COZY BEAR : UMA PRESENÇA NADA ACONCHEGANTE NO CIBERESPAÇO

Amós Kinsley Barbosa de Santana
Bruna Braz da Silva
Mel Zion Cordeiro
Renan Santana Costa
Vladson Henrique Ribeiro Marinho

akbs@cin.ufpe.br
ssilvabbruna1@gmail.com
mzc@cin.ufpe.br
rsc8@cin.ufpe.br
vhrm@cin.ufpe.br

Resumo

APT29, *Cozy Bear*, *Nobelium*, *Midnight Blizzard*, UNC2452. Vinculado ao Serviço de Inteligência Estrangeira da Rússia (SVR) e furtivo até nas múltiplas formas como é conhecido, este é um dos mais sofisticados grupos de espionagem cibernética já vistos pela humanidade. Sua aplicação cirúrgica de *weaponization*, comprometimento à cadeia de suprimentos, *spear phishing*, escalação de privilégios, entre inúmeras outras táticas, técnicas e procedimentos (TTPs), incluindo ferramentas intrínsecas aos sistemas operacionais atacados, já foi capaz de tornar esse grupo um agente de perturbação em eventos de repercussão global, tais como a pandemia da COVID-19, eleições estadunidenses e até mesmo um ataque a uma das maiores fornecedoras de software de monitoramento de redes do mundo. Isso posto, o presente trabalho destina-se a explorar o que torna esse ator um alvo inegociável da cibersegurança, mostrando que sua eficiência está vinculada não só a uma profundidade computacional, mas também psicológica e metodológica. Com isso, objetiva-se compor um material útil para futuros profissionais da segurança digital, bem como contribuir para o conhecimento geral acerca da atuação de agentes maliciosos no mundo virtual, em particular os de ameaça persistente avançada (APT).

Palavras-chave: APT29. Perfil de ataque. Eventos notórios.

1. Introdução

O APT29, amplamente conhecido como *Cozy Bear*, é um grupo de ameaça persistente avançada (APT) associado, de acordo com múltiplas fontes de inteligência ocidentais, ao Serviço de Inteligência Estrangeiro da Federação Russa (SVR). Sua origem remonta ao final dos anos 2000, período no qual a Rússia consolidava estratégias de guerra híbrida e ciberespionagem como instrumentos de projeção de poder. Atribui-se ao APT29 um papel central na execução da política de Estado russo voltada para a obtenção de inteligência estratégica em escala global.

Ao longo dos anos, o APT29 demonstrou notável sofisticação técnica, persistência operacional e capacidade de adaptação, evoluindo de campanhas de *spear phishing* direcionado para complexos ataques à cadeia de suprimentos. Essa evolução técnica reflete investimentos estatais substanciais em capacidades cibernéticas ofensivas, sugerindo uma agenda alinhada diretamente aos interesses geopolíticos russos, incluindo a defesa de sua

influência internacional, a proteção de interesses econômicos estratégicos e o fortalecimento de sua posição em negociações diplomáticas.

A motivação principal do APT29 não é o lucro direto ou a extorsão financeira, mas a coleta sistemática de inteligência estratégica. Suas operações visam apoiar decisões políticas e diplomáticas do governo russo, obter vantagem econômica em setores sensíveis e enfraquecer a confiança de adversários em suas próprias infraestruturas e processos democráticos. O grupo opera com foco claro em espionagem cibernética, buscando acesso prolongado e discreto a informações sensíveis de alto valor. Sua meta é possibilitar ao Estado russo a obtenção de conhecimento privilegiado sobre políticas externas, estratégias de segurança nacional, avanços científicos e tecnológicos críticos, bem como processos políticos internos de nações-alvo.

No contexto histórico dos ataques atribuídos ao APT29, observa-se uma clara correspondência entre os alvos escolhidos e momentos de tensão geopolítica ou transformações estratégicas globais. Em 2014, durante o agravamento das relações entre Rússia e Ocidente após a anexação da Crimeia, o grupo realizou ataques sofisticados contra sistemas de e-mail de agências governamentais dos EUA, buscando informações sensíveis de política externa e segurança.

Em 2016, no auge da disputa eleitoral norte-americana, o APT29 participou da violação dos servidores do Comitê Nacional Democrata, em uma campanha que teve impacto direto na confiança pública e no discurso político. Em 2020, durante a pandemia de COVID-19, o grupo adaptou rapidamente suas operações para visar centros de pesquisa e farmacêuticas envolvidas no desenvolvimento de vacinas, refletindo a urgência do Estado russo em garantir vantagem científica e logística em meio à crise sanitária.

A violação da SolarWinds, também em 2020, marcou um ápice técnico e estratégico, explorando a cadeia de suprimentos para acessar dezenas de agências federais e empresas globais em um contexto de competição acirrada por influência geopolítica e domínio tecnológico. Esses ataques não ocorrem isoladamente, mas inserem-se em um padrão mais amplo de uso da ciberespionagem como ferramenta de Estado para sustentar ambições políticas, militares e econômicas em um cenário internacional cada vez mais contestado.

Historicamente, os alvos do APT29 incluem:

a) **Entidades governamentais e diplomáticas**: com o objetivo de acessar comunicações confidenciais, estratégias de segurança nacional e posicionamentos diplomáticos sensíveis.

b) **Infraestrutura crítica**: para mapear vulnerabilidades estratégicas e influenciar políticas de defesa.

c) **Instituições políticas**: visando obter e potencialmente explorar informações que possam interferir em processos democráticos.

d) **Empresas de alta tecnologia e saúde**: especialmente nos setores farmacêutico e de desenvolvimento de vacinas, como forma de promover avanços nacionais ou obter vantagem competitiva em contextos globais críticos.

2. Ataques Notáveis

1) Ataque a Sistemas de E-mail do Governo dos Estados Unidos

O grupo de hackers Cozy Bear conduziu um ataque direcionado com o objetivo de infiltrar-se em ambientes seguros e canais de comunicação privados de agências governamentais dos Estados Unidos, incluindo a Casa Branca. A operação teve início por meio de engenharia social e da técnica de *spear phishing*, com o envio de e-mails convincentes contendo links capazes de executar scripts maliciosos.

Após comprometer os sistemas de e-mail, os atacantes mantiveram presença prolongada nos ambientes invadidos, executando malwares de forma seletiva e implantando *backdoors* para assegurar sua permanência. Uma característica marcante da ação foi o movimento lento e discreto do grupo dentro dos sistemas, o que permitiu que a invasão persistisse por meses. Esses ataques consecutivos resultaram no comprometimento da comunicação entre membros do governo norte-americano e na possível exposição de dados confidenciais.

2) Invasão ao Comitê Nacional Democrata (DNC)

A invasão à rede do Comitê Nacional Democrata (DNC) envolveu a atuação conjunta dos grupos de hackers Fancy Bear e Cozy Bear. Enquanto o Fancy Bear foi responsável pelo vazamento de comunicações sensíveis que impactaram diretamente o cenário político dos Estados Unidos, o Cozy Bear manteve uma postura mais silenciosa durante a operação, concentrando-se no mapeamento da rede e na extração cautelosa de dados. Essa divisão de tarefas é característica de operações APT, com grupos atuando de formas diferentes para atingir certos objetivos. Esse ataque evidencia o forte caráter político das operações cibernéticas conduzidas por ambos os grupos, cujas ações têm o potencial de influenciar diretamente processos democráticos e decisões governamentais.

3) Ataques a pesquisas da COVID-19

Durante a pandemia, o APT29 realizou uma série de ataques a instituições de pesquisa envolvidas no desenvolvimento da vacina da COVID-19 nos EUA, Reino Unido e Canadá. O objetivo do grupo era o roubo de informações sobre possíveis fórmulas para o desenvolvimento da vacina, com o provável objetivo de favorecer o desenvolvimento da vacina em laboratórios russos. Para a realização desses ataques o grupo usou *spear phishing*, além de explorarem vulnerabilidades associadas ao acesso remoto emergencial adotado por muitas instituições de pesquisa.

4) Ataque à cadeia de suprimentos da SolarWinds

O ataque teve como vetor inicial a empresa americana SolarWinds, que desenvolve softwares para outras empresas com o objetivo de ajudar no gerenciamento de suas redes. A invasão afetou diversas organizações (incluindo agências federais dos EUA) que utilizavam o software Orion da SolarWinds.

O grupo APT29 primeiramente se infiltrou na rede da SolarWinds inserindo o malware SUNBURST em uma das atualizações do software, garantindo que o malware seria disseminado digitalmente por meio do *update* do software legítimo da SolarWinds. Com o SUNBURST disseminado, os atacantes passaram a ter múltiplos pontos de acesso nas redes comprometidas.

Após a infiltração, para garantir a persistência da invasão nas redes, o grupo utilizou técnicas e ferramentas como Cobalt Strike e TEARDROP para movimento lateral e evasão de detecção, além de usarem tokens SAML para evitar autenticações de multifator.

Esse ataque à rede da SolarWinds teve repercussão global e mostrou como investidas cibernéticas podem se estender por meio de relações entre organizações. Ademais, o evento é mais uma demonstração do elevado nível de **segurança operacional** do grupo, visto, por exemplo, no comprometimento de múltiplas contas, destinando algumas para reconhecimento cibernético e outras, para movimentação lateral, permitindo que se, porventura, uma fosse detectada pelos agentes de segurança, diminuíssem-se as chances de isso expor a real abrangência do ataque.

O ataque poderia ter causado um impacto ainda maior caso o seu objetivo fosse diferente. A invasão ao sistema da SolarWinds usou das suas vulnerabilidades para comprometer um grande número de sistemas e obter informações sensíveis, assim, pode-se pensar que, caso o grupo tivesse como objetivo a interrupção das redes, o impacto teria sido catastrófico para as empresas vítimas da ação.

3. Técnicas Utilizadas

3.1 Acesso Inicial

"Acesso inicial" diz respeito ao conjunto de técnicas utilizadas por agentes maliciosos para estabelecer, pela primeira vez, uma presença em um ambiente alvo. Essas estratégias viabilizam o ponto de entrada que irá possibilitar a execução de fases seguintes à intrusão, como reconhecimento, movimentação lateral, exfiltração e persistência.

No caso de grupos como o APT-29 (Cozy Bear), esse estágio é conduzido com um alto grau de sofisticação técnica e inteligência contextual, evidenciado pela seleção cuidadosa de vetores de ataque, desde o comprometimento de cadeias de suprimento (*supply chain compromise*), até campanhas de *spear phishing* com documentos maliciosos ou manipulação de APIs em ambientes em nuvem. Essas práticas são projetadas não apenas para obter o acesso, mas também para fazer de maneira furtiva, resiliente e, idealmente, indetectável.

É nesse ponto que a operação ofensiva de um APT revela sua maior parte estratégica: o acesso inicial não é somente abrir uma porta de entrada, mas sim a construção de um canal que permita continuidade e controle, utilizando-se de engenharia social, abuso de ferramentas nativas *(living off the land*), arquivos maliciosos e credenciais comprometidas.

A seguir, serão detalhadas algumas das principais TTPs (Táticas, Técnicas e Procedimentos) utilizadas pelo APT-29 para obtenção desse acesso inicial.

1) *Supply Chain Compromise* (MITRE T1195.002)

Característica notória do APT29, o **comprometimento de cadeia de suprimento** é uma das técnicas de acesso inicial utilizado pelo grupo. Essa técnica consiste em inserir código malicioso em *scripts* de *build*, nos binários ou bibliotecas de softwares terceiros que dão suporte à aplicação do alvo.

O Cozy Bear conseguiu utilizar essa técnica ao inserir um *backdoor* em uma *DLL* (*Dynamic Library Link)* adicionada pelo software Orion da SolarWinds, *SolarWinds.Orion.Core.BusinessLayer.dll*, um sistema de monitoramento de infra-estrutura. Esse código malicioso era adicionado no processo de *build* do binário da *DLL* e, com isso, era assinado e entregue oficialmente pela SolarWinds. Essa brecha aberta pelo *backdoor* permitia, posteriormente, a conexão com os alvos por via de softwares de C2 e eram utilizados tunelamento *DNS* para mascarar os acessos maliciosos para o *firewall* de rede. Além disso, o código malicioso era executado no método *RefreshInternal* onde sua execução era carregada após 12 a 14 dias depois da instalação, ajudando a evitar detecção.

Essa técnica de tunelamento *DNS* é usada para encapsular código em chamadas de *DNS*, como forma de burlar bloqueios de *firewall* impedindo de abrir conexões *HTTP*. Esse tunelamento funciona com comandos do tipo "*dns query:seclicar.eutehacke.io"* onde será buscado dados em uma aplicação previamente feita pelo atacante de forma a enviar os comandos que ele deseja executar na máquina alvo. Essa técnica funciona contando que chamadas de *DNS* normalmente não são bloqueadas, por serem essenciais para o funcionamento do sistema conectado à internet.

Esse tipo de ataque pode ser evitado ao estabelecer uma metodologia de *deploy* mais segura, ao efetuá-lo primeiro em ambientes de teste e ao analisar o funcionamento dessas dependências mais a fundo, verificando se há alguma alteração nas execuções do sistema no uso da *DLL*. O empecilho disso, todavia, é que é necessário ter um domínio maior sobre como funcionam as ferramentas terceiras.

2) *Phishing* (MITRE T1566)

Phishing é uma técnica amplamente utilizada como vetor de ataque inicial por diversos grupos, justamente por utilizar engenharia social para viabilizar a intrusão. Nesse viés, consiste em fazer comunicações enganosas, passando-se por alguma autoridade, para que isso induza a vítima a fazer alguma ação que leve à execução de códigos maliciosos. Essas comunicações podem ser desde e-mails à sites e plataformas falsas, que mimetizem outras, legítimas. O acesso inicial pode ser promovido por arquivos infectados que explorem falhas em leitores de arquivos ou por sites que capturam credenciais de acessos, que podem ser utilizadas pelo grupo para acessar plataformas oficiais. O APT29 se utilizou bastante dessa forma de acesso, especialmente em 2020, com a migração acelerada para o trabalho remoto, de forma que muitas medidas de segurança e muitas comunicações oficiais eram feitas de forma flexível devido à pressão para ser feita celeremente.

Tais campanhas de *phishing* se davam com e-mails personalizados (conhecidos como "*spear phishing"*, por terem alvos específicos e e-mails feitos de forma dedicada à esse usuário) para cada alvo que continham documentos anexos com códigos de *backdoor* que eram executados pelos leitores de arquivos ".docx" e ".pdf". Além disso, se utilizavam de sites falsos que capturavam credenciais de OAuth, ao imitar sistemas de login de sites legítimos.

Esses *backdoors* eram normalmente uma das aplicações autorais da Cozy Bear, como parte das medidas para mitigar estratégias de defesa. Algumas dessas aplicações são: GOLDMAX (MITRE S0588), WELLMAIL (MITRE S0515), WELLMESS (MITRE S0514), COMMODONK (sem código) e HAMMERTOSS (MITRE S0037).

Como forma de prevenção para esse tipo de ataque, o esforço está em treinar e fazer campanhas de testes com os funcionários para que esses tipos de comunicação fraudulenta sejam identificadas, mas não acessadas. Fora isso, existem configurações para os serviços de email para que sejam autenticados os emails, dando garantia de que o destinatário do email é real e realizar download e execução desses arquivos anexos em ambiente de testes, sem comprometer o sistema principal do usuário. Credenciais devem ter validades bem reguladas, acesso multifatores e políticas de *zero trust* sejam configuradas.

3) PowerShell (MITRE T1059.001)

Essa ferramenta é uma linguagem de *scripts* do Windows, similar ao *bash* do Linux. Muito utilizada para fazer execução remota de código, coletar dados, apagar registros de *log*, mascarar a presença de software malicioso e assegurar persistência de conexão. Essa

linguagem pode ser usada para download e execução de código em memória, como pode ser feito executando *(New-Object Net.WebClient).DownloadString("urlmalvadona")*, não deixando registro em discos rígidos de arquivos maliciosos e dificultando a detecção desses códigos.

Além disso, são utilizadas para enganar *scanners antimalware*, como manipulando a *DLL* do *AMSI (Antimalware Scan Interface),* que é responsável por criar uma interface de comunicação entre aplicações e sistemas *Anti Malware* instalados, para definir manualmente um indicador de que o *AMSI* falhou ao inicializar, fazendo o *bypass* da avaliação do código.

Sendo utilizado pelo APT29 como forma de fazer download e execução de códigos maliciosos hospedados em servidores ou em serviços de hospedagem de código. Além disso, é bastante utilizado como forma de aplicar técnicas de desabilitar *logs* ou até excluir *logs* de execução maliciosa.

Esse tipo de utilização maliciosa da ferramenta pode ser bloqueado com estratégias e configurações de bloqueio de edição de manipulação de logs ou a hospedagem de *logs* em outros ambientes, de forma que eles não possam ser excluídos pelo usuário. Restrição de execução de códigos e estratégias de permissões também podem ser empregadas para evitar que sejam executados *scripts* maliciosos. Além disso pode ser definido um bloqueio para a execução do código com a flag *-EncodedCommand* onde o código será recebido com uma ofuscação do tipo Base64.

4) Windows Command Shell (MITRE T1059.003)

O Windows Command Shell é uma ferramenta amplamente conhecida para executar códigos nativos do Windows, análogo ao Terminal do Linux. Essa ferramenta é utilizada amplamente para executar tarefas ou executar ferramentas. É a forma que os ambientes de C2 (Comando e Controle) normalmente utilizam para executar os códigos.

O APT29 tem como uso, para essa ferramenta, atividades como a criação de novos usuários com privilégios administrativos para que sejam utilizados para executar códigos maliciosos, executar scripts de automação e coleta de dados e disfarçar comandos maliciosos, técnica essa conhecida como *living off the land*, que é a utilização de recursos do sistema para fazer a execução de código, mascarando tarefas com códigos maliciosos como tarefas legítimas do sistema.

Como forma de defesa para a utilização dessa ferramenta de forma ilegítima, ferramentas como AppLocker, limitando a execução de arquivos .bat, auxiliam no controle de execução de diversos códigos maliciosos, além de sistemas de EDR (*Endpoint Detection and Response*) que ajudam a monitorar a execução de códigos em sistemas computadorizados.

5) Cloud API (MITRE T1059.009)

Cloud API são interfaces de comunicação entre serviços em nuvem para que sejam controlados recursos da infraestrutura de uma aplicação. Esse tipo de ferramenta é utilizado, de forma maliciosa, para que sejam exfiltrados dados. Essa comunicação é feita, normalmente, utilizando serviços REST com tokens de autenticação (que muitas vezes são roubados com o uso das técnicas de *phishing*). Essa comunicação permite fazer consultas nos sistemas, de forma a permitir identificar a infra-estrutura do alvo, acessar dados de listas de emails, usuários e permissões.

O APT29 viabiliza o uso dessa ferramenta com o uso de técnicas de phishing ou até mesmo com contas já comprometidas das ferramentas de infraestrutura em rede. Com isso, pode fazer um reconhecimento silencioso, muitas vezes indetectável, do alvo.

Para evitar esse tipo de utilização maliciosa, o gerenciamento das permissões deve ser feito de forma muito planejada, evitando que usuários tenham permissões demais. Além disso, é necessário configurar formas de múltiplos fatores de autenticação e o tempo de validade das chaves de acesso.

6) Malicious File (MITRE T1204.002)

A utilização de arquivos para fins maliciosos se dá em adição de códigos em arquivos legítimos ou na criação de arquivos que apenas executam códigos maliciosos. Esses arquivos, por sua vez, dependem da interação do usuário em os executar, sendo necessário técnicas de engenharia social para que isso seja feito. Esse conteúdo dos códigos são normalmente feitos para que sejam criadas backdoors ou shell reversas.

A adoção dessa técnica é utilizada amplamente por diversos grupos e o APT29 não foge a regra, é utilizada como forma de executar scripts do PowerShell para baixar ferramentas ou implantar um de seus diversos *malwares*.

As defesas para esse tipo de infecção é dada pelo bloqueio de execução de determinados tipos de arquivos, a execução de arquivos suspeitos em ambientes de sandbox ou de testes, monitoramento das tarefas executadas pelos arquivos e seus logs gerados e o treinamento de usuários para que esses arquivos provenientes de técnicas de phishing não sejam executados.

3.2 Persistência e Escalação de Privilégio

"Persistência" é o termo que alude às TTPs que proporcionam a um agente malicioso permanecer controlando o(s) dispositivo(s), não obstante os esforços para mitigá-lo, quer por reinicialização, por troca de credenciais ou qualquer outra medida de defesa. Nesse sentido, fica evidente a importância de tais estratégias para grupos de ameaça persistente avançada, como o Cozy Bear, pois, com elas, as invasões, outrora eventos pontuais, transformam-se em moradores de longo prazo nos sistemas-alvo.

Já "escalação de privilégio" refere-se ao ganho de direitos e acessos administrativos por parte do agente malicioso através da manipulação de vulnerabilidades de segurança do sistema. Isso permite que o dano do ataque se aprofunde, alcançando, por exemplo, informações confidenciais do usuário.

Sob essa ótica, nota-se que essas duas estratégias caminham juntas, pois, muitas vezes, medidas de persistência têm como consequência escalação de privilégios e vice-versa. Não à toa, o glossário da MITRE Corporation (diretriz "MITRE ATT&CK") apresenta interesecções ao falar dessas ações, com técnicas que são classificadas como pertencentes a ambas, como T1574.009 (mudança de atalhos).

Esmiucemos, então, algumas das TTPs concernentes à persistência e/ou à escalação de privilégios.

1) Manipulação de contas (MITRE T1098)

Segundo o glossário da MITRE Corporation, "manipulação de contas" diz respeito a "toda ação que mantém ou preserva o acesso do adversário à conta comprometida, tais como modificação de credenciais ou de grupos de permissões".

Também citado pelo glossário, um exemplo mais detalhado de ação dentro dessa definição é, uma vez comprometida a conta, realizar atualizações constantes da senha,

burlando os sistemas de expiração das credenciais. Essas ações muitas vezes são acompanhadas de controle do email vinculado, excluindo notificações de alteração de senha e alterando configurações de segurança. Dessa forma, caso o usuário desconecte-se da sua conta e tente entrar novamente, a senha legitimamente definida não mais funcionará. Caso tente solicitar troca de senha, os emails podem ser igualmente interceptados pelo hacker.

É importante salientar que essas ações ocorrem após a invasão, isto é, elas não viabilizam o primeiro acesso, mas a longevidade do efeito deste. Logo, a aplicação desses métodos requer uma certa amplitude de permissões, as quais podem ser escaladas por meio da própria manipulação de contas.

1.1) Credenciais de nuvem adicionais (MITRE T1098.001)

Trata-se, na verdade, de uma subtécnica de manipulação de contas. Nesse caso, porém, atinge especificamente as contas de nuvens, ou seja, dos ambientes de armazenamento online, não em disco rígido.

Na explicação geral acerca da técnica T1098, citou-se a possibilidade de mudar diversas vezes uma senha, concedendo ao invasor o verdadeiro controle sobre a conta da vítima. Tal ação, porém, pode ser identificada com certa facilidade por um usuário atento à renovação de suas palavras-passe ou que, simplesmente, execute logout e depois seja impedido de fazer login. Nesse caso, uma possível estratégia de persistência do atacante é criar suas próprias credenciais na conta da nuvem do alvo. Algumas ferramentas que podem ser alvo dessa abordagem são os chamados *service principals*, "identidades criadas para uso de aplicações, serviços hospedados e ferramentas automáticas", de acordo com definição da Microsoft, sendo uma ferramenta de segurança da Azure, plataforma de computação em nuvem dessa empresa. Nesse viés, os invasores aproveitam-se de credenciais legítimas - como os certificados X.509 -, para adicionar as suas próprias, obtendo, então, mais permissões.

Em ambientes que adotam o modelo de Infraestrutura como Serviço (sigla em inglês: *IaaS*: *Infrastructure as a Service*), adversários também conseguem gerar suas próprias chaves do tipo *SSH* (do inglês, *security shell*, credencial usada para o acesso seguro de servidores remotos), usando comandos como "CreateKeyPair" ou "ImportKeyPair", quando se trabalha com os serviços de nuvem da Amazon (conhecidos pela sigla AWS: Amazon Web Services), ou o comando "gcloud compute os-login ssh-keys add", ao se usar a Google Cloud Platform (GCP). Também é possível manipular interfaces de programação de aplicações (API) para fins semelhantes. Um exemplo disso é a API "CreatLoginProfile", do AWS, por meio da qual é possível adicionar uma senha que permita o acesso ao painel de controle da nuvem (*Management Console for Cloud Service Dashboard*). Caso o perfil que o hacker esteja atualmente usando para requisitar os acessos tenha menos permissões do que a conta-alvo (que, geralmente, é um *service principal*), ao criar essa nova senha, a conta menos privilegiada escalona.

Além disso, outro método relevante de adição de credenciais em nuvens é o escape à autenticação multifator (*MFA*): isso ocorre porque, em programas mais antigos, esse recurso não é suportado e, como alternativa, estabelece-se uma senha de aplicativo. Isso, porém, pode constituir-se em uma brecha, visto que é possível, em algumas situações, hackers criarem uma senha desse tipo para uma aplicação que naturalmente requereria MFA e, por existir essa senha de aplicativo, a autenticação não ser solicitada.

A presente descrição, embora resumida, mostra que MITRE T1098.001 é uma subtécnica ampla, e as vulnerabilidades dos sistemas de computação em nuvem que ela explora precisam ser objeto de particular atenção por parte dos agentes de segurança do ciberespaço, em particular no enfrentamento de cibercriminosos de alto nível, como o APT29.

2) Modificação de atalhos (MITRE T1547.009)

Como o nome sugere, essa subtécnica consiste na modificação de atalhos (isto é, links, arquivos ou de combinações de teclas que apontam para um arquivo específico do computador ou que executam uma determinada ação de forma facilitada) para atender a interesses do ataque, como a implantação de um *malware*. Embora a infecção da máquina seja, de fato, um dos usos mais comuns da MITRE T1547.009, ela também é muito útil para estabelecer persistência, sendo uma tática característica de grupos como o APT29.

3) Falsificação ou roubo de tokens (MITRE T1134.001)

Dispositivos eletrônicos geradores de senha (tokens) podem, por meio de comandos como "DuplicateToken" ou "DuplicateTokenEx", ser duplicados e, então, pelo comando "ImpersonateLoggedOnUser", incorporar os privilégios do token violado. Além disso, o comando "SetThreadToken" conecta tokens (adulterados ou não) a uma sequência de instruções, chamadas "threads", executando-as conforme as especificações de segurança do token. É possível, também, em vez de uni-lo a um processo já existente, criar um novo, pelo comando "CreatProcessWithTokenW" ou "CreatProcessAsUserW" (sendo "W" um nome genérico). Ademais, outros processos realmente se apropriam de tokens já existentes, enquanto outros realmente criam um novo, em vez de duplicar algum. Nota-se, então, a forma por que TTPs desse tipo permitem ao invasor disseminar sua presença e poderio sobre o alvo.

4) Modificação na relação de confiança (*trusts*) de domínio (MITRE T1484.002)

Segundo definição do site BrasilCloud, "domínio" é um nome que serve para "localizar e identificar conjuntos e redes de computadores na Internet", ou seja, é o que popularmente se chama de "nome do site". Já a expressão "relações de confiança de domínio" ou "trusts de domínio" se refere aos processos que permitem que um domínio possa trocar recursos com outro. Dito isso, uma TTP que viabiliza tanto persistência, quanto escalação de privilégio é a modificação das regras que regulam o "relacionamento" entre os domínios.

Alguns exemplos de modificações que podem ser feitas nessas relações de confiança é alterar os usuários que são considerados "federados", ou seja, que podem acessar diversos recursos do domínio com o mesmo conjunto de credenciais, ou promover mudanças nas permissões dos *tenants* (do inglês, "inquilinos"), nome dado a um grupo de usuários de uma mesma organização que compartilham acesso e privilégios específicos em uma determinada instância (cópia do programa em execução no momento) do software.

Relações de confiança estão relacionadas ao funcionamento de senhas, credenciais e diversos outros materiais de autenticação, os quais são utilizados em diversas partes de um sistema computacional, particularmente nos em nuvem. Por isso, manipular ilicitamente *trusts* é uma forma astuta de obter privilégios indevidos e de se esquivar de políticas de segurança.

3.3 Evasão de Defesa

A evasão de defesas refere-se ao conjunto de TTPs empregados para evitar a detecção por mecanismos de segurança, tais como antivírus, *endpoint detection and response* (*EDRs*), *firewalls*, entre outros. O objetivo dessas ações é permanecer invisível no sistema durante todo o período da intrusão. Esse tipo de técnica é essencial em operações conduzidas por grupos APT, como o APT29 (Cozy Bear), uma vez que essas operações visam a permanência prolongada e silenciosa nos sistemas-alvo. Algumas dessas técnicas também se relacionam a

outras categorias do *framework* MITRE ATT&CK, como execução, persistência e exfiltração, demonstrando o caráter versátil das técnicas de evasão na arquitetura de um ataque. Diante disso, analisamos a seguir algumas das principais TTPs utilizadas pelo grupo Cozy Bear para evadir sistemas de defesa, como a esteganografia, a injeção de processos, a deleção segura de arquivos e o sequestro da ordem de pesquisa.

1) Esteganografia (MITRE T1027.003)

A esteganografia é a técnica de esconder dados (maliciosos ou não) dentro de arquivos aparentemente inofensivos, como imagens, áudios, ou vídeos. Diferentemente da criptografia que transforma os dados com o uso de um algoritmo para que não possam ser decifrados, a esteganografia esconde os dados, transformando a tarefa de detecção consideravelmente mais complexa. Posteriormente, os dados escondidos podem ser extraídos e usados por meio da execução de um script no sistema da vítima.

O grupo de hackers realizava ataques com essa técnica usando como vetor imagens que escondiam *payloads* maliciosos capazes de executar um *malware* no sistema alvo. Esse tipo de ataque pode ser evitado por meio do uso de *anti-malwares* capazes de analisar a presença de padrões e *payloads* ocultos em arquivos de mídia.

2) Injeção de Processos (MITRE T1055.002)

Chamada em inglês de *Portable Executable Injection*, essa técnica consiste em injetar um executável malicioso na memória de um processo legítimo, dessa forma o executável com carga maliciosa usará o processo para burlar sistemas de antivírus, o executável não é exposto como um novo processo no sistema, permanecendo discreto na lista de processos do sistema.

A escrita de códigos maliciosos em processos ocorre por meio de chamadas de APIs nativas do Windows, como:

a) VirtualAllocEx: alocação de memória;
b) WriteProcessMemory: escrita na memória;
c) CreateRemoteThread: criação de uma thread remota para execução do payload.

Uma grande dificuldade encontrada nesse tipo de ataque é que o código malicioso precisa ser posicionado corretamente no endereço do processo alvo, visto que o endereço do processo é calculado de forma pseudo randômica, exigindo que os atacantes criem scripts para realizar o novo cálculo do endereço para a execução do código.

Ciclo de vida de uma injeção de processos:

1. Seleção do processo no qual o executável será injetado;
2. Seleção do executável que será injetado;
3. Alocação da memória no processo local do atacante, que irá conter a imagem do executável;
4. Alocação da memória no processo alvo criando espaço para o código a ser injetado;
5. Cálculo de endereçamento (rebasing);
6. Transferência da imagem do código para o processo alvo;
7. E, por fim, a criação de uma thread remota para iniciar a execução do payload.

O Cozy Bear usou essa técnica para executar *shellcodes* e bibliotecas (*DLLs*) maliciosas de forma furtiva em sistemas alvo. Esse tipo de ataque pode ser evitado pelo monitoramento de chamadas suspeitas de API nativas do Windows. Também é possível aplicar as regras YARA para detecção de malwares.

3) Deleção de Arquivos (MITRE T1070.004)

A deleção de arquivos foi uma técnica muito utilizada pelo grupo APT29 para remover seus traços em sistemas comprometidos, dificultando a detecção de uma invasão no sistema. Para a execução dessa técnica os atacantes utilizam o SDelete, uma aplicação da Microsoft que realiza remoção de dados de forma segura, sem chance de recuperação. Dessa forma, o grupo Cozy Bear usava dessa ferramenta para apagar logs de atividade, sobrescrevendo todos os dados que existiam sobre as atividades do grupo no sistema.

- Exemplo do uso do SDelete:

sdelete.exe -p 3 C:\temp\malicious_file.exe

Esse comando sobrescreve os dados do arquivo "malicious_fil.exe" realizando três operações de sobrescrita sobre o arquivo para garantir que os dados não possam ser recuperados facilmente.

4) Sequestro de ordem de Pesquisa

Essa técnica consiste em explorar a forma na qual o Windows executa programas que não fornecem nenhum caminho. No Windows é comum a realização de uma busca no diretório que inclui o programa a ser executado, sabendo disso, é possível criar um executável malicioso localizado no mesmo diretório, e com o mesmo nome do programa a ser executado. O sistema operacional do Windows possui um arquivo que define a ordem dos tipos de executáveis (PATHEXT), de acordo com a qual um programa que possui a extensão “.exe" tem menos prioridade de execução se comparado com um arquivo “.com". Assim, ao criar, por exemplo, um arquivo "net.exe" e um” outro arquivo "net.com", executando o comando “/C net user”, o arquivo a ser executado será o “net.com", devido a ordem definida no PATHEXT.

O APT29 aproveitou dessa vulnerabilidade para explorar aplicações que não informam caminhos ao carregar bibliotecas. Os atacantes criavam *DLLs* maliciosas que possuíam o mesmo nome da biblioteca, assim, o sistema carregava as *DLLs* por engano sem apontar nenhum erro. Uma forma simples de evitar essa vulnerabilidade é sempre utilizar caminhos absolutos para carregar bibliotecas. Outra forma, é o uso do *Process Monitor* para detectar carregamentos de arquivos suspeitos.

3.4 Credenciais de Acesso

O roubo de credenciais de acesso é particularmente comum em campanhas de espionagem cibernética, como as conduzidas pelo grupo APT29 (Cozy Bear), cujo foco é o acesso silencioso e prolongado a alvos estratégicos. Técnicas voltadas à coleta de credenciais muitas vezes se aproveitam de falhas humanas (como engenharia social) ou de fragilidades técnicas em mecanismos de autenticação.

Um exemplo recente é a campanha UNC6293 (2024–2025), associada ao APT29, que explora o uso de senhas de aplicativo para contornar a autenticação de dois fatores (*2FA*) em contas do Gmail. A técnica envolve campanhas de spear-phishing bem elaboradas, que se passam por convites oficiais do governo dos EUA e solicitam que a vítima gere e envie uma senha de aplicativo sob pretexto de liberar acesso a documentos restritos. Por serem geradas fora dos fluxos modernos de autenticação, essas senhas permitem acesso contínuo e invisível às caixas de e-mail, sem alertas ao usuário.

Essa abordagem se soma a outras já utilizadas historicamente pelo grupo, como o uso de portais falsos de login e o sequestro de tokens OAuth, demonstrando a capacidade adaptativa do APT29 em comprometer sistemas por meio da manipulação da camada humana. A seguir, analisamos algumas das principais técnicas empregadas pelo grupo para obter credenciais de acesso, explorando o papel da engenharia social, a persistência silenciosa proporcionada por métodos legados e a transição de vetores técnicos para manipulações psicológicas sofisticadas.

3.5 Exploração

O APT29 emprega técnicas sofisticadas de exploração para consolidar o acesso a sistemas-alvo, com ênfase na utilização de ferramentas nativas e na exploração de vulnerabilidades conhecidas.

Uma técnica amplamente observada é o uso de PowerShell (MITRE T1059.001). Após comprometer credenciais válidas ou explorar vulnerabilidades de acesso inicial, o grupo utiliza comandos PowerShell ofuscados para baixar *payloads* adicionais, executar *scripts* maliciosos e realizar movimentação lateral. Essa abordagem aproveita ferramentas legítimas do sistema operacional, reduzindo a probabilidade de detecção por soluções tradicionais de segurança. Além disso, o uso de PowerShell permite automatizar etapas de reconhecimento, coleta de credenciais e implantação de *backdoors*, tornando as operações mais resilientes e menos visíveis.

Outra técnica significativa é a exploração de vulnerabilidades locais para escalonamento de privilégios (MITRE T1068). Em múltiplas campanhas, o APT29 demonstrou a capacidade de incorporar rapidamente novas vulnerabilidades ao seu arsenal, como exemplificado pela exploração do CVE-2021-36934 (“SeriousSAM”). Ao obter privilégios elevados em sistemas comprometidos, o grupo consegue expandir seu alcance, criar contas administrativas ocultas e desativar controles de segurança, garantindo acesso persistente e facilitando a movimentação lateral para sistemas críticos adicionais.

3.6 Movimentação Lateral

“Movimentação lateral” diz respeito ao processo pelo qual invasores, de um ponto de entrada, espalham-se para o resto da rede. No geral, a primeira máquina infectada não é a de fato desejada - o propósito é justamente passar por múltiplos dispositivos, criando uma rede de comando e controle (C2), até chegar ao alvo. Com isso, mesmo que o ataque seja identificado, pode ser muito difícil mitigá-lo, pelo fato de vários computadores já estarem comprometidos. Durante o ataque à SolarWinds, por exemplo, o APT29 usou a estratégia de agendamento de tarefa (MITRE T1053.005) para, a cada máquina para a qual avançava na movimentação, fazia com que tarefas já programadas fossem alteradas, de forma que o seu escopo passasse a ser executar o código malicioso. Além disso, uma tarefa agendada foi alterada para manter o *malware* SUNSPOT mesmo com o reinício do computador.

Observa-se, nessa situação, a importância da movimentação lateral para grupos de ameaça persistente avançada, bem como a intersecção dessa abordagem com outras, como a persistência.

3.7 Exfiltração de Dados

O APT29 adota métodos avançados para exfiltrar dados de forma furtiva, priorizando a evasão de sistemas de monitoramento e a segmentação cuidadosa da informação violada.

Uma técnica recorrente é a **exfiltração por canal de comando e controle (C2)** (MITRE T1041). O grupo utiliza canais criptografados e protocolos comuns como *HTTPS* ou *DNS tunneling* para transferir dados roubados para servidores sob seu controle, dificultando a detecção por sistemas de prevenção de perda de dados (*DLP*) e *firewalls*. Essa abordagem permite que o tráfego malicioso se misture com comunicações legítimas, reduzindo alertas de segurança e assegurando a transmissão estável e segura de grandes volumes de informações.

Outra técnica empregada é o **fracionamento e encadeamento de dados exfiltrados**. Em ataques como o da cadeia de suprimentos SolarWinds, o APT29 demonstrou a capacidade de dividir grandes conjuntos de dados em fragmentos menores, transmitidos em sessões distintas ao longo de períodos prolongados. Essa fragmentação reduz o risco de alertas por volumes atípicos de tráfego e impede que sistemas de detecção correlacionem facilmente todas as partes da informação roubada. Além disso, a escolha de horários de baixo tráfego e o uso de canais redundantes garantem a resiliência da operação mesmo em caso de interrupções.

3.8 Reconhecimento/Forensics

A identificação de grupos APT é realizada por meio da análise de Indicadores de Comprometimento (*IOCs*), artefatos digitais que funcionam como evidências da presença de um invasor na rede, dispositivo ou sistema. Esses indicadores podem incluir endereços IP maliciosos, domínios de comando e controle, nomes de arquivos suspeitos, *hashes* de *malware* e padrões anômalos em *logs*. Durante a investigação do ataque à SolarWinds, por exemplo, pesquisadores detectaram comunicações com IPs associados a servidores russos, além da presença de domínios e arquivos relacionados ao *malware* Sunburst, utilizado pelo grupo APT29 (Cozy Bear). Os analistas descobriram que os atacantes utilizaram uma infraestrutura de rede distribuída, com endereços IP de diversos países, incluindo Estados Unidos, Turquia e até o Brasil, como forma de mascarar a origem real do ataque. Essa é uma tática comum entre grupos APT sofisticados, que recorrem a servidores de comando e controle (C2) hospedados em serviços de nuvem legítimos e em diversas regiões geográficas para evitar uma correlação direta com um país específico, como a Rússia, e burlar sistemas de detecção baseados em geolocalização. Durante a análise do *malware* Sunburst, especialistas da FireEye e Microsoft observaram que o tráfego das máquinas comprometidas era redirecionado para domínios maliciosos como avsvmcloud[.]com, e a comunicação posterior com IPs hospedados em diferentes países fazia parte dessa sofisticada estratégia de ocultamento e evasão.

4. Considerações Finais

No fim, percebe-se que as atividades do APT29 se refletem em formas de espionagem industrial e governamental, de forma a exfiltrar dados importantes para a estratégia política do país e promover vantagem competitiva em contextos mundiais, como foi evidenciado no processo de espionagem científica nas pesquisas de vacinas da COVID-19. Em complemento,

foi dado um contexto histórico-político dos ataques mais notáveis publicamente. Além disso, foram discutidas as principais técnicas e ferramentas utilizadas pelo grupo, de forma a criar um entendimento nas formas de atuação e em técnicas de prevenção.

5. Bibliografia Consultada

PICUSSECURITY.COM. Disponível em: <https://www.picussecurity.com/resource/blog/apt29-cozy-bear-evolution-techniques>. Acesso em: 01 jul. 2025.

ATTACK.MITRE.ORG. Disponível em: <https://attack.mitre.org/ >. Acesso em: 01 jul. 2025.

TRAININGCAMP.COM. Disponível em: <https://trainingcamp.com/glossary/password-expiration-policy/#:~:text=Password%20Expiration%20Policy...>. Acesso em: 03 jul. 2025.

WWW-PROOFPOINT-COM.TRANSLATE.GOOG. Disponível em: <https://www-proofpoint-com.translate.goog/us/threat-reference/privilege-escalation?_x_tr_sl=en...>. Acesso em: 04 jul. 2025.

REDFOXSEC.COM. Disponível em: <https://redfoxsec.com/blog/domain-trusts-a-comprehensive-exploitation-guide/>. Acesso em: 04 jul. 2025.

ONELOGIN.COM. Disponível em: <https://www.onelogin.com/learn/federated-identity#:~:text=Federated%20identity...>. Acesso em: 04 jul. 2025.

MADDEVS.IO. Disponível em: <https://maddevs.io/glossary/cloud-tenant/>. Acesso em: 04 jul. 2025.

EXPRESSVPS.COM.BR. Disponível em: <https://expressvps.com.br/glossario/o-que-e-instance/>. Acesso em: 04 jul. 2025.

CLOUDFLARE.COM. Disponível em: <https://www.cloudflare.com/pt-br/learning/security/glossary/what-is-lateral-movement/>. Acesso em: 04 jul. 2025.

TECHTARGET.COM. Disponível em: <https://www.techtarget.com/searchsecurity/definition/steganography#:~:text=Steganography...>. Acesso em: 02 jul. 2025.

PICUSSECURITY.COM. Disponível em: <https://www.picussecurity.com/resource/blog/t1055-002-portable-executable-injection>. Acesso em: 02 jul. 2025.

PICUSSECURITY.COM. Disponível em: <https://www.picussecurity.com/resource/glossary/what-is-a-yara-rule>. Acesso em: 03 jul. 2025.

OKTA.COM. Disponível em: <https://www.okta.com/identity-101/dll-hijacking/>. Acesso em: 03 jul. 2025.

THEGUARDIAN.COM. Disponível em: <https://www.theguardian.com/world/2020/dec/14/suspected-russian-hackers-spied-on-us-federal-agencies>. Acesso em: 01 jul. 2025.

NCSC.GOV.UK. Disponível em: <https://www.ncsc.gov.uk/news/advisory-apt29-targets-covid-19-vaccine-development>. Acesso em: 01 jul. 2025.

BITSIGHT.COM. Disponível em: <https://www.bitsight.com/blog/the-financial-impact-of-solarwinds-a-cyber-catastrophe-but-insurance-disaster-avoided>. Acesso em: 01 jul. 2025.

CFCS.DK. Disponível em: <https://www.cfcs.dk/globalassets/cfcs/dokumenter/rapporter/en/CFCS-solarwinds-report-EN.pdf>. Acesso em: 01 jul. 2025.

FIREEYE.COM. Disponível em: <https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises.html>. Acesso em: 01 jul. 2025.

RESEARCH.NCCGROUP.COM. Disponível em: <https://research.nccgroup.com/2020/04/08/dns-tunneling-techniques/>. Acesso em: 01 jul. 2025.

FREEMINDTRONIC.COM. Disponível em: <https://freemindtronic.com/apt29-exploits-app-passwords/>. Acesso em: 02 jul. 2025.