MITRE ATT&CK PARA O SETOR AEROESPACIAL

Silvio R. A. de Oliveira Filho, Carlos R. A. Figueiredo e Cesar A. Marcondes
Instituto Tecnológico de Aeronáutica ITA

Resumo — Com o aumento da digitalização e da dependência tecnológica é necessário que as equipes de proteção cibernéticas se antecipem ao ataques. O framework do MITRE ATT&CK fornece informações cruciais de como foram realizados ataques cibernéticos, com o intuito de aumentar a resiliência de sistemas à esses ataques. Entendendo as formas de atuação é possível ainda, identificar os grupos atacantes, os APT. Existem grupos especializados em sistemas espaciais, como o APT33, assim, a proposta desse trabalho é apresentar uma proposta de MITRE ATT&CK focado nos Sistemas Aeroespaciais, de forma a proteger e tornar esses sistemas mais resilientes. Pois, esses sistemas, como os controles de espaço aéreos, bem como os sistemas espaciais, possuem diversas especificidades e vulnerabilidades, que são foco de Estados que patrocinam os ataques desses grupos.

I. INTRODUÇÃO

Com o avanço da digitalização na vida das pessoas e nas organizações, os ataques cibernéticos estão cada vez mais sofisticados, proficientes e difíceis de identificar. Mesmo com as ferramentas de proteção cada vez melhores, ainda é necessário para as equipes de defesa das instituições - *Blue Teams* - acompanhar essa evolução para responder e mitigar o ataque em tempo hábil.

Uma abordagem, para aumentar a proteção, é identificar formas de ação e padrões de ataques, que são conceitos que generalizam a inteligência de ameaças, melhoram e atualizam os sistemas de detecção e defesa de incidentes. Isso é possível construindo e mapeando a cronologia das técnicas, táticas e procedimentos (TTP) usados por atacantes, aproveitando recursos e informações compartilhadas da comunidade.

Entre os tipos de ameaças e atacantes, as mais sofisticados são as APTs (*Advanced Persistent Threat*), grupos altamente especializados, patrocinados por governos, possuem objetivos políticos e de espionagem. Uma forma de descrever um ataque desses grupos é o *framework*: *Cyber Security Kill Chain* (CSKC) [3], figura 1.

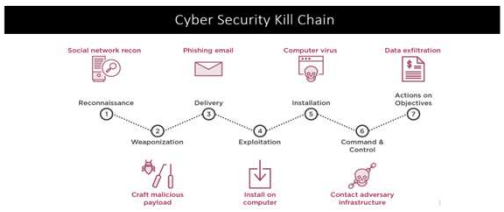

Fig. 1: Cyber Security Kill Chain

II. MITRE ATT&CK

Com a finalidade de mapear as TTPs dos ataques conhecidos, em 2013 foi criado outro *framework, o* MITRE ATT&CK (*Adversarial Tactics, Techniques, and Common Knowledge*) [5]. A ideia é traçar o perfil de comportamento dos atacantes cibernéticos, baseado em observações e descrições de ataques reais, divididos em três tipos de sistemas: Enterprise (Windows, macOS, Linux etc.), Sistemas Mobile e Sistemas de Controle Industrial (ICS). Como visto na figura 2.

O MITRE ATT&CK tem o modelo comportamental dos ataques divididos em 3 componentes:

- táticas são os objetivos de curto prazo (*Why*);
- técnicas são os mecanismos utilizados pelo atacante para atingir o objetivo (*How*);
- e agrupando o conhecimento comum do adversários, através da união das técnicas utilizadas e outros metadados (*Who*).

Fig. 2: Táticas do MITRE ATT&CK

III. APTS COM FOCO NO SETOR AEROESPACIAL

O setor aeroespacial de um país é considerado crítico. A comunicação e a navegação aéreas não podem ficar indisponíveis, caso haja o comprometimento de algum sistema de informação do controle aéreo. Essas interrupções, podem ser causadas por invasões cibernéticas, tanto em solo quanto nos próprios sistemas das aeronaves.

Diferentemente dos atacantes isolados, como foco financeiro, os APTs objetivam ataques em infraestrutura crítica com interesses de degradar a confiabilidade do controle do espaço aéreo e/ou adquirir segredos industriais sobre satélites e aeronaves, com o intuito de favorecer o Estado patrocinador.

Portanto, é de suma importância estudar APTs (observados na figura 3) que já tiveram foco no setor Aeroespacial e identificar suas técnicas de ação e mitigar esses ataques.

Fig. 3: APTs que possuem algum foco no setor aeroespacial

IV. APT 33

Um exemplo de grupo com foco aeroespacial, o APT33 também conhecido como Elfin, Magnallium e Holmium, é um grupo Iraniano que opera desde 2013 e tem como foco principal o setor Aeroespacial e o setor Petroquímico. Foram identificadas campanhas desse grupo em países do Oriente Médio, Estados Unidos e Coréia do Sul [4]. Como o Brasil possui esses dois setores citados, aeroespacial e petroquímico, bastante fortes, destacando-se empresas como Embraer e Petrobras, é de importância nacional o estudo das formas de atuação, ferramentas e técnicas descritas no MITRE ATT&CK, conforme figura 4, para mitigar esses tipos de ataques. Além dessas áreas, o Brasil tem alta confiabilidade no sistema de controle do espaço aéreo, sendo referência mundial [2] e, por isso, também pode ser um alvo com intenções políticas. Sendo primordial que medidas de defesa cibernética para esses sistemas sejam intensificadas.

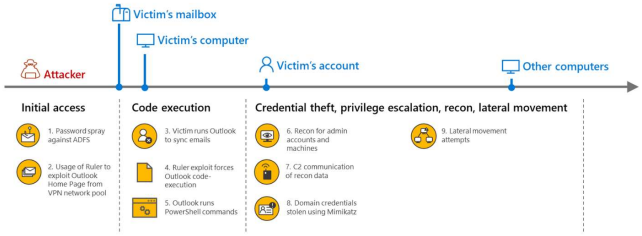

Fig. 4: Timeline de um ataque do grupo APT33

V. ATAQUES A SISTEMAS AEROESPACIAIS

Sistemas espaciais são alvos de ataques cibernéticos por diversos motivos como: falta de segurança dos sistemas antigos e com pouca capacidade de processamento; notoriedade do ataque, pois é bastante divulgado; e pelo alto custo dos equipamentos, entre outros motivos.

Tanto os segmentos de solo como os próprios satélites são bastante vulneráveis e são grandes desafios para a segurança cibernética. São esses desafios para o setor espacial [1], conforme demonstrado na figura 5, e ainda:

- Único ponto de falha para indústrias;
- Falta de padrões e regulamentações para a cibersegurança no Espaço;
- Ciclo de vida e cadeia de suprimentos são mais complexos;
- Uso generalizado de *software* comercial pronto para uso;
- Força de trabalho altamente especializado; e
- Restrições de recursos (técnicos e financeiros).

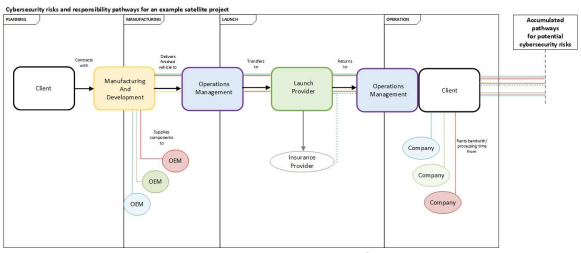

Fig. 5: Ataques na cadeia de suprimento de Sistema Espacial

VI. CONSIDERAÇÕES FINAIS

A crescente expansão de ameaças obriga as equipes de segurança a se protegerem cada vez mais. Para o setor aeroespacial, essa afirmação é ainda mais válida, e com o conhecimento de TTPs de ataques anteriores, obtidos por meio do MITRE ATT&CK, é possível identificar comportamentos de futuros APTs com mais facilidade e impedir campanhas de ataques nos níveis iniciais da *Cyber Security Kill Chain*.

Dessa forma, antecipando-se a ataques e melhorando a segurança de sistemas críticos e de elevado custo para a Força Aérea e para o Brasil.

REFERÊNCIAS

1. G. Falco. Cybersecurity principles for space systems. Journal of Aerospace Information Systems, 16(2):61–70, 2019.
2. A. Feu, J. A. Soares, C. H. Rosa, F. L. Madeira and R. Stanev. Relatório de avaliação operação do sistema de controle do espaço aéreo (SISCEAB), 2020.
3. E. M. Hutchins, M. J. Cloppert, and R. M. Amin. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains, 2011.
4. J. O'Leary, J. Kimble, K. Vanderlee, and N. Fraser.https://www.mandiant.com/resources/apt33-insights-into-iranian-cyber-espionage, 2017.
5. B. E. Strom, A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington, and C. B. Thomas. Mitre att&ck: Design and philosophy, 2020.