MARINHA DO BRASIL
DIRETORIA DE ENSINO DA MARINHA
CENTRO DE INSTRUÇÃO ALMIRANTE ALEXANDRINO

CURSO DE APERFEIÇOAMENTO AVANÇADO EM SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

TRABALHO DE CONCLUSÃO DE CURSO

ANÁLISE DA IMPORTÂNCIA DE SISTEMAS IDS EM MEIOS EMBARCADOS NA PREVENÇÃO CONTRA ATAQUES DDOS

PRIMEIRO-TENENTE DIEGO DOS SANTOS SILVA DE ARAÚJO

Rio de Janeiro
2023

PRIMEIRO-TENENTE DIEGO DOS SANTOS SILVA DE ARAÚJO

ANÁLISE DA IMPORTÂNCIA DE SISTEMAS IDS EM MEIOS EMBARCADOS NA PREVENÇÃO CONTRA ATAQUES DDOS

Monografia apresentada ao Centro de Instrução Almirante Alexandrino como requisito parcial à conclusão do Curso de Aperfeiçoamento Avançado em Segurança da Informação e Comunicações.

Orientador:
Prof. Dr. Davidson Rodrigo Boccardo

CIAA
Rio de Janeiro
2023

PRIMEIRO-TENENTE DIEGO DOS SANTOS SILVA DE ARAÚJO

ANÁLISE DA IMPORTÂNCIA DE SISTEMAS IDS EM MEIOS EMBARCADOS NA PREVENÇÃO CONTRA ATAQUES DDOS

Monografia apresentada ao Centro de Instrução Almirante Alexandrino como requisito parcial à conclusão do Curso de Aperfeiçoamento Avançado em Segurança da Informação e Comunicações.

Aprovada em _____

Banca Examinadora:

_____

CMG (RM1-EN) Gian Karlo Huback Macedo de Almeida – CIAA

_____

CT Rafael Gomes dos Santos - ComEsqdE-1

_____

Davidson Rodrigo Boccardo, D. Sc. – Hospital Israelita Albert Einstein

_____

Lucila Maria de Souza Bento, D. Sc. – UERJ

Dedico este trabalho à Deus, de onde provém toda a nossa força e conhecimento e à minha esposa, Bianca, pois tudo o que fazemos e nos dedicamos é em prol de nossa família.

AGRADECIMENTOS

Primeiramente agradeço a Deus pelo dom da vida e por ser minha maior fonte de inspiração e ensinamento. Sem Ele nada somos e nada faz sentido.

Também agradeço aos meus pais pela minha criação e por me ensinarem os valores de honestidade, integridade e por me mostrarem que tudo o que precisamos conquistar na vida é através de nossos próprios esforços.

Agradeço também o meu orientador, Prof. Dr. Davidson, por me abrir os olhos para o mundo acadêmico. As suas aulas sempre denotavam paixão pela arte do ensino e por trazer de forma tão didática assuntos relativamente complexos. Tenha certeza de que em mim foi despertada uma sede de conhecimento que será carregada para o resto da vida.

Agradeço aos meus amigos do quarto de SIC pela convivência desde 2011 e por compartilharem a rotina durante todo este período do curso. As nossas brincadeiras e colaboração tornaram nossos dias muito mais leves. Tenham certeza de que vocês são amigos que carregarei para toda vida.

À minha esposa e melhor amiga, Bianca, me faltam palavras para agradecer por todo o seu apoio e pelo seu amor. Só nós dois sabemos as nossas lutas diárias e o que fazemos para vencê-las. Obrigado por ser minha confidente, conselheira, mentora e por estar ao meu lado todos os dias. Você é a minha fonte de inspiração. Eu não poderia ter escolhido alguém melhor para estar ao meu lado. A nossa família é o que temos de mais precioso. Te amo.

“Nenhum homem é melhor do que uma máquina
e nenhuma máquina é melhor do que um homem
com uma máquina”
(Paul Tudor Jones)

ANÁLISE DA IMPORTÂNCIA DE SISTEMAS IDS EM MEIOS EMBARCADOS E A PREVENÇÃO CONTRA ATAQUES DDOS

RESUMO

Este trabalho tem por objetivo identificar as principais ameaças aos meios embarcados em um cenário de guerra. A situação geopolítica mundial tem demandado cada vez mais do mundo cibernético. Diferentemente do século passado, onde a maior demanda era por armas de infantaria e artilharia, hoje é preciso voltar nossos olhos ao mundo digital e entender como neutralizar o inimigo para garantir a soberania dos nossos meios. A principal linha de pesquisa foi a análise da ação do grupo APT28 e como ele atua para invadir e dominar sistemas digitais. Além disso, são apresentadas formas de ataques de negação de serviço, que visam interromper ou reduzir significativamente a velocidade de operação das comunicações e propor um sistema de detecção de intrusão como solução parcial na prevenção de ataques aos sistemas embarcados.

Palavras-chave: APT28; DDoS; DoS; Fancy Bear; IDS.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTAS DE SIGLAS E ABREVIATURAS

ACK	Acknowledge
AIDS	Anomaly-based Intrusion Detection System
DDoS	Distributed Denial of Service
DNS	Domain Name Server
DoS	Denial of Service
HIDS	Host-based Intrusion Detection System
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IP	Internet Protocol
NIDS	Network-based Intrusion Detection System
NTP	Network Transfer Protocol
RST	Reset
SIDS	Signature-based Intrusion Detection System
SYN	Sinchronize
UDP	User Datagram Protocol
VOIP	Voice Over IP

SUMÁRIO

1. INTRODUÇÃO

A Política Nacional de Defesa afirma que a Marinha do Brasil tem como propósito preparar e empregar o Poder Naval, a fim de contribuir para a Defesa da Pátria; para a garantia dos poderes constitucionais e, por iniciativa de qualquer destes, da lei e da ordem; para o cumprimento das atribuições subsidiárias previstas em Lei; e para o apoio à Política Externa (Brasil, 2020a).

Além disso, a Marinha deve dispor de meios capazes de detectar, identificar e neutralizar ações que representem ameaça nas Águas Jurisdicionais Brasileiras (AJB), como por exemplo: pesca ilegal, crimes ambientais, entre outros atos ilícitos. Para tal, o Poder Naval deverá também ser capaz de manter a segurança nas linhas de comunicação marítimas onde houver interesse nacional (Brasil, 2020a).

As comunicações entre navio e terra são realizadas através de equipamentos que operam nas frequências VHF, UHF, HF e MF, tanto para voz quanto para radiodados, além de links satelitais, que são utilizados para transmissão de dados e telefonia VOIP.

Quando um navio se afasta por distâncias maiores que 200 milhas náuticas da costa, a comunicação em VHF torna-se inviável, sendo necessário adotar o uso de faixas de frequências mais baixas, como HF ou MF, porém, essas faixas de frequências tornam impossível o estabelecimento de link de dados em taxas de transmissão aceitáveis, sendo utilizadas apenas para casos emergenciais.

Para que haja a transmissão de dados em taxas que suportem sistemas de criptografia mais avançados e de forma viável, é necessário estabelecer link de dados através de comunicações satelitais. Esse tipo de comunicação garante taxas de transmissão que variam entre 128Kbps e 4096Kbps, possibilitando suporte para tráfego de dados, videochamadas e ligações telefônicas via VOIP (Voice over IP).

1.1. Apresentação do Problema

Ao possibilitar o tráfego de dados, os navios ficam vulneráveis à ataques cibernéticos, caso não adotem sistemas de proteção adequados. O que de um lado representa um ganho substancial, por outro pode expor fragilidades indesejadas.

Um dos possíveis ataques é o *Denial of Service* (DoS) ou *Distibuted Denial of Service* (DDoS), que é uma tentativa de interromper o funcionamento de um servidor ou serviço de internet através de inundações de tráfego (Cloudflare, 2021).

Estando a uma longa distância da costa, este tipo de ataque pode comprometer seriamente as comunicações entre navio e terra, fazendo com que o meio recorra aos seus modos de comunicação emergenciais e diminua consideravelmente a sua capacidade de comunicação. Isso pode gerar problemas de segurança, coordenação e logística para as operações navais.

1.2. Justificativa e Relevância

De acordo com Cunningham (2020), desde que surgiram alegações de atores patrocinados pelo Estado russo visando as eleições presidenciais dos EUA em 2016, a extensão da interferência cibernética russa tornou-se cada vez mais divulgada e discutida pela mídia. Apesar de sua aparente novidade, é importante ressaltar que isso não é algo novo e vem acontecendo desde a década de 1990. No entanto, sob o comado do presidente Vladimir Putin, a Rússia tornou-se um dos atores mais eminentes no ciberespaço, quando se trata de execução de ações maliciosas.

A guerra de informação da Rússia não é uma ameaça exclusiva para a Europa e EUA, mas sim uma estratégia global que afeta cada região do mundo, separando-se em diferentes graus devido ao seu tamanho, massa e complexidade. A abordagem russa para a guerra de informação é holística e inclui ataques cibernéticos e operações de informação, com elementos coesos que trabalham em conjunto para alcançar os seus objetivos. Além disso, tal abordagem busca não se limitar apenas a minar as forças armadas de seus alvos, mas também influenciar as percepções da população-alvo de tal forma que favoreça os interesses russos (Cunningham, 2020).

Embora os ataques cibernéticos em grande escala só tenham se tornado possíveis na década de 1990, com advento da popularização da internet, as operações de informação são uma prática muito mais antiga - que o Kremlin usa há muito tempo. Os líderes soviéticos sempre entenderam o valor da informação e como ela poderia ser usada para influenciar as massas, tanto no país quanto no exterior. Posteriormente, a Federação Russa foi capaz de usar a internet para aumentar a eficácia da guerra de informação com baixo custo (Cunningham, 2020).

Ainda, de acordo com Cunningham (2020), ações cibernéticas atribuídas pela Rússia foram encontradas em 85 países, abrangendo um total de 6 continentes e 16 regiões do mundo, dentre elas: América Central, Ásia Central, África Oriental, Ásia Oriental, Europa Oriental, América do Norte, Europa do Norte, América do Sul, Sudeste Asiático, África Austral, Sul da Ásia, Europa do Sul, Ásia Ocidental e Europa Ocidental. Apesar de a maioria dos ataques estar centrada na Europa e nos EUA, também vemos regiões ao redor da Rússia sendo fortemente visadas, incluindo Ásia Central, Ásia Ocidental, Sul da Ásia e Ásia Oriental.

Figura 1 - Mapa de países-alvo da Federação Russa.

Fonte: Cunningham, 2020.

Após a dissolução da União Soviética, as responsabilidades de inteligência da KGB foram divididas em outros ramos de inteligência recém-criados. Dentre esses ramos, podemos citar o Serviço Federal de Segurança (FSB), o Serviço de Inteligência Estrangeira (SVR) e a Direção Principal do Estado-Maior General das Forças Armadas da Federação Russa (GU), que ficou mais conhecida por seu nome da era soviética, a Diretoria Principal de Inteligência (GRU) (Cunningham, 2020).

Acredita-se que essas três organizações estejam conectadas aos grupos de hackers russos mais importantes. O FSB é responsável pela contrainteligência, vigilância e supervisão na Federação Russa, apesar de estar se envolvendo cada vez mais em operações no exterior. O SVR realiza, principalmente, inteligência humana, mas as suas capacidades cibernéticas são inferiores ao FSB ou GRU. No entanto, o SVR trabalha em coordenação com o FSB e a GRU em operações cibernéticas. A GRU é diferente dos outros serviços de inteligência porque é o serviço de inteligência das forças armadas russas. Ela parece ser o grupo mais ativo, com acesso a grandes quantidades de recursos para apoiar suas operações cibernéticas. Acredita-se que a GRU seja a organização-mãe da APT28 e da *Sandworm Team* (Cunningham, 2020).

APT28 ou *Fancy Bear* é o APT (*Advanced Persistent Threat*) russo mais conhecido. Em 2015, o APT28 violou com sucesso as redes do Pentágono e, em 2016, as do Comitê Nacional Democrata, nos EUA. Acredita-se que ele seja o ator de ameaças russo com mais recursos, ativo desde pelo menos 2004 e acredita-se que seja afiliado ao GRU. Graças às capacidades tecnológicas e operacionais superiores da GRU, sua área de atuação é global. Esse grupo possui um grande conjunto de ferramentas de *malware* que desenvolve e expande continuamente. Eles geralmente usam uma combinação de *spear phishing* e registro de domínios falsos para violar sistemas inimigos (Cunningham, 2020).

As operações APT28 estão presentes em quase todas as partes do globo. Embora os seus principais alvos sejam os países da OTAN, houve uma transição para uma perspectiva mais global nos últimos oito anos (Cunningham, 2020).

1.3. Objetivos

1.3.1. Objetivo Geral

Esta pesquisa possui como objetivo geral analisar a aplicabilidade e importância da implementação de sistemas IDS (*Intrusion Detection System*) em sistemas embarcados através da ótica de atuação do grupo APT28.

1.3.2. Objetivos Específicos

Os objetivos específicos desta pesquisa são:

a) Caracterizar o grupo APT28, exemplificando as suas principais técnicas de ataque;
b) Identificar os principais riscos e vulnerabilidades dos sistemas de comunicações navais, especificamente sistemas que utilizam link de dados com acesso à internet;
c) Apresentar os principais ataques de negação de serviço e como eles influenciam na interrupção dos sistemas;
d) Apresentar o framework Mitre ATT&CK como uma ferramenta para avaliar e mitigar as ameaças do grupo APT28 nos sistemas embarcados; e
e) Propor um modelo de sistema IDS baseado no framework Mitre ATT&CK para proteger os sistemas de comunicações navais.

2. REFERENCIAL TEÓRICO

Para alcançar a compreensão do conhecimento proposto, serão apresentados os principais conceitos necessários ao entendimento dos mecanismos de ataque do APT28, suas consequências e formas de mitigação. Além disso, serão apresentados o funcionamento do framework Mitre ATT&CK (*Adversarial Tactics, Tecnhiques, and Common Knowledge*), ataques DDoS mais comuns e sistemas IDS que podem ser aplicados para a solução destes problemas.

2.1. Mitre ATT&CK

Segundo Strom et al. (2020), o MITRE ATT&CK é uma base de conhecimento e modelo elaborado sobre o comportamento dos adversários cibernéticos, refletindo as várias fases do ciclo de ataque de um adversário e as plataformas visadas por eles. O ATT&CK concentra-se em como adversários externos operam e comprometem redes de informações de computadores. Em um nível mais alto, o ATT&CK é um modelo comportamental que consiste nos seguintes componentes principais:

a) **Táticas:** que indicam os objetivos táticos de curto prazo dos adversários durante um ataque;
b) **Técnicas:** que descrevem os meios pelos quais os adversários atingem seus objetivos táticos;
c) **Subtécnicas:** que descrevem meios mais específicos pelos quais os adversários atingem seus objetivos táticos; e
d) Uso documentado pelo adversário de técnicas, seus procedimentos e outros metadados.

2.1.1. Histórico

O ATT&CK foi criado a partir da necessidade de sistematizar o comportamento de adversários como parte da realização de exercícios estruturados de emulação de adversários no ambiente de pesquisa FMX do Mitre. Criado em 2010, o FMX proporcionou uma capacidade de "laboratório vivo" que permitiu aos pesquisadores acesso a uma área da rede corporativa do Mitre para implantar ferramentas, testar e refinar ideias sobre como detectar ameaças de forma mais eficaz. O Mitre começou a pesquisar fontes de dados e processos analíticos dentro do FMX para detectar ameaças persistentes avançadas (APTs) de forma mais rápida, adotando uma mentalidade de "assumir a violação". Exercícios de ciberjogos foram realizados periodicamente

para emular adversários dentro do ambiente altamente monitorado, e a caça a ameaças foi realizada para testar hipóteses analíticas com base nos dados coletados. O objetivo era melhorar a detecção pós-comprometimento de ameaças que penetravam em redes empresariais por meio de telemetria e engenharia social. A métrica principal de sucesso era: "Como estamos indo na detecção de comportamento de adversários documentados?". Para trabalhar efetivamente em direção a esse objetivo, mostrou-se útil categorizar o comportamento observado em grupos de adversários do mundo real relevantes e usar essas informações para realizar exercícios controlados que emulam esses adversários no ambiente FMX. O ATT&CK foi usado tanto pela equipe de emulação de adversários (para o desenvolvimento de cenários) quanto pela equipe de defensores (para medir o progresso analítico), tornando-se uma força motriz na pesquisa FMX (Strom et al, 2020).

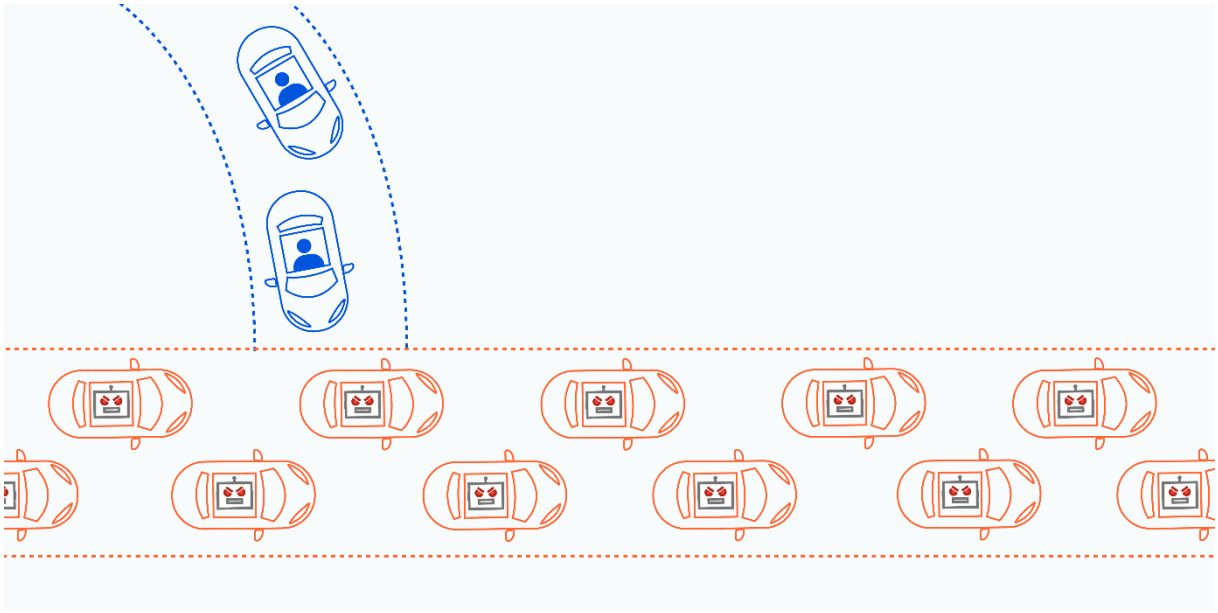
O primeiro modelo ATT&CK foi criado em setembro de 2013 e tinha como foco principal o ambiente empresarial Windows. Ele foi refinado por meio de pesquisa e desenvolvimento interno e posteriormente lançado publicamente em maio de 2015 com 96 técnicas organizadas em 9 táticas. Desde então, o ATT&CK experimentou um crescimento enorme com base nas contribuições da comunidade de segurança cibernética. O ATT&CK original foi expandido em 2017 para incluir Mac e Linux, sendo referido como ATT&*CK for Enterprise*. Um modelo complementar chamado PRE-ATT&CK foi publicado em 2017 para focar no comportamento "antes da exploração". O ATT&CK *for Mobile* também foi publicado em 2017 para se concentrar no comportamento no domínio específico de dispositivos móveis. O ATT&CK for Cloud foi publicado em 2019 como parte do *Enterprise* para descrever o comportamento em relação a ambientes e serviços em nuvem. O ATT&CK for ICS foi publicado em 2020 para documentar o comportamento em sistemas de controle industrial (Strom et al, 2020).

2.2. ANATOMIA DO ATAQUE DDOS

2.2.1. Definição

Um ataque DDoS pode ser entendido como um “engarrafamento digital”. Cada componente de rede, como servidores, *switches* ou *access points* possui um número máximo de requisições que podem ser processadas (Cloudflare Inc., 2020). Caso o número de requisições seja superior ao que o sistema pode suportar, ele ficará muito lento ou indisponível para novos usuários, como na metáfora apresentada na Figura 2:

Figura 2 - Metáfora de representação de um ataque DDoS.



Fonte: Cloudflare, 2020.

Segundo Mello, Junior e Rocha (2010), um ataque de negação de serviço é composto por um atacante (aquele que deseja causar a negação do serviço), um ou mais computadores *mestre* e, sob o comando deste, milhares de outros computadores, chamados *escravos*. O ataque consiste em fazer com que os escravos se preparem para acessar um determinado recurso em um determinado servidor num mesmo instante. Ao atingir o número máximo de requisições suportadas, o sistema pode apresentar lentidão, reiniciar ou ficar travado.

Um dos ataques mais famosos foi o da *Botnet Mirai*, em 2016. O nome *Botnet* vem da junção de *Bot* (Robô) com *Network* (Rede), que é uma rede de computadores que foram comprometidos por um *malware* específico e são controladas remotamente por um atacante. Esses computadores ou dispositivos comprometidos são chamados de *zumbis* e são usados para realizar tarefas maliciosas, como ataques DDoS. No caso da *Botnet Mirai*, ela foi a responsável por dificultar o acesso a sites como *Twitter, Amazon* e portais de notícias através do ataque contra o provedor de DNS *Dyn* (*Center for internet security*, 2021).

Os principais ataques DDoS podem se valer das seguintes técnicas:

a) UDP Flood;
b) ICMP Flooding;
c) TCP Reset Flooding; e
d) SYN Flooding.

Estes ataques têm por objetivo sobrecarregar a largura de banda da rede ou dos recursos de um servidor/sistema alvo, utilizando uma quantidade massiva de tráfego de dados, tornando os serviços inacessíveis para usuários legítimos. Mesmo sendo caracterizado por uma quantidade de tráfego massiva, ele não precisa de grandes quantidades de dados para ser gerado (Cloudflare Inc., 2020).

2.2.1.1. UDP Flood

UDP é um protocolo bastante utilizado em comunicações em tempo real, como streaming, telefonia VoIP, entre outros. A sua característica principal é ser um protocolo *stateless* (sistemas em que cada solicitação ou interação é tratada de forma independente, sem levar em consideração qualquer contexto anterior), diferentemente do protocolo TCP, que é *stateful* (sistemas que mantêm informações sobre o estado das interações ou sessões). Neste caso, não é necessário nenhum tipo de estabelecimento de conexão e não é utilizada nenhuma comunicação para informação de estado (Cloudflare Inc., 2020).

O UDP funciona da seguinte maneira:

a) O cliente envia um pacote UDP para uma porta do servidor;
b) O servidor verifica se há algum serviço ativo na porta; e
c) Se não há nenhum serviço ativo nesta porta, o servidor retorna uma mensagem de "ICMP *host unreacheble*".

No caso do UDP Flood, o atacante envia uma grande quantidade de pacotes UDP a taxas altíssimas, visando consumir recursos do sistema atacado, como memória e capacidade de processamento, fazendo com que ele se torne indisponível para outros usuários legítimos. Porém, se o atacante utilizar o seu próprio IP como endereço fonte, cada pacote UDP será respondido com um pacote ICMP do servidor, fazendo com que o próprio atacante sofra o UDP Flooding (Cloudflare Inc., 2020).

A chave para a condução de um ataque DDoS bem-sucedido é o DNS *spoofing*, onde o atacante mascara o seu endereço IP, garantindo que todos os pacotes ICMP serão enviados para o IP mascarado. Isso faz com que o atacante consiga consumir os recursos de memória e CPU do servidor/serviço atacado e deixe de processar requisições de tráfego legítimo (Cloudflare Inc., 2020).

2.2.1.2. ICMP Flooding

O ICMP é frequentemente associado ao comando "*ping*", utilizado para verificar a conectividade entre os dispositivos em uma rede. Este comando envia solicitações ICMP *"echo*

request" a um dispositivo remoto e aguarda a resposta *"echo reply"*. Caso o dispositivo esteja ativo e conectado, o dispositivo solicitante receberá a resposta (AKAMAI INC., 2021).

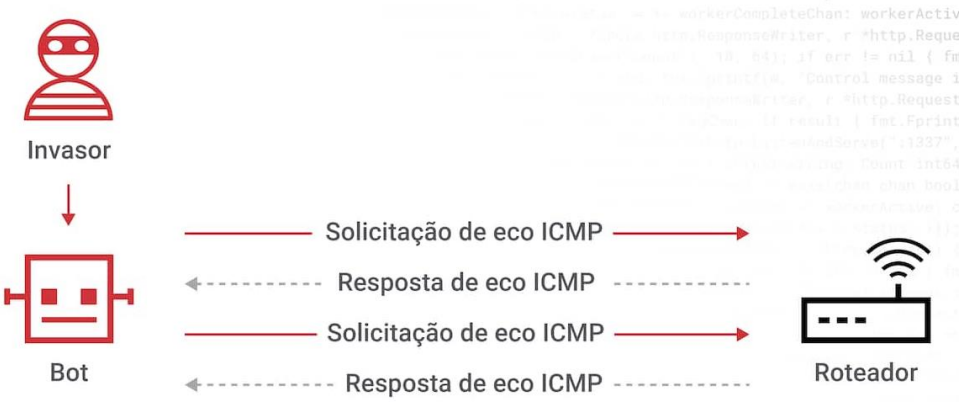
Além da verificação da conectividade, o ICMP é utilizado para relatar erros de roteamento, através da mensagem de "host ou rede inatingível", redirecionamento de roteamento e fragmentação de pacotes (Akamai Inc., 2021).

Quando um servidor ou outro dispositivo recebe a mensagem *"echo request"*, ele utiliza recursos de processamento e largura de banda para gerar a mensagem *"echo reply"*. O ataque de ICMP Flooding visa explorar a utilização destes recursos e sobrecarregar a largura de banda do servidor atacado (Cloudflare Inc., 2020).

O atacante então envia diversos pacotes ICMP, de origem real ou falsos (através de técnicas de *spoofing*), esperando a resposta do servidor alvo, que retorna o mesmo número de pacotes enviados até que todo o processamento ou largura de banda seja consumido, causando a interrupção dos serviços. É importante ressaltar que, por conta da grande largura de banda consumida, outros dispositivos de rede próximos podem ser afetados (Akamai Inc., 2021).

O ICMP Flooding pode ser realizado a partir de uma única máquina ou através de uma *BotNet*, causando um ataque em maior escala (Akamai Inc., 2021). Na Figura 3 está um exemplo de como este ataque é realizado:

Figura 3 – Representação de um ataque ICMP Flooding



Fonte: Akamai Inc., 2021

Esses ataques são facilmente mitigáveis, quando utilizados como vetor único de ataque, bastando, por exemplo, desativar a funcionalidade ICMP do dispositivo visado. O ponto negativo é que, ao desativar esta funcionalidade, perde-se a capacidade de testes de conectividade com o dispositivo, que é um ponto importante para comunicações de dados (Akamai Inc., 2021).

2.2.1.3. TCP RESET Flooding

Assim como o UDP, o TCP é um protocolo que permite a conexão entre dois dispositivos quaisquer. A diferença é que o TCP é um protocolo orientado à conexão, ou seja, um protocolo que garante a entrega de dados (Wallarm Inc., 2021).

Antes de iniciar a troca de dados, é utilizado um processo chamado "*Three Way Handshake*" (handshake de três vias), que consiste nos seguintes processos:

a) O dispositivo que inicia a conexão, chamado cliente, envia um pacote TCP SYN para o dispositivo que irá receber a conexão, chamado servidor;
b) O servidor responde com um pacote SYN-ACK; e
c) O cliente finaliza o handshake enviando um pacote ACK.

Após estabelecida a conexão, os dispositivos podem começar a trocar dados. Os dados são fragmentados em pacotes menores e são montados de volta no destino. Porém, é preciso considerar que tanto o cliente quanto o servidor possuem limites de processamento para esses pacotes. Para que não haja sobrecarga no recebimento dos pacotes, é realizado um controle de fluxo, que estabelece janelas de recepção de dados para indicar ao remetente a quantidade de dados que ele pode receber antes da sobrecarga (Wallarm Inc., 2021).

Assim que o dispositivo recebe os dados TCP, ele envia confirmações de recebimento de volta ao remetente, informando que os dados foram recebidos com sucesso. Se o remetente não receber a confirmação dentro de um período pré-estabelecido, ele envia novamente os dados para garantir que o destinatário recebeu todas as informações solicitadas (Wallarm Inc., 2021).

Porém, existe mais um sinalizador, chamado RST. Este sinalizador tem por objetivo encerrar a conexão caso ocorra algum problema, análogo a um botão do pânico virtual, onde a conexão é encerrada abruptamente (Santos; Gomes, 2011). Dentre os problemas de conexão mais comuns, podemos destacar:

a) **Conexão rejeitada:** quando um servidor recebe o pedido de conexão, mas não pode atender por algum motivo;
b) **Conexão encerrada abruptamente:** ocorre quando uma das partes da conexão TCP deseja encerrar a comunicação imediatamente. Geralmente pode ocorrer quando há um erro grave na aplicação ou na comunicação;
c) **Detecção de pacotes inválidos:** caso o dispositivo receba um pacote que não faz sentido dentro do contexto da conexão, ele pode responder com um RST e encerrar a conexão;

d) ***Timeout* de conexão:** Se uma parte não recebe resposta após tentar estabelecer uma conexão e espera por um determinado período, ela pode enviar um pacote RST para encerrar a tentativa de conexão; e
e) **Proteção contra ataques:** caso haja um ataque SYN *flooding*, onde um atacante tenta inundar o servidor com solicitações de conexões falsas, o servidor poderá enviar a mensagem RST para encerrar a comunicação.

No ataque TCP RESET Flooding, o atacante precisará se posicionar como um *man-in-the-middle* para encerrar as conexões entre duas estações. O atacante executa o seu ataque através de um simples pacote de dados com poucos bytes de tamanho (Heaton, 2020).

A realização se dá ao analisar as conexões entre as estações, obter os dados da conexão e enviar mensagens RST falsas para uma das partes. A chave para o sucesso do ataque se dá na capacidade do atacante de se infiltrar na conexão e enviar a mensagem RST como se fosse ou cliente ou servidor (Heaton, 2020).

Uma das formas de mitigar este ataque é através do uso do IPSec, que exige uma camada extra de autenticação do IP no envio dos pacotes (Heaton, 2020).

2.2.1.4. SYN Flooding

Como explicado no tópico anterior, uma das formas de esgotar os recursos do servidor é através do excesso de requisições. No ataque de SYN Flooding, o atacante envia milhares de pacotes SYN através de endereços IP ilegítimos. O servidor então envia um SYN-ACK e aguarda a resposta para validar a conexão (F5 Networks Inc., 2022).

No caso de poucas conexões, o servidor pode esperar o tempo de *time-out* e enviar um sinal RST para encerrar a conexão, porém, ao se deparar com muitas requisições, o serviço ficará sobrecarregado, apresentando lentidão ou indisponibilidade.

Este tipo de ataque pode ser realizado de três maneiras distintas:

a) **Ataque direto:** neste caso, o atacante não mascara o IP ao atacar. Ele apenas envia pacotes SYN e, através de regras de firewall, ele impede que a o seu dispositivo responda às requisições de SYN-ACK. Este é um ataque raramente utilizado, pois o atacante pode ser facilmente identificado e bloqueado (Cloudflare Inc., 2021);
b) **Ataque falsificado:** o atacante pode falsificar o seu IP para atacar o usuário. Desta forma, os esforços de mitigação são maiores, pois a sua identidade se torna mais difícil de ser descoberta (Cloudflare Inc., 2021); e

c) **Ataque distribuído de negação de serviço:** se o ataque for criado através de *BotNets*, a probabilidade de identificar a origem do atacante é bem pequena. Para aumentar o nível de dissimulação, o atacante pode falsificar o IP de cada dispositivo distribuído. Este é o tipo de ataque mais eficiente (Cloudflare Inc., 2021).

2.3. APT28 (Fancy Bear)

O APT28 é um grupo de ameaças que foi atribuído à unidade militar 85 da Direção Principal de Inteligência do Estado-Maior (GRU) da Rússia, 26165º Centro de Serviços Especiais Principais (GTsSS). Esse grupo está ativo pelo menos desde 2004 (Ruel et al., 2017).

O *modus operandi* deste grupo, de acordo com o apresentado no framework Mitre ATT&CK, é o seguinte:

a) Acesso Inicial;
b) Execução;
c) Persistência;
d) Escalonamento de privilégios;
e) Evasão de Defesas;
f) Acesso a credenciais;
g) Descoberta;
h) Movimentação lateral;
i) Coleta;
j) Comando e controle;
k) Exfiltração; e
l) Impacto.

Todos os tópicos apresentados acima são técnicas utilizadas por esse grupo para realizar ataques em sistemas-alvo. Como veremos a seguir, nem todos serão são utilizadas sequencialmente, assim como nem todos serão utilizadas na realização de um ataque.

Neste trabalho, serão apresentadas apenas as que são detectáveis ou mitigáveis através de sistemas IDS, de acordo com o exposto no framework Mitre ATT&CK.

2.3.1. Acesso Inicial

O Acesso Inicial consiste em técnicas que usam diferentes formas de entrar em uma rede. Essas técnicas permitem obter uma posição inicial dentro da rede. Os pontos de apoio que são conseguidos por meio do Acesso Inicial podem possibilitar o acesso contínuo, como por

exemplo, usando contas válidas e serviços remotos externos, ou podem ter um uso limitado, se as senhas forem alteradas.

2.3.1.1. Comprometimento por visita

Os adversários podem conseguir acesso a um sistema quando um usuário visita um site durante a navegação normal na internet. Com essa técnica, o navegador do usuário pode ser alvo de uma exploração, mas os adversários também podem usar sites comprometidos para outras ações, como obter o *Token* de Acesso ao Aplicativo (Sakowicz; Agrawal, 2018).

Existem várias maneiras de enviar um código de exploração para um navegador, incluindo:

a) Um site legítimo é comprometido quando os adversários injetam algum tipo de código malicioso, como JavaScript, iFrames e scripts entre sites (Sakowicz; Agrawal, 2018);
b) Os arquivos de script que são fornecidos a um site legítimo a partir de um armazenamento em nuvem público e editável são alterados por um adversário (Sakowicz; Agrawal, 2018);
c) Os anúncios maliciosos são comprados e distribuídos por meio de provedores de anúncios legítimos (ou seja, Malvertising) (Sakowicz; Agrawal, 2018);
d) As interfaces de aplicativos web integradas são usadas para inserir qualquer outro tipo de objeto que possa ser usado para mostrar conteúdo da web ou conter um script que seja executado no navegador do usuário que visita o site (por exemplo, postagens em fóruns, comentários e outros conteúdos da *web* que podem ser controlados pelo usuário) (Sakowicz; Agrawal, 2018); e
e) Muitas vezes, o site usado por um adversário é visitado por uma comunidade específica, como governo, uma indústria específica ou região, onde o objetivo é comprometer um usuário específico ou grupo de usuários com base em um interesse comum. Esse tipo de campanha direcionada é frequentemente chamada de comprometimento estratégico na *web* ou ataque de *watering hole* (Sakowicz; Agrawal, 2018).

Um processo típico de comprometimento por acesso automático se dá da seguinte forma:

a) Um usuário visita um site que é usado para hospedar o conteúdo controlado pelo adversário;

b) Os scripts são executados automaticamente, normalmente verificando as versões do navegador e dos plug-ins para encontrar uma versão potencialmente vulnerável;
c) O usuário pode ser induzido a colaborar com esse processo, ativando scripts ou componentes ativos do site e ignorando caixas de diálogo de alerta;
d) Ao encontrar uma versão vulnerável, o código de exploração é enviado ao navegador;
e) Se a exploração for bem-sucedida, ela dará ao adversário a execução de código no sistema do usuário, a menos que outras proteções estejam em vigor; e
f) Em alguns casos, uma segunda visita ao site após a verificação inicial é necessária antes que o código de exploração seja enviado.

O objetivo dessa técnica é explorar o software em um dispositivo do cliente ao visitar um site. Isso geralmente dará a um adversário acesso a sistemas na rede interna em vez de sistemas externos, que podem estar em uma DMZ (Sakowicz; Agrawal, 2018).

Os adversários também podem usar sites comprometidos para levar um usuário a um aplicativo malicioso projetado para roubar tokens de acesso a aplicativos, como tokens OAuth, para obter acesso a aplicativos e informações protegidos. Esses aplicativos maliciosos são entregues por meio de pop-ups em sites confiáveis (Sakowicz; Agrawal, 2018).

2.3.2. Comando e controle

Comando e controle referem-se a técnicas que os adversários podem usar para se comunicar com sistemas que estão sob seu domínio dentro de uma rede de vítimas. Os adversários geralmente tentam simular o tráfego normal e esperado para evitar a detecção. Existem muitas formas de um adversário estabelecer comando e controle com diferentes graus de discrição, dependendo da estrutura da rede e das defesas da vítima (Mitre, 2019).

2.3.2.1. Transferência de ferramentas de ingresso

Os adversários podem transferir ferramentas ou outros arquivos de um sistema externo para um ambiente comprometido. Ferramentas ou arquivos podem ser copiados de um sistema externo controlado pelo adversário para a rede da vítima através do canal de comando e controle ou por meio de protocolos alternativos, como FTP. Uma vez presentes, os adversários também podem transferir/distribuir ferramentas entre os dispositivos da vítima dentro de um ambiente comprometido (Page; Wee, 2017).

Os arquivos também podem ser transferidos usando vários serviços da web, além de ferramentas nativas ou disponíveis no sistema da vítima (Page; Wee, 2017).

2.3.3. Exfiltração

A exfiltração envolve técnicas que os adversários podem usar para roubar dados da sua rede. Depois de coletar dados, os adversários geralmente os empacotam para evitar a detecção ao removê-los. Isso pode incluir compressão e criptografia. As técnicas para extrair dados de uma rede alvo normalmente incluem transferi-los pelo seu canal de comando e controle ou um canal alternativo e podem incluir a imposição de limites de tamanho na transmissão (Mitre, 2018).

2.3.3.1. Limites de tamanho de transferência de dados

Um adversário pode exfiltrar dados em blocos de tamanho fixo em vez de arquivos inteiros ou limitar tamanhos de pacotes abaixo de determinados limites. Essa abordagem pode ser usada para evitar o disparo de alertas de limite de transferência de dados de rede (Mitre, 2017).

2.3.4. Impacto

O impacto envolve técnicas que os adversários usam para interromper a disponibilidade ou comprometer a integridade manipulando processos operacionais e de negócios. As técnicas usadas para o impacto podem incluir a destruição ou alteração de dados. Em alguns casos, os processos de negócios podem parecer normais, mas podem ter sido modificados para beneficiar os objetivos dos adversários. Essas técnicas podem ser usadas por adversários para atingir seu objetivo final ou para fornecer cobertura para uma violação de confidencialidade (Mitre, 2019).

2.3.4.1. Network Denial of Service

Os adversários podem realizar ataques de negação de serviço (DoS) na rede para degradar ou bloquear a disponibilidade de recursos destinados aos usuários. Como apresentado em tópicos anteriores, o DoS na rede pode ser realizado esgotando a largura de banda da rede da qual os serviços dependem. Exemplos de recursos incluem sites específicos, serviços de e-mail, DNS e aplicativos baseados na web (Manral; Weizman, 2019).

Um DoS de rede ocorrerá quando a capacidade de largura de banda da conexão de rede com um sistema for esgotada devido ao volume de tráfego mal-intencionado direcionado

ao recurso ou às conexões de rede e dispositivos de rede dos quais o recurso depende. Por exemplo, um adversário pode enviar 10 Gbps de tráfego para um servidor hospedado por uma rede com uma conexão de 1 Gbps com a Internet. Esse tráfego pode ser gerado por um único sistema ou vários sistemas espalhados pela internet, o que é comumente chamado de DoS distribuído (DDoS) (Manral; Weizman, 2019).

2.4. IDS

Invasão pode ser definida como qualquer tipo de atividade não autorizada que cause prejuízos a um sistema de informação. Isso significa que qualquer ataque que possa representar um risco à confidencialidade, integridade ou disponibilidade das informações será considerado uma invasão. Por exemplo, atividades que impeçam os serviços de computador de atender aos usuários legítimos são consideradas uma invasão (Khraisat et al, 2019).

O objetivo de um IDS é detectar diferentes tipos de atividades maliciosas na rede e no computador, que não podem ser bloqueadas por um firewall tradicional. Isso é essencial para garantir alta proteção contra ataques que afetem a disponibilidade, integridade ou confidencialidade dos sistemas de computação (Khraisat et al, 2019).

Os IDS podem ser classificados em dois grupos: Sistema de Detecção de Intrusão Baseado em Assinatura (SIDS) e Sistema de Detecção de Intrusão Baseado em Anomalias (AIDS).

2.4.1. Sistema de Detecção de Intrusão Baseado em Assinatura (SIDS)

Segundo Khraisat et al (2019), os sistemas de detecção de intrusão por assinatura (SIDS) são baseados em técnicas de reconhecimento de padrões para identificar um ataque previamente conhecido.

Nos SIDS, métodos de reconhecimento são usados para detectar uma intrusão anterior. Em outras palavras, quando uma assinatura de intrusão coincide com a assinatura de uma invasão anterior que já está no banco de dados de assinaturas, um alerta é acionado (Khraisat et al, 2019).

Nos SIDS, os registros do host são analisados para encontrar sequências de comandos ou ações que foram previamente reconhecidas como malware ou outras atividades maliciosas. No entanto, o SIDS tem limitação para detectar ataques de *zero day*, pois nenhuma assinatura correspondente existe no banco de dados até que a assinatura do novo ataque seja obtida e armazenada (Khraisat et al, 2019).

As abordagens tradicionais do SIDS analisam pacotes de rede e tentam compará-los com um banco de dados de assinaturas, mas essas técnicas são incapazes de identificar ataques que envolvem vários pacotes. Como o malware moderno é mais complexo, pode ser necessário extrair informações de assinatura em vários pacotes. Isso requer que o IDS reconstrua o conteúdo de pacotes anteriores (Khraisat et al, 2019).

A taxa crescente de ataques de *zero day* tornou as técnicas de SIDS progressivamente menos eficientes, pois não há assinatura prévia para tais ataques. Variantes polimórficas do malware e a crescente quantidade de ataques direcionados podem comprometer ainda mais a adequação desse paradigma tradicional. Uma possível solução para esse problema seria o uso de técnicas de AIDS, que operam definindo o perfil do que é um comportamento normal e não do que é anormal, que será descrito a seguir (Khraisat et al, 2019).

2.4.2. Sistema de Detecção de Intrusão Baseado em Anomalias (AIDS)

Segundo Khraisat et al (2019), na AIDS, um modelo normal do comportamento de um sistema de computação é criado usando aprendizado de máquina, métodos baseados em estatística ou baseados em conhecimento. Qualquer desvio significativo entre o comportamento observado e o modelo é considerado uma anomalia, que pode ser interpretada como uma invasão. O conceito por trás do funcionamento é que o comportamento mal-intencionado difere do comportamento típico do usuário. Portanto, o comportamento de usuários “anormais” que diferem do comportamento “padrão” é considerado como intrusão.

O desenvolvimento da AIDS envolve duas fases: a fase de treinamento e a fase de teste. Na fase de treinamento, o perfil de tráfego normal é usado para construir um modelo de comportamento normal e, em seguida, na fase de teste, um novo conjunto de dados é usado para avaliar a capacidade do sistema de detectar intrusões desconhecidas (Khraisat et al, 2019).

A principal vantagem da AIDS é a capacidade de identificar ataques de *zero day*, pois o reconhecimento da atividade anormal do usuário não depende de um banco de dados de assinaturas (Khraisat et al, 2019). Além disso, a AIDS tem vários benefícios:

a) **Descoberta de atividades maliciosas internas:** se um invasor começar a fazer transações em uma conta roubada e que não se enquadra na atividade típica do usuário, ele criará um alarme; e
b) **Personalização de perfis:** o cibercriminoso não consegue reconhecer o que é um comportamento normal do usuário sem criar um alerta no sistema.

No quadro 1 está representada uma tabela com as vantagens e desvantagens de cada método:

Quadro 1 – Correlação entre SIDS e AIDS

Método de detecção	Vantagens	Desvantagens
SIDS	- Eficiente para identificar intrusões com baixo número de alarmes falsos; - Alta velocidade na detecção de intrusão; e - Fácil implementação.	- Precisa de atualizações constantes; - Quando há alterações nas variantes, mesmo que pequenas, o sistema encontrará dificuldades na detecção; - Não imune a ataques de *zero day*.
AIDS	- Pode ser implementado para detectar ataques novos; e - Pode ser usada na criação de novas assinaturas de intrusão.	- Alto número de alarmes positivos; - Dificuldade de definir o que é um perfil normal em sistemas de computação dinâmicos; e - Necessário treinamento inicial

Fonte: Khraisat et al, 2019

2.4.3. Métodos adicionais

Os tópicos anteriores classificaram os IDS quanto à sua forma de identificar intrusões. Mas, além disso, o IDS também pode ser classificado de acordo com as fontes de dados de entrada (Khraisat et al, 2019).

Em termos de fontes de dados, existem dois tipos principais de tecnologias IDS, que são os IDS baseados em host (HIDS) e os IDS baseados em rede (NIDS).

O HIDS examina dados provenientes do sistema hospedeiro e de fontes de auditoria, como sistema operacional, registros de servidor de janela, registros de *firewalls*, auditorias do sistema de aplicação ou registros de banco de dados. O HIDS pode detectar ataques internos que não envolvem tráfego de rede (Khraisat et al, 2019).

O NIDS monitora o tráfego de rede obtido de uma rede por meio da captura de pacotes, do *NetFlow* e de outras fontes de dados de rede. O IDS baseado em rede pode ser usado para monitorar vários computadores que fazem parte de uma mesma rede, sendo também capaz de monitorar as atividades maliciosas externas que podem ser iniciadas por uma ameaça externa em uma fase anterior, antes que as ameaças se propaguem para outro sistema de computação.

Por outro lado, os NIDSs têm capacidade limitada de inspecionar todos os dados em uma rede de alta largura de banda devido ao volume de dados que circulam pelas modernas redes de comunicação de alta velocidade (Khraisat et al, 2019).

3. METODOLOGIA

Neste capítulo serão apresentadas as classificações da pesquisa, bem como os métodos utilizados para a coleta e tratamento dos dados, além de abordar as limitações do método.

3.1. Classificação da Pesquisa

Segundo Kauark, Manhães e Medeiros (2010), existem várias formas de classificar as pesquisas. Essas formas dependerão da abordagem, do propósito e dos dados. Para isso, é necessário que o pesquisador saiba utilizar os instrumentos adequados para encontrar respostas ao problema que ele tenha levantado.

Do ponto de vista da abordagem do problema, a pesquisa pode-se enquadrar como pesquisa Qualitativa, uma vez que foi concentrada na compreensão e na interpretação dos significados, percepções, experiências e conceitos subjacentes a um fenômeno específico.

3.1.1. Classificação Quanto aos Fins

De acordo com Gil (2007), do ponto de vista dos objetivos, a pesquisa pode ser de caráter exploratório, descritivo ou explicativo.

Por se tratar de uma pesquisa onde foram realizados levantamentos bibliográficos e para obter maior familiaridade com o problema, esta pesquisa pode ser enquadrada como caráter exploratório.

3.1.2. Classificação Quanto aos Meios

Os procedimentos técnicos podem ser definidos de acordo com as seguintes categorias: Pesquisa Bibliográfica, Pesquisa Documental, Pesquisa Experimental, Estudo de Caso, Pesquisa E*x Post Facto,* Pesquisa-Ação e Pesquisa Participante (Gil, 2007).

Neste trabalho, os critérios de pesquisa adotados quanto aos meios foram a Pesquisa Bibliográfica e Pesquisa Documental, justificado pela ampliação do embasamento teórico com referências acadêmicas, acesso a documentos históricos para contexto, verificação de dados e a possibilidade de explorar diferentes perspectivas sobre o tema. Esses métodos permitem uma análise abrangente, fundamentada e validada por fontes confiáveis.

3.2. Limitações do Método

Ao abordar a importância do estudo das aplicações dos IDS em meios embarcados, foram levantados cerca de 136 grupos hackers conhecidos, todos listados no framework Mitre ATT&CK.

A motivação para a escolha destes grupos foram as recentes mudanças no cenário geopolítico atual e a implementação em grande escala de “armas” cibernéticas. Segundo Mitre (2020), podemos dar destaque a 3 grupos de grande relevância:

a) APT19, ou *Cozy Bear*;
b) APT41, ou *Barium*; e
c) APT28, ou *Fancy Bear.*

Além do método de atuação, o APT28 foi escolhido para esta pesquisa devido ao seu ataque, realizado em 2016, que violou com sucesso as redes do Pentágono, ao ataque realizado em 2018, que resultou no vazamento de documentos da Agência Mundial Antidoping e a campanha de desinformação contra a vacina Pfizer-BioNTech, em 2020 (Cunningham, 2020).

Este trabalho teve como limitação a ausência de aquisição de modelos ou ferramentas prontas para simulação dos ataques representados. Somado a isso, a principal fonte de consulta foi o framework MITRE ATT&CK, que possui informações atualizadas constantemente, mas que não esgotam todas as possibilidades de atuação do grupo APT28, visto que, ao se tratar de um grupo ligado a um órgão governamental, pouco se sabe sobre métodos adicionais de atuação, os equipamentos utilizados e a motivação por trás da sua atuação.

4. DESCRIÇÃO E ANÁLISE DOS RESULTADOS

No Capítulo 2, foi apresentado todo o referencial teórico que embasa esta análise, de forma a possibilitar o entendimento do funcionamento de um ataque DDoS, do modo de operação do grupo APT28 e do funcionamento geral do IDS.

Na Seção 2.3 foi apresentada a metodologia utilizada pelo grupo APT28 para se infiltrar em sistemas e a descrição do seu modo de execução. Ao todo, foram levantadas 12 táticas de execução, com o total de 86 técnicas distintas, o que mostra a grande complexidade de atuação deste grupo e a capacidade de se adaptar a diversos cenários.

Nem todas as técnicas possuem como forma de mitigação a utilização de IDS e, por isso, elas não foram incluídas no segundo capítulo. Nas subseções a seguir, será apresentada a consolidação do IDS como forma de mitigação de cada técnica.

4.1. Comprometimento por visita

Como explicado na Subseção 2.3.1., uma forma de conseguir acesso a um sistema é através da navegação do usuário em um site ou navegador comprometido.

Segundo Sakowicz e Agrawal (2018), a melhor forma de detectar essa intrusão é através do monitoramento de outras atividades incomuns na rede que possam indicar ferramentas adicionais transferidas para o sistema.

A forma mais adequada de uso é através de IDS com inspeção SSL/TLS, para procurar por scripts maliciosos conhecidos (scripts de reconhecimento, heap spray e identificação de navegador), ofuscação comum de scripts e código de exploração (Sakowicz; Agrawal, 2018).

4.2. Transferência de ferramentas de ingresso

Conforme explorado na Subseção 2.3.2. o adversário pode querer transferir ferramentas ou outros dados do sistema interno ao sistema comprometido. Além disso, é também possível fazer a distribuição desses dados dentro do sistema comprometido.

Segundo Page e Wee (2017), sistemas de detecção e prevenção de intrusão na rede que usam assinaturas de rede para identificar o tráfego de malware específico do adversário ou transferência de dados incomuns sobre protocolos conhecidos como FTP podem ser usados para mitigar a atividade no nível da rede.

As assinaturas são frequentemente utilizadas para indicadores únicos dentro dos protocolos e podem ser baseadas na técnica específica de ofuscação usada por um determinado

adversário ou ferramenta, e provavelmente serão diferentes entre várias famílias e versões de *malware.* Os adversários provavelmente mudarão as assinaturas das ferramentas ao longo do tempo ou construirão os protocolos de tal forma a evitar a detecção por ferramentas defensivas comuns (Page; Wee, 2017).

4.3. Limites de tamanho de transferência de dados

Na Subseção 2.3.3. foi apresentada a possibilidade da exfiltração através de blocos de tamanho fixo para evitar o disparo de alertas de limite de transferência de dados de rede.

Uma forma eficaz de mitigar essa técnica de ataque é através da adoção de IDS que usam assinaturas de rede para identificar o tráfego de infraestrutura de comando e controle e *malwares* específicos do adversário (Mitre, 2017).

4.4. Network Denial of Service

Conforme descrito na Seção 2.2. e no Capítulo 1, o DoS é uma forma de ataque poderosa e que pode causar prejuízos para todo o sistema de comunicação do meio.

Cada uma das três técnicas apresentadas nas seções anteriores contribui para que o atacante execute, com sucesso, um ataque DoS ou DDoS, por exemplo:

- Ao efetuar o comprometimento por visita, é possível manipular um site de forma a conter um *exploit* que instala um *malware* no computador do visitante, podendo transformá-lo em um zumbi ou *bot*. Esses zumbis ou *bots* podem ser utilizados para realizar ataques DoS nos próprios servidores ou outros dispositivos internos;
- Já ao utilizar a técnica de ferramentas de ingresso, o atacante pode manter persistência, escalar privilégios, executar comandos ou movimentar-se lateralmente pela rede. Além disso, essa técnica pode ser usada para enviar pacotes excessivos e que sobrecarregam os recursos do alvo; e
- Quando o adversário utiliza o limite de tamanho de transferência de dados, ele pode manipular os dados para atingir o limite e causar atrasos no serviço legítimo.

4.5. IDS como solução na defesa de ataques DoS

Conforme discutido na Seção 2.4., o IDS é um sistema fundamental na detecção de intrusão/anomalias na rede. Ele se diferencia de um firewall por ser um sistema mais complexo e robusto, o que não impede que os dois possam trabalhar em conjunto.

Quando se trata de ataques DoS, não podemos nos limitar a apenas um tipo de IDS, seja ele SIDS ou AIDS. É preciso utilizar os dois sistemas em conjunto, de forma a garantir as vantagens únicas que cada um possui, conforme apresentado na Tabela 1.

Considerando que o invasor já tenha conseguido acesso ao meio através das técnicas supramencionadas, o IDS ainda pode fornecer camadas extras de informação ao administrador do sistema, como monitoramento de tráfego e detecção de anomalias.

Além disso, o IDS pode fornecer uma defesa eficaz contra ataques DoS, ao identificar e bloquear o tráfego suspeito. No caso de um ataque DoS, o IDS pode detectar um aumento anormal no tráfego ou um grande número de solicitações de uma única fonte. Ao identificar esses padrões, o IDS pode alertar o administrador do sistema e tomar medidas para mitigar o ataque.

Vale ressaltar que é importante que o administrador do sistema tenha profundo conhecimento dos sistemas para saber distinguir o que são ataques legítimos ou falsos positivos, visto que o AIDS tem como característica o alto índice de falsos positivos em sistemas complexos de rede.

4.6. Aplicação prática na defesa contra o APT28

Nesta pesquisa, foi apresentado todo o arcabouço teórico das metodologias de funcionamento de cada técnica, mas é preciso consolidar as informações apresentadas em aplicações no mundo real.

Segundo Mitre (2017), o grupo APT28 utiliza, em seus meios de abordagem, o *malware X-Agent*, o *backdoor* Sednit e a ferramenta *Zebrocy*. Eis aqui dois cenários de aplicação comuns, considerando que o administrador local configure ambos SIDS e AIDS na infraestrutura, a fim de monitorar o tráfego de entrada e saída da rede:

4.6.1. Integrando SIDS e AIDS

O SIDS usa uma base de dados atualizada de assinaturas de ataques conhecidos ou suspeitos, incluindo os atribuídos ao grupo APT28.

O AIDS usa um algoritmo de aprendizado não supervisionado para construir um modelo do comportamento normal da rede. Esse comportamento se baseará em dados históricos e em tempo real. Os dados a serem considerados poderão ser variáveis como origem, destino, protocolo, porta, tamanho e frequência dos pacotes

Supondo que o APT28 utilize o *malware X-Agent*, o SIDS detectará um pacote de rede correspondente à sua assinatura, gerará um alerta e bloqueará o pacote, impedindo a comunicação entre o malware e o servidor de controle do atacante.

Logo em seguida, o AIDS detecta uma anomalia no comportamento da rede, observando um aumento repentino no número de conexões TCP para uma porta incomum em um host externo. Neste instante, o AIDS gera um alerta e investiga a origem das conexões, descobrindo que se trata de um computador da rede interna que está infectado pelo *backdoor Sednit*, usado para manter o acesso persistente ao sistema comprometido. O AIDS isola o computador infectado e notifica o administrador da rede.

Após verificar os alertas gerados pelo SIDS e pelo AIDS, o administrador poderá confirmar que se trata de uma tentativa de ataque do grupo APT28. De posse dessas informações, ele poderá realizar uma análise forense dos sistemas afetados e aplicará as medidas necessárias para restaurar a segurança da rede.

5. CONCLUSÃO

Este trabalho engloba a análise das técnicas de ataque utilizadas pelo grupo APT28, um dos mais sofisticados e persistentes grupos de hackers patrocinados por um Estado-nação. O objetivo foi identificar as formas de mitigação dessas técnicas através do uso de sistemas de detecção de intrusão (IDS). Para isso, foram revisados os conceitos básicos de um ataque DDoS, do modo de operação do grupo APT28 e do funcionamento geral do IDS.

No Capítulo 2, foram apresentadas as 12 táticas utilizadas por este grupo, de acordo com o *framework* MITRE ATT&CK. Em seguida, foram selecionadas as técnicas que possuem como forma de mitigação o uso de IDS e foram descritas as características e requisitos desses sistemas para cada caso. Foram abordadas quatro técnicas: comprometimento por visita, transferência de ferramentas de ingresso, limites de tamanho de transferência de dados e *Network Denial of Service*.

No Capítulo 4, foi feita uma análise crítica dos resultados obtidos e foram discutidas as limitações e desafios do uso de IDS para mitigar as técnicas do grupo APT28. Foi destacado que os IDS devem ser constantemente atualizados com assinaturas e regras que possam identificar os padrões de tráfego e comportamento dos *malwares* utilizados pelo grupo. Além disso, foi ressaltado que os IDS não são suficientes para garantir a segurança completa da rede, sendo necessário o uso de outras medidas complementares.

Ademais, foram descritos os sistemas de detecção de intrusão baseados em assinatura (SIDS), que são baseados em técnicas de reconhecimento de padrões para identificar um ataque previamente conhecido. Foram apresentadas as características, os requisitos, as vantagens e as desvantagens dos SIDS, sendo discutidos os principais desafios dos SIDS, como a necessidade de atualização constante das assinaturas, a incapacidade de detectar ataques desconhecidos ou variantes e a possibilidade de gerar falsos positivos ou negativos.

Em seguida, foram descritos os sistemas de detecção de intrusão baseados em anomalia (AIDS), que são baseados em técnicas de aprendizado de máquina, métodos estatísticos ou baseados em conhecimento para identificar um comportamento anormal do sistema. Foram apresentadas as características, os requisitos, as vantagens e as desvantagens dos AIDS e ainda discutidos os principais desafios dos AIDS, como a definição do que é normal ou anormal, a escolha do algoritmo adequado, a necessidade de treinamento e validação dos modelos e a possibilidade de gerar falsos positivos ou negativos.

Diante desses fatos, pode-se concluir que não há uma única técnica utilizada em IDS que seja superior a outra em todos os aspectos. Cada técnica tem suas próprias

características, vantagens e desvantagens. A escolha do tipo mais adequado depende do contexto, dos objetivos e dos recursos disponíveis para cada situação. Uma possível solução seria combinar tanto SIDS e AIDS em um sistema híbrido, que consiga aproveitar os pontos positivos e minimizar as limitações de cada um.

5.1. Considerações Finais

Ao passar dos dias, a guerra cibernética tem tomado proporções cada vez maiores. Os métodos de guerra convencional, antes baseados em munições de infantaria ou artilharia, já não são mais suficientes para manter a supremacia de uma nação.

Hoje podemos dizer que o inimigo é invisível. Ele é capaz de invadir o seu território e cumprir seu objetivo sem causar alarde ou deixar rastros.

Este trabalho explorou uma fração de um ecossistema incomensurável. Como visto anteriormente, um único grupo hacker conhecido possui 86 técnicas distintas de atuação, sendo que apenas 3 são claramente defendidas através de um IDS. Ao longo desta pesquisa, foram observados aproximadamente 136 grupos conhecidos. Agora imaginemos o universo de soluções que precisaríamos ter para defender nossos sistemas de todos esses grupos.

Isso mostra o quão imperativo é o aumento dos campos de estudo do mundo cibernético. É preciso ter em mente que problemas complexos requerem soluções complexas e que é impossível haver apenas um remédio que cure diversas doenças.

Além dos problemas apresentados, é preciso entender que o principal elo de fraqueza de um sistema é o ser humano. Outras técnicas estudadas, que não foram exploradas envolvem engenharia social, *phishing,* exploração de senhas fracas, entre outros.

5.2. Sugestões para futuros trabalhos

Como sugestão para trabalhos futuros, este autor sugere a abordagem dos seguintes tópicos:

a) Exploração de outras técnicas que não foram abordadas nesta pesquisa;
b) Apresentação de outras soluções, além do IDS, para mitigação dos ataques do grupo APT 28;
c) Realização de testes práticos para comprovar a eficácia na detecção e prevenção das técnicas do grupo APT 28;
d) Investigar técnicas de evasão e ofuscação utilizadas pelo grupo APT28 para burlar os IDS; e

e) Realizar uma análise comparativa entre o grupo APT28 e outros grupos hackers patrocinados por estados-nação.

REFERÊNCIAS

AKAMAI INC. **O que é um ataque de inundação ICMP?** Disponível em: <https://www.akamai.com/pt/glossary/what-is-icmp-flood-ddos-attack>. Acesso em: 27 set. 2023.

CENTER FOR INTERNET SECURITY. **Blog | The Mirai Botnet - Tips to Defend Your Organization**. Disponível em: <https://www.cisecurity.org/insights/blog/the-mirai-botnet-threats-and-mitigations>. Acesso em 22 set. 2023.

CLOUDFLARE INC. **Ataque DDoS de inundação ping (ICMP).** Disponível em: <https://www.cloudflare.com/pt-br/learning/ddos/ping-icmp-flood-ddos-attack>. Acesso em: 27 set. 2023.

CLOUDFLARE INC. **Ataque de inundação de protocolo UDP**. Disponível em: <https://www.cloudflare.com/pt-br/learning/ddos/udp-flood-ddos-attack/>. Acesso em: 25 set. 2023.

CLOUDFLARE INC. **O que é ataque de DDoS?** Disponível em: <https://www.cloudflare.com/pt-br/learning/ddos/what-is-a-ddos-attack/>. Acesso em: 22 set. 2023.

CLOUDFLARE INC. **SYN flood DDoS attack**. Disponível em: < https://www.mybib.com/pt/ferramentas/gerador-referencias-abnt >. Acesso em: 30 set. 2023.

CUNNINGHAM, **C. A Russian Federation Information Warfare Primer.** Disponível em: <https://jsis.washington.edu/news/a-russian-federation-information-warfare-primer/>. Acesso em 30 set. 2023.

DEMASKE, M; RED CANARY. **Deobfuscate/Decode Files or Information.** Disponível em: <https://attack.mitre.org/techniques/T1140/>. Acesso em 01 out. 2023.

EDDY, Wesley M. **Transmission Control Protocol Specification. RFC 9293.** Disponível em: <https://datatracker.ietf.org/doc/html/rfc9293>. Acesso em 27 set. 2023.

F5 NETWORKS INC. **O que é um ataque de inundação de SYN?** Disponível em: <https://www.f5.com/pt_br/glossary/syn-flood-attack>. Acesso em: 30 set. 2023.

FFCLAVIS. **Mirai Botnet - Visão geral de suas Ameaças e Mitigações**. Disponível em: <https://seginfo.com.br/2021/08/23/mirai-botnet-visao-geral-de-suas-ameacas-e-mitigacoes/>. GIL, Antônio Carlos. **Como elaborar projetos de pesquisa**. São Paulo: Atlas, 2007.

HEATON, R. **How does a TCP Reset Attack work?** Disponível em: <https://robertheaton.com/2020/04/27/how-does-a-tcp-reset-attack-work/>. Acesso em 27 set. 2023.

KAUARK, F. D. S.; MANHÃES, F. C.; MEDEIROS, C. H. **Metodologia da Pesquisa: Um guia prático.** Itabuna: Via Litterarum, 2010.

KHRAISAT, A. et al. **Survey of intrusion detection systems: techniques, datasets and challenges.** Cybersecurity, v. 2, n. 1, 17 jul. 2019.

MANRAL, V; WEIZMAN, Y. **Network Denial of Service**. Disponível em: < https://attack.mitre.org/techniques/T1498/>. Acesso em 01 out. 2023.

Mello, Fábio Pinhão Junior, Ricardo da Cruz Mendes e Rocha, Daniel Guimarães **ANÁLISE DE ATAQUES DDOS.** / Fábio Pinhão Mello, Ricardo da Cruz Mendes Junior e Daniel Guimarães Rocha - Rio de Janeiro: Instituto Militar de Engenharia, 2010.

MENACHEM, G; STERNSTEIN, J; WEE, M; NETSKOPE; PRAETORIAN; SOMASAMUDRAM, P; FAROOQH, S. U; WEIZMAN, Y. **Valid Accounts.** Disponível em: <https://attack.mitre.org/techniques/T1078/>. Acesso em 01 out. 2023.

MENEZES, **W. Decifrando a rede Mirai**. Disponível em: <https://blog.nec.com.br/decifrando-a-rede-mirai>. Acesso em: 25 set. 2023.

MITRE. **APT28, SNAKEMACKEREL, Swallowtail, Group 74, Sednit, Sofacy, Pawn Storm, Fancy Bear, STRONTIUM, Tsar Team, Threat Group-4127, TG-4127, Group G0007 | MITRE ATT&CK®.** Disponível em: < https://attack.mitre.org/groups/G0007/>. Acesso em: 01 out. 2023.

MITRE. **Archive Collected Data, Technique T1560 - Enterprise | MITRE ATT&CK®.** Disponível em: <https://attack.mitre.org/techniques/T1560/>. Acesso em 01 out. 2023.

MITRE. **Collection, Tactic TA0009 - Enterprise | MITRE ATT&CK®.** Disponível em: <https://attack.mitre.org/tactics/TA0009/>. Acesso em 01 out. 2023.

MITRE. **Command and Control, Tactic TA0011 - Enterprise | MITRE ATT&CK®.** Disponível em: <https://attack.mitre.org/tactics/TA0011/>.

MITRE. **Data Transfer Size Limits, Technique T1030 - Enterprise | MITRE ATT&CK®.** Disponível em: <https://attack.mitre.org/techniques/T1030/>. Acesso em 01 out. 2023.

MITRE. **Exfiltration, Tactic TA0010 - Enterprise | MITRE ATT&CK®.** Disponível em: <https://attack.mitre.org/tactics/TA0010/>. Acesso em 01 out. 2023.

MITRE. **Impact, Tactic TA0040 - Enterprise | MITRE ATT&CK®.** Disponível em: <https://attack.mitre.org/tactics/TA0040/>. Acesso em 01 out. 2023.

NETSCOUT. **What is an ICMP Flood Attack?** Disponível em: <https://www.netscout.com/what-is-ddos/icmp-flood>. Acesso em 27 set. 2023.

OWASP. **Intrusion Detection | OWASP**. Disponível em: <https://owasp.org/www-community/controls/Intrusion_Detection>. Acesso em 10 out. 2023.

PAGE, J; WEE, M. **Ingress Tool Transfer.** Disponível em: < https://attack.mitre.org/techniques/T1105/>. Acesso em 01 out. 2023.

RUEL, S; CHURCH, D; RATLIFF, E; GOLD, R. **APT28.** Disponível em: <https://attack.mitre.org/groups/G0007/>. Acesso em 01 out. 2023.

SAKOWICZ, J; AGRAWAL, S. **Drive-by Compromise.** Disponível em: <https://attack.mitre.org/techniques/T1189/>. Acesso em 01 out. 2023.

SANTOS, F. G.; GOMES, R. **Sequestro de Conexões TCP - Uma Abordagem Contemporânea**. Cadernos de Informática, v. 6, n. 1, p. 141–146, 1 jan. 2011.

SILVA, E. L.; MENEZES, E. M. **Metodologia da pesquisa e elaboração de dissertação**. 4. ed. rev. atual. Florianópolis: UFSC, 2005.

STROM, Blake E. et al. **MITRE ATT&CK®: Design and Philosophy.** MITRE ATT&CK®: Design and Philosophy, McLean, VA, ano 2020, mar. 2020.

TZU, S.; PIETRO NASSETTI. **A arte da guerra**. São Paulo: Martin Claret, 2007.
UPX TECNOLOGIA LTDA. **O que é SYN Flood?** Disponível em: <https://upx.com/post/syn-flood/>. Acesso em 30 set. 2023.

WALLARM INC. **What is TCP Reset Attack? How to mitigate the effects?** Disponível em: <https://www.wallarm.com/what/what-is-syn-spoofing-or-tcp-reset-attack>. Acesso em 27 set. 2023.

WESTCON-COMSTOR, E. S. **Saiba como funcionam os 5 principais tipos de ataques DDoS e como evitá-los.** Disponível em: <https://blog-pt.lac.tdsynnex.com/saiba-como-funcionam-os-5-principais-tipos-de-ataques-ddos-e-como-evita-los>. Acesso em: 22 set. 2023.