiti esclusivamente a investitori qualificati, definiti nella legge svizzera sugli investimenti collettivi di capitale (LICo) ovvero nella sua ordinanza di attuazione (e singolarmente modificate di volta in volta). Il rappresentante e agente per i pagamenti dei comparti in Svizzera è Société Générale Paris, Filiale di Zurigo, Talacker 50, PO Box 5070, 8021 Zurigo, Svizzera. Il prospetto, il documento contenente le informazioni chiave per gli investitori (KIID), lo statuto e le relazioni annuali e semestrali dei comparti sono disponibili gratuitamente presso il rappresentante e agente per i pagamenti svizzero. Con riferimento alla distribuzione in Svizzera, il luogo di giurisdizione e prestazione del servizio è la sede del rappresentante e agente per i pagamenti.

Per investitori francesi: le informazioni riportate nel presente documento sono destinate esclusivamente agli investitori professionali (secondo quanto definito dalla MiFID) che investono per proprio conto e ne è vietata la distribuzione al pubblico. La distribuzione del Prospetto e l'oerta, la vendita e la consegna di Azioni in altre giurisdizioni possono essere soggette a restrizioni di legge. L'Emittente è un OICVM di diritto irlandese, approvato dall¼Autorità di Vigilanza Finanziaria come OICVM conforme alle normative europee, sebbene potrebbe non essere tenuto ad adempiere alle stesse disposizioni vigenti per un prodotto simile approvato in Francia. Il Fondo è stato registrato per la commercializzazione in Francia dall¼Autorità dei Mercati

Finanziari (Autorité des Marchés Financiers) e può essere distribuito agli investitori in Francia. Le copie di tutti i documenti (ovvero il Prospetto, il Documento contenente le informazioni chiave per gli investitori, eventuali supplementi o appendici, le ultime relazioni annuali, l'Atto costitutivo e lo Statuto) sono disponibili, gratuitamente, presso l'agente centralizzatore francese, Societe Generale con sede in 29, boulevard Haussmann – 75009 Parigi, Francia. La sottoscrizione delle Azioni del Fondo sarà eettuata conformemente alle condizioni indicate nel Prospetto e in eventuali integrazioni o appendici.

Per Investitori Maltese: Questo documento non costituisce o forma parte di qualsiasi oerta od invito alla pubblica sottoscrizione o acquisto di quote nel Fondo, non potrà essere interpretato come tale e nessuna persona al di fuori di quella al quale questo documento stato indirizzato od inviato sarà considerata come potenziale sottoscrittore di quote nel Fondo. Le quote del fondo non verranno commercializzate in alcun modo al pubblico a Malta senza la precedente autorizzazione dell¼Autorità Finanziaria Maltese.