KASPERSKY lab

O PODER DA PROTEÇÃO

FUTUROS RISCOS: PREPARE-SE

Relatório especial sobre estratégias de atenuação para ameaças avançadas

kaspersky.com/enterprise
#EnterpriseSec

CONTEÚDO

AMEAÇAS PERSISTENTES AVANÇADAS E O CENÁRIO DE AMEAÇA

A segurança virtual não é um jogo de números. Quando precisa apenas de uma simples brecha para causar sérios danos em sua empresa, a defesa contra a maioria dos ataques não é suficiente.

É por isso que é melhor voltar nossa atenção para as ameaças mais perigosas que enfrentamos, não apenas para as que conhecemos.

O 'ecossistema' de malware é categorizado em ameaças **conhecidas** (70%), **desconhecidas** (29%) e **avançadas** (1%).

As ameaças conhecidas, que somam cerca de 70% de malware, são relativamente fáceis de combater. Contanto que consigamos reconhecer o código malicioso, podemos bloqueá-lo: os métodos tradicionais com base em assinatura costumam lidar com isso.

29% do malware aparece na forma de banner de 'ameaças desconhecidas'. Combatê-las requer ferramentas mais sofisticadas. Mas ao usar métodos que vão além de softwares antivírus comuns – como listas brancas heurísticas e dinâmicas – conseguimos combatê-las também.

E então sobra 1%. As ameaças avançadas são ataques multifacetados, contínuos e direcionados. Feitas para penetrar uma rede, espreitar o que não foi visto e coletar dados sigilosos, quando instaladas, podem permanecer não detectadas por anos.

Uma APT conhecida como 'Darkhotel' usou o Wi-Fi de hotéis de luxo para roubar dados dos hóspedes por sete anos antes de ser descoberta. Essa foi uma APT particularmente interessante, pois era altamente direcionada (foco nos executivos seniores e CEOs) e ilustrava muito nitidamente o desafio da segurança quando endpoints (laptops e tablets da empresa) deixavam a segurança da rede da empresa.

Uma APT conhecida como 'Darkhotel' usou o Wi-Fi de hotéis de luxo para roubar dados dos hóspedes por sete anos antes de ser descoberta.

Embora algumas organizações de alto perfil tenham se tornado vítimas das APTs, você não precisa estar nos olhos públicos para ser alvo de criminosos virtuais. As empresas devem conseguir atenuar o risco apresentado pelas APTs e as consequências que um ataque pode acarretar – seja perda de dados, tempo de inatividade extensivo ou sérios danos à reputação. E com as APTs operando silenciosa e secretamente, a prevenção é muito menos dispendiosa do que a neutralização pós-ataque (já que o ataque pode ter acontecido antes e causado estragos desconhecidos há meses ou até anos).

Não há solução para esse problema. Embora úteis, as tecnologias que usamos para combater ameaças conhecidas e desconhecidas não são adequadas para combater APTs. Um cenário de ameaças cada vez mais completo e sofisticado pede uma abordagem de segurança em várias camadas, em que a combinação de tecnologias integradas forneça detecção e proteção abrangentes contra malware conhecido, desconhecido, avançado e outras ameaças.

Este relatório foi elaborado para ajudá-lo a se preparar para combater APTs.

O custo médio de um incidente de malware é US$ 56.000 para uma SMB e US$ 649.000 para uma grande empresa.[1]

As APTs podem trazer consequências gigantescas. Durante 2014, a Kaspersky Lab ajudou a desvendar o funcionamento do Carbanak. Esse complexo ataque possibilitou que um grupo internacional de criminosos roubasse US$ 1 bilhão de uma rede de instituições financeiras. Depois de infectar uma rede do banco, o grupo conseguiu gravar tudo o que acontecia nas telas dos funcionários e saber como transferir dinheiro sem ser detectado.

[1] O alto custo de uma violação de segurança, Kaspersky Lab.

A EMPRESA É UM ALVO - 5 PONTOS PRINCIPAIS

Como uma grande empresa, você conhece as ameaças de segurança que o assolam. Essas ameaças só se tornam mais direcionadas e sofisticadas.

1 A primeira etapa para criar uma estratégia apropriada para tratar APTs é entender que você é um alvo em potencial. A verdade é que – seja propriedade intelectual, detalhes de contato ou informações financeiras – sua organização retém informações que podem ser vantajosas para os criminosos. Mesmo que não sejam seus dados que eles estejam procurando, eles podem usar sua rede como porta para chegar até seus clientes ou parceiros (como no caso do Darkhotel).

2 Em segundo lugar, precisamos desenvolver uma conscientização melhor sobre vulnerabilidade. Nas organizações em que diversos funcionários trabalham com diversos dispositivos, aplicativos e plataformas, pode ser difícil supervisionar todos os riscos e 'vetores de ataque' possíveis que existem para os criminosos virtuais explorarem. As APTs são direcionadas a vulnerabilidades, humanas ou técnicas – portanto, quanto maior e mais complexa uma organização, mais pontos de entrada em potencial existem.

3 O aumento da iniciativa BYOD (Traga seu próprio dispositivo) e do trabalho flexível só agrega mais desafios. Assim como estar vulnerável a seu próprio direito, telefones e tablets costumam ser usados para estabelecer conexão com redes desprotegidas. Para piorar, é mais difícil – especialmente com sistemas operacionais como o iOS da Apple – saber se um dispositivo está infectado. Uma equipe de trabalho móvel é como um alvo em movimento; os dispositivos que operam fora da segurança de seu perímetro são mais difíceis de policiar, tornando a segurança eficiente de endpoints um componente significativo de sua estratégia de segurança.

4 Essa ampla variedade de endpoints, aliada aos tantos métodos que os criminosos virtuais podem usar para infectar uma rede, significa que as medidas de segurança semelhantes não são suficientes. Em vez disso, medidas robustas de atenuação precisam combinar inteligência de ameaças, políticas de segurança e tecnologias especializadas que não apenas bloqueiem as ameaças iminentes reconhecidas, mas identifiquem as novas – enquanto usam medidas como listas brancas para impedir ameaças ainda desconhecidas de executar.

5 A atenuação precisa de um foco renovado no endpoint. Os criminosos virtuais exploram vulnerabilidades – e a empresa costuma estar em seu momento de fraqueza no endpoint: quando a segurança é comprometida não só pelo dispositivo em si, mas pelo comportamento negligente do funcionário, ou as imediações desprotegidas onde ele está sendo usado. Se seus endpoints não tiverem proteção em vários níveis, toda a organização pode estar em risco.

POR QUE A ATENUAÇÃO É TÃO IMPORTANTE

A atenuação é por onde as empresas precisam começar. A prevenção é muito mais eficiente e econômica do que uma neutralização pós-ataque.

Os agentes de ameaças que desenvolvem as APTs são altamente especializados, determinados e equipados. No entanto, assim como todos os criminosos virtuais – salvo algumas exceções – eles ainda encontram o caminho do menor atrativo à resistência. Por isso, embora você não consiga garantir a imunidade às APTs, existem medidas a implementar para dificultar a ocorrência de um ataque.

Assim como as APTs costumam ser ameaças em vários níveis por si sós, uma resposta de APT eficiente precisa ser em vários níveis. Ferramentas de segurança simples não são o bastante.

Então como é essa abordagem? O Australian Signals Directorate desenvolveu o que a Kaspersky Lab considera uma lista estendida e completa de estratégias para atenuar ameaças avançadas. Acreditamos que essas estratégias sejam aplicáveis às empresas, sendo ainda um bom ponto de partida.

Essas estratégias são detalhadas em quatro categorias principais:

1 POLÍTICAS DE SEGURANÇA E EDUCAÇÃO

Segurança não envolve apenas TI. O erro humano é um grande colaborador para os criminosos virtuais. Ao oferecer uma educação abrangente e regular sobre os problemas de segurança, estimular os comportamentos corretos e implementar políticas realistas e relevantes, você consegue reduzir a chance de os funcionários carregarem ameaças virtuais para dentro da organização.

2 SEGURANÇA DE REDE

A estrutura de sua rede pode ajudar bastante a reduzir o possível impacto de uma infecção. Existem várias estratégias de segurança de rede capazes de reduzir riscos e atenuar ameaças, como, por exemplo: segregar certas partes da rede significa que você pode reduzir o número de endpoints que acessam dados sigilosos, diminuindo exponencialmente seu nível de risco.

3 ADMINISTRAÇÃO DO SISTEMA

Controlar e realmente restringir os privilégios de administração do usuário por meio de políticas de segurança pode reduzir significativamente o número de vulnerabilidades com que você lida. Acima disso, aproveitar os recursos de segurança integrados em programas que você usa faz uma grande diferença. Desabilitar recursos indesejados significa que você pode aproveitar melhor o software enquanto interdita vias que podem ser exploradas.

Desativar a execução do código Java em seu navegador é um bom exemplo de como eliminar vulnerabilidades dos recursos que seus funcionários usam.

4 SOLUÇÕES DE SEGURANÇA ESPECIALIZADAS

Além dessas etapas, recursos específicos de softwares especializados podem agregar camadas valiosas de proteção. No entanto, fazer as soluções se integrarem não precisa envolver muitos níveis de investimento ou centenas de horas trabalhadas. Na verdade, as três soluções de segurança especializadas a seguir, com os direitos de administração restritivos (consulte a estratégia de Administração do sistema, acima) atenuam 85% das ameaças de segurança. As três principais soluções de segurança especializadas são:

- Usar controle de aplicativos, listas brancas e modo de negação padrão
- Corrigir a maioria dos aplicativos mais atacados
- Corrigir vulnerabilidades em seus sistemas operacionais

PRINCIPAIS ESTRATÉGIAS DE ATENUAÇÃO

Existem diversas estratégias de atenuação que toda empresa já deveria ter ou pelo menos pensar em ter.

CONTROLE DE APLICATIVOS E LISTAS BRANCAS

Listas brancas é uma poderosa ferramenta capaz de atenuar APTs e outros ataques. Em vez de questionar se um aplicativo é prejudicial, as listas brancas perguntam se temos certeza de sua legitimidade. Isso coloca o controle nas mãos no administrador, seja qual for o comportamento do usuário. Uma lista branca é criada de aplicativos conhecidos e confiáveis – e apenas aplicativos que estejam na lista são permitidos.
O malware costuma se manifestar como um arquivo executável de algum tipo – que é bloqueado e impedido de usar essa abordagem. Essa é a abordagem oposta das tradicionais 'listas negras' de antivírus, que apenas impedem que um aplicativo abra se aparecer em uma lista de 'ofensores conhecidos'.

Levados ao extremo mais seguro, os administradores podem configurar um cenário de 'negação padrão', em que apenas aplicativos pré-aprovados por administradores podem ser executados: o que limita massivamente a exposição. Embora esta seja uma forma eficiente de manter o malware fora da rede, você precisa ver se não está bloqueando ferramentas que seus colegas realmente precisam usar no trabalho. Usar um controle de aplicativos mais granular, com listas brancas dinâmicas, propicia mais ferramentas de controle à sua disposição. Você pode bloquear ou controlar o uso de aplicativos por categoria de software, unidade de negócios, usuário individual e outros fatores.

É claro que, antes de usar listas brancas eficientemente, você precisa saber quais aplicativos já estão em execução em suas máquinas. Por isso é vital fazer um inventário. Afinal de contas, você não pode monitorar algo que não consegue ver.

RECURSO DA KASPERSKY LAB: CONTROLE DE APLICATIVOS COM LISTA BRANCA DINÂMICA

O banco de dados de listas brancas dinâmicas da Kaspersky Lab com aplicativos legítimos já conta com mais de 1 bilhão de entradas, incluindo 97,5% de todos os softwares relacionados ao setor corporativo. Nossa inteligência de ameaças contínua é constantemente atualizada via nuvem pela Kaspersky Security Network.

Nosso controle de aplicativos vai além da funcionalidade de 'parar/iniciar'. Quando um aplicativo não precisa ser bloqueado, permitimos que todos os componentes não modificados do sistema operacional sejam executados normalmente. Isso quer dizer que você pode parar ataques sem interromper as atividades de seus usuários. A Kaspersky Lab também torna muito mais fácil implementar um modo de negação padrão conforme fornecemos um modo de teste para ajudá-lo a ver antecipadamente se haverá complicações no 'lançamento'.

RECURSOS DA KASPERSKY LAB: VERIFICAÇÃO DE VULNERABILIDADES E GERENCIAMENTO DE CORREÇÕES

O banco de dados que nossa tecnologia usa para verificar vulnerabilidades é extensivo: o Kaspersky Endpoint Protection for Business automaticamente encontra e instala atualizações da Microsoft, além de atualizações (renovações) de aplicativos não Microsoft. Isso significa que você pode manter todos os seus aplicativos e sistemas operacionais atualizados, sem dedicar mais horas de trabalho à tarefa.

"No modo de negação padrão, somente programas confiáveis podem ser executados em seu computador, e eu posso dizer que a maioria do malware usado nos ataques de APT vem de aplicativos não confiáveis ou não corrigidos".

Costin Raiu, Diretor da equipe do Global Research and Analysis Team da Kaspersky Lab.

APLICATIVOS DE CORREÇÕES E VULNERABILIDADES NO SISTEMA OPERACIONAL

Tanto os aplicativos como os sistemas operacionais contêm vulnerabilidades que podem ser exploradas pelos criminosos. É importante estar ciente dessas brechas de segurança e fechá-las antes que o código malicioso seja introduzido. E são os aplicativos populares que contêm vulnerabilidades quando deixados sem correção.

As ferramentas de gerenciamento de correções são importantes para a segurança de vários níveis, já que conseguem automatizar a tarefa de manter os aplicativos atualizados em diversos endpoints. Como resultado, você garante que possíveis pontos de entrada de um ataque sejam fechados o quanto antes.

Mais uma vez, é necessário enfatizar que não existe uma forma simplória de proteger você contra APTs.

Mas, quando corretamente implementada, uma combinação dessas quatro estratégias (privilégios de administração, controle de aplicativos, gerenciamento de correções e gerenciamento do sistema operacional) pode proteger contra 85% dos incidentes relacionados a ataques direcionados. Juntas, elas dificultam para o código malicioso executar ou permanecer não detectado. Isso porque elas habilitam diversas linhas de defesa.

Em 2014, vulnerabilidades no Oracle Java, navegadores conhecidos e no Adobe Reader representaram 92% dos exploits de malware.[2]

[2] Boletim de segurança da Kaspersky de 2014, Kaspersky Lab

OUTRAS ESTRATÉGIAS ALTAMENTE EFICIENTES

Conforme mencionamos no início deste documento, a segurança virtual não é um jogo de números. Embora você consiga se proteger contra a maioria das invasões que usam as principais estratégias de atenuação que analisamos, ainda é necessário ir além.

Seguem aqui algumas técnicas adicionais que você pode usar para adicionar mais camadas de defesa:

ATENUAÇÃO DE EXPLOITS DO SISTEMA OPERACIONAL

Embora as tecnologias nativas façam muito para atenuar exploits genéricos nos sistemas operacionais, soluções especializadas podem ajudar você a fazer ainda mais. E existe um bom motivo para isso. Por exemplo, mesmo que você aplique constantemente as correções em seus aplicativos e sistemas operacionais, ainda estará suscetível a um ataque que usa vulnerabilidade de dia zero.

RECURSO DA KASPERSKY LAB: PREVENÇÃO AUTOMÁTICA CONTRA EXPLOITS (AEP)

Prestando atenção a programas comumente direcionados, como Internet Explorer, Microsoft Office e Adobe Reader, a AEP faz uma série de verificações de segurança. Ao monitorar continuamente os processos na memória, ela consegue discernir padrões de comportamento suspeito característicos dos exploits, que são muito mais limitados em números do que os próprios exploits. Essa abordagem permite que a AEP da Kaspersky Lab pare ainda nos exploits de dia zero.[3]

[3] De acordo com o teste independente da MRG Effitas, a AEP conseguiu proteger endpoints de teste contra ataques com base em exploits em 95% dos testes com todos os outros mecanismos de defesa desativados'

É por isso que é importante ter uma solução que identifica e neutraliza ameaças conhecidas, mas que também detecta anomalias e comportamento suspeito – protegendo-o contra ameaças desconhecidas. Dessa forma você se defende contra ataques que nunca foram vistos antes.

PREVENÇÃO DE INVASÕES COM BASE NO HOST

Como já comprovado, as APTs são um malware silencioso que permanece escondido por meses e até anos. Portanto, ter um perímetro de defesa não é suficiente – e se o código malicioso já tiver penetrado sua organização? É necessário ter uma tecnologia que reconheça e impeça atividades de programas 'muito arriscadas', mesmo que não sejam maliciosas. Os sistemas de Prevenção de invasão com base no host (HIPS) restringem atividades de aplicativos no sistema de acordo com seu nível de confiança. O HIPS identifica 'anomalias de execução' – aplicativos que realizam funções ou atividades que estejam fora de contexto e sugiram risco. Isso é bem feito imediatamente depois que os aplicativos são instalados (ou seja, antes de terem qualquer chance de serem corrompidos por um ataque de malware silencioso).

RECURSO DA KASPERSKY LAB: SYSTEMS WATCHER E APPLICATION PRIVILEGE CONTROL

Entre esses dois recursos, eventos que acontecem em seus sistemas de computadores podem ser monitorados e gravados, garantindo que os aplicativos não tentem realizar ações maliciosas. O Inspetor do sistema e seu subsistema de reversão é capaz de impedir alterações indesejadas, enquanto o Controle de privilégios evita que essas alterações ocorram quando iniciadas por aplicativos com baixo nível de confiança.

ANÁLISE DINÂMICA DO CONTEÚDO DO E-MAIL E DA WEB

Assim como uma abordagem com base em assinatura não é capaz de combater ataques de "dia zero", usar as tradicionais 'análises estáticas' para comparar o conteúdo dos e-mails e páginas da Web com um banco de dados de malware conhecido não garante sua proteção contra novas ameaças.

Por isso a análise dinâmica é tão importante. Você precisa de uma solução que procure características suspeitas codificadas em páginas da Web e e-mails – como tentar encontrar e modificar programas executáveis – e bloqueá-las antes de serem abertas.

Um ataque de 'dia zero' é um dos que direciona uma vulnerabilidade não reconhecida anteriormente em um sistema operacional ou aplicativo, antes de uma correção ser disponibilizada.

RECURSOS DA KASPERSKY LAB: ANTIVÍRUS DA WEB E ANTIVÍRUS DA WEB

Nossa tecnologia de Controle da Web permite a você decidir se deseja permitir que os usuários acessem sites, individualmente ou por uma classificação de tipo de site (por exemplo, sites de jogos de azar, etc). Ao monitorar o tráfego de HTTP(S), você faz a correspondência dos recursos acessados nos endpoints com sua lista branca.

Enquanto isso, nosso antivírus da Web usa a análise dinâmica para identificar código malicioso entregue por protocolos HTTP(S) e FTP, protegendo contra APTs que usam downloads ou infecções conduzidas para penetrar no sistema.

RECURSOS DA KASPERSKY LAB: ANTIVÍRUS E SEGURANÇA PARA O SERVIDOR DE E-MAIL

Usando uma combinação de análises dinâmicas e estáticas e heurística, o Kaspersky Endpoint for Business ajuda a bloquear as ameaças transmitidas por e-mail. Ao emular como os anexos podem se comportar, nossa tecnologia pode detectar exploits com base em arquivos nos anexos de e-mails.

O Kaspersky Security for Mail Server, com sua opção de Prevenção contra perda de dados (DLP), também consegue interromper a saída de informações importantes. Ao processar arquivos 'não compartilháveis', você assegura que eles não saiam da empresa por anexos de e-mail.

A ABORDAGEM DA KASPERSKY LAB: PROTEÇÃO EM VÁRIOS NÍVEIS

O cenário de ameaças à segurança é complexo e crescente. Na Kaspersky Lab, trabalhamos com grandes organizações em uma estratégia de vários níveis – da atenuação aos serviços de inteligência de ameaças.

Como uma empresa orientada por tecnologias, desenvolvemos as ferramentas necessárias para você criar uma estratégia de atenuação ideal. E como elas são criadas a partir da mesma base de código, são continuamente integradas, assim você formula uma estratégia de segurança abrangente sem deixar brechas desnecessárias na estrutura.

No cerne de nossa abordagem está a premiada tecnologia antimalware e firewall de endpoint. Juntos, eles bloqueiam as **ameaças** conhecidas, os 70%. Com as ferramentas mais **avançadas**, como análise comportamental, heurística, controle de aplicativos com listas brancas dinâmicas e controle da Web, garantimos a proteção contra as ameaças **conhecidas**. E para as ameaças avançadas, adicionamos mais uma camada de proteção para ajudar, usando ferramentas avançadas, como a Prevenção Automática contra Exploits da Kaspersky e o Inspetor do sistema.

INTELIGÊNCIA E DETECÇÃO – PARA IDENTIFICAR ATAQUES 'EM TEMPO REAL'... RAPIDAMENTE

Embora uma abordagem completa de atenuação seja vital, sua estratégia contra-APT também deve incluir medidas que assegurem a detecção de um ataque 'em tempo real' – sem causar falsos alarmes que consomem tempo. Além disso, sua estratégia deve incluir tecnologias que bloqueiem rapidamente um ataque e minimizem os danos causados à sua empresa.

Nossa abordagem recomendada inclui detecção de nível do endpoint, detecção do nível de rede, área restrita inteligente e um abrangente banco de dados de eventos.

Recentemente, a detecção de nível de rede capturou a imaginação de diversos fornecedores – e muitos deles introduziram dispositivos exclusivos para detecção de rede. No entanto, acreditamos que uma solução alternativa – que use uma arquitetura de sensor distribuída – possa oferecer vantagens significativas. Ao colocar sensores nos principais pontos na rede – todos alimentando dados em um ponto central – ela ajuda a aprimorar a detecção. Além disso, ela pode permitir mais escalabilidade, ajudando a reduzir custos quando redes complexas e empresariais precisarem ser protegidas.

ALÉM DA TECNOLOGIA: SERVIÇOS DE INTELIGÊNCIA DE AMEAÇAS

Embora a atenuação reduza muito os riscos de qualquer organização, não é possível que uma solução de segurança garanta 100% de proteção.

Se um ataque for bem-sucedido, sua empresa precisará determinar:

- Exatamente quais dados foram roubados – para você tomar uma providência de limitar os danos causados pela perda
- Como o ataque foi habilitado – para você tratar vulnerabilidades específicas e brechas na segurança

Por isso é importante ter o que há de melhor em análise pericial à sua disposição – pronto para fornecer a você acesso rápido à experiência de segurança necessária.

A Kaspersky Lab oferece diversos serviços de inteligência – você pode escolher o nível de serviço ideal para sua empresa:

- Análise de malware – para clientes que contam com uma equipe pericial interna própria
- Serviços de perícia digital – incluindo análise de malware
- Serviços completos de resposta a incidentes – incluindo perícia

POR QUE KASPERSKY LAB

A Kaspersky Lab é uma das organizações que dominam o combate de APTs. Nossa equipe GReAT (Global Research and Analysis Team, Equipe de pesquisas e análises globais) já esteve envolvida na descoberta de muitas das mais complexas e perigosas ameaças do mundo, desde a Red October até a recente não divulgada 'Equation Group' das ferramentas de espionagem virtual.

Infelizmente, para os criminosos virtuais, escala não chega a ser um problema. Quando armas virtuais avançadas são desenvolvidas, não demora muito para que os grupos as redirecionem para alvos empresariais. Isso quer dizer que até mesmo as armas secretamente desenvolvidas a altos custos por estados nacionais podem acabar nas mãos de gangues do crime.

Nós sabemos disso. É por isso que estamos mudando para nivelar o campo de jogo. Usamos a inteligência adquirida de investigações de APTs para orientar os governos sobre como combater ataques virtuais. Mas não paramos aí. Usamos tudo o que aprendemos desse trabalho para criar soluções que sejam eficientes e práticas no nível empresarial.

Para isso, combinamos nossa inteligência de segurança inigualável com a inovação tecnológica. Temos uma proporção consideravelmente maior de pessoas trabalhando em pesquisas e desenvolvimento do que qualquer um de nossos concorrentes.

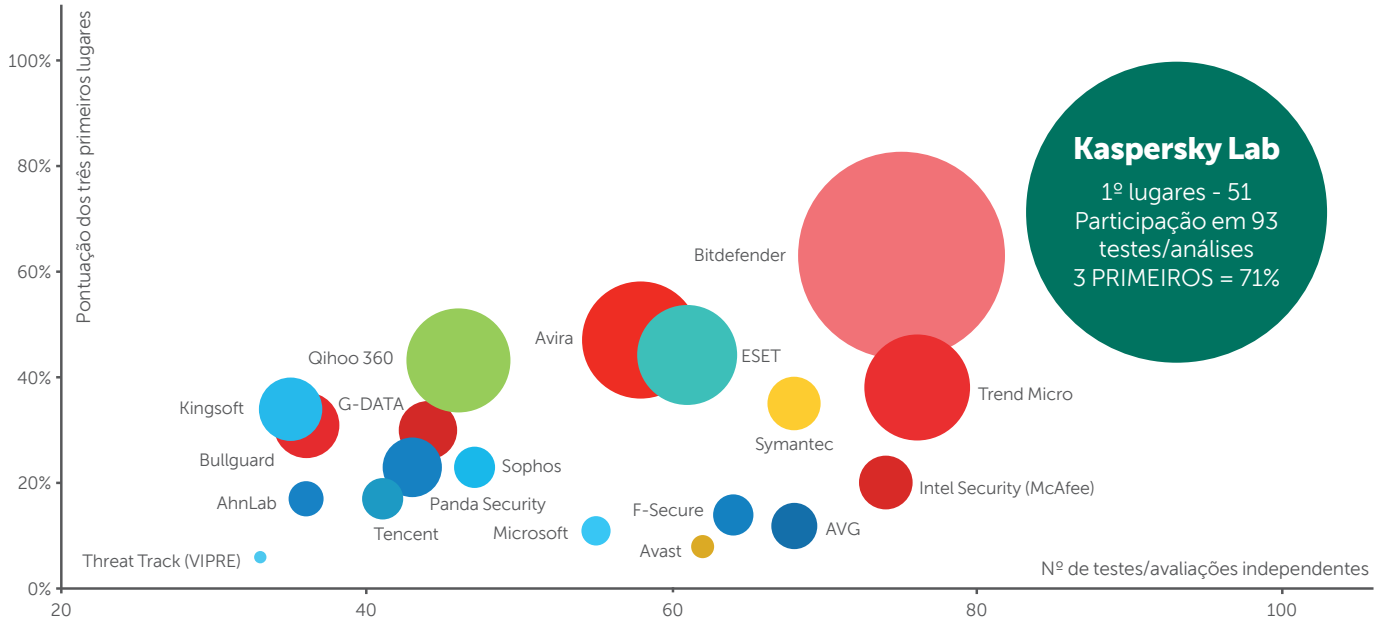
O resultado é uma abordagem de várias camadas da segurança empresarial, que pode ajudar a formar o suporte principal para qualquer empresa que esteja em busca de uma estratégia de atenuação contra-APT.

A confiança que temos em nossas soluções nos levou a participar de mais testes independentes do que outros fornecedores. Atingimos índices de detecção de malware de mais de 99% e, dos 93 testes independentes dos quais participamos em 2014, acabamos entre os três melhores de 66, e entre os primeiros de 51[4] – resultados dos quais nenhum de nossos concorrentes chegou perto. A tecnologia da Kaspersky Lab também é usada e bem aceita por mais de 130 parceiros de OEM – por isso, você também poderia estar usando a Kaspersky Lab hoje.

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

KASPERSKY LAB: A MELHOR PROTEÇÃO DO MERCADO*

Em 2014, os produtos da Kaspersky Lab participaram de 93 testes e análises independentes. Nossos produtos receberam 51 prêmios de primeiro lugar e 66 três melhores acabamentos.



* Notas:
De acordo com o resumo dos resultados dos testes independentes em 2014 de produtos corporativos, para o consumidor e produtos móveis.

O resumo inclui testes conduzidos pelos seguintes laboratórios e revistas de testes independentes:
AV- Comparatives, AV-Test, Dennis Technology Labs, MRG Effitas, NSS Labs, PC Security Labs, VirusBulletin.
O tamanho da bolha reflete a quantidade de primeiros lugares conquistados.

PROTEÇÃO HOJE, SEGURANÇA NO FUTURO

Um cenário de ameaças cada vez mais completo e sofisticado pede uma plataforma de segurança em várias camadas que proteja contra ameaças conhecidas, desconhecidas e avançadas.

Visite **kaspersky.com/enterprise** para obter mais detalhes sobre as Soluções de Segurança Corporativa e sobre a expertise única da Kaspersky Lab.

SAIBA MAIS

PARTICIPE DA CONVERSA

#EnterpriseSec

Veja-nos no YouTube

Curta-nos no Facebook

Siga-nos no Twitter

Junte-se a nós no LinkedIn

Comente em nosso blog

Junte-se a nós no Threatpost

Acompanhe-nos no Securelist

SOBRE A KASPERSKY LAB

A Kaspersky Lab é a maior fornecedora privada de soluções de proteção de endpoints do mundo. A empresa está classificada entre as quatro maiores fornecedoras de soluções de segurança do mundo para usuários de endpoints*. Há mais de 17 anos a Kaspersky Lab inova a segurança e oferece soluções de segurança digital eficazes para grandes empresas, empresas de pequeno e médio porte e clientes. A Kaspersky Lab, com sua matriz registrada no Reino Unido, opera atualmente em quase 200 países e territórios no mundo todo, oferecendo proteção para mais de 400 milhões de usuários mundialmente. Saiba mais em www.kaspersky.com.

*A empresa ocupa o quarto lugar na classificação da IDC de Receita de segurança de endpoints global por fornecedor de 2013. A classificação foi publicada no relatório da IDC de "Previsão de 2014 a 2018 de segurança de endpoints global e participações de fornecedor de 2013 (IDC nº 250210, agosto de 2014). O relatório classificou fornecedores de software de acordo com lucros das vendas de soluções de segurança de endpoints em 2013.