Crowe Horwath™

Auditoria | Impostos | Consultoria | Riscos

Fernando Flauto

IT GRC & SEGURANÇA DE TECNOLOGIA DA INFORMAÇÃO

fernando.flauto@crowehorwath.com.br

Lições do Ataque WannaCry

O ataque WannaCry que teve seu ápice na ltima sexta-feira, dia 12 de maio, foi predominantemente realizado através de e-mails phishing convidando inocentes usuários finais para abrir um arquivo. O tremendo impacto do ataque pegou as organizações de surpresa, muitas das quais estavam despreparadas para responder ou impedir eficazmente as infecções. Os usuários finais direcionados simplesmente clicaram nos links para desencadear uma cadeia de eventos, que resultou em organizações ficando offline, perda de acesso a registros críticos, serviços redirecionados e clientes incapazes de receber serviços críticos.

O malware segmentou uma vulnerabilidade conhecida da Microsoft® para a qual um patch ficou disponível em março no Boletim de Segurança da Microsoft MS17-010. Quando a vítima, usuário final, iniciou a instalação do malware em uma máquina não atualizada, os dados da vítima foram criptografados e mantidos para resgate pelo invasor. Os atacantes pediram o pagamento anônimo em bitcoin, moeda eletrônica, em troca de liberar os arquivos e retornar o acesso do sistema ao usuário final.

Além dos bons controles de gerenciamento de patches e de backup de dados, a melhor maneira de impedir uma infecção é evitar a exposição do malware em primeiro lugar. O n mero informado de um ponto de entrada para malware neste ataque, como em muitos ataques anteriores, foi através de computadores de usuário final com acesso dado pelos próprios usuários. Como exemplo desse ataque, as organizações que implementam campanhas efetivas e contínuas de conscientização de segurança e anti-phishing estão decididamente em risco muito menor de infecção por meio desses ataques comuns e cada vez mais sofisticados.

No entanto, mesmo com as melhores proteções, não é possível ser 100 por cento imune a cada ataque. Reconhecendo que se tornar o alvo de um ataque cibernético não é uma questão de se, mas sim quando, as organizações precisam estar preparadas para responder com um plano de resposta a incidentes devidamente projetado. Um plano completo e atualizado ajudará a garantir que as organizações estão preparadas para responder.

Infelizmente, essa ameaça não é nova. O malware existe há mais de 20 anos, tem usado vulnerabilidades não propagadas para espalhar e propagar por muitos anos, e tem mantido computadores e dados reféns há mais de 10 anos. As organizações não precisam de proteções especiais. Elas simplesmente precisam usar uma abordagem de segurança em camadas para se proteger de todas as ameaças de malware. As organizações devem considerar a implementação das seguintes táticas:

Gerenciamento rápido de patches. As organizações devem instalar o MS17-010 - mas isso só resolve o problema de hoje. E o dia de amanhã? Um programa de segurança de natureza reacionária não vai ser eficaz a longo prazo. As organizações devem implementar um robusto programa de gerenciamento de vulnerabilidades e remendos para identificar proativamente vulnerabilidades e corrigi-las antes que os adversários possam aproveitá-las.

Princípio do privilégio mínimo. Os usuários não devem ter direitos administrativos locais. Se o fizerem, eles estão realizando algumas das atividades de maior risco (e-mail e navegação na web - onde a maioria dos malwares vem) com o maior privilégio, o que poderia, por sua vez, inadvertidamente conceder esse direito a malware.

Menos é mais. Somente os serviços que são necessários para que um sistema funcione devem ser expostos à Internet. As organizações que são boas no princípio da segurança de minimização (em redes internas e externas) reduzem drasticamente a quantidade de dados que podem ser atacados para se tornar um alvo muito menor e mais difícil para atores de ameaças oportunistas.

Filtragem de conte do de rede. Controlar o que é permitido dentro e fora da rede através de soluções de filtragem de conte do (como proxies da web e filtros de e-mail) pode reduzir ainda mais a exposição de uma organização ao ataque e prevenir ameaças conhecidas.

Proteções de códigos maliciosos. Essas proteções podem vir de várias formas - incluindo anti-vírus e whitelisting de aplicativos - ambas as quais podem ser eficazes para ajudar a evitar a execução de código indesejada.

Backups. As organizações devem assegurar que eles tenham a capacidade de recuperar seus dados se todos os outros controles preventivos falharem.

Plano de resposta a incidentes. Como ter backups, é essencial ter um plano descrevendo como responder no caso de um incidente cibernético.

Focalizar na ameaça mais recente pode conduzir a uma aproximação míope à segurança. Em vez disso, as organizações precisam usar uma abordagem de segurança em camadas para fornecer a melhor proteção possível para hoje e para amanhã também.

As medidas escritas aqui não são novas e com certeza, as empresas infectadas na ultima sexta-feira já as viam vistas, em alguma carta de recomendação da Auditoria que ficou esquecida em alguma gaveta.