Expressão Digital

De: Microsoft Partner Network [PartnerNetwork@email.microsoft.com]
Enviado em: segunda-feira, 21 de dezembro de 2020 18:36
Para: info@expressaodigital.com
Assunto: Responder a ataques cibernéticos sofisticados

Sinalizador de acompanhamento: Acompanhar
Status do sinalizador: Sinalizada

Etapas importantes para parceiros e clientes se protegerem contra ataques cibernéticos

Exibir como página da Web

Microsoft

Histórico

A Microsoft está ciente de um ataque sofisticado de cadeia de suprimentos que visou uma grande variedade de vítimas ao longo do último ano. O ataque utiliza arquivos mal-intencionados do SolarWinds que possivelmente concederam acesso dos criminosos cibernéticos às redes de algumas vítimas. Os especialistas em segurança cibernética da Microsoft estão investigando o ataque para ajudar a garantir que os clientes da Microsoft estejam o mais seguros possível.

Orientações

Veja abaixo as orientações de comunicação de preparação do cliente que você pode aproveitar ao se comunicar com clientes:

A Microsoft está ciente de um ataque sofisticado que utiliza o software mal-intencionado SolarWinds. Em 17 de dezembro de 2020, Brad Smith publicou uma postagem no blog compartilhando as informações técnicas detalhadas e mais recentes para os defensores.

Como esta é uma investigação contínua, as equipes de segurança cibernética da Microsoft continuam atuando como os primeiros profissionais responsáveis por respostas a esses ataques. Sabemos que os clientes e parceiros terão perguntas contínuas, e a Microsoft está comprometida em fornecer atualizações oportunas à medida que novas informações forem disponibilizadas. Faremos atualizações por meio do nosso blog do Microsoft Security Response Center (MSRC) em https://aka.ms/solorigate.

Há vários recursos publicados para ajudar os clientes na proteção dos ambientes:

- Publicamos uma postagem no blog descrevendo este cenário dinâmico de ameaças e os princípios que estão regendo nossa abordagem da investigação.
- Publicamos uma postagem de respaldo no com detalhes técnicos do ataque. Este blog será atualizado com novas informações à medida que a investigação continuar. Os clientes devem ver este blog como o lugar central de atualizações sobre ataques sofisticados.
- O antivírus Microsoft Defender e o Microsoft Defender for Endpoint lançaram proteções para o software mal-intencionado SolarWinds e outros artefatos contra o ataque.
- O Microsoft Azure Sentinel lançou orientações para ajudar os clientes do Azure Sentinel a verificar os ambientes em busca de atividades relacionadas que observamos com esse ataque sofisticado.
- Os clientes do Microsoft 365 Defender e do Microsoft Defender for Endpoint devem ler o artigo do Threat Analytics no console do Defender (entrada necessária) para obter informações sobre detecção e possíveis impactos no ambiente.
- Para todos os clientes do Especialistas em Ameaças da Microsoft (MTE), em que observamos atividades suspeitas nos ambientes dos clientes, concluímos notificações de contas visadas.
- Se um cliente tem necessidades relacionadas ao suporte de produtos, continue direcionando-o ao suporte da Microsoft (CSS), que permanece como o principal lugar para todas as necessidades de suporte de clientes.
- Para profissionais de identidade e administração do Microsoft 365, publicamos uma postagem no blog sobre como proteger o Microsoft 365 de ataques locais.

Postagens de blog da Microsoft

- 13 de dezembro – Orientações ao cliente sobre ataques cibernéticos recentes de estado-nação – Microsoft Security Response Center
- 13 de dezembro – Etapas importantes para parceiros e clientes se protegerem contra ataques cibernéticos recentes de estado-nação
- 15 de dezembro – Como garantir que os clientes estejam protegidos contra o Solorigate
- 16 de dezembro – Postagem sobre o SolarWinds – Busca de comprometimentos com o Azure Sentinel – Microsoft Tech Community
- 17 de dezembro – Um momento de reconhecimento: a necessidade de uma

resposta de segurança cibernética global e forte

- 18 de dezembro – Análise do Solorigate, o arquivo DLL comprometido que começou um ataque cibernético sofisticado e como o Microsoft Defender ajuda na proteção – Segurança da Microsoft
- 18 de dezembro – Como proteger o Microsoft 365 de ataques locais

Consultorias e recursos adicionais

- Se o seu cliente tiver uma dúvida específica sobre o FireEye, encaminhe-o à Consultoria do FireEye.
- Se o seu cliente tiver uma dúvida específica sobre o SolarWinds, encaminhe-o à Consultoria do SolarWinds.
- A Cybersecurity and Infrastructure Security Agency (CISA) publicou um conjunto de informações e orientações aqui. Para obter orientações individuais de países específicos, clientes e parceiros devem consultar as informações de autoridades legais apropriadas ou outra entidade governamental nesta jurisdição.

Obrigado por sua parceria com a Microsoft.