14/07/2016 - Que lições tirar do ciberataque ao SWIFT?

*Por Otto Berkes**

Como as bactérias que se transformam para sobreviver a potentes antibióticos, as ameaças nos ambientes virtuais de hoje estão mudando constantemente para explorar novas vulnerabilidades. Assim, da mesma maneira que os antibióticos devem evoluir, nossos sistemas de segurança digital - em níveis pessoal, comercial e governamental - precisam mudar com os tempos e serem igualmente ativos, robustos e inovadores.

O último lembrete dessa constante luta são os relatos recentes de que cibercriminosos roubaram US$ 81 milhões em fundos do Banco Central de Bangladesh, bem como um banco no Equador e em pelo menos um outro país. O roubo é uma lição dolorosa nos mostrando que os bandidos nunca dormem, e que aquilo que já foi "bom o bastante" em termos de segurança digital agora não é mais. Para realizar esse assalto digno de filme de ação, os ladrões digitais driblaram o sistema de mensagens financeiras que todos pensavam ser o mais seguro do mundo, conhecido como SWIFT, uma cooperativa belga de propriedade dos bancos membros que é usada por 11 mil instituições financeiras globalmente.

O ataque à rede bancária SWIFT não mostrou um novo tipo de ataque a computadores, mas revelou um esquema combinando vários métodos de ataque existentes de uma forma tortuosa, sofisticada e única. O SWIFT informou que os ladrões roubaram credenciais legítimas de operadores, o que lhes permitiu enviar mensagens aparentemente autênticas para realizar transferências fraudulentas. Em seguida, eles instalaram o software malicioso em computadores do banco, a chave para manipular impressoras e ocultar vestígios das mensagens fraudulentas.

Em comunicado, o SWIFT disse que "os agressores claramente apresentam um conhecimento profundo e sofisticado de controles operacionais específicos dentro dos bancos visados - conhecimento que pode ter sido adquirido com gente de dentro das empresas ou por ataques cibernéticos - ou uma combinação de ambos".

Hoje, proteger o SWIFT e seus membros, ou qualquer ecossistema interligado semelhante, requer uma abordagem colaborativa e multifacetada que deve ser gerenciada como um desafio sério ao negócio, e não simplesmente uma questão tecnológica.

Em primeiro lugar, a engenharia social de fraquezas humanas praticada pelos bandidos deve ser combatida com a engenharia social dos mocinhos. Ataques anteriores em redes de pagamentos eram geralmente relacionados aos chamados ataques spear phishing, uma variação do já conhecido fishing em que os criminosos induzem as pessoas a abrirem e-mails falsos e a clicarem em links que fazem o download do software malicioso no computador do usuário, deixando os fraudadores livres para roubar credenciais quando o logon for feito nos sistemas.

Além do malware, os cibercriminosos implantaram ferramentas de hackeamento, incluindo software key-logger, um programa que registra tudo que é digitado, para roubar credenciais

bancárias de Bangladesh do sistema SWIFT.
Uma educação contínua tanto dentro como fora da organização de tecnologia sobre as mais recentes técnicas de spear phishing ajudará a despertar consciência e reduzir as fraudes. Dispositivos móveis e outros "conectáveis", a Internet das Coisas, são novos pontos de vulnerabilidade e devem ser protegidos. Os ladrões de banco também aproveitaram o elo fraco na cadeia de segurança - um leitor de PDF modesto usado para gerar relatórios de confirmações de pagamento. Uma abordagem de revisão regular de portfólio centrada na segurança em toda a empresa ajuda a identificar ameaças emergentes, lacunas e estratégias de mitigação.
Nós também precisamos entender que as fronteiras de segurança não são mais as paredes do castelo, não importa o quão fortificado ele seja. O novo perímetro é a identidade. É esse ponto onde o usuário - os milhões de usuários – acessa um sistema qualquer em um canto da rede. As empresas devem ter a certeza de que os usuários são quem eles dizem que são, e que as informações e serviços que podem acessar correspondem exatamente ao papel que ocupam. Nomes de usuários e senhas não são mais suficientes para comunicações sensíveis. Ampliar a identidade básica com protocolos de autenticação avançados, como o multifatores, pode ajudar a garantir a autenticidade da identidade, fazendo com que os bancos menores atualizem sua segurança de uma maneira relativamente fácil e com bom custo-benefício.
Alguns dados e serviços podem também necessitar de maior segurança do que outros. Por exemplo, uma senha simples pode ser suficiente para que um consumidor acesse informações de saldo em um ambiente de banco online. Mas a transferência de fundos por funcionários do banco deve exigir uma verificação de identidade adicional, a fim de completar a transação.
Importante: precisamos aumentar o monitoramento e a análise de contas de usuários privilegiados. A crescente interconectividade dos nossos sistemas comerciais, financeiros - e mesmo governamentais - significa que mais usuários do que nunca estão tendo acesso privilegiado para executar esses vários sistemas.
O acesso privilegiado deve ser dado apenas enquanto necessário e precisa ser monitorado em todos os momentos. A atividade deve ser acompanhada de perto, especialmente com o cibercrime sendo perpetrado por pessoas de dentro das empresas. O software de detecção de fraudes pode identificar comportamentos anômalos, como tentativas de obtenção de privilégios ou mudanças nos padrões de atividade destas contas. Se o acesso privilegiado está comprometido, o histórico de acesso da conta vai ajudar a entender melhor o que aconteceu e por quê.
Os ataques ao SWIFT são significativos não só porque uma grande quantidade de dinheiro foi roubada, mas porque os ladrões usaram uma combinação de métodos bem conhecidos para comprometer uma operação financeira que atua no sistema nervoso central da economia global. As empresas devem aprender com isso e examinar cuidadosamente as suas próprias práticas. Precisamos nos perguntar se estamos indo além da segurança "boa o bastante" para permanecermos vigilantes na manutenção da saúde e segurança dos nossos sistemas. Precisamos combater fogo com fogo, usando uma combinação comprovada de antídotos de segurança conhecidos para conter e evitar a propagação de outro ataque como o do SWIFT. Caso contrário, o saqueio de Bangladesh terá mais sequelas.

* Um dos inventores do Xbox, Otto Berkes é CTO (Chief Technology Officer) da CA

Technologies
ZENO GROUP
A DJ EDELMAN COMPANY