

PHISHING: Estudo Empírico de Caso de Multinacional Certificada ISO 2700

*André Ricardo Saraiva¹, João Batista Lopes Coelho Júnior², Marcelo Coutinho Ribeiro³,
Mateus Barbosa Lopes⁴, Matheus Almeida de Carvalho⁵ e Victor Reis Furtado⁶*

RESUMO

Este trabalho tem como objetivo demonstrar que, mesmo nos tempos contemporâneos, quando empresas conduzem e promovem treinamentos e palestras de conscientização sobre segurança da informação, o principal obstáculo persiste sendo a falibilidade humana. O teste de segurança realizado neste projeto consistiu em um ataque de engenharia social, mais especificamente, um ataque de *phishing*. Nesse contexto, foi simulado o envio de e-mails fraudulentos para os funcionários da empresa multinacional brasileira certificada ISO 27001 e consolidada no mercado há mais de três décadas. O objetivo era testar a capacidade dos funcionários de identificar e evitar ataques de *phishing*. Os resultados obtidos revelaram que, apesar da certificação ISO 27001 e da reputação estabelecida da empresa, as vulnerabilidades relacionadas à falibilidade humana persistem, permitindo evidenciar de forma prática as fragilidades existentes no ambiente corporativo, mesmo em organizações de renome e com ampla experiência no setor.

Palavras-chave: phishing; ISO 27001; multinacional; cibersegurança; engenharia social

¹ Universidade de Vassouras. e-mail: andre.saraiva@univassouras.edu.br, ORCID: [0009-0000-4397-5906](https://orcid.org/0009-0000-4397-5906)

² Universidade de Vassouras. E-mail: joao.coelho@univassouras.edu.br, ORCID: [0000-0002-9409-5623](https://orcid.org/0000-0002-9409-5623)

³ Universidade de Vassouras. E-mail: ra202221026@univassouras.edu.br

⁴ Universidade de Vassouras. E-mail: ra202210692@univassouras.edu.br, LATTES: [1163640407302960](https://lattes.cnpq.br/1163640407302960):

⁵ Universidade de Vassouras. E-mail: ac_matheus18@hotmail.com, ORCID: [0000-0002-0232-6245](https://orcid.org/0000-0002-0232-6245)

⁶ Universidade de Vassouras. E-mail: ra202210760@univassouras.edu.br, LATTES: [4129662716287841](https://lattes.cnpq.br/4129662716287841)

PHISHING: Empirical Case Study of ISO 27001 Certified Multinational

ABSTRACT

This work aims to demonstrate that, even in contemporary times, when companies conduct and promote training sessions and awareness lectures on information security, the main obstacle remains human fallibility. The security test conducted in this project consisted of a social engineering attack, more specifically, a phishing attack. In this context, the sending of fraudulent emails to the employees of the certified ISO 27001 Brazilian multinational company, which has been established in the market for over three decades, was simulated. The objective was to test the employees' ability to identify and prevent phishing attacks. The obtained results revealed that, despite the ISO 27001 certification and the established reputation of the company, vulnerabilities related to human fallibility persist, allowing for the practical demonstration of existing weaknesses in the corporate environment, even in renowned organizations with extensive experience in the sector.

Keywords: phishing; ISO 27001; multinational; cybersecurity; social engineering

1. INTRODUÇÃO

Este trabalho focou na falha humana e realizou um teste de *phishing*, em colaboradores de alto escalão, em uma empresa multinacional brasileira, que segue as melhores práticas descritas em (Calder, 2006). Os resultados indicaram mais de 33% de colaboradores acessando o link malicioso e fornecendo suas credenciais de acesso.

Como os ataques de *phishing* visam explorar as fraquezas encontradas em humanos, ou seja, usuários finais do sistema, é difícil mitigá-los. Por exemplo, os usuários finais falharam para detectar 29% dos ataques de *phishing*, mesmo quando treinados com o programa de conscientização do usuário com melhor desempenho. (Khonji et al., 2013)

Segundo (TRENDSCE, 2022), os dados da União Internacional de Telecomunicações (UIT) e da Nações Unidas (ONU) relacionados à Tecnologia da Informação e Comunicação, o Brasil saiu da 70ª posição para o 18º lugar no ranking mundial de cibersegurança e o 3º lugar entre os países das Américas, segundo o Índice Global de Cibersegurança de 2020.

As empresas estão direcionando consideráveis investimentos em tecnologias com o objetivo de fortalecer suas defesas contra ameaças, contudo, o principal desafio persiste na forma da falibilidade humana.

Conforme uma pesquisa realizada pela empresa de segurança cibernética Fortinet (FORTINET, 2021), em 2020, o Brasil, mesmo tendo avançado em posições no ranking mundial, enfrentou mais de 8,4 bilhões de tentativas e ameaças de ataques cibernéticos. Essa estatística representa mais de 20% do total de casos registrados em toda a região da América Latina, os quais somaram 41 bilhões.

O ano de 2020 foi marcado pela pandemia de COVID-19, e os cibercriminosos aproveitaram a situação para lançar ataques de *phishing* relacionados à pandemia. De acordo com (Proofpoint, 2023), os ataques de *phishing*, em 2020, foram na casa dos 241.324 casos, caracterizando um aumento de 110%. Ainda, segundo (Ciso Advisor, 2021), no cenário brasileiro, em 2021, houve um aumento de 35%, e segundo o ESET Security Report, esse número aumentou em 235% no ano de 2022 (Eset, 2022).

Durante este período, várias campanhas de cavalos de Troia foram identificadas, as quais executaram atividades sem o conhecimento do usuário.

Essas atividades incluíram o estabelecimento de conexões de acesso remoto, a captura de entradas do teclado, a coleta de informações do sistema, o download/upload de arquivos e a inserção de outros tipos de malware no sistema. Os ativos infectados demonstraram capacidade para realizar ataques de negação de serviço (DoS) (Laufer et al. 2005) e para executar ou eliminar processos. Nesse período, o JS/ScrInject.B! (VirusResearch, 2017) foi o cavalo de Troia mais ativo na região.

O restante deste artigo está organizado da seguinte forma. A Seção 2 apresenta uma breve história e conceitua a Segurança da Informação. A Seção 3 é apresentada a metodologia abordada no teste de *phishing*. A Seção 4 avalia os resultados obtidos no teste. Por fim, a Seção 5 apresenta as considerações finais e sugestões para trabalhos futuros.

2. FUNDAMENTAÇÃO TEÓRICA

Durante a Primeira Guerra Mundial, um ensaio de criptografia de Alexander's Weekly (Xifre Solana, 2009) foi crucial para os britânicos quebrarem os códigos alemães. A máquina Enigma (Krischer, 2013), desenvolvida por Arthur Scherbius (Krischer, 2013) em 1918, teve seu potencial desconhecido até que matemáticos como Newman e Turing a decifrassem (IMasters, 2016). Essa conquista antecipou o fim da Segunda Guerra Mundial em um ano.

Segundo (Proofpoint, 2023), o termo *phishing* foi criado na década de 1990 quando hackers, comumente chamados de phreaks, usavam e-mails falsos para pescar informações de usuários desavisados. Esses ataques ocorriam no serviço AOL, que era muito popular na época. Já na década de 2000, os atacantes mudaram de alvos, com o declínio do AOL e a ascensão de serviços como o Gmail do Google e a crescente informatização que se baseava no e-mail.

Atualmente, o *phishing* se divide em várias vertentes de ataques, cada uma com suas particularidades, como por exemplo:

- *Phishing* de e-mail: Termo amplamente utilizado para descrever qualquer tipo de mensagem de e-mail maliciosa que busca enganar os usuários a fim de obter informações confidenciais e é conhecido como “*phishing*”. Os atacantes geralmente têm como alvo a obtenção de credenciais de conta, informações de identificação pessoal (PII) e segredos comerciais corporativos.
- Manipulação de link: Possuem um link para um site malicioso que se parece oficial, porém o destinatário é levado para um servidor totalmente controlado pelo invasor, onde são persuadidos.
- *Smishing*: Os invasores utilizam mensagens SMS para induzir usuários a acessar site maliciosos de seus telefones.

Esses são apenas alguns exemplos de técnicas básicas de *phishing* que foram aprimoradas ao longo dos anos. Cabe ressaltar que esse tipo de ameaça sempre possui o objetivo de roubar dados de suas vítimas. O que muda constantemente é o *modus operandi*, que se torna cada vez mais sofisticado, exigindo que as organizações invistam cada vez mais em medidas de mitigação.

A ISO 27001 (ISO 27001 2022) prevê a realização de testes periódicos nos sistemas da empresa, a fim de garantir o cumprimento das boas práticas e a resiliência da organização contra-ataques comuns.

A empresa, por sua vez, tem a responsabilidade de fornecer treinamento adequado, o que permite que esses ataques sejam evitados ou prontamente mitigados. É fundamental estabelecer uma cultura de treinamento constante na empresa, tornando assim esses ataques malsucedidos.

Portanto, a segurança da informação deve ser um conceito intrinsecamente ligado às estratégias de vigilância e proteção tanto das estruturas físicas quanto virtuais que compõem as fronteiras, sistemas e infraestruturas críticas da empresa, bem como ao fator humano, que é o foco deste trabalho.

O objetivo deste trabalho é avaliar a resiliência da organização frente a ataques de engenharia social, especificamente por meio do método *phishing*. Sendo assim, destaca-se a importância de examinar a capacidade de resiliência da empresa diante dos ataques direcionados aos seus colaboradores, tendo em vista que tais ataques têm sido amplamente empregados tanto em ambientes corporativos como em âmbitos pessoais.

Ao conduzir testes de *phishing*, será possível identificar algumas vulnerabilidades na segurança da organização, bem como avaliar a preparação dos colaboradores para reconhecer e lidar adequadamente com tentativas de manipulação e ataques de engenharia social.

A análise do comportamento dos indivíduos frente a situações de risco cibernético permitiu o aprimoramento das estratégias e políticas de segurança, tornando-as mais eficientes, além de promover o aprimoramento contínuo dos treinamentos de conscientização e educação em segurança da informação.

Dessa forma, por meio deste estudo, busca-se contribuir para a proteção e fortalecimento da infraestrutura de segurança da organização, resguardando-a contra potenciais ameaças e assegurando a integridade, confidencialidade e disponibilidade das informações sensíveis.

3. METODOLOGIA

Nesta seção, abordaremos brevemente sobre as algumas das especificações utilizadas no trabalho. É relevante destacar que o *phishing* teve uma duração de 12 horas, iniciada durante o horário de almoço dos colaboradores, com o propósito de instigá-los a abrir, aproveitando o momento em que se encontravam distraídos realizando outras tarefas.

3.1 AMBIENTE DE TESTES

Após realizar uma pesquisa nas redes sociais, identificamos o principal domínio utilizado pela empresa na comunicação por e-mail entre seus colaboradores. Com isso, utilizamos um domínio similar ao da empresa, com uma única modificação em uma das letras e com o sufixo .com.br, enquanto o domínio da empresa é caracterizado por ser um domínio .com.

Posteriormente, selecionamos a ferramenta GoPhish, uma ferramenta de código aberto, para realizar os testes. Para isso, configuramos uma instância EC2 (Amazon Elastic Compute Cloud) do tipo t2.micro na AWS (Amazon Web Services). Essa instância foi configurada com a AMI (Amazon Machine Image) do Ubuntu Server 22.04 LTS, fornecida pela Canonical.

A escolha da instância t2.micro foi baseada no escopo e nos requisitos do ambiente de testes. Essa instância é uma opção de baixo custo e possui recursos adequados para testes e desenvolvimento de projetos leves.

Para melhor organização do projeto, ele foi dividido em tópicos, facilitando o entendimento e a compreensão de cada etapa.

1. Instalação do GoPhish (Wright, 2020): Esta é uma etapa bem simples, basta acessar o site do GoPhish (Jordan Wright 2020), e seguir os passos de instalação.
2. Configuração do GoPhish (Wright, 2020): Após a instalação, é necessário configurar detalhes básicos, como portas e endereço de IP na qual o GoPhish (Jordan Wright 2020) será executado.
3. Configuração dos usuários e grupos: Com o andamento deste trabalho, foi possível identificar vários colaboradores nas redes sociais, desde o mais alto até o mais baixo escalão. Após a coleta desses dados, os mesmos foram importados para a ferramenta, criando várias listas de colaboradores.
4. Customização do e-mail: A customização do e-mail é uma das etapas mais importantes do *phishing*, senão a mais importante, onde criamos o template de e-mail. Neste projeto, optamos por criar um e-mail do zero, tornando-o o mais próximo possível do e-mail comumente enviado aos colaboradores.
5. Customização da página: Nesta etapa, é necessário criar uma página de login falsa. O objetivo dessa página é imitar os formulários de login do site real, tornando assim o *phishing* mais convincente.
6. Criação e configuração de um servidor SMTP: Para prosseguir para a próxima etapa, foi necessária a criação e configuração de um servidor SMTP para o envio de e-mails. Com a conclusão dessa etapa, torna-se possível avançar para a configuração do envio.

7. Configuração de envio: Nesta última configuração, foi necessário adicionar algumas das informações do SMTP criadas na etapa anterior, tais como email, host, nome e senha.

Após a conclusão de todas as etapas mencionadas, você pode executar a campanha de *phishing*. Sendo assim, o GoPhish (Jordan Wright 2020) enviará os e-mails de *phishing* para os alvos conforme configurado e rastreará as interações dos alvos com os e-mails e as páginas de login, gerando relatórios e estatísticas detalhadas sobre a campanha.

Neste trabalho, os e-mails enviados aos colaboradores foram divididos em 11 blocos, compostos por 10 colaboradores cada, e um bloco adicional com 6 colaboradores. A transmissão dos e-mails ocorreu em intervalos de 2 a 3 min, a fim de evitar que os mesmos fossem classificados como SPAM.

3.2 FALIBILIDADE HUMANA

Atualmente, diante do contínuo avanço da tecnologia, tornou-se inegável que o ser humano se transformou no elo mais frágil quando se trata da segurança de dados. Ao desenvolver este trabalho, utilizamos uma abordagem que consistiu no envio de e-mails, nos quais nos passamos por um funcionário de alto escalão da empresa, a fim de solicitar uma demanda urgente.

Após algumas horas de testes, identificamos que diversos colaboradores responderam ao e-mail, uma vez que, ao inserirem suas credenciais no site falso, não conseguiram acessar a suposta demanda. Esse resultado demonstra um cenário muito preocupante atualmente, onde as empresas investindo consideráveis recursos financeiros em palestras de conscientização, treinamentos e outras medidas, persistem lacunas consideráveis no sistema de segurança, causando danos irreparáveis à reputação da empresa e seus ativos.

5. RESULTADOS E DISCUSSÕES

Nesta seção, analisa-se os resultados obtidos pela ferramenta GoPhish, referente aos 116 e-mails enviados aos colaboradores de alto escalão da multinacional brasileira, alvo do teste. O teste teve como objetivo a coleta de dados como logins e senhas dos colaboradores. O e-mail

falso criado era convincente, utilizando logotipo e até assinatura virtual de um colaborador importante desta empresa.

A Tabela 1 demonstra os horários exatos em que houve algum tipo de interação com os e-mails enviados da lista 1. Quando há um "X", significa que não houve interação, ou mesmo que a interação não foi registrada.

Nota-se que com 1 minuto, o e-mail número 8, direcionado a um colaborador de alto escalão do Departamento Pessoal, foi aberto e 15 segundos após, o colaborador clicou no link, informando suas credenciais de login e senha. Com isso, em um ataque real, o atacante teria acesso a sistemas críticos. Com este tipo de acesso, o atacante poderia infiltrar-se no sistema interno desta empresa, podendo espalhar malware, roubar dados ou até mesmo extorqui-la, com os dados roubados. O prejuízo seria enorme.

Os resultados obtidos deste teste foram relativamente expressivos, mostrando um ponto crítico desta empresa.

Tabela 1: Tabela contendo o resultado da primeira lista de e-mails enviados

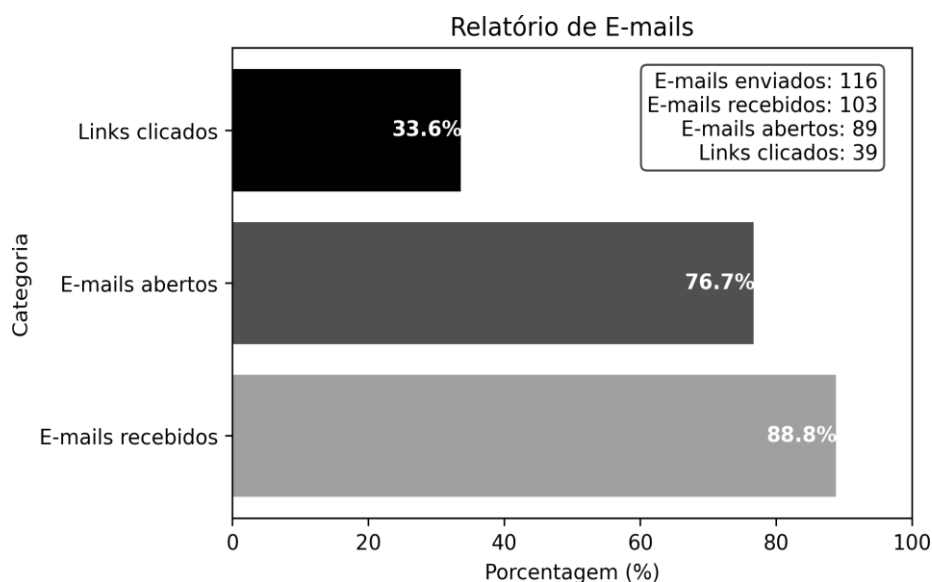
Lista de Envio 1 E-mail	Hora de Envio	Hora de Abertura	Horário de Acesso
1	12:58:22	X	X
2	12:58:24	X	X
3	12:58:22	13:48:02	X
4	12:58:25	14:50:37	X
5	12:58:26	13:12:48	13:12:48 13:13:11
6	12:58:26	14:15:33	X
7	12:58:27	12:59:52	13:00:05 15:31:05
8	12:58:28	12:59:28	12:59:43
9	12:58:28	16:18:03	X
10	12:58:22	15:00:03	15:00:13

Fonte: Os autores.

A primeira lista foi enviada às 12 horas e 58 minutos, um horário no qual os colaboradores poderiam estar mais suscetíveis a erros. A última lista foi enviada às 13 horas e 10 minutos, com um intervalo de 2 a 3 minutos do envio de cada bloco de lista.

Na Figura 1, é apresentado um gráfico que ilustra as estatísticas resultantes após a conclusão do processo de *phishing*. A análise dos dados coletados revela informações relevantes e conclusivas, permitindo uma visão abrangente sobre os resultados decorrentes.

Figura 1: Gráfico apresentando os resultados obtidos após a finalização do teste



Fonte: Os autores.

Adendo que o objetivo primordial do *phishing* consiste em avaliar o grau de instrução e conscientização dos colaboradores sobre segurança da informação, bem como observar suas ações e reações durante uma simulação. Importa ressaltar que qualquer resultado diferente de zero é considerado negativo, pois indica a presença de vulnerabilidades e setores que demandam fortalecimento na prevenção de ataques cibernéticos.

Com base nos resultados obtidos após finalizar os testes, observou-se um alto índice de acesso ao link do *phishing*. Essa constatação é bastante preocupante, pois demonstra uma

maior suscetibilidade dos colaboradores a clicar em links, promoções e e-mails suspeitos, o que potencialmente pode comprometer a segurança da empresa.

Além disso, é relevante mencionar que, devido ao redirecionamento para uma página clonada da empresa e a tentativa de efetuar o login em sua conta, alguns colaboradores clicaram mais de uma vez no link fornecido. Esse comportamento reforça a importância de aprimorar ainda mais a conscientização dos colaboradores em relação às práticas seguras de navegação na Internet e ao reconhecimento de tentativas de *phishing*.

6. CONSIDERAÇÕES FINAIS

Durante a realização deste trabalho e estudos realizados, constatou-se que, apesar da existência de diversas medidas de segurança e inúmeros softwares, o ser humano continua sendo o elo mais fraco. O teste de *phishing* realizado demonstra a vulnerabilidade humana e como ela pode ser explorada, resultando em danos tanto para empresas quanto para indivíduos. Sendo assim, essa constatação fortalece a importância e a necessidade de empreendimentos adotarem uma nova estratégia de segurança.

Destaca-se que a falha humana pode ocorrer de diversas maneiras. Um exemplo bastante frequente e observado atualmente é quando um colaborador da empresa anota sua senha de forma visível ao público, ou até mesmo um computador ou dispositivo móvel sem senha, o que representa um risco significativo para a empresa e seus dados confidenciais. Essas simples ações podem abrir brechas para ataques e comprometer a integridade das informações.

No total foram enviados 116 e-mails, dos quais 13 não foram recebidos, devido a falhas ou férias dos colaboradores. Assim, efetivamente, foram enviados 103 e-mails. Destes 103 e-mails enviados, 39 foram abertos e o link contido no e-mail fake foi clicado. Destaca-se que 89% dos colaboradores abriram o e-mail fake.

Portanto, esse teste de *phishing* se mostra um recurso importante para a melhoria contínua da segurança das organizações, contribuindo para a maior resiliência dos dados da organização contra-ataques de engenharia social.

Nesse sentido, é possível concluir que é de extrema importância as empresas investirem em educação e treinamentos de segurança da informação, os quais podem contribuir significativamente para reduzir a possibilidade de ataques futuros.

Sendo assim, tais testes desempenham um papel significativo no acúmulo de conhecimento, o qual se revelará fundamental para pesquisas posteriores. Nesse sentido, ao ampliar a quantidade de dados disponíveis acerca da maturidade da proteção das organizações, tais testes fortalecem o embasamento empírico necessário para pesquisas futuras.

8. REFERÊNCIAS

CALDER, A. *Information Security Based on ISO 27001/ISO 1779: A Management Guide*. Zaltbommel: Van Haren Publishing, 2006.

CISO ADVISOR. *phishing no Brasil em 2021: 35% mais vítimas*. Disponível em: <<https://www.cisoadvisor.com.br/phishing-no-brasil-em-2021-35-mais-vitimas/>>. Acesso em: 8 jul. 2023.

ESET. *ESET Security Report*. Disponível em: <<https://www.eset.com/br/security-report/>>. Acesso em: 10 jul. 2023.

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

FORTINET. *A América Latina sofreu mais de 41 bilhões de tentativas de ataques cibernéticos em 2020*. Disponível em: <<https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2021/latin-america-suffered-more-than-41-billion-cyberattack-attempts-in-2020>>. Acesso em: 8 jul. 2023.

IMASTERS. *Uma breve viagem ao desenvolvimento da Segurança da Informação – Passado, presente e futuro*. Disponível em: <<https://imasters.com.br/devsecops/uma-breve-viagem-ao-desenvolvimento-da-seguranca-da-informacao-passado-presente-e-futuro>>. Acesso em: 8 jul. 2023.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *ISO/IEC 27001: Information security, cybersecurity and privacy protection – Information security management systems – Requirements*. Geneva, CH, 2022.

WRIGHT, Jordan. Gophish. Disponível em: <<https://getgophish.com/#/>>. Acesso em: 10 jul. 2023.

KHONJI, M.; IRAQI, Y.; JONES, A. phishing detection: a literature survey. *IEEE Communications Surveys & Tutorials* v. 15, n. 4, p. 2091-2121, 2013.

LAUFER, R. P. et al. *Negação de serviço: Ataques e contramedidas*. Sociedade Brasileira de Computação, 2005.

MUELLER, P.; YADEGARI, B. *The stuxnet worm*. Département des sciences de l'informatique, Université de l'Arizona, 2012. Disponível em: <<https://www2.cs.arizona.edu/~collberg/Teaching/466566/2012/Resources/presentations/topic9-final/report.pdf>>. Acesso em: 10 jul. 2023.

PROOFPOINT. História do phishing. Disponível em: <<https://www.proofpoint.com/br/threat-reference/phishing>>. Acesso em: 8 jul. 2023.

TRENDSCE. Brasil ocupa 18º lugar no ranking mundial de cibersegurança. Disponível em: <<https://www.trendsce.com.br/2022/10/24/brasil-ocupa-18o-lugar-no-ranking-mundial-de-ciberseguranca/>>. Acesso em: 9 jul. 2023.

VIPERIT. Segurança Cibernética: Como criar senhas fortes e seguras. Disponível em: <<https://www.viperit.com.br/3323/seguranca-cibernetica-como-criar-senhas-fortes-e-seguras/>>. Acesso em: 12 jul. 2023.

VIRUSRESEARCH. How to remove JS/ScrInject.B Trojan Completely. Disponível em: <<https://virusresearch.org/remove-jsscrinject-b-trojan-completely/>>. Acesso em: 12 jul. 2023.

XIFRÉ SOLANA, P. *Antecedentes y perspectivas de estudio en historia de la criptografía*. 2008. Tese (Doutorado em Engenharia Técnica em Informática de Gestión) – Universidad Carlos III de Madrid, Madrid, Espanha, 2008.