SICUREZZA AZIENDALE ADATTABILE

L'odierno panorama delle minacce sarebbe stato inimmaginabile una decina di anni fa. I cybercriminali hanno adattato le proprie tecniche per aggirare le difese tradizionali e non vengono rilevati dai sistemi per mesi o anche anni. È tempo per le protezioni aziendali di adattarsi con un approccio intelligete e multilivello alla sicurezza IT.

"L'intelligenza è la capacità di adattarsi al cambiamento."
– Stephen Hawking.

SICUREZZA AZIENDALE ADATTABILE

APT (Advanced Persistent Threats), malware sofisticati e attacchi mirati sono solo alcune delle nuove minacce in continua evoluzione che rappresentano un rischio per l'azienda. I cybercriminali sono estremamente consapevoli dei limiti delle protezioni tradizionali basate sul perimetro: è la prima porta a cui suonano quando cercano una fessura nella corazza aziendale.

Le diverse tecnologie aziendali forniscono una comoda rete di supporto ai vettori di attacco: i dispositivi mobili, le applicazioni web, gli archivi portatili, le tecnologie di virtualizzazione basate sul cloud, tutti rappresentano un'opportunità per i cybercriminali a cui la tradizionale sicurezza "previeni e blocca" non è in grado di rispondere.

Per fronteggiarle è necessario un nuovo approccio più integrato e adattabile costruito sui pilastri di previsione, prevenzione, rilevamento e risposta.

I QUATTRO PILASTRI DELLA SICUREZZA AZIENDALE ADATTABILE

Previsione: nessuno ha la sfera di cristallo, ma le imprese con accesso alle più recenti informazioni sulle minacce e sulle tendenze sono meglio in grado di anticipare ed evitare gli incidenti. La formazione dei dipendenti sul riconoscimento delle tattiche usate per gli attacchi aumenta le capacità di analisi predittiva, così come la capacità di imparare dagli errori commessi grazie all'analisi scientifica delle violazioni; il penetration test, allo stesso tempo, può aiutare a esporre i punti deboli.

Prevenzione: un obiettivo chiave qui è quello di ridurre la superficie di attacco, sia che si tratti di vulnerabilità tradizionali, di anti-malware basato su firma, di controlli dei dispositivi o di applicazione delle patch, l'irrigidimento dei sistemi e l'aggiunta di molti ostacoli sulla strada dei criminali rappresentano solo due componenti di un approccio complessivo che include la limitazione della capacità di diffusione degli attacchi e la riduzione dei danni che questi sono in grado di provocare.

Rilevamento: una ricerca di Kaspersky Lab sulle ATP di alto profilo mostra che gli attacchi sofisticati possono passare inosservati per anni. Si stima che in media l'attacco a un'impresa passa inosservato per oltre 200 giorni[1]; prima si scopre un incidente, meglio è. Le tecnologie di rilevazione supportate dalla migliore analisi delle minacce incrementano la scoperta: dal momento che le minacce si evolvono velocemente, la migliore strategia di rilevamento è spesso costituita dalla capacità di individuare comportamenti e sequenze di eventi che suggeriscono l'esistenza di una violazione.

Risposta: una protezione aziendale efficace ha la capacità di rispondere e di attenuare gli effetti di una violazione. Su un livello, può interessare la regola del "se/allora" per le procedure che possono essere automatizzate, come le patch. Su un altro livello, potrebbe includere l'analisi post-violazione o l'uso di team specializzati nella risposta agli incidenti per arrestare, mitigare e analizzare attacchi, violazioni e altri incidenti di sicurezza.

Per essere veramente efficace, tutte queste funzionalità devono lavorare insieme come un sistema multilivello. Supportato dall'Intelligence, incentrato sulla minaccia, integrato, olistico e supportato dalla strategia: queste sono le caratteristiche chiave di un'architettura per la sicurezza aziendale adattabile e completa. Kaspersky Lab si trova in una posizione privilegiata per offrire una piattaforma di sicurezza aziendale adattabile. Diamo allora uno sguardo ad alcuni degli elementi.

[1] https://www.siliconrepublic.com/enterprise/2014/04/11/advanced-cyberattacks-can-go-undetected-for-typically-229-days

SICUREZZA AZIENDALE. POWERED BY INTELLIGENCE.

Kaspersky Lab ha una lunga esperienza nella realizzazione di alcune scoperte di minacce di altissimo profilo ed estremamente rilevanti, compresi:

- Carbanak: il "cyberfurto del secolo" ai danni delle banche
- Dark Hotel: che mira ai viaggiatori aziendali di livello senior
- Mask/Careto: che mira, tra gli altri, a imprese, governi e società di private equity
- Wild Neutron: che mira alle imprese globali e ad altre aziende
- Icefog: attaccato alla catena di approvvigionamento delle aziende
- Red October: sfrutta i sistemi aziendali per condurre operazioni di sorveglianza di massa

Più di un terzo dei nostri dipendenti lavora nel settore della ricerca e dello sviluppo, concentrandosi esclusivamente sullo sviluppo delle tecnologie per contrastare e anticipare le minacce in costante evoluzione che i nostri team dedicati di intelligence e ricerca studiano ogni giorno.

Kaspersky Lab, tramite lo studio del funzionamento interno di alcune delle minacce mondiali più sofisticate, ci ha consentito di sviluppare un portfolio di tecnologie e servizi strategici multilivello per la sicurezza in grado di offrire un approccio alla sicurezza completamente integrato e adattabile. Grazie alla nostra competenza, Kaspersky Lab ha raggiunto i primi posti nelle classifiche dei test indipendenti sul rilevamento e sulla mitigazione delle minacce un numero di volte maggiore rispetto ad altre aziende del settore della sicurezza IT.

PREVISIONE

Le capacità di previsione e le strategie di migrazione create intorno ad esse sono al centro di ogni azione di Kaspersky Lab, dal nostro team dedicato GReAT (Global Research and Analysis Team) a KSN (Kaspersky Security Network), fino al nostro portfolio SIS (Security Intelligence Services):

Kaspersky Security Network: uno dei componenti più importanti della piattaforma multilivello di Kaspersky Lab, Kaspersky Security Network è un'architettura distribuita e complessa basata su cloud, dedicata alla raccolta e all'analisi della threat intelligence per la sicurezza da milioni di sistemi in tutto il mondo.

A tutti gli effetti un laboratorio globale di minacce basato su cloud, KSN rileva, analizza e gestisce minacce sconosciute e nuove e risorse di attacco online in pochi secondi fornendo l'intelligence necessaria direttamente ai sistemi del cliente. Per le imprese con problemi molto specifici riguardanti la privacy dei dati, Kaspersky Lab ha sviluppato un'opzione Kaspersky Private Security Network.

Security Intelligence Services: alcune organizzazioni hanno le risorse per sviluppare livelli elevati di security intelligence strategica necessari per tenere il passo con la continua evoluzione di minacce sofisticate. Ecco perché Kaspersky Lab ha sviluppato un ampio portfolio di servizi di intelligence:

Istruzione e formazione: dai più generici fondamenti di cybersicurezza all'analisi forense digitale avanzata, dall'analisi del malware alla reverse engineering, Kaspersky Lab offre una gamma completa di corsi di formazione e programmi di sensibilizzazione per le imprese, sia in loco che online. In aggiunta a giochi interattivi, valutazioni delle competenze e promozione generale della cybersicurezza, sono anche disponibili corsi di 2-5 giorni su alcuni dei seguenti argomenti:

- **Fondamenti di cybersicurezza:** comprensione delle minacce, utilizzando la tecnologia in modo sicuro.
- **Analisi forense digitale:** costruzione di un laboratorio di analisi forense digitale, ricostruzione dell'incidente, strumenti.
- **Analisi del malware generale e reverse engineering:** creare un ambiente sicuro per l'analisi dei malware, condurre analisi rapide.
- **Analisi forense digitale avanzata:** analisi approfondita del file system, recupero dei file eliminati, ricostruzione della tempistica dell'incidente.
- **Analisi del malware avanzata e reverse engineering:** analizzare il codice della shell degli exploit, malware diversi da Windows, utilizzo di best practice globali.

Valutazione di sicurezza:

- **Penetration test:** comprendere la sicurezza dell'infrastruttura dalla prospettiva di un utente malintenzionato, ottenendo al contempo la conformità con standard di sicurezza quali PCI DSS.
- **Applicazione di test di sicurezza:** analisi delle applicazioni web (inclusi i servizi di online banking e con WAF abilitato), applicazioni mobili, fat client.

Threat intelligence:

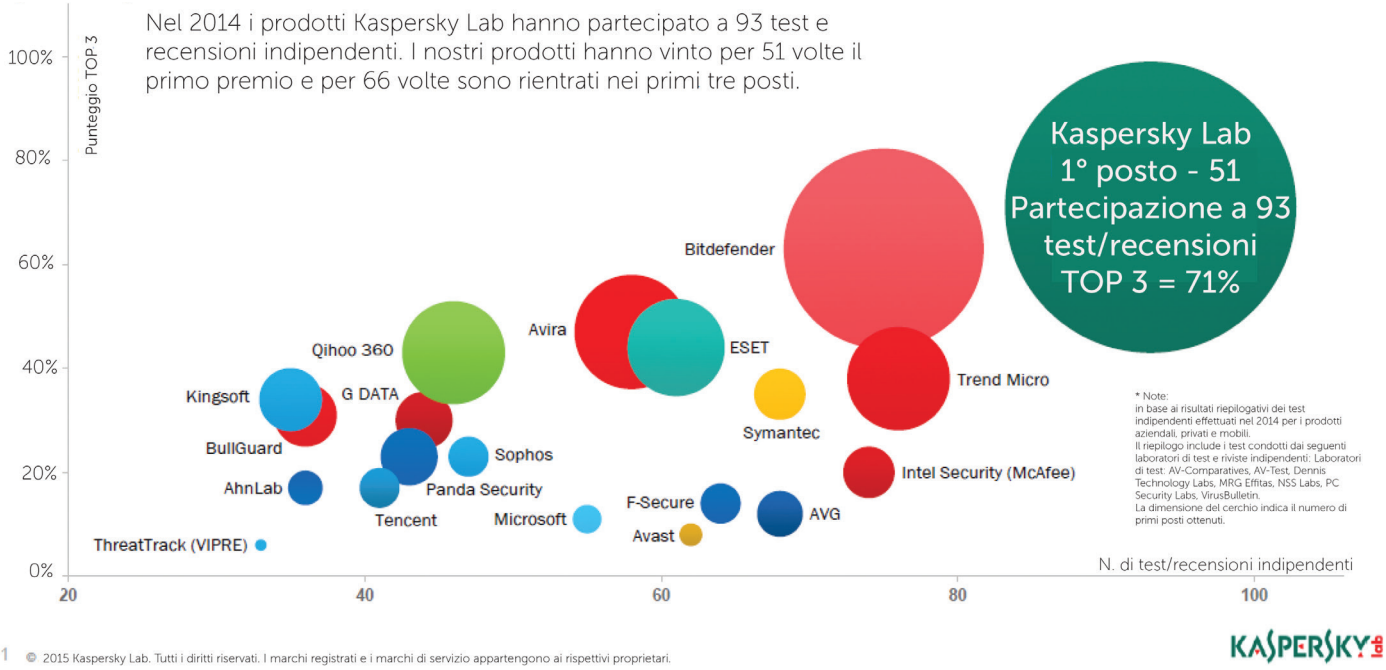
- Un sistema di avviso precoce, supportato dall'esperienza del team GReAT e da KSN, include feed di dati sulle minacce, monitoraggio delle minacce botnet e rapporti sull'intelligence. L'accesso anticipato ai file di configurazione relativi ad APT e ai campioni di malware, insieme all'integrazione con SIEM (HP Arcsight) aiuta le imprese a sviluppare informazioni di intelligence complete.

PREVENZIONE

Kaspersky Lab rileva 325.000 nuovi malware *ogni giorno*. Ogni singolo punto percentuale aggiuntivo nella percentuale di rilevamento può tradursi in centinaia di migliaia di malware che riescono a penetrare nella rete. I risultati dei test indipendenti dimostrano costantemente che Kaspersky Lab fornisce la migliore protezione del settore. Nel 2014, abbiamo preso parte a 93 test e revisioni indipendenti e ci siamo classificati al primo posto 51 volte e nei primi tre il 71% delle volte, un record assoluto.[2] E questo è solo uno dei motivi per cui numerosi OEM, tra cui Microsoft, Cisco Meraki, Juniper Networks e Alcatel Lucent, si affidano a Kaspersky Lab per garantire la massima sicurezza ai propri prodotti.

[2] Per ulteriori dettagli sui test e le metriche, visitare: http://media.kaspersky.com/en/business-security/TOP3_2013.pdf
Il nuovo link per il report aggiornato è: http://media.kaspersky.com/en/business-security/TOP3_2014.pdf.

KASPERSKY LAB GARANTISCE LA MIGLIORE PROTEZIONE DEL SETTORE*



Il nostro portfolio di sicurezza aziendale combina un anti-malware leader del settore con diverse tecnologie per la riduzione delle superfici di attacco in un'esclusiva combinazione di tecnologie guidate dall'intelligence.

Le minacce conosciute, sconosciute e avanzate vengono prevenute usando livelli multipli di protezione, inclusi:

Network Attack Blocker: esegue una scansione di tutto il traffico di rete utilizzando firme conosciute per rilevare e bloccare attacchi basati sulla rete, compresi scansione delle porte, attacchi DoS (Denial-of-Service). Per un ulteriore livello di protezione, Kaspersky DDoS Protection (KDP) è disponibile come parte di una soluzione per la protezione contro gli attacchi DDoS (Distributed Denial of Service). Si tratta di una soluzione di migrazione e prevenzione DDoS integrata e completa che include un'analisi 24 ore su 24, 7 giorni su 7 e report postattacco.

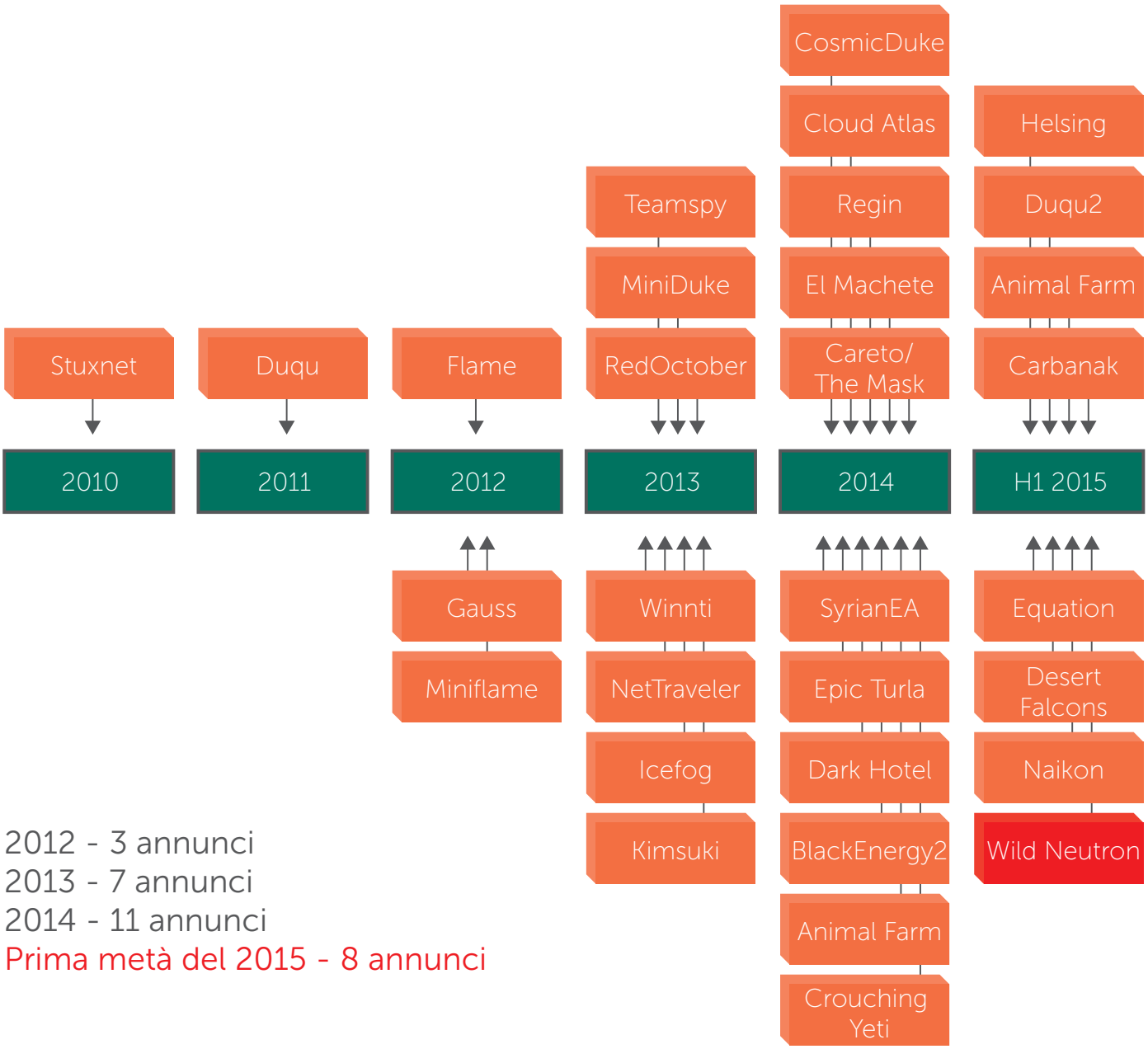
Anti-phishing euristico: in grado di prevenire alcune delle più recenti tecniche di attacco via phishing mediante la ricerca di ulteriori prove di attività sospette, superando gli approcci tradizionali di phishing basati sul database. Controllo Applicazioni e Whitelisting Dinamico: Application Control blocca o consente l'esecuzione delle applicazioni specificate dall'amministratore. Basandosi sul whitelisting dinamico: le liste di applicazioni e categorie di software attendibili vengono aggiornate costantemente da Kaspersky Lab.

Host Intrusion Prevention System (HIPS): consente di controllare il modo in cui le applicazioni si comportano e limita l'esecuzione di programmi potenzialmente dannosi senza influenzare le prestazioni di applicazioni autorizzate e sicure.

RILEVAMENTO

L'esperienza senza paragoni di Kaspersky Lab nel rilevamento di alcune delle più sofisticate minacce alimenta direttamente le nostre capacità di rilevamento delle minacce aziendali. A partire dal 2008, i nostri ricercatori hanno scoperto alcuni degli attentati multicomponente più sofisticati che il mondo abbia visto. Queste informazioni e l'intelligence informano direttamente il nostro dipartimento di sviluppo dei prodotti; in aggiunta alla nostra capacità di rilevare sofisticati attacchi mirati alle imprese, Kaspersky Lab ha utilizzato le conoscenze acquisite grazie alla scoperta di importanti minacce finanziarie, come Carbanak, per sviluppare soluzioni interamente orientate verso il rilevamento delle frodi finanziarie.

ANNUNCI APT KASPERSKY LAB



2012 - 3 annunci
2013 - 7 annunci
2014 - 11 annunci
Prima metà del 2015 - 8 annunci

RISPOSTA

In una architettura per la sicurezza adattabile, la capacità di rispondere alle minacce è importante quanto la capacità di prevederle e prevenirle per salvare sia il tempo che il denaro delle aziende. Vale inoltre la pena riconoscere che una diretta conseguenza di una rilevazione avanzata sarà una capacità di risposta potenziata. Kaspersky Lab affronta la questione sia a livello di tecnologia che di servizi:

System Watcher: il monitor proattivo ed esclusivo di Kaspersky Lab è in grado di reagire ai complessi eventi del sistema, come l'installazione di driver e rilevare un comportamento sospetto.

Servizi di indagine: risolvere incidenti di sicurezza in tempo reale grazie all'aiuto di Kaspersky Lab. Dall'analisi del malware all'analisi forense digitale, ai rapporti e alla risposta agli incidenti, i clienti sono in grado di imparare dagli incidenti e di ridurre l'impatto di un attacco e ripristinare i sistemi danneggiati.

SICUREZZA AZIENDALE PROATTIVA, REATTIVA E GUIDATA DALL'INTELLIGENCE

Le minacce avanzate sfuggono alle tradizionali tecniche di blocco, è possibile acquistare online kit pronti per i malware e gli strumenti in grado di effettuare automaticamente la creazione di varianti personalizzate di un unico pezzo di malware sono solo la punta di un enorme iceberg di malware.

Un panorama di minacce sempre più sofisticate e complesse impone un approccio multilivello adattabile, in cui una combinazione di tecnologie integrate fornisca funzionalità complete di rilevamento e protezione dal malware e da altre minacce conosciute, sconosciute e avanzate che mirano alle aziende.

Gli impareggiabili successi nella scoperta delle minacce più sofisticate e rilevanti, in combinazione con i servizi e le tecnologie leader del settore, permettono a Kaspersky Lab di occupare una posizione privilegiata nella fornitura di una sicurezza completa e adattabile per le esigenze delle aziende. Mentre la soluzione Kaspersky Security Network si basa su un'intelligence in tempo reale generata da oltre 60 milioni di nodi in tutto il mondo, il team GReAT apporta un eccezionale contributo in termini di competenze ed esperienza, che si aggiunge alle nostre capacità in materia di ricerca delle minacce. Questa collaborazione è la culla di soluzioni sempre efficienti nella lotta contro minacce sempre più complesse e avanzate.

PARTNER DI FIDUCIA DI AZIENDE, GOVERNI ED ENTI DI REGOLAMENTAZIONE

Essendo un'azienda privata, Kaspersky Lab è libera di investire ingenti risorse nella ricerca e nello sviluppo senza i vincoli imposti dal mercato a breve termine. Quasi la metà dei nostri 3000 dipendenti a livello globale opera nei nostri laboratori di ricerca e sviluppo, concentrandosi sullo sviluppo di tecnologie innovative e svolgendo indagini sulla guerra informatica, il cyberspionaggio e su tutti i tipi di minacce e di tecniche.

Grazie a questa particolare attenzione dedicata al settore interno e di alta qualità della ricerca e dello sviluppo, Kaspersky Lab è riconosciuta come leader del settore nel campo delle tecnologie di sicurezza IT. E questo è solo uno dei motivi per cui più di 100 OEM leader, tra cui Microsoft, Cisco Meraki, IBM, Juniper Networks e Alcatel Lucent, si affidano a Kaspersky Lab per garantire la massima sicurezza ai propri prodotti.

È anche il motivo per cui siamo un partner fidato di governi, forze dell'ordine e grandi aziende di tutto il mondo. Stimate organizzazioni internazionali, tra cui INTERPOL, Europol e numerosi CERT hanno tutte invitato Kaspersky Lab a collaborare e si consultano con l'azienda su base costante; oltre a tenere regolarmente corsi di formazione per gli ufficiali di polizia di INTERPOL in diversi paesi, abbiamo supportato il lancio del Digital Forensics Laboratory di INTERPOL.


Twitter.com/
KasperskyLabIT


Facebook.com/
Kasperskylabitalia


Youtube.com/
Kasperskyitalia

Kaspersky Lab, Mosca, Russia
www.kaspersky.it

Tutto sulla sicurezza in Internet:
www.securelist.com

Trovate il partner più vicino:
www.kaspersky.it/buyoffline

KASPERSKY lab