RESUMO TÉCNICO

Remediação de ransomware com FlashArray SafeMode

Utilize snapshots do FlashArray™ SafeMode™ da Pure Storage® para proteger seus dados.

Ransomware (quando o invasor criptografa seus arquivos de forma oculta e demanda pagamento para descriptografá-los ou desbloqueá-los) pode ser desastroso para as organizações. A perda dos seus dados e o impacto monetário não são apenas preocupações; em muitos casos, um ataque resulta em um desligamento completo das operações da empresa por dias e a permanência no holofote do público pelas razões erradas. Sua reputação comercial e valor de marca também podem ser danificados. Em um ataque de ransomware em 2020 à Garmin, o tempo de inatividade durou quase cinco dias e, embora o valor do resgate não seja conhecido, é estimado em cerca de 10 milhões de dólares.[1]

O que é ransomware?

Na primeira metade de 2020, o número de relatórios de ransomware globais aumentou 715% em relação ao ano anterior, de acordo com o mais recente Relatório do panorama de ameaças de 2020 da Bitdefender. Com mais pessoas trabalhando remotamente e um ambiente empresarial alterado devido à pandemia, os cibercriminosos capitalizaram a oportunidade.

O ransomware afeta todos os setores: tecnologia, seguros, petróleo e gás, educação superior, entre outros. Em 2019, mais de 500 escolas foram atingidas por ransomware.[2] O software de ransomware é um grande negócio, e as vítimas são cada vez maiores, tendo que pagar somas exorbitantes para voltar à atividade normal.

O que muitas pessoas não sabem é que o software de ataque de ransomware estão tão acessíveis quanto softwares comerciais. Ele pode ser baixado e adquirido facilmente, normalmente com uma parte dos lucros do ataque indo para o desenvolvedor. Os invasores não são particularmente especialistas ou habilidosos. Eles podem ser funcionários insatisfeitos e minimamente qualificados com acesso a infraestrutura crítica. Com um rápido download na dark web, eles podem lançar um ataque de ransomware antes que as contas do funcionário sejam bloqueadas.

Segurança

Proteja seus dados de ataques de ransomware maliciosos, danos à reputação e demandas caras de resgate.

Proteção

Não importa quem ataque você, os dados só podem ser excluídos em conjunto com o Suporte da Pure.

Simples

O SafeMode só precisa de três etapas simples para ser configurado e está pronto para ser ativado.

1 https://techcrunch.com/2020/07/27/garmin-confirms-ransomware-attack-outage/

2 https://www.zdnet.com/article/over-500-us-schools-were-hit-by-ransomware-in-2019/

Como o SafeMode protege dados críticos

Vamos analisar dois exemplos de um ataque em potencial, considerando que um invasor obteve direitos de administrador para um FlashArray.

1. **O invasor criptografa volumes e elimina os originais:** Nesse cenário, os volumes originais são destruídos. Quando um volume é "destruído", ele fica em uma área especial do FlashArray, que é removida do inventário do volume, mas ainda existe em um bucket de erradicação. O bucket de erradicação tem um temporizador padrão de 24 horas, em que os objetos podem ser recuperados ou permanentemente erradicados. Se o invasor também tiver erradicado os volumes, todos os dados do volume desaparecerão, e agora você está sujeito às demandas dos invasores. Para ficar claro, com o SafeMode ativado, o invasor não pode remover os dados do volume do bucket de erradicação, mesmo com privilégios de administrador. No nosso exemplo aqui, o invasor pode erradicar volumes porque o SafeMode não está ativado.
2. **O invasor criptografa volumes e elimina todos os snapshots, além dos volumes:** Nesse caso, há pontos de recuperação para retornar na forma de snapshots. No entanto, o invasor os destruiu e os eliminou de forma que não há nada para restaurar. Isso foi possível porque, assim como no Exemplo 1, o invasor eliminou os snapshots porque o SafeMode não estava habilitado.

Em cada uma das situações, habilitar o SafeMode evita a eliminação de qualquer volume ou snapshot durante o período configurado para a eliminação. Se o temporizador da eliminação for definido para 14 dias, os dados de recuperação que você precisa para restaurar serviços essenciais serão completamente protegidos por duas semanas. O SafeMode não só evita que até os usuários mais privilegiados eliminem volumes e snapshots, como também garante que os snapshots do FlashArray são imutáveis (não podem ser alterados). Utilizar o SafeMode com snapshots sempre permitirá um ponto de recuperação garantido após um ataque.

Como se recuperar de um ataque de ransomware

Revisitando nossos exemplos, se o SafeMode tivesse sido habilitado no Exemplo nº 1, você poderia eliminar os volumes criptografados do invasor e assim restaurar seus volumes, instantaneamente, e voltar para um estado anterior à criptografia dos volumes.

No Exemplo nº 2, o processo é o mesmo. Você consegue erradicar os volumes criptografados do invasor e restaurá-los a partir dos snapshots. Como o invasor não consegue erradicar os snapshots, eles permanecem disponíveis para recuperação. Em ambos os exemplos, seria de extrema importância investigar o vetor do ataque e atuar para evitar uma recorrência.

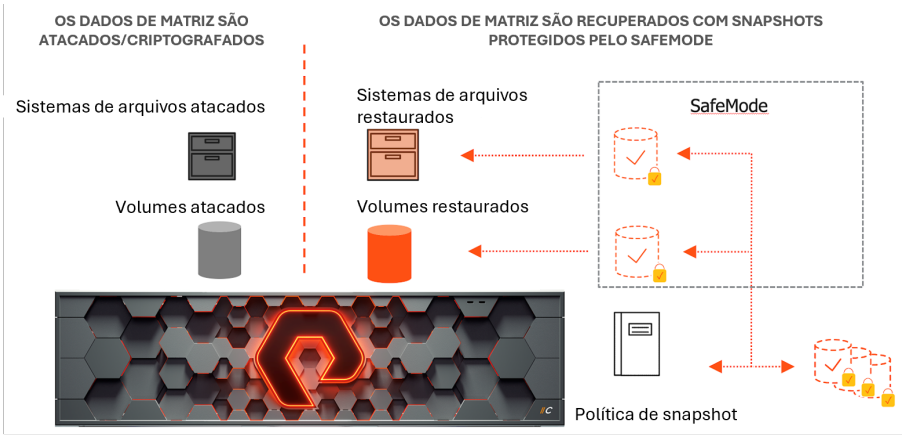

Figura 1. Os volumes atacados/criptografados são facilmente substituídos pelos snapshots de um ponto anterior no tempo.

Configuração do SafeMode

O SafeMode por si só é fácil de configurar. Ligue para o Suporte da Pure para solicitar que o SafeMode seja habilitado e forneça contatos adicionais (até cinco) que sejam autorizados para solicitar alterações no SafeMode. O suporte enviará um PIN de seis dígitos para cada usuário autorizado a ser usado para qualquer mudança futura. O próprio SafeMode tem a opção de estar habilitado ou desabilitado, entretanto o temporizador tem tempo de retenção configurável. A maioria dos nossos clientes estabelece 14 dias, mas o temporizador pode ser estendido até 30 dias.

É obrigatório criar uma política de snapshot para o SafeMode proteger seus dados. Isso é realizado por meio de Grupos de proteção FlashArray, em que hosts, volumes, grupos de volume, arquivos e diretórios podem ser registrados de forma automática e regular. A retenção e a frequência de snapshots são personalizáveis. Mesmo um terceiro dispositivo, um "alvo", pode ser adicionado para enviar snapshots para outro FlashArray, serviço em nuvem ou FlashBlade®.

Se você precisar recuperar um espaço de FlashArray, que pode acontecer por exemplo após as migrações de dados para uma matriz, você precisará fazer uma chamada para o Suporte da Pure Storage, com dois contatos autorizados e seus PINs atribuídos para possibilitar a eliminação permanente de qualquer item. No entanto, esse processo não é necessário para a recuperação instantânea de objetos que ainda estão com a eliminação pendente.

Conclusão

O SafeMode é um recurso fácil e sem custo extra que evita a perda permanente de dados devido a erros do administrador ou a ataques maliciosos de ransomware. Ele funciona simplesmente evitando a eliminação de objetos durante um determinado período. No caso de um ataque, em vez de uma interrupção nas atividades desgastante e pública para acabar pagando um resgate, você simplesmente remove os dados criptografados do invasor e restaura instantaneamente seus dados a partir de um ponto anterior no tempo.

Para habilitá-lo, basta você ligar para o suporte, estabelecer seus contatos e definir o período. Essas três etapas proporcionarão uma vitória simples e proativa antes que o desastre em potencial ocorra.

PS2024-01-pt-br 12/24