Como a Proofpoint defende contra ransomware

Evite que o ransomware se instale e se espalhe pela sua organização

Produtos

- Proofpoint Advanced Threat Protection
- Proofpoint Cloud Security

Principais vantagens

- Evitar uma infecção inicial
- Evitar descoberta, movimentação lateral e persistência
- Evitar vazamento de dados

O ransomware é, atualmente, uma das formas mais perturbadoras de ataque cibernético. Ele impede suas vítimas de trabalhar, obriga hospitais a recusar pacientes e paralisa governos inteiros. Ele evoluiu a ponto de se tornar a ameaça cibernética mais impactante de hoje em dia. Apenas no ano passado, os Estados Unidos sofreram mais de 65.000 ataques de ransomware. A ameaça é uma prioridade para CISOs e se tornou uma questão de segurança nacional. O mais alarmante é que muitas organizações estão completamente despreparadas para um ataque de ransomware. Apenas 13% dos especialistas de TI consultados pelo Ponemon Institute afirmaram que suas empresas conseguem evitar o ransomware. E mais de 68% consideram-se “vulneráveis” ou “muito vulneráveis”.[1]

O e-mail e a Web são os principais vetores de ataque do ransomware. A maioria dos ataques de ransomware atualmente ocorre em múltiplos estágios. Em tais ataques, o e-mail ou sites comprometidos desempenham um papel fundamental nos estágios iniciais da cadeia de ataque. Eles frequentemente entregam uma carga viral inicial, como um downloader de malware. Essas cargas virais são desenvolvidas para penetrar no sistema do usuário. Elas são frequentemente utilizadas para roubar credenciais e obter acesso à rede do usuário.
Os perpetradores de ransomware também utilizam credenciais roubadas para obter acesso a serviços expostos à Internet. Táticas comuns incluem e-mails de phishing de credenciais, uso de força bruta em senhas e comprometimentos de passagem (drive-by).

Uma vez obtido o acesso inicial, os perpetradores de ransomware estabelecem persistência, realizam reconhecimento e se movimentam lateralmente. Lá dentro, os atacantes não apenas criptografam arquivos confidenciais, mas também vazam informações sigilosas para uso em extorsão dupla.

Conforme medidas de backup e recuperação tornaram-se mais bem-sucedidas em frustrar ataques de ransomware, as táticas dos perpetradores de ameaças evoluíram para superá-las. Os perpetradores de ransomware agora estão utilizando o que chamamos de ransomware de extorsão dupla. Essa tática primeiro vaza dados confidenciais e, em seguida, criptografa os arquivos.

1 The Ponemon Institute. “The Rise of Ransomware” (A ascensão do ransomware). Janeiro de 2017.

Caso a organização vitimada se recuse a pagar para que os arquivos sejam descriptografados, o perpetrador de ameaças tem três maneiras de exigir o pagamento:

- Ameaçar a vítima com o vazamento dos dados on-line
- Vendê-los para quem pagar mais
- Enviar e-mails diretos para os clientes e parceiros da vítima ameaçando vazar seus dados

Como o e-mail é o ponto de infecção inicial na maioria dos ataques de ransomware, um grande percentual do ransomware começa, direta ou indiretamente, com um e-mail de phishing. Esses e-mails induzem os usuários a abrir um anexo malicioso ou a clicar em um URL malicioso. Você precisa de soluções avançadas para detectar e bloquear tais ameaças de maneira que elas não comprometam as credenciais dos usuários. Conforme cada vez mais dados da sua organização são armazenados na nuvem, o mesmo ocorre com dados sigilosos e arquivos de senhas. Limitar a exposição de dados na nuvem é importante para ajudar a minimizar o que é compartilhado com os perpetradores de ameaças.

A Proofpoint prevê que os ataques de ransomware passarão a ser mais direcionados, mais prejudiciais e cada vez mais perturbadores para operações empresariais. O Proofpoint Advanced Threat Protection e o Proofpoint Cloud Security podem ajudar a evitá-los. Nossas plataformas integradas e abrangentes reduzem o risco de ataques de ransomware ao dispor de camadas de controles para:

- Evitar uma infecção inicial
- Detectar acesso inicial e evitar descoberta, movimentação lateral e persistência
- Evitar vazamento de dados

Evite uma infecção inicial

O Proofpoint Advanced Threat Protection e o Proofpoint Cloud Security evitam infecções iniciais:

- Detectando e bloqueando downloaders de ransomware e malware que resultam em ransomware
- Evitando o comprometimento de credenciais
- Oferecendo visibilidade sobre os riscos do ransomware
- Isolando cliques em URLs com base no risco
- Treinando os usuários para que estes identifiquem e denunciem mensagens maliciosas
- Automatizando a remediação de ameaças de e-mail

Detecte e bloqueie downloaders de ransomware e malware

A plataforma Proofpoint Advanced Threat Protection detecta e bloqueia o ransomware como carga viral inicial. Ela também bloqueia o malware que resulta em ransomware. Nós oferecemos diversos mecanismos baseados em autoaprendizagem para detectar malware, código malicioso e técnicas de evasão de detecção. Isso protege os usuários contra sites maliciosos ou arquivos infectados por ransomware.

A plataforma realiza análises de reputação e de conteúdo. Ela também opera sandboxes (áreas restritas) para análise detalhada de ameaças baseadas em URLs e em anexos. Nós empregamos análises preditivas que identificam e isolam em uma área restrita URLs suspeitos com base em mudanças nas táticas dos atacantes. Por exemplo, como os atacantes frequentemente utilizam sites legítimos de compartilhamento de arquivos para hospedar malware, a plataforma isola em uma área restrita qualquer URL de compartilhamento de arquivos. Soluções que se baseiam somente em análises de reputação deixariam passar tais ataques.

Evite o comprometimento de credenciais

Os atacantes utilizam diversas táticas para roubar as credenciais de um usuário. Alguns métodos incluem phishing, ataques de força bruta, Dark Web e exposição de informações contidas no armazenamento de nuvem de um usuário. Quando um atacante obtém acesso às suas credenciais, não há mais necessidade de enviar um downloader. Ele pode simplesmente fazer login na sua VPN ou inscrever-se em serviços voltados para a Internet utilizando as suas credenciais. Assim eles podem roubar dados confidenciais ou criptografar arquivos. Conforme as organizações adotam serviços de nuvem adicionais, usuários negligentes podem fazer upload de arquivos de senhas e dados confidenciais para a nuvem.

O Proofpoint Advanced Threat Protection detecta e bloqueia mensagens de phishing utilizando múltiplos mecanismos de detecção, incluindo classificadores baseados em autoaprendizagem que inspecionam URLs. O Proofpoint Cloud Security pode identificar informações confidenciais expostas em contas de nuvem que os atacantes podem explorar.

Obtenha visibilidade sobre o seu risco de ransomware

A Proofpoint oferece visibilidade sobre suas Very Attacked People™ (VAP ou “pessoas muito atacadas”). VAPs são as pessoas da sua empresa mais expostas a ataques.

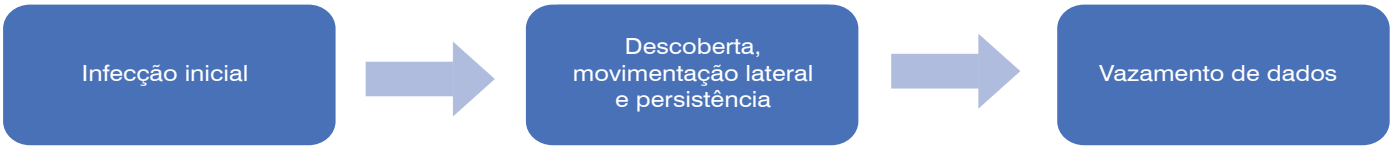

Figura 1. As três camadas de proteção.

Figura 2. A Proofpoint oferece visibilidade sobre suas Very Attacked People (VAP ou "pessoas muito atacadas").

Essa visibilidade revela quem é mais visado e quais ameaças os atingem. Os dados permitem ajustar a sua estratégia de defesa às ameaças específicas enfrentadas pelas suas VAPs.

A Proofpoint também fornece informações detalhadas sobre ameaças e campanhas. O dashboard de insights sobre ameaças mostra análises forenses detalhadas. Esses dados incluem o perpetrador da ameaça, a disseminação, amostras de mensagens, destinatário desejado, progressão do ataque etc.

Reduza o impacto com isolamento integrado do e-mail

Os atacantes podem utilizar como arma o que ocorre após a entrega dos URLs. Essa estratégia os ajuda a evitar a detecção inicial. Porém, o Proofpoint Browser Isolation reduz o impacto causado por usuários clicando em URLs maliciosos. Ele oferece proteção no momento do clique para URLs dentro de e-mails corporativos. Ele também isola a atividade de navegação em um compartimento seguro que apresenta aos usuários apenas uma versão renderizada com segurança. Ele ainda previne downloaders de estágio inicial e o roubo de credenciais. Isso, essencialmente, quebra a cadeia de ataque.

Você pode implementar o isolamento baseado no risco de acordo com a política e com os insights das suas VAPs. Você pode enviar os URLs mais arriscados para sessões de navegação isoladas. Você também pode estabelecer políticas mais restritivas para pessoas visadas isolando todos os cliques desses usuários. Dependendo de quais usuários estão sendo visados, também podemos adaptar a política de isolamento com base nos riscos associados a cada usuário e ao URL no qual ele clica.

Conscientize seus usuários quanto à segurança

A prevenção do ransomware exige que você treine o seu pessoal. Afinal, os seus usuários são a sua última linha de defesa. Os ataques de ransomware exigem que o usuário clique em um link ou faça o download de um anexo. Segundo o relatório mais recente (2021) de investigações de violações de dados (DBIR) da Verizon, 85% das violações no ano passado envolveram um elemento humano.[2]

A plataforma Proofpoint Threat Protection inclui treinamento para conscientização quanto à segurança. Esse treinamento permite educar os seus usuários sobre o ransomware e instruí-los a não clicar em mensagens suspeitas. Você pode atribuir mais treinamento para os usuários mais visados e para os que realmente interagiram com ameaças reais. Para consolidar ainda mais o treinamento dos usuários finais, você pode utilizar o conteúdo de nossa ampla biblioteca nos seus alertas de segurança e comunicações aos funcionários. Você também pode executar ataques simulados utilizando modelos baseados em iscas da vida real vistas em bilhões de mensagens analisadas pela Proofpoint. A plataforma oferece mecanismos fáceis para denunciar e-mails suspeitos por meio de nosso botão PhishAlarm e nossos tags de advertência de e-mail.

2 Verizon. "DBIR: Data Breach Incident Report" (Relatório de incidentes de violações de dados). 2021.

As credenciais das contas de usuário são as chaves do seu castelo. Com apenas um nome de usuário e uma senha, um operador de ransomware pode lançar ataques dentro e fora da sua organização.

Automatize a remediação de mensagens maliciosas

As equipes de segurança frequentemente enfrentam falta de pessoal. E costumam estar assoberbadas com alertas que precisam ser triados e investigados rapidamente. A plataforma Proofpoint Threat Protection oferece automação de coordenação de segurança e resposta (mSOAR) com foco no e-mail. Ela automatiza a investigação e a remediação de e-mails maliciosos ou indesejados denunciados pelos usuários.

As mensagens denunciadas pelos usuários são analisadas e enriquecidas automaticamente por meio de múltiplos sistemas de reputação e inteligência contra ameaças. Quando uma mensagem é maliciosa, ela e quaisquer mensagens relacionadas podem ser colocadas em quarentena automaticamente. Isso evita a necessidade de investigar cada alerta e de remediar mensagens maliciosas manualmente. Portanto, a sua equipe de segurança economiza muito tempo e trabalho. Fechando o círculo, os usuários recebem um e-mail personalizado que confirma que a mensagem era maliciosa. Isso serve para reforçar seu bom comportamento.

A plataforma Proofpoint Threat Protection analisa as mensagens mesmo após elas serem entregues. Se a plataforma identificar que algo é malicioso após a entrega, será acionada uma remoção automática na caixa de entrada do usuário. Serão removidas até mesmo mensagens que tenham sido encaminhadas a outros usuários ou enviadas em listas de distribuição.

Detecte acesso inicial e evite descoberta, movimentação lateral e persistência

O Proofpoint Cloud Security detecta ameaças de ransomware:

- Monitorando e detectando contas de nuvem comprometidas
- Monitorando uploads de arquivos maliciosos para contas de nuvem
- Protegendo contra comando e controle com segurança de Web

Detecte sequestros de contas de nuvem

As credenciais das contas de usuário são as chaves do seu castelo. Com apenas um nome de usuário e uma senha — especialmente em aplicativos de nuvem como Microsoft 365 ou Google Workplace — um operador de ransomware pode lançar ataques dentro e fora da sua organização. O CASB da Proofpoint Cloud Security oferece controles de acesso adaptáveis em tempo real. Estes se baseiam em risco, contexto e função. O acesso aos aplicativos de nuvem é bloqueado automaticamente quando se origina de locais arriscados ou de perpetradores de ameaças conhecidos. O CASB também utiliza dados contextuais para confirmar a identidade do usuário e evitar acessos arriscados. Os dados contextuais incluem localização do usuário, dispositivo, rede e quando ocorreu o login. Você pode definir controles de política de acesso, como exigir autenticação por múltiplos fatores e restringir o acesso de dispositivos não gerenciados para se proteger contra perpetradores de malware.

A Proofpoint oferece a visibilidade necessária para revelar a propagação lateral ou o risco para os seus dados em decorrência de uma conta comprometida. Você pode ver se um login suspeito está correlacionado a uma conta que envia e-mails suspeitos. Isso permite determinar se um perpetrador de ameaças tentou instalar um acesso persistente configurando regras de delegação ou encaminhamento de e-mail ou utilizando tokens OAuth. Isso também possibilita saber qual atividade suspeita de arquivo ocorreu.

Evite a distribuição de ransomware por aplicativos de nuvem

O ransomware pode se espalhar pelo compartilhamento de arquivos infectados e por sincronização automática. Ele tem o potencial de afetar gravemente a sua organização, seus parceiros e seus clientes. O Proofpoint Cloud Security monitora ativamente os seus compartilhamentos de arquivos na nuvem e avisa quando há um arquivo suspeito. Com a análise de arquivos em aplicativos de nuvem e a área restrita da Proofpoint, você pode conter os arquivos maliciosos da nuvem por meio de uma quarentena automática ou de outros passos de mitigação.

Proteção contra comando e controle com segurança de Web

Quando um dispositivo é comprometido, ele envia um sinal para os servidores do perpetrador de ameaças. Em seguida, o perpetrador procura pelo próximo conjunto de instruções. Com controle sobre o dispositivo, o perpetrador de ransomware pode realizar uma variedade de ações. Essas ações variam da distribuição de ransomware ao vazamento de dados.

O Web Security e o Browser Isolation do Proofpoint Cloud Security bloqueiam conexões com sites comprometidos. Isso impede que o operador de ransomware controle o dispositivo e cause mais danos. A inteligência é fornecida pelo Proofpoint Nexus Threat Graph. Ele combina trilhões de pontos de dados em tempo real entre múltiplos vetores de ameaças do mundo todo, autoaprendizagem e inteligência artificial avançadas e uma equipe de pesquisa global que mantém você à frente das maiores ameaças cibernéticas de hoje em dia.

Evite vazamentos de dados

O Proofpoint Advanced Threat Protection e o Proofpoint Cloud Security evitam vazamentos de dados:

- Observando sinais preliminares de vazamento de dados
- Detectando e evitando movimentações de dados não autorizadas

O Web Security e o Browser Isolation do Proofpoint Cloud Security proporcionam uma segurança de dados que leva em consideração os riscos e que pode realizar prevenção de perda de dados (DLP) em tempo real. Juntamente com o Browser Isolation, o Web Security proporciona controles de dados granulares, como acesso somente de leitura e permissão ou bloqueio para aplicativos de nuvem e de Web. O Proofpoint Browser Isolation protege o acesso dos usuários a aplicativos e dados isolando sessões de navegador em um compartimento seguro.

Além disso, o CASB da Proofpoint ajuda você a obter rapidamente visibilidade sobre atividades suspeitas em arquivos. Tais atividades normalmente estão vinculadas a logins suspeitos. Os responsáveis pela resposta a incidentes podem separar rapidamente as atividades de arquivo iniciadas por atacantes das iniciadas por usuários. E, com essa capacidade, eles podem responder em menos tempo.

Além de proteger dados confidenciais em aplicativos de nuvem, a Proofpoint pode impedir que algum conteúdo sigiloso seja vazado para servidores de comando e controle, transferido por download para dispositivos não gerenciados (do operador de ransomware) ou enviado para fora por e-mail.

SAIBA MAIS

Para obter mais informações, visite **proofpoint.com**.

SOBRE A PROOFPOINT

A Proofpoint, Inc. é uma empresa líder em cibersegurança que protege as organizações em seus maiores riscos e seus ativos mais valiosos: sua equipe. Com um pacote integrado de soluções baseadas em nuvem, a Proofpoint ajuda empresas do mundo todo a deter ameaças direcionadas, proteger seus dados e tornar seus usuários mais resilientes contra ataques cibernéticos. Organizações líderes de todos os portes, incluindo mais de metade das empresas da Fortune 1000, contam com a Proofpoint para obter soluções de segurança e conformidade centradas nas pessoas e que minimizem seus riscos mais críticos em e-mail, nuvem, redes sociais e Web. Mais informações estão disponíveis em **www.proofpoint.com**.