KASPERSKY ENDPOINT SECURITY FOR BUSINESS: TECNOLOGIA IN AZIONE

Per le minacce visibili e per quelle che non si vedono

KASPERSKY lab

THE POWER OF PROTECTION

kaspersky.it/business
#Securebiz

SOMMARIO

il 94% delle aziende ha subito minacce esterne alla sicurezza di vario genere.

Fonte: Kaspersky Lab – Rapporto sui rischi globali IT 2014

PROTEGGERE L'AZIENDA DALLE MINACCE VISIBILI... E DA QUELLE CHE NON SI VEDONO

Poter contare sulla giusta protezione IT non è mai stato più importante.

CIÒ CHE NON SI CONOSCE *PUÒ* ESSERE PERICOLOSO

Oltre il 30% delle violazioni di sicurezza interessano aziende con un massimo di 100 dipendenti.[1] Il 44% delle piccole e medie imprese (PMI) ha subito un attacco da parte di criminali informatici.[2]

Tuttavia, in molti ancora non conoscono le minacce molto reali costituite da cybercriminali e malware avanzato. Mentre meno di un quinto delle piccole imprese ammette di non aver preso alcuna precauzione contro il cybercrimine, solo il 60% mantiene aggiornato il software anti-malware in uso.[3]

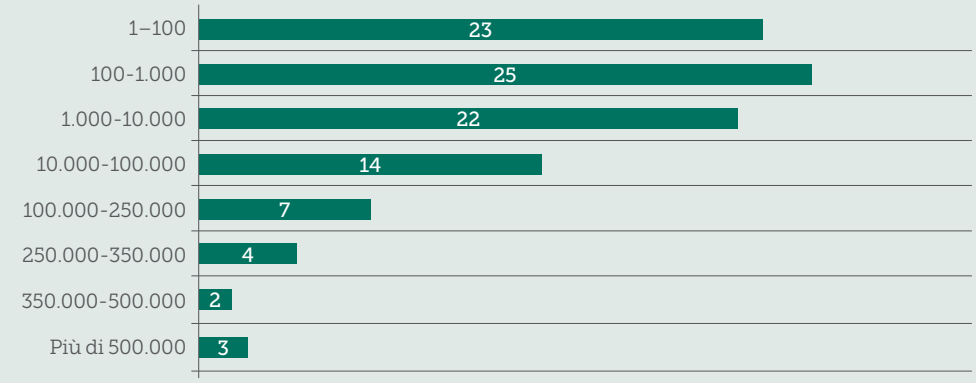
L'errata convinzione che le piccole dimensioni di un'azienda la tengano al riparo da attacchi malware sempre più sofisticati è proprio ciò su cui i cybercriminali fanno affidamento per lavorare indisturbati. Sanno che molte PMI si ritengono, sbagliando, un obiettivo di scarso interesse.

[1] Verizon - 2013 Data Breach Investigations Report (Report sull'indagine sulle violazioni dei dati 2013)
[2] Sondaggio della National Small Business Association (2013)
[3] Kaspersky Lab, Threatpost, 24 maggio 2013

CIÒ CHE NON SI VEDE

Immaginiamo che la vostra azienda faccia parte dell'80% di PMI dotate di una soluzione per la sicurezza IT. Non pensiate che sia sufficiente: la maggior parte delle aziende sottovaluta enormemente i volumi delle minacce.[4] Solo il 4% delle aziende partecipanti al sondaggio si è avvicinato al numero effettivo di minacce scoperte ogni giorno.[4]

NUMERO PERCEPITO DI NUOVI CAMPIONI DI MALWARE SCOPERTI QUOTIDIANAMENTE (%)



Fonte: Kaspersky Lab – Rapporto sui rischi globali IT 2014

In un simile contesto, non sorprende che alcuni utenti considerino la sicurezza IT come un "lusso" senza vedere le diverse opzioni a disposizione. Si tratta di un mito pericoloso. Persino una differenza dell'1% sulle percentuali di rilevamento può tradursi in migliaia di minacce malware che non vengono fermate nel corso dell'anno. Come lo sappiamo?

- Kaspersky Lab rileva 325.000 nuovi malware ogni giorno.
- Nel secondo trimestre del 2014, le nostre soluzioni anti-malware hanno rilevato 528.799.591 attacchi di virus a sistemi degli utenti finali e identificato un totale di 114.984.065 oggetti nocivi.[5]

Le minacce più pericolose sono quelle che non si conoscono: le minacce che gli esperti di Kaspersky Lab monitorano, analizzano e mitigano ogni giorno. Siamo in cerca di problemi. E quando li troviamo, utilizziamo più di un decennio di threat intelligence ed esperienza per fornire protezione aggiuntiva contro le minacce più pericolose per la vostra organizzazione, specialmente quando si tratta di malware avanzato e Advanced Persistent Threat (APT).

Esiste un divario crescente tra l'opinione delle aziende riguardo alle minacce e la realtà delle cose. Lo abbiamo chiamato un "divario di percezione". Mostra che le organizzazioni, indipendentemente dalle loro dimensioni, sottovalutano enormemente il volume e la gravità delle minacce che devono affrontare.

Costin Raiu, Global Research & Analysis Team, Kaspersky Lab

[4] Kaspersky Lab – Rapporto sui rischi globali IT 2014
[5] Kaspersky Lab Q2 Threat Evolution Report 2014
(Rapporto sull'evoluzione delle minacce nel secondo trimestre del 2014)

PROATTIVO, REATTIVO, INTELLIGENTE

Kaspersky Lab ha una lunga esperienza alle spalle nella scoperta di alcune delle minacce più pericolose e di più alto profilo della storia, tra cui Carbanak ("cyberfurto del secolo" ai danni delle banche), Dark Hotel, The Mask, Icefog e Red October. Oltre un terzo dei nostri dipendenti lavora nel settore della ricerca e sviluppo.
Si concentrano 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.

La conoscenza del funzionamento interno di alcune delle minacce più sofisticate del mondo ci ha consentito di sviluppare una piattaforma di sicurezza multilivello per combattere le minacce conosciute, sconosciute e avanzate. Le nostre tecnologie rilevano e mitigano le minacce visibili e quelle invisibili.

Come ci riusciamo? Di seguito, spieghiamo come le tecnologie anti-malware e di rilevamento delle minacce di Kaspersky Lab siano in grado di lavorare insieme contemporaneamente, fin dal caricamento del file. Si tratta di una combinazione unica di tecnologie di intelligence in grado di garantire rilevamento e prevenzione multilivello dalle minacce su più endpoint e altri elementi delle infrastrutture IT.

RILEVAMENTO DELLE MINACCE CONOSCIUTE

A partire dal download del file, dalla visualizzazione della pagina Web o dal lancio dell'applicazione, gli avanzati motori anti-malware di Kaspersky Lab controllano, rilevano e proteggono contemporaneamente il sistema da virus, trojan, rootkit, worm, spyware, script, adware e altre minacce e oggetti nocivi conosciuti, sconosciuti e avanzati, basati su Web o e-mail. A partire dalle minacce conosciute, che ne costituiscono il nucleo, questi motori comprendono:

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), overrun del buffer e altre attività nocive remote.

BLACKLISTING

Team dedicati di analisti del malware provvedono a mantenere aggiornati i database di Kaspersky Lab con le firme e i dati più recenti. Questi vengono utilizzati automaticamente per bloccare tutto il malware conosciuto.

FILTRO URL

Scansiona e verifica gli URL nel traffico in entrata e in uscita in base al database di siti Web pericolosi e di phishing di Kaspersky Lab al fine di bloccare gli attacchi basati sul Web, il malware polimorfo lato server e i server di Command and Control (C&C).

FIREWALL

Analizza ogni singolo pacchetto in entrata e in uscita sulla rete, bloccandolo o autorizzandolo, in base ai rischi per la sicurezza. Le connessioni non autorizzate vengono bloccate riducendo la superficie dell'attacco e le possibilità di infezione. L'attività di rete dei sistemi infettati o altrimenti compromessi viene limitata riducendo così la diffusione del malware e limitando i danni causati dalle violazioni dei criteri di sicurezza.

Tecnologie basate su firma di Kaspersky Lab, realizzate sulla base di anni di conoscenze ed esperienza accumulate. Tutte le tecnologie sopra riportate sono eccellenti nel bloccare malware conosciuto (e grazie a Kaspersky Security Network, come descritto in seguito, molte minacce restano sconosciute solo per un breve periodo di tempo). E per quanto riguarda le minacce sconosciute o avanzate di cui abbiamo parlato in precedenza? Ci occupiamo anche di quelle...

[6] La tecnologia antispam di Kaspersky Lab ha ottenuto il primo posto nel VB Spam Test svolto nel novembre 2014, con una percentuale di rilevamento pari al 99,75% e zero falsi positivi.

RILEVAMENTO DI MINACCE SCONOSCIUTE

Una volta superati i controlli basati su firma per le minacce conosciute, il file viene monitorato durante la sua esecuzione. Le tecnologie proattive e multilivello di Kaspersky Lab analizzano e controllano i file al momento dell'esecuzione e cercano attività sospette e nocive che suggeriscono la potenziale presenza di una minaccia.

EURISTICA

L'analisi euristica offre una protezione proattiva dalle minacce che non possono essere rilevate utilizzando i tradizionali database antivirus. L'euristica di Kaspersky Lab consente il rilevamento di nuovo malware o modifiche sconosciute al malware conosciuto. L'analisi statica scansiona il codice alla ricerca di comandi sospetti associali al malware mentre l'analisi dinamica esamina il codice del computer che il file potrebbe tentare di eseguire rispondendo a "chiamate" simulate con "risposte" probabili per capire se il codice è sicuro o meno.

ANTI-PHISHING EURISTICO

In caso di attacchi di phishing estremamente nuovi, che interessano solo un piccolo numero di utenti, la tecnologia Kaspersky Lab può ricercare ulteriori prove di attività sospette quali parole, moduli di input o sequenze illeggibili di simboli. Ciò si aggiunge all'approccio più tradizionale e basato su database descritto in precedenza.

Le minacce basate su phishing sono state il punto di partenza per molte delle minacce più recenti e pericolose.

HOST INTRUSION PREVENTION SYSTEM (HIPS)

Il sistema HIPS di Kaspersky Lab aggiunge un ulteriore livello di protezione mediante il rilevamento e la gestione di applicazioni e attività sospette al fine di prevenire il lancio delle minacce. HIPS consente di controllare il comportamento delle applicazioni impostando livelli di affidabilità in seguito all'analisi iniziale. Questi livelli definiscono quali risorse possono essere utilizzate, il tipo di dati al quale è possibile accedere o che possono essere modificati, ecc. Limita l'esecuzione di programmi potenzialmente pericolosi senza influire sulle prestazioni di applicazioni sicure e autorizzate. Un'applicazione non attendibile non viene autorizzata ad alcuna azione, avvio compreso.

APPLICATION CONTROL E WHITELISTING

Application Control blocca o consente l'esecuzione delle applicazioni specificate dall'amministratore. L'approccio di Kaspersky Lab si basa sul whitelisting dinamico: le liste di applicazioni attendibili vengono aggiornate costantemente così come le categorie di software che possono essere eseguite in base a regole e criteri specifici. Kaspersky Lab possiede un database e un laboratorio di whitelisting dedicati comprendenti più di un miliardo di file e con un incremento di un milione al giorno.

L'uso di Application Control e del whitelisting riduce i rischi posti dalle minacce che ancora non conosciamo; la maggior parte del malware viene fornito in un file eseguibile non incluso nella whitelist. Le organizzazioni che adottano questo aspetto (e le relative tecnologie) possono pertanto prevenire l'esecuzione dei file nocivi senza dover identificare o conoscere quali siano nello specifico.

KASPERSKY SECURITY NETWORK

A tutti gli effetti un laboratorio globale di minacce basato su cloud, Kaspersky Security Network rileva, analizza e gestisce minacce conosciute, sconosciute e nuove e risorse di attacco online in pochi secondi fornendo l'intelligence necessaria direttamente ai sistemi del cliente.

Utilizzando dati in tempo reale e in forma anonima provenienti da 60 milioni di sensori endpoint in tutto il mondo, ogni file che supera i sistemi protetti di Kaspersky Lab viene sottoposto ad analisi in base alla minaccia pertinente. Gli stessi dati garantiscono che venga intrapresa l'azione più adatta. Lavorando insieme a tutti gli altri componenti del motore di Kaspersky Lab, Kaspersky Security Network consente la protezione dalle minacce sconosciute prima che sia disponibile la relativa firma. Mentre le risposte basate su firma tradizionale possono richiedere alcune ore, Kaspersky Security Network impiega circa 40 secondi.

RILEVAMENTO DELLE MINACCE AVANZATE

Il file è stato scaricato e avviato; le tecnologie Kaspersky Lab lo hanno scansionato, analizzato e applicato l'intelligence necessaria per bloccarlo o autorizzarlo in base a eventuali minacce conosciute o sconosciute.

Ma cosa sono le minacce avanzate?

Le tecnologie di rilevamento delle minacce avanzate di Kaspersky Lab sono studiate per rilevare e bloccare le minacce avanzate utilizzando una gamma di meccanismi comportamentali proattivi e sofisticati capaci di monitorare i comportamenti dei processi, individuare modelli sospetti, bloccare attività nocive ed eseguire il rollback delle modifiche nocive, compreso Cryptors.

Diamo un'occhiata...

SYSTEM WATCHER

Monitora e raccoglie dati sull'applicazione e altre importanti attività di sistema mediante il monitoraggio delle attività e l'individuazione di modelli comportamentali. Le informazioni ottenute vengono fornite agli altri componenti di protezione di Kaspersky Lab come descritto in precedenza. Le attività che corrispondono ai modelli della minaccia vengono gestite in base ai criteri impostati dall'amministratore oppure in base all'impostazione predefinita che prevede di terminare il processo nocivo e metterlo in quarantena per un'analisi successiva.

Il driver che intercetta le operazioni del file per il componente anti-malware di Kaspersky raccoglie anche le informazioni sulle modifiche apportate al registro mentre il firewall raccoglie i dati sull'attività di rete delle applicazioni. Tutte queste informazioni vengono fornite a System Watcher che, a sua volta, possiede il proprio modulo capace di reagire a eventi complessi di sistema come l'installazione di driver.

Le azioni nocive e i modelli di comportamento distruttivi che suggeriscono la presenza di malware vengono bloccati.

PREVENZIONE AUTOMATICA DEGLI EXPLOIT (AEP)

Questa tecnologia è destinata specificamente al malware che prende di mira le vulnerabilità dei software. Sviluppata mediante l'analisi approfondita delle caratteristiche e dei comportamenti degli exploit più diffusi, questa tecnologia è in grado di identificare i modelli di comportamento che caratterizzano un exploit ed evitare che vengano portati a termine.

AEP agisce come una rete di sicurezza, un ulteriore livello di protezione che integra le altre tecnologie Kaspersky Lab. Funziona insieme a System Watcher di Kaspersky Lab.

ROLLBACK

Il monitoraggio continuo e dettagliato dei sistemi rende possibile una funzionalità di rollback estremamente precisa, limitando l'impatto delle infezioni e ripristinando i sistemi in base a parametri sicuri. I meccanismi di rollback possono essere aggiornati e funzionano con file eseguibili creati e modificati, modifiche MBR e importanti file Windows e chiavi di registro.

DEFAULT DENY

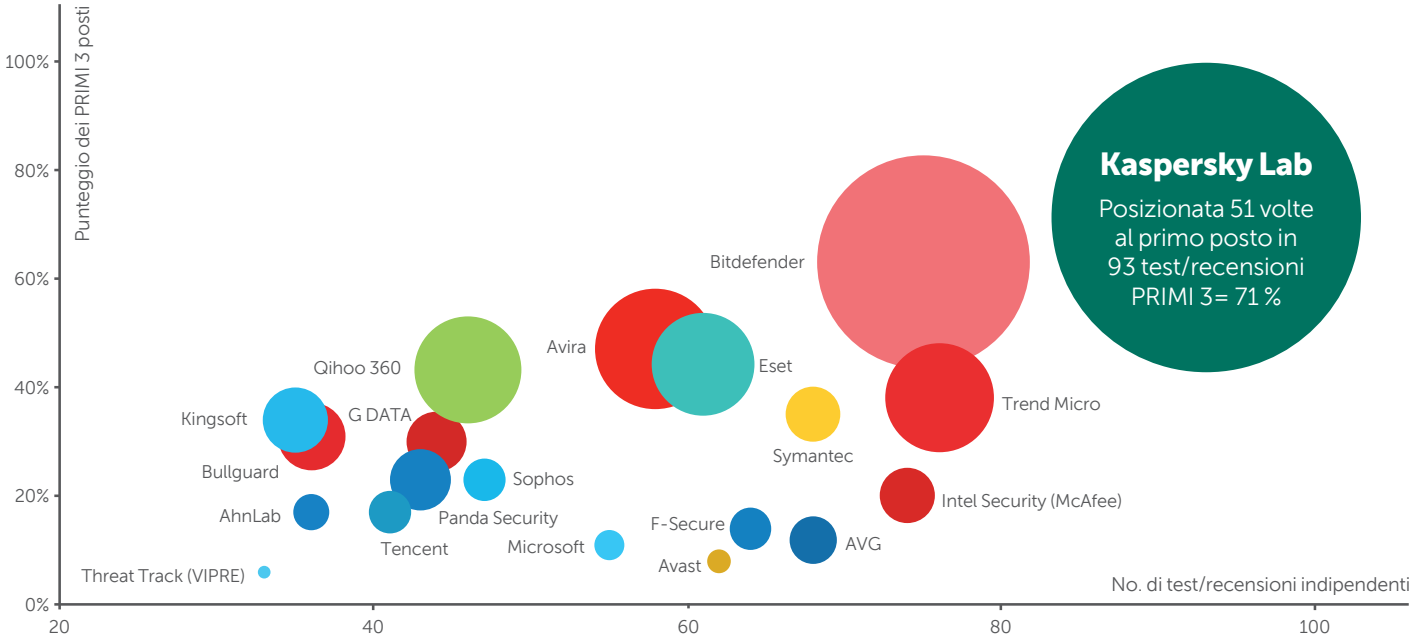
Viene attualmente ritenuto l'approccio di sicurezza più efficace da adottare in caso di minacce avanzate e in evoluzione. Semplicemente, blocca l'esecuzione di tutte le applicazioni su qualsiasi workstation, a meno che non sia stata esplicitamente consentita dall'amministratore.

Default Deny significa che tutte le nuove varietà di malware basate su file vengono bloccate automaticamente, anche per attacchi mirati.

UNA PICCOLA MODIFICA PUÒ FARE UNA GRANDE DIFFERENZA

Come abbiamo visto, ogni singolo punto percentuale aggiuntivo nella percentuale di rilevamento può tradursi in centinaia di migliaia di malware che riescono a penetrare nella rete. Inoltre, abbiamo visto come le "reti" aggiuntive di mitigazione, rilevamento e analisi di Kaspersky Lab siano in grado di bloccare minacce sconosciute e persino avanzate prima che riescano ad agire.

KASPERSKY LAB: LA MIGLIORE PROTEZIONE DEL SETTORE*



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. 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.

Tutte le tecnologie di sicurezza di Kaspersky Lab vengono sviluppate e aggiornate in sede, dalla stessa base di codice e, pertanto, sono perfettamente integrate e consentono di strutturare una piattaforma multilivello migliore della somma delle parti. Un simile livello di integrazione si traduce anche in prestazioni ottimizzate, aggiornamenti più rapidi e un look unificato tra tutte le soluzioni al fine di consentire agli utenti finali di concentrarsi sulle loro mansioni principali mentre Kaspersky Lab si occupa della sicurezza.

* Note:
In base ai risultati riepilogativi dei test indipendenti effettuati nel 2014 per i prodotti aziendali, privati e mobili.

Il riepilogo include test condotti dai seguenti laboratori di test e riviste indipendenti:
AV-Comparatives, AV-Test, Dennis Technology Labs, MRG Effitas, NSS Labs, PC Security Labs, VirusBulletin.
La dimensione del cerchio indica il numero di primi posti ottenuti.

INIZIATE OGGI STESSO: VERSIONE DI PROVA GRATUITA PER 30 GIORNI

Scoprite come la nostra eccellente sicurezza sia in grado di proteggere la vostra azienda dal malware e dal cybercrimine con una prova non vincolante.

Visitate **kaspersky.it/trials** oggi stesso per scaricare le versioni complete dei prodotti e valutare l'efficacia della loro protezione per l'infrastruttura IT, gli endpoint e i dati aziendali riservati.

DOWNLOAD GRATUITO

PARTECIPATE ALLA CONVERSAZIONE

#Securebiz

Guardateci su YouTube

Visitate la nostra pagina Facebook

Seguiteci su Twitter

Collegatevi su LinkedIn

Visualizzateci su SlideShare

Leggete il nostro blog

Collegatevi su Threatpost

Visualizzateci su Securelist

INFORMAZIONI SU KASPERSKY LAB

Kaspersky Lab è il maggior fornitore privato di soluzioni per la protezione degli endpoint al mondo. L'azienda è tra i primi quattro fornitori mondiali di prodotti di sicurezza per utenti endpoint*. Da più di 17 anni Kaspersky Lab è pioniere della sicurezza IT e offre soluzioni efficaci per la sicurezza digitale a grandi aziende e piccole e medie imprese e a privati. Kaspersky Lab, la cui società madre ha sede legale nel Regno Unito, è attualmente presente in quasi 200 Paesi e territori a livello globale e offre soluzioni di protezione a oltre 400 milioni di utenti in tutto il mondo. Ulteriori informazioni sul sito Web: www.kaspersky.it/business

* La società ha conseguito il quarto posto nella classifica 2013 di IDC relativa ai fornitori nel settore della sicurezza degli endpoint con il maggior fatturato. La classifica è stata pubblicata nella relazione di IDC dal titolo "Worldwide Endpoint Security 2014–2018 Forecast and 2013 Vendor Shares" (IDC # 250210, agosto 2014). Nella relazione viene stilata una classifica di fornitori software basata sui ricavi ottenuti dalla vendita di soluzioni per la sicurezza degli endpoint nel 2013.

kaspersky.it/business
#Securebiz