KASPERSKY lab

THE POWER OF PROTECTION

RISCHI FUTURI: COME PREPARARSI

Rapporto specifico sulle tecniche di protezione dalle minacce avanzate

kaspersky.it/enterprise
#EnterpriseSec

SOMMARIO

ADVANCED PERSISTENT THREATS (APT) E PANORAMA DELLE MINACCE

La cybersicurezza non è una questione di numeri. Quando basta solo un singolo attacco per causare gravi danni ad un'azienda, la difesa dai tradizionali attacchi non basta.

Ecco perché è meglio concentrare l'attenzione sulle minacce più pericolose a cui siamo esposti, anziché su quelle più frequenti.

L'ecosistema del malware si suddivide in minacce **conosciute** (70%), minacce **sconosciute** (29%) e minacce **avanzate** (1%).

Le minacce conosciute, che rappresentano circa il 70% del malware, sono relativamente facili da contrastare. Purché riconosciuto, il codice dannoso può essere bloccato e i tradizionali metodi basati sulle firme consentono in generale di gestirlo.

Un ulteriore 29% del malware rientra nel campo delle "minacce sconosciute". Per contrastarle, sono necessari strumenti più sofisticati, ma grazie all'utilizzo di metodi che vanno oltre il software antivirus standard, ad esempio analisi euristica e whitelisting dinamico, è possibile combattere anche queste minacce.

C'è poi un rimanente 1% rappresentato dalle minacce avanzate, che sono costituite da attacchi multiforme, continui e mirati. Progettati per penetrare in una rete, rimanere nascosti e raccogliere dati sensibili, una volta in azione possono rimanere per anni senza essere rilevati.

Una APT nota come "Darkhotel" ha utilizzato la connessione Wi-Fi degli hotel di lusso per sottrarre i dati degli ospiti per un periodo di sette anni prima di essere scoperta. Si è trattato di una APT particolarmente interessante poiché puntava a bersagli di fascia elevata (alti dirigenti e CEO) e ha mostrato in modo molto preciso i problemi per la sicurezza IT posti dagli endpoint (laptop e tablet aziendali) quando lasciano la sicurezza della rete aziendale.

Una APT nota come "Darkhotel" ha utilizzato la connessione Wi-Fi degli hotel di lusso per sottrarre i dati degli ospiti per un periodo di sette anni prima di essere scoperta.

Anche se alcune organizzazioni di altissimo profilo sono cadute vittime delle APT, non è necessario essere visibili pubblicamente per essere bersaglio dei cybercriminali. Le aziende devono essere in grado di mitigare il rischio rappresentato dalle APT e le conseguenze che potrebbero derivare da un attacco, sia che si tratti di perdita di dati, tempi di inattività prolungati o grave danno alla reputazione. Inoltre, poiché le APT operano in genere in modo silente e occulto, la prevenzione è molto meno costosa della correzione dopo un attacco, dato che quest'ultimo potrebbe essere avvenuto molto tempo prima e aver procurato danni incalcolabili per mesi e persino anni.

Non esiste una soluzione unica a questo problema. Anche se utili, le tecnologie utilizzate per contrastare le minacce conosciute e sconosciute non sono da sole sufficienti a combattere le APT. Un panorama di minacce sempre più sofisticate e complesse impone un approccio multilivello, in cui una combinazione di tecnologie integrate fornisca funzionalità complete di rilevamento e protezione dal malware e da altre minacce conosciute, sconosciute e avanzate.

Questo rapporto è stato creato con lo scopo di acquisire maggiori conoscenze per contrastare le APT.

Il costo medio di un attacco malware è di 56.000 dollari per una PMI e di 649.000 dollari per una grande azienda.[1]

Le APT possono avere enormi conseguenze. Durante il 2014 Kaspersky Lab ha contribuito a scoprire il funzionamento di Carbanak. Questo complesso attacco ha consentito a un gruppo internazionale di criminali di sottrarre 1 miliardo di dollari da una serie di istituti finanziari. Dopo aver infettato la rete di una banca, il gruppo è riuscito a registrare tutto ciò che accadeva sugli schermi dei dipendenti e a scoprire come trasferire denaro senza che fosse rilevato.

[1] The high cost of a security breach, Kaspersky Lab.

L'AZIENDA È UN BERSAGLIO: 5 PUNTI CHIAVE

Le grandi aziende sanno di essere esposte a minacce alla sicurezza IT. Queste minacce stanno semplicemente diventando più mirate e sofisticate.

1 Il primo passo per creare una strategia appropriata per affrontare le APT è rendersi conto di essere un potenziale bersaglio. La verità è che, indipendentemente dal fatto che si tratti di proprietà intellettuale, dettagli di contatto o informazioni finanziarie, la vostra organizzazione possiede dati da cui i criminali potrebbero trarre profitto. Anche se non sono i dati dell'organizzazione quelli a cui danno la caccia, possono utilizzarne la rete come mezzo per arrivare ai partner o ai clienti, come nel caso di Darkhotel.

2 In secondo luogo, è necessario acquisire una maggiore conoscenza delle vulnerabilità. Nelle organizzazioni in cui un elevato numero di dipendenti opera su vari dispositivi, applicazioni e piattaforme, può essere difficile avere il controllo totale di tutti i rischi e di tutti i potenziali "vettori di attacco" che i cybercriminali possono sfruttare. Poiché le APT puntano alle vulnerabilità, umane o tecniche, quanto più grande e complessa è un'organizzazione, tanti più sono i potenziali punti di ingresso.

3 La diffusione del modello BYOD e del lavoro flessibile aumenta ulteriormente le difficoltà. Oltre a essere vulnerabili in sé, telefoni e tablet sono spesso utilizzati per la connessione a reti non protette. A peggiorare le cose, è spesso più difficile, specialmente con sistemi operativi come iOS di Apple, stabilire se un dispositivo sia infettato. Una forza lavoro mobile è come un bersaglio in movimento: i dispositivi che operano all'esterno del perimetro di sicurezza dell'azienda sono più difficili da controllare, per cui la sicurezza efficace degli endpoint è un componente importante della strategia di sicurezza.

4 Questa ampia varietà di endpoint, abbinata al numero di metodi a disposizione dei cybercriminali per infettare una rete fa sì che le misure di sicurezza singole semplicemente non bastano. Al contrario, efficaci misure di protezione devono combinare intelligence sulle minacce, criteri di sicurezza e tecnologie specializzate che non solo blocchino le minacce in entrata, ma anche individuino le nuove, utilizzando al contempo misure come il whitelisting per evitare l'esecuzione delle minacce ancora sconosciute.

5 La mitigazione ha bisogno di una nuova attenzione incentrata sugli endpoint. I cybercriminali sfruttano le vulnerabilità e l'azienda ha spesso il suo punto più debole negli endpoint, dove la sicurezza è frequentemente compromessa non solo dal dispositivo stesso, ma anche dal comportamento meno attento del dipendente o dagli ambienti circostanti non protetti in cui il dispositivo viene utilizzato. Se gli endpoint non dispongono di una protezione multilivello, l'intera organizzazione può essere esposta a rischi.

PERCHÉ LA MITIGAZIONE È COSÌ IMPORTANTE

La mitigazione è il punto da cui le aziende devono partire, poiché la prevenzione è notevolmente più efficace ed economicamente conveniente della correzione dopo un attacco.

I cybercriminali che sviluppano APT sono estremamente esperti, determinati e dotati di numerose risorse. Tuttavia, come tutti i cybercriminali, con alcune considerevoli eccezioni, trovano ancora maggiormente attraente la strada più semplice. Di conseguenza, anche se non è possibile garantire l'immunità dalle APT, esistono misure da adottare che renderanno più difficile il successo di un attacco.

Così come le APT sono spesso minacce multilivello, una risposta efficace deve essere altrettanto multilivello. I semplici strumenti di sicurezza non bastano.

Com'è quindi questo approccio? L'Australian Signals Directorate ha sviluppato quello che Kaspersky Lab considera un elenco ampio e approfondito di strategie per mitigare le minacce avanzate. Riteniamo che queste strategie siano applicabili anche alle aziende e che rappresentino un valido punto di partenza.

Queste strategie sono suddivise in quattro categorie principali:

1 CRITERI DI SICUREZZA E FORMAZIONE

La sicurezza IT non riguarda solo l'IT. L'errore umano rappresenta un grande aiuto ai cybercriminali. Offrendo una formazione completa e regolare sui problemi di sicurezza, incoraggiando comportamenti corretti e implementando criteri pertinenti e realistici, è possibile ridurre la possibilità che i dipendenti consentano l'ingresso delle minacce informatiche nell'organizzazione.

2 SICUREZZA DELLA RETE

La struttura della rete può aiutare notevolmente a ridurre l'impatto potenziale di un'infezione. Esistono varie strategie di sicurezza di rete in grado di ridurre i rischi e mitigare le minacce. Ad esempio, separando determinate sezioni della rete, è possibile ridurre il numero di endpoint a cui è consentito accedere ai dati sensibili, riducendo in modo esponenziale il livello di rischio.

3 AMMINISTRAZIONE DEL SISTEMA

Il controllo e senza dubbio la limitazione dei privilegi di amministrazione degli utenti tramite criteri di sicurezza possono ridurre notevolmente il numero di vulnerabilità da gestire. Inoltre, l'uso delle funzionalità di sicurezza integrate nei software di protezione determina un'enorme differenza. La disattivazione di funzionalità non necessarie consente di utilizzare al massimo il software e contemporaneamente chiudere strade che potrebbero potenzialmente essere sfruttate.

La disattivazione dell'esecuzione del codice Java nel browser è un ottimo esempio di come sia possibile eliminare vulnerabilità dalle risorse utilizzate dai dipendenti.

4 SOLUZIONI DI SICUREZZA SPECIFICHE

Oltre a queste misure, le funzionalità specifiche di software specifici possono aggiungere livelli di protezione incomparabili. Le soluzioni da integrare non devono tuttavia comportare elevati livelli di investimento o centinaia di ore-uomo. Di fatto, le tre soluzioni di sicurezza specializzate riportate di seguito, insieme alla limitazione dei diritti di amministrazione (vedere la precedente strategia Amministrazione di sistema), consentono una mitigazione dell'85% delle minacce alla sicurezza. Le tre principali soluzioni di sicurezza specializzate sono:

- Utilizzo di funzionalità di controllo delle applicazioni, whitelisting e modalità default deny
- Applicazione di patch alle applicazioni attaccate più comunemente
- Applicazione di patch alle vulnerabilità presenti nei sistemi operativi

PRINCIPALI STRATEGIE DI MITIGAZIONE

Esistono alcune principali strategie di mitigazione che ogni azienda dovrebbe già aver messo in atto o almeno preso in considerazione.

CONTROLLO DELLE APPLICAZIONI E WHITELISTING DINAMICO

Il whitelisting è un potente strumento in grado di mitigare notevolmente le APT e altri attacchi. Anziché verificare se un'applicazione può essere dannosa, il whitelisting consente di verificare con certezza la sua attendibilità. Il controllo è quindi nelle mani dell'amministratore, indipendentemente dal comportamento degli utenti. Una volta creata una whitelist delle applicazioni conosciute e attendibili, saranno consentite solo le applicazioni contenute in tale lista. Il malware si manifesta spesso sotto forma di un file eseguibile di un certo tipo, che con questo approccio verrà bloccato e prevenuto. È l'opposto dell'approccio delle tradizionali "blacklist" antivirus, che impediscono l'avvio di un'applicazione se contenuta in una lista di "responsabili di attacchi conosciuti".

Per elevare al massimo le sicurezza, gli amministratori possono configurare uno scenario "default deny", in cui verranno eseguite solo le applicazioni precedentemente approvate dagli amministratori, limitando notevolmente l'esposizione ai rischi. Sebbene sia un modo efficace per mantenere il malware all'esterno della rete, è necessario assicurarsi di non bloccare gli strumenti che i colleghi hanno realmente bisogno di utilizzare per lavorare in modo efficiente. L'impiego di un controllo delle applicazioni più granulare, insieme al whitelisting dinamico, consente di avere a disposizione più strumenti di controllo. È possibile bloccare o controllare l'utilizzo delle applicazioni per categoria di software, unità operativa, singolo utente e altri fattori.

Prima di poter utilizzare efficacemente il whitelisting, è ovviamente necessario sapere quali applicazioni sono già in esecuzione sui propri computer. È pertanto fondamentale eseguire un inventario. Dopo tutto, non è possibile monitorare qualcosa se non si sa che esiste.

FUNZIONALITÀ DI KASPERSKY LAB: APPLICATION CONTROL CON WHITELISTING DINAMICO

Il database di whitelisting dinamico di Kaspersky Lab contiene oltre 1 miliardo di applicazioni attendibili e include il 97,5% di tutto il software correlato al settore aziendale. La nostra costante intelligence sulle minacce informatiche ne consente l'aggiornamento costante dalla Kaspersky Security Network tramite il cloud.

Il controllo delle applicazioni fornito va al di là della semplice funzionalità di "arresto/avvio". Quando un'applicazione non ha bisogno di essere bloccata, a tutti i componenti non modificati del sistema operativo viene consentito di operare normalmente. Ciò significa la possibilità di arrestare gli attacchi senza interrompere le attività degli utenti. Kaspersky Lab consente inoltre di implementare con maggior facilità una modalità default deny, poiché fornisce una modalità di test che aiuta a determinare in anticipo se ci saranno complicazioni nel momento in cui diventerà attiva.

FUNZIONALITÀ DI KASPERSKY LAB: VALUTAZIONE DELLE VULNERABILITÀ E GESTIONE DELLE PATCH

Il database utilizzato dalla nostra tecnologia per eseguire la scansione alla ricerca delle vulnerabilità è molto vasto: Kaspersky Endpoint Protection for Business rileverà e installerà automaticamente gli aggiornamenti Microsoft, nonché gli aggiornamenti per le applicazioni non Microsoft. In questo modo è possibile mantenere aggiornate tutte le applicazioni e i sistemi operativi, senza dover dedicare preziose ore-uomo a questa attività.

"Nella modalità default deny, è consentita sul computer solo l'esecuzione dei programmi attendibili e posso dire che la maggior parte del malware utilizzato negli attacchi APT proviene da applicazioni non attendibili o prive di patch".

Costin Raiu, Direttore del Team Ricerca Globale e Analisi di Kaspersky Lab.

APPLICAZIONE DI PATCH ALLE VULNERABILITÀ DELLE APPLICAZIONI E DEI SISTEMI OPERATIVI

Sia le applicazioni che i sistemi operativi contengono vulnerabilità che possono essere sfruttate dai criminali. È importante avere il controllo di queste falle della sicurezza e chiuderle prima che possa essere introdotto codice dannoso. Sono le applicazioni più diffuse quelle che spesso contengono vulnerabilità se lasciate prive di patch.

Gli strumenti di gestione delle patch sono cruciali per la sicurezza IT multilivello, poiché possono automatizzare l'attività di aggiornamento delle applicazioni su molti endpoint. In questo modo sarà possibile garantire che i possibili punti di ingresso di un attacco vengano chiusi il più rapidamente possibile.

Occorre nuovamente sottolineare che non esiste un modo infallibile per proteggersi dalle APT.

Tuttavia, se correttamente implementata, una combinazione di tutte queste quattro strategie (privilegi di amministrazione, controllo delle applicazioni, gestione delle patch e gestione dei sistemi operativi) può proteggere dall'85% degli incidenti correlati ad attacchi mirati. Insieme, tali strategie rendono più difficile l'esecuzione di codice dannoso o la possibilità che sfugga al rilevamento, in quanto attivano più linee di difesa.

Nel 2014 le vulnerabilità presenti in Oracle Java, nei browser più diffusi e in Adobe hanno determinato il 92% degli exploit di malware.[2]

[2] Kaspersky Security Bulletin 2014, Kaspersky Lab

ALTRE STRATEGIE ALTAMENTE EFFICACI

Come affermato all'inizio di questo documento, la cybersicurezza non è un gioco di numeri. Anche se ci si può proteggere dalla maggior parte delle intrusioni utilizzando le principali strategie di mitigazione finora esaminate, è comunque necessario andare oltre.

Di seguito sono riportate alcune tecniche aggiuntive che possono essere utilizzate per aggiungere ulteriori livelli di difesa.

MITIGAZIONE DEGLI EXPLOIT NEI SISTEMI OPERATIVI

Anche se le tecnologie native possono essere di grande aiuto per mitigare gli exploit generici nei sistemi operativi, le soluzioni specializzate possono contribuire ad aumentare ulteriormente la difesa. E c'è un motivo molto valido per farlo. Ad esempio, anche se si applicano costantemente le patch alle applicazioni e ai sistemi operativi, si è sempre potenzialmente esposti a un attacco che utilizza una vulnerabilità zero-day.

FUNZIONALITÀ DI KASPERSKY LAB: PREVENZIONE AUTOMATICA DEGLI EXPLOIT (AEP)

Con una particolare attenzione rivolta ai programmi mirati con maggiore frequenza come Internet Explorer, Microsoft Office e Adobe Reader, la tecnologia AEP esegue una serie di controlli di sicurezza. Monitorando continuamente i processi in memoria, è in grado di distinguere gli schemi di comportamento sospetto caratteristici degli exploit, che sono di numero molto più limitato rispetto agli exploit stessi. Questo approccio consente alla tecnologia AEP di Kaspersky Lab di arrestare persino gli exploit zero-day.[3]

[3] In base a un test indipendente condotto da MRG Effitas, la tecnologia AEP è riuscita a proteggere gli endpoint dagli attacchi basati su exploit nel 95% dei test con tutti gli altri meccanismi difensivi disattivati.

Ecco perché è importante disporre di una soluzione che individui e neutralizzi le minacce conosciute, ma anche che rilevi anomalie e comportamenti sospetti, proteggendo di conseguenza l'azienda dalle minacce sconosciute. In questo modo è possibile difendersi persino da attacchi che non sono mai stati osservati prima.

PREVENZIONE DELLE INTRUSIONI BASATA SU HOST

Come è stato dimostrato, le APT sono malware occulto e possono rimanere nascoste per mesi, se non per anni. Disporre quindi di una difesa perimetrale non basta. Cosa accadrebbe se il codice dannoso si è già annidato latente all'interno dell'organizzazione? Quel che occorre è una tecnologia in grado di riconoscere e prevenire le attività dei programmi che sono "troppo rischiose", anche se non sono con certezza dannose. I sistemi di prevenzione delle intrusioni basata su host (HIPS) limitano le attività delle applicazioni all'interno del sistema in base al loro livello di attendibilità. Il sistema HIPS individua le "esecuzioni anomale", ovvero le applicazioni che eseguono funzioni o attività che sono fuori contesto e che suggeriscono la presenza di rischi. È preferibile che questa attività sia eseguita immediatamente dopo l'installazione delle applicazioni, prima che abbiano la possibilità di essere danneggiate da un attacco di malware nascosto.

FUNZIONALITÀ DI KASPERSKY LAB: SYSTEM WATCHER E APPLICATION PRIVILEGE CONTROL

Con queste due funzionalità, è possibile monitorare e registrare gli eventi che si verificano all'interno dei sistemi informatici, garantendo che le applicazioni non tentino di eseguire azioni dannose. System Watcher con il proprio sistema di roolback è in grado di ripristinare modifiche impreviste, mentre Privilege Control previene il verificarsi di cambiamenti se questi sono attuati da applicazioni che hanno una basso livello di affidabilità.

ANALISI DINAMICA DEI CONTENUTI DI EMAIL E PAGINE WEB

Così come un approccio basato su firme non è in grado di contrastare gli attacchi zero-day, l'utilizzo della tradizionale "analisi statica" per mettere a confronto il contenuto di email e pagine Web con un database di malware conosciuto non può proteggere dalle nuove minacce.

Ecco perché l'analisi dinamica è così importante. Occorre una soluzione in grado di ricercare le caratteristiche sospette codificate nelle pagine Web e nelle email, che tentano ad esempio di trovare e modificare programmi eseguibili, e di bloccarle prima che vengano aperte.

Un attacco "zero-day" è un attacco che ha come obiettivo una vulnerabilità precedentemente non riconosciuta presente in un sistema operativo o in un'applicazione, prima che sia disponibile una patch.

FUNZIONALITÀ DI KASPERSKY LAB: WEB CONTROL E WEB ANTI-VIRUS

La nostra tecnologia Web Control consente di decidere se consentire agli utenti l'accesso ai siti, sia su base individuale che in base alla classificazione del tipo di sito Web (ad esempio sito di gioco d'azzardo e così via). Attraverso il monitoraggio del traffico HTTP(S), è possibile garantire che le risorse Web a cui accedono gli endpoint corrispondano alla propria whitelist.

Al contempo, Web Anti-virus utilizza l'analisi dinamica per individuare la presenza di codice dannoso introdotto dai protocolli HTTP(S) e FTP, proteggendo dalle APT che utilizzano i download o infezioni drive-by per penetrare in un sistema.

FUNZIONALITÀ DI KASPERSKY LAB: MAIL ANTIVIRUS E SECURITY PER SERVER DI POSTA

Tramite una combinazione di analisi statica, dinamica ed euristica, Kaspersky Endpoint for Business aiuta a bloccare le minacce trasmesse via email. Emulando il modo in cui gli allegati potrebbero comportarsi, la nostra tecnologia è in grado di rilevare la presenza di exploit basati su file negli allegati email.

Kaspersky Security per Server di Posta, con l'opzione di prevenzione della perdita dei dati (DLP), può inoltre bloccare la fuoriuscita di informazioni importanti. Rendendo i file "non condivisibili", è possibile garantire che non escano dall'azienda tramite gli allegati email.

L'APPROCCIO DI KASPERSKY LAB: PROTEZIONE MULTILIVELLO

Il panorama delle minacce alla sicurezza è complesso e in rapida evoluzione. In Kaspersky Lab, collaboriamo con grandi organizzazioni a una strategia multilivello, dalla mitigazione fino ai servizi di intelligence sulle minacce informatiche.

In quanto azienda basata sulle tecnologie, abbiamo sviluppato gli strumenti necessari per una strategia di mitigazione completa. Essendo creati a partire dalla stessa base di codice, tali strumenti sono perfettamente integrati e consentono quindi di formulare una strategia di sicurezza completa senza lasciare falle scoperte nella difesa.

Al centro di questo approccio è la nostra pluripremiata tecnologia antimalware e il nostro firewall per gli endpoint. Insieme, bloccano le minacce **conosciute** al 70%. Attraverso strumenti più **avanzati**, quali analisi comportamentale, euristica, controllo delle applicazioni con whitelisting dinamico e controllo Web, proteggiamo dalle minacce **sconosciute**. Inoltre, per le minacce avanzate, aggiungiamo un altro livello di protezione di supporto, mediante strumenti avanzati quali Kaspersky Automatic Exploit Prevention e System Watcher.

INTELLIGENCE E RILEVAMENTO PER IDENTIFICARE GLI ATTACCHI "IN TEMPO REALE"... RAPIDAMENTE

Anche se un approccio completo alla mitigazione è di fondamentale importanza, la strategia di contrasto alle APT deve includere anche misure che garantiscano la possibilità di rilevare un attacco "dal vivo", senza causare falsi allarmi, che sono dispendiosi in termini di tempo. Inoltre, la strategia deve includere tecnologie in grado di bloccare rapidamente un attacco e di ridurre al minimo i danni causati alla propria attività.

L'approccio da noi consigliato prevede il rilevamento a livello di endpoint, il rilevamento a livello di rete, il sandboxing intelligente e un database completo degli eventi.

Ultimamente, il rilevamento a livello di rete ha catturato l'attenzione di vari fornitori IT e molti di essi hanno introdotto appliance dedicate alla protezione della rete. Tuttavia, riteniamo che una soluzione alternativa che utilizzi un'architettura a sensori distribuiti possa offrire notevoli vantaggi. Posizionando i sensori sui punti chiave della rete, che forniscono i dati a un punto centrale, tale soluzione può contribuire a migliorare il rilevamento. Inoltre, può consentire una maggiore scalabilità e aiuta a ridurre i costi nei casi in cui sia necessario proteggere reti di livello enterprise complesse.

OLTRE LA TECNOLOGIA: SERVIZI DI INTELLIGENCE SULLE MINACCE INFORMATICHE

Anche se la mitigazione riduce enormemente i rischi di qualsiasi organizzazione, è impossibile che una soluzione di sicurezza garantisca una protezione al 100%.

Se un attacco riesce, l'azienda dovrà determinare:

- Esattamente quali dati sono stati sottratti, in modo da poter intraprendere azioni volte a limitare i danni causati dalla perdita
- In che modo è stato realizzato l'attacco, in modo da poter risolvere le vulnerabilità e le falle di sicurezza specifiche

Ecco perché è importante disporre dei migliori strumenti di analisi forense, pronti a fornire un rapido accesso alle competenze necessarie nel campo della sicurezza.

Kaspersky Lab offre una serie di servizi di intelligence, tra cui è possibile scegliere il livello più adatto alla propria attività:

- Analisi del malware, per i clienti che dispongono di un proprio team interno di analisi forense
- Servizi di analisi forense digitale, inclusa l'analisi del malware
- Servizi completi di risposta agli incidenti, inclusa l'analisi forense

PERCHÉ KASPERSKY LAB

Kaspersky Lab è una delle organizzazioni all'avanguardia nella lotta alle APT. Il nostro team di ricerca globale e analisi (GReAT, Global Research and Analysis Team) è stato coinvolto nella scoperta di molte delle minacce più pericolose e complesse del mondo, da Red October fino al cosiddetto "Equation Group" di strumenti di cyberspionaggio, da poco scoperto.

Sfortunatamente per i cybercriminali, la scalabilità non è un grande problema. Una volta sviluppate armi informatiche avanzate, i gruppi non impiegano molto a riutilizzarle per colpire bersagli aziendali. Di conseguenza, anche le armi segretamente sviluppate a costi elevati dagli stati nazionali possono finire nelle mani di organizzazioni criminali.

Ne prendiamo atto. Per questo motivo ci stiamo muovendo per competere ad armi pari. Utilizziamo l'intelligence raccolta dalle attività di indagine sulle APT per consigliare ai governi come difendersi dai cyberattacchi. Ma non ci fermiamo lì. Utilizziamo tutto quanto apprendiamo da questo lavoro per creare soluzioni efficaci e pratiche a livello aziendale.

A questo scopo, uniamo la nostra ineguagliabile intelligence sulla sicurezza all'innovazione tecnologica. La percentuale del nostro personale che lavora nel campo della ricerca e dello sviluppo è notevolmente più elevata rispetto ai concorrenti.

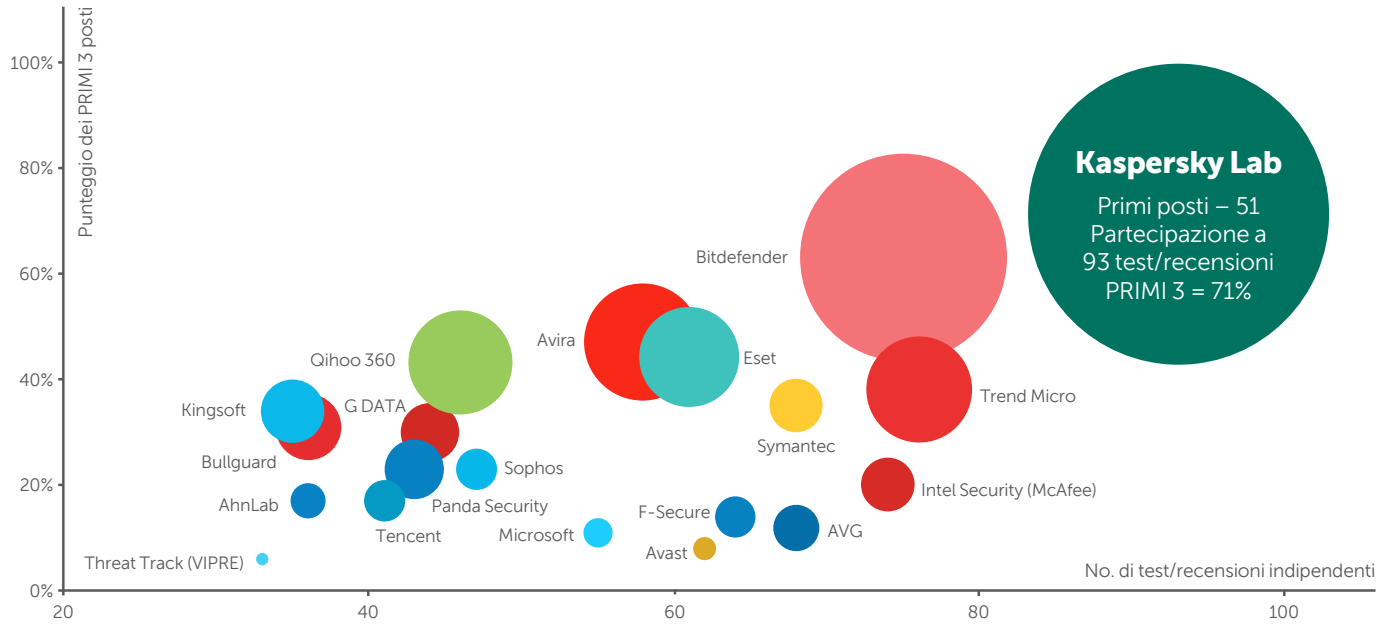
Il risultato è un approccio multilivello alla sicurezza aziendale, in grado di contribuire a formare la colonna portante per ogni azienda che intenda creare una strategia di mitigazione di contrasto alle APT.

La nostra fiducia in queste soluzioni ci ha portato a partecipare a più test indipendenti rispetto a qualsiasi altro fornitore. Abbiamo ottenuto livelli di rilevamento del malware di oltre il 99% e, nei 93 test indipendenti a cui abbiamo preso parte nel 2014, ci siamo classificati nei primi tre posti in 66 di essi e primi in 51[4], risultati a cui nessuno dei concorrenti si è avvicinato. La tecnologia di Kaspersky Lab viene inoltre utilizzata e ritenuta attendibile da oltre 130 partner OEM, per cui è possibile che la vostra azienda stia già utilizzando attualmente Kaspersky Lab.

[4] http://media.kaspersky.com/en/business-security/TOP3_2014.pdf

KASPERSKY LAB: LA MIGLIORE PROTEZIONE DEL SETTORE*

Nel 2014 i prodotti Kaspersky Lab hanno partecipato a 93 test e recensioni indipendenti. I nostri prodotti hanno vinto 51 primi premi e per 66 volte sono rientrati nei primi tre posti.



* 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.

PROTEZIONE PRESENTE E SICUREZZA FUTURA

Un panorama di minacce sempre più sofisticate e complesse impone una piattaforma di sicurezza multilivello che difenda dalle minacce conosciute, sconosciute e avanzate.

Per ulteriori informazioni sulle competenze esclusive e le soluzioni di sicurezza per le aziende di Kaspersky Lab, visitare **kaspersky.it/enterprise**

PER SAPERNE DI PIÙ

PARTECIPA ALLA CONVERSAZIONE

#EnterpriseSec

Guardateci su YouTube

Visitate la nostra pagina Facebook

Seguici su Twitter

Collegatevi su LinkedIn

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 sono disponibili sul sito Web www.kaspersky.it.

* 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.