proofpoint.

Ataques a cadeias de fornecimento

Fatos breves

DESCRIÇÃO

Os ataques a cadeias de fornecimento dividem-se em duas categorias principais: fraude de e-mail e software de terceiros. Nesses ataques, criminosos cibernéticos comprometem fornecedores e provedores de serviços para atacar seus clientes e parceiros. O comprometimento inicial do fornecedor costuma ser por phishing ou por malware. Uma vez dentro do sistema do fornecedor, os atacantes podem praticar uma impostura de contas de e-mail para iniciar phishing, fraude de fatura ou outros tipos de ataque contra os clientes. Após invadir os sistemas dos clientes, eles podem roubar dados confidenciais, instalar ransomware ou utilizar o acesso para desencadear mais uma onda de ataques de phishing ou de fraude de e-mail.

FERRAMENTAS DE TRABALHO

As ameaças contra cadeias de fornecimento costumam envolver phishing de credenciais (sequestro de contas), malware (Stuxnet, NotPetya, Sunburst, Kwampirs) e ameaças de impostura, como comprometimento de e-mail corporativo (BEC).

TIPOS

- **Comprometimento de e-mail corporativo (BEC ou fraude de e-mail).** Os atacantes fazem-se passar por uma pessoa da confiança do destinatário — normalmente um parceiro comercial, fornecedor ou vendedor. O destinatário é solicitado a fazer uma transferência bancária, pagar uma fatura falsa ou modificada, desviar fundos de pagamento de salários ou alterar dados bancários de pagamentos futuros. Em alguns esquemas de fraude de e-mail, o atacante pode comprometer a conta de e-mail do próprio fornecedor para se passar por este e até entrar em conversas de e-mail já existentes.
- **Ataques a cadeias de fornecimento de software.** Os atacantes obtêm acesso aos sistemas de um provedor de serviços gerenciados ou de software e infectam compilações futuras, posteriormente distribuídas para clientes e parceiros. Tais ataques são raros em comparação com as formas citadas anteriormente, mas podem afetar múltiplas vítimas com uma única violação.

FATORES DE RISCO

- Interagir com fornecedores ao procurar serviços profissionais ou consultoria
- Não adotar uma proteção de cibersegurança adequada
- Oferecer acesso a pessoal negligente ou sem treinamento para conscientização quanto à segurança
- Complexidade da cadeia de fornecimento — as empresas dependem cada vez mais de uma variedade de plataformas de nuvem e serviços SaaS

Ataques a cadeias de fornecimento nas manchetes

Target pagará US$ 18,5 milhões por violações de dados de 2013 que afetou 41 milhões de consumidores

Credenciais de contas roubadas de um dos fornecedores da Target permitiu que os atacantes invadissem os sistemas da gigante varejista e roubassem informações de pagamento confidenciais de mais de 41 milhões de consumidores.

Hackers atacam cadeia de fornecimento de vacinas para COVID-19

Um ataque de phishing visou executivos de 44 empresas em vários continentes em uma tentativa de comprometer a cadeia global de fornecimento de vacinas para COVID-19.

Organização comunitária sem fins lucrativos de apoio a pessoas sem teto perde US$ 1,2 milhão em fraude de BEC

Os atacantes falsificaram o domínio de um fornecedor para roubar quase £1 milhão de uma associação de moradia cooperativa perto de Londres, no Reino Unido.

Anatomia de um ataque a cadeias de fornecimento

1. **Infiltração**

   Os atacantes utilizam uma variedade de métodos para a violação inicial:

- Ataques de força bruta com ferramentas automatizadas para experimentar pares de nome de usuário e senha até que uma correspondência seja encontrada.

- Fazer-se passar por um contato confiável para enviar phishing, e-mails impostores e/ou links/anexos com malware, como keyloggers ou software para roubo de senhas.

- Sequestro da conta de um fornecedor confiável.

2. **Reconhecimento**

- Após roubar credenciais de login válidas, o atacante pode começar a explorar a rede e a reputação do fornecedor. Em busca de vítimas, ele monitora as comunicações entre o fornecedor e seus clientes.

3. **Ataque**

- Quando o reconhecimento está concluído, o atacante pode utilizar os sistemas do fornecedor comprometido para obter credenciais por meio de phishing, enviar faturas fraudulentas ou enviar malware para os clientes.

Insights de pesquisa

Ao longo de um período de uma semana em fevereiro de 2021, a Proofpoint analisou dados de 3.000 organizações de vários segmentos verticais nos EUA, Reino Unido e Austrália. Durante esse período, a ampla maioria sofreu ataques a cadeias de fornecimento.

98% receberam uma ameaça de um fornecedor que sofreu impostura ou que foi comprometido.

Os ataques foram igualmente distribuídos em todos os países e setores da amostra.

Dessas ameaças, quase três quartos envolveram phishing ou impostura.

Menos de 30% dos e-mails enviados de domínios de fornecedores continham malware.

COMO O "CRIME COMO SERVIÇO" ALIMENTOU OS ATAQUES A CADEIAS DE FORNECIMENTO

A Dark Web é um mercado notório para kits de exploração e malware personalizado utilizados para vender serviços, como aluguel de redes de bots e software para ransomware. Tal como a maioria dos provedores de SaaS, os criminosos cibernéticos fornecem ferramentas e plataformas para quem realiza ataques a cadeias de fornecimento, ataques de ransomware e outros crimes cibernéticos. Perpetradores de ameaças que carecem de habilidades técnicas avançadas agora podem realizar ataques facilmente.

Como proteger a sua organização

Para lidar com fraudes de cadeias de fornecimento e ataques a cadeias de fornecimento de software, seguem alguns controles de segurança fundamentais cuja implementação as organizações devem considerar.

Fraude de cadeias de fornecimento

Para fraude de faturas de fornecedores, as organizações devem adotar uma abordagem holística e multicamada, pois os atacantes frequentemente utilizam conjuntamente impostura de fornecedores e contas comprometidas de fornecedores.

Para fraude de faturas de fornecedores, as organizações devem adotar uma abordagem holística e multicamada, pois os atacantes frequentemente utilizam conjuntamente impostura de fornecedores e contas comprometidas de fornecedores.

O BEC costuma começar com um e-mail no qual o atacante faz-se passar por uma pessoa da confiança da vítima ou "realmente torna-se" essa pessoa comprometendo sua conta. Como não há carga maliciosa, os ataques de BEC são dificilmente detectados por gateways tradicionais que contam apenas com reputação e análise de malware em área restrita (sandbox) para detecção.

Veja como deter os ataques mais comuns — e mais caros — a cadeias de fornecimento.

Obtenha visibilidade sobre os riscos de fraude de e-mail do seu fornecedor
Para melhor compreender, comunicar e mitigar, obtenha respostas para as seguintes perguntas:

- Quais são os seus riscos de BEC?
- Quais usuários são os mais vulneráveis?
- Quais fornecedores constituem risco para suas organizações?
- O que devemos fazer para mitigar os riscos?

Você deve saber quais dos seus usuários são mais atacados por ameaças de impostura e quem é mais propenso a se deixar enganar por esses tipos de ameaças.

Ao mesmo tempo, ter visibilidade granular sobre detalhes de ameaças de BEC e identificar temas comuns de BEC, como fraude de fatura de fornecedor e desvio de pagamento de salários, pode ajudar você a compreender e a comunicar melhor o risco de BEC.

Detecte e bloqueie ameaças de impostura antes que elas entrem
Deter ataques de fornecedor realizados por e-mail significa revelar todas as táticas de fraude de e-mail, inclusive falsificação do nome exibido, domínios parecidos e fraude de fornecedor sofisticada. Procure uma solução que analise mensagens dinamicamente à procura de diversas táticas associadas à fraude de fatura de fornecedor, como:

- Alterações do endereço de resposta
- Uso de IPs maliciosos
- Uso de domínios parecidos com os do fornecedor
- Palavras ou frases frequentemente utilizadas nesses ataques de fraude de fornecedor

(A maioria dos produtos de segurança de e-mail conta apenas com correspondência de regras estáticas ou dados contextuais limitados que exigem ajustes manuais.)

Torne os usuários resilientes contra ataques de BEC em cadeias de fornecimento
O BEC visa pessoas e depende de que elas executem inadvertidamente o ataque. Como esses ataques impostores usam engenharia social e impostura, frequentemente os seus usuários se tornam a ultima linha de defesa. É por isso que a mitigação dos riscos de BEC exige tanto tecnologia quanto treinamento.

Treine os seus usuários para identificar e denunciar e-mails impostores suspeitos. Isso dará a eles o conhecimento e as habilidades necessárias para proteger sua organização contra ameaças ativadas por humanos.

Tags de advertência de e-mail podem ajudar a revelar o risco que cada e-mail representa. Por exemplo, avisar os usuários quando uma mensagem é enviada por um remetente externo ou de um domínio recém-registrado pode ajudá-los a tomar decisões mais informadas sobre e-mails incertos.

Proteja sua própria marca de ser utilizada em ataques de fraude de e-mail
Enquanto você se preocupa com o risco que os seus fornecedores podem representar, os seus próprios clientes podem ter preocupações semelhantes em relação a você.

Os atacantes podem colocar você contra os seus clientes e parceiros comerciais utilizando o nome e a marca da sua empresa para roubá-los. Ainda que falsificação da marca não cause perdas financeiras diretas para a sua organização, ela pode afetar a reputação da sua organização, abalar a confiança dos clientes e, em última instância, prejudicar seus negócios.

Evite o envio de e-mails fraudulentos utilizando autenticação de e-mail DMARC, tanto de e-mails enviados diretamente por você ou por terceiros designados.

Ataques a cadeias de fornecimento de software

Além dos ataques a cadeias de fornecimento mais comuns discutidos acima, o uso crescente de software gerenciado e terceirizado criou mais um tipo de risco para cadeias de fornecimento.

Se um fornecedor comprometido oferece software ou serviços de nuvem, atacantes podem alterar o código fonte e injetar malware nos processos de compilação e atualização. Programas ou serviços infectados são, então, distribuídos para clientes e parceiros, juntamente com a carga maliciosa incluída pelo atacante.

Os usuários raramente têm a capacidade de inspecionar os programas de terceiros que utilizam e, portanto, precisam que seus fornecedores de software tenham proteções fortes implementadas. Se uma organização recebe software comprometido, ela pode ficar aberta a toda sorte de ataques, de roubo de dados a infecção por ransomware.

Esse tipo de ataque é particularmente difícil de evitar. Vulnerabilidades de software não corrigidas são um dos vetores mais comuns de ataque cibernético. Por isso, atualizar o software até a versão mais recente é sempre uma prática recomendada. Agora, porém, isso também se tornou um vetor de ataque.

Saiba mais

Com ataques a cadeias de fornecimento dominando as manchetes, é evidente que serviços, fornecedores e prestadores terceirizados constituem um grave risco para a postura de segurança das organizações. Uma solução de segurança centrada em pessoas e que detecte novas ferramentas, alvos e táticas de ataque pode ajudar a mitigar esse risco.

Para saber mais sobre como deter efetivamente ataques a cadeias de fornecimento, visite **www.proofpoint.com**.