Aluno: Rodrigo Alves de Almeida

The Diamond Model of Intrusion Analysis

O modelo diamante analisa intrusões dividindo-as em quatro fatores principais: adversário, capacidade, infraestrutura e vítima. Além disso, as intrusões podem ser divididas até seus elementos atômicos, os eventos. De acordo com o modelo, para todo evento de uma intrusão há um adversário realizando um ataque por meio de uma capacidade sobre uma infraestrutura contra uma vítima, com o objetivo de obter um resultado.

Além dos fatores principais, também são meta-fatores: período de tempo (começo e fim do evento), fase, resultado, direção, metodologia e recursos. De acordo com o modelo, para analisar um evento de uma intrusão, é possível atribuir a cada fator um grau de confiança, como tentativa de quantificar a acurácia dos dados e presunções realizadas.

Assim, podemos analisar mais profundamente os quatro fatores principais:

Em um evento, os adversários podem ser internos, externos, individuais, grupos ou até organizações. O *operador* é o adversário que utiliza as capacidades e infraestruturas para realizar o ataque, ou seja, é o 'hacker'. Esse operador, por sua vez, pode ter um *contratante*, o qual fornece as capacidades necessárias e se beneficia do ataque.

A capacidade diz respeito às ferramentas e técnicas que o adversário utiliza para realizar um evento. Desse modo, o modelo sugere uma busca pela documentação de todas as possíveis vulnerabilidades que podem ser aproveitadas pela capacidade do adversário, assim como uma lista das capacidades dele (seu arsenal).

A infraestrutura, por sua vez, são os elementos de comunicação físicos ou lógicos que são utilizados pelo adversário para aplicar uma capacidade, manter controle dessas capacidades e obter efeitos da vítima. A infraestrutura pode ser de posse direta do adversário ou pode apenas estar sendo manipulada por ele.

Por fim, a vítima é quem sofre o ataque do adversário. Todo sistema possui vulnerabilidades e exposições, de modo que toda vítima deve ter conhecimento dos possíveis pontos fracos de suas posses.

Além dos quatro fatores principais analisados acima e os meta fatores citados, o modelo diamante também pode ser estendido para outros meta fatores, como o *social-político* e o *tecnológico*, que influenciam respectivamente as relações adversário-vítima e capacidade-infraestrutura.

Uma das ferramentas mais poderosas do modelo diamante é o *pivoteamento analítico*, que consiste em, a partir de um ou mais dados obtidos sobre fatores de um evento, descobrir outros elementos relacionados. O sucesso do *pivoteamento* depende da habilidade de dedução e correlacionamento do analista, que deve, a partir de uma certa informação obtida, criar hipóteses e testar essas hipóteses, com o objetivo final de descobrir outros fatores que compunham o evento estudado.

Um esforço dos analistas, de acordo com o modelo diamante, deve ser ordenar todos os eventos realizados ao longo de um ataque no formato de um grafo orientado, onde os arcos mostram a sequência e correlação dos eventos, além do grau de confiabilidade desse acontecimento. Esse grafo é denominado *linha de atividades*, e facilita a organização, detecção de padrões e criação/teste de hipóteses.

Ao juntar *linhas de atividade* e eventos semelhantes, é possível formar um *grupo de atividades*, que tem dois principais propósitos: formar uma biblioteca que sirva de base para responder questões analíticas e ajudar o desenvolvimento de estratégias de mitigação de possíveis ameaças. Os *grupos de atividades* são formados geralmente com o objetivo de identificar e estudar um certo adversário que realiza ataques de maneira similar.

A criação dos *grupos de atividades* é feita em 6 passos. Primeiramente, o problema analítico é definido através da determinação do problema particular que deve ser resolvido por agrupamento. Então, é feita uma seleção dos fatores dos eventos e processos do adversário para formar uma base de agrupamento. Depois, é feita a criação dos *grupos de atividades* a partir dos eventos e *linhas de atividade* selecionados. O quarto passo consiste no crescimento do *grupo* com a obtenção de mais dados, eventos e estudos. No quinto passo, o *grupo de atividades* é utilizado para realizar a análise de um problema particular. Por fim, pode ser que haja necessidade de remodelar o *grupo* periodicamente, com a finalidade de mantê-lo atualizado e eficaz.

A partir da análise realizada sobre a metodologia e as ferramentas do modelo diamante, verifica-se que ele é capaz de fornecer um entendimento mais completo dos eventos e ataques. Com um amplo conhecimento das próprias vulnerabilidades e das possíveis ações de um adversário, o modelo possibilita que sejam desenvolvidas melhores políticas de prevenção e mitigação.

Apesar disso, o modelo diamante não sugere diretamente como essas políticas devem ser desenvolvidas ou como deve ser a estratégia de mitigação contra ataques. Para essa finalidade, os autores sugerem outras obras, como a *Joint Intelligence Preparation of the Battlespace*, *Kill Chain Analysis*, *Vulnerability Cover* e *Gaming*.

Assim, minha conclusão sobre o artigo lido é que o Modelo Diamante pode ser muito útil para orientar um analista sobre os passos que devem ser tomados após sofrer um ataque: dividi-lo em eventos, descobrir os fatores principais e os meta fatores de cada evento, aplicar o *pivoteamento analítico*, etc. A utilização das *linhas* e *grupos de atividades* também pode ser

uma boa base de ação para realizar tarefas de prevenção e estudo de ataques. Desse modo, o artigo lido é de grande valor para a área de segurança cibernética, contribuindo para a consolidação e desenvolvimento de sistemas de proteção.