INSTITUTO DE ENGENHARIA NUCLEAR

EDUARDO ANDRADE DE JESUS

SOBRE ATAQUES CIBERNÉTICOS QUE EXPLORAM VULNERABILIDADES HUMANAS E TECNOLÓGICAS NO SETOR NUCLEAR: ESTUDO DE CASO EM UM INSTITUTO DE PESQUISA.

Rio de Janeiro

2023

EDUARDO ANDRADE DE JESUS

SOBRE ATAQUES CIBERNÉTICOS QUE EXPLORAM VULNERABILIDADES HUMANAS E TECNOLÓGICAS NO SETOR NUCLEAR: ESTUDO DE CASO EM UM INSTITUTO DE PESQUISA.

Dissertação apresentada ao Programa de Pós-graduação em Ciência e Tecnologia Nucleares do Instituto de Engenharia Nuclear da Comissão Nacional de Energia Nuclear como parte dos requisitos necessários para a obtenção do grau de Mestre em Ciências e Tecnologias Nucleares.

Orientadores: Dr. Guilherme Dutra Gonzaga Jaime e
Prof. Dr. Claudio Márcio do Nascimento Abreu Pereira

RIO DE JANEIRO

2023

ANDR Andrade de Jesus, Eduardo
Sobre ataques cibernéticos que exploram vulnerabilidades humanas e tecnológicas no setor nuclear: estudo de caso em um instituto de pesquisa / Eduardo Andrade de Jesus – Rio de Janeiro: CNEN/IEN, 2023.

127 f.

Orientadores: Guilherme Dutra Gonzaga Jaime e Cláudio Márcio do Nascimento Abreu Pereira

Dissertação (Mestrado) – Instituto de Engenharia Nuclear, PPGIEN, 2023.

1. Segurança Cibernética. 2. Ataques cibernéticos. 3. Infraestruturas críticas. 4. Instalações nucleares. 5. Engenharia Social e Phishing. 6.exploração de vulnerabilidades

Aqui entra a folha de aprovação original

Dedico este trabalho à minha família, cujo amor, apoio e incentivo foram fundamentais para a realização desta dissertação. À memória amorosa da minha mãe e ao meu pai minha gratidão eterna. Seus valores, amor e apoio são a base dessa conquista.

AGRADECIMENTOS

Gostaria de expressar meus sinceros agradecimentos a todos aqueles que contribuíram para a realização deste trabalho.

Minha família, e em especial minha esposa Vanessa, merecem uma gratidão profunda por estarem sempre ao meu lado, oferecendo apoio incansável durante esse período de dedicação aos estudos. Sua presença constante, auxílio nas tarefas cotidianas e dedicação à educação de nossos três filhos - Ana Beatriz, Pedro Henrique e Caio Victor - foram fundamentais para que eu pudesse me concentrar em minhas pesquisas.

Quero estender minha profunda gratidão ao meu orientador, Dr. Guilherme Dutra Gonzaga Jaime, por sua dedicação exemplar, paciência infinita e vasto conhecimento. Seus ensinamentos enriquecedores moldaram minha jornada de progresso e crescimento acadêmico, orientando-me com sabedoria e inspiração.

Também não posso deixar de reconhecer a orientação e o apoio inestimáveis do Professor Dr. Cláudio Márcio do Nascimento Abreu Pereira. Suas ideias instigantes e incentivo constante transformaram essa experiência em algo genuinamente inspirador para mim.

Enfim, agradeço a todos aqueles que, de uma maneira ou de outra, contribuíram para o sucesso deste trabalho. Cada gesto de apoio, palavra gentil e orientação valiosa foram peças essenciais nessa jornada, e estou profundamente grato por toda a colaboração e incentivo que recebi.

RESUMO

O setor nuclear, de forma geral, lida com materiais radioativos e informações sensíveis que podem representar riscos para a população e o meio ambiente se não forem tratadas com os devidos cuidados. Essas instalações dependem de recursos tecnológicos robustos para operar de forma ininterrupta. No entanto, assim como outros setores industriais, o setor nuclear tem sido alvo frequente de ataques cibernéticos perpetrados por indivíduos mal-intencionados e grupos de cibercriminosos. Esses ataques envolvem o uso de ferramentas automatizadas, técnicas de engenharia social, códigos maliciosos e outros métodos prejudiciais. È essencial que o setor nuclear brasileiro esteja constantemente vigilante em relação às ameaças cibernéticas. A manutenção eficaz dessas instalações é crucial para garantir a integridade das tecnologias, dos dados, das pessoas e das organizações envolvidas, possibilitando a continuidade das operações em ambientes críticos. Neste trabalho de pesquisa, foram utilizados recursos reais e foram aplicados padrões de testes práticos com base em técnicas e metodologias de segurança cibernética. Com base no *framework* Cyber Kill Chain, foi conduzido um estudo de caso em um ambiente controlado de um instituto de pesquisa do setor nuclear brasileiro, investigando o comportamento humano e das tecnologias sob possíveis ameaças cibernéticas. Como resultado, foram identificadas vulnerabilidades e ameaças que afetavam os fatores humanos e tecnológicos daquela organização, propondo-lhe correções e melhorias por meio de procedimentos, treinamento de conscientização, políticas e normas voltadas para pessoas que trabalham em infraestruturas críticas, como o setor nuclear brasileiro, com base nas lições aprendidas neste estudo de caso.

Palavras-chave: segurança cibernética, ataques cibernéticos, infraestruturas críticas, instalações nucleares, engenharia social, *phishing*, exploração de vulnerabilidades

ABSTRACT

The nuclear sector, in general, deals with radioactive materials and sensitive information that can pose risks to the population and the environment if not handled with due care. These facilities rely on robust technological resources to operate continuously. However, like other industrial sectors, the nuclear sector has been a frequent target of cyberattacks perpetrated by malicious individuals and cybercriminal groups. These attacks involve the use of automated tools, social engineering techniques, malicious code, and other harmful methods. It is essential for the Brazilian nuclear sector to remain constantly vigilant against cyber threats. Effective maintenance of these facilities is crucial to ensure the integrity of technologies, data, people, and organizations involved, enabling the continuity of operations in critical environments. In this research work, real resources were used, and practical testing standards were applied based on cybersecurity techniques and methodologies. Based on the Cyber Kill Chain framework, a case study was conducted in a controlled environment of a Brazilian nuclear sector research institute, investigating the behavior of humans and technologies under potential cyber threats. As a result, vulnerabilities and threats affecting both human and technological factors of that organization were identified, proposing corrections and improvements through procedures, awareness training, policies, and regulations aimed at individuals working in critical infrastructure, such as the Brazilian nuclear sector, based on the lessons learned in this case study.

Keywords: cyber security, cyber attacks, critical infrastructure, nuclear facilities, social engineering, phishing, exploitation of vulnerabilities

LISTA DE QUADROS

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA ABREVIATURAS E SIGLAS

CNEN	-	Comissão Nacional de Energia Nuclear
IAEA	-	International Atomic Energy Agency
IEN	-	Instituto de Engenharia Nuclear
IDS	-	Intrusion Detection System
IPS	-	Intrusion Prevention System
NEA	-	Nuclear Energy Agency
NRC	-	Nuclear Regulatory Commission
NIST	-	National Institute of Standards and Technology
SIC	-	Industrial Control Systems
SOC	-	Security Operations Center
SIEM	-	Security Information and Event Management

SUMÁRIO

1. INTRODUÇÃO

1.1. EXPOSIÇÃO DO TEMA

A crescente adoção de sistemas computacionais trouxe consigo um aumento expressivo das ameaças cibernéticas em todo o mundo. Os ataques cibernéticos vêm se tornando mais frequentes, sofisticados e direcionados, representando uma ameaça de crescimento cada vez mais acelerado à segurança e privacidade das pessoas e das organizações (SECURITY REPORT, 2023).

Uma forma muito usada e de difícil detecção/prevenção é o *phishing*. Um ataque de *phishing* é uma tentativa fraudulenta de obter informações sensíveis, como nomes de usuário, senhas, detalhes de cartões de crédito, entre outros, disfarçando-se como uma entidade confiável em uma comunicação eletrônica (CHIEW *et al*., 2018). O *phishing* é comumente usado como uma das primeiras etapas de um ataque cibernético direcionado, e pode levar a perdas financeiras significativas, divulgação não autorizada de informações confidenciais, como também pode, se combinado com outras formas de ataques, resultar em interrupção das operações de organizações, incluindo infraestruturas críticas (MITNICK, 2003).

Os hackers e grupos de cibercriminosos estão se especializando cada vez mais em técnicas sofisticadas de engenharia social, como o *phishing*, para realizarem o acesso inicial a uma infraestrutura tecnológica (ALABDAN, 2020). Através de campanhas direcionadas de e-mail *phishing* eles conseguem penetrar as proteções computacionais, por meio das vulnerabilidades humanas, ou seja, sem que as pessoas percebam que estão sendo vítimas de um ataque. Desta forma, tem se tornado cada vez mais difícil para o ser humano saber diferenciar um e-mail autêntico de um e-mail malicioso.

Embora muitas organizações tomem as devidas precauções para aumentar a segurança cibernética, os ataques de *phishing* continuam sendo uma ameaça significativa para as empresas e instituições (KASPERSKY, 2023). É necessário um esforço constante para educar e conscientizar os indivíduos sobre as ameaças cibernéticas, e desenvolver a consciência necessária para aumentar a proteção contra esses ataques virtuais.

Assim, o fortalecimento do aparato tecnológico de segurança cibernética em instalações críticas deve estar diretamente alinhado aos cuidados que o ser humano deve ter no seu ambiente de trabalho, pois essas ameaças podem se concretizar

quando as pessoas agem de forma desatenta, por autoconfiança ou são induzidas a realizarem ações precipitadas, descuidando-se assim da segurança da informação e negligenciando as políticas protetivas de uma organização.

As instituições do setor nuclear brasileiro são responsáveis por fornecer energia elétrica, além de desempenhar um papel fundamental na pesquisa e desenvolvimento. Essas instalações têm sido alvos de ataques cibernéticos, conforme mencionado por Venkatachary *et al.* (2017), o que tem o potencial de causar danos e prejuízos, pondo em risco as pessoas, o meio ambiente, a infraestrutura crítica e até mesmo a segurança nacional.

O tema em questão (Segurança Cibernética em instalações nucleares) tem sido abordado em diversos trabalhos recentes (TAVARES *et al.*, 2021; PETERSON *et al*., 2019; ZHANG *et al.* e 2020; LINNOSMAA et al, 2021). No Brasil, encontram-se formado o grupo técnico e grupo redator responsáveis pelos estudos e criação da norma CNEN NN 2.07- “Segurança Cibernética de Instalações Nucleares” (CNEN/DRS/DISEN, 2020)

Nesse contexto específico, esta dissertação tem como objetivo simular um ataque *phishing* a um instituto de pesquisa do setor nuclear, somado a um estudo de vulnerabilidades de sistemas importantes para a instituição, bem como analisar como as ameaças do mundo real podem comprometer a segurança.

A presente proposta baseia-se na elaboração de um estudo de caso prático e realístico, em que serão discutidos os impactos causados por esses ataques quando bem-sucedidos.

Por fim, são feitas sugestões de melhorias e ações corretivas que sejam capazes de mitigar riscos de ataques similares aos usados neste trabalho. Contribuindo-se, assim, para fortalecer a segurança cibernética da organização alvo do estudo.

1.2. PROBLEMA DE PESQUISA E OBJETIVOS DA PESQUISA

1.2.1 PROBLEMA DE PESQUISA

Por meio da revisão da literatura realizada, ficou evidente que alguns dos principais incidentes cibernéticos ocorridos em instalações nucleares, até o presente

momento, foram decorrentes da exploração inicial de vulnerabilidades humanas (KROMBHOLZ, 2015).

A falta de aplicação de correções de segurança (*patch*[1]) e descoberta de falhas do tipo "*zero-day*[2]") também são causas de incidentes. Dentre esses fatores, ainda podemos destacar a falta de modernização dos equipamentos, dispositivos e sistemas industriais. (ZHANG et al., 2020)

Assim, a questão norteadora considerada como problema de pesquisa deste trabalho é:

"Como contribuir para o fortalecimento da segurança cibernética de pessoas e de organizações do setor nuclear brasileiro?"

1.2.2 OBJETIVOS DA PESQUISA

O objetivo geral desta dissertação é investigar vulnerabilidades humanas e tecnológicas em ambientes de infraestruturas críticas através de um estudo de caso.

Para atingir o objetivo geral deste trabalho, foram definidos os seguintes objetivos específicos: (1) descrever os principais incidentes cibernéticos e as ameaças que podem afetar as infraestruturas críticas, decorrentes de ataques de engenharia social; (2) combinar engenharia social com técnicas computacionais para realizar um ataques cibernético simulado a um instituto de pesquisa; e (3) propor melhorias nos mecanismos de segurança cibernética da instituição que não estejam de acordo com as normas técnicas e as boas práticas aplicadas ao cenário global.

1.3 HIPÓTESE

Os ambientes industriais atualmente possuem em suas instalações a arquitetura de rede de Tecnologia da Informação (TI) e de Tecnologia Operacional (TO) integradas (BRANQUINHO *et al.*, 2021). No passado, havia essa segmentação física e lógica.

De um lado, temos a rede de TI que é composta por equipamentos de computação tradicionais como estações de trabalho, servidores físicos e virtualizados,

---

[1] Atualizações e correções efetuadas em um programa, sistema ou equipamento existente, com intenção de corrigir uma vulnerabilidade específica (ABNT NBR ISO/IEC 27002:2022).

[2] Falha de segurança de um software, que ainda não é conhecida por seus desenvolvedores, pelos fabricantes de soluções de segurança e pelo público em geral (MCA 7-1, 2023).

equipamentos de interconectividade (switches e roteadores), firewalls, rede wireless, serviços e aplicações, além dos protocolos TCP/IP. Por outro lado, temos a rede de TO que consiste em ambientes compostos por sistemas SCADA *(Supervisory Control And Data Acquisition),* PLC (*Programmable Logic Controller*), bem como sistemas supervisórios, dispositivos e protocolos industriais específicos.

De acordo com Garcia (2018), essas redes apresentam pouca maturidade a nível de segurança cibernética, tendo se tornado alvos de ataques direcionados com objetivo de inviabilizar as operações de setores considerados essenciais para a sociedade.

Por essa razão, os sistemas de controles industriais necessitam estar disponíveis de forma ininterrupta. Como mencionado por Segundo (2019), a parada de serviços essenciais decorrente de um ataque cibernético poderá impactar diretamente no risco da sobrevivência humana, enquanto a indisponibilidade em sistemas de TI para determinados setores, poderá impactar financeiramente.

Este trabalho explora a hipótese de que atacantes possam ingressar em um ambiente de Tecnologia da Informação (TI) e/ou de Tecnologia Operacional (TO) de um instituto de pesquisa da área nuclear, através de técnicas de envio de e-mail *phishing* para funcionários da referida organização.

Em sendo a hipótese inicial validada, será possível sugerir ações que possam mitigar vulnerabilidades humanas (treinamentos e conscientização) e tecnológicas (*hardening*[3]).

1.4 JUSTIFICATIVA

A justificativa desta pesquisa baseia-se no aumento significativo dos ataques cibernéticos em todo o mundo, inclusive no Brasil no período pós-pandemia (LALLIE, 2021). Em 2022, dados revelaram que o país foi alvo de mais de 100 bilhões de tentativas de ataques cibernéticos (SECURITY REPORT, 2023).

É evidente que esse tema é de extrema relevância, inclusive para a segurança nacional, uma vez que, caso ações maliciosas sejam bem-sucedidas, elas podem impactar vários setores cruciais, incluindo a economia, o setor energético, o meio

[3] Processo de aplicação de configuração de segurança e outras medidas técnicas que tornam o sistema mais seguro. (ABNT NBR ISO/IEC 27002:2022)

ambiente, o setor industrial, o setor nuclear e outros componentes do Sistema de Infraestruturas Críticas (SIC) (PNSIC, 2018) do país.

Portanto, a expectativa é de que esta pesquisa contribua de forma positiva para o tema em questão, buscando colaborar ainda mais com a segurança cibernética no setor nuclear. Além disso, espera-se que esse trabalho estimule a realização de mais pesquisas com o objetivo de reduzir e mitigar as ameaças cibernéticas que visam impactar as instalações nucleares.

1.5 ABORDAGEM METODOLÓGICA

Neste trabalho, a pesquisa foi conduzida em várias etapas para abordar de forma abrangente o problema de pesquisa. Inicialmente, realizou-se uma revisão da literatura para estabelecer o contexto e identificar as lacunas de conhecimento relevantes, relacionados ao tema segurança cibernética em instalações do setor nuclear e infraestruturas críticas. Em seguida, conduziu-se uma pesquisa descritiva e exploratória com abordagem qualitativa para coletar dados e aprofundar a compreensão sobre o tema em questão. Por fim, realizou-se um estudo de caso para aplicação dos conceitos teóricos previamente identificados.

O estudo de caso abrangeu a utilização de engenharia social, onde foi criado um contexto convincente de um programa de capacitação nuclear que deveria ser realizado por funcionários daquela instituição. Nesse contexto, foram enviados e-mails de *phishing* na tentativa de convencer os colaboradores do instituto de pesquisa a clicarem nos respectivos links contidos no corpo da mensagem. Caso essa ação fosse bem-sucedida na obtenção de informações por meio desse procedimento, um ataque cibernético simulado e controlado seria realizado, com objetivo de avaliar a viabilidade de uma intrusão não autorizada na infraestrutura tecnológica da instituição de pesquisa. Dessa forma, seria possível identificar se há vulnerabilidades e fraquezas, abrangendo tanto os fatores humanos quanto os recursos tecnológicos. A etapa final deste processo compreendeu a conscientização e o treinamento para o corpo de colaboradores da instituição, bem como a sugestão de propostas visando mitigar essas ameaças.

1.6 ESTRUTURA DO TRABALHO

O restante deste trabalho está estruturado da seguinte forma:

O Capítulo 2 trata do referencial teórico, apresenta conceitos, definições e aspectos importantes relacionados à segurança cibernética, inclusive em instalações nucleares. O Capítulo 3 apresenta a metodologia do trabalho, especificando os detalhes de cada etapa. No Capítulo 4, são apresentados os resultados e discussões. Por fim, o Capítulo 5 apresenta a conclusão e o Capítulo 6 as sugestões para trabalhos futuros.

Adicionalmente, no Apêndice A é apresentada uma cartilha de segurança cibernética contra os ataques de *phishing,* adaptado para o uso no instituto alvo deste trabalho.

2 REFERENCIAL TEÓRICO

Neste capítulo, apresentamos a fundamentação teórica do estudo, que tem como objetivo fornecer os conceitos essenciais para a compreensão das teorias e métodos abordados nesta dissertação.

2.1 SEGURANÇA CIBERNÉTICA EM INSTALAÇÕES NUCLEARES

2.1.1 Ameaças e incidentes de Segurança Cibernética

Um ataque cibernético é toda prática maliciosa que tem por objetivo a utilização de meios furtivos para acessar um ambiente tecnológico não autorizado com diversas finalidades criminosas, sendo capaz de inviabilizar o acesso legítimo.

De acordo com a ABNT NBR ISO/IEC 27032:2015, o conceito de ataque cibernético pode ser definido como:

> Um ataque cibernético é uma ação intencional realizada por indivíduos, grupos ou organizações com o objetivo de explorar vulnerabilidades em sistemas de informação, redes de computadores ou infraestruturas digitais, visando comprometer a confidencialidade, integridade ou disponibilidade desses recursos, causando danos, interrupções ou obtendo benefícios ilícitos.

No cenário global, os ataques cibernéticos se tornaram cada vez mais frequentes e sofisticados (GSA, 2021). Conforme Tabela 1, existem atualmente diversas categorias de tipos de ataques e grupos hackers especializados em cada uma delas:

Tabela 1: Categorias de ameaças cibernéticas

Tipos de ameaças	**Descrição**
Malwares	Software malicioso projetado para danificar, acessar ou controlar um sistema sem autorização, como vírus, *worms*, *trojans*, *ransomware* e *spyware*. (ABNT NBR ISO/IEC 27002:2022)

Ataques de *phishing*	De acordo com a norma ABNT NBR ISO/IEC 27032:2015, o conceito de *phishing* é definido como um processo fraudulento de tentativa de adquirir informações confidenciais disfarçando-se de entidade confiável em uma comunicação eletrônica
Ataques de negação de serviço (DoS)	Tentativas de inundar um sistema ou rede com tráfego excessivo para sobrecarregá-lo e torná-lo inacessível aos usuários legítimos. (MCA 7-1, 2023)
Ataques *Defacement*	Consiste na técnica de realização de modificação de conteúdos de páginas web, onde o conteúdo da página original é substituído por conteúdos embaraçosos, manifestações ofensivas e assinaturas do invasor. (JAIME *et al.*, 2019)
Ataques de injeção SQL	Exploração de vulnerabilidades em aplicativos da web para inserir comandos SQL maliciosos e obter acesso não autorizado ao banco de dados. (MCA 7-1, 2023)
Ataques de engenharia social	Manipulação psicológica dos usuários para obter acesso não autorizado a informações confidenciais ou sistemas. (MCA 7-1, 2023)
Ataques de *ransomware*	Bloqueio ou criptografia de dados por hackers, exigindo um resgate (geralmente em criptomoedas) para restaurar o acesso aos dados. (MCA 7-1, 2023)
APT (*Advanced Persitent Threats*)	APTs são ataques cibernéticos executados por adversários sofisticados e com bons recursos visando informações específicas em empresas e governos de alto perfil, geralmente em uma campanha de longo prazo envolvendo diferentes etapas. (KROMBHOL, 2015)

2.1.1.1 Grupos de hackers

Os grupos hackers, também conhecidos como grupos de cibercriminosos, são organizações ou indivíduos que se unem para realizar atividades ilícitas no mundo digital (KROMBHOLZ, 2015). Esses grupos compartilham conhecimentos técnicos e recursos para explorar vulnerabilidades em sistemas de informação, redes de computadores e infraestruturas digitais, com o objetivo de obter acesso não autorizado, causar danos, roubar informações valiosas ou lucrar de forma ilícita (CHEN; DESMET; HUYGENS, 2014).

Acrescentando a isso, esses grupos têm motivações diversas, que variam desde fins políticos, ideológicos ou ativismo cibernético até interesses financeiros. Algumas organizações hackers focam em atividades como espionagem cibernética, roubo de dados pessoais, ataques de *ransomware*, desfiguração de sites, fraude financeira, entre outros (CHEN; DESMET; HUYGENS., 2014). Eles se comunicam e coordenam suas ações por meio de fóruns online, redes sociais, mensagens criptografadas e outras plataformas de comunicação.

Conforme mencionado por Hawamleh *et al.* (2020), é importante destacar que nem todos os grupos hackers têm intenções maliciosas. De acordo com o estudo de Sinha e Aroro (2020), existem também grupos de hackers éticos, conhecidos como "hackers do bem" ou "*white-hackers"*, que utilizam suas habilidades para identificar vulnerabilidades e ajudar a melhorar a segurança cibernética de empresas e organizações, atuando de forma legal e ética.

No entanto, é essencial saber distinguir os grupos hackers legítimos, como os mencionados anteriormente, e os grupos criminosos que praticam atividades ilegais, já que a maioria das atividades realizadas por grupos hackers é ilegal e prejudicial, causando danos financeiros, violações de privacidade e interrupções em serviços digitais (SINHA; ARORA, 2020).

Segundo a pesquisa de XU, Y. *et al*. (2022), muitos grupos hackers ganharam notoriedade no cenário global pós-pandemia do COVID-19 devido às suas atividades e ataques cibernéticos coordenado, dentre eles podemos destacar:

- **APT29** (também conhecido como Cozy Bear ou The Dukes): O grupo APT29 é atribuído à Rússia e é conhecido por suas atividades de espionagem cibernética. Eles têm como alvo governos, organizações militares e instituições

acadêmicas. O APT29 esteve envolvido em várias campanhas de ataques cibernéticos, como o ataque à Agência Nacional de Segurança dos EUA (NSA) em 2015.

- **APT28** (também conhecido como Fancy Bear ou Sofacy): Outro grupo atribuído à Rússia, o APT28 é conhecido por conduzir operações de espionagem cibernética em grande escala. Eles têm como alvo governos, instituições militares, organizações de defesa e empresas de energia. O APT28 esteve envolvido em ataques como a intrusão nos servidores do Comitê Nacional Democrata (DNC) dos Estados Unidos em 2016.

- **Lazarus Group**: O grupo Lazarus é atribuído à Coreia do Norte e está envolvido em uma ampla gama de atividades cibernéticas maliciosas. Eles têm como alvo governos, instituições financeiras e empresas de diferentes setores. O Lazarus Group ficou famoso por ataques como o ataque ao Sony Pictures Entertainment em 2014 e o ataque ao Banco Central de Bangladesh em 2016, que resultou no roubo de cerca de US$ 81 milhões.

- **DarkSide**: O grupo DarkSide ganhou destaque em 2021 devido a seus ataques de ransomware. Eles têm como alvo empresas e organizações, geralmente visando setores críticos, como energia e transporte. O ataque mais notório do DarkSide foi o ataque ao Colonial Pipeline nos Estados Unidos, que causou interrupções no fornecimento de combustível para a costa leste do país.

- **REvil** (também conhecido como Sodinokibi): O grupo REvil é conhecido por sua atividade de ransomware e por conduzir ataques contra empresas em todo o mundo. Eles exigem resgates em criptomoedas em troca da liberação dos dados sequestrados. O REvil ficou conhecido por ataques de alto perfil, como o ataque à empresa de gerenciamento de TI Kaseya em 2021, que afetou centenas de empresas em todo o mundo.

2.1.1.2 Dados históricos de incidentes cibernéticos

Os ataques cibernéticos têm se tornado cada vez mais proeminentes, causando consequências alarmantes para instalações nucleares, setor elétrico e outras infraestruturas críticas. Entre esses ataques de destaque, podemos mencionar:

- **Usina nuclear de Natanz**: Em 2010, a usina nuclear de Natanz, no Irã, foi alvo de um ataque cibernético por meio de um *malware* chamado Stuxnet. O ataque foi supostamente realizado pelos Estados Unidos e Israel, e teve como alvo as centrífugas de enriquecimento de urânio (RISI Online Incidente Database, 2012).

  O Stuxnet é amplamente reconhecido como um dos ataques cibernéticos mais notáveis e sofisticados da história. Considerado a primeira instância de um ataque de redes de computadores conhecido por causar danos físicos além das fronteiras internacionais, comenta Linsay (2013). Já Farwall e Rohozinski (2011) relatam que o *worm* foi projetado para sabotar o programa nuclear do Irã, concentrando-se nas centrífugas de enriquecimento de urânio. Ao explorar vulnerabilidades nos sistemas de controle industrial, o Stuxnet conseguiu se infiltrar e se espalhar por meio de dispositivos USB, estabelecendo um novo marco na era dos ataques cibernéticos direcionados a infraestruturas críticas (LINDSAY, 2013).

  Conforme discutido no estudo de Lindsay (2013), a descoberta e análise do Stuxnet trouxeram à tona a conscientização sobre a vulnerabilidade das infraestruturas críticas aos ataques cibernéticos. Esse caso emblemático demonstrou a sofisticação e a capacidade destrutiva que os ciberataques podem ter, especialmente quando direcionados a setores estratégicos e sensíveis, como a energia nuclear. Consequentemente, reforçou-se a necessidade de aumentar a segurança cibernética nessas áreas, a fim de proteger as infraestruturas críticas contra ameaças cada vez mais avançadas (BAEZNER; ROBIN, 2017).

- **Usina nuclear de Gundremmingen**: Em 2016, a usina nuclear de Gundremmingen, na Alemanha, foi alvo de um ataque cibernético que visou a rede de computadores da instalação. O ataque foi realizado por meio de um e-

mail *phishing*, que permitiu que os invasores tivessem acesso ao sistema de controle da usina. (RISI Online Incidente Database, 2016).

- **Usina nuclear de Khmelnytskyi**: Em 2020, a usina nuclear na Ucrânia, foi alvo de um ataque cibernético que visou o sistema de informação da instalação. O ataque foi realizado por meio de um malware chamado "Pioneer", que foi disseminado por meio de um e-mail de *phishing* (TI SAFE Incidente Hub, 2020).

- **Sistema elétrico ucraniano**: Em 2015 e 2016, o sistema elétrico da Ucrânia foi alvo de uma série de ataques cibernéticos que resultaram em apagões em larga escala. Os ataques foram atribuídos a um grupo de hackers russos conhecido como SandWorm, que usou malware para desligar os sistemas de energia da região (RISI Online Incidente Database, 2015).

- **Empresa Colonial Pipeline**: Em 2021, a empresa Colonial Pipeline, que é responsável pelo fornecimento de combustível para a Costa Leste dos Estados Unidos, foi alvo de um ataque cibernético que resultou no fechamento temporário do oleoduto da empresa. O ataque foi realizado por um grupo de hackers chamado DarkSide, que usou ransomware para criptografar os dados da empresa e exigiu um resgate em Bitcoin para desbloquear os sistemas (TI SAFE Incidente Hub, 2021).

- **Rede elétrica da Índia**: Em 2021, a rede elétrica da Índia foi alvo de um ataque cibernético que resultou em apagões em larga escala em várias partes do país. O ataque foi atribuído a um grupo de hackers chineses que usou malware para invadir os sistemas de controle de energia da Índia (TI SAFE Incidente Hub, 2021).

- **Empresa Eletronuclear**: Em 2021, a empresa foi alvo de um ataque cibernético no ambiente da tecnologia da informação causado por um ataque de ransomware que alcançou parte dos servidores da rede administrativa. A Eletrobras ressalta que a rede administrativa não se conecta com os sistemas

operativos das usinas nucleares de Angra 1 e Angra 2 que são, por razões de segurança, isolados da rede administrativa (CISO ADVISOR, 2021).

2.1.2 A incidência dos ataques cibernéticos durante a pandemia

Antes da pandemia de COVID-19, os ataques cibernéticos já eram uma preocupação significativa, mas com a crescente digitalização e dependência da tecnologia durante a pandemia, para Lallie (2021) os ataques aumentaram de forma exponencial tanto em frequência quanto em sofisticação.

Durante a pandemia, os ataques cibernéticos se intensificaram, sendo exploradas vulnerabilidades de sistemas e usuários mal treinados para lidar com as mudanças rápidas e a dependência da tecnologia, conforme descrito em SILVA (2021). Além disso, o trabalho remoto global e o aumento das aplicações web forneceram novas oportunidades para os cibercriminosos explorarem.

De acordo com a Tabela 2, algumas ações foram mais incentivadas que outras durante a pandemia, como podemos verificar.

Tabela 2 - Atividades incentivadas durante a pandemia Covid-19

Atividades em expansão	**Incentivo**
Aumento de ataques de *phishing*	Com o aumento do trabalho remoto e da comunicação online, BUIL-GIL (2020) relata que tenha havido um aumento de 400% nos ataques de *phishing* relacionados ao COVID-19 em 2020.
Aumento de ataques de *ransomware*	Empresas de saúde, instituições governamentais e até instalações críticas foram alvos. O relatório da empresa de segurança SONICWALL (2021) aponta um aumento de 62% nos ataques de ransomware em comparação com o ano anterior.

Exploração de vulnerabilidades em *software* e sistemas	Várias vulnerabilidades críticas em softwares foram descobertas, resultando em ataques em larga escala do tipo zero-day (KUMAR; SINHA, 2021).
Ataques direcionados a instituições	Os ataques cibernéticos direcionados a instituições do governo aumentaram significativamente durante a pandemia. De acordo com a (Check Point, 2022) o setor de saúde sofreu um aumento de 45% nos ataques cibernéticos no primeiro semestre de 2020.
Aumento do uso de serviços de nuvem	O uso de serviços de nuvem aumentou consideravelmente, atraindo a atenção dos hackers, e consequentemente levando a um aumento nos ataques direcionados a infraestruturas de nuvem e a fornecedores de serviços (CISCO, 2021).

2.2 A ENGENHARIA SOCIAL COMO UM VETOR DE ATAQUE

2.2.1 Conceitos e técnicas de Engenharia Social

A Engenharia Social é uma técnica utilizada para manipular pessoas almejando obter informações confidenciais, acesso privilegiado a tecnologias ou realizar ações não autorizadas (ALDAWOOD, 2019). De acordo com Salahdine e Kaabouch (2019), essas técnicas quando aplicadas em instalações críticas, como sistemas de energia, telecomunicações, saúde e transporte, podem representar uma ameaça significativa à segurança.

Algumas técnicas de Engenharia Social que podem ser usadas para explorar instalações do setor nuclear:

a) *Phishing*: consiste em uma técnica de engenharia social que envolve o envio de e-mails ou mensagens fraudulentas que se passam por entidades confiáveis, como empresas ou organizações conhecidas. Essas mensagens geralmente pedem informações pessoais ou solicitam que o destinatário clique em links maliciosos,

levando a vazamento de dados ou instalação de malware (SALAHDINE; KAABOUCH, 2019)

b) *Pretexting*: consiste na criação de um cenário falso ou uma história inventada para obter informações das pessoas, como se passar por um funcionário de suporte técnico. (SALAHDINE; KAABOUCH, 2019)

c) *Spear phishing*: consiste em uma forma mais direcionada de *phishing*, na qual os cibercriminosos pesquisam informações específicas sobre um indivíduo ou organização para personalizar e direcionar os ataques, tornando-os mais convincentes (SALAHDINE; KAABOUCH, 2019)

d) *Pharming*: consiste em redirecionar o tráfego da Internet de uma pessoa para um site falso, no qual são solicitadas informações pessoais ou financeiras da vítima, fazendo com que esses dados caiam nas mãos de criminosos (SALAHDINE; KAABOUCH, 2019).

2.2.2 Estruturação da metodologia e construção dos artefatos tecnológicos deste trabalho de pesquisa

Com o intuito de realizar um experimento que refletisse de forma realístico sobre as ameaças cibernéticas atuais que exploram as vulnerabilidades humanas no setor nuclear, adotou-se uma abordagem contextualizada fictícia, levando em consideração o fator humano, inicialmente.

Essa abordagem foi construída com base em três desafios que as organizações concentram seus esforços para mitigar e/ou previnir os ataques de engenharia social: fator individual, fator organizacional e fator tecnológico (POLLINI *et al.*, 2021).

1) O fator individual

Com base em estudos, pesquisas e relatórios amplamente divulgados anualmente referentes às principais ameaças cibernética, a empresa de segurança Fortinet disponibilizou em sua página o Relatório do Cenário Global de Ameaças 2023

apontando que as tentativas de *phishing* e as técnicas sofisticadas que evitam a detecção, combinadas com o grande volume de SPAM recebido diariamente, alertam as organizações sobre a segurança de e-mail como sendo ainda um problema em sua estratégia cibernética (FORTINET, 2023).

Nesse contexto, o fator individual, algumas vezes, torna-se um ponto vulnerável na segurança cibernética de diversas organizações. Embora as medidas técnicas e os controles de segurança empregados sejam eficientes, para POLLINI *et al.* (2021) as ações comportamentais das pessoas têm um impacto significativo na eficácia geral e no fortalecimento da segurança cibernética de um sistema ou organização.

2) O fator organizacional

As organizações possuem políticas, processos e procedimentos formais para orientar os funcionários e manter o sistema seguro. É esperado que os funcionários sigam essas diretrizes; no entanto, estudos acadêmicos demonstraram que os procedimentos formais por si só não influenciaram o comportamento humano (POLLINI *et al.*, 2021 *apud* MAALEM *et al.*, 2020).

3) O fator tecnológico

A pesquisa aponta que as organizações estão aumentando seus esforços para se proteger e investindo em recursos tecnológicos que podem mitigar uma variedade de ameaças cibernéticas conhecidas. (AHSAN et al., 2022)

Levando isso em consideração, foram empregados inúmeros artefatos autênticos e recursos cuidadosamente selecionados, a fim de parecerem legítimos tanto para as pessoas quanto para os sistemas de segurança do instituto de pesquisa alvo. O objetivo foi ilustrar, por uma perspectiva mal-intencionada, por outro lado, como os atacantes estão aprimorando suas técnicas para contornar as defesas e explorar vulnerabilidades, enfatizando a importância de uma postura proativa na proteção contra ameaças cibernéticas.

2.3 ATAQUES DE PHISHING EM AMBIENTES INDUSTRIAIS

2.3.1 Conceitos e técnicas de ataques de *phishing*

Segundo a pesquisa de Aldawood e Skinner (2019), os ataques de *phishing* visam roubar ou danificar dados confidenciais enganando as pessoas para que revelem informações pessoais, como senhas e números de cartão de crédito. Servem ainda para desferir outros ataques sofisticados, através desse acesso inicial pelos colaboradores de uma empresa. A infraestrutura poderá ser comprometida caso não esteja protegida corretamente contra essas ameaças.

Com a modernização dos ataques de *phishing*, houve a necessidade por parte dos *hackers* modificarem suas formas de ações ofensivas. Com relação a isso, surgiram os ataques de *spear phishing* que são mais sofisticados do que os ataques de *phishing* comuns, conforme destaca QUINTERO-BONILLA e ANGEL (2020), pois usam informações personalizadas sobre o alvo pretendido e apresentam um desafio maior para a detecção, tanto pelas vítimas em potencial quanto pelos filtros de *phishing* de e-mail da organização (HALEVI, 2015).

Os criminosos digitais que realizam o *spear phishing* fazem uma pesquisa minuciosa sobre suas vítimas em potencial, vasculhando e coletando informações pessoais e das organizações com detalhes específicos sobre suas atividades online, como apontado no estudo de Alshamrani (2019). Essas informações são usadas para criar e-mails, domínios, sites, contextos e histórias aparentemente reais. Devido ao seu grau de direcionamento na comunicação, faz parecerem legítimos e confiáveis, muitas vezes se passando por uma pessoa ou organização conhecida pela vítima.

É relevante destacar que, de acordo com Chen et al. (2014) e outros estudos, HEJASE *et al*. (2020), RASTENIS *et al*.(2020) e ALKHALIL *et al.* (2021), observa-se que os ataques avançados de *phishing* frequentemente são estruturados em fases, conforme representado na Figura 1. Nesse contexto, podemos observar que as etapas planejadas são claramente definidas, empregando técnicas furtivas e evasivas, o que muitas vezes torna esse tipo de ataque indetectável, mesmo após a concretização de suas ações no alvo (CHEN *et al.,* 2014).

1. Identificação do alvo
2. Criação do ambiente
3. Armando a isca

4. Exploração da falha humana
5. Exploração dos recursos tecnológicos
6. Concretização do ataque

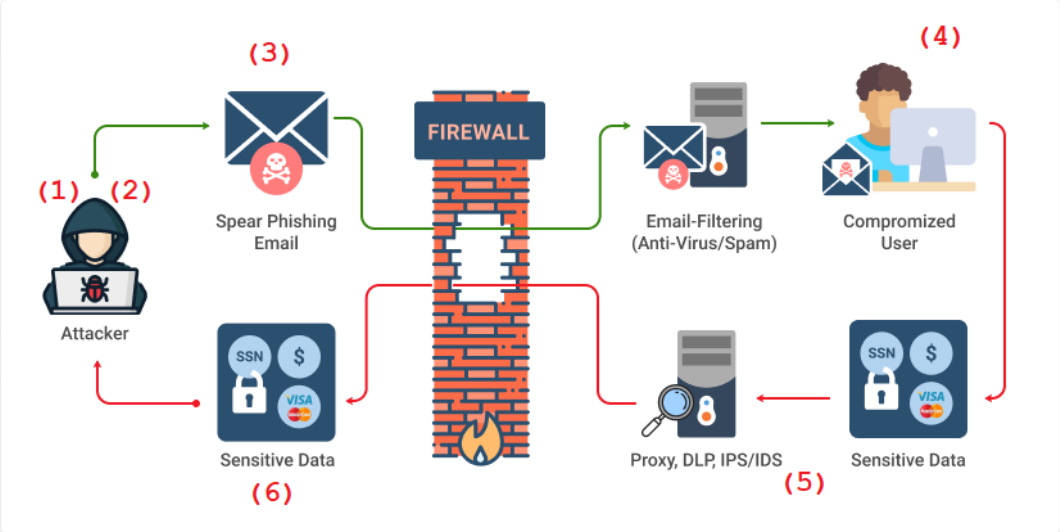


Figura 1: Fases de um ataque de *phishing*
Fonte: Site MSP360[4]

De acordo com a empresa Knowb4 (2023), maior plataforma de treinamento, conscientização em segurança e simulação de *phishing* do mundo, os humanos são hackeados por um conjunto de fatores que dependem do contexto em que as pessoas se encontram envolvidas e o seu estado emocional. Na maioria das vezes essas vítimas caem em golpes pelo fato de as mensagens passarem características de urgência, medo, desespero, curiosidade, simpatia e confiança.

Dentre elas, a mais preocupante são aquelas mensagens que passam confiança, uma vez que os cibercriminosos tentam coletar o máximo de informações sobre os alvos, a fim de parecerem legítimos e convincentes (RASTENIS, 2020). No caso de *spear phishing*, esses criminosos digitais criam mensagens personalizadas que aumentam a probabilidade de engajamento e induzem os alvos a divulgarem informações confidenciais, realizar ações maliciosas ou comprometer a segurança de seus sistemas e redes (EFTIMIE et al., 2022).

[4] Disponível em: <https://www.msp360.com/resources/blog/types-of-phishing/>. Acesso em: 23 jun 2023

2.3.2 Cuidados que devem ser tomados para evitar ataques de *Phishing*

De acordo com FAN (2017), para se proteger contra as ameaças que envolvam a engenharia social e os ataques de *phishing*, é importante seguir algumas práticas recomendadas:

- ficar atento a e-mails ou mensagens suspeitas, especialmente se solicitarem informações pessoais ou financeiras,
- certificar cuidadosamente o remetente de um e-mail, procurando por erros de ortografia ou endereços de e-mail estranhos.
- evitar clicar em links ou baixar anexos de fontes desconhecidas ou suspeitas que estejam inseridas no corpo desses e-mails e sempre que possível inspecionar as URLs antes de clicar.
- verificar a autenticidade de sites acessando-os diretamente pelo navegador, em vez de clicar em links contidos nos e-mails e sempre desconfiar de páginas de empresas conhecidas que não tenham um certificado digital válido para acesso HTTPS.
- manter o software de antivírus e os sistemas operacionais atualizados, pois as atualizações geralmente contêm correções de segurança importantes.
- utilizar autenticação em dois fatores sempre que possível, para adicionar uma camada extra de segurança às contas online.

De acordo com Branquinho (2021), os riscos associados à engenharia social em instalações críticas podem ser mitigados investindo em conscientização e treinamento dos funcionários. A implementação de políticas de segurança robustas, adoção de medidas de autenticação multifator (MFA), bem como a realização constante de monitoramento e auditorias sobre atividades suspeitas fazem parte deste escopo de medidas protetivas.

Para empresas e órgãos de médio e grande porte, é fundamental manter uma estrutura centralizada de operações de segurança (SOC – *Security Operation Center*) em funcionamento 24/7/365 que compreenda o ambiente de Tecnologia da Informação e Tecnologia Operacional (BRANQUINHO, 2021). Também é fundamental implementar um ambiente que seja constituído de ferramentas de gerenciamento de eventos e informações de segurança - SIEM (*Security Information Events*

Management), para prover a aplicação de políticas de segurança de forma global em toda a infraestrutura, compreendendo os dispositivos físicos, canais de comunicação, ativos de software e condutas humanas no ambiente (PODZINS; ROMANOVS, 2019).

2.3.3 Ataques de *spear phishing* (*phishing* direcionados)

Nesta seção, são apresentadas duas plataformas para identificar ataques direcionados de *phishing* ocorridos em ambiente de IC (infraestruturas críticas).

Segundo o estudo de Chiew *et al*. (2018), o *spear-phishing* representa uma ameaça crescente para os funcionários de uma organização, devido à sua precisão na seleção de alvos. Nesse tipo de ataque, os invasores pesquisam informações publicamente disponíveis sobre a empresa e perfis de redes sociais para obter detalhes precisos sobre a vítima-alvo (KROMBHOLZ et al., 2015).

Com base nessas informações, os atacantes constroem e-mails personalizados para ganhar a confiança das vítimas. Esses e-mails, normalmente são enviados para um grupo seleto de indivíduos e podem conter anexos maliciosos contendo software que permite ao atacante obter o controle remoto sobre o sistema da vítima, como verificado no estudo de Chiew *et al*. (2018).

Por meio dessa exploração, os invasores conseguem acessar informações sensíveis e a rede interna da empresa. As plataformas (RISI e HUB TI SAFE) disponibilizam acesso a banco de dados para pesquisar sobre incidentes cibernéticos ocorridos em ambientes industriais no Brasil e no mundo, dentre eles podem ser verificados alguns casos concretos de *spear-phishing* em cenários reais e os efeitos decorrentes desses ataques.

RISI Online Incidente Database

O RISI é um Repositório de Incidentes de Segurança Industrial (Figura 1) disponível para acesso no site < https://www.risidata.com/ >, possui um banco de dados de incidentes de natureza de cibersegurança que afetam (ou poderiam afetar) sistemas de controle de processos, automação industrial ou sistemas de controle de supervisão e aquisição de dados (SCADA).

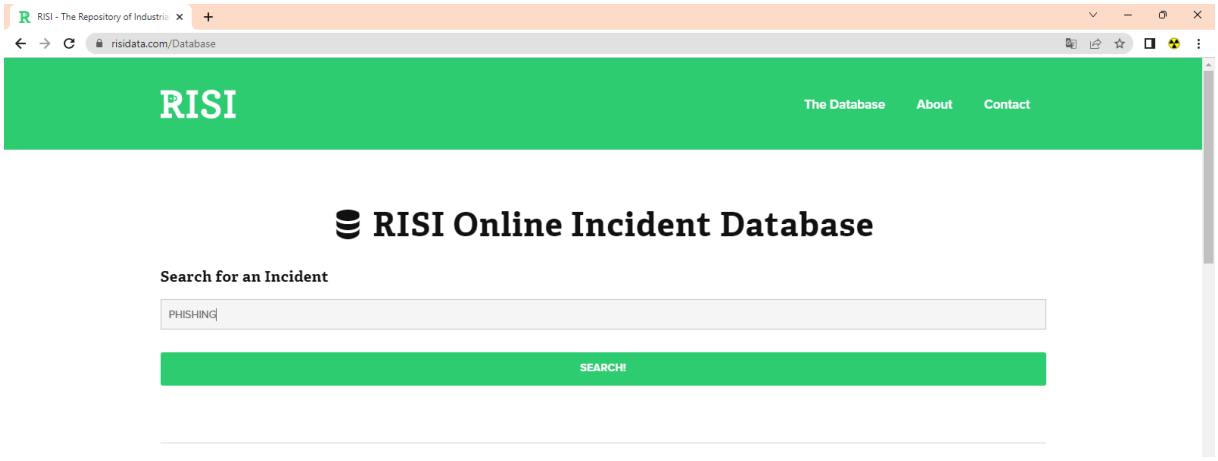


Figura 2: Captura de tela do site RISIDATA

Fonte: https://www.risidata.com/, acesso em 03 jul 2023.

TI Safe Incidente HUB

O portal da TI Safe apresenta um banco de dados de incidentes de segurança cibernética industrial (Figura 3) e está disponível para acesso no site < https://hub.tisafe.com/ >

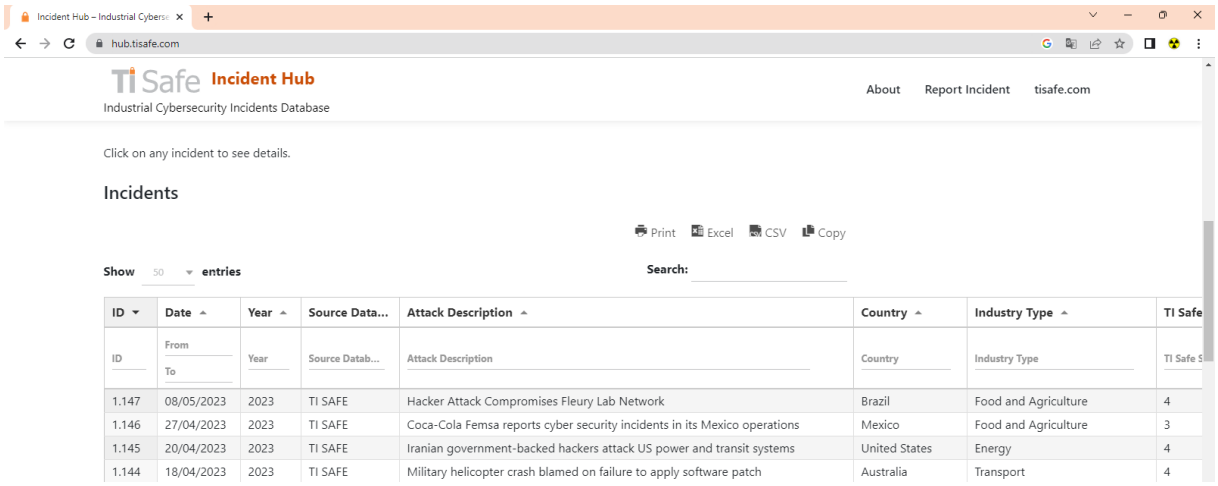


Figura 3: Captura de tela do site Hub TI Safe

Fonte: https://hub.tisafe.com/, acesso em 3 jul 2023.

2.3.4 Estruturação e compreensão de ataques, mapeamento de defesas e exercício cibernético

2.3.4.1 Conceitos relacionados

No presente momento, os ataques cibernéticos evoluíram em termos de suas estratégias e alvos, sendo reconhecidos como APT (Ameaças Persistentes Avançadas). Esse tipo de ataque utiliza técnicas de invasão sofisticada para evitar que seja detectado, relata Wrightson (2015). O objetivo é ter acesso à rede alvo e permanecer nela por muito tempo pesquisando e planejando como extrair com o máximo de informações do alvo. Esses ataques comumente utilizam uma combinação de *malware*, *ransomware*, *trojans*, técnicas de *spoofing* e estratégias de engenharia social, visando a invasão bem-sucedida dos sistemas (WRIGHTSON, 2015).

O Cyber Kill Chain é uma metodologia que descreve as etapas sequenciais pelas quais um atacante cibernético geralmente passa durante um ataque. Desde o reconhecimento inicial até a realização do objetivo final (AHMED, 2021). Essa sequência fornece uma visão abrangente das atividades realizadas pelo atacante ao longo de um ataque. Compreender essas etapas é fundamental para antecipar e interromper as ações maliciosas antes que elas causem danos significativos para as organizações (LOCKHED MARTIN).

Já o framework MITRE ATT&CK (*Adversarial Tactics, Techniques, and Common Knowledge*) oferece um catálogo de táticas e técnicas usadas pelos atacantes em cada fase do ataque. Ele fornece uma estrutura detalhada para entender como os adversários realizam suas atividades maliciosas, permitindo assim o desenvolvimento de contramedidas mais eficazes.

2.3.4.2 O *framework* MITRE ATT&CK

O MITRE ATT&CK possui atualmente 14 táticas. As táticas representam o porquê de uma técnica ou subtécnica ATT&CK. Representa o objetivo tático do adversário, ou seja, o motivo para realizar uma ação. Na Tabela 3, estão dispostas as táticas da matriz *enterprise* do Mitre.

Tabela 3: Etapas do MITRE ATT&CK

Tática	Descrição
Reconhecimento	Coleta de informações da organização alvo para preparar futuras atividades adversárias
Desenvolvimento de Recursos	Aquisição de infraestrutura e recursos para apoiar atividades adversárias contra a organização-alvo.
Acesso inicial	Obter acesso inicial à rede de destino
Execução	Técnicas para executar códigos maliciosos na rede, geralmente para explorar ou roubar dados
Persistência	Manter o acesso à rede de destino ao longo do tempo contornando medidas como alterações de credenciais ou reinicializações que podem interromper o acesso
Escalação de privilégios	Obter permissões de administrador ou outras permissões de alto nível na rede de destino.
Evasão de defesa	Evitar a detecção por software de segurança e equipes de segurança de TI.
Acesso a credenciais	Roubar nomes de contas e senhas, permitindo que o adversário contorne as medidas de segurança acessando a rede com credenciais legítimas.
Descoberta	Explorar a rede e coletar informações, como quais aplicativos e serviços estão em execução, quais contas existem, quais recursos estão disponíveis, etc.
Movimento Lateral	Acessar e controlar serviços remotos na rede de destino.
Coleta	Agregar dados de uma variedade de fontes na rede de destino.
Comando e Controle	Técnicas para comunicação com sistemas sob controle do adversário dentro da rede alvo.
Exfiltração	Técnicas para roubar dados da rede de destino e transferi-los para um servidor externo controlado pelo adversário.
Impacto	Técnicas para destruir dados ou interromper a disponibilidade de aplicativos, serviços ou a própria rede de destino.

O MITRE é dividido em matrizes. No site da ferramenta <https://attack.mitre.org> é possível verificar a presença das matrizes Enterprise, Mobile e a recentemente incorporada à matriz ICS (*Industrial Control System*). As técnicas do MITRE são os blocos de construção da estrutura MITRE ATT&CK. Elas representam como um adversário atinge um objetivo tático realizando uma ação. No momento deste trabalho, a estrutura contém informações sobre **196 técnicas** e **411 subtécnicas** distintas.

A Figura 4 apresenta a estrutura exemplificada de uma técnica, que inclui:

- A **descrição** da técnica.
- Lista de **subtécnicas** relacionadas à técnica.
- Lista de métodos de **mitigação** conhecidos para a técnica.
- Lista de métodos de **detecção** conhecidos para a técnica.
- Alguns **metadados** relacionados à técnica.
- **Referências** e recursos adicionais relacionados à técnica.

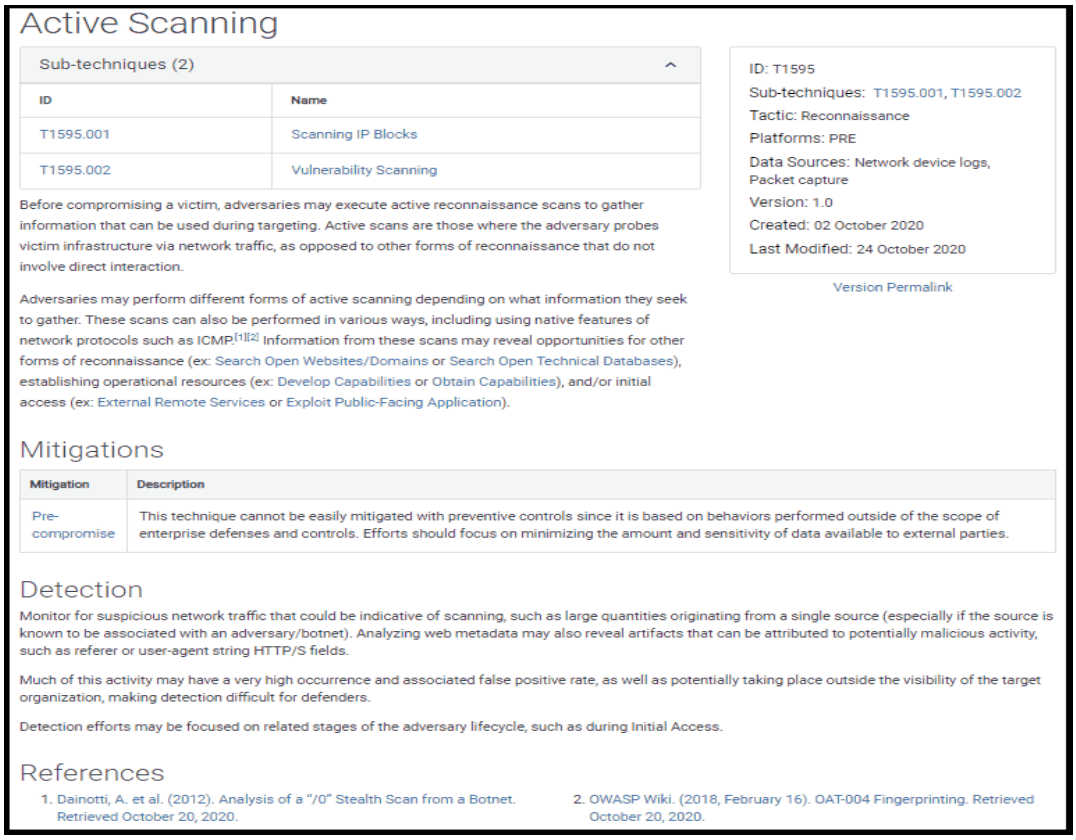


Figura 4: Representação de uma técnica encontrada no MITRE ATT&CK
Fonte: Site MITRE ATT&CK[5]

[5] Disponível em: <https://attack.mitre.org/>. Acesso em: 20 jun 2023

O *framework* pode ser utilizado para exemplificar, categorizar, entender e sugerir melhorias para os eventos que envolvam incidentes cibernéticos que possam afetar uma infraestrutura nuclear.

De modo que, quando uma atividade suspeita for detectada no ambiente, haverá a possibilidade de responder às seguintes perguntas:

1) Qual foi o objetivo geral ou objetivo (tática) do comportamento?
2) Que método foi usado (técnica) para tentar atingir o objetivo?

Dessa forma, os profissionais de segurança cibernética poderão correlacionar as atividades suspeitas com grupos de ameaças ou softwares conhecidos e identificar formas de encerrar o ataque.

2.3.4.3 A metodologia do Cyber Kill Chain

O método Cyber Kill Chain, também conhecido como cadeia de ataque, pode ser aplicado durante a realização de testes de intrusão (*pentest*). Segundo o estudo de Ahmed (2021), ao demonstrar como possíveis atacantes se movimentam através de redes para identificar vulnerabilidades que possam ser exploradas, é possível estruturar efetivamente as defesas de uma organização e implementar contramedidas adequadas em cada etapa da cadeia. Essa cadeia de ataque é composta pelas etapas a seguir, de acordo com a Tabela 4:

Tabela 4: Descrição das etapas do modelo Cyber Kill Chain

Etapa	Nome	Descrição
1ª etapa	**Reconhecimento**	Coleta e compilação de informações. A adoção de práticas de higiene de segurança cibernética é necessária para prevenir essa etapa.
2ª etapa	**Armamento**	Fase em que o invasor cria o ataque, geralmente com poucos controles de segurança que possam impactar essa etapa.

3ª etapa	**Entrega**	Refere-se aos vetores de ataque utilizados para entregar cargas maliciosas. Geralmente e-mail e USB.
4ª etapa	**Exploração**	Direcionada às vulnerabilidades de um sistema operacional ou aplicação. Nessa etapa, o ataque é executado, destacando a importância de manter sistemas atualizados e proteções ativas.
5ª etapa	**Instalação**	Momento em que o invasor instala o malware no alvo.
6ª etapa	**Controle e comando**	O invasor obtém controle manual sobre o sistema comprometido.
7ª etapa	**Ações no objetivo**	Com acesso e controle dentro da rede alvo, o atacante pode executar seus objetivos, como extração de dados e informações.

2.3.4.4 Comparativos entre os *frameworks*

A Tabela 5 ilustra um comparativo entre as etapas existentes nos dois *frameworks.*

Tabela 5: Cyber Kill Chain versus Mitre ATT&CT

CYBER KILL CHAIN	MITRE ATT&CK
● Reconhecimento ● Armamento ● Entrega ● Exploração ● Instalação ● Comando e controle ● Ações no objetivo	● Reconhecimento ● Desenvolvimento de Recursos ● Acesso inicial ● Execução ● Persistência ● Escalação de privilégios ● Evasão de defesa ● Acesso a credenciais ● Descoberta ● Movimento Lateral ● Coleta ● Comando e Controle ● Exfiltração ● Impacto

2.3.5 Exercício Guardião Cibernético

O Exercício Guardião Cibernético 4.0 é um evento de destaque na área de defesa cibernética no hemisfério sul, organizado pelo Comando de Defesa Cibernética do Exército. Com mais de 120 participantes de organizações públicas e privadas, o exercício ocorre em uma plataforma virtual e envolve simulações de crises em tempo real. Ele inclui quatro áreas principais de ação, como Simulação Construtiva, Simulação Virtual, Palestras de Conscientização e Grupos de Estudos, juntamente com um desafio CTF (Capture The Flag). (GSI, 2022)

Empresas renomadas, como Cisco, Claro e Kryptus, juntamente com instituições como a Comissão Nacional de Energia Nuclear (CNEN), participaram do exercício, que teve sua sede em Brasília e um hub adicional em São Paulo. As simulações empregam um Simulador de Operações Cibernéticas e gabinetes de crise para abordar eventos cibernéticos, exigindo ações em níveis decisórios e técnicos para enfrentar ameaças cibernéticas em constante evolução (CISO Advisor, 2022).

2.4 ETAPAS DO ATAQUE CIBERNÉTICO UTILIZANDO O MODELO CYBER KILL CHAIN

Existem diversas técnicas de ataques e formas de defesa em segurança cibernética, conforme já mencionado nesta pesquisa. Adicionalmente, é importante ressaltar que este trabalho não se concentra apenas nas medidas ofensivas utilizadas para mitigar ataques cibernéticos como veremos. É fundamental estarmos alinhados sobre as últimas ameaças e seguir as melhores práticas de defesa cibernética para garantir a proteção adequada dos sistemas e dados, conforme mencionado por CHEN *et al (*2014).

Considerando isso, optou-se no Capítulo 3 IMPLEMENTAÇÃO DO ESTUDO DE CASO, explorar a anatomia de um ataque cibernético utilizando o *framework* **Cyber Kill Chain (CKC)** de forma simulada e em ambiente controlado.

Por meio da exploração da anatomia dos ataques cibernéticos, utilizando essa metodologia, espera-se contribuir para o campo da segurança cibernética.

Conforme ilustrado na Figura 5, é possível obter uma visão mais abrangente e prática que auxilie na compreensão dos ataques cibernéticos e no desenvolvimento de estratégias eficazes de defesa.

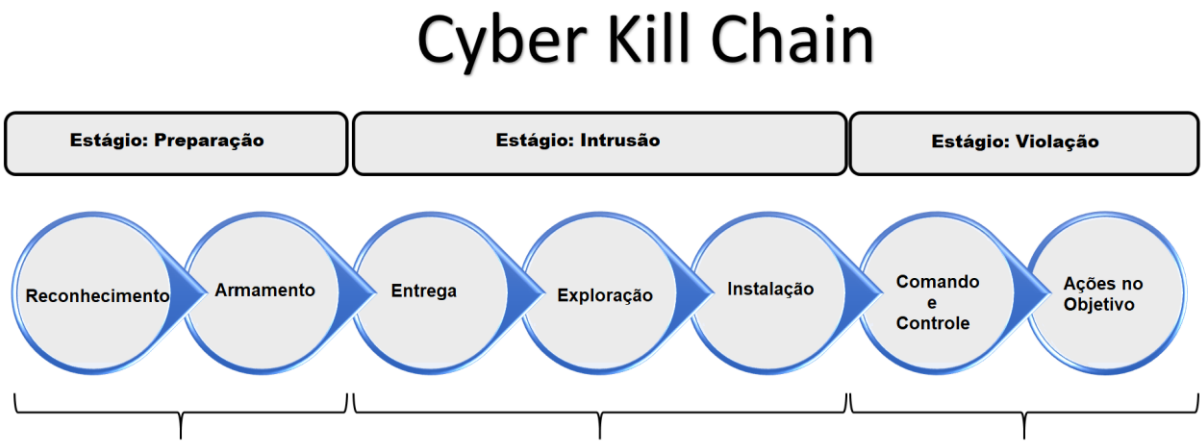


Figura 5: Estágios e etapas do Cyber Kill Chain
Fonte: Adaptada de <https://learning.oreilly.com>

A seguir, serão destacadas as técnicas e conceitos relacionados a cada etapa do modelo Cyber Kill Chain que serão aplicados na execução do estudo de caso:

1. Reconhecimento (Reconnaissance): Será fundamentado na realização de uma pesquisa detalhada sobre o alvo, utilizando técnicas de engenharia social e coleta de informações que serão empregadas por cibercriminosos. O objetivo será obter o máximo de endereços de e-mails válidos da organização alvo para subsidiar os ataques simulados de *phishing*.

2. Armamento (Weaponization): Será fundamentado na realização de pesquisas, testes e implementações de ferramentas e técnicas reais que poderão subsidiar o ataque simulado ao instituto de pesquisa. Essa etapa envolverá a preparação dos recursos necessários para a realização das outras etapas, como software de simulação, scripts, criação de sites, domínios e e-mails corporativos fictícios, dentre outros recursos.

3. Entrega (Delivery): Será utilizada a técnica de engenharia social para validar a ação no alvo pretendido. Nesse cenário, serão enviados e-mails de *phishing*, com o objetivo de persuadir os funcionários daquela instituição para interagirem com o conteúdo e links disponibilizados no e-mail. Essa etapa, no presente estudo, possibilitará avaliar a capacidade de discernimento do fator humano em relação à

engenharia social, bem como a eficácia das medidas de segurança cibernética implementadas no instituto de pesquisa testado (YADAV; RAO, 2015).

4. Exploração (Exploitation): Será fundamentado na realização de investigações em busca de informações que serão úteis para a exploração de vulnerabilidades técnicas na infraestrutura alvo, com base nas tecnologias identificadas nesta etapa. Isso envolverá a análise dos sistemas operacionais, das redes e dos serviços em busca de possíveis brechas de segurança que poderão ser exploradas (YADAV; RAO, 2015). Um dos objetivos dessa fase será explorar no instituto alvo as estratégias para contornar as defesas existentes, como firewalls, antivírus e políticas de segurança (MITRE, 2018). Um ataque simulado desse tipo buscará encontrar vulnerabilidades nos sistemas, utilizar técnicas de engenharia social e aproveitar-se de falhas na configuração para prosseguir para a próxima etapa: instalação do malware.

5. Instalação (Installation): Essa etapa envolverá a busca de meios para realização da instalação de um agente (malware simulado) nos computadores das “vítimas” (funcionários do instituto). De forma análoga, terá o objetivo de (1) identificar quais medidas protetivas estão sendo implementadas na organização para prevenir a instalação de softwares maliciosos e (2) identificar se existem vulnerabilidades e fraquezas presentes naquela infraestrutura que permitam a execução desses códigos. O objetivo principal dessa etapa será estabelecer uma presença persistente nos alvos comprometidos, permitindo aos invasores manterem o acesso e realizarem atividades fraudulentas sem serem detectados (YADAV; RAO, 2015).

6. Comando e Controle (Command and Control): Após a etapa de instalação, a fase de comando e controle terá o objetivo de implementar um servidor C2 (Command and Control) com a finalidade de estabelecer uma comunicação segura e oculta entre os agentes maliciosos instalados nos computadores das vítimas e do invasor (YADAV; RAO, 2015). O servidor de comando e controle que será implementado para esta atividade desempenhará um papel importante como uma central de comando, permitindo a realização de comandos simulados e ações que evidenciarão como os invasores gerenciam e controlam as atividades dos agentes maliciosos de forma remota (CHEN et al., 2014).

Através dessa comunicação, os invasores terão a capacidade de enviar comandos, receber informações e coletar dados dos sistemas comprometidos (MITRE, 2018). Essa técnica será ilustrada no Capítulo 3. É necessário enfatizar que o modelo de C2 adotado nesta dissertação será desenvolvido com base no comando e controle construído durante o treinamento de Evasão de Defesas fornecido pela empresa de tecnologia DESEC Information Security (DESEC, 2023).

7. Ações no objetivo: Essa fase consistirá na realização simulada da coleta de dados e informações sensíveis durante um ataque, bem como na verificação de vulnerabilidades em um sistema de simulação, além do processo de exfiltração desses dados conduzidos pelos adversários (YADAV; RAO, 2015). Durante o ataque cibernético, o atacante poderá explorar sistemas operacionais Windows e Linux. Em ambientes controlados e de testes, poderão ser realizados os procedimentos que um atacante real faria em uma infraestrutura crítica caso conseguisse consolidar todas as fases anteriores deste ataque.

O teste para essa etapa buscará, de forma ética, extrair informações valiosas, como dados pessoais, credenciais de acesso, vulnerabilidades em sistemas, propriedade intelectual e outras informações estratégicas (ASSANT; LEE, 2015). Após a coleta desses dados, os adversários tentarão realizar o processo de exfiltração, que consistirá na transferência dos dados comprometidos de volta para sua infraestrutura de controle (ASSANT; LEE, 2015). Eles utilizarão técnicas de ocultação e criptografia para evitar detecção durante a transferência, garantindo que as informações sejam transmitidas com segurança e sem levantar suspeitas (TARNOWSKI, 2017).

Por fim, de acordo com Tarnowski (2017), é importante destacar que o modelo Cyber Kill Chain fornecerá uma estrutura para entender e prevenir intrusões em redes e sistemas. As etapas descritas, desde o reconhecimento até as ações no objetivo, representarão o processo pelo qual os adversários costumam passar para atingir seus objetivos maliciosos (YADAV; RAO, 2015).

2.5 NORMAS E REGULAÇÕES APLICÁVEIS AO SETOR NUCLEAR

Durante o desenvolvimento desta dissertação, a norma **CNEN NN 2.07 ("Segurança Cibernética de Instalações Nucleares")** encontrava-se em processo de criação. Atualmente, o setor nuclear brasileiro apresenta uma lacuna regulatória, uma vez que ainda não foi publicado um instrumento normativo que exija dos operadores nucleares a responsabilidade de garantir a segurança cibernética de seus recursos tecnológicos.

Em um contexto internacional existem normas, regulamentações e recomendações de grande importância que podem ser adaptadas para atender às necessidades específicas do setor nuclear brasileiro. Além disso, no Brasil existem leis e normativos técnicos que tratam do assunto segurança cibernética (ABNT NBR). A seguir, são destacadas algumas referências relacionadas ao tema, porém não se limitam ao conteúdo abordado nesta seção:

2.4.1 Normas, regulamentações, recomendações e órgãos internacionais

IAEA Nº 42

A norma IAEA No. 42 é uma diretriz publicada pela Agência Internacional de Energia Atômica (IAEA) que trata da segurança cibernética em instalações nucleares. O documento aborda questões como identificação e avaliação de vulnerabilidades, implementação de medidas de proteção cibernética, resposta a incidentes e gestão de riscos relacionados à segurança cibernética. Seu objetivo é promover a segurança dos sistemas nucleares diante das ameaças cibernéticas.

IAEA Nº 17-T (Rev. 1)

O objetivo desta publicação, segundo informações contidas na documentação, é auxiliar os Estados Membros na implementação da segurança cibernética em instalações nucleares, visando prevenir e proteger contra a remoção não autorizada de material nuclear, sabotagem de instalações nucleares e acesso não autorizado a informações nucleares sensíveis. Esta publicação aborda a segurança cibernética para atividades e organizações de apoio, como fornecedores e empreiteiros. Embora o foco desta publicação seja a segurança das instalações nucleares, a aplicação

destas orientações também pode beneficiar a segurança e o desempenho operacional das instalações.

NRC RG 5.71

O NRC Regulatory Guide 5.71 é um documento regulatório publicado em 2010, pela Comissão Reguladora Nuclear dos Estados Unidos (NRC) que fornece orientações sobre programas de segurança cibernética para usinas nucleares. Este guia (RG 5.71) descreve os requisitos regulatórios e as práticas recomendadas para estabelecer e manter medidas eficazes de segurança cibernética para proteger ativos e sistemas digitais críticos em usinas nucleares. O objetivo do NRC Regulatory Guide 5.71, segundo informações contidas na documentação, é auxiliar os operadores de usinas nucleares a desenvolverem programas robustos de segurança cibernética que abordam os riscos e desafios únicos associados à infraestrutura digital das instalações nucleares.

NIST 800-82 Ver2

A norma NIST SP 800-82 é uma publicação do Instituto Nacional de Padrões e Tecnologia dos Estados Unidos (NIST) que trata da segurança cibernética de sistemas industriais de controle. De acordo com a NIST 800-82 v2, o objetivo é fornecer diretrizes e recomendações para proteger os sistemas de controle utilizados em infraestruturas críticas, como redes elétricas, sistemas de água, transporte e manufatura, contra ameaças cibernéticas. Ela aborda áreas como a segmentação de redes, autenticação e controle de acesso, monitoramento de sistemas, detecção e resposta a incidentes, e gestão de mudanças. O objetivo da norma NIST SP 800-82, conforme descrito na documentação, é melhorar a segurança dos sistemas de controle industrial, reduzindo os riscos de ataques cibernéticos e minimizando o impacto desses ataques nas operações críticas.

ISA/IEC 62443

A norma ISA/IEC 62443 é uma série de normas internacionais desenvolvida pela Sociedade Internacional de Automação (ISA) e pela Comissão Eletrotécnica Internacional (IEC) que aborda a segurança cibernética de sistemas de automação e controle industrial. O objetivo dessas normas, conforme descrito na documentação, é fornecer um *framework* abrangente para a implementação de medidas de segurança

cibernética em sistemas de automação industrial, contribuindo para a proteção das infraestruturas críticas e a continuidade das operações industriais.

2.4.2 Legislações e normas brasileiras

Decreto Nº 10.748/2021 (Rede Federal De Gestão De Incidentes Cibernéticos)

O Decreto Nº 10.748, de 16 de julho de 2021, institui a Rede Federal de Gestão de Incidentes Cibernéticos no Brasil. Esta rede é composta por órgãos governamentais da administração pública federal direta, autárquica e fundacional, bem como por empresas públicas e sociedades de economia mista que optarem por aderir a ela (BRASIL, 2021).

O objetivo principal da Rede Federal de Gestão de Incidentes Cibernéticos, segundo o Decreto Nº 10.74, é melhorar a coordenação entre esses órgãos e entidades para prevenir, tratar e responder a incidentes cibernéticos, aumentando a resiliência da segurança cibernética de seus ativos de informação. Para alcançar esse propósito, a rede visa divulgar medidas de prevenção, compartilhar alertas sobre ameaças cibernéticas, promover a cooperação entre os participantes e agilizar as respostas a incidentes cibernéticos (BRASIL, 2021).

Conforme descrito no Decreto Nº 10.748, o Gabinete de Segurança Institucional da Presidência da República (GSI) é o responsável por coordenar essa rede, convocando reuniões em casos de incidentes cibernéticos graves ou alto risco cibernético. Outros órgãos, como agências reguladoras e a Comissão Nacional de Energia Nuclear (CNEN), possuem funções específicas na rede (BRASIL, 2021).

As normas ABNT NBR ISO/IEC 27000 referem-se a uma série de normas brasileiras que adotam e adaptam as normas internacionais ISO/IEC 27000 relacionadas à segurança da informação. Embora as normas ABNT NBR ISO/IEC 27000 sejam amplamente baseadas nas normas internacionais ISO/IEC, elas podem conter modificações e adições específicas para se adequar ao cenário brasileiro de segurança cibernética. A seguir, destacamos algumas das principais normas e legislações brasileiras que podem ser utilizadas no setor nuclear brasileiro, conforme a necessidade:

ABNT NBR ISO/IEC 27001:2022 - Segurança da informação, segurança cibernética e proteção à privacidade – Sistema de gestão de segurança da informação – Requisitos

A norma 27001 foi elaborada para prover os requisitos para estabelecer, implementar, manter e melhorar um sistema de gestão de segurança da informação. De acordo com a norma 27001, são incluídos os requisitos para avaliar e tratar os riscos de segurança da informação voltados para as necessidades da organização. Em seu Anexo A são encontrados os controles de segurança da informação, dentre eles: controles organizacionais, controle de pessoas, controles físicos e controles tecnológicos.

ABNT NBR ISO/IEC 27002:2022 - Segurança da informação, segurança cibernética e proteção à privacidade – Controles de segurança da informação.

A norma ABNT 27002 foi projetada para organizações de qualquer tamanho, podendo ser utilizado como referência para determinar e implementar controles para tratamento de riscos de segurança da informação em um SGSI (Sistema de Gestão de Segurança da Informação) com base na ABNT NBR ISO/IEC 27001. De acordo com a norma 27002, é destinada a ser utilizada no desenvolvimento de diretrizes de gestão de segurança da informação específicas para a indústria e a organização, a considerar o seu ambiente específico de riscos de segurança da informação.

ABNT NBR ISO/IEC 27701:2019 – Técnicas de segurança – Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade de informação – Requisitos e diretrizes

A norma ABNT 27701 especifica os requisitos e as diretrizes para o estabelecimento, implementação e melhoria contínua de um Sistema de Gestão de Privacidade da Informação (SGPI). De acordo com a referida norma 27701, é aplicável a todos os tipo e tamanhos de organizações, incluindo as companhias públicas e privadas, entidades governamentais e organizações sem fins lucrativos, que são controladoras de dados pessoais (DP) ou que são operadoras desses dados.

ABNT NBR ISO/IEC 27032:2015 – Tecnologia da Informação – Técnicas de segurança – Diretrizes para segurança cibernética

A norma ABNT 27032 fornece diretrizes para melhorar a estado de Segurança Cibernética, delineando os pontos típicos e outros domínios como segurança de rede, segurança de Internet e proteção da infraestrutura crítica de informação (CIIP – *Critical Information Infrastructure Protection*). A norma ABNT 27032 descreve que a falta de Segurança Cibernética pode causar um impacto negativo sobre a disponibilidade de sistemas críticos de infraestrutura de informação, proporcionados pelos fornecedores de infraestruturas críticas. A norma ainda cita que o conhecimento das fraquezas de infraestruturas críticas, caso não seja usado corretamente, pode haver uma implicação direta na segurança nacional.

ABNT NBR ISO/IEC 27037:2014 – Tecnologia da informação – Técnicas de segurança – Diretrizes para identificação, coleta, aquisição e preservação de evidência digital.

Essa norma está relacionada com as atividades relacionadas às evidências digitais que são a identificação, coleta, aquisição e preservação de evidência digital que possuam um valor de prova, que possam servir de evidências digitais em investigações forenses. De acordo com a norma 27037, é uma referência importante para profissionais de segurança da informação, investigadores forenses e outras partes envolvidas em atividades de resposta a incidentes e investigações relacionadas a evidências digitais.

ABNT NBR ISO/OEC 27035-3:2021 – Tecnologia da informação - Gestão de incidentes de segurança da informação Parte 3: Diretrizes para operações de resposta a incidentes de TIC

A norma 27035-3 aponta as principais fases para realização da gestão de incidentes de segurança da informação que consistem em:

- Planejamento e preparação
- Detecção e geração de relatórios
- Avaliação e decisão
- Respostas
- Lições aprendidas

As fases do processo de operação e resposta a incidentes, segundo a ABNT 27035-3, são compostas por operações para identificação de incidentes, avaliação e

qualificação de incidentes, coleta de inteligência de ameaças, contenção, erradicação e recuperação de incidentes, análise de incidentes e operações para geração de relatórios.

De acordo ainda com a ABNT 27035-3, os eventos de segurança cibernética podem ser detectados internamente por pessoas ou por meio tecnológicos, ou ainda, através de relatos de fontes externas. Desse modo, a classificação desses eventos pode advir dos meios técnicos, de pessoas e de organizações.

2.6 TRABALHOS RELACIONADOS

Como ficará evidente nesta seção, questões de cibersegurança do setor nuclear são consideradas importantes, sendo inclusive classificadas como questões de segurança nacional. A despeito disso, o número de trabalhos de estudo de casos de cibersegurança direcionados ao setor nuclear é baixo, o que reforça a importância do tema abordado nesta dissertação.

Em Greiman (2023), a autora realizou um estudo sobre o progresso da cibersegurança na indústria nuclear mundial. Sob este prisma, investigou-se, por meio de uma análise comparativa, os recentes regulamentos, normas, regras e padrões governamentais para segurança de cibersegurança nuclear nos Estados Unidos e internacionalmente para determinar se essas leis protegem adequadamente a infraestrutura de energia contra os ataques cibernéticos e responsabilizam as partes responsáveis. O referido trabalho está relacionado à pesquisa de literatura desta dissertação de mestrado, que inclui uma breve cobertura dos principais regulamentos e normas de cibersegurança relacionadas ao setor nuclear.

Em Almutairi e Alghamdi (2022), verificou-se, através de um questionário, o nível de conscientização da engenharia social, considerando diversos grupos populacionais. Entre os resultados alcançados, destaca-se a indicação de que as pessoas que têm o conhecimento prévio dos métodos de engenharia social têm melhor conhecimento sobre segurança da informação, e são menos propensas a serem vítimas deste tipo de ataque. A presente dissertação de mestrado se diferencia deste trabalho, pois efetivamente foram utilizadas as técnicas de engenharia social para que fosse possível mensurar a incidência de colaboradores suscetíveis a este tipo de ataque e, ao fim, fornecê-los uma cartilha customizada e direcionada aos

colaboradores da organização alvo, com o objetivo de promover maior conscientização sobre cibersegurança e engenharia social.

Em Aslan *et al.* (2010), os autores se concentraram na realização de um conjunto de testes de ataques baseados em técnicas de engenharia social direcionados à Nuclear Malásia. Os experimentos incluíram e-mails, *phishing* e páginas web com conteúdo malicioso. O objetivo era conscientizar as equipes da Nuclear Malaysia sobre o funcionamento dos métodos de engenharia social, bem como os respectivos métodos de prevenção.

As diferenças entre o trabalho de Aslan *et al.* (2010) e a presente dissertação de mestrado, destaca-se (1) Aslan *et al.* (2010) considera a suposição de que os hackers sabem sobre o cliente de e-mail nuclear da Malásia por meio de informações de funcionários como colegas próximos, ex-colegas de escritório, ex-colegas de escola e assim por diante.

Por outro lado, essa dissertação incluiu, na etapa de reconhecimento, a utilização de ferramentas disponíveis publicamente em fontes abertas de inteligência cibernética para a obtenção dos endereços de e-mail dos servidores da organização alvo. (2) Aslan *et al.* (2010) não englobou etapas posteriores típicas de um ataque mais elaborado, como exploração e comando & controle, enquanto nesta dissertação o faz.

Já em Peterson, Haney e Borrelli (2019), os autores se concentraram em revisar criticamente incidentes anteriores de vulnerabilidade cibernética em instalações nucleares e outras instalações críticas. Adicionalmente, analisou-se os desafios às vulnerabilidades no contexto da modernização da frota nuclear atual e propôs-se futuras direções de pesquisa necessárias para resolver esses problemas. O trabalho, portanto, descreve que:

> um primeiro esforço nesse caminho de pesquisa que se concentra em incidentes anteriores de cibersegurança em instalações nucleares para identificar semelhanças nesses incidentes e considerar como uma metodologia tradicional de avaliação de vulnerabilidade pode ser modificada ou aprimorada (PETERSON; HANEY; BORRELLI, 2019).

Ao contrário do que foi feito nesta dissertação de mestrado, o estudo realizado por Peterson, Haney e Borrelli (2019) não envolveu a realização de testes e experimentos que utilizassem tanto técnicas amplamente reconhecidas de invasão de sistemas quanto estratégias de engenharia social.

O trabalho desenvolvido em Rowland (2020) teve como objetivo fornecer evidências de que a importância e a urgência da conscientização sobre engenharia social, como complemento aos treinamentos técnicos em cibersegurança, são frequentemente subestimadas. Também foram fornecidas recomendações para a criação de um treinamento para orientar operadores de instalações nucleares, com assistência e cooperação internacional, para prover cibersegurança eficaz.

Ao comparar o trabalho desenvolvido por Rowland (2020), o presente trabalho identifica que o estudo de Rowland (2020) estaria mais relacionado à última etapa desta dissertação, disponibilizada através do APENDICE A, onde é apresentada uma cartilha customizada para a conscientização dos colaboradores da organização alvo do estudo visando mitigar sua suscetibilidade à esta categoria de técnicas de ataque.

No estudo apresentado em Sá (2020), o autor realizou uma revisão da literatura, baseando-se em ataques de engenharia social para o setor nuclear. Um dos objetivos verificados no trabalho de Sá (2020) foi compreender como a Central Nuclear Almirante Álvaro Alberto (CNAAA) trata as questões relacionadas à segurança cibernética como meio de mitigar ataques de engenharia social direcionados aos seus funcionários. O estudo de Sá (2020) tomou como base a realização de entrevistas com profissionais dos setores nuclear e cibernético, pesquisa na literatura especializada e consulta à Eletronuclear por meio da Lei de Acesso à Informação.

Essa dissertação apresentou uma perspectiva semelhante ao trabalho de Sá (2020); no entanto, buscou-se desenvolver uma hipótese de forma pragmática, ao realizar um ataque cibernético simulado em um instituto de pesquisa na área nuclear, utilizando a engenharia social como estratégia inicial, por meio do envio de e-mails de *phishing*.

Em seguida, neste trabalho, foram realizados procedimentos para verificar a resistência dos controles tecnológicos, por meio de técnicas de intrusão e avaliação de vulnerabilidades do ambiente. Um dos propósitos dessa dissertação é contribuir e sinalizar com correções e proteções baseados nas melhores práticas aplicadas à segurança cibernética no setor nuclear brasileiro, buscando fortalecer ainda mais a conscientização dos fatores humanos e a proteção dos sistemas.

3 IMPLEMENTAÇÃO DO ESTUDO DE CASO

Este capítulo tem por objetivo discorrer sobre a metodologia que foi utilizada neste trabalho.

O principal norte da metodologia empregada foi a de seguir de forma simulada, controlada, ética e com as devidas autorizações dos gestores da instituição, etapas típicas de um ataque cibernético direcionado a uma instituição de pesquisa da área nuclear.

Com efeito, como será detalhado neste capítulo, geram-se resultados que se dignam a motivar campanhas de conscientização nas instituições, colaborando para a redução de riscos ligados aos fatores humanos. Este é o caso do uso de técnicas de engenharia social por meio de e-mails *phishing*,

Outras etapas efetivamente mais técnicas, como detecção de vulnerabilidades em sistemas específicos, geram resultados proveitosos para que a instituição possa tomar ações de controle, correção e/ou contenção de riscos.

Espera-se, dessa forma, contribuir para a melhoria contínua dos processos que envolvem o tema segurança cibernética das instalações do setor nuclear.

Neste trabalho, as etapas de **Reconhecimento**, **Armamento**, **Entrega e Exploração** ilustradas na Figura 6 são efetivamente executadas.

Já as etapas de **Instalação, Controle e Comando, e Ações no Objetivo** são tratadas de maneira demonstrativa em um ambiente controlado e/ou simulado. Isso visa atingir o objetivo do trabalho com o cuidado da execução de experimentos e ensaios não destrutivos.

3.1 Etapas do ataque cibernético simulado utilizando o modelo Cyber Kill Chain

Vale ressaltar que serão cobertas as 07 (sete) etapas que compõem o modelo **Cyber Kill Chain,** evidenciando cada uma das fases em detalhes, de acordo com a Figura 6.

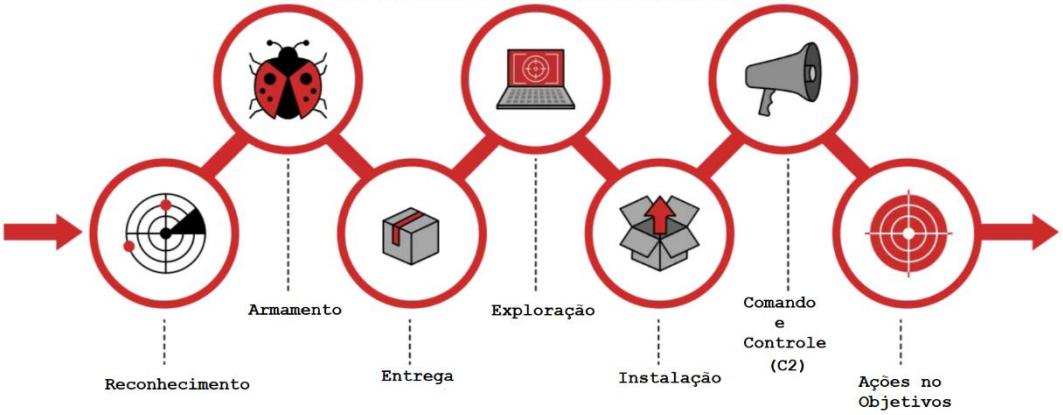


Figura 6: Etapas do modelo Cyber Kill Chain
Fonte: Adaptada de Site Medium[6]

3.1.1 Reconhecimento

Nessa etapa, conhecida também como a fase de ***information gathering*** (coleta de informações), foram reunidos endereços de e-mail sobre a instituição alvo. Para efetivação da coleta de informações, foram realizadas pesquisas utilizando os recursos contidos no *framework* OSINT (*Open Source Intelligence)*. Esse termo refere-se à coleta e análise de informações disponíveis publicamente, obtidas de fontes abertas, como sites, mídias sociais, fóruns, blogs, registros públicos e outras fontes de dados acessíveis ao público. Além disso, é importante destacar que este é atualmente um dos *frameworks* mais conhecidos para pesquisas digitais em fontes abertas. (OSINT Framework, 2023)

Como apresentado neste trabalho, a utilização de técnicas que envolvem OSINT, ainda que legítima, foi empregada como forma de obter os e-mails da organização alvo.

Dessa forma, a coleta de informações para reunir uma lista de endereços de e-mails foi empregada, por meio do uso de ferramentas de fontes abertas. Esse procedimento ilustra a ação de um atacante para efetivar seus objetivos maliciosos. Por outro lado, serve também para conscientizar e fortalecer as medidas de segurança cibernética, ajudando a identificar e mitigar possíveis vulnerabilidades em um sistema.

[6] Disponível em: <https://medium.com/@haircutfish>. Acesso em: 23 jun 2023

A Figura 7 ilustra a categorização de *frameworks* da base de dados abertos de inteligência disponibilizado pelo OSINT.

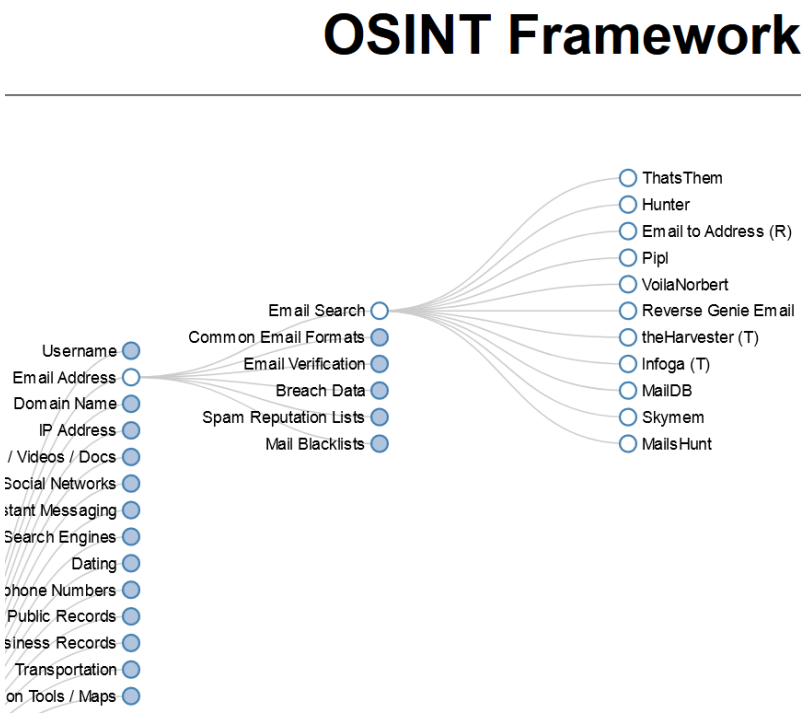


Figura 7: OSINT Framework
Fonte: Site OSINT[7]

Ao acessar o site OSINT *Framework*, disponível na URL de < https://osintframework.com/ >, este funciona como uma de árvore ramificada de categorias de fontes abertas de informações de inteligência. É possível escolher por uma categoria desejada e clicar até o recurso ou ferramenta desejada.

Com o objetivo de levantar os endereços de e-mail dos colaboradores da organização alvo deste trabalho, foi escolhida a opção "*Email Address*", em seguida "*Email Search*".

Dentre as opções de bases de endereços de e-mail disponíveis, a que retornou maior quantidade de endereços, considerando o domínio de Internet da organização alvo, foi a opção "*Skymem*", conforme ilustrado na Figura 8. Ao clicar em "*Find email addresses*", após o preenchimento do domínio, será apresentada a listagem dos endereços e-mails disponíveis.

[7] Disponível em: <https://osintframework.com/>. Acesso em: 15 mai 2023

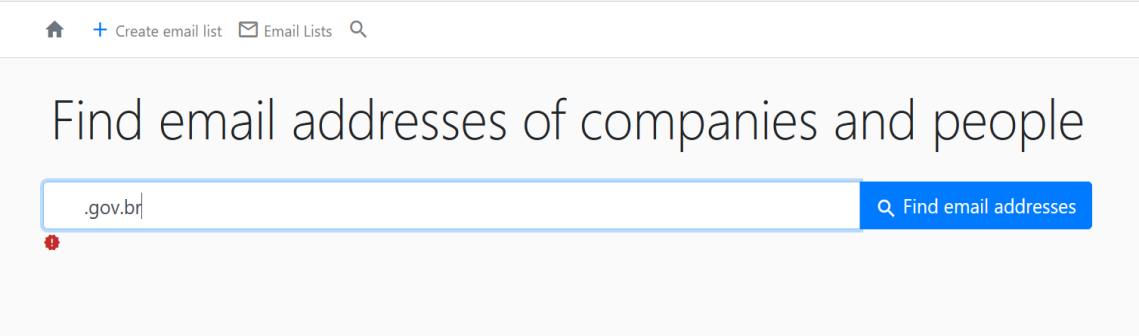


Figura 8: Encontrar e-mail de companhias e pessoas
Fonte: Site Skymem[8]

Nessa fase da pesquisa, utilizou-se como referência um domínio “GOV.BR” de um instituto de pesquisa. Por meio de técnicas e buscas avançadas na Web (utilizando OSINT e Google Dorks), foi possível obter e-mails pertencentes a funcionários do quadro daquele instituto e de setores relacionados. Cabe ressaltar que o fato de e-mails estarem disponíveis na internet não representa um ameaça. No entanto, em alguns casos muitos e-mails de empresas, órgão públicos e instituições podem ter sido vazados em algum incidente passado. De qualquer forma, sites como LinkedIn, Plataforma Lattes, página de instituições, artigos científicos, dentre outros, permitem visualizar informações de contato e locais de trabalho, o que pode ser utilizado para realização de ataques de *phishing* direcionados, após as coletas dessas informações.

3.1.2 Armamento

Nessa etapa, foram utilizados e implementados recursos tecnológicos para sustentar os testes de validação e realizar os ataques simulados propriamente ditos, ou seja, foram criados os artefatos metodológicos.

Artefatos utilizados para testes preliminares

A Tabela 6 apresenta ferramentas e ações que fizeram parte de uma etapa exploratória preliminar que, embora não tenham efetivamente sido usadas na etapa

[8] Disponível em: < http://www.skymem.info/>. Acesso em: 15 mai 2023

de entrega, descrita na Seção 3.1.3 Entrega , foram importantes para os aprendizados que serão descritos nessa seção.

Tabela 6: Ações experimentais exploratórias realizadas no início da etapa de armamento

Ferramentas usadas: Registro BR, Google Gmail, Amazon AWS, Canva, GoPhish	**Status na pesquisa:**
Descrição das ações realizadas: a) Criação de um domínio no Registro BR (@educanuclear.com.br) b) Criação de um e-mail no Gmail (educanuclear@gmail.com) c) Criação de uma conta de acesso na Amazon AWS para utilização de serviços em nuvem; d) Implementação de uma instância EC2 Linux na nuvem da Amazon AWS e) Instalação e configuração do serviço HTTP Apache na instância Linux f) Desenvolvimento de páginas Web para integração ao servidor Linux g) Criação de um site (<http://www.educanuclear.com.br>) que corrobora a história de cobertura contada pelo e-mail *phishing* enviado na etapa de entrega. h) Instalação do serviço GoPhish na nuvem para criação de campanhas de teste de *phishing.*	**Funcionou?** **( ) SIM (X) NÃO** **Foi aproveitado para a próxima etapa?** **( ) SIM (** X **) NÃO**

Essas ações experimentais acabaram não sendo efetivamente empregadas na etapa de entrega, pois:

- ao implementar a ferramenta GoPhish no servidor Linux hospedado na Amazon AWS, não foram obtidos resultados satisfatórios que pudessem garantir a eficácia e a entrega dos e-mails aos integrantes daquele instituto. Isso ocorreu, pois a ferramenta não notificava corretamente a leitura e abertura dos e-mails enviados. Essa informação é imprescindível para o sucesso da etapa de entrega,
- os servidores de e-mail do Google e Microsoft acusaram a possibilidade de atividade maliciosa em mensagens que contivessem links apontando para

<http://www.educanuclear.com.br> no corpo do e-mail, ou seja, o domínio **educanuclear.com.br** foi categorizado pelo Gmail e Outlook como suspeito e perigoso (*phishing*), o que representou um impasse para a continuação dos testes com esse domínio. Isso comprometeria todo esforço inicial realizado, consequentemente, todo o estudo de caso da pesquisa, caso essa etapa importante falhasse, se a entrega dos e-mails não chegasse aos seus destinatários.

Portanto, foi necessário adquirir um novo domínio**, educanuclear.com**, e tomar as devidas precauções para evitar problemas semelhantes.

- Evitou-se realizar envios para endereços inválidos ou inativos;
- A lista de e-mails foi segmentada em listas menores;
- Evitou-se utilizar palavras e frases comuns em spam;
- Não foram realizados testes de clonagem de sites legítimos com o novo domínio adquirido;
- Foram realizados testes antes do envio, certificando-se que os e-mails estavam sendo entregues corretamente.

Artefatos utilizados na etapa de entrega

Com as lições aprendidas, elaborou-se um novo conjunto de ferramentas e nova sequência de ações para esta etapa, conforme ilustrado na Tabela 7. Essas foram efetivamente utilizadas na etapa descrita na Seção 3.1.3 Entrega .

Tabela 7: Ações efetivamente aproveitadas para a etapa de entrega

Ferramentas usadas: Google Domains, Hostgator, E-mail Titan, Microsoft Forms	**Status na pesquisa:**
Descrição das atividades: a) Criação de um domínio no Google Domains (educanuclear.com) b) Aquisição de hospedagem de sites na empresa Hostgator c) Aquisição do plano de e-mails profissional Titan Hostgator	**Funcionou?** **(** X **) SIM ( ) NÃO**

d) Criação, configuração e hospedagem de um Website no provedor Hostgator e) Criação de e-mails profissionais com o padrão nome@educanuclear.com f) Configurações internas de parâmetros e logs na estrutura da aplicação hospedada g) Configurações dos textos, links e parâmetros de verificações nos e-mails h) Criação e configuração de um formulário de inscrição de treinamento	**Foi aproveitado para a próxima etapa?** **(X) SIM ( ) NÃO**

A seguir são descritos em detalhes os aparatos tecnológicos criados para viabilizar as ações da Tabela 7.

Modelo de e-mail corporativo

Os e-mails utilizados no teste de *phishing* foram coletados através do processo de OSINT em plataformas públicas, simulando o processo que um hacker ou grupo criminoso teria que realizar. Em seguida foram salvos arquivos de texto para posterior utilização. A lista de e-mail (Quadro 1) foi dividida com a finalidade de segmentar o envio. Os e-mails foram encaminhados através dos endereços:

capacitacao@educanuclear.com	ensino@educanuclear.com
inscricao@educanuclear.com	treinamento@educanuclear.com

Quadro 1: E-mails utilizados como endereço de remetente para os experimentos

A Figura 9 ilustra o conteúdo da mensagem de teste de *phishing* enviada aos funcionários do instituto de pesquisa alvo.

Figura 9: Mensagem contida nos e-mails enviados
Fonte: O autor (2023)

Foram habilitados nos 04 (quatro) endereços de e-mail um recurso que possibilita obter as métricas referentes à abertura de e-mail. Esse campo permite analisar essas informações. Ele é identificado por um símbolo verde e acompanha um número ao lado entre parênteses indicando a quantidade de pessoas que abriram o e-mail com os respectivos horários de cada abertura. Por questões de privacidade, todas as referências que possam identificar pessoas foram suprimidas, tendo em vista que o objetivo deste trabalho é proteger a privacidade e os dados pessoais. Com relação ao nome que consta na assinatura de e-mail, este foi criado de forma fictícia, não se tratando, portanto, de pessoa real vinculada ao contexto do referido trabalho.

Website EducaNuclear: um portal fictício para treinamentos

A página principal do website (Figura 10), quando acessada pelo link fornecido no e-mail, era direcionada para URL <https://educanuclear.com/***/index.html>. No entanto, uma página idêntica também estava disponível ao acessar a URL <https://educanuclear.com>. Isso significa que a página principal foi clonada para um

diretório específico com objetivo de quantificar apenas os acessos provenientes da campanha de *phishing* realizada. Todos esses procedimentos eram registrados nos logs do serviço HTTP a cada clique.

Figura 10: Website Educanuclear - página de treinamentos
Fonte: O autor (2023)

O site Educanuclear possui outras duas abas acessíveis, sendo as páginas Home e Contate-nos, conforme Figura 11 e Figura 12.

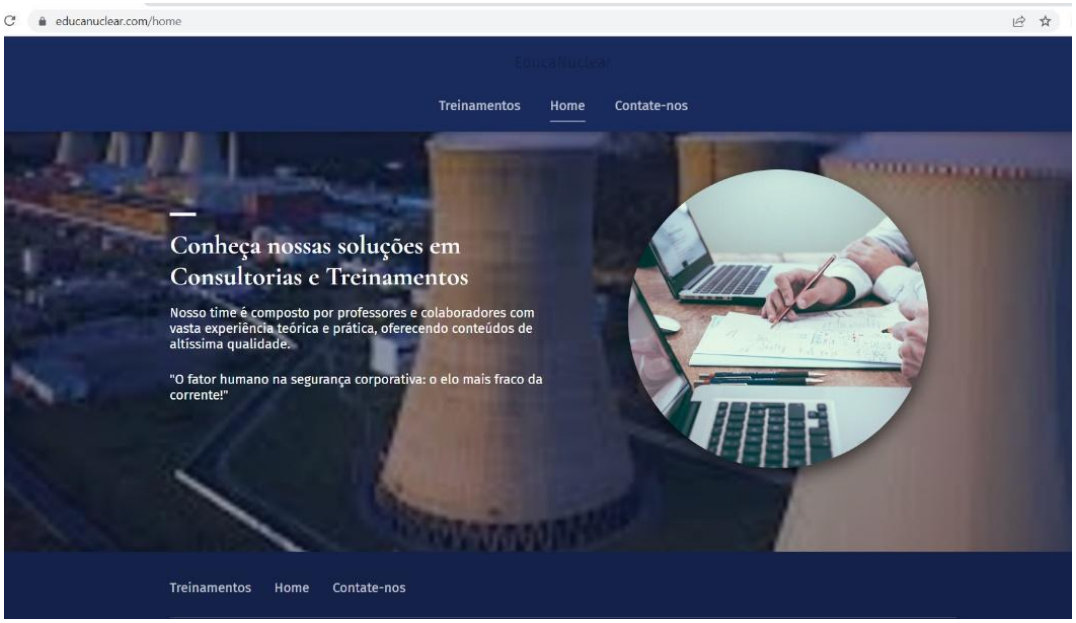


Figura 11: Página Home do site Educanuclear

Fonte: O autor (2023)

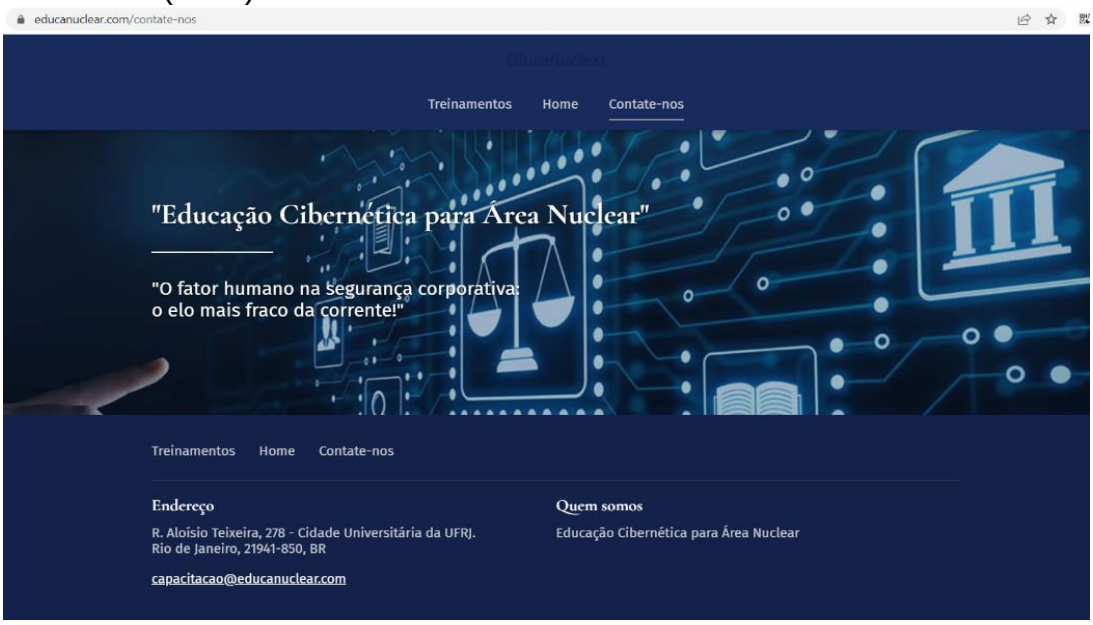


Figura 12: Página Contate-nos do site Educanuclear

Fonte: O autor (2023)

Um portfólio ilustrativo foi incorporado ao site Educanuclear. Utilizou-se um modelo pré-existente disponível no Canva e foram adicionadas informações extras conforme mostrado na Figura 13.

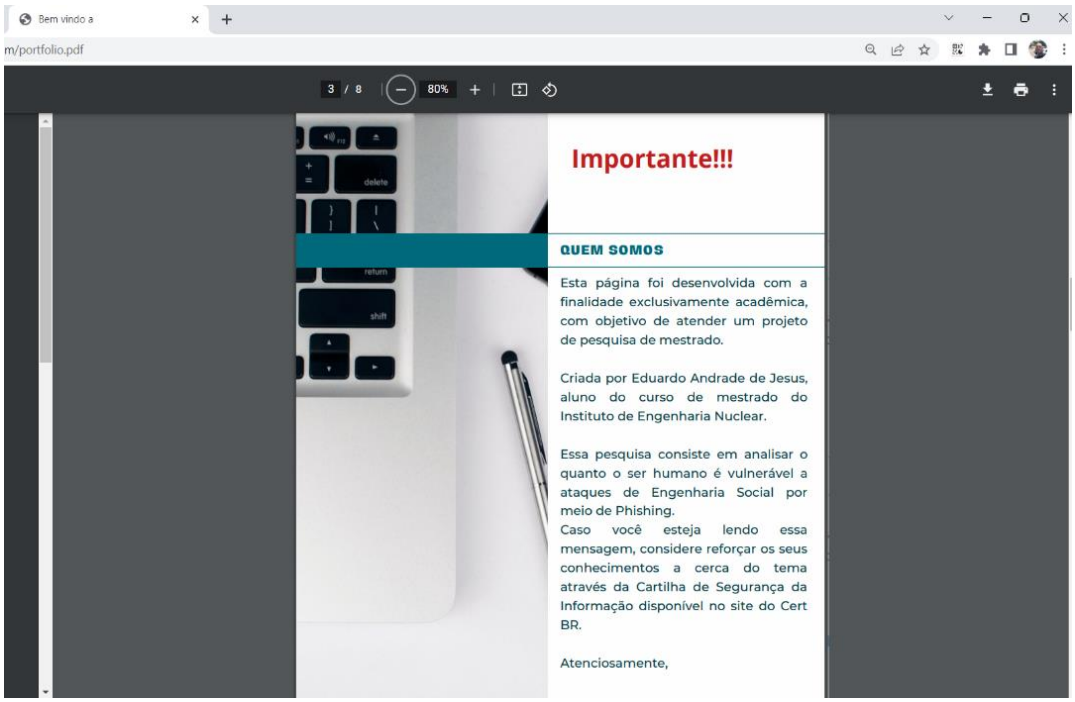


Figura 13: Mensagem contida no arquivo portfólio.pdf

Fonte: O autor (2023)

Formulário de inscrição no Programa de Capacitação Nuclear

À medida que os e-mails foram enviados como parte dos testes da campanha de *phishing*, era esperado que os colaboradores clicassem nos links fornecidos no corpo do e-mail, como exemplificado anteriormente. É importante destacar que abrir um e-mail e ler seu conteúdo não representa uma ameaça ou vulnerabilidade, pois o assunto pode ser relevante para os funcionários do instituto de pesquisa. No entanto, existem técnicas para identificar previamente quais e-mails podem representar ameaças e explorar vulnerabilidades se as ações forem executadas, ou seja, identificar um ataque de *phishing* (SALAHDINE, 2019).

Supondo que após o envio dos e-mails uma pessoa demostrasse interessada em realizar um dos treinamentos oferecidos, teríamos então duas possibilidades:

a) A pessoa poderia preencher o formulário com a indicação do treinamento desejado, ou;
b) Poderia responder diretamente o e-mail indicando o interesse em realizar algum treinamento.

Caso a pessoa opte por realizar a inscrição do treinamento através do formulário, será aberto uma página contendo as informações, conforme Figura 14.

Figura 14: Formulário de inscrição
Fonte: O autor (2023)

Ao iniciar o preenchimento do formulário, será apresentada uma lista de cursos disponíveis para a inscrição, conforme mostrado na Figura 15. Optou-se por disponibilizar apenas um treinamento no formulário e não solicitar nenhuma informação pessoal durante o processo de preenchimento da inscrição.

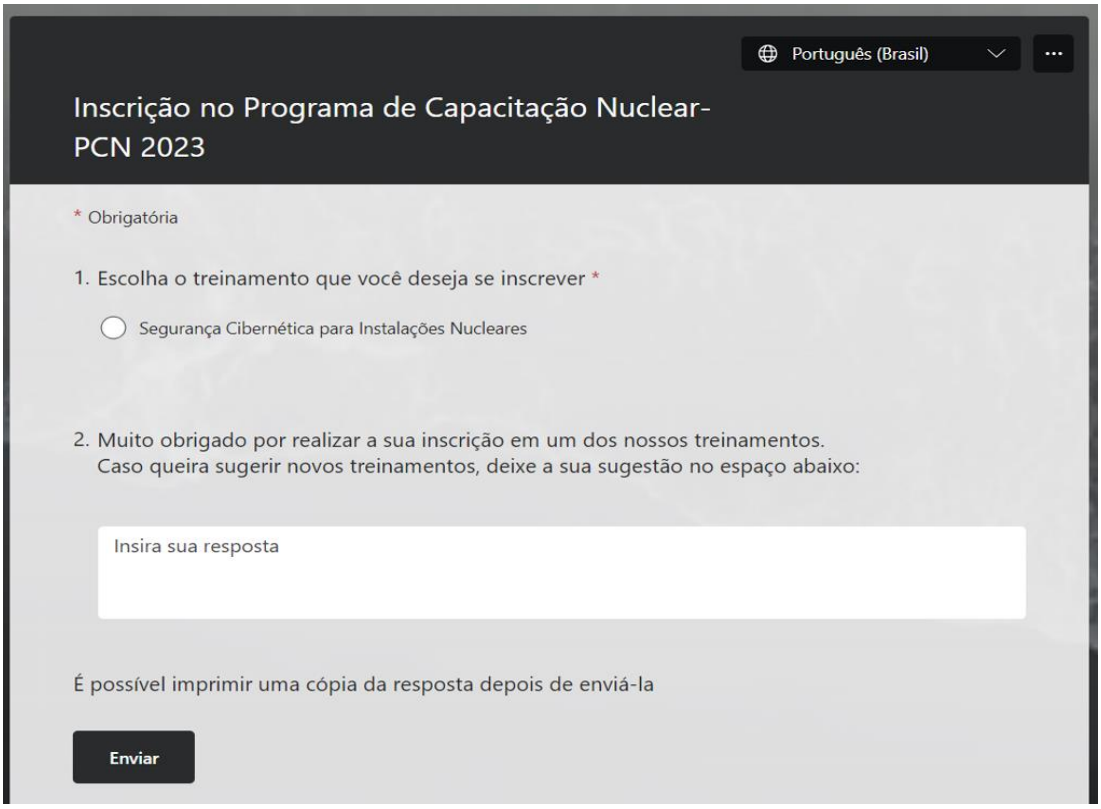


Figura 15: Página de preenchimento do formulário de inscrição
Fonte: O autor (2023)

Após finalizar o preenchimento do formulário, a pessoa é prontamente notificada com a mensagem representada na Figura 16. Essa abordagem transmite a sensação da pessoa estar se inscrevendo em um curso legítimo.

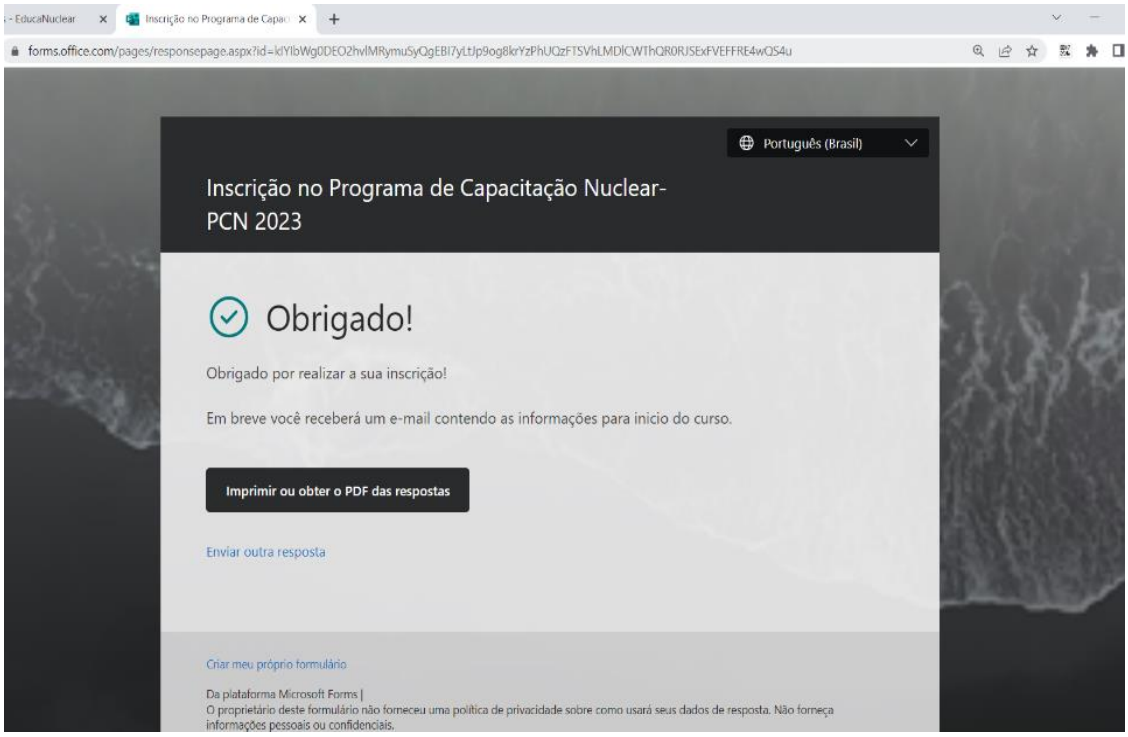


Figura 16: Página de conclusão do preenchimento do formulário
Fonte: O autor (2023)

Aplicação do teste de *phishing* em uma organização do setor nuclear

A aplicação do teste de *phishing* baseou-se no envio dos e-mails customizados para uma lista de funcionários da instituição alvo.

Monitoramento dos e-mails enviados e abertos

Um *pixel* de rastreamento de abertura de e-mail é uma técnica utilizada para monitorar se um e-mail foi aberto e visualizado pelo destinatário. Consiste em um pequeno elemento gráfico (geralmente um pixel transparente) incorporado no conteúdo do e-mail. Ao ser carregado, o *pixel* envia uma solicitação para um servidor externo, que registra a atividade de abertura do e-mail. Essa técnica envolve a inclusão de um código HTML que aponta para a imagem remota, disponível no servidor do atacante. Quando a imagem/pixel é carregado, o servidor do atacante registra a solicitação de envio da imagem, e registra atividade, indicando que um dos e-mails enviados e-mail foi lido.

Alguns atacantes podem utilizar em suas atividades estratégias que são comumente utilizadas por serviços de marketing para monitorar a abertura e a

visualização de e-mails. Segundo (RAMZAN, 2010) essa técnica permite ao remetente coletar informações sobre a abertura do e-mail, o endereço IP do destinatário, o tipo de dispositivo ou cliente de e-mail utilizado e a data e hora em que o e-mail foi aberto. Com esses dados em mão, é possível aos cibercriminosos realizarem outros tipos de ataques mais sofisticados e direcionados.

Embora não existam técnicas específicas para proteção direta contra esses rastreamentos de abertura e-mail, podem ser adotadas medidas para minimizar seu impacto e proteger a privacidade (FAN,2017):

a) Bloquear o carregamento automático de imagens
b) Utilizar extensões de privacidade
c) Verificar configurações de privacidade do seu cliente de e-mail
d) Optar por serviços de e-mail que respeitam a privacidade
e) Manter sempre os softwares atualizados

Análise do setor nuclear através da revisão bibliográfica

Ao analisar o contexto do setor nuclear, ficou evidente que para um maior convencimento de um público interno por e-mail, seria necessário criar argumentos fortes que levem a crer na veracidade das informações entregues por e-mail. Tal estruturação foi consolidada através da criação de nomes de domínios reais (educanuclear.com), criação de sites e hospedagem em provedor reconhecido no mercado, utilização de páginas providas por meio de certificado digital válido (HTTPS) e criação de e-mails profissionais utilizando o domínio real.

Dessa forma, uma história de cobertura envolvendo a criação de um “Programa de Capacitação Nuclear – 2023” com o mesmo teor no campo assunto, bem como a elaboração de um texto simples e convincente no corpo do e-mail seria a forma de mais viável para as pessoas que receberem o e-mail, abram e leiam!

Configuração de parâmetros na página do website Educanuclear

A página (/***/index.html) foi criada como solução de contorno no interior da estrutura de diretórios da página principal (/public_html). Desse modo, a página principal retorna uma página em branco durante a campanha. Com isso, os acessos realizados através dos links disponibilizados no corpo do e-mail puderam ser medidos,

validados e rastreados por meio da origem dos acessos, sem que houvesse falsos positivos que pudessem interferir nas coletas de informação.

Os links de acesso foram modificados de tal forma que a pessoa que abrisse o e-mail teria o registro de evidência individualizado para cada conexão de acesso ao site e gravado no arquivo de log do servidor web apache. Finalmente, após o envio dos e-mails, o acesso inicial ao site EducaNuclear deu-se através do link contido no corpo da mensagem do e-mail. Esses dois links foram ofuscados para "https://www.educanuclear.com/***/index.html", em que cada acesso era registrado como uma conexão estabelecida, conforme indicado na tabela dos principais códigos de status de resposta HTTP, de acordo com a RFC 2616.

A Tabela 8: Status code do protocolo HTTP ilustra alguns dos códigos de status HTTP mais comuns. Existem outros códigos disponíveis na seção *Status Code Definitions* da RFC 2616. Cada código possui uma finalidade e significado. Esses códigos de status são retornados pelos servidores web para fornecer informações sobre o resultado de uma requisição HTTP por um cliente.

Tabela 8: Status code do protocolo HTTP

Código	**Descrição**
200	OK - Requisição bem-sucedida
201	Criado - Requisição bem-sucedida, recurso criado
204	Sem Conteúdo - Requisição bem-sucedida, sem retorno
301	Movido Permanentemente - Recurso movido
400	Solicitação Inválida - Erro no cliente
401	Não Autorizado - Acesso não autorizado
403	Proibido - Acesso proibido
404	Não Encontrado - Recurso não encontrado
500	Erro Interno do Servidor - Erro no servidor
502	Bad Gateway - Servidor recebeu resposta inválida
503	Serviço Indisponível - Servidor temporariamente indisponível

As ações descritas nesta seção foram submetidas a testes e experimentação, resultando em uma conclusão bem-sucedida, como será descrito a seguir.

Os testes preliminares foram realizados por meio do envio de e-mail para a caixa de correio funcional de um funcionário da instituição alvo, que estava apoiando o projeto de pesquisa. Esses testes foram conduzidos durante o período que antecedeu o envio efetivo. Após cada envio realizado durante os testes preliminares, os registros de acesso no servidor eram verificados para confirmar se o usuário recebeu, abriu o e-mail e clicou no link especificado.

Também foi realizado um teste de preenchimento do formulário de inscrição para verificar se estava tudo correto. Durante a realização desses procedimentos, foram feitos ajustes para garantir que o envio dos e-mails pudesse ser realizado sem o risco de serem bloqueados, como otimizar o conteúdo, verificar a formatação correta e evitar palavras ou anexos que pudessem ser identificados como suspeitos pelo sistema de segurança.

3.1.3 Entrega

Nesta seção, iremos analisar como foram desencadeados os procedimentos dos envios dos e-mails *phishing* que foram realizados como parte desta pesquisa.

Baseando-se nas ferramentas e ações elencadas na Tabela 7, e descritas na seção anterior, optou-se por dividir o envio dos 159 e-mails *phishing* aos colaboradores da organização alvo em quatro grupos de 40 endereços de destino cada um. Isso foi importante, pois como parte dos endereços obtidos na etapa de reconhecimento poderiam ser inválidos ou desativados, corria-se o risco, no caso de apenas um grupo de envio, de que o provedor, devido a um potencial alto número de retornos de erro, classificar o endereço do remetente como um endereço suspeito, o que inviabilizaria a entrega.

A primeira sequência de envio de e-mails ocorreu no dia 06 de junho de 2023, às 12:00h (GMT-3) - horário de Brasília, Brasil. Respeitando um intervalo de tempo de dezenas de minutos, seguiu-se, sequencialmente, com os outros três envios.

Os resultados alcançados nesta etapa são apresentados na Seção 4. RESULTADOS E DISCUSSÕES.

Para executar a etapa de entrega, foi utilizado um gerenciador de e-mails profissional fornecido pela HostGator (Titan Mail), que permitiu o gerenciamento das quatro contas de e-mail criadas para realizar o ataque simulado, conforme ilustrado na Figura 17.

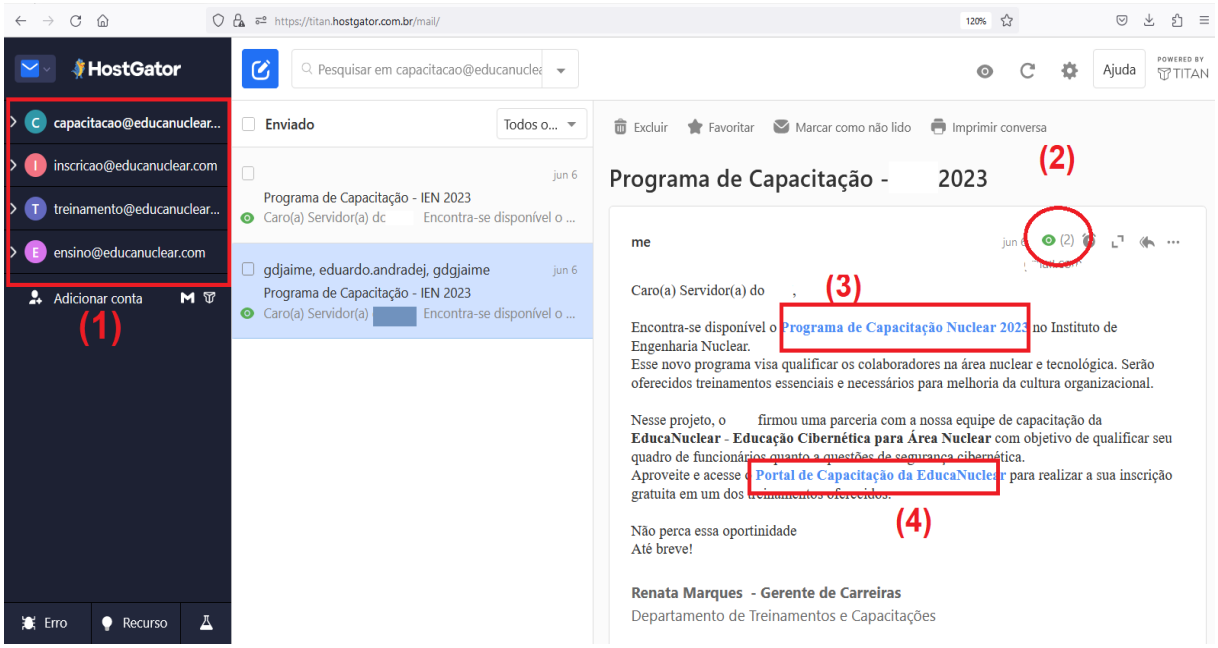


Figura 17: Gerenciador de e-mails Titan Webmail
Fonte: O autor (2023)

Referência numérica contida na imagem:
1) Contas de e-mails gerenciadas
2) Confirmação de leitura do e-mail pelo destinatário
3 e 4) Links ofuscados redirecionando para URL `<https://www.educanuclear.com/***/index.html>` com objetivo específico de identificar e registrar, de forma inequívoca nos logs, os acessos ao site "isca" que foram provenientes dos e-mails enviados.

Rastreamento de e-mails devolvidos com algum tipo de erro

Durante o envio, e-mails com erros ortográficos ou inexistentes não foram entregues ao servidor de destino e uma mensagem de erro foi retornada. Essa situação ocorreu em algumas ocasiões devido à lista de e-mails de destino não ter sido obtida oficialmente na instituição de pesquisa em questão. Isso foi intencional, pois parte do escopo da pesquisa era demonstrar como os invasores podem obter e-

mails de instituições ou organizações. É importante destacar que essas listas nem sempre possuem todos os endereços válidos, como foi evidenciado durante o envio dos e-mails.

3.1.4 Exploração

Essa etapa utilizou ferramentas comuns para scan de rede baseados em endereços IP, recursos como o Whois para identificar a origem dos endereços que acessaram o site Educanuclear, bem como o sistema operacional Kali Linux e a ferramenta Shodan[9] para identificar portas e serviços abertos nos endereços IPs registrados nos logs de acesso do servidor web. Cabe ressaltar que essa é uma etapa de exploração externa, ou seja, quando o atacante ainda não conseguiu realizar a intrusão em sistemas e rede do alvo. Após a fase de entrega ocorrerá outra exploração, nesse caso, a rede interna.

3.1.5 Instalação

Nessa etapa, o objetivo foi simular as ações que um atacante deve realizar para induzir a vítima a executar o *malware* em seu sistema operacional. Como parte do ataque simulado, foram conduzidos testes de dentro da instituição alvo para avaliar a possibilidade de *download* de arquivos externos para a rede interna.

Devido às rigorosas políticas de segurança aplicadas à rede interna da instituição alvo, os controles tecnológicos foram efetivamente implementados para garantir a segurança do ambiente de trabalho. Como resultado, a transferência do arquivo executável "agente.exe", que se comunica com o servidor C2, foi bloqueada como medida de precaução devido aos potenciais riscos associados a esse tipo de arquivo.

Os testes foram conduzidos de maneira controlada, utilizando a estação de trabalho de um funcionário da instituição, que executava o sistema operacional Linux Ubuntu 22.04 LTS, e um computador pessoal, que executa o sistema operacional Windows 10 64 bits. Essas estações de trabalho foram utilizadas para simular a

[9] Shodan é uma ferramenta de pesquisa e monitoramento de segurança que permite aos usuários encontrar dispositivos conectados à Internet e identificar informações sobre eles. (<https://www.shodan.io/>)

instalação do *malware* e verificar o seu comportamento na etapa de Comando e Controle.

A título de ilustração, foi enviado um outro e-mail com um texto dando as boas-vindas aos participantes do treinamento, nesse caso, dois servidores da instituição alvo simularam o recebimento do e-mail de contato em que a empresa de treinamento Educanuclear entra em contato com os participantes, informando a data de início do treinamento. Esse e-mail possuía um link e um anexo contendo a descrição dos procedimentos, especificado para cada tipo de software, as orientações de como baixar e instalar no sistema operacional para participar do treinamento.

Esse segundo envio refere-se a entrega do *malware* simulado para instalação. Caso esse ataque fosse realizado por um atacante real e os contornos protetivos da organização não fossem efetivos para contê-lo, é provável que o atacante obtivesse êxito nessa etapa e conseguisse implantar uma persistência no ambiente tecnológico. Esse tipo de ataque permite que cibercriminosos permaneçam na infraestrutura alvo por um longo período sem serem detectados.

Figura 18: E-mail contendo instruções para instalação de software
Fonte: O autor (2023)

A Figura 19 representa a página de acesso que o usuário visualiza após clicar no link fornecido no corpo do e-mail que dava as boas-vindas para início do treinamento. Consta também um arquivo “.pdf” anexado ao e-mail e disponível pelo link incorporado ao conteúdo, contendo as instruções de como instalar o programa que seria pré-requisito para realizar o treinamento, porém, na verdade, trata-se de um *malware* (simulado). Isso demonstra o quanto uma pessoa pode estar vulnerável caso venha a instalar programas de fontes desconhecidas em seu dispositivo.

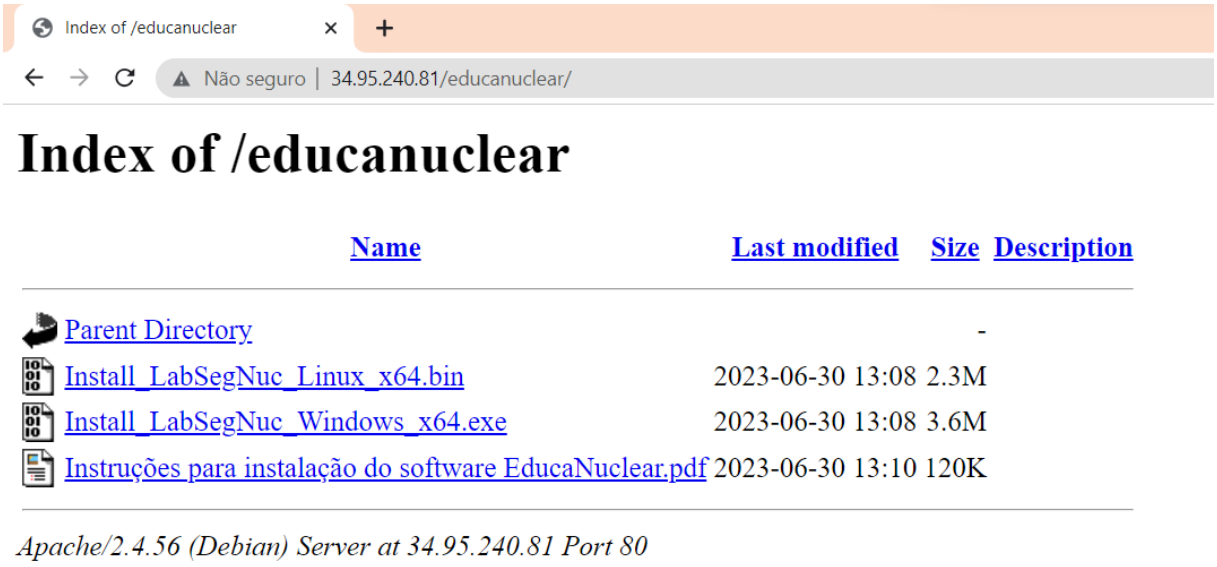


Figura 19: Link indicado no e-mail para download do software (malware)
Fonte: O autor (2023)

3.1.6 Comando e Controle

Cabe ressaltar que o servidor utilizado nesta pesquisa estava hospedado na nuvem do Google Cloud Platform (GCP), no endereço IP público fixo (34.95.240.81), executando um sistema operacional Linux Debian 11, em um ambiente seguro e controlado.

O acesso a esse servidor é restrito apenas a um computador próprio, o qual possui as chaves criptografadas para garantir a segurança dos dados envolvidos. Essas medidas foram adotadas para prevenir qualquer tipo de vazamento de dados relacionados a esta pesquisa (LGDP, 2018).

Experimentos realizados entre o Servidor C2 e um sistema Windows 10 executando o agente do C2

1) Primeiramente, a execução do Servidor C2 (DESEC, 2023), denominado como **“ncr2-server”**, é realizada ao invocar o arquivo de nome “nrc2” por meio do seguinte comando: `'$ sudo ./nrc2'`. Esse comando é executado com privilégios de superusuário (sudo) para garantir as permissões adequadas durante a sua execução, conforme Figura 20. Dessa forma, o C2 é ativado e fica em execução, aguardando novas conexões. O servidor C2 permanece em um estado pronto para receber e processar novas solicitações de conexão, estabelecendo assim uma comunicação eficiente e contínua com os dispositivos e agentes envolvidos.

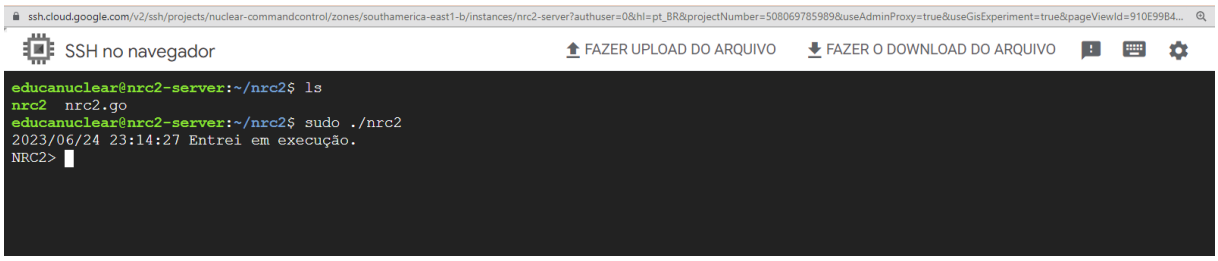


Figura 20: Entrada em execução do C2
Fonte: O autor (2023)

2) A seguir, é possível observar pela Figura 21 que uma nova conexão foi estabelecida no C2, sendo atribuído a ela um ID que representa a identificação única de cada agente que se comunica com o servidor C2. Esse ID é utilizado para distinguir e rastrear individualmente os agentes envolvidos na comunicação com o C2.

É possível ainda verificar o endereço IP público e porta pelo qual cada agente (vítima) estabelece a conexão. Essa informação permite identificar o IP público associado ao dispositivo da vítima na rede externa, possibilitando rastrear o ponto de origem da conexão realizada pelo agente. Nesse caso, o endereço IP externo atribuído a conexão do alvo é o 177.12.48.201 e as portas 10106 e 10107.

```
educanuclear@nrc2-server:~/nrc2$ sudo ./nrc2
2023/06/24 22:10:35 Entrei em execução.
NRC2> 2023/06/24 22:11:02 Nova conexão:  177.12.48.201:10106
2023/06/24 22:11:02 Agente ID:  91e3ea61544fafe0daff8381b11eb5ab
2023/06/24 22:11:07 Nova conexão:  177.12.48.201:10107
2023/06/24 22:11:07 Agente ID:  c1ea4f99c85fd1271de8ab79839bd541
```

Figura 21: Conexão de um agente com o C2
Fonte: O autor (2023)

3) Após esse procedimento, o "atacante" executa o comando "`show agentes`" para listar os computadores alvos que se conectaram ao C2. Em seguida, seleciona um alvo específico utilizando o comando "`select ID-do-alvo`" para estabelecer a conexão com o alvo selecionado, conforme ilustrado na Figura 22.

Ao estabelecer a conexão com o computador alvo, o “atacante” executa três comandos consecutivos: “`whoami`”, “`ipconfig`” e “`ls`”. O objetivo desses comandos é obter, respectivamente, o nome do computador, o endereço IP local e listar o conteúdo do diretório do computador alvo.

```
NRC2> show agentes
Agente ID: 91e3ea61544fafe0daff8381b11eb5ab->Vinicius@C:\Users\vinic\Downloads
Agente ID: c1ea4f99c85fd1271de8ab79839bd541->Vinicius@C:\Users\vinic\Downloads
NRC2> select c1ea4f99c85fd1271de8ab79839bd541
c1ea4f99c85fd1271de8ab79839bd541@NRC2# whoami
c1ea4f99c85fd1271de8ab79839bd541@NRC2# ipconfig
c1ea4f99c85fd1271de8ab79839bd541@NRC2# ls
```

Figura 22: Visualização de agentes conectados ao C2 e realização de comandos
Fonte: O autor (2023)

De forma intencional, o C2 Server em questão foi implementado para fornecer respostas em períodos aleatórios, variando entre 5 segundos e 30 segundos. Essa abordagem tem por objetivo fazer com que as defesas de segurança do alvo não o classifiquem como um *malware*. Com isso, o servidor C2 adquire um aspecto furtivo e é capaz de contornar as medidas de segurança instaladas no computador da vítima, evitando, assim, ser detectado ou bloqueado.

4) A resposta do comando "`whoami`" (Figura 23) no computador alvo irá exibir o nome do usuário atualmente logado na máquina. Esse comando fornece informações sobre a identidade do usuário que está executando o comando no sistema operacional, permitindo identificar o contexto do usuário ativo no momento da execução.

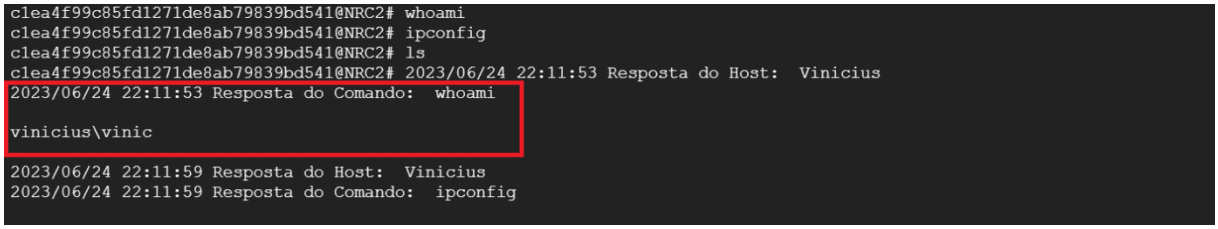


Figura 23: Resposta do comando "whoami"
Fonte: O autor (2023)

5) A resposta do comando "`ipconfig`" (Figura 24) no computador alvo irá exibir informações sobre a configuração de rede desse computador. Essas informações geralmente incluem o endereço IP, máscara de sub-rede, *gateway* padrão, endereços de DNS e outras informações relevantes sobre a interface de rede. O resultado pode variar dependendo do sistema operacional do computador alvo. Nesse caso, o endereço IP interno atribuído ao computador da vítima é o 192.168.0.120 e o endereço de *gateway é* 192.168.0.1.

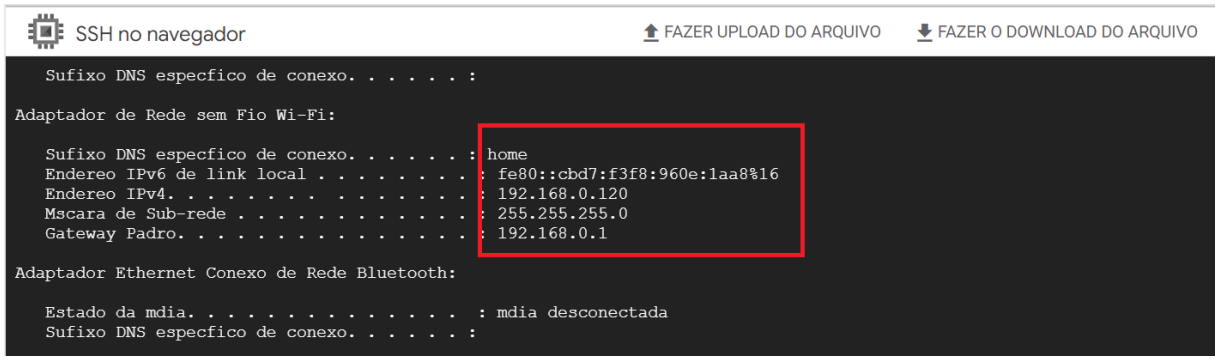


Figura 24: Resposta do comando "ipconfig"
Fonte: O autor (2023)

7) O comando "`ls`" (Figura 25) será refletido no computador da vítima e retornará uma listagem dos arquivos e diretórios presentes no sistema de arquivos do mesmo. Ele exibirá o nome dos arquivos e diretórios disponíveis no diretório atual ou no diretório especificado, caso seja fornecido um caminho como argumento para o comando. A listagem pode incluir informações como permissões de acesso, data de modificação e tamanho dos arquivos.

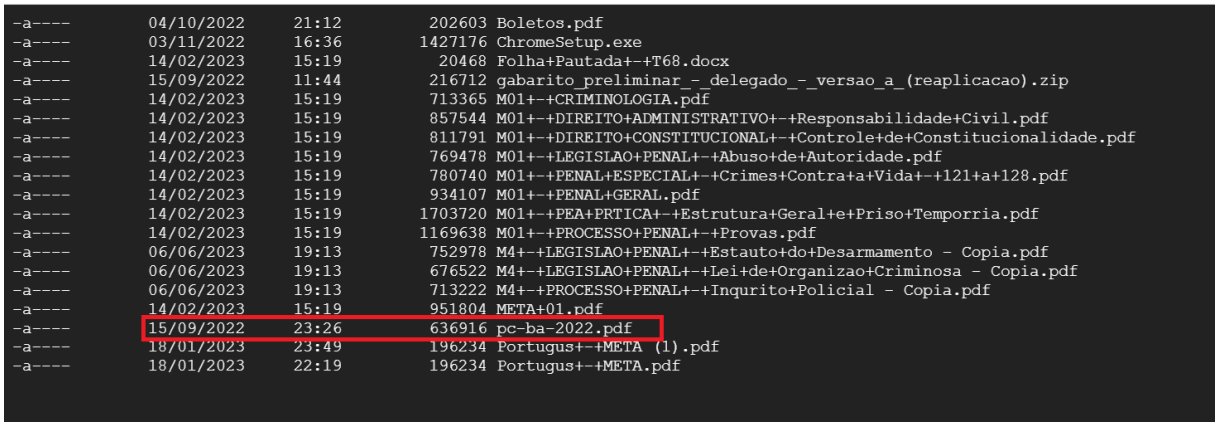


Figura 25: Resposta do comando "ls"
Fonte: O autor (2023)

3.1.7 Ações no Objetivo

Essa etapa é a continuação da etapa Comando e Controle e tem o objetivo de demonstrar como ocorre a exfiltração de dados sensíveis de um sistema alvo e a realização de movimento lateral em uma rede de Tecnologia da Informação (TI) para uma rede de Tecnologia Operacional (TO).

3.1.7.2 Etapa de exfiltração de dados a partir de uma máquina Windows 10

1) Na Figura 25, foram identificados diversos arquivos, dentre eles um arquivo de nome “pc-ba-2022.pdf” para ser exfiltrado do computador alvo. Para realizar essa ação, foi executado o comando “`# get pc-ba-2022.pdf`”, como pode ser verificado na Figura 26. Esse comando indica que o arquivo especificado está sendo enviado do computador alvo e transferido para outro local ou sistema, nesse caso para o servidor C2.

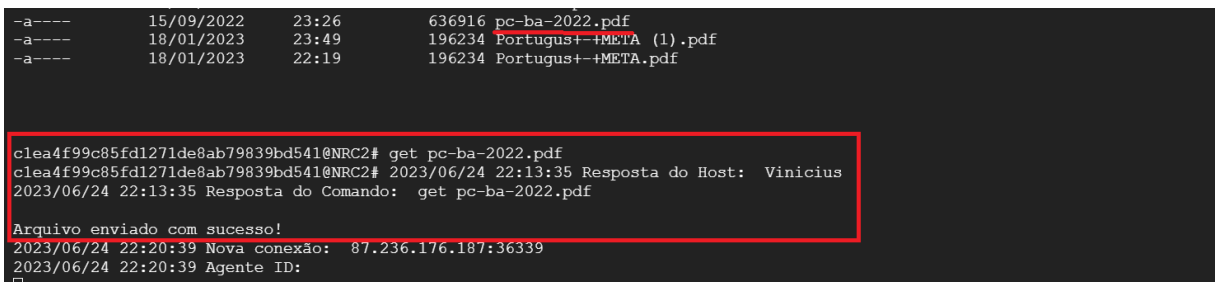


Figura 26: Comando para exfiltração de dados
Fonte: O autor (2023)

2) Após a exfiltração do arquivo do computador da vítima para o servidor C2, é possível verificar a presença desse arquivo no servidor. Por meio de comandos específicos no C2, nesse caso o "`ls`", foi possível listar os arquivos armazenados no diretório de destino no servidor e verificar que o arquivo "pc-ba-2022.pdf" encontra-se armazenado no C2 (Figura 27). Essa verificação permite confirmar se a exfiltração foi bem-sucedida e se o arquivo alvo foi transferido com sucesso para o servidor C2.

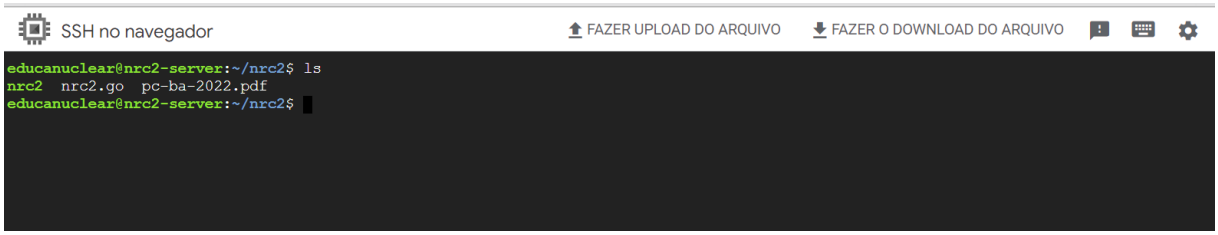


Figura 27: Verificação do arquivo exfilfrado para o C2
Fonte: O autor (2023)

3) É possível então proceder com o download do arquivo do servidor C2 para a máquina do "atacante", conforme ilustrado na Figura 28. Esse procedimento possibilita baixar do servidor C2 o arquivo "pc-ba-2022.pdf" para a máquina do "atacante", permitindo que seja armazenado localmente no sistema do "atacante" para análise, manipulação ou outros fins determinados pelo "atacante".

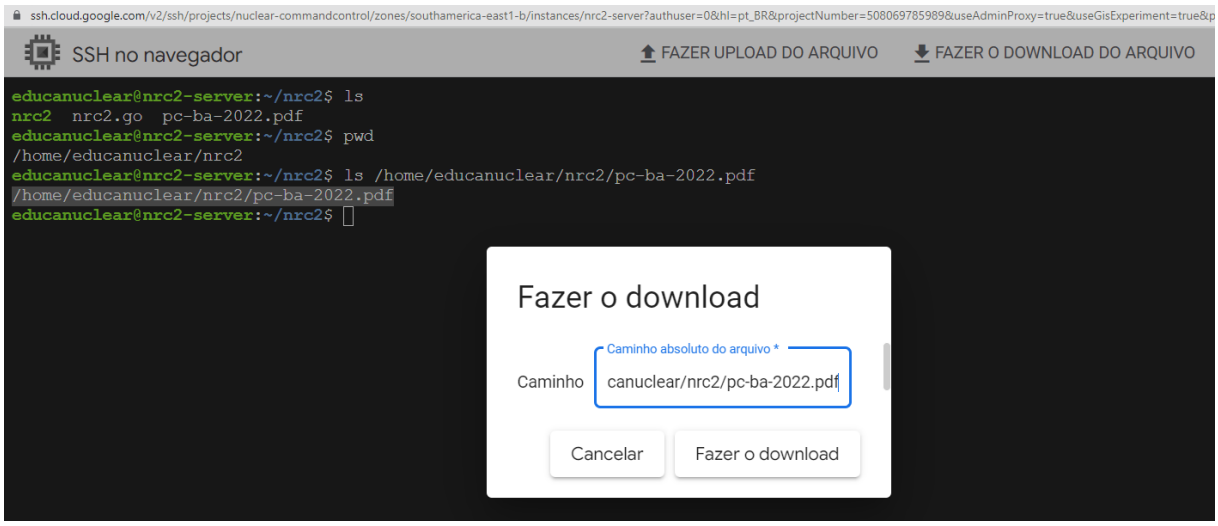


Figura 28: Download do arquivo exfiltrado
Fonte: O autor (2023)

4) Após o download bem-sucedido do arquivo do servidor C2 para o computador do “atacante”, o arquivo está agora disponível localmente e pode ser analisado no sistema do “atacante” (Figura 29: Arquivo exfiltrado para máquina do atacante). O “atacante” pode realizar diversas análises, como verificar o conteúdo do arquivo, examinar metadados, executar ferramentas de análise específicas ou realizar investigações adicionais para obter informações relevantes contidas no arquivo. Essa etapa de análise é importante para entender o conteúdo do arquivo exfiltrado e pode ajudar o “atacante” a alcançar seus objetivos específicos.

Figura 29: Arquivo exfiltrado para máquina do atacante
Fonte: O autor (2023)

3.1.7.2 Etapa de exfiltração de dados, movimentação lateral e verificação de vulnerabilidades a partir de uma estação Linux Ubuntu.

O agente do C2 (*malware* simulado) foi executado de forma controlada em uma estação de trabalho, localizada no interior das instalações do instituto alvo, e que na ocasião encontrava-se rodando o sistema operacional Linux Ubuntu 22.04.

Após o estabelecimento da conexão da estação Linux alvo com o servidor C2, foram executados comando iniciais para verificação de conexão, histórico de comandos executados e dados sensíveis que pudessem ser exfiltrados da estação alvo.

1) Na Figura 30, é possível verificar que foram estabelecidas duas conexões provenientes de mesmo endereço IP público (ofuscado intencionalmente). Ao

observar a saída emitida pelo comando `"NRC2> show agentes"`, fica evidente que os sistemas operacionais são diferentes, pois cada saída possui um ID diferente. No entanto, o que diferencia de fato uma saída da outra saída com relação aos sistemas operacionais são as informações contidas após o @. Uma apresenta o caminho `/instituto`, característico de sistema operacional Linux e a outra apresenta o caminho `C:\User\eduar\Documents\diversos`, característico de sistemas operacionais Windows. Nesse contexto, temos então a presença de dois sistemas distintos conectados ao mesmo servidor C2, vindo da mesma origem (instituto de pesquisa alvo de teste).

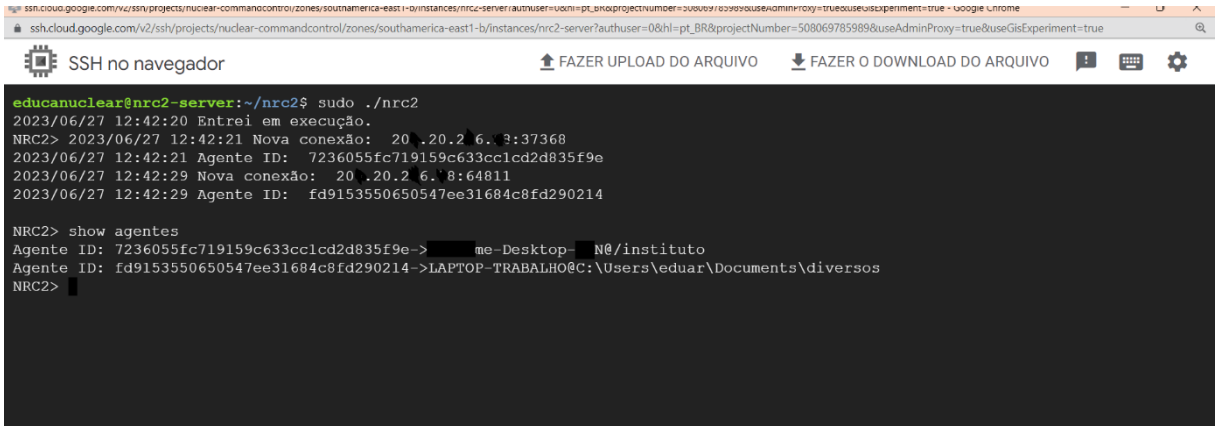


Figura 30: Listando agentes conectados do instituto alvo
Fonte: O autor (2023)

2) Na Figura 31, ilustra a representação da execução dos comandos “route -n” e “nmap localhost”. Esses comandos foram executados, respectivamente, para verificar a tabela de roteamento da estação Linux e se o aplicativo nmap estava instalado, em sendo assim, verificar se há as portas de serviços abertas naquela estação de trabalho. Em alguns casos isso indica que o computador funciona como um *gateway* entre duas redes.

Nesse caso, não foram constatadas outras rotas a não ser a do *gateway* padrão e o comando nmap estava presente na máquina, apontou apenas a porta 631/tcp aberta que é uma porta comum usada para compartilhamento de impressora e não representa risco. Encontrando-se esta estação de trabalho aparentemente segura.

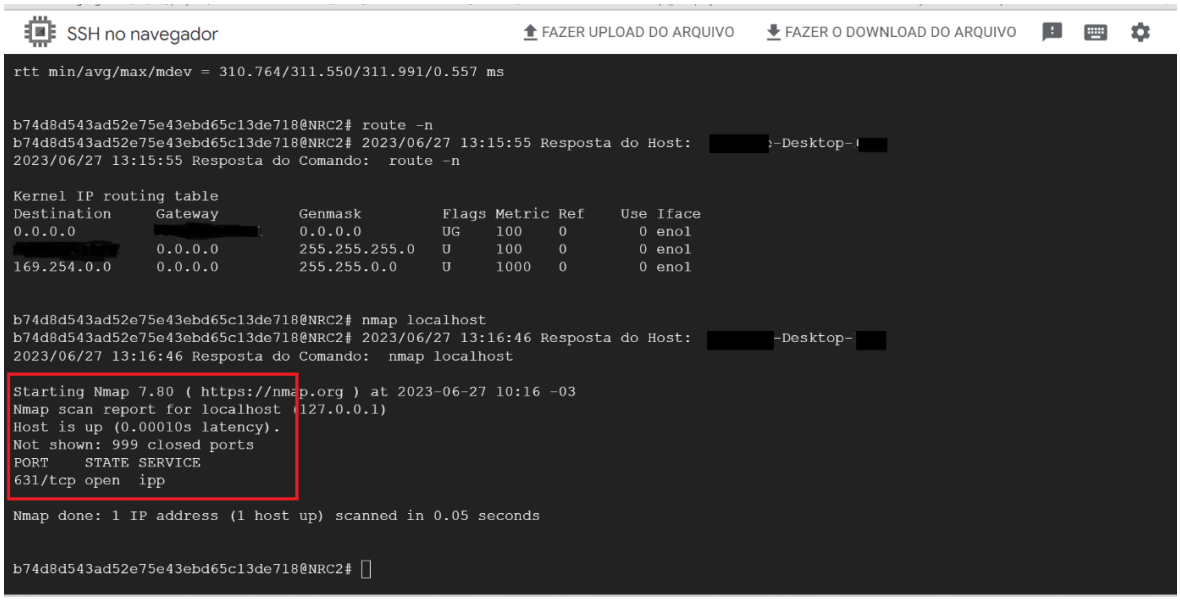


Figura 31: Execução do comando route e nmap

Fonte: O autor (2023)

3) Continuando com a exploração no host, foi executado o comando "`cat`" para ler o conteúdo do arquivo `.bash_history` do usuário atual, uma vez que a tentativa de execução do comando "`history`" através do C2 não retornou informações. Esse procedimento tem como objetivo verificar os últimos comandos que foram executados localmente na estação de trabalho, conforme ilustrado na Figura 32.

O arquivo `.bash_history` armazena o histórico de comandos digitados no terminal, o que pode fornecer informações importantes sobre atividades recentes e ajudar na análise da situação ou das ações realizadas pelo usuário.

Figura 32: Saída dos últimos comandos digitados na estação

Fonte: O autor (2023)

Na Figura 32 constam históricos de comando que foram realizados da estação local para um host remoto. Esses comandos são característicos de testes e conexão remota com um servidor, por exemplo.

4) Em seguida, conforme ilustrado na Figura 33, foi efetuado um mapeamento de portas para o endereço IP `(***.105.212.***)`, exibido no histórico de comandos recentes, utilizando o comando `"nmap IP-do-alvo"`. O Nmap ("Network Mapper") é uma ferramenta de código aberto para exploração de rede e auditoria de segurança. Ela foi desenhada para escanear rapidamente redes amplas, embora também funcione muito bem contra hosts individuais. A saída do Nmap é uma lista de alvos escaneados, com informações adicionais de cada um dependendo das opções utilizadas. (Guia de Referência do Nmap, 2023)

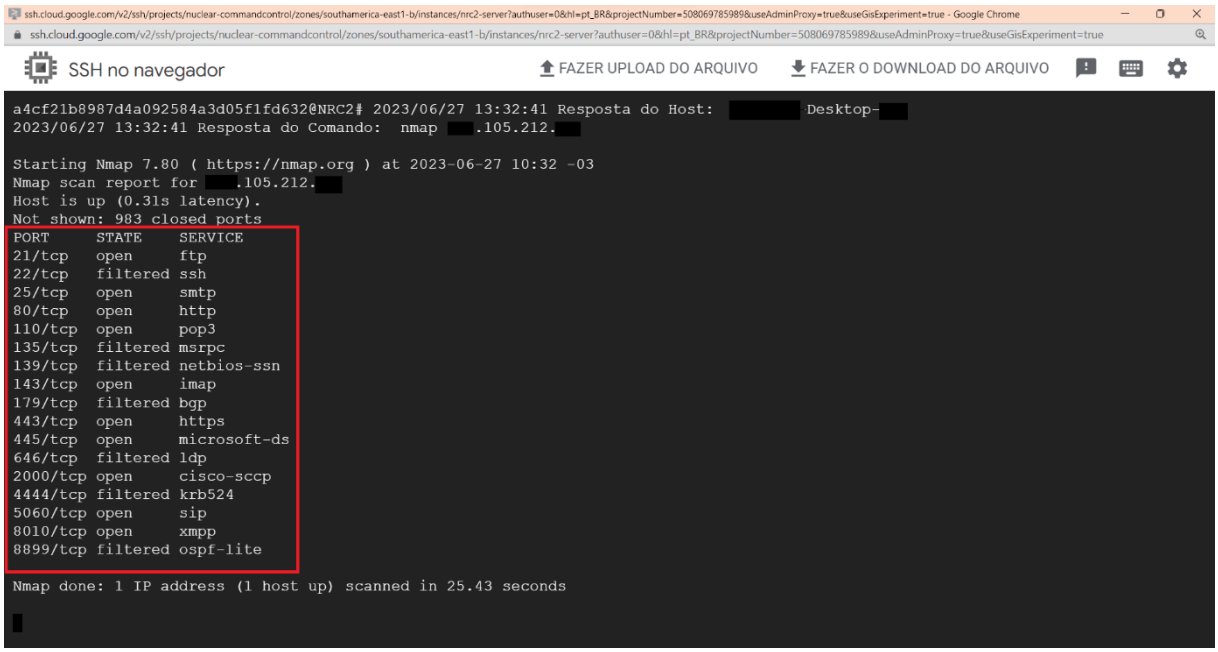


Figura 33: Mapeamento de portas no simulador
Fonte: O autor (2023)

O host identificado no mapeamento de porta é um simulador localizado em uma rede separada, designada como rede de Tecnologia Operacional (TO), que não possui conectividade com a internet. Essa rede é especificamente configurada para treinamento e simulação, proporcionando um ambiente controlado e isolado.

No contexto atual, foi iniciado um processo de movimentação lateral, envolvendo a exploração e progressão de um ambiente de rede de Tecnologia da

Informação (TI) para a rede de Tecnologia Operacional (TO). A movimentação lateral é uma etapa em uma intrusão cibernética em que um invasor compromete um sistema inicial e, em seguida, procura se mover lateralmente através da rede ou do ambiente para explorar outros sistemas. Durante essa fase, o invasor tenta obter acesso e controle a outros sistemas internos, a fim de ampliar seu alcance e comprometer mais recursos (MITRE, 2023).

5) Com relação ao simulador mapeado, trata-se de um servidor que executa o **sistema operacional HP-UX na versão 11.11**. Para realizar uma pesquisa por vulnerabilidades baseadas em CVEs (*Common Vulnerabilities and Exposures*), existem várias opções disponíveis. Um dos sites amplamente utilizados para essa finalidade é o CVE Details <https://www.cvedetails.com/>, onde é possível pesquisar por vulnerabilidades conhecidas nessa base de dados.

Ao acessar o site CVE Details, inserindo o sistema operacional HP-UX versão 11.11 na barra de pesquisa, foi obtida uma lista de vulnerabilidades conhecidas que afetam esse sistema. A plataforma oferece informações detalhadas sobre cada vulnerabilidade, incluindo a descrição, o impacto potencial e as soluções ou correções recomendadas (CVE DETAILS, 2023). Após a pesquisa por vulnerabilidades em diferentes sites relacionados a CVEs, foram encontradas as seguintes informações:

- CVE Details, foram encontrados 120 CVEs. Dentre esses, 19 foram classificados com o score máximo (10.0), indicando um alto nível de gravidade.
- CVE Mitre, foram encontradas 31 CVEs (Common Vulnerabilities and Exposures).
- NVD (*National Vulnerability Database*) do NIST, foram encontradas 105 ocorrências de CVE.

Essas informações indicam a existência de várias vulnerabilidades conhecidas que afetam o sistema operacional HP-UX versão 11.11.
Como o sistema HP-UX não recebe mais atualizações de segurança, considera-se a possibilidade de adotar medidas alternativas para mitigar os riscos de segurança.

- **Implementação de controles de segurança adicionais**: Adotar soluções de segurança complementares, como firewalls, sistemas de detecção de intrusões (IDS), sistemas de prevenção de intrusões (IPS) e antivírus atualizados.
- **Isolamento do sistema**: Isolar o sistema HP-UX em uma rede separada ou em uma zona restrita, limitando o acesso a partir de outras redes ou sistemas.
- **Monitoramento constante**: Implementar soluções de monitoramento de segurança para detectar atividades suspeitas ou tentativas de intrusão. Isso inclui a análise de logs, monitoramento de tráfego de rede e detecção de comportamentos anômalos.
- **Segmentação da rede**: Dividir a rede em segmentos menores ou zonas separadas, com base nas necessidades de comunicação e nos níveis de confiança.

6) Por fim, a Figura 34 ilustra de forma simulada a exfiltração de dados sensíveis de um computador com sistema operacional Linux, enviando a arquivo para o servidor C2, dessa forma, caracterizando um vazamento de dados ou roubo de propriedade intelectual/industrial, exemplificado pelo arquivo `"teste-exfiltracao.pdf".`

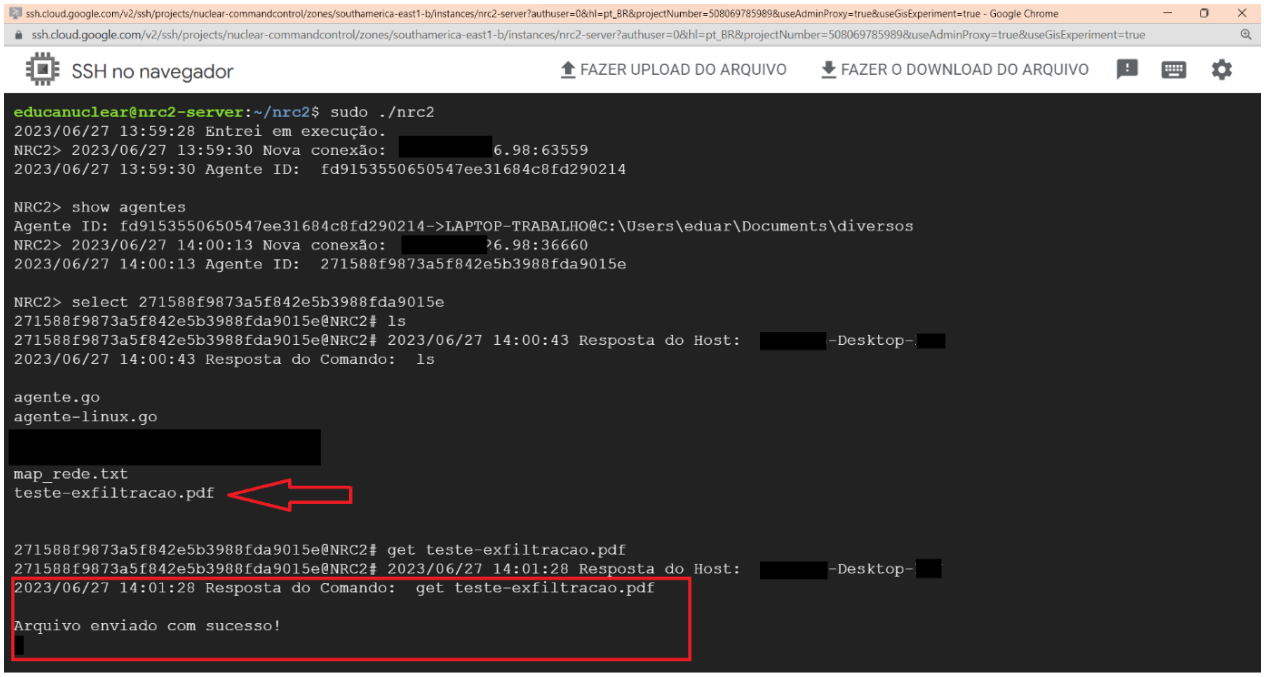


Figura 34: Exfiltração de arquivo do agente Linux para o C2
Fonte: O autor (2023)

No primeiro momento foram considerados os aspectos de se construir uma imagem de uma empresa fictícia chamada EducaNuclear, e por conseguinte, esse protótipo deveria ser o mais próximo possível da realidade que pudesse passar despercebido, inclusive para os profissionais mais experientes da área de Tecnologia da Informação.

Prosseguindo com a concepção desse objeto empírico, foi possível utilizar essa metodologia para realizar todos os testes de simulação de um ataque cibernético direcionado, utilizando como vetor inicial a engenharia social (*phishing*) direcionada aos funcionários de em um instituto de pesquisa do setor nuclear. É importante mencionar que este modelo foi utilizado para testar a resistência cibernética dessa infraestrutura crítica contra os ataques de *phishing*.

Esses testes envolveram diversas ações como: a coleta de informações em fontes abertas, a aquisição de domínios reais, a hospedagem e desenvolvimentos de Website, criação de caixas de correios personalizadas, o envio dos e-mails de *phishing*, a criação de máquinas virtuais na nuvem do Google (GCP) e na Amazon (AWS), a utilização de técnicas de intrusão usando o sistema operacional Kali Linux, a análise de logs, a instalação de um servidor C2, a compilação dos agentes para se comunicarem com o C2, a utilização de técnicas de exploração de vulnerabilidades

com ferramentas nmap, shodan, , com o propósito de avaliar a capacidade de resistência a esses ataques, principalmente em relação ao fator humano.

Dessa forma, o emprego de um servidor de Comando e Controle reforça a tese de que por mais que uma organização se mantenha em conformidade com as normas, políticas e tecnologias, o fator humano sempre será a primeira barreira necessária para evitar a propagação de um ataque direcionado.

4. RESULTADOS E DISCUSSÕES

Nessa seção, são apresentados os resultados na mesma sequência em que foi aplicada a metodologia.

4.1 Resultados da etapa de Reconhecimento

Durante a fase de reconhecimento, foram realizadas diversas técnicas de coleta de endereços de e-mail da instituição alvo. Inicialmente, foi utilizado o buscador Google por meio de palavras-chave específicas relacionadas ao domínio da organização (*****.gov.br). Essas buscas resultaram em **29 endereços de e-mail**.

Para ampliar a quantidade de endereços de e-mail, foram utilizadas ferramentas especializadas, como o theHarvester e o *framework* OSINT. O theHarvester, disponível no sistema operacional Kali Linux, retornou **5 endereços de e-mail** relevantes para o contexto.

O *framework* OSINT foi utilizado em conjunto com as ferramentas Hunter.io e Skymem.info. A ferramenta Hunter.io retornou um total de **125 endereços de e-mail** associados à instituição alvo. Já o Skymem.info forneceu uma lista mais abrangente, contendo **159 endereços de e-mail**.

Com base na quantidade de endereços de e-mail listados, conforme a Tabela 9, a decisão foi utilizar os endereços fornecidos pelo Skymem.info, pois abrangiam uma quantidade maior de funcionários da organização alvo. Dessa forma, seria possível alcançar mais pessoas pelo envio de e-mails *phishing*.

Tabela 9: E-mails encontrados em fontes abertas

Ferramentas/recursos utilizados	Quantidade de E-mails encontrados
theHarvester	5
Google Dorks	29
Hunter.io	125
Skymem.info	159

A Figura 35 ilustra um gráfico contendo a distribuição dos endereços de e-mail coletados ao longo das diferentes etapas do processo de reconhecimento, destacando

a contribuição de cada ferramenta utilizada. Esses resultados forneceram *insights* valiosos para entender a superfície de ataque e a exposição dos endereços de e-mail da instituição alvo. Cabe ressaltar que as ações descritas foram conduzidas exclusivamente para fins de testes e demonstrações, de acordo com as políticas de segurança, privacidade e as autorizações necessárias.

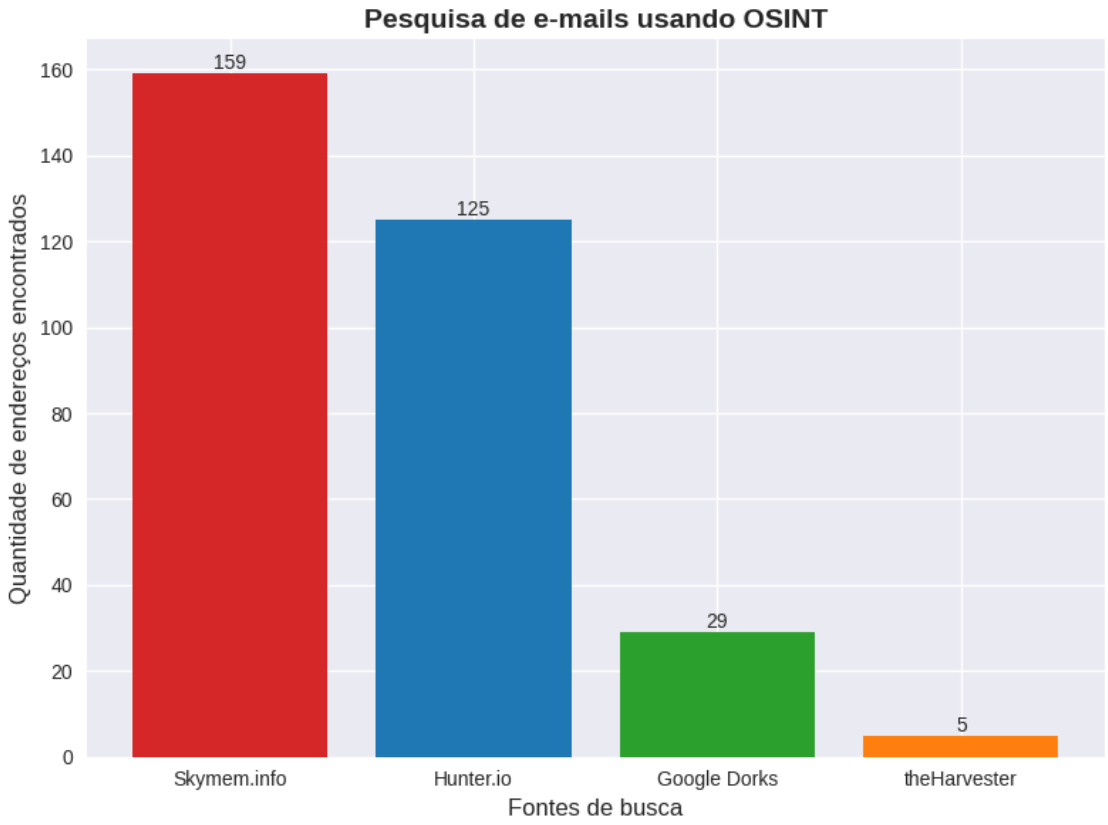


Figura 35: Comparativo de e-mails encontrado pelas buscas
Fonte: O autor (2023)

A coleta de e-mails pode ter um impacto significativo na segurança e privacidade da instituição-alvo. Ao obter uma lista de endereços de e-mail, cibercriminosos podem realizar ataques de *phishing* direcionados, tentando enganar os usuários para que revelem informações confidenciais, como senhas e dados bancários ou a instalar *malware* em seus dispositivos.

É essencial que as organizações estejam cientes dessas práticas e adotem medidas de segurança adequadas, como a conscientização dos funcionários, políticas de privacidade sólidas, controle de acesso

Por outro lado, é fundamental que as pessoas, os profissionais de TI e as organizações em geral adotem as devidas precauções para evitar que listas de e-mails caiam nas mãos de criminosos. É importante adotar práticas de segurança adequadas, conforme prescreve a ABNT NBR ISO/IEC 27701:2019:

- **Treinamento de conscientização em segurança:** Educar os funcionários sobre as melhores práticas de segurança cibernética, incluindo a importância de proteger as listas de e-mails.
- **Políticas de privacidade e consentimento:** Garantir que sua organização siga políticas de privacidade adequadas e obtenha o consentimento explícito dos indivíduos antes de incluir seus e-mails em uma lista.
- **Monitoramento e detecção:** Implementar sistemas de monitoramento e detecção de atividades suspeitas nos sistemas que armazenam as listas de e-mails.
- **Criptografia:** Utilizar a criptografia para proteger os dados sensíveis, incluindo as listas de e-mails.
- **Acesso restrito:** Limitar o acesso às listas de e-mails apenas a pessoas autorizadas.
- **Proteção de senha:** Utilizar senhas fortes e complexas para proteger os sistemas e bancos de dados que armazenam as listas de e-mails.
- **Atualizações de segurança:** Manter os sistemas e softwares atualizados com as últimas correções de segurança.

Além disso, é fundamental ter conhecimento acerca dos procedimentos para solicitar a remoção de conteúdos indexados em sites de pesquisa e outras bases de dados, caso seja necessário, de acordo com a Lei Geral de Proteção de Dados (LGPD, 2018). Cabe ressaltar que esses procedimentos podem variar entre os detentores de base de dados, sendo necessário que o titular dessas informações faça a solicitação diretamente à empresa responsável.

4.2 Resultados da etapa de Armamento

A etapa de armamento consistia em construir a maioria dos artefatos que apoiaram a estratégia do ataque cibernético simulado, iniciando pelo ataque de

phishing, para então seguir para outros ataques e técnicas de invasão. O ataque de *phishing* é frequentemente utilizado como uma entrada inicial para comprometer a segurança de sistemas e redes (MITRE,2020). Após o sucesso do ataque de *phishing*, os atacantes irão realizar outras ações criminosas para atingirem seus objetivos.

Durante essa fase, foram desenvolvidas e preparadas, para esse trabalho de pesquisa, as ferramentas e os recursos necessários para simular um ataque cibernético seguindo o modelo Cyber Kill Chain, de acordo com a Tabela 10.

Tabela 10: Quantidade de recursos na fase armamento

Recursos/armamentos utilizados	Quantidade
Endereços de e-mails criados e utilizados	08
E-mails elaborados contendo estratégias de *phishing*	02
Criação de domínios "`.com`" e "`.com.br`"	03
Instalação de servidores virtuais na nuvem AWS e GCP	04
Criação de portfólio ilustrativo em "`.pdf`"	01
Criação do formulário de inscrição em treinamento MS Forms	01
Criação do tutorial de Instalação de programa (*malware*)	01
Provedor para hospedar o site <`www.educanuclear.com`>	01
Desenvolvimento do site Educanuclear com três páginas	01
Configuração do Webmail Titan para enviar e-mails	04
Utilização de ferramentas: Shodan e nmap	02
Criação de um diretório `/***/index.html` para registro de logs	01
Instalação do servidor web apache para compartilhar e entregar os artefatos (agentes C2)	01
Implementação do servidor C2 em uma instância Linux hospedada no Google Cloud Platform	01
Compilação de agentes do C2 em arquivos "`.exe`" e "`.bin`"	01
Sistema Operacional Kali Linux	01

A etapa de Armamento teve como resultado a seleção cuidadosa das ferramentas adequadas e dos artefatos necessários para apoiar a estratégia das outras fases do ataque simulado que foi realizado neste trabalho. Essa etapa foi de

extrema importância para criar um ambiente realista capaz de confundir os usuários e testar efetivamente as capacidades de defesa tanto do fator humano quanto dos recursos tecnológicos.

É importante lembrar que o objetivo do ataque simulado não é apenas testar a capacidade de defesa do fator humano e tecnológico, mas também aprender com os resultados e implementar melhorias para fortalecer a postura de segurança da organização (MITRE, 2020).

4.3 Resultados da etapa de Entrega

Na metodologia desta dissertação, essa etapa foi subdividida em duas entregas distintas. Primeiramente, houve a entrega do e-mail de *phishing* e, posteriormente, o resultado da entrega do *software* malicioso, conhecido como agente do C2 (Command and Control). Essas entregas representam resultados diferentes, pois a entrega do *malware* simulado foi realizada em um ambiente controlado, com o propósito de avaliar sua efetividade, e não para verificar quantas pessoas estariam suscetíveis a esse tipo de ataque.

No contexto de testes de *phishing* autorizados, foi realizado um estudo com o objetivo de avaliar a eficácia de uma campanha de *phishing* simulada. Nesse estudo, foram coletados os e-mails por meio de técnicas de OSINT durante a fase de reconhecimento. O teste consistiu no envio de e-mails para uma lista específica de destinatários, conforme (Tabela 11), com o intuito de avaliar o comportamento dos usuários em relação à abertura dos e-mails, cliques em links e interações subsequentes. Os e-mails enviados direcionam os usuários para um site específico, cujos acessos foram registrados por meio do log do servidor web apache.

Tabela 11 – Métricas obtidas no teste de *phishing*

Métrica	Valor
E-mails enviados	159
E-mails entregues	92
E-mails rejeitados	67
E-mails abertos e com clique	17

Ao analisar os resultados do teste de *phishing* (ataque simulado), observou-se que do total de 159 e-mails enviados, 92 foram entregues com sucesso, 67 foram rejeitados, retornando às respectivas caixas e 17 foram abertos e tiveram o link do e-mail clicado pelos destinatários. Desses valores, podemos obter outras porcentagens importantes sobre esse estudo.

É importante destacar que a porcentagem de entrega dos e-mails durante o teste de *phishing* realizado nesta dissertação poderia ter sido potencialmente maior, caso fosse aplicado por meio de uma lista de endereços de e-mails válidos fornecidos diretamente pela instituição alvo. Assim, a maioria dos e-mails enviados provavelmente teria sido considerada válida e entregue aos destinatários, uma vez que os endereços seriam provenientes da própria organização.

No entanto, é fundamental destacar que o objetivo deste trabalho foi simular um ataque real efetuado por um hacker externo, com o intuito de avaliar a segurança e a capacidade de defesa da organização alvo em relação ao fator humano e aos recursos tecnológicos empregados. Dessa forma, a estratégia adotada foi enviar os e-mails para uma lista de endereços de e-mails obtidos através de pesquisas em fontes abertas, representando, assim, um cenário o mais próximo de um ataque real.

O foco principal desse teste de *phishing* autorizado foi avaliar a preparação e a resposta da organização, baseando-se em pessoas e tecnologias, em relação a esse tipo de ataque. Isso incluiu analisar a conscientização dos usuários em relação às práticas seguras de e-mail, a eficácia dos filtros e os mecanismos de detecção de ameaças, bem como a resposta e mitigação adequadas diante de tentativas de *phishing*.

Portanto, o objetivo deste trabalho foi justamente simular um ataque real na perspectiva de um atacante externo, mesmo sabendo que a porcentagem de entrega dos e-mails poderia ter sido maior se utilizássemos uma lista de endereços válidos fornecidos pela instituição-alvo. O foco estava na avaliação da segurança e da capacidade de defesa da organização-alvo, desde a sua preparação até a concepção, com o intuito de identificar possíveis vulnerabilidades e fornecer recomendações para o fortalecimento da segurança cibernética.

Porcentagem de entrega

A porcentagem de entrega pode ser calculada como a proporção de e-mails entregues em relação ao total de e-mails enviados. A porcentagem de entrega é uma métrica importante em testes de *phishing* que indica a proporção de e-mails enviados que são efetivamente entregues aos destinatários.

$$Percentual\ de\ entrega\ = \left(\frac{Nº\ de\ emails\ entregues}{Total\ de\ emails\ enviados} \right) * 100$$

Nesse caso, o resultado da **porcentagem de entrega foi 92/159 ≈ 0.5786 ou 57.86%.**

Porcentagem de Sucesso (ou percentual de cliques)

A porcentagem de cliques é calculada dividindo o número de usuários que clicaram em um link no e-mail pelo total de e-mails entregues. Ela mede a porcentagem de usuários que interagiram com o conteúdo do e-mail, clicando em um link específico.

$$Porcentagem\ de\ cliques\ = \left(\frac{Nº\ de\ emails\ de\ cliques}{Total\ de\ emails\ entregues} \right) * 100$$

A porcentagem de sucesso do teste de *phishing* foi calculada em relação aos e-mails entregues. Considerando o número de e-mails abertos e com clique (17) e o total de e-mails entregues (92), **a porcentagem de sucesso foi de aproximadamente 18,48%.**

Porcentagem de rejeição

A porcentagem de rejeição é calculada dividindo o número de e-mails que foram devolvidos (rejeitados) pelo total de e-mails enviados. Isso pode ocorrer quando o servidor de destino não consegue entregar o e-mail devido a problemas técnicos, como um endereço de e-mail inválido ou uma caixa de correio cheia.

$$Porcentagem\ de\ rejeição\ = \left(\frac{Nº\ de\ emails\ rejeitados}{Total\ de\ emails\ enviados} \right) * 100\%$$

A porcentagem de rejeição pode ser calculada como a proporção de e-mails rejeitados em relação ao total de e-mails enviados. Nesse caso, **o resultado da porcentagem de rejeição foi 67/159 ≈ 0.4214 ou 42.14%.**

Porcentagem de abertura sem clique

Devido à alta porcentagem de rejeição durante o teste de *phishing* autorizado, ou seja, o grande número de e-mails que retornaram para as caixas de envio, é importante destacar que **a quantificação precisa dessa porcentagem não foi possível avaliar**. Isso ocorre porque o provedor de e-mail interpretou os e-mails enviados como possíveis mensagens de spam e deixando de registrar no cliente de e-mail as informações sobre essas entregas e aberturas.

É importante ressaltar que a limitação mencionada anteriormente está relacionada à verificação dos e-mails abertos e não clicados, e não reflete necessariamente a eficácia do ataque de *phishing* em si. A métrica dos cliques, por sua vez, foi registrada por meio do servidor web independente do serviço de e-mail, utilizando logs de acesso a uma página de URL específica disponível apenas pelos links dos e-mails enviados. Por outro lado, a métrica para validação de abertura era registrada pelos clientes de e-mail e em determinado momento parou de funcionar.

Essa seria uma porcentagem interessante, pois poderia evidenciar a quantidade de pessoas que abriram o e-mail, mas não clicaram no link. Porém, como o escopo da pesquisa refere-se a possibilidade de um atacante ingressar em uma estrutura tecnológica através do envio de e-mail *phishing*, o que mais interessava eram os cliques nos links.

Outras informações

Durante a fase de entrega dos e-mails, houve uma pessoa que respondeu ao e-mail recebido e outra que preencheu o formulário de inscrição disponível no site para o qual o link direcionava. Essas interações demonstram a existência de usuários suscetíveis a ataques de *phishing* e a importância de conscientizar e educar os usuários sobre os riscos associados a e-mails maliciosos.

Representação dos resultados desta etapa

Após realizar os cálculos, foram gerados um gráfico e uma tabela representativa que retratam os percentuais de entrega, rejeição e abertura dos e-mails. Esses dados fornecem uma visualização clara e objetiva das proporções de cada categoria, permitindo uma análise mais detalhada dos resultados obtidos, conforme representado na Tabela 12.

Tabela 12 - Resultado do teste de acordo com a entrega durante um período

	Dia 1 (06 jun 2023)	**Dia 2** (07 jun 2023)	**Dia 3** (08 jun 2023)
E-mails entregues	159	0	0
E-mails rejeitados	67	0	0
E-mails abertos e com clique no link	12	5	0

Após a minuciosa análise dos logs de acesso e os dados documentados na Tabela 12, foi observado que, do terceiro dia até o oitavo dia após o início do teste de *phishing*, não foram mais evidenciados quaisquer registros de acesso originados da instituição alvo testada

A Figura 36 refere-se à distribuição dos resultados do teste de *phishing*. O eixo vertical representa a quantidade de e-mails, enquanto o eixo horizontal indica as categorias correspondentes. Essa representação proporciona uma visualização mais clara e comparativa das diferentes porcentagens de entrega, rejeição e abertura dos e-mails (clicados), permitindo uma análise mais precisa dos resultados obtidos

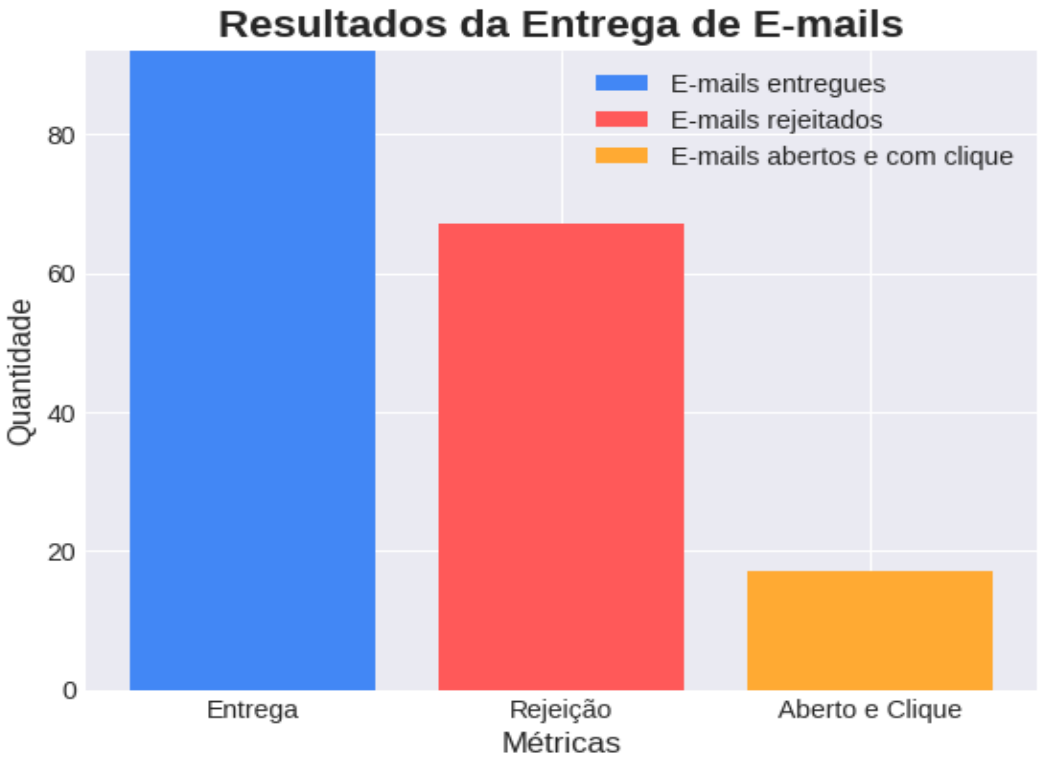


Figura 36: Resultado da Entrega de E-mails
Fonte: O autor (2023)

Modelo das informações registradas no log do servidos apache

De acordo com a RFC 2616, o log de conexão do servidor web apache registra informações importantes sobre as interações entre o servidor e os clientes que acessam um site. Ele inclui o endereço IP do cliente, data e hora da solicitação, método HTTP (como GET ou POST), URL solicitada, código de status da resposta, tamanho da resposta e agente do usuário. Essas informações são úteis para análise de tráfego, diagnóstico de problemas, segurança e desempenho do site. O log de conexão é uma ferramenta fundamental para o monitoramento e análise do tráfego do site hospedado no servidor Apache.

Os campos de logs do apache são dispostos linha a linha no arquivo access.log do servidor e são registrados em tempo real, à medida que cada conexão for sendo estabelecida, ou seja, a cada click no link informado no corpo do e-mail, esse arquivo é acrescido de linha. Os campos compreendem as informações contidas no Quadro 2:

```
200.20.***.*** - - [06/Jun/2023:12:45:10 -0300] "GET /nie/index.html HTTP/2.0"
200 43462 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36" www.educanuclear.com
```

Quadro 2: Registro de uma conexão no servidor web

Para entender melhor os resultados desta etapa, é de suma importância como funcionam os logs. Os campos apresentados são comumente localizados a cada linha criada no log do servidor apache. Esses campos podem variar dependendo da configuração do servidor e das opções de registro selecionadas, conforme descritos na Tabela 13.

Tabela 13: Identificação dos campos do log do Apache

Campo	**Informação contida**	**Explicação**
1º	Endereço IP da origem	Neste exemplo, o endereço IP do cliente é "200.20.***.*8". É o endereço IP da máquina que fez a solicitação ao servidor.
2º	Identificação do Cliente	O campo de identificação do cliente (geralmente indicado por "-") é usado para autenticação de identidade do cliente, mas pode estar vazio ou não ser utilizado.
3º	Nome de usuário	O campo de nome de usuário (geralmente indicado por "-") é usado para autenticação do usuário, mas pode estar vazio ou não ser utilizado.
4º	Data e Hora	A data e a hora em que a solicitação foi feita são exibidas entre colchetes. Neste exemplo, a data e hora são [06/Jun/2023:12:45:10 -0300]
5º	Método HTTP	O método HTTP usado na solicitação é exibido entre aspas duplas. Neste exemplo, o método é "GET", indicando que foi uma solicitação de obtenção de dados.
6º	URL Solicitada	A URL solicitada pelo cliente é exibida após o método HTTP. Neste exemplo, a URL solicitada /***/index.html

7º	Versão do HTTP	A versão do protocolo HTTP usada na solicitação é exibida após a URL. Neste exemplo, a versão é "HTTP/2.0".
8º**)**	Código de Status HTTP	O código de status HTTP retornado pelo servidor é exibido após a versão HTTP. Neste exemplo, o código de status é "200", indicando que a solicitação foi bem-sucedida.
9º	Tamanho da Resposta	O tamanho da resposta enviada pelo servidor é exibido após o código de status. Neste exemplo, o tamanho da resposta é "43462" bytes.
10º	Referer	O campo "Referer" exibe a página de origem que levou o cliente a fazer a solicitação atual. Neste exemplo, o campo está preenchido com "-", indicando que a informação não está disponível.
11º	User-Agent	O campo "User-Agent" (ou agente do usuário) exibe informações sobre o navegador ou o agente de usuário utilizado pelo cliente para fazer a solicitação. Neste exemplo, é exibido o User-Agent do navegador Chrome.

O Quadro 3 representa um trecho da captura extraída do log durante um período.

```
179.190.108.7 - - [06/Jun/2023:12:50:19 -0300] "GET /nie/index.html HTTP/1.1" 200 43462 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.0.0 Safari/537.36" www.educanuclear.com 69.49.241.24
200.20.***.*** - - [06/Jun/2023:13:52:54 -0300] "GET /nie/index.html HTTP/2.0" 200 43462 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36" www.educanuclear.com 69.49.241.24
177.26.82.137 - - [06/Jun/2023:13:54:31 -0300] "GET /nie/index.html HTTP/2.0" 200 43462 "-" "Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Mobile Safari/537.36" www.educanuclear.com 69.49.241.24
200.20.***.*** - - [06/Jun/2023:14:09:24 -0300] "GET /nie/index.html HTTP/2.0" 200 43462 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/113.0" www.educanuclear.com 69.49.241.24
40.77.167.108 - - [06/Jun/2023:16:00:01 -0300] "GET /robots.txt HTTP/2.0" 200 68 "-" "Mozilla/5.0 AppleWebKit/537.36 (KHTML, like Gecko; compatible; bingbot/2.0; +http://www.bing.com/bingbot.htm) Chrome/103.0.5060.134 Safari/537.36" www.educanuclear.com 69.49.241.24
187.67.203.44 - - [06/Jun/2023:20:36:35 -0300] "GET / HTTP/2.0" 200 43462 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36" www.educanuclear.com 69.49.241.24
187.67.203.44 - - [06/Jun/2023:20:37:22 -0300] "GET /portfolio.pdf HTTP/2.0" 200 3342221 "https://www.educanuclear.com/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36" www.educanuclear.com 69.49.241.24
```

Quadro 3 – Captura dos logs de acesso

Com base no Quadro 3, foram extraídas informações que possibilitaram obter os resultados apresentados:

No registro de acessos acima, temos que na 1ª, 2ª, 3ª e 4ª linha foram realizados acessos de origens distintas (IPs de origem) 179.190.108.7, 200.20.***.***, 177.26.82.37 e 200.20.***.*** novamente. Foi verificado que existem endereços IPs repetidos ao longo do arquivo de Logs. Porém isso não significa tratar-se do mesmo acesso, isto é, do mesmo usuário final. Analisando cuidadosamente cada linha, campo a campo, e comparando-as com as demais, podemos perceber algumas diferenças importantes relacionadas ao IP 200.20.***.***.
O primeiro acesso listado na captura ocorreu em `[06/Jun/2023:13:52:54 -0300]`, já o segundo acesso desse mesmo endereço ocorreu em `[06/Jun/2023:14:09:24 -0300]`.

Continuando a análise dos registros, ainda correlacionando esses dois acessos, da 2ª e 4ª linha, é possível observar que um acesso foi proveniente de um User-Agent utilizando um SO `(Windows NT 10.0; Win64; x64)` e outro acesso teve origem através de um SO `(X11; Ubuntu; Linux x86_64; rv:109.0)`, onde o X11 representa um sistema operacional Linux com interface gráfica.

Encerrando a análise desses dois registros de acesso, é possível identificar que um está utilizando o navegador Chrome e o outro o navegador Firefox. Resta a seguinte pergunta: Caso os dois acessos fossem em horários distintos, porém os logs apontassem para o mesmo endereço IP de origem, o mesmo sistema operacional e o mesmo navegador, podeíamos afirmar que se trata de um acesso originado pelo mesmo *endpoint*? Resposta: Não.

Em continuidade ao trecho de log, na 3ª linha identifica-se o IP de origem `177.26.82.137` e o User-Agent possui a informação referente a um sistema operacional `Android 10`, indicando referir-se a um dispositivo móvel.

Na 5ª linha nota-se uma diferença na composição do acesso e do User-Agent.

```
40.77.167.108 - - [06/Jun/2023:16:00:01 -0300] "GET /robots.txt HTTP/2.0" 200
68 "-" "Mozilla/5.0 AppleWebKit/537.36 (KHTML, like Gecko; compatible;
bingbot/2.0; +http://www.bing.com/bingbot.htm)
```

O "Bingbot/2.0" é um User-Agent utilizado pelo Bingbot, um *crawler web* do mecanismo de busca Bing, da Microsoft. O Bingbot é responsável por rastrear e indexar páginas da web para inclusão nos resultados de pesquisa do Bing.

De acordo com (Bing Webmaster Guidelines), quando o Bingbot visita um site, ele envia o User-Agent "Bingbot/2.0" como parte do cabeçalho HTTP para identificar-se como um agente do Bingbot. Essa informação permite que os proprietários de sites acompanhem a atividade do Bingbot em seus registros de servidor e ajuda a distinguir as solicitações feitas pelo bot de outras solicitações de usuários reais.

A presença do User-Agent "Bingbot/2.0" em registros de servidor pode indicar que o Bingbot está visitando e rastreando o conteúdo de um site. É importante que os proprietários de sites estejam cientes das visitas do Bingbot para garantir que suas páginas sejam adequadamente rastreadas e indexadas pelo Bing, o que pode ajudar a melhorar a visibilidade e a classificação nos resultados de pesquisa do Bing.

Os arquivos de logs são de suma importância para ajudar a identificar evidências de atacantes, das ferramentas utilizadas, principalmente informações de horários/datas de quando ocorreram os ataques e as tentativas. Essas informações são úteis e podem servir de parâmetros para aumentar a segurança cibernética de alguns servidores.

Com base nos resultados obtidos, pode-se concluir que a campanha de *phishing* simulada obteve uma porcentagem de sucesso moderada.

Esses resultados fornecem *insights* valiosos para o aprimoramento de estratégias de segurança cibernética e podem servir como base para a implementação de treinamentos e políticas de conscientização para os usuários, com o objetivo de reduzir a vulnerabilidade organizacional a ataques de *phishing*.

É importante ressaltar que os testes de *phishing* realizados devem ser autorizados e conduzidos dentro de um ambiente controlado, com o objetivo de melhorar a segurança e promover a conscientização, sem causar danos ou violar a privacidade dos usuários.

4.4 Resultados da etapa de Exploração

A etapa de exploração do ataque simulado teve como resultado mais significativo a realização de um exercício simulado, no qual exploramos uma estação Linux conectada à internet (representando a rede de Tecnologia da Informação). Por meio dessa estação, conseguimos explorar o ambiente de um servidor que atua como simulador, ambiente de TO, e teoricamente não possui acesso à internet. Esse tipo de progressão do ataque, conhecido como movimentação lateral, foi observado, conforme descrito anteriormente. Essas técnicas podem aproveitar dispositivos e sistemas *dual-homed* que residem nas redes de TI e TO (MITRE ATT&CK, 2023).

Essa etapa proporcionou *insights* valiosos sobre as vulnerabilidades presentes no ambiente simulado e destacou a importância de implementar medidas de segurança eficazes para prevenir a movimentação lateral e proteger a rede contra os ataques desse tipo.

Conforme mencionado por Branquinho (2021), o sucesso ou fracasso desse tipo de ataque está diretamente relacionado às soluções de segurança implementadas no ambiente, especialmente a adoção de uma abordagem de defesa em camadas. Nesses casos, fica evidente a necessidade de implementar um firewall adicional entre a rede de TI e a rede de automação, além do uso de soluções complementares de segurança específicas para a planta industrial (BRANQUINHO, 2021).

A implementação de um firewall adicional entre as redes de TI e de automação é uma medida eficaz para impedir a movimentação lateral e restringir o acesso não autorizado aos sistemas críticos da planta industrial (MITRE). Essa camada adicional de segurança contribui para a proteção dos ativos industriais e a mitigação dos riscos relacionados aos ataques cibernéticos.

4.5 Resultados da etapa de Instalação

Essa etapa de Instalação, em casos práticos ocorre logo após a fase de Entrega, pois nesse caso, há um contexto prévio envolvendo o ataque que encoraja os usuários executarem o *malware* achando tratar-se de um *software* legítimo.

Após a instalação do *malware*, caracterizado nesse estudo como um agente do C2 multiplataforma, desenvolvido para Windows e para Linux, o invasor realizará outras ações.

Como resultado desta etapa, podemos inferir que a instalação/execução simulada do *malware* ocorreu em ambiente controlado com resultados satisfatórios com relação às ações ofensivas.

Foi observado que a execução do agente, tanto no Windows quanto no Linux, quando disponibilizado fisicamente através de uma mídia UBS, ocorria sem alertar os controles protetivos das estações de trabalho.

Já a tentativa de execução a partir do envio do arquivo “agente.exe” por e-mail foram bloqueados pelos controles de compartilhamento de arquivos suspeitos. Cabe ressaltar que foi realizada uma pesquisa exploratória prévia para verificar quais portas estavam abertas no *firewall* da instituição alvo, sendo verificadas apenas a portas 443 e 541 abertas.

Em continuidade, o servidor C2 foi configurado para escutar na porta 443, dificultando ainda mais a detecção e bloqueio por parte de algum *firewall.*

Para mitigação desse tipo de ameaças, pode ser utilizado a implementação de controles do tipo DPI (*Deep Packet Inspection*), ou seja, inspeção profunda de pacotes que consiste em uma medida importante para fortalecer a segurança cibernética de uma organização (FORTINET, 2023). Segundo a empresa Fortinet (2023), esse recurso envolve a análise minuciosa dos pacotes de dados que transitam em uma rede, permitindo uma visão mais detalhada do tráfego de rede e identificação de potenciais ameaças.

É importante ressaltar que a organização não está desprotegida; no entanto, o tipo de Comando e Controle utilizado possui a característica de evasão de defesas, o que torna crucial que a equipe de segurança humana seja capaz de interromper esses ataques sofisticados desde o início. A atuação dos profissionais de segurança desempenha um papel fundamental na detecção precoce e no combate efetivo a essas ameaças evasivas.

4.6 Resultados da etapa de Comando e Controle

Essa etapa de comando e controle atingiu o objetivo desejado para este trabalho. Conforme descrito em Varonis (2021), a maioria das organizações tem defesa de perímetro eficaz, tornando difícil um atacante iniciar uma conexão da internet para a rede interna sem ser detectado. No entanto, essa dissertação utilizou a metodologia sob a hipótese de ingressar dentro da rede interna utilizando um

contexto de que havia uma parceria para treinamento em segurança cibernética para instalações nucleares com o instituto alvo. Sendo o tema de grande relevância, certamente haveria alguém interessado. Com esses recursos montados, bastava solicitar aos que se mostraram interessados em realizar o treinamento em uma ocasião anterior para que realizassem a instalação de um software que seria utilizado para emulação do treinamento. Com a instalação do software, esse objetivo dessa etapa foi concluído.

Uma vez que as conexões de saída não são fortemente monitoradas na maioria das instituições, após simular a introdução do *malware* por meio de um canal diferente, um *phishing* ou uma mídia USB, torna-se possível estabelecer uma conexão de saída para o C2 através de portas conhecidas.

Identificar o tráfego de Comando e Controle (C2) pode ser uma tarefa notoriamente desafiadora, uma vez que os invasores se esforçam ao máximo para evitar detecção (MITRE, 2018). No entanto, os defensores têm uma oportunidade significativa, pois a interrupção do C2 pode impedir que uma infecção por malware evolua para um incidente mais grave, como uma violação de dados (VARONIS, 2021).

De fato, muitos ataques cibernéticos em larga escala foram inicialmente descobertos quando pesquisadores observaram atividades suspeitas de C2. Para detectar e interromper o tráfego de Comando e Controle temos algumas ações:

- Monitorar e filtrar o tráfego de saída.
- Correlacionar dados de várias fontes.
- *Beacons* podem ser um sinal revelador de atividade de comando e controle em sua rede.
- Coletar arquivos de log o maior número possível de fontes é vital ao procurar sinais de tráfego de comando e controle.

4.7 Resultados da etapa de Ações no Objetivo

A fase de Ações no Objetivo foi executada com sucesso, de acordo com o planejado na metodologia. Foram conduzidos testes de exfiltração de arquivos, os quais poderiam conter dados sensíveis da organização. É importante destacar que, em um ataque real, o invasor tende a permanecer por um longo período explorando o alvo até alcançar todos os seus objetivos (KLINCZAK, 2019). A persistência e a

determinação do atacante são características fundamentais em um cenário de ataque real, o que reforça a necessidade de medidas de segurança robustas e uma resposta ágil por parte da equipe de defesa cibernética (RFC 2350, 1998).

Durante o ataque simulado e a execução das ações no objetivo, foram obtidos valiosos *insights* sobre a postura de segurança da organização, identificando eventuais vulnerabilidades e pontos de melhoria. Essas informações são fundamentais para fortalecer as defesas da organização, implementar medidas corretivas e adotar boas práticas de segurança cibernética (ABNT 27001).

Com base nos resultados e nas lições aprendidas, de acordo com NIST *Cybersecurity Framework* é possível aprimorar os protocolos de segurança, treinamentos e políticas internas, visando fortalecer a segurança organizacional diante de potenciais ataques reais.

4.8 Recomendações para melhoria segurança cibernética no setor nuclear

- Realização de programas de conscientização e treinamento contínuo para os colaboradores com a finalidade de aprimorar a identificação de ataques de *phishing* e outras técnicas de engenharia social.
- Aprimorar as tecnologias de detecção e monitoramento para identificar atividades maliciosas em estágios iniciais. Soluções como detecção de comportamento anômalo e inteligência artificial ajudam a detectar e responder a ataques de forma mais eficiente.
- Implementação de políticas de segurança mais robustas, que incluem práticas recomendadas de proteção de dados pautadas em normas técnicas e legislações vigentes ajudam a reduzir o impacto de um ataque cibernético bem-sucedido.
- Colaboração entre instituições do setor nuclear para compartilhar informações sobre ameaças cibernéticas e melhores práticas de segurança.

5. CONCLUSÃO

A presente dissertação teve como objetivo realizar um estudo de caso utilizando um ataque de phishing simulado em um instituto de pesquisa do setor nuclear brasileiro. O modelo Cyber Kill Chain foi aplicado para explorar as etapas de um ataque cibernético e avaliar o impacto causado. O estudo evidenciou a hipótese do comprometimento da segurança cibernética da instituição alvo através do acesso inicial proveniente do envio de e-mails de *phishing* para funcionários de um instituto de pesquisa.

O ataque simulado de *phishing* foi realizado em um contexto real, contemplando as etapas de reconhecimento, armamento, entrega, exploração, instalação, comando e controle, e ações no objetivo. Através do estudo de caso empregado, validou-se a hipótese de que seria possível realizar o acesso não autorizado à infraestrutura de Tecnologia da Informação (TI) e/ou Tecnologia Operacional (TO) utilizando técnicas de engenharia social, iniciando o ataque pelo envio de e-mail *phishing*.

A etapa de reconhecimento evidenciou valiosas informações sobre a organização alvo e seus colaboradores, incluindo a coleta dessas informações utilizando inteligência de fontes abertas. O ataque cibernético simulado foi aprimorado na etapa de armamento, em que foram criados artefatos convincentes e persuasivos. Já na fase de entrega, o envio de e-mails *phishing* foi bem-sucedido para boa parte dos e-mails coletados. Essa etapa teve o propósito de subsidiar a exploração de vulnerabilidades humanas e tecnológicas, sendo realizada com a autorização da direção e do setor de tecnologia de informação da organização.

A fase de exploração revelou a falta de conscientização por parte de alguns funcionários, levando-os a fornecerem informações sensíveis ou clicarem em links não confiáveis. Entre as informações sensíveis destacam-se as informações pessoais, tais como nome completo, número de identidade ou CPF, e endereço residencial. Além disso, as informações relacionadas aos aspectos tecnológicos, incluindo o endereço IP de origem, o tipo e a versão do sistema operacional utilizado, o tipo e a versão do navegador, bem como o horário em que o acesso foi realizado. Esses dados não apenas identificaram o usuário, como também permitiram diferenciar se o acesso foi realizado por um computador ou dispositivo móvel, e se originou do ambiente de

trabalho ou da residência. Essas informações forneceram *insights* valiosos para aprimorar as demais fases do ataque cibernético simulado.

Após a exploração, realizou-se um experimento em um ambiente controlado para testar a viabilidade de execução de um *malware* com a capacidade de efetuar o acesso não autorizado aos sistemas da instituição de maneira furtiva e evasiva. Isso visou simular a consequência efetiva de usuários vítimas de *phishing* que clicam em links ou arquivos maliciosos. O agente mostrou-se indetectável por soluções de antivírus e segurança de rede, viabilizando a fase de comando e controle. Durante a fase de ações no objetivo, ilustrou-se os riscos resultantes da falta de conscientização e treinamento em segurança cibernética, como: exfiltração de dados e ataques a sistemas legados sujeitos a vulnerabilidades.

Esse tipo de ataque representa grave ameaça à segurança nacional em ambientes críticos, como o setor nuclear. Isso ocorre devido ao fato de que é comum, em setores como o nuclear, o uso de sistemas legados. É importante destacar que os resultados deste estudo podem ter limitações na generalização para outras instituições do setor nuclear brasileiro ou contextos industriais diferentes, devido às peculiaridades de cada organização. O ambiente simulado e controlado utilizado, fundamentais para o caráter não-destrutivo deste trabalho, também limita a extrapolação direta dos resultados para situações reais e devem ser considerados com a devida cautela.

O nível de conhecimento dos funcionários sobre ameaças cibernéticas pode influenciar o sucesso do ataque de *phishing*, variando em casos com funcionários mais ou menos treinados. Além disso, o modelo adotado, o Cyber Kill Chain, pode ter suas próprias limitações, e outras questões técnicas específicas podem ter impactado os resultados do estudo.

Após a conclusão desse estudo de caso e dos resultados obtidos, retomamos aos objetivos específicos, em que foram descritos os principais incidentes cibernéticos e ameaças às infraestruturas críticas a que as instituições estão sujeitas, bem como a realização combinada de técnicas de engenharia social com técnicas de segurança ofensiva que objetivaram verificar as lacunas referentes aos fatores humanos e aos recursos tecnológicos. Sendo assim, propomos melhorias na segurança cibernética que possam fortalecer os recursos de segurança cibernética e mitigar ataques direcionados, como o realizado nesse trabalho.

Como indicado na literatura, ficou evidente que não existe uma solução única que ofereça proteção eficaz. É necessário adotar uma defesa em profundidade, ou seja, defesa em camadas, para garantir a segurança e proteção de sistemas, redes, informações e ativos contra ameaças cibernéticas. A defesa em profundidade envolve a implementação de várias camadas de medidas protetivas, cada uma projetada para detectar, prevenir ou mitigar diferentes tipos de ameaças.

Algumas ações importantes que podem ser adotadas pelas organizações incluem:

- Treinamento e conscientização sobre segurança.
- Adoção de Next Generation Firewall (NGFW) com DPI (Deep Packet Inspection), capaz de monitorar parte do tráfego de entrada e saída dos equipamentos conectados à rede.
- Gerenciamento de patches, softwares antivírus, firewall, IDS, IPS, SIEM e SOC.
- Detecção avançada de malware.
- Detecção de anomalias de eventos.
- Prevenção contra perda de dados (DLP).

Sob este prisma, ressalta-se a necessidade de fortalecer os fatores humanos para enfrentar os desafios em constante evolução apresentados pelas ameaças cibernéticas. Para isso, foi disponibilizada uma cartilha de conscientização contra os principais ataques de engenharia social, direcionada ao corpo de colaboradores da instituição, a fim de mitigar os riscos potenciais desses ataques.

6. SUGESTÕES PARA TRABALHOS FUTUROS

Neste capítulo, são apresentadas as sugestões para trabalhos futuros que podem estender e aprofundar o conhecimento desenvolvido nesta pesquisa. Essas sugestões baseiam-se nos resultados e nas conclusões obtidas de acordo com o estudo de caso que foi aplicado no instituto de pesquisa do setor nuclear, bem como as possíveis lacunas ou áreas de interesse identificadas durante o estudo, podemos apontar:

6.1 Investigação de outras ameaças cibernéticas que podem impactar o setor nuclear brasileiro

Embora esta pesquisa tenha se concentrado em ataques de *phishing* juntamente com o modelo Cyber Kill Chain aplicado em instalações nucleares, há diversas outras ameaças relevantes que poderiam ser exploradas em estudos futuros. Sugere-se a investigação de ameaças como *ransoware* específico para o setor nuclear, ataques de negação de serviço (DDoS), ameaças internas. Essas investigações podem fornecer *insights* adicionais sobre a segurança cibernética em instalações nucleares e aprimorar as estratégias de defesa.

6.2 Realização de um estudo mapeando a matriz do MITRE ATT&CK para ICS como base no setor nuclear brasileiro

Como visto na literatura, as ameaças aos sistemas críticos nem sempre se originam exclusivamente da internet, como evidenciado pelo notório caso do vírus Stuxnet. Para garantir uma maior proteção desses sistemas, é essencial adquirir um conhecimento profundo das técnicas empregadas pelos atacantes nos sistemas de controle e aquisição de dados de supervisão (SCADA) e sistemas de controle industrial (ICS). Sugere-se a realização de um estudo aprofundado da matriz ICS do MITRE ATT&CK, desse modo, pesquisas futuras poderão identificar as ameaças cibernéticas atuais mais significativas que podem impactar o setor nuclear brasileiro, proporcionando valiosas percepções para o aprimoramento de medidas protetivas cibernéticas.

6.3 Medidas de proteção e defesa cibernética através da implementação de SOC e SIEM

Considerando a importância crítica da segurança cibernética em instalações nucleares, sugere-se explorar medidas adicionais de proteção e defesa cibernética. Pesquisas futuras poderão se concentrar no desenvolvimento e na avaliação de estratégias avançadas de detecção, prevenção e resposta a ataques cibernéticos.

Uma área promissora para investigação é o uso de tecnologias emergentes, como inteligência artificial e aprendizado de máquina, para aprimorar as capacidades de detecção e resposta. Outro estudo que pode ser realizado em conjunto, seria basear-se estudos em um modelo de Centro de Operações de Segurança (SOC) e de um Sistema de Gerenciamento de Eventos e Informações de Segurança (SIEM) específicos para ambientes industriais, baseados em plataformas de segurança de código aberto, como o caso do Wahzu, pode trazer benefícios significativos.

6.4 Aplicação de inteligência artificial e aprendizado de máquina para segurança cibernética no setor nuclear

Uma área promissora para pesquisas futuras é a aplicação de inteligência artificial e aprendizado de máquina na detecção proativa de ameaças cibernéticas em instalações nucleares. Algoritmos avançados poderão ser desenvolvidos para analisar padrões de tráfego (principalmente de saída), comportamentos de usuários e outros dados relevantes, a fim de identificar possíveis ameaças com antecedência e fornecer alertas precoces para ações de defesa.

REFERÊNCIAS BIBLIOGRÁFICAS

ABNT NBR ISO/IEC 27001, Segurança da informação, segurança cibernética e proteção à privacidade – Sistemas de gestão da segurança da informação – Requisitos, 2022.

ABNT NBR ISO/IEC 27002, Segurança da informação, segurança cibernética e proteção à privacidade – Controles de segurança da informação 2022

ABNT NBR ISO/IEC 27032, Tecnologia da Informação - Técnicas de segurança - Diretrizes para segurança cibernética, 2015

ABNT NBR ISO/IEC 27035-3, Tecnologia da informação - Gestão de incidentes de segurança da informação - Parte 3: Diretrizes para operações de resposta a incidentes de TIC, 2021

ABNT NBR ISO/IEC 27701, Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes, 2019

AHMED, Y.; ASYHARI, A. TAUFIQ.; ARAFATUR R., M. A Cyber Kill Chain Approach for Detecting Advanced Persistent Threats. Computers, Materials & Continua, v. 67, n. 2, p. 2497–2513, 2021.

ALABDAN, Rana, Phishing Attacks Survey: Types, Vectors, and Technical Approaches; Future Internet, 2020

ALDAWOOD, H.; SKINNER, G. Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. Future Internet, v. 11, n. 3, p. 73, 2019.

ALMUTAIRI, S., ALGHAMDI, A. "The Role of Social Engineering in Cybersecurity and Its Impact." Journal of Information Security 13.4 (2022): 363-379.

ALKHALIL, Z. et al. Phishing attacks: A recent comprehensive study and a new anatomy. Frontiers in Computer Science, v. 3, p. 563060, 2021.

ASLAN, Mostofa et al. Cybersecurity threats and their mitigation approaches using Machine Learning—A Review. Journal of Cybersecurity and Privacy, v. 2, n. 3, p. 527-555, 2022.

ASLAN, M., *et.al*. Social engineering awareness in Nuclear Malaysia. RnD Seminar 2010: Research and Development Seminar 2010, Malaysia

ALSHAMRANI, Adel et al. A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. IEEE Communications Surveys & Tutorials, v. 21, n. 2, p. 1851-1877, 2019.

ANI, U. D., HE, H., e TIWARI, A. (2018). Human factor security: evaluating the cybersecurity capacity of the industrial workforce. Journal of Systems and Information Technology. doi:10.1108/jsit-02-2018-0028

ASSANTE, M. J.; LEE, R. M. The industrial control system cyber kill chain. SANS Institute InfoSec Reading Room, v. 1, p. 24, 2015.

BAEZNER, Marie; ROBIN, Patrice. Stuxnet. ETH Zurich, 2017.

BRANQUINHO, T; BRANQUINHO, M. Segurança Cibernética Industrial. Rio de Janeiro-RJ: Altas Books, 2021

Brasil e os ataques de phishing por WhatsApp. Disponível em: <https://www.kaspersky.com.br/blog/brasil-ataques-phishing-2022/20943/>. Acesso em: 20 abr. 2023.

BRASIL. Decreto nº 10.748, de 16 de julho de 2021. Institui a Rede Federal de Gestão de Incidentes Cibernéticos. Disponível <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/D10748.htm> Acesso em: 01 set 2023.

BUIL-GIL, D. et al. Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. European Societies, v. 23, n. sup1, p. S47-S59, 2021.

CHATCHALERMPUN, S.; DAENGSI, T. Improving cybersecurity awareness using phishing attack simulation. In: IOP Conference Series: Materials Science and Engineering. IOP Publishing, 2021

CHEN, P.; DESMET, L.; HUYGENS, C.. A study on advanced persistent threats. In: Communications and Multimedia Security: 15th IFIP TC 6/TC 11 International Conference, CMS 2014, Aveiro, Portugal, September 25-26, 2014. Proceedings 15. Springer Berlin Heidelberg, 2014. p. 63-72.

CHIEW, K. L.; YONG, K. S. C.; TAN, C. L. A survey of phishing attacks: Their types, vectors and technical approaches. Expert systems with applications, v. 106, p. 1–20, 2018.

CHIEW, K. L.; YONG, K. S. C.; TAN, C. L. A survey of phishing attacks: Their types, vectors and technical approaches. Expert Systems with Applications, v. 106, p. 1-20, 2018.

CNEN/DRS/DISEN. Revisão e Elaboração de Normas Junho de 2020. Disponível em: <http://appasp.cnen.gov.br/seguranca/normas/pdf/RevNormasJun20.pdf>. Acesso em: 23 jun. 2023.

COLEMAN, G. Hacker, hoaxer, whistleblower, spy: The many faces of Anonymous. Verso books, 2015.

CYBER KILL CHAIN. Disponível em: <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>. Acesso em: 26 jun. 2023.

Desafios da Cibersegurança no Brasil. Disponível em: <https://www.cisco.com/c/dam/global/pt_br/solutions/pdfs/report1-distrito.pdf> Acesso em: 25 mai. 2023

Desec Information Security. Disponível em: <https://desecsecurity.com/curso/evasao-defesas>. Acesso em: 25 jun. 2023.

EFTIMIE, Sergiu; MOINESCU, Radu; RĂCUCIU, Ciprian. Spear-phishing susceptibility stemming from personality traits. IEEE Access, v. 10, p. 73548-73561, 2022.

Eletrobras relata ataque à Eletronuclear, mas descarta risco às usinas. Disponível em: <https://www.cisoadvisor.com.br/eletrobras-anuncia-ataque-a-eletronuclear-mas-descarta-risco-as-usinas-nucleares/>. Acesso em: 23 jun. 2023.

FAN, W.; KEVIN, L.; RONG, R. Social engineering: IE based model of human weakness for attack and defense investigations. IJ Computer Network and Information Security, v. 9, n. 1, p. 1-11, 2017.

FARWELL, James P.; ROHOZINSKI, Rafal. Stuxnet and the future of cyber war. Survival, v. 53, n. 1, p. 23-40, 2011.

GARCIA, C, GARCIA-DIAZ, V et al. Protocol and Applicattion for the Industrial Internet of Things. Hershey.IGI Global, 2018.

GALLOWAY, B.; HANCKE, G.P. Introduction to industrial control networks. IEEE Communications surveys & tutorials, v. 15, n. 2, p. 860-880, 2012.

GONÇALVES, P.; COUTINHO, F.; JAIME, G. Defacebot: Uma ferramenta de detecção e notificação de ataques de desfiguração utilizando mecanismos gerenciados por bot de aplicativo de mensagens instantâneas Uma abordagem como ferramenta de apoio ao CSIRT. In: SIMPÓSIO BRASILEIRO DE SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS (SBSEG), 2019, São Paulo. Anais. Porto Alegre: Sociedade Brasileira de Computação, 2019 . p. 445-451.

GREIMAN, V. "Nuclear Cyber Attacks: A Study of Sabotage and Regulation of Critical Infrastructure." International Conference on Cyber Warfare and Security. Vol. 18. No. 1. 2023.

GRIMMICK, R. What is C2? Command and Control Infrastructure Explained. Varonis.comVaronis,26 abr. 2021. Disponível em: <https://www.varonis.com/blog/what-is-c2>. Acesso em: 2 jul. 2023

Guia de Referência do Nmap (Página do Manual). Disponível em: <https://nmap.org/man/pt_BR/index.html>. Acesso em: 30 jun. 2023.

Hacking com Kali Linux: Técnicas Práticas Para Testes de Invasão Capa comum – 19 fevereiro 2014 Novatec

HAKIM, Ziad M. et al. The Phishing Email Suspicion Test (PEST) a lab-based task for evaluating the cognitive mechanisms of phishing detection. Behavior research methods, v. 53, p. 1342-1352, 2021.

HALEVI, T; MEMON, N; NOV, O. Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks, 2015.

HAWAMLEH, A. M. A. et al. Cyber security and ethical hacking: The importance of protecting user data. Solid State Technology, v. 63, n. 5, p. 7894-7899, 2020.

HEJASE, Hussin J.; FAYYAD-KAZAN, Hasan F.; MOUKADEM, Imad. Advanced persistent threats (apt): an awareness review. Journal of Economics and Economic Education Research, v. 21, n. 6, p. 1-8, 2020.

HP Hp-ux version 11.11 : Security vulnerabilities. Disponível em: <https://www.cvedetails.com/vulnerability-list.php>. Acesso em: 30 jun. 2023.
Incident hub. Disponível em: <https://hub.tisafe.com/>. Acesso em: 23 jun. 2023.

IAEA No. 42: Computer Security for Nuclear Security, 2021. Disponível em <https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1918_web.pdf> . Acessado em 14 mai. 2023

IAEA No. 17-T (Rev. 1): Standard for Cybersecurity in Nuclear Installations and Related Activities, 2011. Disponível em <https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf> . Acessado em 14 mai. 2023

JONH, P., HANEY, M., BORRELLI."An overview of methodologies for cybersecurity vulnerability assessments conducted in nuclear power plants." Nuclear Engineering and Design 346 (2019): 75-84.

KLINCZAK, M. Uso da Inteligência na Detecção de Ameaças Cibernéticas. In: THE ELEVENTH INTERNATIONAL CONFERENCE ON FORENSIC COMPUTER SCIENCE AND CYBER LAW. Anais. São Paulo. 2019. p. 15-22.

KNOWBE4. Security Awareness Training. Disponível em: <https://www.knowbe4.com/>. Acesso em: 26 jun. 2023.

KROMBHOLZ, K; HOBEL, H.; HUBER, M; WEIPPL, E. Advanced social engineering attacks. Journal of Information Security and applications, v. 22, p. 113-122, 2015.

KUMAR, Vikash; SINHA, Ditipriya. A robust intelligent zero-day cyber-attack detection technique. Complex & Intelligent Systems, v. 7, n. 5, p. 2211-2234, 2021.

LALLIE, H. et al. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & security, v. 105, p. 102248, 2021.

LINDSAY, Jon R. Stuxnet and the limits of cyber warfare. Security studies, v. 22, n. 3, p. 365-404, 2013.

LINNOSMAA, J., PAPAKONSTANTINOU, N., MALM, T., KOTELBA, A., & PÄRSSINEN, J.. Survey of cybersecurity standards for nuclear instrumentation and control systems. In International Symposium on Future I&C for Nuclear Power Plants, ISOFIC 2021: Proceedings Okayama University. 2021

MCA 7-1. Manual do Glossário de Segurança da Informação do Departamento de Controle do Espaço Aéreo, 2023. Disponível em <https://publicacoes.decea.mil.br/publicacao/mca-07-1>. Acesso em: 23 jun. 2023.

MITNICK, Kevin D. A Arte de Enganar: Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação. São Paulo: Editora Pearson, 2002.
OSINT Framework. Disponível em: <https://osintframework.com/>. Acesso em: 24 jun. 2023.

National Institute of Standards and Technology (NIST). NIST SP 800-82 Ver2: Guide to Industrial Control Systems (ICS) Security, 2015.
Disponível em <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf>. Acessado em 15 mai. 2023

NRC Regulatory Guide 5.71: Cybersecurity Programs for Nuclear Facilities, 2010. Disponível em <https://www.nrc.gov/docs/ML0903/ML090340159.pdf>. Acessado em 15 mai. 2023

PETERSON, J.; HANEY, M.; BORRELLI, R. A. An overview of methodologies for cybersecurity vulnerability assessments conducted in nuclear power plants. Nuclear engineering and design, v. 346, p. 75–84, 2019.

PODZINS, O.; ROMANOVS, A. Why SIEM is irreplaceable in a secure it environment?. In: 2019 Open Conference of Electrical, Electronic and Information Sciences (eStream). IEEE, 2019. p. 1-5.

Política Nacional de Segurança de Infraestruturas Críticas (PNSIC). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9573.htm>.
Acesso em: 23 jun. 2023.

POLLINI, A., CALLARI, TC, TEDESCHI, A. ET AL. Leveraging human factors in cybersecurity: an integrated methodological approach. Cogn Tech Work 24 , 371–390 (2022).
QUINTERO-BONILLA, S.; ANGEL, M. D. R. A new proposal on the advanced persistent threat: A survey. Applied Sciences, v. 10, n. 11, p. 3874, 2020.

RASTENIS, Justinas et al. E-mail-based phishing attack taxonomy. Applied Sciences, v. 10, n. 7, p. 2363, 2020.

RIZZONI, Fabio et al. Phishing simulation exercise in a large hospital: A case study. Digital Health, v. 8, p. 20552076221081716, 2022.

Relatório de Ameaças Cibernéticas da Sonicwall. Disponível em: <https://www.sonicwall.com/medialibrary/pt/infographic/2021-mid-year-update-

sonicwall-cyber-threat-report.pdf>. Acesso em: 15 mai. 2023

Relatório global de tecnologia operacional da Fortinet. Disponível em: <https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2023/fortinet-global-report-finds-75-percent-ot-organizations-experienced-intrusion-last-year>. Acesso em: 23 jun. 2023.

RISI - the Repository of Industrial Security Incidents. Disponível em: <https://www.risidata.com/Database/event_date/asc/P180>. Acesso em: 23 jun. 2023.

RFC 2350. Expectations for Computer Security Incident Response. Disponível em: <https://www.ietf.org/rfc/rfc2350.txt>. Acesso em: 3 jul. 2023.

ROWLAND, T. Computer and information security training and awareness programmes for nuclear facilities. No. SAND2020-1298C. Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), 2020.

SÁ, A. L. N.. Segurança cibernética de usinas nucleares: uma análise sobre medidas de mitigação de ataques de engenharia social na central nuclear Almirante Álvaro Alberto. 2020.

SALAHDINE, F.; KAABOUCH, N. Social engineering attacks: A survey. Future Internet, v. 11, n. 4, p. 89, 2019.

SEGUNDO, C. B. T. A defesa cibernética em ambientes de infraestrutura crítica e os riscos dos ataques cibernéticos. 2019

SILVA, B. Como encarar um cenário de pandemia cibernética? Disponível em: <https://www.securityreport.com.br/como-encarar-um-cenario-da-pandemia-cibernetica/>. Acesso em: 29 mai. 2023.

SINHA, Shivanshi; ARORA, Dr Yojna. Ethical hacking: the story of a white hat hacker. International Journal of Innovative Research in Computer Science & Technology (IJIRCST), ISSN, p. 2347-5552, 2020.

STANKOVIĆ, S.; GAJIN, S., PETROVIĆ, R. A Review of Wazuh Tool Capabilities for Detecting Attacks Based on Log Analysis.
Tabela 1 Taxonomia de erros humanos e violações https://link.springer.com/article/10.1007/s10111-021-00683-y/tables/1

TANG, B.; QIU, H. Indicators of Compromise Automatic Identification Model Based on Cyberthreat Intelligence and Deep Learning, 2022 5th International Conference on Pattern Recognition and Artificial Intelligence (PRAI), Chengdu, China, 2022, pp. 282-287

TARNOWSKI, I. How to use cyber kill chain model to build cybersecurity?. European Journal of Higher Education IT, 2017

TAVARES, R.L.A., LEMOS, F. L., SILVA, A. T., Computer Security on Brazilian Nuclear Facilities: challenges, actions, and the path forward, International Nuclear Atlantic Conference – INAC 2021

Tentativas de ataques cibernéticos no Brasil. Disponível em: <https://www.securityreport.com.br/brasil-sofreu-10316-bilhoes-de-tentativas-de-ataques-ciberneticos-em-2022/>. Acesso em: 10 mai. 2023.

Understanding the Cyber Kill Chain. Disponível em: <https://learning.oreilly.com>. Acesso em: 24 jun. 2023.

VENKATACHARY, S. K.; PRASAD, J.; SAMIKANNU, R. Economic Impacts of Cyber Security in Energy Sector: A Review. International Journal of Energy Economics and Policy, 2017, 7(5), 250-262., 2017

WRIGHTSON, T. Advanced Persistent Threat Hacking : The Art and Science of Hacking Any Organization. New York, N.Y.: Mcgraw-Hill Education, 2015.

XU, Y. et al. HGHAN: Hacker group identification based on heterogeneous graph attention network. Information Sciences, v. 612, p. 848-863, 2022.

YADAV, T.; RAO, A. M.. Technical aspects of cyber kill chain. In: Security in Computing and Communications: Third International Symposium, SSCC 2015, Kochi, India, August 10-13, 2015. Proceedings 3. Springer International Publishing, 2015. P. 438-452.

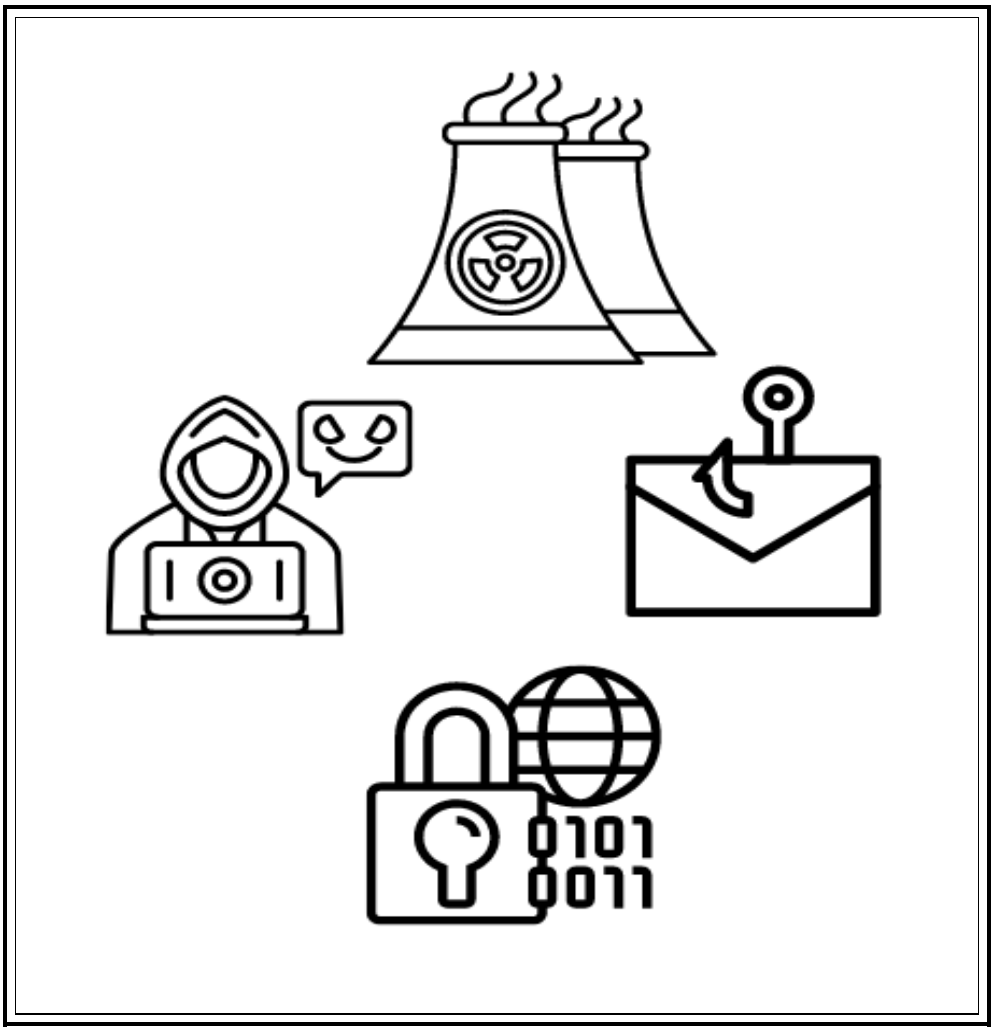
ZHANG, F.; HINES, J. W.; COBLE, J. B. A robust cybersecurity solution platform architecture for digital instrumentation and control systems in nuclear power facilities. Nuclear technology, v. 206, n. 7, p. 939–950, 2020.

ZHANG, F; HINES, J. W.; COBLE, J. B. A Robust Cybersecurity Solution Platform Architecture for Digital Instrumentation and Control Systems in Nuclear Power Facilities, Nuclear Technology, 206:7, 939-950, 2020

APÊNDICE A

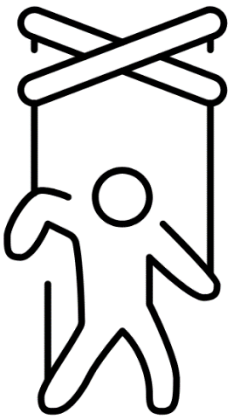
CARTILHA DE EDUCAÇÃO E CONSCIENTIZAÇÃO EM SEGURANÇA CIBERNÉTICA CONTRA OS ATAQUES DE PHISHING

“Desvendando a Engenharia Social: conheça as principais ameaças e proteja-se!"



AGOSTO 2023

O que é Engenharia Social?



A engenharia social é uma estratégia de ataque que se baseia na manipulação psicológica para levar as pessoas a cometerem equívocos.

A prática de engenharia social envolve o uso de técnicas manipulativas para alcançar determinados objetivos, muitas vezes fraudulentos ou enganosos, tais como:

a) Obter acesso não autorizado a ativos físicos e digitais de uma organização.

b) Persuadir e convencer as pessoas a realizarem procedimentos e divulgares informações confidenciais.

c) Realização de fraudes contra organizações com objetivos diversos, incluindo motivações políticas, governamentais, roubo de informações confidenciais e propriedade intelectual

Os engenheiros sociais têm como principal empreendimento instigar e influenciar erros humanos.

Vamos refletir um pouco do ponto de vista de um cibercriminoso!!

Considere a seguinte situação: um cibercriminoso deseja obter acesso a um e-mail e senha.

Qual seria a maneira mais simples desse criminoso tentar e alcançar sucesso?

Opção 1 - Hackear o computador e roubar as suas credenciais de logins.

Opção 2 - Criar uma história fictícia, muito parecida com a realiade, com o objetivo de persuadir alguém a fornecer essas informações.

Embora a Opção 1 também seja válida, os engenheiros sociais acreditam que, frequentemente, é mais simples persuadir as pessoas a fornecerem voluntariamente suas credenciais de login do que recorrer a ferramentas tecnológicas sofisticadas.

Os engenheiros sociais visam hackear os fatores humanos, não os computadores!

Principais técnicas de engenharia social mais comuns

Phishing: É uma tentativa de obter informações confidenciais, como senhas e números de cartão de crédito, por meio de e-mails, mensagens ou sites falsos que se fazem passar por entidades confiáveis.

Spear Phishing: Uma forma mais direcionada de *phishing*, em que os atacantes personalizam suas mensagens e informações para se adequarem a um alvo específico, como um funcionário de uma empresa, aumentando a probabilidade de sucesso.

Whaling: É uma forma de spear phishing direcionada a indivíduos de alto nível hierárquico em uma organização, como executivos, CEOs e diretores. O objetivo é obter informações confidenciais ou acesso privilegiado.

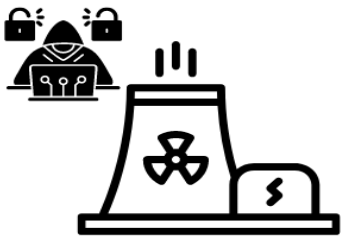
Pretexting: Nessa técnica, o atacante cria uma história fictícia ou pretexto convincente para obter informações pessoais ou confidenciais do alvo.

Burlando o Fator Humano

Por que a engenharia social consegue ter sucesso?

Muitas das vezes, estamos ocupados, cansados ou distraídos, tornando-se uma oportunidade para os cibercriminosos. Quando isso acontece, torna-se mais fácil cometer erros.

Os criminosos tentam encontrar a pessoa certa, no momento oportuno e com a história adequada. Desse modo, torna-se possível burlar o raciocínio lógico da pessoa.



No **setor nuclear**, a negligência de apenas um usuário em relação às políticas de segurança da organização pode ser suficiente para possibilitar o acesso de atacantes à sua infraestrutura.

A importância de todos os usuários aderirem rigorosamente às medidas de segurança é fundamental para proteger a integridade e a confidencialidade dos sistemas.

Alguns exemplos de como as pessoas são alvos de ataques cibernéticos e como previnir essas ações

- Os engenheiros sociais buscam coletar o máximo de informações sobre seus alvos, a fim de parecerem legítimos.
- Eles empregam técnicas persuasivas para burlar o pensamento crítico.
- Seu objetivo é nos levar a tomar decisões rápidas e agir sem considerar as consequências.
- Normalmente, suas abordagens vêm disfarçadas de ofertas atraentes, como descontos, prêmios, sorteios, entre outros.

CONFIANÇA E URGÊNCIA

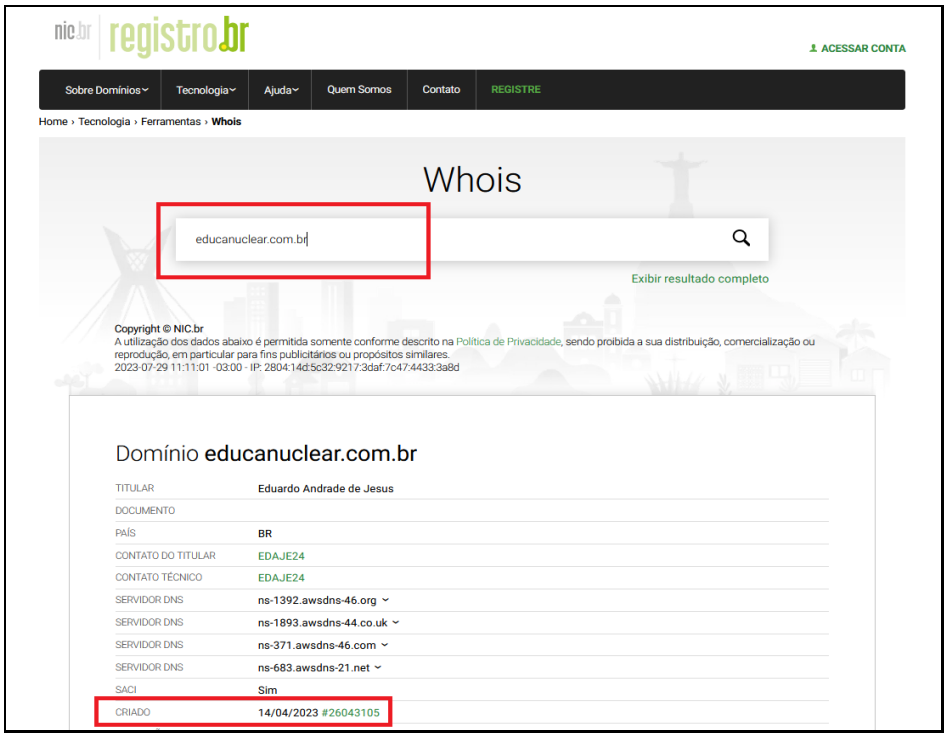
Como geralmente ocorre:

- Essa é a tática frequentemente empregada em ataques de phishing, onde os cibercriminosos buscam induzi-lo a clicar rapidamente em um link ou baixar um anexo presente em um e-mail.
- No spear phishing, os atacantes desenvolvem mensagens personalizadas para aumentar a chance de interação do alvo.

Como evitar:

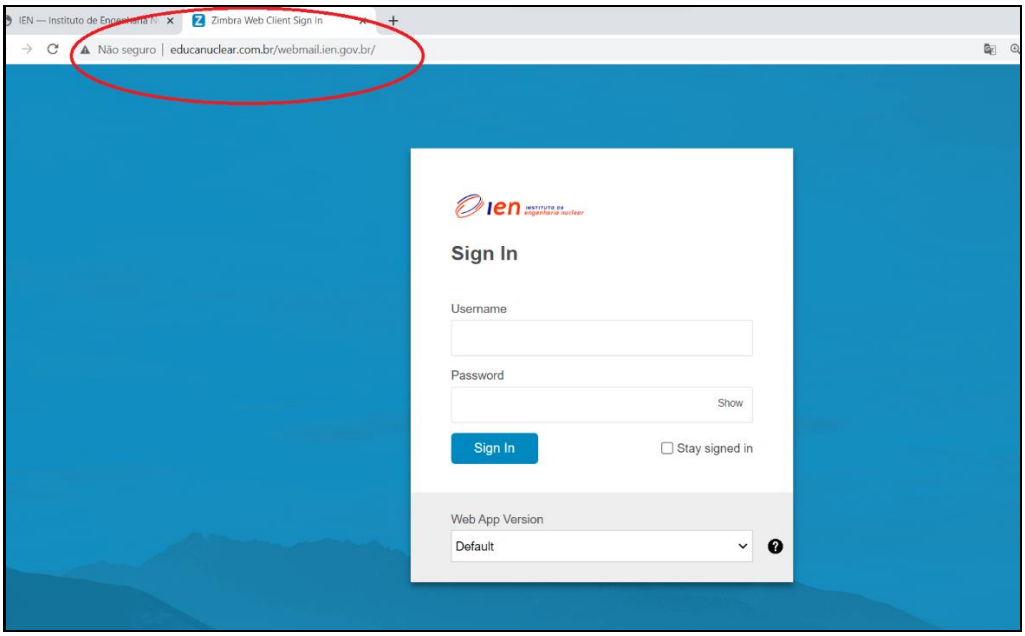
- Desenvolver um senso crítico e manter a calma ao ler qualquer mensagem de e-mail.
- Evitar clicar diretamente em links enviados no corpo do e-mail.
- Inspecionar cuidadosamente a URL para a qual o link está direcionando. Ao passar o mouse sobre o hiperlink em seu aplicativo de e-mail, será possível verificar a verdadeira URL que está oculta.
- Verificar o domínio e a presença de um certificado digital válido no site.
- Utilizar o site VirusTotal para verificar a autenticidade e possíveis ameaças associadas à URL.
- Antes de executar qualquer arquivo recebido por e-mail ou mídia USB, realizar uma inspeção adicional pelo site VirusTotal ou por um software antivírus confiável. Endereço do site: https://www.virustotal.com

- É recomendado pesquisar a data de criação dos domínios, uma vez que domínios recém-criados podem ser indícios de possíveis golpes.
- Endereço do site Whois para pesquisas de domínos “.com.br” : https://registro.br/tecnologia/ferramentas/whois/



- Endereço do site Whois para pesquisas de domínos “.com”: https://www.whois.com/whois/

- É fundamental observar com atenção os links de acesso e as solicitações de trocas de senhas em aplicativos de e-mails, a fim de assegurar a legitimidade da origem. Em alguns cenários, as páginas desses aplicativos podem ter sido clonadas. É importante verificar cuidadosamente antes de prosseguir.



MEDO E DESESPERO

Como geralmente ocorre:

- Receber uma intimação para comparecer em juízo.
- Receber um telefonema alegando que um pagamento está atrasado.
- Receber uma mensagem de texto informando que uma conta foi comprometida.
- Ser alvo de golpes durante momentos de pandemia, elevado estresse, como desastres naturais, doenças ou dificuldades financeiras.

Como evitar:

- Sempre desconfie antes de tomar qualquer ação, especialmente ao lidar com comunicações suspeitas.
- Em caso de dúvida, comunique imediatamente o setor de Tecnologia da Informação (TI) da empresa para obter orientação e verificação.
- Bloqueie e exclua imediatamente mensagens ou e-mails suspeitos que possam representar ameaças à segurança.
- Verifique se o remetente é autêntico antes de abrir links ou anexos.
- Evite fornecer informações confidenciais ou pessoais sem confirmar a legitimidade da solicitação.
- Esteja alerta durante momentos de elevado estresse, pois os cibercriminosos podem tentar se aproveitar dessas situações para aplicar golpes.

CURIOSIDADE E SIMPATIA

Como geralmente ocorre:

a) As pessoas são naturalmente curiosas, quando alguém encontra uma unidade flash USB qualquer, pode conectá-la para visualizar o seu conteúdo.
b) Essa é uma forma fácil de se infectar computadores com malware para roubo de dados.
c) Alguém se aproxima de uma entrada do escritório com as mãos ocupadas, carregando coisas. A reação simpática pode permitir que um invasor tenha acesso físico não autorizado a uma área protegida.

Como evitar:

Risco de midias USB desconhecidas:

- Evite conectar unidades flash USB de locais públicos ou desconhecidos, pois podem conter malware.
- Use unidades flash de fontes confiáveis e verifique o conteúdo com software antivírus antes de abrir os arquivos.

Ameaça de malware através de dispositivos USB:

- Cibercriminosos podem deixar unidades flash USB maliciosas em áreas estratégicas para atrair vítimas.
- Conscientize os funcionários sobre os riscos e proíba o uso de dispositivos desconhecidos nos computadores da empresa.

Ação de invasores utilizando engenharia social:

- Invasores podem se passar por entregadores, funcionários de limpeza ou visitantes para obter acesso não autorizado.
- Implemente procedimentos rigorosos de identificação e autorização para garantir que apenas pessoas autorizadas acessem áreas restritas.

Treinamento em conscientização sobre segurança:

- Realize treinamentos regulares para conscientizar os funcionários sobre as táticas de engenharia social e os riscos associados.
- Eduque a equipe sobre como identificar sinais de possíveis ameaças cibernéticas e como reagir em situações suspeitas.

Políticas de segurança cibernética e física:

- Estabeleça políticas claras de segurança abordando o uso de dispositivos desconhecidos e a identificação de visitantes.
- Reforce a importância do cumprimento dessas políticas para proteger a segurança geral da organização.

Proteção com softwares de segurança:

- Mantenha todos os sistemas protegidos com softwares de segurança atualizados, incluindo antivírus e firewalls.
- Faça verificações periódicas para detectar e bloquear possíveis ameaças cibernéticas.

Como se proteger dessas ameaças

A engenharia reversa é uma prática educacional pela qual analisamos minuciosamente algo para entender como foi construído ou criado. No contexto de segurança cibernética, a engenharia reversa também pode ser aplicada para entender as táticas e estratégias utilizadas pelos engenheiros sociais.

Para evitar cair em golpes de Engenharia Social, é possível aplicar um tipo de "engenharia reversa" na forma de medida preventiva:

1º) Questione tudo!

- Você conhece pessoalmente a pessoa que está entrando em contato com você?
- Qual é o motivo específico para essa pessoa entrar em contato com você?
- Por que ela precisa exatamente dessa informação que está solicitando?
- Existe alguma evidência da existência real da empresa que está entrando em contato com você?
- Antes de clicar em um link, verifique se ele é seguro e proveniente de uma fonte confiável.
- Antes de abrir um arquivo, certifique-se de que ele é seguro e não contém malware ou vírus.
- Verifique a autenticidade de um programa de capacitação ou evento antes de fornecer informações pessoais ou financeiras.
- Esteja alerta para possíveis sinais de golpes e questione qualquer solicitação suspeita que receber.

2º) Fique atento!

- Fique atento às solicitações de dinheiro ou informações confidenciais.
- Tenha cuidado com pedidos para instalar softwares de acesso remoto.
- Preste muita atenção ao contexto da situação.
- Seja extremamente cuidadoso com mensagens contendo links ou anexos.
- Mesmo que pareçam vir de alguém conhecido, seja criterioso.
- Não presuma que alguém é quem afirma ser.
- Limite o que você compartilha em mídias sociais e outros fóruns.
- Considere configurar seus perfis sociais como privados.
- Utilize o bom-senso para frustrar a maioria dos golpes.
- Mantenha a consciência situacional tanto on-line quanto na vida real.

3º) Comunique! 

- Entrar em contato com a equipe de TIC (Tecnologia da Informação e Comunicação) da organização informando o ocorrido e dar ciência aos demais membros.
- Ao receber um e-mail de phishing, telefonema suspeito ou identificar qualquer possível ameaça cibernética, relate imediatamente.
- A comunicação de ataques cibernéticos é crucial para que as organizações investiguem o ocorrido e tomem medidas para mitigar possíveis danos.

Por fim: Lembre-se!

- A maioria dos ataques cibernéticos de engenharia social tem como objetivo criar histórias convincentes e encontrar alguém vulnerável para acreditar nelas.
- Como "firewalls humanos", é nossa responsabilidade usar o bom senso, pensar antes de clicar e sempre seguir as políticas de segurança.
- Caso receba um e-mail de phishing, denuncie imediatamente para que possamos investigar a situação e alertar os outros membros da organização.

Vídeo: Principais formas de como evitar golpes de *phishing.*