Aluno: Rodrigo Alves de Almeida

Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains

Recentemente, houve o surgimento de uma nova classe de ameaças cibernéticas. Essa classe tem o objetivo de comprometer dados utilizados pelo governo na área econômica e militar, e tem como característica a capacidade de driblar os meios mais tradicionais de prevenção contra ataques, pois eles se baseiam em dois pontos que não são válidos para essas novas ameaças: o fato de que uma resposta deve vir após o ataque e que o comprometimento foi consequência de uma falha corrigível.

Nomeadas APT (ameaça avançada e persistente), essa nova categoria de ataques utiliza ferramentas avançadas, *malwares* customizados e explorações "zero-day", de modo que é necessária uma abordagem inteligente e focada na ameaça, se colocando no lugar do atacante. A discretização das etapas de uma intrusão é nomeada "kill chain" e é uma técnica que pode ser utilizada por analistas para auxiliar na mitigação das APTs.

Assim, uma CND (defesa de rede de computadores) baseada em inteligência é uma estratégia de gerência de riscos, realizando análise de adversários, suas capacidades, objetivos, doutrinas e limitações. A CND requer que as intrusões sejam entendidas como eventos progressivos e divididos em fases.

De acordo com o modelo "kill chain", acabar com uma etapa de uma intrusão é suficiente para quebrar a corrente e mitigá-la, de modo que qualquer repetição do adversário pode ser facilmente detectada e destruída. Assim, defensores podem implementar medidas de proteção mais rapidamente que o desenvolvimento dos atacantes, de modo que, no modelo CND baseado em inteligência, o atacante não tem nenhuma vantagem inerente.

No modelo apresentado pelo artigo, o principal elemento de inteligência chama-se *indicador*, que é definido como qualquer informação que descreva objetivamente uma intrusão. Os *indicadores* podem ser de três tipos: *atômicos*, quando não podem ser subdivididos; *computados*, quando são derivados de dados envolvidos em um incidente; *comportamental*, quando são junções de indicadores atômicos e computados, gerando uma ideia lógica. Os indicadores devem ser revelados, amadurecidos e utilizados, de modo que novos indicadores podem surgir desse ciclo.

Assim, é fornecida uma definição de "kill chain", focada nas intrusões. Ela é definida pelas fases de reconhecimento, armamento, entrega, exploração, instalação, *command and control (C2)* e ações em objetivos.

O reconhecimento é marcado pela busca, identificação e seleção de alvos. No armamento, é gerado o *trojan* malicioso que será utilizado para ataque. Na entrega, é feita a transmissão do *trojan* para o alvo. A exploração consiste no acionamento e execução do código inserido. A instalação de um programa no sistema alvo implica uma presença definitiva no ambiente. Na fase *command and control*, o ambiente comprometido abre uma conexão por meio da internet para enviar os dados para o adversário. Por fim, na fase de ações em objetivos, os intrusos podem agir para atingir seus objetivos, como por exemplo a coleta e envio de dados.

A partir do modelo “kill chain” fornecido, defensores podem alinhar seus esforços para agir sobre cada uma das fases definidas pelo modelo. Assim, a performance e efetividade dessas tentativas de defesa podem ser medidas, orientando as ações futuras dos defensores. Esse tipo de abordagem é a essência do CND baseado em inteligência: basear as estratégias de defesa a partir do conhecimento pleno do adversário.

De acordo com a lógica do modelo estudado pelo artigo, é importante notar que as explorações “zero-day”, que são tradicionalmente definidas como explorações que eram antes desconhecidas pelos defensores, são na realidade explorações já conhecidas com apenas mudança em uma ou mais fases do “kill chain”. Desse modo, se os defensores tiverem defesas consolidadas e endurecidas para todas as fases, será muito difícil para os atacantes desenvolver uma nova exploração que quebre todas as barreiras simultaneamente.

A detecção de um ataque geralmente é realizada sobre uma das fases do “kill chain”, e fornecerá informações sobre apenas a fase avistada. Desse modo, um trabalho importante dos analistas, de acordo com o modelo CND baseado em inteligência, é fazer um rastreamento das fases anteriores, analisando como foi realizado o ataque em cada uma dessas fases, de modo a obter informações que podem ser utilizadas para a criação de ferramentas de mitigação. Assim, os atacantes não irão conseguir reaproveitar as técnicas utilizadas para avançar sobre essas fases novamente.

Assim, quando tratamos de APTs, a análise das sucessivas tentativas de intrusão poderão formar padrões e *indicadores* repetidos. Esses *indicadores*, denominados *indicadores chave de campanha*, são um ponto em comum de ataques realizados de forma semelhante, que caracterizam uma *campanha*. Dessa forma, as *campanhas* poderão ser de grande utilidade para os defensores, pois indicam o comportamento dos adversários, suas táticas, técnicas e procedimentos.

De acordo com a resenha lida, posso concluir que a CND baseada em inteligência é de grande utilidade quando há necessidade de se proteger contra inimigos mais estruturados e mais resilientes. Em meios onde há uma grande necessidade de proteção de dados, como por exemplo o governamental, é muito válido que o time de defesa aplique os ensinamentos desse modelo para precaução e resposta a ataques.

Um diferencial do modelo apresentado nesse artigo é o fato dele não ser focado nas vulnerabilidades dos defensores, mas sim no adversário e nas suas ameaças. Desse modo, é

possível organizar estratégias de defesa específicas, aumentando o custo e desencorajando o oponente.