SONICWALL®
Tipos de estratégias contra ataques cibernéticos e como derrotá-los
E-BOOK

Introdução

Os criminosos cibernéticos modernos aprimoraram suas técnicas já complexas para evitar a detecção, enquanto se ocultam incógnitos nas redes por uma série de motivos, geralmente em busca de ganhos financeiros. Os autores das ameaças estão tentando roubar propriedade intelectual, cometer atos de espionagem, interferir em processos ou bloquear arquivos para cobrar um resgate, entre vários outros crimes. Eles empregam as técnicas mais recentes para se evadirem da detecção, com o objetivo de manter seu acesso e executar suas atividades mal-intencionadas sem serem notados.

Assim que conseguem invadir um alvo, os criminosos tentam baixar e instalar malware no sistema comprometido. Em muitos casos, o malware utilizado é uma variante recente e evoluída que as soluções antivírus tradicionais ainda não conhecem.

Este e-book detalha as estratégias contra ataques cibernéticos e ferramentas que criminosos cibernéticos utilizam para se infiltrar na sua rede, bem como uma descrição detalhada de como você pode combater essas estratégias para interromper a ação dos criminosos cibernéticos no ato.

Os criminosos cibernéticos trabalham 24 horas por dia para explorar seus pontos fracos.

Estratégia contra ataques cibernéticos nº 1 Bombardear as redes com malware 24 horas por dia

O malware está em alta em relação ao volume total de ataques, com alguns países registrando vários milhões de tentativas. Os ataques pode vir de todos os vetores e almejar e comprometer sua rede. E-mails, dispositivos móveis, tráfego na internet, entre outros meios, são todos alvos em potencial, e os hackers podem até mesmo comprometê-los utilizando recursos de exploração automatizados. Em todos os casos, pouco importa o tamanho da sua empresa. Para um hacker, você é um endereço IP, um endereço de e-mail ou um cliente em potencial e uma fonte para ataques. Os criminosos utilizam ferramentas automatizadas para realizar invasões ou lançar e-mails de phishing dia e noite.

O problema enfrentado por muitas organizações não conta com as ferramentas necessárias para o trabalho. Muitas não contam com ferramentas automatizadas para ajudar a depurar o tráfego nas redes, proteger endpoints e filtrar e isolar e-mails mal-intencionados. Outras instalam firewalls que não são capazes de fazer detecções no tráfego criptografado, de ameaças ocultas ou confiar em uma memória instalada limitada em seu sistema para armazenar as assinaturas de malware.

Contra-ataque nº 1
Proteja sua rede a cada minuto, todos os dias

Com centenas de variantes de malware nunca vistas antes, desenvolvidas a cada hora, as organizações precisam de uma proteção em tempo real, atualizada a cada minuto, contra essas novas ameaças. Uma solução de segurança eficaz deve ter a tecnologia mais recente para detectar os riscos em tempo real, protegendo sua organização 24 horas por dia, sete dias por semana. Com o grande fluxo de tipos e variantes de malware, a memória disponível de qualquer firewall se esgota. Uma solução de serviços de segurança que inclui tecnologias como a Inspeção profunda de memória em tempo real (Real-Time Deep Memory Inspection – RTDMI™) detecta e bloqueia proativamente ameaças em massa e no dia zero no mercado, bem como variantes de malware desconhecidas.

Os firewalls devem utilizar um sandbox operando em nuvem para fornecer um panorama mais amplo do malware e descobrir e identificar novíssimas variantes. Também é crítico assegurar que a sua solução de segurança permite a atualização dinâmica da proteção, não apenas no gateway dos firewalls, mas também nos dispositivos móveis e nos endpoints remotos da mesma forma, porque os dispositivos da internet das coisas (IOT) podem servir como pontos de partida para os criminosos.

Insista em uma plataforma de segurança que potencialize o poder da nuvem para oferecer a detecção e prevenção automatizadas em tempo real, para combater as ameaças mais recentes com malware.

Os criminosos cibernéticos utilizam diferentes tipos de malware para pegar você desprevenido.

Estratégia contra ataques cibernéticos nº 2
Infectar redes com diferentes formatos de malware

Os criminosos cibernéticos utilizam múltiplos vetores de ataque e variantes de malware para comprometer as redes. Os cinco tipos mais comuns são vírus, worms, cavalos de Troia, spyware e ransomware.

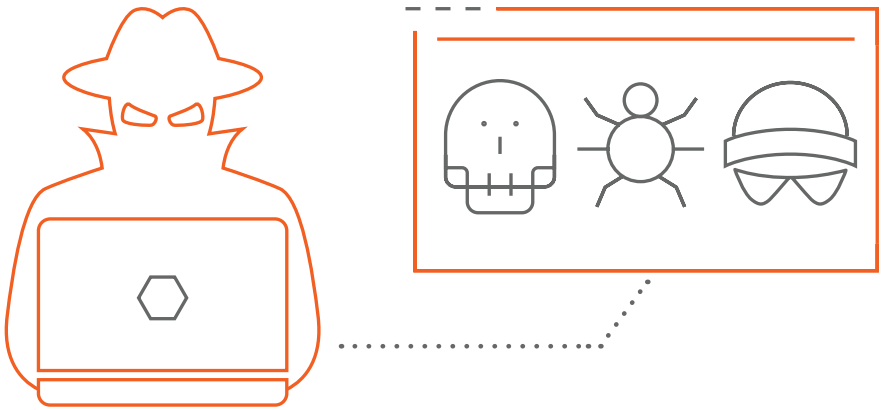
Os vírus de computador se espalharam originalmente pelo compartilhamento de mídia infectada. À medida que a tecnologia evoluiu, os métodos de distribuição evoluíram da mesma forma. Atualmente, os vírus comumente se espalham por meio de programas legítimos, compartilhamento de arquivos, downloads via internet e anexos a e-mails. Eles podem cometer uma série de ações mal-intencionadas de corrupção de dados a travamento de sistemas quando são abertos ou executados.

Os worms de computador já existem desde o final do anos 1980, mas não foram predominantes até que a infraestrutura de redes em organizações se tornou algo comum. Ao contrário dos vírus de computador, os worms se replicam e podem rastejar pelas redes sem qualquer interação humana. Eles podem causar infecções rápidas e sobrecarregar as redes com tráfego.

Os cavalos de Troia são programas mal-intencionados que se passam por software legítimo ou arquivos projetados especificamente para extrair dados sigilosos de uma rede. Muitos tipos de cavalo de Troia assumem o controle do sistema infectado e abrem as portas dos fundos para os criminosos terem acesso mais tarde. Os cavalos de Troia também costumam ser utilizados na criação de botnets.

O spyware não é tipicamente malicioso por natureza, mas é um grande incômodo, porque costuma infectar navegadores da internet, tornando-os quase inoperantes. O spyware muitas vezes se disfarça como um aplicativo legítimo, oferecendo ao usuário alguns benefícios, mas ao mesmo tempo gravando em segredo as teclas pressionadas e o histórico de navegação, roubando dados pessoais ou monitorando o comportamento do usuário e seus padrões de utilização. Os dados roubados serão então enviados para o criminoso, comprometendo a privacidade e a segurança do usuário.

O ransomware é um ataque que muitas vezes criptografa os arquivos em um endpoint ou em um servidor, tornando-os inacessíveis. Os criminosos cibernéticos exigem um resgate da organização, geralmente em Bitcoins, para cederem a chave criptográfica que libera os arquivos. Quando se espalha em sistemas críticos para uma empresa, o custo do ransomware pode chegar a centenas de milhares de dólares, ou mais.



Para antecipar-se às ameaças, considere a implementação de múltiplas camadas de proteção contra malware.

Contra-ataque nº 2
Certificar-se de que a rede está protegida contra todos os tipos de malware

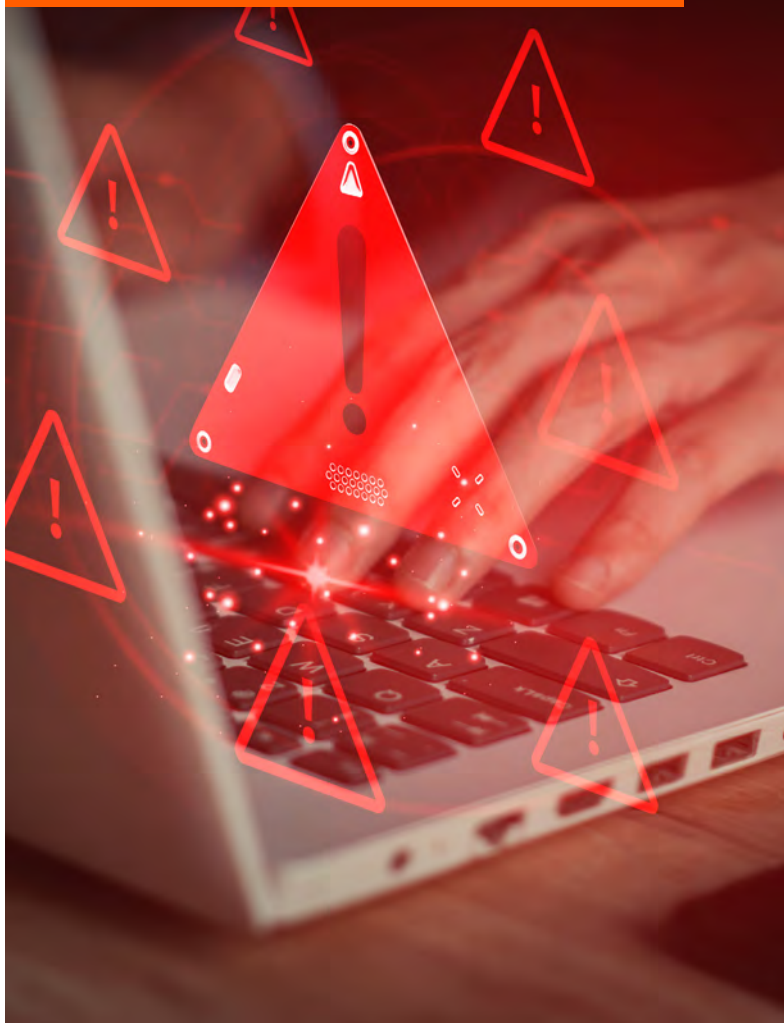
Todos os firewalls devem proteger as organizações contra todos os tipos de ameaças cibernéticas. Para obter melhores resultados, é preciso integrar essas proteções em um único passe, uma abordagem de baixa latência que bloqueie os vetores de ataque não apenas nos gateways, mas também nos endpoints, além do perímetro tradicional. Procure recursos que incluam:

- Proteção contra malware em redes para impedir os criminosos de baixar ou transmitir malware para um sistema comprometido
- Atualizações regulares e tempestivas para proteger as redes 24 horas por dia contra milhões de novas variantes de malware, assim que são descobertas
- Serviço de Prevenção de Intrusões (Intrusion Prevention Service – IPS) para impedir que os criminosos explorem as vulnerabilidades
- Sandboxing para enviar códigos suspeitos para um ambiente isolado, operando em nuvem, que possa realizar uma análise e detectar variantes de malware nunca vistas antes
- Segurança de acesso, incluindo contramedidas de controle de acesso de usuário em endpoints móveis e remotos, dentro e fora do perímetro da rede
- Segurança de e-mails para bloquear ataques de phishing, spam, cavalos de Troia e engenharia social transmitidos por e-mail

Certifique-se de que todos os dispositivos que têm acesso à sua rede estão com o software de proteção antivírus atualizado para fornecer uma camada adicional de proteção contra o malware em rede. Quando as organizações utilizam uma combinação de antivírus abrangente executados em PCs com firewalls em rede, elas podem impedir a ação de várias ferramentas que os criminosos cibernéticos utilizam para comprometer uma rede.

Estratégia contra ataques cibernéticos nº 3 Localizar e comprometer as redes mais fracas

Os criminosos cibernéticos muitas vezes almejam suas vítimas com base nos pontos fracos que identificam nas redes.



Embora muitos fornecedores de firewall aleguem que oferecem uma proteção superior contra ameaças, poucos são capazes de demonstrar a eficácia de suas soluções. Organizações que já têm firewalls instalados podem acreditar que suas redes estão protegidas, mas criminosos cibernéticos mais hábeis podem passar despercebidos por firewalls que não contam com as medidas de segurança correta, utilizando algoritmos complicados para evadir a detecção e comprometer a rede.

Alguns firewalls oferecem segurança em detrimento do desempenho, que podem levar as organizações clientes a utilizá-los desativando ou limitando suas medidas de segurança para atender à demanda de alto desempenho de sua rede. Trata-se de uma prática extremamente arriscada, que deve ser evitada.

Outra vulnerabilidade surge na segurança da rede devido a fatores humanos. Os criminosos dependem do potencial das ações ou do comportamento humano para comprometer inadvertidamente a integridade, confidencialidade e disponibilidade de uma rede. As ações que podem oferecer riscos e enfraquecer as medidas de segurança para aplicar golpes de phishing e engenharia social em sistemas mal configurados, software necessitando de reparos, políticas de segurança ignoradas, entre outras. Os autores das ameaças exploram essas táticas para obterem acesso aos sistemas e a informações de autorização que permitam que simplesmente contornem as proteções dos firewalls, instigando ataques de dentro do sistema. Além de tudo isso, os funcionários costumam conectar dispositivos pessoais à rede corporativa, sem adotar as medidas de segurança cabíveis. Isto pode gerar acessos não autorizados se um dispositivo pessoal for perdido ou deixado sem supervisão, expondo a organização a uma violação quando estiverem fora do perímetro de segurança da rede.

> Todos os firewalls precisam de um mecanismo que proteja as redes contra ataques tanto internos quanto externos, sem comprometer o desempenho.

Contra-ataque nº 3

Escolha uma plataforma de segurança abrangente, que ofereça proteção superior contra ameaças, alto desempenho e gerenciamento centralizado.

Procure soluções de segurança que tenham sido testadas e certificadas de forma independente, para garantir a proteção contra malware em rede.

Considere um projeto de plataforma com vários núcleos, que possa fazer a varredura de arquivos de qualquer tamanho e tipo para responder a mudanças no fluxo do tráfego. Todos os firewalls precisam de um mecanismo que proteja as redes contra ataques tanto internos quanto externos, sem comprometer o desempenho.

Procure um firewall que ofereça serviços de sandbox em nuvem para ajudar a identificar novíssimas formas de malware que podem estar visando ao seu ambiente de rede. Essas opções podem fazer a diferença entre um dia de trabalho normal e um dia em que os criminosos cibernéticos podem sequestrar seus ativos digitais.

Sua estratégia de segurança deve incluir a proteção de endpoints móveis e remotos, tanto dentro quanto fora do perímetro, para garantir a segurança no acesso de dispositivos móveis.

Além disso, você precisa de segurança de e-mails para se proteger contra phishing, spam, vírus, engenharia social e outras ameaças transmitidas por e-mail. Use ferramentas como o SonicWall Phishing Quiz, um recurso gratuito para educar seus colaboradores.

Estratégia contra ataques cibernéticos nº 4
Metamorfose frequente e ataque global

Muitos criminosos cibernéticos são bem-sucedidos inventando constantemente novas formas de malware e compatilhando-as com seus comparsas pelo mundo afora. Isto quer dizer que novas ameaças aparecem a cada segundo em todos os continentes. Muitos criminosos cibernéticos utilizam uma abordagem de "esmagar e prender" (smash and grab) em seus ataques: entrar, pegar o que querem e sair antes que alguém possa soar o alarme. Eles podem conseguir sair da rede antes mesmo que você saiba o que atingiu sua rede. Outros voam baixo e lentamente, na tentativa de obter acesso a mais dados por um período mais longo. Alguns ataques ocorrem pela internet e outros passam por um e-mail ou diretamente na rede em dispositivos infectados que estiveram funcionando em roaming anteriormente, fora do perímetro de segurança da rede.

Novas ameaças aparecem a cada segundo em todos os continentes.

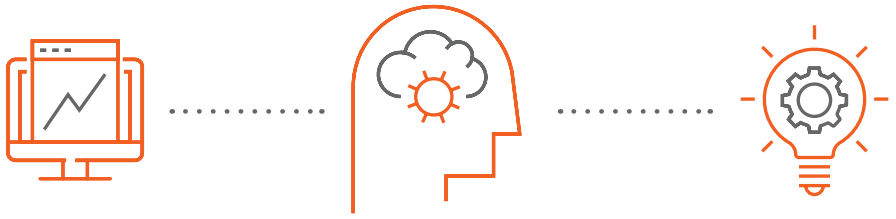
Para bloquear as mais recentes ameaças globais, invista em uma solução de segurança com inteligência global em ameaças.

Contra-ataque nº 4
Escolha um firewall que proteja você contra as ameaças globais

Reagir rapidamente às ameaças é crítico para maximizar a proteção. Para implementar rapidamente contramedidas contra ameaças emergentes, procure fornecedores de soluções de segurança que tenham sua própria inteligência em ameaças, equipes de pesquisas e contramedidas. Além disso, essa equipe deve estender seu alcance colaborando com uma comunidade mais ampla de segurança, assim como o Relatório de Ameaças Cibernéticas da SonicWall.

Uma solução de espectro amplo utiliza um catálogo de malware abrangente que atua internacionalmente em nuvem, para expandir as análises dos firewalls locais.

Finalmente, embora um firewall simples possa identificar e bloquear conforme a região, um firewall com tecnologia de ponta e mais sofisticado acrescenta recursos de filtração de botnets para reduzir a exposição a ameaças globais conhecidas, bloqueando o tráfego contra domínios de risco ou conexões de e para locais mal-intencionados.



Conclusão

Ao desenvolver estratégias defesa eficazes contra ataques cibernéticos a redes, você deve implementar uma abordagem holística, que inclua práticas comprovadas de segurança e o uso de ferramentas de segurança eficazes que detectem e respondam a comportamentos anormais nas redes, sem comprometer o desempenho. Proteja a si mesmo e a sua organização contra o desconhecido, mantendo-se proativo quanto a adaptação às ameaças em franca evolução.

Quando você estiver pronto para avaliar as soluções de contra-ataque que atendam às necessidades exclusivas da sua organização, entre em contato com o representante da SonicWall ou visite-nos on-line para saber mais sobre os Firewalls com Tecnologia de Ponta da SonicWall (Next-Generation Firewalls – NGFW).

Como posso me informar mais?

Ente em contato conosco para conhecer um especialista em segurança da SonicWall.

Confira a Demonstração ao Vivo da nossa linha de produtos SonicWall.

Visite nossa página na internet, Firewalls com tecnologia de ponta

Saiba onde estão ocorrendo os ataques, atualizados pelo Central de Segurança do Capture Labs.

Sobre a SonicWall

A SonicWall fornece segurança cibernética sem limites na era da hiperdistribuição, em uma realidade de trabalho onde todos estão remotos, móveis e inseguros. Ao conhecer o desconhecido, oferecer visibilidade em tempo real e possibilitar economia disruptiva, a SonicWall preenche as lacunas de cibersegurança para grandes empresas, governos e PMEs em todo o mundo. Para mais informações, visite www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Consulte nosso site na internet para obter informações adicionais.
www.sonicwall.com

© 2023 SonicWall Inc. TODOS OS DIREITOS RESERVADOS.
SonicWall é uma marca registrada da SonicWall Inc. e/ou de suas afiliadas nos EUA e/ou em outros países. Todas as demais marcas e marcas registradas são de propriedade dos respectivos titulares. As informações deste documento foram fornecidas em relação aos produtos da SonicWall Inc. e/ou de suas afiliadas. Nenhuma licença, expressa ou implícita, por preclusão ou de qualquer espécie, para qualquer direito de propriedade intelectual será concedida por meio deste documento ou em relação à venda de produtos da SonicWall. Salvo na forma estabelecida nos termos e condições, conforme especificado no contrato de licenciamento deste produto, a SonicWall e/ou suas afiliadas presumem isenção de responsabilidade, qualquer que seja, e de qualquer garantia expressa, implícita ou prevista em lei relacionada a seus produtos, incluindo, entre outras, a garantia implícita de comerciabilidade, adequação a um objetivo específico ou não violação. Em hipótese alguma, a SonicWall e/ou suas afiliadas se responsabilizam por qualquer tipo de dano direto, indireto, consequencial, cominatório, especial ou eventual (incluindo, entre outros, danos por lucros cessantes, interrupção de negócios ou perda de informações) decorrentes da utilização ou da incapacidade de utilizar este documento, mesmo se a SonicWall e/ou suas afiliadas foram orientadas da possibilidade de ocorrência de tais danos. A SonicWall e/ou suas afiliadas não fazem qualquer declaração nem oferecem garantias em relação à precisão ou integridade do conteúdo deste documento, e reservam para si o direito de realizar alterações nas especificações e descrições de produtos a qualquer momento e sem aviso prévio. A SonicWall Inc. e/ou suas afiliadas não assumem qualquer compromisso pela atualização das informações contidas neste documento.
Ebook-TypesofCyberattacks-JK-8854