INFO & INSIGHTS

RANSOMWARE
MÉTODOS COMUNS DE ATAQUE

Para melhor prevenir contra ransomware, é fundamental compreender as táticas que os invasores usam para entregar essa ameaça. Há diversas variantes de ransomware em uso em diversos vetores de ataque, incluindo através da rede, aplicativos baseados em SaaS e diretamente no endpoint. Essas informações permitirão que você concentre seus controles de segurança nas áreas com maior probabilidade de serem exploradas e reduza o risco de infecção.

Kits de exploração

Os kits de exploração são kits de ferramentas sofisticadas que exploram vulnerabilidades. Na maioria das vezes, os kits de exploração são executados quando uma vítima visita um site comprometido. O código malicioso oculto no site, muitas vezes em um anúncio malicioso, redireciona você para a página inicial do kit de exploração sem que você perceba. Se o sistema estiver vulnerável, um download não autorizado de uma carga maliciosa será executado, o sistema será infectado e os arquivos serão sequestrados.

Anexos de e-mail maliciosos

Com anexos de e-mail maliciosos, o invasor cria um e-mail, provavelmente de uma fonte crível, como Recursos Humanos ou TI, e anexa um arquivo malicioso, como um arquivo executável portátil (PE), um documento do Word ou um arquivo .JS. O destinatário abre o anexo pensando que o e-mail foi enviado por uma fonte confiável. Após o arquivo ser aberto, a carga de ransomware é baixada sem o usuário saber, o sistema é infectado e os arquivos são sequestrados.

Links de e-mail maliciosos

Semelhantes aos anexos de e-mail, os links de e-mail maliciosos são URLs no corpo do e-mail. Da mesma forma, esses e-mails são enviados por alguém ou alguma organização que você acredita ser uma fonte confiável. Após clicar nelas, essas URLs baixam arquivos maliciosos através da Web, o sistema é infectado e os arquivos são sequestrados.

Essa evolução, assim como a facilidade com a qual esses ataques são executados, significa que qualquer organização pode ser a próxima vítima e provavelmente já é um alvo atual. Contudo, existem soluções. A prevenção é fundamental para manter as organizações seguras. A estratégia mais eficiente para impedir um ataque de ransomware é nunca deixar que o ataque entre em sua organização.