http://www.cio.com.br

TECNOLOGIA

Cibercrime usa tráfego criptografado para esconder ameaças avançadas

(http://cio.com.br/tecnologia/2015/09/22/cibercrime-usa-trafego-criptografado-para-esconder-ameacas-avancadas)

Marcos Oliveira *
Publicada em 22 de setembro de 2015 às 14h02

A saída para endereçar o problema das ameaças embutidas na encriptação SSL é, sem sombra de dúvidas, inspecionar o tráfego

Quase um terço do tráfego empresarial da Internet já é criptografado e essa proporção está crescendo rapidamente. É bom que seja assim, mas a primeira grande questão que isso traz é que as empresas perderam a visibilidade desse tráfego justamente por estar criptografado.

A criptografia é necessária, pois ajuda a proteger a privacidade dos dados, mas agora os criminosos cibernéticos aprenderam a esconder-se e a mascarar seus ataques no tráfego SSL (Secure Sockets Layer) -- e seu sucessor, o TLS (Transport Layer Security) -- que são protocolos padrão de criptografia para as comunicações via web, nuvem e dispositivos móveis. Os cibercriminosos fazem isso porque sabem muito bem que os dispositivos de segurança perimetral são incapazes de identificar a intrusão, tanto é que cerca de 50% das novas ameaças chegam por meio do SSL, estima o Gartner.

Isso levanta várias questões:

1- As empresas devem desistir de criptografar seus dados?

2 - Se não, como podem se proteger desse tipo de ataque?

3 - Como inspecionar o tráfego SSL em busca de ameaças sem perder performance e produtividade da rede?

4 - Como inspecionar o tráfego sem violar a privacidade do usuário e as regras de compliance/políticas de governança corporativa?

Bem, antes de mais nada é importante destacar que a criptografia continua sendo uma solução eficaz para proteger a privacidade dos dados. Ainda que criminosos escondam ameaças nesse tráfego, não poderão descriptografá-lo facilmente e violar a sua privacidade. Não por acaso, milhares de aplicações usam criptografia SSL, incluindo Gmail, Microsoft SharePoint, Microsoft Exchange, Facebook, LinkedIn, Youtube, Salesforce.com, Amazon Web Services (AWS), Google Apps, entre outras.

Veja os benefícios.

Sessões de usuário criptografadas: O protocolo SSL criptografa informações sigilosas enviadas pela Internet para que somente o destinatário possa compreendê-las.

Autenticação facilitada: Quando um servidor incorpora um certificado SSL, os usuários podem estar confiantes de que os seus dados sigilosos não cairão em mãos erradas e só serão usados pelo servidor seguro apropriado.

Proteção contra phishing: Frequentemente, os e-mails de phishing e spearphishing contêm links que levam os usuários incautos a réplicas malignas, mas convincentes de websites confiáveis. Entretanto, ao conectar-se a websites falsos e ver mensagens de "autoridade certificadora não confiável", a maioria dos usuários sai do website sem compartilhar informações confidenciais.

Maior confiança do cliente: Consumidores que levam a segurança a sério e clientes comerciais ficam tranquilos ao fazer negócios pela Internet com a segurança do protocolo SSL. Isso se evidencia, por exemplo, na atitude do Google de atribuir, segundo o seu mecanismo de busca, uma melhor classificação aos websites criptografados com SSL/HTTPS do que aos não criptografados.

Embora os benefícios da criptografia SSL sejam maiores do que as desvantagens – tipicamente, custo adicional e necessidades de desempenho – esses novos riscos agora são uma realidade e devem ser tratados. Os hackers e a Deep Web não podem mesmo descriptografar o tráfego SSL na velocidade que compense para o crime, pois quebrar uma chave criptográfica leva muito tempo; mas eles podem e estão escondendo ameaças que ficarão adormecidas em sua rede até que acordem um dia e abram portas para a invasão externa.

80% das empresas não inspecionam seu tráfego SSL

A saída para endereçar o problema das ameaças embutidas na encriptação SSL é, sem sombra de dúvidas, inspecionar o tráfego. O Gartner estima que 80% das empresas não inspecionam seu tráfego SSL. Já uma pesquisa feita no Brasil com cerca de 50 grandes empresas de diversos segmentos, encomendada pela Blue Coat, revelou que 73% não inspecionam seu tráfego encriptado. Se as empresas não mitigarem os riscos através da visibilidade na camada SSL, poderão se abrir a malwares e ao acesso indevido de dados.

A maioria dos dispositivos de segurança de rede é incapaz de inspecionar o tráfego SSL, a menos que esse tráfego seja previamente descriptografado. Sem isso, os malwares podem facilmente obter acesso à rede e causar grandes danos. Não descriptografar o tráfego também reduz a eficiência de outros investimentos em segurança, como sistemas de detecção e prevenção de intrusão (IDS/IPS) e tecnologias de prevenção de perda de dados (DLP).

Esse problema tem continuidade em cenários pós-ataque ou de invasão, nos quais as empresas dependerão de ferramentas de perícia de rede -- também denominadas Security Analytics -- para analisar a atividade da rede e investigar as causas e os efeitos de ameaças avançadas. Entretanto, sem a capacidade de descriptografar o tráfego da rede, eles são incapazes de obter todas as provas periciais necessárias para avaliar o efeito e até a origem de um ataque bem sucedido.

Outra questão fundamental é que as empresas que se decidirem por inspecionar seu tráfego SSL deverão fazê-lo sem quebrar regras de compliance. Por exemplo, não se pode descriptografar dados pessoais, financeiros e de saúde, de acordo com os requisitos do HIPAA (Health Insurance Portability and Accountability Act), PCI Security Standards Council e PII Laws (Personally Identifiable Information). Do ponto de vista de conformidade não pode haver nenhuma mudança ou manipulação do dado inspecionado que quebre a sua integridade. Exatamente por isso a ferramenta escolhida deverá acatar e se ajustar às políticas de governança interna e externas que regulam os mercados

Acreditamos que somente a adoção de uma estratégia holística de administração de tráfego criptografado pode reduzir esses novos riscos. Estamos falando das soluções de ETM - Encrypted Traffic Management. Essa estratégia inclui dispositivos de visibilidade de SSL que não apenas monitoram, mas gerenciam a partir de pontos centralizados -- com excelente relação custo-benefício -- a inspeção e a descriptografia de tráfego SSL, ao mesmo tempo em que obedecem às exigências de privacidade e conformidade e defende as redes contra ameaças avançadas sem perder performance.

Os cibercriminosos continuarão a esconder malwares e a buscar novos caminhos para ter acesso às redes e aos dados das empresas. O protocolo SSL continuará a ser usado como importante componente para proteger a privacidade. Às empresas resta se prevenir com a adoção de tecnologias inteligentes, flexíveis e com controle de políticas antes que percam mais que dados, mas sua reputação e credibilidade.

(*) Marcos Oliveira *é Country Manager da Blue Coat Brasi*