RESUMO DA SOLUÇÃO

Não Caia na Rede de um Hacker:

Proteja sua Empresa contra Ataques de Phishing com a WatchGuard

Introdução

Os ataques de phishing continuam a ser uma preocupação importante para pequenas empresas e organizações de médio porte. Na verdade, 83% das empresas afirmam ter sido vítimas de um ataque de phishing apenas no último ano.[1] Isso não é uma surpresa. Afinal, esses ataques são de simples execução e especialmente rentáveis quando bem-sucedidos.

Mas há uma boa notícia para os administradores de TI: com um pouco de educação sobre phishing e uma defesa em camadas, é possível proteger sua empresa de um ataque de phishing.

O que É Phishing?

O tipo mais comum de ataque de phishing é quando um criminoso envia um e-mail fingindo ser outra pessoa ou exercer determinado cargo para extrair dados confidenciais dos alvos. Eles costumam usar táticas para provocar medo, despertar curiosidade ou gerar uma sensação de urgência com o objetivo de obrigar o alvo a abrir um anexo ou clicar em um link malicioso.

O que pode ser ainda mais eficaz para um hacker é realizar um ataque de spear phishing altamente direcionado (e-mails que incluem informações específicas sobre o alvo). Os invasores geralmente pesquisam o alvo em canais de mídia social como LinkedIn e Facebook para criar um perfil da vítima desejada que os ajude a elaborar uma mensagem personalizada a fim de aumentar suas chances de sucesso.

Defesa contra Ataques de Phishing

Os programas mais bem-sucedidos contra phishing têm quatro componentes: proteção, educação, avaliação e comunicação. Essas quatro etapas funcionam juntas para usar sua equipe como um escudo humano, possibilitado pela tecnologia.

A proteção contra phishing requer uma abordagem em camadas da segurança cujo objetivo é manter os usuários seguros na Internet. A base dessa abordagem em camadas inclui:

- Monitoramento e bloqueio de solicitações DNS de saída maliciosas para garantir que os funcionários não possam acessar sites prejudiciais por meio de links suspeitos nem se comunicar por meio de canais de comando e controle.
- Ferramentas de varredura para garantir que arquivos maliciosos não consigam entrar na rede e segurança de endpoint que pode detectar e eliminar malware.
- Soluções de sandbox em nuvem que permitem destruir arquivos suspeitos em um ambiente virtual emulado que imita um endpoint autêntico para descobrir intenções maliciosas.
- Autenticação multifator para proteger contra fraudes, roubos de identidades e de credenciais.

Também é fundamental oferecer regularmente educação sobre phishing para os funcionários, juntamente com a avaliação de suas taxas de cliques. Há uma variedade de opções gratuitas e pagas disponíveis para treinamentos, inclusive sessões de treinamento de conscientização sobre computadores, exercícios de simulação de e-mail de phishing e até mesmo o simples compartilhamento com a equipe de vídeos e cartazes educativos sobre phishing. As empresas com funcionários bem treinados que passam por testes de phishing regulares e

[1] https://www.proofpoint.com/us/resources/threat-reports/state-of-phish

monitorados com precisão podem ter uma taxa de suscetibilidade baixa, de 5%.[2]

Como parte do processo educativo, é importante informar sua equipe sobre o destino de encaminhamento de e-mails suspeitos. Normalmente, o e-mail suspeito deve ser encaminhado para a equipe de assistência ou para a TI. Esses e-mails são muito úteis para entender o método de um ataque e sua autoria. Ao coletar e examinar os materiais de phishing, é possível perceber tendências em relação a como a empresa está sendo atacada (e-mails do Office 365, faturas falsas etc.) e quem (Vendas, P&D, RH) são os alvos. O autor do ataque está mostrando suas cartas, e nós podemos usar isso para direcionar nosso programa de segurança e oferecer uma proteção superior.

Proteção contra Phishing da WatchGuard

Toda empresa tem funcionários que não são muito cuidadosos com os cliques. Mesmo se um percentual baixo de seus funcionários for propenso a clicar em links perigosos ou fazer download de anexos infectados, é necessário ter os serviços certos de segurança em funcionamento. Com a WatchGuard, você pode proteger os usuários finais de um ataque e, ao mesmo tempo, reforçar a educação sobre phishing.

Proteção contra "Happy Clickers"

O DNS é o Commtouch da Internet e funciona como uma lista telefônica que de fato traduz nomes de domínio para endereços IP. O DNS permite que o usuário médio navegue até google.com em vez de inserir um endereço IP numérico. O DNS é quase sempre o primeiro passo no processo de conexão com a Internet e é usado por quase todos os dispositivos que precisam de uma conexão. Também é uma das ferramentas preferidas dos hackers que enganam usuários e redirecionam o tráfego para servidores maliciosos, falsificando o registro DNS de sites legítimos.

Como primeira linha de defesa, inspecionar cada solicitação de DNS para determinar qual é malicioso e qual é legítimo pode impedir que o clique arriscado de um usuário se transforme em um grande incidente de segurança. Com as soluções de segurança de nível DNS baseadas em nuvem da WatchGuard, as solicitações DNS maliciosas são detectadas e bloqueadas automaticamente com base nas informações mais recentes sobre ameaças.

A WatchGuard Oferece Dois Tipos de Proteção de Nível DNS:

- DNSWatch – Incluído no Total Security Suite, o DNSWatch oferece proteção com o Firebox da WatchGuard para todos os usuários conectados à sua rede.
- DNSWatchGO – Oferece proteção leve e sempre ativada contra phishing e malware para usuários em qualquer lugar.

As duas ofertas oferecem treinamento imediato de conscientização de segurança aos usuários quando eles encontram um phishing para reforçar a educação sobre segurança que você já proporcionou. Lembrar os funcionários sobre o treinamento no momento em que eles clicam em um link ou anexo é a forma mais eficaz de impedir que isso aconteça novamente. Uma mensagem customizada é exibida juntamente com esse treinamento, talvez solicitando que entrem em contato ou que encaminhem o e-mail que originou o clique.

Defesa contra Fraudes, Roubo de Identidades e de Credenciais

Uma das maneiras mais eficazes de os hackers violarem uma rede é por meio de credenciais perdidas. Isso permite ao invasor ter acesso total aos recursos corporativos e até mesmo se passar pela vítima para causar mais danos. Considerando a prevalência do malware que rouba credenciais e o fato de que a criação de senhas fracas é algo cada vez mais comum, já não é mais possível confiar apenas em nomes de usuário e senhas.

O WatchGuard AuthPoint permite controlar o acesso a ativos, contas e informações com a autenticação multifator. O AuthPoint acrescenta uma camada adicional de certificação se comparado com a autenticação simples de nome de usuário e senha. O login com o AuthPoint é feito por meio de um telefone celular e requer algo que você saiba (senha), que você tenha (telefone celular) e que seja seu (impressão

[2] https://siliconangle.com/blog/2017/11/30/phishing-attacks-cost-1-6m-average-enterprises-successfully-fighting-back/

digital, biometria) para autenticar um usuário. Entregue a partir da nuvem, o AuthPoint permite eliminar o risco de senhas fracas ou roubadas.

Eliminação de Malware que Rouba Credenciais

O malware que rouba credenciais ou que tenta roubar nomes de usuário e senhas é comum e faz parte das 10 principais ameaças de malware encontrados pelas empresas médias.[3] Não é possível detectar e eliminar essas e outras ameaças de malware apenas com um antivírus baseado em assinatura.

A WatchGuard Oferece Várias Soluções de Segurança para Detectar e Eliminar Malware:

- **Gateway AntiVirus e IntelligentAV** – Quando um usuário estiver conectado por meio da sua rede, o WatchGuard Gateway AntiVirus e o IntelligentAV baseado em IA examinam os arquivos e o tráfego que flui pelo Firebox para identificar malware e riskware. Se uma ameaça é detectada, a conexão é bloqueada ou o arquivo é separado. Isso protege os funcionários de anexos maliciosos incluídos em um ataque de phishing, impedindo que eles cheguem a usuários finais ansiosos por um clique.
- **APT Blocker** – O WatchGuard APT Blocker oferece uma camada adicional de proteção contra ameaças evasivas e de dia zero que atingem a sua rede, como as de ataques de spear phishing altamente direcionados. O APT Blocker executa o arquivo em um ambiente de sandbox em nuvem e analisa seu potencial de ameaça. Os arquivos maliciosos são postos em quarentena e os administradores do sistema são alertados sobre a ameaça.
- **ThreatSync** – O ThreatSync é um mecanismo de pontuação e correlação de ameaças com base em nuvem da WatchGuard que melhora a detecção e a resposta em todo o ambiente, da rede ao endpoint. Se um malware for detectado, o ThreatSync passará a conter o host, colocará o arquivo em quarentena, eliminará os processos associados e excluirá a persistência da chave de registro.

[3] https://www.watchguard.com/wgrd-about/press-releases/new-security-research-reveals-password-inadequacy-top-threat-need-mfa

Sobre a WatchGuard

A WatchGuard® Technologies, Inc. é líder global em segurança de rede, Wi-Fi seguro, autenticação multifator e inteligência de rede. Os premiados produtos e serviços da empresa são adotados em todo o mundo por cerca de 10 mil revendedores de segurança e prestadores de serviços, para proteger mais de 80 mil clientes. A missão da empresa é tornar a segurança corporativa simples e acessível a empresas de todos os tipos e tamanhos, o que faz da WatchGuard a solução ideal para médias empresas e empresas distribuídas. A WatchGuard tem sede em Seattle, Washington, EUA, com escritórios na América do Norte, Europa, Ásia Pacífico e América Latina. Para saber mais, acesse WatchGuard.com.

Para obter mais informações gerais, de promoções e de atualizações, siga a WatchGuard no Twitter @WatchGuard, no Facebook ou na página do LinkedIn. Acesse também nosso blog InfoSec, Secplicity, para obter informações em tempo real sobre as últimas ameaças e como lidar com elas em www.secplicity.org.

VENDAS NOS EUA 1.800.734.9905 VENDAS INTERNACIONAIS +1.206.613.0895 www.watchguard.com/br