RELATÓRIO

FireEye

# RELATÓRIO REGIONAL DE AMEAÇAS AVANÇADAS

América Latina 1S2014

SECURITY REIMAGINED

# ÍNDICE

## Introdução

Agradecemos a oportunidade de lhes apresentar uma perspectiva única a respeito do cenário de ameaças na América Latina no primeiro semestre de 2014. Há anos afirmamos que, sem saber, mais de 95% das empresas têm PCs comprometidos dentro de suas redes corporativas, e este ano não foi diferente. Durante nossa avaliação, identificamos todos os tipos de atores de ameaças que comprometem as redes dos nossos clientes, incluindo atores suspeitos apoiados por estados-nação em busca de espionagem cibernética, cibercriminosos e "hacktivistas" que desejam declarar suas convicções.

Atores de ameaças bem financiados ajustaram suas técnicas, deixando para trás um modelo genérico, oportunista e que “dava tiro para todos os lados” e adotaram um modelo direcionado, resistente e evasivo. Temos o prazer de apresentar uma análise que propicia uma avaliação abrangente do cenário de ameaças na América Latina. Estamos ansiosos para discutir esse relatório com você e ajudá-lo a definir e executar sua estratégia de segurança cibernética para o futuro.

## Resumo Executivo

Este Relatório de Ameaças Avançadas da FireEye para a América Latina apresenta um panorama das Ameaças Avançadas Persistentes (APT) que a FireEye descobriu que têm como alvo as redes de computadores na América Latina ao longo do primeiro semestre de 2014.

Atores de ameaças motivados por objetivos financeiros, políticos e sociais estão empregando métodos cada vez mais sofisticados para roubar propriedade intelectual confidencial, dados proprietários, informações pessoais e outros dados que possam ser monetizados. Tal violação pode representar para pessoas e organizações riscos de consequência financeira, legal e de reputação.

Este relatório resume os dados recolhidos a partir da nuvem de inteligência da Dynamic Threat Intelligence ™ (DTI) da FireEye. Ao longo dos últimos seis meses, a FireEye identificou na região da América Latina:

• **9 famílias únicas de malware de APT**, de um total de 227 famílias de malware de APT únicas em todo o mundo

• **32.339 sessões de Comando e Controle (C2) únicas**, de um total de 2,7 milhões de sessões C2 únicas em todo o mundo

• **11 países que hospedam infraestrutura C2**, de um total de 84 países que hospedam infraestrutura C2 em todo o globo

• **16 verticais industriais afetados**, comparado a 34 setores verticais afetados em todo o mundo

**Isenção de responsabilidade:** Este relatório abrange apenas a atividade das redes de computadores de certos clientes da FireEye que compartilham suas métricas com a FireEye. O relatório não constitui, de maneira alguma, fonte competente com relação a todas as atividades de APT que tenham a América Latina ou outros lugares como alvo. Neste conjunto de dados, tomamos precauções razoáveis para filtrar o tráfego de "teste" da rede, bem como o tráfego indicativo de compartilhamento manual de inteligência entre nossa base de clientes dentro de várias comunidades de segurança fechadas. Sabemos que algumas táticas, técnicas e procedimentos (TTP) populares de APT podem ser reutilizados e reaproveitados por muitos atores de ameaças diferentes. Para lidar com esse problema, empregamos filtros conservadores e fazemos verificações cruzadas para reduzir a probabilidade de erros de identificação.

## Definições

**Ameaça Avançada Persistente (ATP)** A FireEye Intelligence define atores de ameaça avançada persistente (APT) como atores de ameaças que recebem orientação e apoio de um governo nacional. Quer sua missão seja roubar informações ou causar perturbação ou destruição, eles buscam seus objetivos com tenacidade empregando para tanto uma ampla gama de ferramentas e táticas, incluindo diferentes tipos de malware.

**Callback (chamada de retorno):** comunicação não autorizada entre um computador vítima comprometido e uma infraestrutura de Comando e Controle (C2 ou CnC).

**Ferramenta de Administração Remota (RAT):** software que permite que um usuário de computador (para fins do presente relatório, um ator de ameaça) controle um sistema remoto como se tivesse acesso físico a tal sistema. As RATs oferecem inúmeros recursos, como captura de tela, exfiltração de arquivos etc. Normalmente, um atacante instala a RAT em um sistema de destino através de outros meios, como spear phishing ou exploração de uma vulnerabilidade zero-day, e a RAT tenta então não revelar sua existência ao proprietário legítimo do sistema.

**Evento de Segurança:** A FireEye descobre regularmente uma grande variedade de ameaças da web, de e-mail e ameaças baseadas em arquivos, incluindo a abertura de um anexo com malware, um clique em um link malicioso ou um callback de uma máquina infectada para uma rede de Comando e Controle (CnC).

**Ataque direcionado:** evento malicioso único realizado entre um ator de ameaça de APT e uma rede vítima específica.

**Ator de Ameaça:** o autor por trás da atividade cibernética. Este ator pode ser um "hacktivista", um cibercriminoso, ou parte de um grupo mais amplo, como uma unidade militar, agência de inteligência, uma organização contratada ou um ator não-governamental com patrocínio governamental indireto.

**Ferramentas, Técnicas e Procedimentos (TTPs):** características específicas das ações e ferramentas (como malware) de um ator de ameaça que são empregadas contra uma rede vítima. Uma APT normalmente emprega vários TTPs e múltiplos atores de APT também podem utilizar as mesmas TTPs. Essa dinâmica normalmente complica a análise da defesa cibernética.

**Setor Vertical:** uma das 20 categorias de setores de atividade distintos da FireEye: Aeroespacial, Produtos Químicos, Construção, E-Commerce, Educação, Energia, Mídia/Entretenimento, Finanças, Governo, Saúde, Alta Tecnologia, Seguros, Jurídico, Manufatura, Outros, Varejo, Serviços, Telecomunicações, Transporte e Atacadistas.

**Alvo:** o receptor de um ataque de um ator de ameaça. Na maioria dos casos, as baixas taxas "falso-positivas" inerentes aos alertas da FireEye sugerem que o ataque descoberto foi bem sucedido.

## Ameaças cibernéticas aos setores de atividade da América Latina

**Cibercrime**

O cibercrime continua representando uma ameaça para as pessoas e organizações na América Latina na medida em que a população está cada vez mais conectada à Internet e os serviços bancários e sistemas de pagamento on-line tornam-se mais generalizados. Em um relatório conjunto com a Organização dos Estados Americanos, os pesquisadores de segurança descobriram que ocorreu um aumento no cibercrime na região em 2013, na medida em que criminosos estabelecidos desenvolveram seu próprio malware e ferramentas para conduzir operações cibernéticas. Neste salto, os investigadores identificaram um grupo cibercriminoso suspeito que havia roubado até US$3,75 bilhões, desviando transações on-line feitas por meio de Boletos Bancários, um método de pagamento on-line comum no Brasil . Prevemos que os países da América Latina continuarão enfrentando as ameaças do cibercrime devido a protocolos de segurança negligentes e ao maior uso, por parte da população, dos sistemas bancários e de pagamentos on-line.

Cibercriminosos com motivação financeira também se aproveitaram de grandes eventos esportivos, como a Copa do Mundo da FIFA, para realizar fraudes visando informações pessoais ou financeiras; é provável que ocorra o mesmo nas próximas Olimpíadas. A FireEye observou atores de ameaças financeiras realizando 419 golpes envolvendo ingressos e alguns ataques de phishing utilizando temas da Copa do Mundo como isca. Embora não tenhamos observado nenhum grupo de APT conhecido ou suspeito utilizando temas da Copa do Mundo em e-mails de phishing, ainda acreditamos que esses atores de ameaças também podem ter utilizado o evento como isca em e-mails de phishing.

**Espionagem Cibernética**

É provável que organizações ativas na América Latina enfrentem riscos de ciberespionagem de atores de ameaças que trabalham para ou em associação com governos de estados-nação em busca de objetivos econômicos, militares, políticos ou sociais. Vários governos latino-americanos passaram a dar mais atenção à melhoria das práticas de segurança cibernética nacionais após as recentes denúncias de vigilância de governos e pessoas estrangeiras por parte da Agência de Segurança Nacional dos E.U.A.

Recentemente, vimos um ator de ameaça implantar malwares SOGU para invadir uma agência de um governo latino-americano. O grupo de ameaça entregou o malware por meio de um e-mail de phishing que empregava uma isca relacionada a energia; o anexo do e-mail parecia imitar ou, possivelmente, simular ter sido enviado por uma agência nacional de energia de outro governo regional latino-americano. No passado, observamos que grupos de APT baseados na China utilizavam SOGU/PlugX, e é provável que um grupo de APT com base na China tenha tentado invadir a agência do governo para realizar a espionagem cibernética.

No início deste ano, pesquisadores de outra empresa de segurança descobriram um ator de ameaças avançadas realizando operações de espionagem cibernética globais direcionadas a sistemas na Argentina, Bolívia, Brasil, Colômbia, Costa Rica e Venezuela, entre outros países. Pesquisadores da Kaspersky, que chamaram a atividade de "Careto" ou "a Máscara", declararam que os alvos principais eram instituições governamentais, diplomáticas, embaixadas, organizações do setor de energia, petróleo e gás, organizações de pesquisa e ativistas. Os pesquisadores observaram que o grupo de ameaças, que aparentemente está ativo há cerca de sete anos, havia

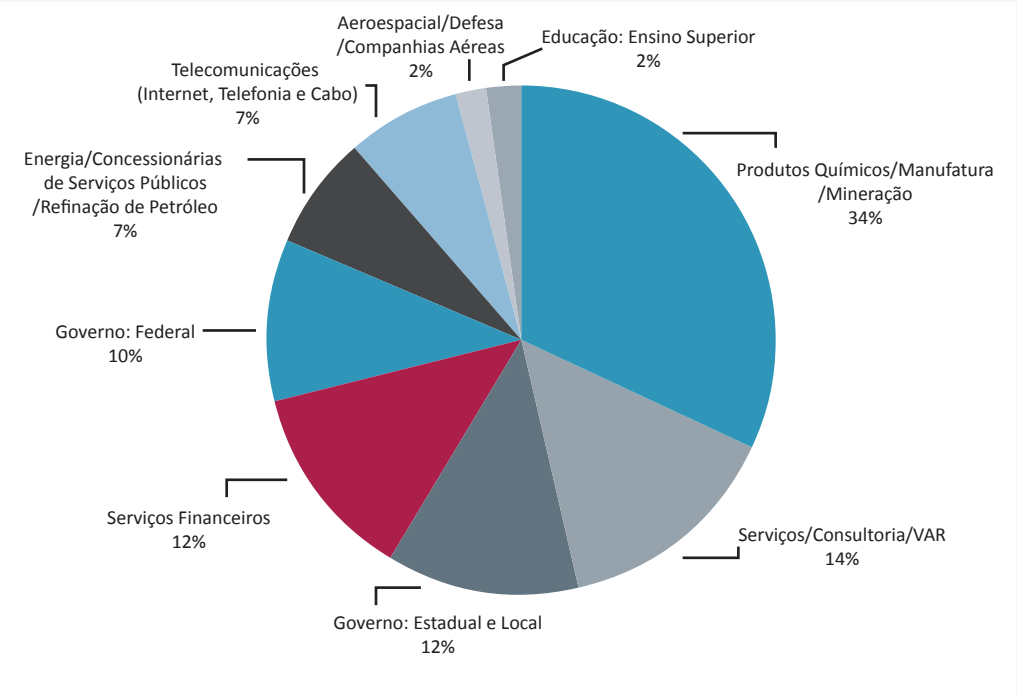
**Hacktivismo**

A FireEye acredita que as organizações continuarão a enfrentar ameaças de segurança cibernética advindas de hacktivistas que fazem uso de invasões de sites para desfigurá-los (defacement), fazer ataques de negação de serviço distribuídas (DDoS) e outros métodos para chamar atenção às suas causas. Durante a turbulência civil ocorrida na Venezuela no início deste ano, pessoas que se identificaram como membros do Anonymous desfiguraram várias páginas da web pertencentes ao governo da Venezuela em resposta à morte de diversos manifestantes. O hacktivismo tem o potencial de constranger vítimas, interromper suas operações e pode causar danos à reputação por conta da exposição de informações sigilosas ou revelação de práticas inadequadas de segurança.

## Infecções únicas por Setor Vertical

Na América Latina, a FireEye observou o maior número de eventos de APT no setor de energia e entre concessionárias de serviços públicos. O gráfico a seguir ilustra os eventos de APT que afetaram organizações na América Latina por setor. Produtos Químicos/Manufatura/Mineração e Serviços/Consultoria/Revendedores de Valor Agregado representam quase metade de todos os alertas de APT:

**Figura 1: Eventos de APT que afetaram organizações na América Latina, por setor**

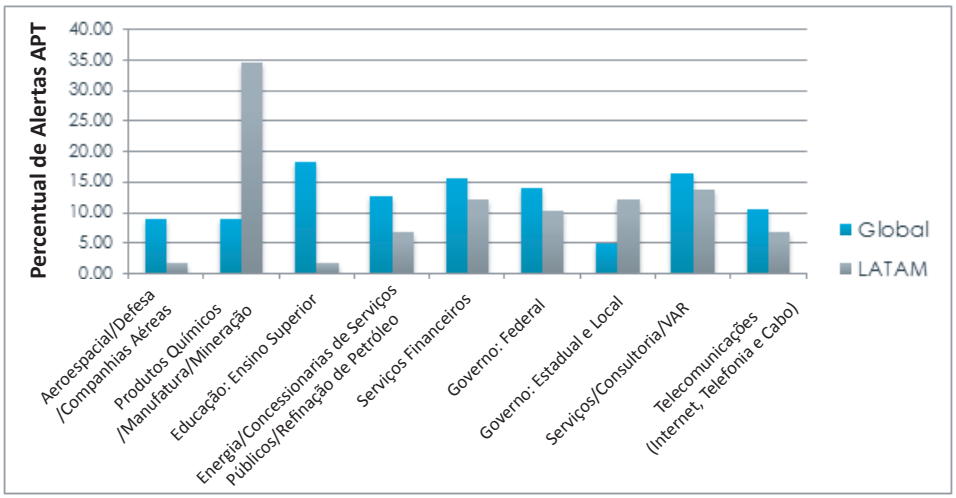


A título de comparação, o gráfico a seguir mostra eventos de APT por setor de atividade de nossos clientes na América Latina como percentual, em comparação com esses mesmos setores verticais globalmente. Esse gráfico sugere que Produtos Químicos/Manufatura/Mineração são atacados de forma desproporcional na região da América Latina em comparação com os clientes dos setores de Produtos Químicos/Manufatura/Mineração em termos globais. Acreditamos que os atores de ameaças ataquem clientes que operam nos setores de Produtos Químicos/Manufatura/Mineração de forma desproporcional na América Latina porque eles são grandes determinantes estratégicos e econômicos da região. Em 2012, as minas da América Latina foram responsáveis por 22%, 20% e 46% das saídas totais de minério de ferro, ouro e cobre do mundo, respectivamente.

É provável que os atores de ameaças que visem esse setor estejam tentando obter informações sobre tecnologias proprietárias, processos de negócios e preços que dariam aos governos ou organizações que os patrocinam vantagens econômicas competitivas nos negócios.

Em termos de grupos de ameaças, vimos nada menos do que 10 grupos de ameaças distintos atacando os setores verticais de Produtos Químicos/Manufatura/Mineração em todo o mundo.

Figura 2: Eventos de APT que os dispositivos da FireEye detectaram por setor como percentual de todos os alertas em todo o mundo, comparados à região da América Latina apenas. Os dados não foram normalizados quanto ao número de clientes de um dado setor.




Do ponto de vista comparativo, para todos os nossos clientes em todo o mundo, vemos a Alta Tecnologia como o setor mais visado.

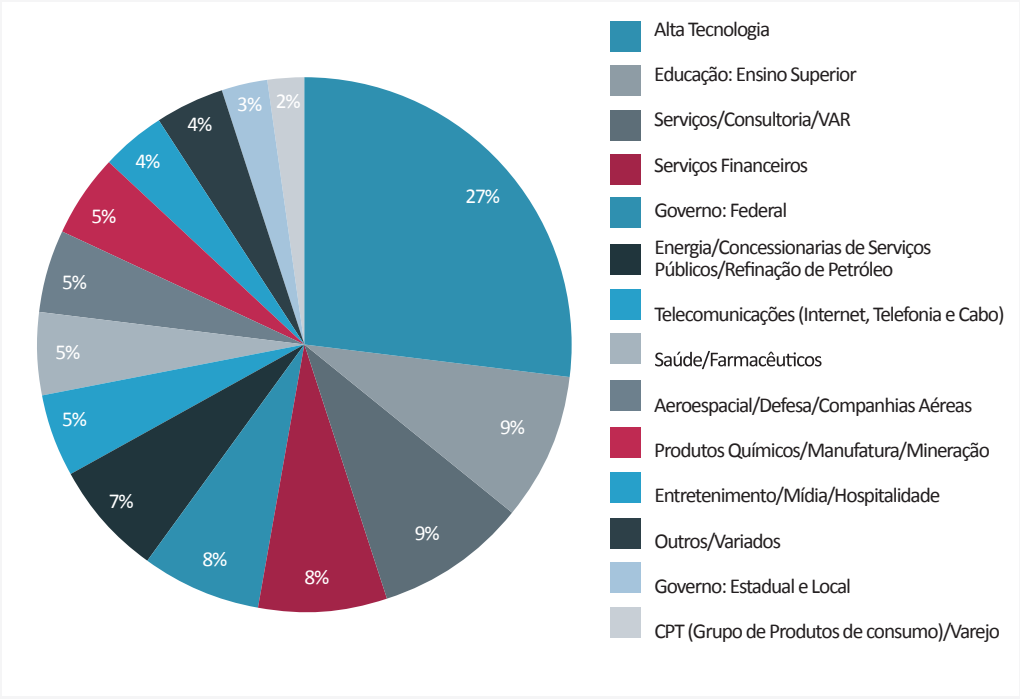
## Principais alertas de malware para a Região

O gráfico a seguir mostra os principais alertas de malware identificados pelos dispositivos da FireEye na região:

Os malwares observados com maior frequência pelos dispositivos da FireEye na região da América Latina, incluindo: XtremeRAT, Darkcomet, SpyNet e LV (também conhecido como njRAT). XtremeRAT, DarkComet, Houdini e Spynet estão todos disponíveis publicamente e são RATs relativamente simples, mas eficazes. Por estarem prontamente disponíveis, podem ser utilizados por atacantes avançados para "se misturar", mas também podem ser utilizados por diferentes tipos de atores de ameaças com todo tipo de motivação devido à facilidade de acessá-los e por conta da baixa barreira à entrada.

Anteriormente, a FireEye havia identificado grupos direcionados de APT baseados na China que utilizavam o Kaba (também conhecido como SOGU ou PlugX) e o malware que chamamos de "9002" (também conhecido como HOMEUNIX) na condução das operações

Figura 3: Eventos de APT que os dispositivos da FireEye detectaram por setor como percentual de todos os alertas



Anteriormente, a FireEye havia identificado grupos direcionados de APT baseados na China que utilizavam o Kaba (também conhecido como SOGU ou PlugX) e o malware que chamamos de "9002" (também conhecido como HOMEUNIX) na condução das operações.

## Contexto do Malware: Detecções globais

O Darkcomet também esteve entre as detecções globais mais frequentes da FireEye, seguido por Gh0stRAT, LV e XTremeRAT. Abaixo estão os principais alertas de malware que os dispositivos da FireEye identificaram em todo o mundo:

**Figura 4: Principais malwares observados pelos dispositivos da FireEye na América Latina**

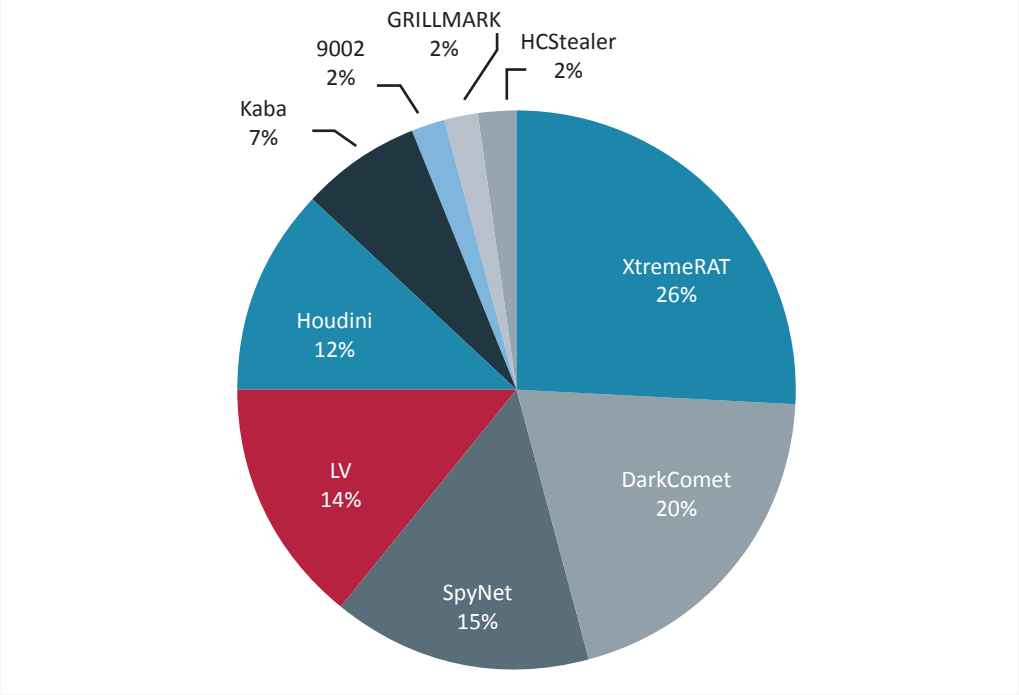
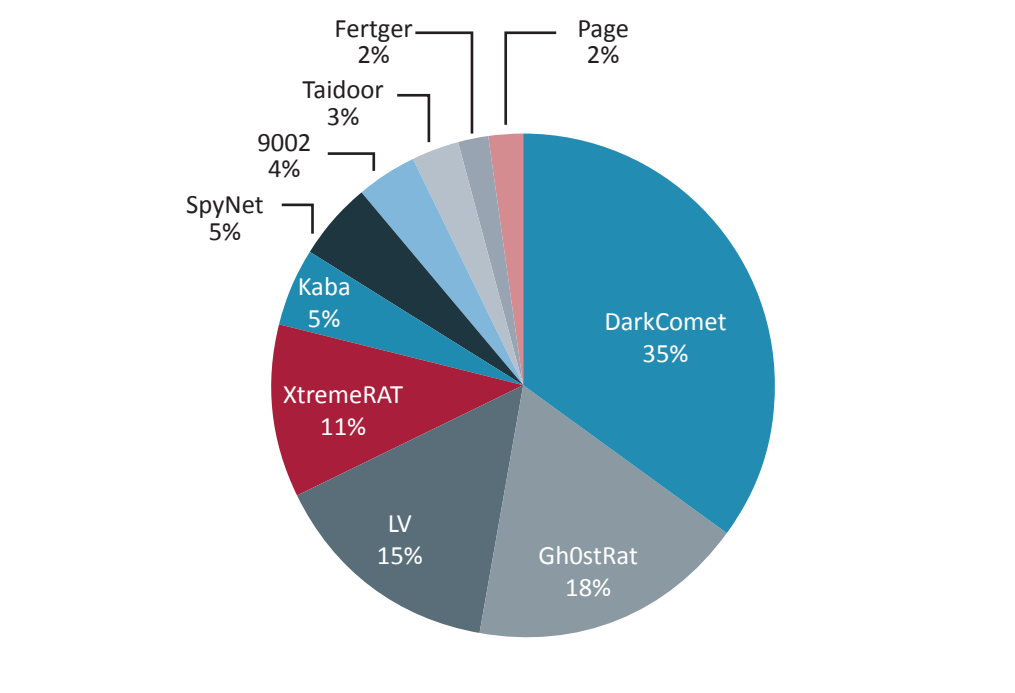


**Figura 5: Principais malwares identificados pelos dispositivos da FireEye em todo o mundo**



## Conclusão e Recomendações

As evidências destacadas neste relatório demonstram que as organizações na América Latina são alvo de ameaças avançadas. O tipo de malware que identificamos neste relatório é consistente com o malware que vemos atacando vítimas em outros países e setores verticais. Esses atacantes são persistentes e continuarão a perseguir seus objetivos por qualquer meio necessário.

Recomendamos o seguinte:

1. Embora as ameaças estejam ficando mais sofisticadas e mais difíceis de detectar, a higiene básica é mais importante do que nunca. Certifique-se de que as ferramentas de segurança existentes estejam atualizadas. A maioria dos malwares comuns pode ser tratada facilmente com ferramentas legado, baseadas em assinaturas.

2. Implemente sistemas de Proteção a Ameaças Avançadas para garantir que dados de alto valor estejam protegidos. Isso inclui tanto mecanismos de detecção sem assinatura baseados em rede/web e em e-mail, quanto capacidade de encontrar ameaças nos endpoints. As organizações precisam ter a capacidade de fazer perguntas entre seus endpoints, não só do ponto de vista da ameaça, mas também de uma abordagem de comportamento e metodologia.

3. Planeje e implemente um recurso de Operações de Segurança (SOC), bem como uma Equipe de Resposta a Incidentes de TI (CIRT) e uma estratégia de Plano de Gestão para fechar brechas de segurança existentes.

   A função SOC/CIRT dentro de uma organização deve ter tanto a função de "alertas de monitoramento" quanto capacidade de "caça" para encontrar ameaças desconhecidas de forma proativa.

4. Utilize, colete e compartilhe informações sobre ameaças, tanto dentro de sua organização quanto em outras organizações em seu setor vertical e em sua região geográfica. Colabore com outras entidades no que tange a ameaças cibernéticas emergentes para otimizar sua postura de segurança. A inteligência de ameaças fornece os fundamentos necessários para ajudar a tratar descobertas e minimizar ameaças. A inteligência de ameaças ocorre de duas formas: estruturada - inteligência formatada para consumo por tecnologia, como por exemplo, um Indicador de Compromisso (COI) ou um endereço/domínio de IP; e não-estruturada - inteligência de análise humana, como por exemplo este relatório, que descreve as tendências geográficas das ameaças, ou talvez um dossiê sobre um grupo de ameaças e suas famílias de malware específicas direcionadas a certos setores.

5. Por fim, a melhor tecnologia do mundo não pode ser eficaz sem pessoas treinadas. As organizações devem investir fortemente na formação e retenção do pessoal de segurança da informação. As organizações devem se preocupar não apenas em reter seu pessoal de segurança de grande valor, mas também procurar por outra fonte de recursos, como serviços gerenciados, recrutamento em universidades e estágios.

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | latam@fireeye.com | www.fireeye.com



FireEye