FireEye™

White paper

Ataques dirigidos avançados

Como se proteger contra a nova geração de ataques cibernéticos

Sumário

Resumo executivo

O novo cenário de ameaças mudou. Criminosos cibernéticos e países estão buscando agressivamente ativos de dados valiosos, como informações sobre transações financeiras, planos de desenvolvimento de produtos, credenciais de usuários para sistemas confidenciais e outras formas de propriedade intelectual. Resumindo, a agressão cibernética evoluiu mais rapidamente do que as tecnologias defensivas utilizadas pela maioria das empresas atualmente.

Os firewalls, sistemas de prevenção de intrusões (IPS, intrusion prevention system), antivírus e gateways de segurança da próxima geração não protegem adequadamente as organizações contra as ameaças da próxima geração. Dos mais de $20 bilhões gastos anualmente em segurança de TI, praticamente tudo é gasto em tecnologia ultrapassada com base em assinaturas. As defesas com base em assinaturas interrompem apenas as ameaças conhecidas, e não os ataques dinâmicos e desconhecidos atualmente em uso. É por isso que mais de 95% das empresas abrigam malware avançado dentro de suas redes, apesar das muitas camadas de defesas tradicionais que as organizações têm distribuído.

Os criminosos cibernéticos estão armados com as mais recentes vulnerabilidades de dia-zero, kits de ferramentas de qualidade comercial e técnicas de engenharia social para perpetrar ataques dirigidos avançados. Essas ameaças movimentam-se de maneira lenta e discreta, utilizando diversos estágios e canais para enganar as defesas tradicionais e encontrar sistemas vulneráveis e dados confidenciais. A defesa contra esses ataques requer uma estratégia que vá além de assinaturas estáticas e de uma heurística comportamental rudimentar.

As defesas tradicionais estão se tornando cada vez mais pontos de cumprimento de políticas, em vez de defesas robustas contra intrusões cibernéticas. Por exemplo, filtros de URL ainda são úteis para cumprir políticas de uso aceitável quanto à navegação da Web pelos funcionários, mas não são mais eficazes na defesa contra ataques dinâmicos por download de passagem. Da mesma forma, os firewalls da próxima geração (NGFW, next-generation firewalls) simplesmente acrescentam opções de políticas da próxima geração em torno de usuários e aplicativos e consolidam proteções tradicionais com base em assinaturas. Embora os NGFW possam consolidar as proteções AV e IPS tradicionais, estas são tecnologias à base de assinaturas que não agregam novos níveis ou inovações à defesa de redes. Integrar essas defesas tradicionais entre si é pouco para frustrar as ameaças da nova geração.

Contra ameaças dinâmicas, defesas tradicionais como firewalls, IPS, antivírus, antispam e gateways de segurança fracassam, deixando uma brecha ampla para os criminosos cibernéticos. Os ataques de hoje utilizam táticas avançadas, como combinação de polimorfismo e personalização, para parecerem desconhecidos para as ferramentas com base em assinaturas, e suficientemente autênticos para contornar filtros de spam e até enganar as vítimas visadas. Por exemplo, ataques de "spear phishing" aproveitam sites de rede social para produzir e-mails personalizados que fornecem URLs dinâmicos e maliciosos que contornam os filtros de URL.

Para recuperar a dianteira contra os ataques da próxima geração, as empresas precisam recorrer a uma verdadeira proteção da próxima geração: sem assinaturas, proativa e em tempo real. Através de análise contínua do código suspeito ao longo de todo o ciclo de vida do ataque, e de bloqueio das comunicações do malware por múltiplos vetores de ameaça, as proteções da próxima geração podem impedir que malware avançado, explorações de dia-zero e táticas de ameaça persistente avançada (APT, advanced persistent threats) ponham em risco dados confidenciais.

"Há um amplo consenso de que ataques avançados contornam nossos controles de segurança tradicionais com base em assinaturas e continuam não detectados em nossos sistemas por longos períodos de tempo. A ameaça é real. Você já está comprometido e não sabe."

– Gartner, Inc., 2012

Natureza das ameaças da próxima geração

Os ataques mudaram em forma, função e sofisticação há apenas alguns anos. As ameaças da próxima geração utilizam tanto malware de comercialização em massa, desenvolvido para infectar muitos sistemas, quanto malware sofisticado de dia-zero para infectar sistemas visados. Elas combinam múltiplos vetores de ataque, como ataques com base em Web, e-mail e aplicativos. Os ataques atuais são voltados para a obtenção de ativos de dados valiosos — informações financeiras confidenciais, propriedade intelectual, credenciais de autenticação, informação privilegiada — e cada ataque costuma ser um esforço de múltiplos estágios para se infiltrar em redes e, em última instância, vazar os dados valiosos.

Desde as infecções comuns de Zeus/Zbot ao malware dirigido Stuxnet, os ataques cibernéticos provaram ser eficazes no roubo de dados confidenciais, causando perdas financeiras e manchando reputações corporativas. Os criminosos cibernéticos estão negociando bilhões de dólares em atividades cibernéticas. Países estão utilizando malware em espionagem cibernética para monitorar ativistas de oposição e prejudicar infraestruturas críticas do adversário. Devido aos grandes interesses envolvidos, o desenvolvimento de explorações de dia-zero e outras atividades criminosas são bem financiados. Isso levou a um movimentado ecossistema clandestino que negocia e vende acesso a sistemas residentes de algumas das redes mais confidenciais do mundo. Operações cibernéticas como GhostNet, Night Dragon e Nitro já afetaram corporações globais e governos utilizando táticas APT dirigidas, spear phishing e malware avançado.

Cada organização na "cadeia de fornecimento" da informação corre risco de ser atacada. Por exemplo, o roubo de algoritmos de autenticação de dois fatores da RSA (uma divisão da EMC) em março de 2011 demonstrou a natureza estratégica desses ataques: a propriedade intelectual que eles roubaram da RSA "poderia ser utilizada para reduzir a eficácia de uma implementação atual de autenticação de dois fatores, como parte de um ataque mais amplo"[1], permitindo que criminosos cibernéticos invadissem empresas do mundo todo.

Em abril de 2012, a VMware (uma subsidiária da EMC) confirmou que um hacker divulgou publicamente uma parte do código fonte do VMware, datada de 2003 e 2004. Com mais data centers utilizando virtualização, "um estudo da IBM em novembro de 2010[2] analisou divulgações de vulnerabilidades de segurança de virtualização e hipervisor da Citrix Systems, IBM, Microsoft, Oracle, Red Hat e VMware ao longo de mais de uma década. Esse estudo indica que 35% das vulnerabilidades de segurança permitem que um invasor escape de um servidor virtual hóspede e afete outros servidores virtuais ou o hipervisor".[3] Estes são apenas dois exemplos de ataques dirigidos avançados buscando propriedade intelectual valiosa para uso em ataques APT posteriores.

"As organizações enfrentam a evolução de um cenário de ameaças e estão despreparadas para lidar com isso".

– Gartner, Inc., 2012

"Os invasores APT estão muito mais motivados. É provável que eles passem a ter mais qualificações, mais financiamento e mais paciência. É provável que eles experimentem vários caminhos de ataque diferentes. E eles têm chances bem maiores de êxito."[4]

1 http://www.rsa.com/node.aspx?id=3872

2 http://public.dhe.ibm.com/common/ssi/ecm/en/wgl03007usen/WGL03007USEN.PDF

3 http://searchservervirtualization.techtarget.com/tip/Virtualization-and-hypervisor-security-vulnerabilities-to-look-out-for

4 http://www.schneier.com/blog/archives/2011/11/advanced_persis.html

Os cinco estágios dos ataques de múltiplos vetores e múltiplos estágios

As ameaças da próxima geração são complexas, combinando múltiplos vetores de ataque para maximizar as chances de invadir defesas de rede complexas. Os ataques de múltiplos vetores costumam ser perpetrados via Web ou e-mail. Eles tiram proveito de vulnerabilidades em aplicativos ou no sistema operacional, explorando a incapacidade dos mecanismos convencionais de proteção de redes de proporcionar uma defesa unificada.

Além de utilizar múltiplos vetores, os ataques dirigidos avançados também utilizam vários estágios para penetrar uma rede e, então, extrair as informações valiosas. Isso aumenta em muito as possibilidades de os ataques não serem detectados. Os cinco estágios do ciclo de vida dos ataques são os seguintes:

Estágio 1: Exploração do sistema. O ataque tenta preparar o primeiro estágio e explora o sistema utilizando "ataques de passagem (drive-by)" em navegação casual. Frequentemente, um ataque misto é perpetrado através dos vetores de ameaça Web ou e-mail, com o e-mail contendo URLs maliciosos.

Estágio 2: Cargas executáveis de malware são transferidas por download e um controle de longo prazo é estabelecido. Uma única exploração se traduz em dezenas de infecções no mesmo sistema. Com uma exploração bem-sucedida, mais executáveis de malware — keyloggers, backdoors de cavalos de Troia, descobridores de senhas e capturadores de arquivos — são, então, transferidos por download. Isso significa que os criminosos passam a ter mecanismos de controle de longo prazo no sistema.

Estágio 3: O malware entra em contato com sua origem. Assim que o malware é instalado, os invasores concluem a primeira etapa para o estabelecimento de um ponto de controle dentro das defesas da organização. Uma vez lá, o malware contacta os servidores criminosos para obter instruções adicionais. O malware também pode se replicar e disfarçar para evitar varreduras, desativar mecanismos de varredura antivírus, reinstalar componentes que faltam após uma limpeza ou permanecer latente por dias ou semanas. Utilizando conexões de retorno de dentro da rede confiável, as comunicações do malware passam pelo firewall e penetram em todas as diversas camadas da rede.

Estágio 4: Vazamento de dados. Os dados capturados dos servidores infectados são vazados em arquivos criptografados através de um protocolo frequentemente permitido, como FTP ou HTTP, para um servidor externo comprometido, controlado pelo criminoso.

Estágio 5: O malware espalha-se lateralmente. O criminoso procura avançar além do único sistema e estabelecer controle de longo prazo dentro da rede. O malware avançado procura unidades mapeadas em laptops e desktops infectados e, em seguida, pode se espalhar lateralmente e mais profundamente em compartilhamentos de arquivos de rede. O malware faz um reconhecimento: ele mapeia a infraestrutura da rede, determina quais são os principais ativos e estabelece uma presença de rede em servidores-alvo.

"Um invasor que tenha comprometido o PC do dono de uma conta pode controlar cada aspecto do que a vítima vê ou não vê porque o malfeitor pode, então, interceptar, excluir, modificar ou redirecionar toda a comunicação que entra e sai do PC infectado".[5]

5 http://krebsonsecurity.com/2011/02/sold-a-lemon-in-internet-banking/

O preço do problema

As empresas pagam um alto preço operacional. Uma pesquisa de 2012 da InformationWeek revelou que em 2011 mais de um quarto das empresas consultadas gastou pelo menos 10% e até mais de 25% de seu orçamento anual de TI apenas em segurança.[6] "O phishing e o malware fazem uma dupla poderosa. De acordo com nossa pesquisa (da InformationWeek), o malware continuou sendo o principal tipo de violação sofrido por nossos entrevistados".[7]

A pesquisa Cost of a Data Breach (Custo de uma violação de dados) do Instituto Ponemon revelou que "o padrão de resultados em 2011 é consistente com o dos anos anteriores, quando as violações mais caras costumavam envolver atos maliciosos contra a empresa, em vez de negligência ou falhas de sistema".[8] "Além disso, essas violações de dados eram as mais caras. Os ataques maliciosos geram mais custos porque são mais difíceis de detectar, sua investigação é mais complicada e são mais difíceis de conter e remediar".[9]

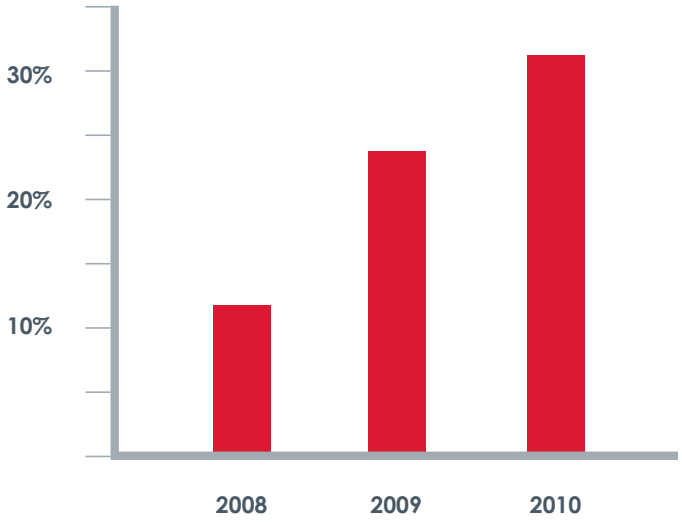

Figura 1: Ataques maliciosos são a causa raiz de um percentual crescente de violações de dados. Fonte: Ponemon

6 2012 Strategic Survey da InformationWeek. Página 34.

7 Ibid. Página 16

8 2011 Cost of Data Breach Study - United States. Benchmark Research Conducted by Ponemon Institute LLC. Report: March 2012 (Estudo sobre custo de uma violação de dados em 2011 - Estados Unidos. Pesquisa comparativa realizada pelo Ponemon Institute LLC. Relatório: Março de 2012). http://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-us.en-us.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2012Mar_worldwide__CODB_US

9 http://www.ponemon.org/blog/post/cost-of-a-data-breach-climbs-higher

Como as ameaças da próxima geração contornam a segurança tradicional

As ameaças da próxima geração ocorrem em vários estágios e em vários vetores de ameaça ao penetrarem em uma rede e, em seguida, ao extraírem informações valiosas. Os criminosos cibernéticos combinam em um ataque ensaiado vetores de ataque com base em Web, e-mail e arquivo, aumentando bastante as chances de que seus ataques não sejam detectados. Os firewalls, IPS, antivírus e gateways de Web atuais têm poucas chances de interromper invasores que utilizam táticas de APT, malware utilizado uma única vez e dia-zero.

Esses ataques mistos e de múltiplos estágios são bem-sucedidos porque as tecnologias de segurança tradicionais contam com correspondências de padrões com base em listas ou com base em assinaturas, muito estáticas. Muitas ameaças dirigidas e de dia-zero penetram os sistemas ocultando malware instalador polimórfico e recém-produzido em páginas inocentes da Web e em arquivos transferíveis por download, como imagens JPEG e documentos PDF. Elas também podem utilizar e-mails de phishing personalizados enviados para vítimas cuidadosamente selecionadas, com uma mensagem de aparência plausível e anexos maliciosos visando uma vulnerabilidade de dia-zero. Uma outra possibilidade é sua presença em sites de mídia social, incorporando tweets que incluam um URL encurtado, ocultando um destino malicioso. Toda vez que uma vítima visitar o URL ou abrir o anexo, uma carga de malware será instalada no computador da vítima. Esse código de malware costuma incluir explorações de múltiplas vulnerabilidades desconhecidas no sistema operacional, plug-ins, navegadores ou aplicativos, para assegurar um posto avançado no sistema. "Internet Explorer 6 no Windows XP? Eu tenho uma exploração para isso."

Além das vantagens tecnológicas das explorações, os criminosos cibernéticos também percebem que podem dividir e conquistar, porque assim são organizados os departamentos de TI e as defesas tradicionais. As defesas de segurança tradicionais costumam ser organizadas para inspecionar cada vetor de ataque como um caminho separado, e cada estágio como um evento independente, em vez de enxergar e analisar os estágios e vetores como uma série orquestrada de incidentes cibernéticos. Ao explorar os compartimentos estanques de negócios e tecnologia dentro dos departamentos de TI, uma infecção de Web de passagem parece um evento aleatório, consequência da decisão impensada de um usuário final de visitar um site duvidoso. Ela não pode ser rastreada até o e-mail de spear phishing originalmente utilizado para enganar o usuário e iniciar um ataque dirigido avançado de múltiplos estágios. Assim, após vários estágios de ataques por e-mail e Web, os criminosos cibernéticos conseguem vazar dados e os defensores não descobrem até ser tarde demais.

"As defesas atuais são precárias… as iniciativas antimalware existentes não são mais suficientes."

– Forrester Research, Inc., 2011

"A RSA foi invadida em algum momento na primeira metade de março, quando um funcionário foi vitimado por spear phishing e abriu uma planilha infectada. Assim que a planilha foi aberta, uma ameaça persistente avançada (APT) — um cavalo de Troia com backdoor — chamada Poison Ivy foi instalada. A partir daí, os invasores basicamente tiveram controle total sobre a rede interna da RSA, o que levou à eventual disseminação de dados pertinentes aos autenticadores de dois fatores da RSA".[10]

10 http://downloadsquad.switched.com/2011/04/06/security-firm-rsa-attacked-using-excel-flash-one-two-sucker-punc/

Como as ameaças da próxima geração ultrapassam as barreiras tradicionais?

- **Firewalls:** Os firewalls deixam passar tráfego HTTP genérico da Web. Os firewalls da próxima geração (NGFW) acrescentam camadas de regras de política com base em usuários e aplicativos. Os NGFW consolidam proteções tradicionais, como antivírus e IPS, mas não agregam uma proteção dinâmica que possa detectar comportamento ou conteúdo de ameaças da próxima geração.
- **IPS:** Assinaturas, inspeção de pacotes, análise de DNS e heurística não detectam nada de incomum em uma exploração de dia-zero, particularmente se o código é muito disfarçado ou fornecido em estágios.
- **Antivírus e filtragem de malware na Web:** Como o malware e a vulnerabilidade que ele explora são desconhecidos (dia-zero) e o site tem uma reputação limpa, antivírus e filtros de Web tradicionais deixam-no passar. O volume de vulnerabilidades em plug-ins de navegador como o Adobe e as combinações exponenciais desses navegadores com sistemas operacionais tornam difícil para os fornecedores de antivírus acompanhar.
- **Filtragem de spam de e-mail:** Sites de phishing falsificados utilizam URLs e domínios dinâmicos, portanto, as listas negras têm um certo atraso em relação às atividades criminosas. São necessários mais de dois dias para derrubar um site de phishing, em média.[11]

O código malicioso também pode ser transportado em laptops, dispositivos USB ou por compartilhamento de arquivos com base em nuvem para infectar uma máquina e disseminar-se lateralmente ao se conectar à rede. É comum que sistemas móveis percam atualizações de arquivos DAT e patches, portanto, eles são mais vulneráveis a explorações conhecidas e desconhecidas. Em geral, até mesmo máquinas atualizadas podem ser infectadas utilizando-se explorações de dia-zero e técnicas de engenharia social, especialmente quando o sistema está fora da rede corporativa.

Uma vez lá, o malware pode se replicar — com alterações sutis para fazer com que cada instância pareça única — e se disfarçar para evitar varreduras. Alguns desativam varreduras de antivírus, reinstalam-se após uma limpeza ou ficam latentes por dias ou semanas.

Eventualmente, o código entrará em contato com o criminoso para obter instruções adicionais, uma nova carga viral ou para entregar credenciais de login, dados financeiros e outros itens valiosos. Muitos hosts comprometidos proporcionam uma base privilegiada para que o criminoso possa explorar ainda mais e expandir sua rede de bots com novas vítimas.

A maioria das empresas não analisa o tráfego de saída para verificar essas transmissões e destinos maliciosos. As organizações que monitoram as transmissões enviadas utilizam ferramentas e procuram dados regulados e endereços de entidades reconhecidamente nocivas.

- **Filtragem da Web:** A maior parte das filtragens de saída bloqueia conteúdo adulto ou sites de entretenimento que desperdiçam tempo. Menos de um quarto das empresas restringe sites de redes sociais.[12] Além disso, URLs dinâmicos, hacks de sites legítimos e endereços ativos por breves períodos tornam obsoletas as listas negras de URLs estáticos.
- **Prevenção contra perda de dados (DLP):** As ferramentas de DLP (data loss prevention) são projetadas principalmente para informações de identificação pessoal (PII) — sequências de caracteres como números de CPF, números de licenças ou dados de saúde — e essas ferramentas são, no máximo, tão boas quanto suas regras. A maioria carece do refinamento e da complexidade necessários para detectar vazamentos de credenciais ou de propriedade intelectual. A criptografia dos canais de comunicação de retorno permite que os dados escapem sem serem vistos. Sua abordagem estática não corresponde à natureza dinâmica das ameaças da próxima geração.

11 Fonte: Symantec, 2010

12 A pesquisa da Sophos revelou que "mais da metade das empresas pesquisadas não impunha limitações ao acesso a Facebook, Twitter e LinkedIn — e menos de um quarto das empresas bloqueava completamente esses sites." https://secure.sophos.com/sophos/docs/eng/papers/sophos-security-threat-report-2011-wpna.pdf

Como fechar a brecha de segurança

A brecha na proteção e a sofisticação crescente dos criminosos cibernéticos exigem uma nova categoria de ferramentas de prevenção de ameaças adaptada à natureza resiliente, evasiva e complexa das ameaças da próxima geração. É por isso que organizações preocupadas com a segurança escolhem a FireEye como proteção líder do segmento contra ameaças da próxima geração que atravessam múltiplos vetores de ameaça e utilizam múltiplos estágios para contornar sistematicamente as defesas tradicionais. O FireEye Malware Protection System (MPS) complementa os firewalls, IPS, AV e gateways da próxima geração e os tradicionais, cujas assinaturas e heurística não conseguem interromper essa nova geração de ameaças.

Os appliances FireEye MPS foram desenvolvidos para proteger contra os vetores de ameaças por Web e e-mail e contra o malware residente em compartilhamentos de arquivos. Trata-se de uma plataforma de segurança integrada que oferece proteção multivetorial e que interrompe todos os estágios de um ataque avançado. Cada um dos appliances de segurança da FireEye conta com o mecanismo Virtual Execution (VX) que oferece análise avançada, sem assinaturas, utilizando máquinas virtuais exclusivas e patenteadas. O Malware Protection System constroi uma análise de 360 graus, estágio a estágio, de um ataque avançado, da exploração do sistema ao vazamento de dados, para interromper de maneira mais eficaz os potenciais atacantes APT.

Operando interna ou externamente, o FireEye Malware Protection System executa análises automatizadas em tempo real de tráfego suspeito na Web, anexos de e-mail e arquivos em servidores de compartilhamento de arquivos em rede. Tudo que parece suspeito é executado no mecanismo VX, onde os ambientes de teste exclusivos e plenos de recursos confirmam, irrefutavelmente, a má intenção e as atividades do invasor, identificando ameaças reais e evitando falsos positivos e falsos negativos.

Uma vez identificado o código malfeitor, suas portas de comunicação, endereços IP e protocolos são bloqueados para interromper transmissões para fora. Os analistas podem utilizar cirurgicamente a impressão digital do código malicioso para identificar e remediar sistemas comprometidos e evitar que a infecção se espalhe. Pesquisadores forenses podem executar os arquivos individualmente através de testes off-line automatizados para confirmar e dissecar o código malicioso. Uma inteligência compartilhada sobre ameaças com base em nuvem mantém todos atualizados quanto às inovações do crime cibernético e aos destinos de comunicação de retorno identificados no FireEye Labs e nos locais de outros clientes.

Esses appliances prontos para proteção de Web, e-mail e compartilhamento de arquivos podem ser distribuídos em menos de 30 minutos, sem a necessidade de criar ou ajustar regras. O preço da aquisição começa a uma minúscula fração do custo de uma violação de dados.

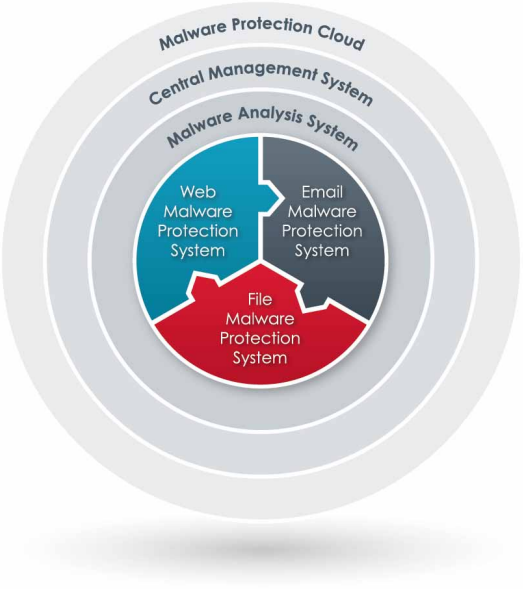

Figura 2: Proteção completa contra ataques dirigidos avançados

Segurança da próxima geração para interromper ataques avançados

O FireEye Malware Protection System fecha a brecha da rede deixada amplamente aberta em praticamente todas as organizações atualmente. Com um mecanismo VX de patente pendente, o FireEye MPS gera dinamicamente um conteúdo de segurança para interromper ataques anteriormente desconhecidos aliados à execução dinâmica de código para detectar as ameaças de dia-zero. Agora as empresas podem ter autênticas proteções de entrada e saída em tempo real contra ataques avançados dirigidos.

Corporações de todos os portes podem reforçar suas defesas tradicionais com uma prevenção de ameaças da próxima geração que compreende a natureza e a intenção desses maliciosos ataques avançados dirigidos, especialmente aqueles que se caracterizam como ameaças avançadas persistentes. Inscreva-se hoje mesmo para uma avaliação de segurança da sua rede pela FireEye para ver as ameaças passando pelas suas proteções atuais.

Sobre a FireEye, Inc.

FireEye, Inc. é líder em interromper ameaças da próxima geração que utilizam malware, explorações de dia-zero e táticas de APT. As soluções da FireEye complementam os firewalls, IPS, antivírus e gateways da próxima geração e os tradicionais, os quais não conseguem interromper ameaças avançadas, deixando brechas na segurança das redes. A FireEye oferece a única solução do mercado que detecta e bloqueia ataques pelos vetores de ameaça de Web e e-mail, bem como malware residente em compartilhamentos de arquivos. Ela abrange todos os estágios do ciclo de vida de um ataque, com um mecanismo sem assinaturas que utiliza análise de ataque em modo stateful para detectar ameaças de dia-zero. Sediada em Milpitas, na Califórnia (EUA), a FireEye conta com o apoio de grandes parceiros financeiros, como Sequoia Capital, Norwest Venture Partners e Juniper Networks.

Saiba mais em www.FireEye.com

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | +1 408.321.6300 | LATAM@FireEye.com | www.FireEye.com