CONHEÇA AS AMEAÇAS CRIPTOGRAFADAS

Como criminosos cibernéticos ocultam ataques na sua rede com SSL/TLS

Resumo

A tecnologia de criptografia, como SSL/TLS e HTTPS, oferece proteção contra hackers e seu uso cresce exponencialmente. Mas os criminosos cibernéticos aprenderam a aproveitar a criptografia como um método eficaz para ocultar malware, ransomware, spear-phishing, zero-day, extração de dados, sites invasores e outros ataques. Felizmente, a segurança de rede avançada com inspeção profunda de pacotes de tráfego SSL/TLS e HTTPS está agora disponível para proteger contra ameaças criptografadas.

Tipos de ameaças criptografadas

A criptografia oferece proteção para tráfego legítimo, assim como meios para que ataques cibernéticos passem despercebidos. Em termos simples, o SSL (Secure Sockets Layer) Camada de Conexão Segura pode cria um túnel criptografado para proteger dados através de um VPN. O TLS (Transport Layer Security) é uma versão atualizada e mais segura do SSL. O HTTPS (Hyper Text Transfer Protocol Secure) aparece no URL quando um site é protegido por um certificado SSL.

Existem várias categorias de ameaças criptografadas. Uma categoria inclui ameaças como vulnerabilidades de certificados. Nesse caso, quando você estiver usando um site, poderá ver um alerta no seu navegador ou uma aplicação com uma mensagem de que a conexão foi determinada como insegura ou não confiável. Nessas situações, a certificação não foi aprovada. A Certificate Authority pode estar inacessível ou o certificado pode ser inválido. Ou a criptografia é menor do que a desejável, independentemente de ser uma forma mais antiga de SSL (já desvalorizada), uma forma inferior de TLS ou assinaturas e hashes que não correspondem aos padrões de criptografia atuais.

Outra categoria de ameaça criptografada inclui malware que incorpora todas comunicações dentro de um túnel criptografado, para que ele possa passar pela segurança da sua rede. Exemplos de aplicações que ofuscam seu tráfego e comunicações de forma deliberada incluem Psiphon, Tor e Ultrasurf.

Também há violações reais do tráfego criptografado, malware que rouba credenciais, como DROWN, Heartbleed, PODDLE e FREAK. Elas são exploits que aproveitam a própria criptografia para jogar man-in-the-middle e interceptar seus e-mails, credenciais, informações privadas, dados de transações on-line, etc. Quando esse tipo de ataque compromete sua rede, ele pode ser usado contra você posteriormente ou incorporar a ameaça dentro das próprias comunicações ao encaminhá-lo a sites de terceiros ou injetar aplicações mal-intencionadas nas suas conexões do navegador.

A história das ameaças criptografadas

Entenda a história para saber o que é realmente necessário para se proteger contra essas ameaças. O modelo de segurança de firewall legado dos anos 90 e início dos anos 2000 é a tecnologia Stateful Packet Inspection (SPI). Na verdade, ainda existem milhões de firewalls SPI na Internet hoje em dia.

O SPI é semelhante a um oficial de trânsito que pode parar ou permitir o tráfego em uma interseção. O oficial só pode ver informações externas sobre os veículos, como marca e modelo, placa do carro e a direção em que os veículos se movem, mas nada que esteja escondido no banco de trás, sob o capô ou no porta-malas. Então, se houver algo mal-intencionado escondido nesses lugares, o policial não saberá.

> A Internet se move rapidamente na direção de um modelo completamente criptografado.

Em contrapartida, o Deep Packet Inspection (DPI), que forma a base para os firewalls de última geração, permite que os firewalls inspecionem na camada 7. É como se o nosso agente de trânsito tivesse uma visão de raio-x para ver esses lugares escondidos nos veículos e então decidir qual pode passar ou não.

No entanto, com essa analogia, a visão de raio-x do policial ainda não consegue enxergar através do lead (que nesse caso é o HTTPS). Para superar essa limitação, o DPI deve incluir a capacidade de inspecionar o tráfego SSL criptografado (DPI-SSL).

O enorme crescimento do tráfego HTTPS criptografado

Seja devido ao "efeito Snowden", ao escândalo de espionagem da NSA ou simplesmente aos melhores esforços para proteger a privacidade on-line contra possíveis invasores e ladrões, uma quantidade significativa do tráfego da Internet hoje é criptografado via HTTPS.

Uma conexão HTTPS é essencialmente uma conexão segura ou privada da aplicação iniciadora (geralmente um navegador) até a rede e a Internet ao servidor ou site de destino. Essas conexões HTTPS incluem webcasts, pesquisas on-line, aplicações de produtividade cloud-based, e-mail baseado na Web, etc. HTTPS é basicamente uma VPN. É uma conexão da Web criptografada do seu navegador até o destino. Por ser uma VPN, você não pode ver dentro dela. Não é possível inspecionar o tráfego que passa pelo HTTPS, determinar a chegada de um malware prejudicial ou o vazamento de dados confidenciais da rede.

A Internet se move rapidamente na direção de um modelo completamente criptografado. Agora existem grandes iniciativas para "criptografar tudo" e até mesmo os principais mecanismos de pesquisa alteraram seus algoritmos para priorizar sites HTTPS em seus resultados. Por exemplo, um varejista on-line pode ter dezenas de milhares de cliques por mês mais do que outro, mas se não estiver usando HTTPS em sua página de entrada, os resultados da pesquisa o colocarão abaixo do concorrente de desempenho inferior, mas que usa HTTPS em sua página de entrada.

Mais da metade das aplicações da Web estão agora em HTTPS. Todas as principais aplicações, como Office 365, YouTube, Amazon, SAP, Salesforce, Skype, Dropbox, Twitter e Gmail, usam criptografia. Analistas líderes preveem que até o próximo ano, 65% do tráfego mundial da Internet será criptografado. Para colocar isso em perspectiva, se você tiver uma conexão de Internet de 100 Mbps, cerca de 65 Mbps desse tráfego não será inspecionado. Ao longo de uma hora, são cerca de quatro a sete DVDs de dados transferidos sem inspeção. Em algumas redes, a quantidade total de dados confidenciais de propriedade pessoal e intelectual pode ser inferior a isso. Considere o impacto de não conseguir ver todos esses dados que entram ou saem da sua rede.

E isso é apenas tráfego típico da Internet. A implementação média de HTTPS é de 60 a 80%, dependendo do setor. Por exemplo, se você for do setor financeiro, jurídico ou de saúde, a maioria dos seus sites já está criptografado.

Uso criminal de criptografia

Enquanto o tráfego criptografado aumenta a segurança nas comunicações diárias, os criminosos cibernéticos aproveitam a privacidade do HTTPS para ocultar seus ataques. Eles aprenderam a manipular a criptografia para contornar a maioria das soluções de firewall legadas. Dessa forma, grande parte do tráfego HTTPS de hoje em dia não é inspecionado, e até mesmo os firewalls comprados recentemente podem não ser capazes de inspecionar o volume do tráfego criptografado atual. Com a maioria do tráfego invisível ao seu firewall, não é uma questão de se ou mesmo quando. Provavelmente a sua rede já foi comprometida.

As violações no Yahoo, IRS e Ashley Madison que saíram nas manchetes envolviam criptografia. Em um caso, mais de um bilhão de contas de e-mail comprometidas resultaram de um único e-mail criptografado por um único funcionário.[1] Da mesma forma, a violação do OPM (na qual mais de 20 milhões de pessoas tiveram suas informações confidenciais vazadas on-line) teve origem em um único download de e-mail pessoal que não foi inspecionado e continha malware.[2] O tráfego criptografado pode conter malware, dados confidenciais vazados de forma acidental ou intencional ou um ataque de spear-phishing contra o CFO para que ele envie um pagamento por transferência eletrônica. Veja a seguir apenas alguns exemplos de ameaças ocultas no tráfego criptografado.

[1] https://www.wsj.com/articles/yahoo-discloses-new-breach-of-1-billion-user-accounts-1481753131

[2] https://www.wsj.com/articles/opm-breach-exposed-19-7-million-background-clearance-forms-1436469626

Malware criptografado por e-mail

Como você impede que um usuário clique em um anexo de e-mail que libera malwares em sua rede? No caso do malware, como o Cryptolocker, ele contém um payload mal-intencionado baixado dentro do webmail ou de outras comunicações criptografadas. Se estiver criptografado, você não poderá inspecioná-lo, controlá-lo e bloqueá-lo. Para bloquear e-mails mal-intencionados, ou seus anexos ou links clicados, você precisaria ser capaz de capturar o tráfego criptografado, descriptografá-lo e inspecioná-lo.

Ransomware criptografado

O principal tipo de malware criptografado atualmente é o ransomware (como WannaCry, CryptoLocker, Zeus, Chimera e Tesla). O ransomware faz uso da criptografia de várias maneiras. A primeira é a entrega real do ransomware em uma comunicação criptografada, seja ela um e-mail, sites de redes sociais, aplicações de mensagens instantâneas ou mensagens de texto. Uma vez entregue por meio de comunicação criptografada, o ransomware geralmente é executado e, em seguida, passa para um servidor de comando e controle (C&C) dentro de outra comunicação criptografada. Portanto, além de a entrega do payload real ser criptografado, as comunicações voltam ao servidor C&C.

Ataques de spear-phishing criptografados

Em um ataque típico de spear-phishing, um usuário faz login em seu e-mail criptografado, abre um e-mail de spear-phishing que parece ser de um colega de confiança, clica em um link HTTPS e executa um arquivo baixado. Os dados do notebook desse usuário são imediatamente criptografados e tornados inacessíveis. Uma tela de aviso solicita o pagamento de um resgate para acessar o arquivo.

De acordo com a US-CERT, mais de US$ 5 bilhões foram desviados das empresas no ano passado devido a ataques de phishing e whaling. O FBI estima que essas perdas tenham ultrapassado US$ 1 trilhão desde 2014. O FACC foi comprometido em US$ 54 milhões em um único ataque de phishing.[3] E esses ataques continuam diariamente.

Sites mal-intencionados criptografados

Só porque um site é criptografado com HTTPS não significa que ele seja seguro. Muitos sites criptografados são mal-intencionados e contêm ameaças zero-day sem assinaturas de firewall correspondentes. Sem essas assinaturas, o firewall pode não reconhecer o malware correspondente no site. Recentemente, a US-CERT relatou 19 novos CVEs (Common Vulnerabilities and Exposures) dentro do sistema operacional Google Android em uma semana, inclusive 11 vulnerabilidades altas e 7 críticas.

Ataques zero-day criptografados

> As principais violações que saíram nas manchetes nos últimos cinco anos foram todas criptografadas ou entregues por meio de payload criptografado.

Embora você tenha uma solução antivírus muito eficiente em sua rede, não terá sempre as assinaturas a tempo de se proteger contra exploits de zero-day. Um malware de zero-day é um código que foi escrito talvez momentos antes do ataque e nunca foi visto antes, portanto, nenhum firewall tem uma assinatura para ele e a capacidade de evitá-lo. O malware pode realmente entrar na rede e desativar o cliente de antivírus. As primeiras linhas de código do vírus são projetadas para desativar a solução antivírus e, em seguida, o malware é detonado. A US-CERT informou recentemente que até mesmo o Microsoft Defender AV integrado foi comprometido para permitir a exploração externa.

Conclusão

Felizmente, existem soluções para combater a exploração mal-intencionada de HTTPS, ao mesmo tempo que mantém a capacidade de criptografar o tráfego antes de ele ser visto por hackers. **Saiba mais** sobre as soluções de ameaças criptografadas avançadas e abrangentes da SonicWall em nossa folha de dados, Descriptografia e inspeção de tráfego criptografado (Decryption and Inspection of Encrypted Traffic).

[3] http://www.securityweek.com/cybercriminals-steal-54-million-aircraft-parts-maker

© 2017 SonicWall Inc. TODOS OS DIREITOS RESERVADOS.

SonicWall é uma marca comercial ou marca registrada da SonicWall Inc. e/ou de suas afiliadas nos Estados Unidos e/ou em outros países. Todas as outras marcas comerciais e registradas são de propriedade de seus respectivos proprietários.

As informações deste documento são fornecidas em relação aos produtos da SonicWall Inc. e/ou de suas afiliadas. Este documento, de forma isolada ou em conjunto com a venda de produtos SonicWall, não concede nenhuma licença, expressa ou implícita, por preclusão ou de outra forma, a qualquer direito de propriedade intelectual. SALVO CONFORME DEFINIDO NOS TERMOS E CONDIÇÕES ESPECIFICADOS NOS CONTRATOS DE LICENÇA PARA ESTE PRODUTO, A SONICWALL E/OU SUAS AFILIADAS NÃO ASSUMEM QUALQUER RESPONSABILIDADE E RENUNCIAM A QUALQUER GARANTIA, EXPRESSA, IMPLÍCITA OU ESTATUTÁRIA, RELACIONADA AOS SEUS PRODUTOS, INCLUINDO, ENTRE OUTROS, A GARANTIA IMPLÍCITA DE COMERCIALIZAÇÃO, ADEQUAÇÃO A DETERMINADO PROPÓSITO OU NÃO VIOLAÇÃO. EM HIPÓTESE ALGUMA A SONICWALL E/OU SUAS AFILIADAS SERÃO RESPONSÁVEIS POR QUAISQUER DANOS DIRETOS, INDIRETOS, CONSEQUENCIAIS, PUNITIVOS, ESPECIAIS OU INCIDENTAIS (INCLUINDO, SEM LIMITAÇÃO, DANOS POR PERDA DE LUCROS, INTERRUPÇÃO DE NEGÓCIOS OU PERDA DE INFORMAÇÕES), DECORRENTES DO USO OU IMPOSSIBILIDADE DE UTILIZAR ESTE DOCUMENTO, MESMO QUE A SONICWALL E/OU SUAS AFILIADAS TENHAM SIDO AVISADAS DA POSSIBILIDADE DE TAIS DANOS. A SonicWall e/ou suas afiliadas não se responsabilizam por qualquer garantia ou declaração referente à exatidão ou à integridade deste documento e reservam-se o direito de fazer alterações em especificações e descrições de produtos a qualquer momento, sem aviso prévio. A SonicWall Inc. e/ou suas afiliadas não se comprometem em atualizar as informações contidas neste documento.

Sobre nós

A SonicWall tem combatido a indústria do crime cibernético por mais de 25 anos, defendendo desde pequenas e médias empresas até grandes corporações mundialmente.A nossa combinação de produtos e parceiros propiciou uma solução de defesa cibernética em tempo real, associada às necessidades específicas de mais de 500.000 empresas globalmente, em mais de 150 países, permitindo que você faça mais em seus negócios com menos preocupações.

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

© 2017 SonicWall Inc. TODOS OS DIREITOS RESERVADOS. SonicWall é uma marca comercial ou marca registrada da SonicWall Inc. e/ou de suas afiliadas nos Estados Unidos e/ou em outros países. Todas as outras marcas comerciais e registradas são de propriedade de seus respectivos proprietários.