SONICWALL

RESUMO EXECUTIVO: O LADO OBSCURO DA CRIPTOGRAFIA

Por que a sua segurança de rede precisa descriptografar o tráfego para interromper ameaças ocultas

Resumo

Hoje em dia, provavelmente a maioria das sessões da Web de seus usuários é criptografada com HTTPS ou com a criptografia Secure Sockets Layer/Transport Layer Security (SSL/TLS). Isso acontece porque existe atualmente uma enorme tendência no setor que almeja partir para uma Internet totalmente criptografada a fim de alcançar dois objetivos principais:

- Dificultar a interceptação de criminosos cibernéticos em conexões da Web
- Manter as informações pessoais protegidas e privadas

Conforme os usuários bem-intencionados aumentam o uso do protocolo de criptografia, a criptografia em si tem se tornado o vetor de ameaça favorito para os hackers mascararem seus ataques, burlarem os sistemas de defesa e, por fim, abrirem backdoors diretamente na sua rede. Afinal, seus controles de segurança não podem impedir o que não conseguem ver. Se não forem combatidos, quaisquer ataques que utilizarem SSL/TLS terão uma taxa de sucesso de 100% no comprometimento da sua rede, o que leva à perda de dados classificados, IP e reputação.

A criptografia está em todo lugar

Geralmente, a criptografia SSL/TLS é utilizada para tudo, desde e-commerce até transações bancárias on-line. Ela protege uma crescente quantidade de tráfego corporativo e representa a maior parte do tráfego na rede em alguns setores. A SSL protege os dados em movimento ao criar um canal criptografado na Internet pública ou em redes privadas, o que impede que os dados sejam capturados ou comprometidos.

Além disso, a SSL verifica se o destino final dos dados não foi falsificado por um hacker como um destino confiável. Dados importantes e confidenciais, como informações de cartões de crédito, nomes de usuários e senhas, são transportados de forma que, exceto pelo destinatário pretendido, qualquer pessoa tenha dificuldade em acessá-los. Enquanto sites e servidores FTP e Telnet eram os usuários originais da SSL, hoje há uma grande variedade de aplicativos que utilizam o protocolo, inclusive aplicativos baseados em Java, serviços de gerenciamento de aplicativos e serviços baseados em cloud. O Facebook e o Twitter são dois dos aplicativos mais populares com a SSL ativada. Add-nos do navegador que podem forçar

Soluções de segurança de rede legadas normalmente não têm capacidade de inspecionar tráfego criptografado por SSL/TLS ou seu desempenho é tão baixo que elas se tornam inutilizáveis ao realizar a inspeção.

o uso da SSL via HTTPS também estão disponíveis.[1]

No quarto trimestre de 2015, as conexões HTTPS (SSL/TLS) totalizaram, em média, 64,6% das conexões da Web, o que superou o crescimento de HTTP durante a maior parte do ano. Em janeiro de 2015, as conexões HTTPS eram 109% maiores do que em janeiro de 2014. Além disso, cada mês de 2015 percebeu um aumento médio de 53% em relação ao mês correspondente em 2014.

Firewalls podem ser desafiados ao inspecionar o tráfego criptografado

Por meio da SSL/TLS, invasores experientes conseguem codificar comunicações de comando e controle, além de códigos mal-intencionados, para burlar os sistemas de prevenção de intrusão (IPS) e os sistemas de inspeção antimalware. Esses ataques podem ser extremamente eficazes, simplesmente porque a maioria das organizações não possui a infraestrutura adequada para detectá-los. Soluções de segurança de rede legadas normalmente não têm capacidade de inspecionar tráfego criptografado por SSL/TLS ou seu desempenho é tão baixo que elas se tornam inutilizáveis ao realizar a inspeção. A inspeção de tráfego de HTTPS por um firewall de próxima geração (NGFW) requer seis processos adicionais de computação, em comparação à inspeção de tráfego de texto sem formatação.

Os dois processos que mais afetam o desempenho são:

- Estabelecer uma conexão segura
- Descriptografar e voltar a criptografar o tráfego para uma troca de dados seguros

A queda do desempenho pode ser alta em alguns casos, o que impede a inspeção de SSL/TLS para empresas que operam em sistemas de segurança legados.

A maioria dos ataques cibernéticos é oportunista e possui motivação financeira. Isso significa que todas as organizações correm o risco de serem comprometidas.

O que isso pode significar para a sua organização

Durante este ano, os invasores têm aproveitado o crescimento do tráfego de HTTPS e a falta de visibilidade. Um ataque utilizou um anúncio no Yahoo exatamente dessa forma e expôs quase 900 milhões de usuários a malware. Essa campanha redirecionava os visitantes do Yahoo para um site infectado pelo kit de exploit Angler. Mais 10 milhões de usuários provavelmente foram afetados nas semanas anteriores ao acessar anúncios publicados por uma empresa de marketing chamada "E-planning".

Conclusão

A criptografia está em todos os lugares e é considerada hoje como o vetor de ameaça favorito para os hackers. A sua segurança de rede precisa descriptografar o tráfego para interromper ameaças ocultas.

Saiba mais. Leia o nosso resumo da solução, *"Melhores práticas para impedir ameaças criptografadas"*.

[1] *E-paper de tecnologia da UBM: Segurança de próxima geração*

Sobre nós

Em uma história de mais de 25 anos, a SonicWall tem sido a parceira de segurança confiável do setor. Desde a segurança de rede até a segurança de acesso e de e-mail, a SonicWall tem evoluído continuamente seu portfólio de produtos, o que permite que as organizações inovem, acelerem e cresçam. Com mais de um milhão de dispositivos de segurança em quase 200 países e territórios no mundo todo, a SonicWall permite que seus clientes digam sim com confiança para o futuro.

Se você tiver dúvidas sobre o possível uso deste material, entre em contato com:

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

Acesse o nosso site para obter mais informações.
www.sonicwall.com

SolutionBrief-DarkSideOfEncryption-EU-IMAG-22649