UNIVERSIDADE FEDERAL DA GRANDE DOURADOS
FACULDADE DE CIÊNCIAS EXATAS E TECNOLOGIA
TRABALHO DE CONCLUSÃO DE CURSO
BACHARELADO EM ENGENHARIA DE COMPUTAÇÃO

CRIMES DE INFORMÁTICA

José Yan Gonçalves Lipu

Orientadora Profª Drª Janne Y. Y. Oeiras Lachi

DOURADOS
2021

JOSÉ YAN GONÇALVES LIPU

CRIMES DE INFORMÁTICA

Trabalho de conclusão de curso apresentado à Faculdade de Ciências Exatas e Tecnologia da Universidade Federal da Grande Dourados, como parte dos requisitos para obtenção do grau de Bacharel em Engenharia de Computação.

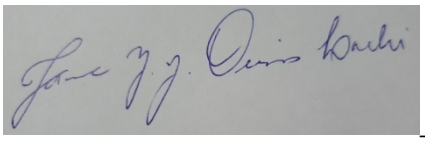
Orientadora: Profª Drª Janne Y. Y. Oeiras Lachi

DOURADOS

2021

Dourados, 27 de Novembro de 2021.

BANCA EXAMINADORA

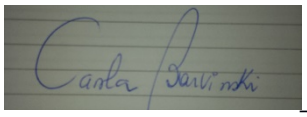


Profa. Dra. JanneYukikoYoshikawa Oeiras Lachi

Universidade Federal da Grande Dourados

Prof. Me. Anderson Bessa da Costa

Universidade Federal da Grande Dourados



Profa. Dra. Carla Adriana Brarvinsk

Universidade Federal da Grande Dourados

AGRADECIMENTO

Quero agradecer primeiramente a Deus, que me abençoou e me deu forças ao longo da jornada e do caminho iniciado anos atrás.

Agradeço aos meus pais, Jose Lipu e Doralice Lipu, e ao meu irmão, Levi Yunes. Sempre fizeram todo esforço possível para que eu concluísse meus estudos. À minha avó Lourdes, minha tia Dorenice e suas filhas. Me acolheram em sua casa durante todo esse período como se eu fosse filho. Não existem palavras para expressar o tamanho da minha gratidão.

À minha orientadora ProfªDrª JanneYukikoYoshikawa Oeiras Lachi, por ter me apoiado e me instruído esplendidamente durante todo desenvolvimento do trabalho. Os conhecimentos passados a mim, foram indispensáveis. Agradeço pela confiança.

À minha namorada Ana Beatriz, que esteve do meu lado nos momentos mais difíceis da minha graduação.

Ao corpo docente do curso de Engenharia de Computação da UFGD. Cujo trabalho é fundamental para ciência e para obtenção do grau de bacharelado.

In memorian de Carlo Fernando MiragliaCastaño.

“Confia ao Senhor as tuas obras, e teus pensamentos serão estabelecidos”.

Provérbios 16:3

RESUMO

Os crimes de informática representam um perigo crescente para a sociedade humana. Os dados trafegados na Internet abrangem uma grande multiplicidade de informação, desde mensagens pessoais, até documentos contendo segredos de estado. Neste artigo busca-se trazer uma revisão bibliográfica, de fontes jornalísticas e da literatura sobre os crimes de informática que se utilizam dos dispositivos eletrônicos e da Internet como meio de aplicação. Crimes cujos objetivos são alterar, manipular e obter dados ilegalmente serão descritos. Além disso, será explicado como funcionam, e os principais modos de proteção contra o crime tipificado. Este trabalho busca trazer ao leitor uma fonte de consulta para entender e se prevenir contra estes crimes.

Palavras-chave: Crimes de Informática, *phishing*, *spoofing, ransomware*.

ABSTRACT

Computer crime is increasingly danger to human society. The data transmitted on the internet cover a great variety of information, from personal messages to documents containing state secrets. This article seeks to bring a literature review, journalistic sources review and literature review on computer crimes that use electronic devices and the internet as a means of application. Crimes whose purpose is to modify, manipulate and illegally obtain data. It will describe what they are, how they work, and the main modes of protection against typified crime. This work seeks to provide the reader with a source of reference to understand and prevent against these crimes.

Key-words: Cyber crimes, *phishing*, *spoofing, ransomware*.

Crimes de Informática

José Yan Gonçalves Lipu[1], Janne Y. Y. Oeiras Lachi[1]

[1]Faculdade de Ciências Exatas e Tecnologia (FACET)

Universidade Federal da Grande Dourados (UFGD)
Dourados – MS – Brasil

jylipu@hotmail.com, janneoeiras@ufgd.edu.br

Abstract. *Computer crime is increasingly danger to human society. The data transmitted on the internet cover a great variety of information, from personal messages to documents containing state secrets. This article seeks to bring a literature review, journalistic sources review and literature review on computer crimes that use electronic devices andthe internet as a means of application. Crimes whose purpose is to modify, manipulate and illegally obtain data. It will describe what they are, how they work, and the main modes of protection against typified crime. This work seeks to provide the reader with a source of reference to understand and prevent against these crimes.*

Resumo. *Os crimes de informática representam um perigo crescente para a sociedade humana. Os dados trafegados na Internet abrangem uma grande multiplicidade de informação, desde mensagens pessoais, até documentos contendo segredos de estado. Neste artigo busca-se trazer uma revisão bibliográfica, de fontes jornalísticas e da literatura sobre os crimes de informática que se utilizam dos dispositivos eletrônicos e da Internet como meio de aplicação. Crimes cujos objetivossão alterar, manipular e obter dados ilegalmente serão descritos. Além disso, será explicado como funcionam, e os principais modos de proteção contra o crime tipificado. Este trabalho busca trazer ao leitor uma fonte de consulta para entender e se prevenir contra estes crimes.*

1. Introdução

O surgimento da Internet possibilitou o avanço da tecnologia em todo o mundo e a forma de comunicação foi transformada drasticamente. Transformações essas que vão desde a transmissão e difusão de informações até o uso da Internet como meio de entretenimento e lazer. A Internet possibilita o acesso à pesquisa e ao conhecimento, aproxima o relacionamento entre pessoas que estão distantes fisicamente e torna possível novas formas de trabalho.

Por outro lado, o uso indevido dessa rede de computadores ocasionou um enorme problema: os crimes de informática. De acordo com Eleutério (2011), os meios informáticos são divididos em duas categorias quando se trata da prática de crimes: utilização do equipamento computacional como ferramenta de apoio aos crimes convencionais e como meio para a realização do crime. Na primeira modalidade, o computador é apenas uma ferramenta para a prática do crime. Por exemplo, ao usar algum editor de texto, poderá ser feita a emissão de uma nota fiscal fria, que acarreta

crime de sonegação fiscal. Este trabalho irá descrever o funcionamento de alguns crimes que se enquadram na segunda categoria, na qual Eleutério (2011) define que o computador é peça central para o que o crime possa ocorrer, ou seja, se o dispositivo não existisse, este não poderia ser praticado. Dessa forma, surgem novas possibilidades de delitos devido ao mau uso do computador e da Internet.

Bishop (2003) define segurança da informação com base em confidencialidade, integridade e disponibilidade. A expansão da Internet possibilita que todos os tipos de informação e de dados possam trafegar na rede. Grande parte do volume transmitido é de informações pessoais e corporativas. Neste cenário, Stallings (2006) considera ataque à segurança qualquer ação que comprometa a segurança de informação pertencente a uma organização. Como a interceptação, perda ou roubo destes dados pode gerar prejuízos a Segurança da Informação se tornou um problema importante da sociedade moderna. No entanto, todos têm o direito de esperar que seus dados privados sejam mantidos intactos e disponibilizados apenas a pessoas autorizadas.

Até o ano de 2012, grande parte dos crimes cometidos na Internet no território brasileiro não possuía legislação específica eeram julgados como delitos comuns já previstos no código penal. Neste contexto, o Conselho Nacional de Justiça (CNJ) publicou um artigo em seu *site*[1] listando os crimes mais comuns cometidos na Internet e que eram previstos em lei: crime de Calúnia (Artigo 138 do Código Penal), crime de Difamação (Artigo 139 do Código Penal), crime de Injúria (Artigo 140 do Código Penal), crime de Ameaça (Artigo 147 do Código Penal) e o crime de Falsa Identidade (Artigo 307 do Código Penal). Esses delitos são comuns em fóruns e nas redes sociais.

Por exemplo, em maio de 2012 um caso se tornou manchete nos principais veículos de comunicação do país: fotos íntimas da atriz Carolina Dieckmann foram divulgadas por *hackers*. Nesse mesmo ano foi sancionada a Lei Nº 12.735, que trata de Crimes Cibernéticos, que dispõe sobre a tipificação criminal de delitos informáticos, principalmente a Invasão de Dispositivos Informáticos. Invadir dispositivos alheios com o fim de obter, adulterar ou destruir informações ou dados, tem pena de três meses a um ano de prisão. No ano de 2017, aproximadamente 62 milhões de brasileiros foram vítimas de crimes virtuais (DIÁRIO DO AMAZONAS, 2018).

Em julho de 2019, o celular do Ministro da Justiça, Sérgio Moro, foi *hackeado*. Os criminosos obtiveram acesso a mensagens privadas de um aplicativo de mensagens rápidas, o Telegram. O caso foi investigado pela Polícia Federal e as investigações concluíram que os *hackers* exploraram uma falha de segurança das caixas postais, aplicando uma técnica conhecida como *spoofing*.

Assim como no mundo real, os criminosos cibernéticos desenvolvem técnicas e métodos sofisticados para alcançar seus objetivos maliciosos. Este artigo propõe apresentar três técnicas usadas como ferramentas para execução de crimes virtuais: *phishing, spoofing* e *ransomware*. O principal objetivo destes tipos de crimes é ter acesso aos dados dos usuários ou organizações por meio da Engenharia Social. Neste trabalho, será descrito no que consistem esses ataques, como podem ser executados e como as pessoas ou empresas podem se proteger.

[1]Disponível em: https://www.cnj.jus.br/crimes-digitais-o-que-sao-como-denunciar-e-quais-leis-tipificam-como-crime/

O interesse da escolha dos três crimes digitais citados acima surge para entender a execução e aplicação de práticas maliciosas que estão causando grandes prejuízos a pessoas físicas e organizações no mundo. Ao longo da explicação desses crimes é possível identificar semelhanças de *modus operandi* e como se utilizam da Engenharia Social - conceito que será descrito neste trabalho - como ferramenta para aplicação.

Na Seção 2 é descrito o crime de *phishing*e o conceito de engenharia social e seu uso na prática desse crime, as formas mais comuns e a também as formas de proteção. A Seção 3 apresenta o crime de *spoofing*e as ameaças que este tipo de ataque representa. A prática conhecida como *ransomware*será descrita na seção 4. Por fim, a seção 5 apresenta as considerações finais deste trabalho.

2. *Phishing*

2.1. Definição

As leis em vigor no Brasil definem que o crime contra o patrimônio é todo o crime que busca apropriar-se do patrimônio alheio, ou causar dano contra propriedades públicas ou privadas (MASTER JURIS, 2019). Neste contexto, os criminosos buscam alternativas de obter dados ilegalmente e a principal maneira utilizada é o *phishing*.

Phishing é um termo originado do inglês (*fishing*, pescar) que em computação se refere a um tipo de roubo de identidade *online*. Esse termo surgiu porque os golpes utilizam principalmente *e-mails* e *sites* falsos para induzirem as vítimas a fornecer voluntariamente dados pessoais sem notarem que se trata de uma fraude. É um tipo de ataque fraudulento que, entre seus principais objetivos, se caracteriza por ocorrer o roubo de credenciais como: senhas, nomes de usuários, *e-mails*, números de cartões de crédito, entre outras informações.

Uma das principais características desse tipo de ataque é chamada de Engenharia Social. No âmbito da Computação, a Engenharia Social é uma técnica que busca adquirir informações privadas utilizando-se de persuasão e manipulação psicológica. Por meio dessa técnica os criminosos criam as chamadas “iscas”, que são mensagens mentirosas que buscam atrair as vítimas. É uma característica marcante, pois a “isca” que é enviada aos usuários tem muita relevância, podendo ser o fator determinante para o sucesso da ação criminosa. Os atacantes contam com a ingenuidade de suas vítimas em ataques de engenharia social (RAINS, 2020).

Durante a pandemia de COVID-19 houve um aumento de 70% nos golpes do tipo *phishing* (SOPHOS LTD, 2021). Um levantamento da companhia de segurança da informação, ESET, com sede em Bratislava, Eslováquia, identificou um ataque explorando a campanha de vacinação do Governo Federaldo Brasil. Os criminosos enviavam *e-mails* com uma falsa assinatura do Ministério da Saúde, solicitando o cadastro das vítimas para uma suposta vacinação contra a COVID-19 (ESET 2021). Ao abrir o *e-mail*, o usuário se deparava com um *link* que fazia o *download* de um

programa infectado com um *trojan*[2]. Na Figura 1, mostra-se um exemplo do ataque identificado.

Figura 1: Exemplo de *phishing* com uma mensagem da campanha de vacinação do COVID-19. Fonte: ESET (2021).

O *Phishing* é considerado um crime contra o patrimônio. Essa definição é importante, pois quando se trata de crimes de informática, as leis de crimes comuns e as leis específicas podem ser usadas de forma conjunta no julgamento e sentenças das condenações.

Segundo um relatório da Kaspersky Lab (KASPERSKY LAB, 2019), uma companhia especializada em desenvolver softwares de segurança, o Brasil foi o país mais atingido no mundo por ataques desse tipo, pois, de todos os ataques do mundo, cerca de 22% aconteceram nessepaís.

O relatório da companhia americana de cibersegurança,RiskIQ, referente ao ano de 2019 mostrou que os prejuízos causados mundialmente por este tipo de fraude totalizam cerca de U$$ 2,9 milhões a cada minuto ao redor do mundo, totalizando US $ 1,5 trilhões ao longo do ano (RISKIQ, 2019).

Existem, a princípio, duas formas de se efetuar uma tentativa de golpe: obtendo o endereço de *e-mail* ou o número de telefone da vítima em potencial. A criatividade e o uso eficiente da Engenharia Social constituem a base de um levantamento destes dados. Segundo Mitnick (2003) a Engenharia Social se utiliza da influência e persuasão para

[2]*Trojan* se refere a um software malicioso que se disfarça como inofensivo. São chamados de softwares maliciosos os programas desenvolvidos com o objetivo de causar danos e interceptar dados

ganhar a confiança de pessoas, e dessa forma, convencê-lasde que a mensagem ou o contato realizado é legítimo. Como resultado, pode ocorrer a obtenção de dados.

As ferramentas mais comuns utilizadas por criminosos atualmente são os aplicativos desconhecidos que prometem algum tipo de entretenimento como jogos e *quizzes*[3] interativos, *sites* desconhecidos, criação de formulários e pesquisas falsas. Aplicativos como o Google Forms, por exemplo, são muito simples de usar e os resultados obtidos possuem boa exatidão motivo pelo qual são ideais para o *phishing*. Por esta razão pode-se afirmar que o *Phishing* é uma técnica que une a criatividade da Engenharia Social ao conhecimento de Computação como crime contra o patrimônio.

Um exemplo do uso dessas ferramentas de forma nociva explora o famoso jogo Fortnite, da companhia americana Epic Games, Inc. Segundo dados da Statista[4] (STATISTA 2020), em maio de 2020 o jogo possuía cerca de 350 milhões de jogadores ao redor do mundo. Um dos fatores que contribuem para esse número expressivo é o fato do jogo ser gratuito para *download*. A receita da Epic Games vem das compras realizadas dentro do jogo utilizando sua moeda virtual, o V-Buck. Criminosos exploram um público que realiza buscas na Internet com intenção de obter V-Bucks de maneira ilegal. Em uma busca no Google com as palavras chave "free v-bucks", encontramos um link que nos leva a uma página com a tela mostrada na Figura 2. Percebe-se que o link da página tem uma menção a V-Bucks.

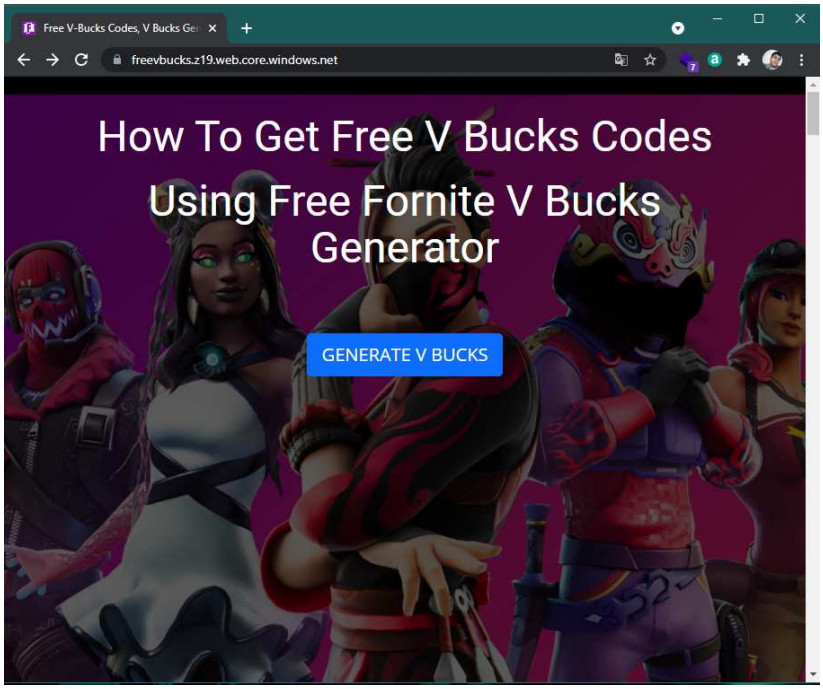


Figura 2: Homepage de um *site* malicioso. Fonte: Imagem do autor.

Quando o botão "GENERATE V BUCKS" é clicado, o *site* induz o usuário a realizar uma sequência de passos, como mostrados na Figura 3. Ao final, o usuário é

[3] *Quiz* é um teste informal.
[4] A Statista é uma empresa alemã especializada em dados de mercado e consumidores.

redirecionado para uma *landing page*[5]com um formulário falso para coleta de dados como nome, *e-mail*, sexo e data de nascimento.

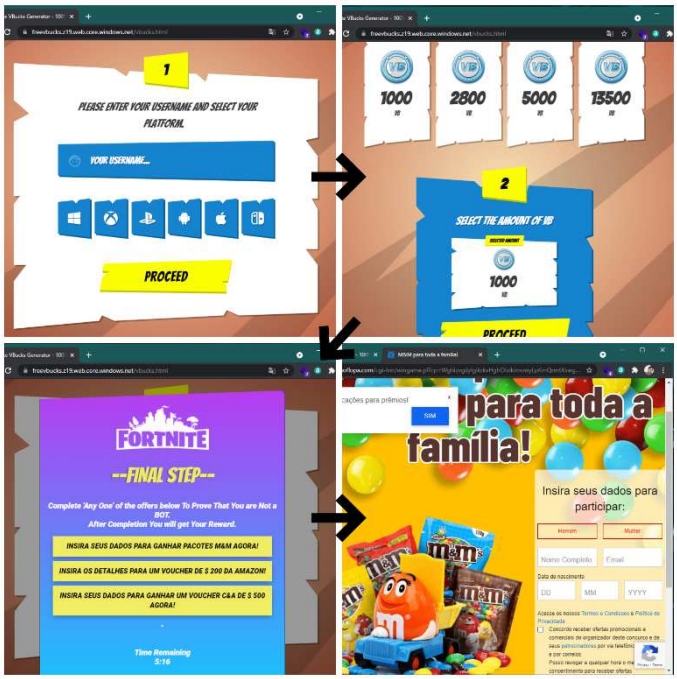


Figura 3: Fluxo do *site* malicioso da Figura 1. Fonte: Imagem do autor.

Em fevereiro de 2019, o *site* britânico The Register (THE REGISTER, 2019), revelou que dados de 620 milhões de contas de 16 *sites* estão sendo vendidos na Internet. O *site* de dublagens de vídeos e entretenimento Dubsmash[6] é um dos 16 *sites* que possuem informações de usuários sendo vendidas ilegalmente na Internet, segundo esse relatório. Essa informação mostra que *e-mails*, senhas e fotos pessoais podem ser encontradas na rede. Ao ter acesso a essas informações os criminosos conseguem desenvolver "iscas" utilizando características mais próximas da realidade dos alvos. Por exemplo, ao utilizar as informações do Dubsmash que estão disponíveis ilegalmente na *web*, os *hackers* podem direcionar e enviar *e-mails* falsos a todos os endereços obtidos.

Para realizar um ataque deste tipo, é necessário saber quais tipos de informações pretendem serem obtidas, como senhas, números de cartão de crédito, informações pessoais, entre outros. Em seguida as mensagens maliciosas são enviadas às vítimas aplicando as técnicas de Engenharia Social e muitas vezes usando dados pessoais obtidos de forma ilegal.

Para alcançar esse objetivo, diversas variações deste ataque foram desenvolvidas ao longo dos anos, a implementação básica consiste em falsificar uma página ou redirecionar o usuário a um endereço falso. As Figuras 4 e 5 apresentam um exemplo de como os criminosos enviam uma mensagem de isca para os usuários.

---

[5]*Landing Page* é uma página web estática que tem como objetivo capturar dados como: nome, *e-mail*, sexo, etc.

[6]Dubsmash é um aplicativo de mensagens em vídeo para Android e para iOS.

A Figura 4 mostra uma mensagem que chegou na caixa de *e-mail* de um usuário, supostamente proveniente de uma loja muito conhecida no Brasil, as Casas Bahia.

Figura 4: Título de um *e-mail* contendo *phishing*. Fonte: Imagem do autor.

Na Figura 5, pode-se ver o *e-mail* criado para enganar as vítimas com uma mensagem que parece ser uma NFe (Nota Fiscal Eletrônica) emitida pela loja conhecida. Ao clicar no *link* "Visualizar PDF – Baixar XML" no fim da mensagem, um *malware*[7] é instalado no computador da vítima.

Figura 5: Conteúdo malicioso de um *e-mail* contendo *phishing*.Fonte: Imagem do autor.

No *site* Github (https://github.com), que é o maior repositório de códigos de software do mundo, pode-se encontrar com facilidade diversos projetos contendo códigos maliciosos em diversas linguagens. Grande parte desses códigos está pronta para uso. Em uma rápida busca com as palavras-chave "*phishingexample*" chega-se ao projeto '*FB-Phishing-Example*'. Esse projeto consiste em um bloco de código pronto, com o objetivo de ser um clone da página de *login* da rede social Facebook. Para ter acesso, basta fazer o *download* dos arquivos do repositório. Ao abrir o arquivo `index.html` com algum editor de código, pode-se depurar e analisar as funções do código e observar como é feito. O código possui duas partes fundamentais para o funcionamento malicioso, mostradas a seguir.

[7] *Malware* vem do inglês *Malicious Software*. Um termo genérico para qualquer tipo de software de computador com intenção maliciosa. Vide Trojan[1].

No Quadro 1 é descrito um trecho HTML(*HyperText Markup Language*), uma linguagem usada para construção de páginas na *web*. Na linha 7 existe uma *tag* do tipo *input*, com o *id* “correo”. Esta *tag* é responsável por capturar os dados inseridos no campo “Correoeletronico”, que é o *e-mail* do usuário. Na linha seguinte existe outra *tag input*, com o *id* “password”. Esta outra *tag* armazenará a senha do usuário. Deve-se guardar essas informações, pois no próximo bloco de código, apresentado no Quadro 2, será mostrado como elas são tratadas e como são enviadas para o *cyber* criminoso.

Quadro 1: Implementação da entrada de dados de uma página falsa.

```
1 <formmethod="post">
2 <table>
3 <tr>
4 <tdclass="logintext">Correoelectronico</td>
5 <tdclass="logintext"><spanclass="loginrowgap">Contraseña</span></td>
6 </tr>
7 <input id="correo" type="text" class="logintextloginfield">
8 <input id="password" type="password" class="logintextloginrowgaploginfield">
9 <input id="send" class="loginrowgap" id="loginbutton" type="button" value="IniciarSesión">
10 <div id="toast_success" class="alertalert-success fade show" role="alert">
11              Tu mensaje se envio correctamente

12 </div>
13 <div id="toast_danger" class="alertalert-danger fade show" role="alert">
14 Llene todos los campos
15
16 </div>
17 </tr>
18 <tr>
19 <td></td>
20 <td><a href="#" class="logintextloginrowgap" id="forgotpw">Olvido lacontraseña?</a></td>
21 </tr>
22 </table>
23 </form>
```

Fonte: Github, 2020.

Após a captura desses dados, o código malicioso os envia via SMTP para uma conta de *e-mail*. Neste exemplo usa-se o servidor SMTP do Gmail na linha 8.

Quadro 2: Implementação da função de envio dos dados.

```
1 functionsendE-mail() {
2 correo = document.getElementById("correo").value;
3 password = document.getElementById("password").value;
4 message = "LOS DATOS INGRESADOS DEL USUARIO " + correo + " SON: \nCORREO: " + correo
5 + "\nCONTRASEÑA: " + password;
6     console.log(message);
7 E-mail.send({
8 Host : "smtp.gmail.com",
9 Username : "2020gvlc@gmail.com",
10 Password : "Operador2020*",
```

```
11 To: 'supp0rtfb20@gmail.com',
12 From: 'correo@gmailcom',
13 Subject: 'Cambio de contraseña',
14       Body: message
15    }).then(
16 location.href ="http://www.facebook.com"
17     );
18   }
19
20 constform = document.getElementById("contact");
21 sendBtnNode.addEventListener("click", () =>{ sendE-mail() })
22 form.addEventListener("input", (event) => {
23 setFieldValues(event.target.id, event.target.value) })
```

Fonte: Github, 2020.

As variáveis ‘correo’, na linha 2 e ‘password’, na linha 3, recebem os valores armazenados nas inseridos nas *tags* HTML, como descrito anteriormente. Em seguida, a variável ‘message’, na linha 3, recebe uma *string* concatenada dinamicamente com as variáveis ‘correo’ e ‘password’. Essa será a mensagem que o criminoso receberá via *e-mail*. A função ‘E-mail.send()’, na linha 7, é responsável por enviar os dados coletados para um endereço de *e-mail* previamente definido na função. A função possui os dados necessários para envio da mensagem via *e-mail*. O primeiro deles é o ‘Host’, na linha 8, que recebe o endereço ‘smtp.gmail.com’, que é o endereço dado para conexão ao servidor de *e-mail* do Google. Em seguida, os campos ‘Username’ e ‘Password’, linhas 9 e 10, respectivamente, armazenam os dados da conta que enviará o *e-mail*. Os campos ‘To’, linha 11, ‘From’, na linha 12, ‘Subject’, na linha 13 e ‘Body’, linha 14, armazenam o cabeçalho de um *e-mail* padrão, que são: o endereço para o qual será enviado, a conta que enviou o *e-mail*, o assunto do *e-mail* e, por fim, a mensagem. Logo após o envio, o código redireciona o usuário para o endereço verdadeiro do Facebook, linha 16.

Esse redirecionamento ou clonagem de páginas e endereços Web ocorre usando o protocolo SMTP (*Simple Mail TransferProtocol*), definido na RFC 821[8] (IETF, 1986), ataque a servidores DNS[9] (*Domain Name System*) e com o envio em massa de SMS’s (*Short Message Service*). O uso de um Gateway GSM (*Global System for Mobile Communications*), conhecido como "chipeira", é um dispositivo que permite envio em massa de SMS’s. Esta atividade é proibida pela ANATEL (Agência Nacional de Telecomunicações), entretanto,as operadoras não bloqueiam completamente, pois é um serviço usado por empresas de telecomunicações. Na Figura 6 mostra-se um exemplo de mensagens de texto contendo mensagens que buscam enganar os usuários. As mensagens levam a crer que são enviadas por agências bancárias. Este tipo de mensagem é muito recorrente em território brasileiro

[8] Disponível em: https://datatracker.ietf.org/doc/html/rfc821.

[9] É um sistema de gestão de nomes para computadores, serviços ou qualquer máquina conectada à Internet ou a uma rede privada.

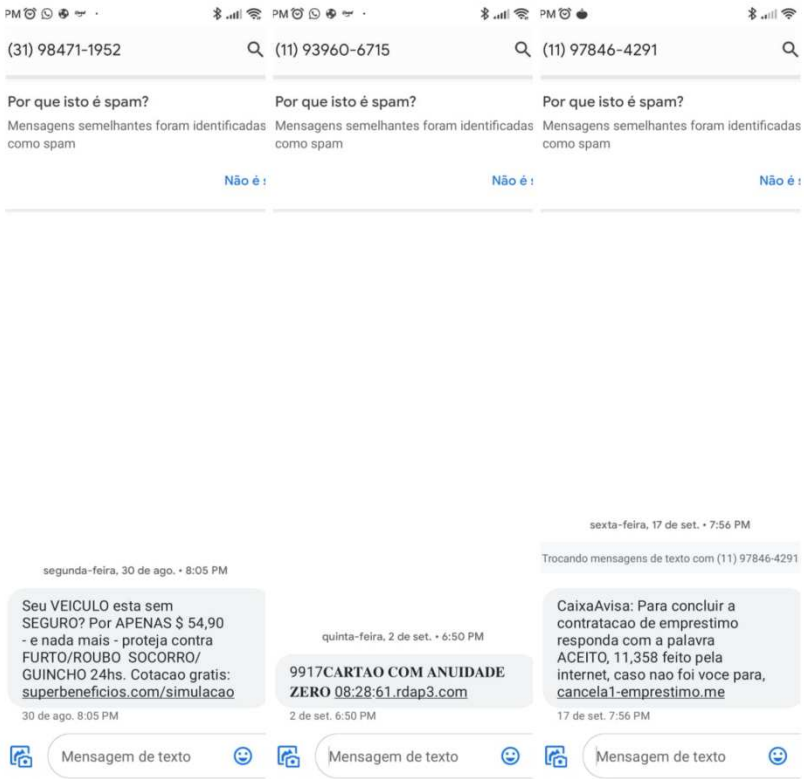


Figura 6: Exemplos de SMS que se passam por agências bancárias.Fonte: Imagem do autor.

Ao classificarmos as técnicas com essa característica de *modus operandi*, pode-se dividir este tipo em subcategorias. A primeira subcategoria encontrada é chamada de *SpearPhishing*, que é uma variante muito similar à técnica principal. O principal aspecto é o ataque direcionado, focado em uma pessoa ou grupo específico. O ataque a um grupo de funcionários de uma empresa ou organização específica é um exemplo deste tipo de ação.

Nos dias atuais é indispensável que as empresas e organizações possuam um *website*. Como prática comum, estes *websites* mostram quem são as pessoas com cargos de alto comando ou até mesmo uma breve lista de contatos. Toma-se como exemplo o *website* institucional da Universidade Federal da Grande Dourados (https://portal.ufgd.edu.br), na lista do corpo docente do curso de Engenharia de Computação tem-se acesso ao *e-mail* de todos os professores do curso. Com esses endereços em mãos, torna-se possível uma tentativa de realização de um ataque do tipo S*pearPhishing*.

De acordo com Ohagan (2018), *anglerphishing* é um tipo de ataque tira proveito da confiança que os usuários possuem em perfis de marcas e *sites* de mídia nas redes sociais. Os criminosos cibernéticos imitam e se passam por marcas legítimas e confiáveis. Quando o usuário envia mensagens, curtidas, comentários ou menciona alguma dessas marcas por meio de publicações nas redes sociais, os criminosos se aproveitam dessa comunicação. O criminoso começa a enviar mensagens privadas ao usuário ou posta *links* maliciosos que desviam o usuário para páginas de *phishing* na esperança de roubar dados pessoais.

Em janeiro de 2021 um total de 4.2 bilhões de pessoas ao redor do mundo eram consideradas ativas nas redes sociais (STATISTA 2021). Esse número cada vez mais crescente mostra que as redes sociais também se tornam um enorme meio de atuação. King (2016) identificou 5 tipos de *scams*[10] mais comuns nas redes sociais, que se classificam como *anglerphishing* que são: criação de contas falsas de atendimento ao cliente para roubar dados sensíveis como logins e senhas de bancos; escrever comentários falsos em postagens populares para atrair atenção desse grande público para *links* com manchetes chamativas que levam os usuários a golpes de *phishing*; falsas transmissões ao vivo,por exemplo, em uma postagem no Facebook sobre algum evento esportivo, os criminosos deixam *links* que levam a *sites* falsos onde pedem informações pessoais para iniciar a transmissão que muitas vezes não existe; falsos descontos *online*, semelhantes as falsas contas de atendimento ao cliente, neste caso oferecem descontos que fingem ser reais e buscam também obter informações pessoais; e por fim, falsas pesquisas e concursos *online*, cujo o objetivo é obter respostas de perguntas pessoais (KING, 2016). A Figura 7 mostra uma simulação de *anglerphishing* usando a rede social Twitter. Na imagem, um falso perfil da UFGD envia um link enganoso para o usuário que realizou uma postagem.

Figura 7: Simulação de um ataque *anglerphishing*.Fonte: Imagem do autor.

Quando se trata da segurança de informação em organizações, um dos aspectos fundamentais é a Governança de Tecnologia da Informação. Pelo fato das organizações serem compostas de pessoas, entende-se que o agente humano nas organizações é o principal fator de risco, por ser uma potencial vítima da Engenharia Social. A KnowBe4, com sede em Clearwater nos Estados Unidos, é uma empresa especializada em segurança corporativa atuando na simulação de ataques de *phishing*, em 2020 publicou um relatório de análise em 17 mil organizações ao redor do mundo e mostrou que 37.9% dos 4 milhões de usuários dessas organizações clicam em *links* ou atenderam um pedido fraudulento (KNOWBE4, 2020).

[10] *Scam*significa fraude em inglês.

2.2 Medidas de proteção anti-*phishing*

Para mitigar possíveis perdas, é necessário ter uma estrutura de processos bem definida, em que cada decisão individual representa o menor risco possível. Para isso, algumas organizações têm como foco desenvolver metodologias, certificações e padrões para alcançar os principais objetivos organizacionais, como conformidade e segurança (UPGUARD TEAM, 2021). Dois exemplos são a AXELOS, fundada em 2014 pelo governo do Reino Unido, e o ISACA (*Information Systems AuditandControlAssociation*), fundado em 1969 na cidade de Schaumburg, nos Estados Unidos. A AXELOS, desde sua fundação, é responsável pelo licenciamento da propriedade intelectual do framework ITIL (*Information Technology Infrastructure Library*[11]), que é uma ferramenta adaptável para gerenciamento de serviços (AXELOS, 2021). ITIL é o corpo de conhecimento das boas práticas que foram aprendidas ao longo de anos por muitas equipes em muitas empresas e que foram documentadas e organizadas nesse corpo de conhecimento (AKITA, 2020). Já a ISACA tem sob seu domínio o *framework* COBIT (*ControlObjectives for InformationandRelated Technology*[12]). O COBIT oferece um programa abrangente de segurança cibernética para Governança de TI corporativa (WALSH, 2018). O Quadro 3 apresenta os princípios da Governança de T.I dos frameworks ITIL e COBIT.

Quadro 3: Comparativo das ferramentas de Governança de TI.

	ITIL	COBIT
1	Comece onde você está.	Defina metas e indicadores de TI concretos e apropriados, com um caminho claro para atender às necessidades das partes interessadas.
2	Progresso iterativamente com *feedback*.	Atribuir camadas / níveis de responsabilidade.
3	Colabore e promova a visibilidade.	Princípio: Cubra a empresa de ponta a ponta.
4	Pense e trabalhe holisticamente.	Informar os membros da organização em toda a organização sobre os ativos de informação que facilitam seus objetivos de negócios ou necessidades de design de serviço.
5	Mantenha-o simples e prático.	Princípio: Separar a governança da gestão.
6	Otimize e automatize.	Crie níveis de autoridade.
7		Estabeleça metas de monitoramento.

Fonte: Elaborada pelo autor.

Além da otimização dos processos organizacionais, existem meios mais objetivos que buscam trazer um aumento da segurança digital no curto prazo. A companhia brasileira de segurança da informação, IT-EAM, com sede em Belo Horizonte,elaborou uma lista com medidas que podem ser tomadas de imediato, pode-se

[11] Tradução: Biblioteca de Infraestrutura de Tecnologia da Informação.
[12] Tradução: Objetivos de Controle para Informação e Tecnologia Relacionada.

destacar alguns itens dessa lista, tais como: treinamento de pessoal, antivírus e filtro *anti-phishing* nos servidores de *e-mail*(IT-EAM, 2021).

Para aplicar a etapa de treinamento, é necessário que os membros da organização ou empresa tenham consciência de que criminosos usarão fraude para manipulá-las psicologicamente (MITNICK; SIMON, 2003). Desta forma, aplicar treinamento interno é fundamental para manter um nível de segurança mais elevado.

Como os ataques do tipo *phishing*são baseados em engenharia social, a vítima muitas vezes acredita que o atacante é um colega ou alguma pessoa que está autorizada a acessar informações confidenciais ou que é alguém autorizado a o instruir para seguir passos que envolvam tomada de ações/decisões em computadores ou equipamentos relacionados (MITNICK; SIMON, 2003). Mitnick e Simon (2003) levantam duas etapas importantes para evitar ataques, são eles: Verificar a identidade da pessoa que faz uma solicitação e verificar se essa pessoa está autorizada.

Nas etapas seguintes, após o treinamento, busca-se implementar soluções que visam eliminar as ameaças depois de terem passado pela barreira humana. Os antivírus são softwares projetados para proteger usuários e computadores de vírus, malwares e uma série de outras ameaças (ESET, 2021). A implementação desses softwares em ambientes corporativos pode evitar, por exemplo um ataque de *ransomware,* que veremos na seção 2.3. Já os filtros *antiphishing* em *e-mail* são soluções implementadas por empresas que fornecem serviços de *e-mail*, como Outlook e Gmail. Os filtros são implementados nos servidores que são responsáveis pela transmissão dos *e-mails*. Muitos desses serviços são baseados em *machinelearning*, que buscam identificar padrões de *phishing* nas mensagens, e após identificar uma possível ameaça, envia os *e-mails* para a caixa de spam do usuário.

O usuário comum, aquele que não faz parte de organizações e que usa a Internet para trabalho ou por lazer, também deve buscar formas de se proteger. Vayansky e Kumar (2018) propõem uma proteção contra *phishing* baseada em 3 passos:

1. Prevenção de *Phishing*: engloba o uso de sistemas, inteligência artificial e *blacklists*para filtrar e bloquear *e-mails* e *websites* de *phishing*. Na computação as *blacklists*são mecanismos que registram endereços previamente identificados como perigosos. Um exemplo é o *site* “aa419” (https://db.aa419.org/fakebankslist.php), que identifica *sites* fraudulentos.
2. Detecção de *Phishing*: acontece depois que o usuário abre um *e-mail* malicioso ou entra em algum *link* desconhecido, os criminosos usam métodos mais sofisticados para garantir que alcance usuários vulneráveis. Muitos navegadores, como o Google Chrome possuem soluções implementadas que alertam o usuário que esteja acessando um *site* não confiável. Essa ferramenta consulta uma *blacklist* de *sites* previamente identificados como maliciosos.
3. Treinamento: treinar os usuários é a terceira abordagem proposta na metodologia de solução. A maioria dos treinamentos *anti-phishing* existentes não combate métodos e correntes mais sofisticados, além de depender que o usuário leia o material. Um método de treinamento proposto é o envio de *e-mail* simulando *phishing*. Esse *e-mail* redireciona o usuário para uma página

contendo informações sobre qual foi o erro do usuário e alertando-os para que esta ação seja evitada no futuro.

Como visto, ganhar a confiança da vítima é fundamental para o sucesso de um ataque *phishing*. Uma das formas que pode ajudar neste ganho de confiança é chamada de *spoofing*. Mostra-se na subseção 2.2 o que é *spoofing*, suas formas de ação e como se proteger.

3*Spoofing*

3.1 Definição.

O *Spoofing* é uma técnica utilizada por criminosos que consiste na falsificação da identidade e de aparelhos no meio digital. Esta técnica, assim como o *Phishing,* tem o objetivo de roubar dados, disseminar *malware* ou contornar controles de acesso. Suas formas mais comuns são *spoofing* de IP[13], *e-mail*, DNS e *Caller ID*[14].

3.2*CallerIDSpoofing*.

O serviço de *CallerID*é responsável por transmitir o número de telefone e/ou o nome de quem efetua a ligação para quem está recebendo. Isso permite que quem recebeu a ligação possa aceitar ou recusar com base nessa informação (MUSTAFA; XU; SADEGHI; SCHULZ, 2014). *Caller ID Spoofing* é a falsificação da identidade de um número de telefone. Assim como em redes de computadores, a realização das ligações telefônicas acontece por meio do roteamento de pacotes e endereços. Ao redirecionar uma chamada a operadora solicita a identificação de destino e origem da ligação. Na prática isso acontece da seguinte forma: a ligação é realizada do número X para o número Y, a falsificação do ID de ligação, que é o número de cada celular, acontece quando um terceiro número W se passa pelo número X. Desta forma, o número Y receberá uma ligação de W com o identificador de X. A Figura 8 ilustra uma ligação dessa natureza. Este tipo de ação se tornou muito mais acessível com o surgimento dos serviços de VoIP (*Voice Over Internet Protocol*), que permitem realizar ligações comuns usando o protocolo IP. Esse serviço permite que o usuário escolha o ID que aparecerá no destino e era uma ação limitada antes do surgimento destes serviços, pois quem controlava os *CallersID's* eram exclusivamente as operadoras.

[13]*Internet Protocoladdress*, é um número atribuído a cada dispositivo conectado a uma rede de computadores que utiliza o Protocolo de Internet para comunicação.
[14]ID é a abreviação de *Identification,* que significa identificação.

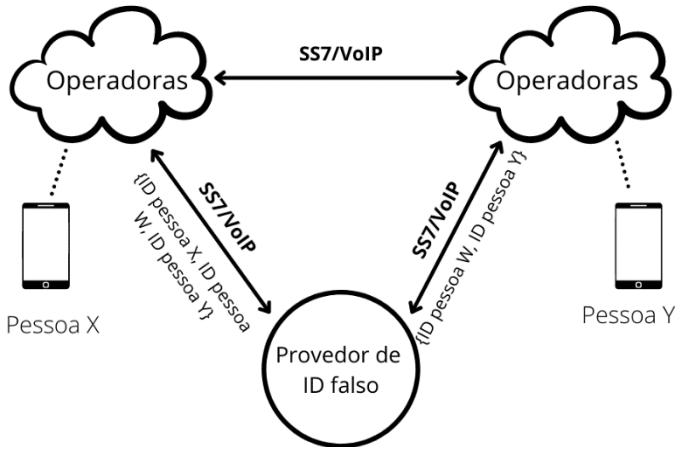


Figura 8: Diagrama do *Caller ID Spoofing*. Figura adaptada de Mustafa, Xu, Sadeghi e Schulz (2014).

Mustafa, Xu, Sadeghi e Schulz (2014) categorizam o *Caller ID Spoofing* em três tipos:

1. **Falsificação por meio de provedores de ID falsos**: Os provedores de identidade falsa oferecem serviços de falsificação de identificador de chamadas. Eles estabelecem conexões SS7 (*Signaling System Number* 7: sistemas de sinalização de canal comum (ITU, 1994)) / VoIP com várias operadoras de telefonia e atuam como intermediários entre os atacantes e as vítimas para retransmitir IDs de chamadas especificadas por seus clientes (atacantes, neste caso).
2. ***Spoofing* via serviços de VoIP:** muitas operadoras VoIP permitem que seus clientes especifiquem seu próprio identificador de chamadas e encaminham o identificador de chamadas para a operadora do receptor sem modificações. Alguém cujo objetivo é efetuar um ataque pode se inscrever em uma operadora de VoIP que permite a manipulação de identificador de chamadas e pode usar o software cliente VoIP ou um telefone VoIP para solicitar identificação de chamadas arbitrárias.
3. **Falsificação por meio de sistemas telefônicos automatizados:** os sistemas telefônicos automatizados fornecem serviços de resposta de voz interativa (IVR) para fins de *marketing*, coleta de pesquisas, etc. Alguns provedores de serviços (por exemplo:Voxeo, Nuance Cafe) permitem que seus assinantes selecionem seus próprios identificadores de chamadas e entregam os identificadores de chamadas selecionados para seus assinantes, independentemente de sua intenção. Porque esses 169 provedores se conectam às principais operadoras de telefonia via SS7 ou nos protocolos VoIP, as operadoras de telefonia *downstream* simplesmente aceitam qualquer identificador de chamadas, incluindo os falsificados.

Em uma rápida busca na Internet são encontrados serviços *online* para falsificar endereços de origem, como o Spooftel e o Asterisk, que implementam em software os recursos encontrados em um PABX, aparelho muito usado em *callcenters* para distribuir linhas e ramais, utilizando tecnologia de VoIP.

Um exemplo da aplicação do *Caller ID Spoofing*ocorreu em território brasileiro em junho de 2019, em que o Ministério da Justiça e Segurança Pública afirmou que o celular do então ministro da justiça, o juiz Sérgio Moro havia sofrido uma tentativa de invasão. Pouco mais de um mês depois, no final de julho, a Polícia Federal prendeu quatro pessoas suspeitas dessa invasão(G1, 2019). O caso repercutiu nas principais manchetes do país, pois a invasão ao celular do ministro da justiça representa um risco à segurança nacional(CORREIO DO POVO, 2019).

Com base na investigação da Polícia Federal e na decisão do juiz Vallisney de Oliveira, da 10ª Vara da Justiça Federal, de Brasília, concluiu-se que este crime foi cometido explorando uma falha na caixa postal das operadoras de telefonia móvel no Brasil. O principal objetivo dos criminosos era ter acesso total às contas do Telegram das vítimas.

O *login* padrão do Telegram solicita que o usuário entre com seu número de telefone, em seguida o aplicativo precisa confirmar a identidade de quem está tentando acessar determinada conta. Para este fim, um código de confirmação é enviado ao usuário que solicitou o *login* e são oferecidas duas opções de envio deste código: o envio de um SMS ou de uma ligação ao número que o usuário informou. Se o usuário informar corretamente o código enviado pelo servidor, o *login* é autorizado. Neste caso o objetivo dos criminosos era conseguir acesso a este código de verificação para acessar o Telegram do alvo.

Para obter os códigos de confirmação, os criminosos exploraram uma antiga falha na caixa postal das operadoras. Se ao solicitar a confirmação por ligação, a linha estiver ocupada, o código é enviado para a caixa postal da pessoa. Até então existiam duas formas de conseguir acessar a caixa postal, discando para o número do serviço, ou discando para o seu próprio número de telefone. A falha se encontrava na segunda opção, pois a operadora ao identificar que a ligação recebida tinha origem do próprio número do usuário não realizava nenhum tipo de confirmação, dando assim acesso total à caixa postal. Neste ponto da ação, o *Caller ID Spoofing* foi usado. Segundo as investigações, os criminososutilizavam o serviço de *VoIP*, BRVoz[15]. Por meio dele realizavam ligações para a vítima usando o próprio número desta mesma vítima como identificador. Quando a operadora identificava que a ligação era originada do "próprio" número, a chamada era redirecionada automaticamente para a caixa postal. Ao acessar a caixa postal os suspeitos tinham acesso ao código de verificação que havia sido salvo automaticamente pela operadora. Com o código em mãos, os suspeitos obtinham acesso total a conta do Telegram das vítimas, podendo acessar todas as trocas de mensagens e listas de contatos. Uma ilustração dessa ação é mostrada na Figura 9.

[15]Empresa que atua no segmento de serviço de VoIP.

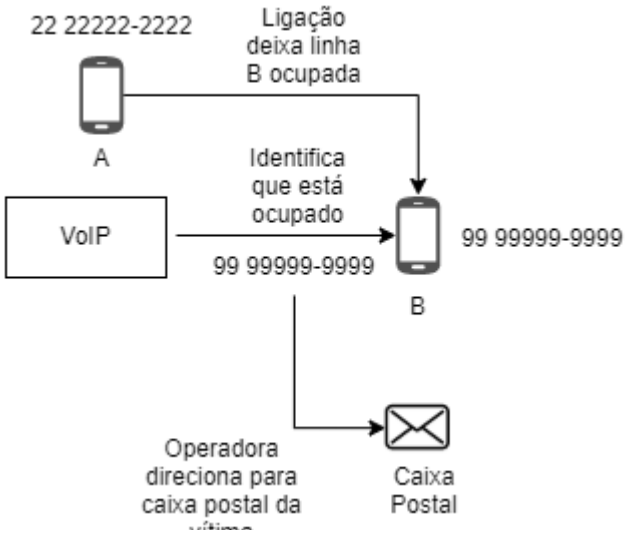


Figura 9: Simulação de um ataque a caixa postal. Fonte: Imagem do autor.

3.2.2 Clonagem de aplicativos e o *CallerIDSpoofing*.

Os aplicativos de mensagens rápidas como Telegram, Whatsapp, Facebook Messenger, Signal, entre outros, se tornam cada vez mais populares no Brasil. Uma pesquisa levantada pela Mobile Time/Opinion Box mostra que o Whatsapp está instalado em 99% dos *smarthphones* do Brasil, acompanhado pelo Facebook Messenger com 76% e pelo Telegram com 53%. Mostra também que 95% dos usuários do Whatsapp acessam o aplicativo todos os dias (MOBILETIME, OPINION BOX 2021). Com o aumento expressivo do uso destes aplicativos, surgem também os crimes efetuados utilizando-os como ferramenta. O *spoofing* via aplicativos de mensagem instantânea acontece quando por meio da Engenharia Social os criminosos se apoderam da conta pessoal de alguém nos aplicativos e enviam mensagens para os contatos das pessoas, essas mensagens podem ser pedindo dinheiro e também dados pessoais.

A PSafe, uma companhia brasileira de segurança da informação, por meio de seu laboratório especializado em segurança digital, divulgou um relatório apontando que no ano de 2020, 5 milhões de brasileiros foram vítimas do golpe da Clonagem de Whatsapp(PSAFE 2020). A clonagem de Whatsapp é um crime em que o objetivo é ter acesso às contas e perfis privados de uma empresa ou indivíduo. Com esse acesso, o criminoso obtém a lista de contatos da vítima para poder disparar mensagens em massa, a fim de obter dados pessoais e também pedindo dinheiro aos contatos. E aí que se aplica o crime de *spoofing*.

3.2.3 Medidas de proteção contra o *CallerIDSpoofing*.

A forma de proteção mais comum que é adotada por grande parte das empresas, incluindo o Telegram e o Whatsapp, para este tipo de situação é a autenticação de dois fatores (2FA). Autenticação de dois fatores é um recurso que acrescenta uma camada adicional de segurança ao processo de *login* (DONOHUE, 2014). Tomando como exemplo o aplicativo Telegram, a autenticação de dois fatores ocorre da seguinte maneira: ao se cadastrar no aplicativo é necessário fornecer um número de celular, em seguida um código de confirmação é enviado via SMS para o usuário com o objetivo de confirmar que essa tentativa de cadastro está sendo feita por uma pessoa com identidade

verdadeira. Em seguida, é necessário cadastrar o código recebido para concluir as configurações da conta de usuário. Nas configurações, o usuário tem a possibilidade de cadastrar uma senha, que será solicitada em cada tentativa de login. Deste modo, temos uma autenticação com dois fatores. Este meio de autenticação pode ser bastante dinâmico, onde um usuário pode cadastrar um endereço de *e-mail* ao invés da senha, e neste endereço será encaminhado um outro código de verificação, por exemplo. Contudo, a forma encontrada pelos criminosos no ataque ao então ministro Sérgio Moro não foi de responsabilidade do aplicativo, mas sim da operadora de telefonia responsável pela linha telefônica. Em 29 de julho de 2019, a ANATEL (Agência Nacional de Telecomunicações) proibiu a ligação para o próprio número (ESTADÃO, 2019).

3.3*E-mail Spoofing*

E-mail Spoofing é uma técnica que envolve a adulteração da fonte de um *e-mail* para que pareça que tenha sido enviado de outra fonte (IYER; ATREY; VARSHNEY; MISRA, 2017). Em 2019, a empresa de tintas AsianPaints, com sede em Mumbai, na Índia, foi vítima do *e-mail spoofing*. Nesse golpe, os criminosos fingiram ser um dos fornecedores da empresa, gerando um prejuízo de U$ 40 mil (THE TIMES OF INDIA, 2019).

Para entender como funciona o *e-mail spoofing*, é necessário compreender o surgimento de seu protocolo de transmissão, oSMTP (*Simple Mail TransferProtocol*), que é na norma RFC 821, que possui o objetivo de transferir *e-mails* com segurança e eficiência. Quando foi projetado, o SMTP não possuía mecanismos de segurança para autenticar a identidade do remetente. O *spoofing* de *e-mail* é uma parte crítica em ataques *phishing*, pois a chance do invasor ganhar confiança da vítima é maior (HU; WANG, 2018). Este protocolo é usado na transmissão e envio de *e-mails*. Banday (2011) diz que *e-mail* possui um corpo (*body*) e um cabeçalho (*header*). O cabeçalho é um componente necessário em qualquer mensagem de *e-mail* (AL-JARRAH; KHATER; AL-DUWAIRI, 2012). No *body* se inclui a mensagem a ser enviada, que pode incluir multimídias como imagens e elementos *HyperText Markup Language* (HTML) e o *header* contém as estruturas de campos que incluem ‘From’, ‘To’, ‘Date’, ‘Subject’, ‘Content-Type’, etc. (GUPTA; PILLI; MISHRA; PUNDIR; JOSHI, 2014). Essas informações são necessárias para o envio e recebimento das mensagens.

No Quadro 4, tem-se uma adaptação da análise forense escrita por Banday (2011). Neste exemplo taric@taric.com deseja enviar uma mensagem para bob@bob.com fingindo ser alice@alice.com. Os campos de endereço do remetente, data de envio, endereço de resposta e outros campos foram alterados. A seguir, será apontado quais campos foram alterados neste exemplo para que a mensagem recebida por Bob mostre dados falsos de Alice. Na linha 2 temos o campo ‘Return-Path’, que determina o endereço de *e-mail* especificado pelo remetente, o campo está preenchido com informações falsas. Na linha 5 mostra-se o endereço de IP do servidor que foi responsável por entregar o *e-mail* a Bob. A linha 11 mostra que o domínio alice.com não possui registros e também não tem uma assinatura *Domain Keys Identified Mail* (DKIM) válida. DKIM é uma especificação do *Internet EngineeringTask Force* (IETF) que define um mecanismo para autenticação de *e-mail* baseado em criptografia de chaves públicas (ANTISPAM.BR, 2006). A linha 12 contém as informações para rastreamento indicando 127.0.0.1 como o endereço IP da máquina que envia a

mensagem. Essa máquina é na verdade chamada mailbox-us-s-7b.tariq.com e tem endereço IP [a2.b2.c2.d2]. Em seguida, a linha 13 contém as informações de rastreamento indicando MTBLAPTOP como o nome da máquina que envia a mensagem. Essa máquina não é conhecida pelo receptor, mas tem um endereço IP [a1.b1.c1.d1] e tariq@tariq.com é o proprietário da caixa de *e-mail* que enviou a mensagem. O cabeçalho From, linha 14, pode ser facilmente falsificado como mostrado neste exemplo de *e-mail* e foi falsificado para conter o endereço Alice@a.com com um nome amigável de Alice. Este é o endereço, o remetente deste *e-mail* deseja que o destinatário use para enviar alguma mensagem de resposta a este*e-mail*. O campo Reply-To, na linha 21, é normalmente usado pelo remetente como um endereço para receber respostas ao *e-mail* enviado, ele é comumente falsificado neste tipo de ataque, pois enviar uma resposta a endereço errado pode gerar altos riscos de segurança. O endereço smith@smith.com, linha 21 e linha 24, é um endereço aleatório que pode não ter nenhuma relação com o remetente. Por fim, na linha 26, é indicado um nome de domínio enviado pelo servidor de envio.

Quadro 4: Cabeçalho de *e-mail spoofing*.

Linha	***Header***	***Value***
1	***X-Apparently-To:***	*bob@bob.com via a4.b4.c4.d4; Tue, 30 Nov 2010 07:36:34 -0800*
2	***Return-Path:***	*< alice@alice.com >*
3	***Received-SPF:***	*none (mta1294.mail.mud.bob.com: domainof alice@alice.com does notdesignatepermittedsender hosts)*
4	***X-Spam-Ratio:***	*3.2*
5	***X-Originating-IP:***	*[a2.b2.c2.d2]*
6	***X-Sieve:***	*CMU Sieve 2.3*
7	***X-Spam-Charsets:***	*Plain='utf-8' html='utf-8'*
8	***X-Resolved-To:***	*bob@bob.com*
9	***X-Delivered-To:***	*bob@bob.com*
10	***X-Mail-From:***	*alice@alice.com*
11	***Authentication-Results:***	*mta1294.mail.mud.bob.com from=alice.com; domainkeys=neutral (no sig); from=alice.com; dkim=neutral (no sig)*
12	***Received:***	*from 127.0.0.1 (EHLO mailbox-us-s-7b.tariq.com) (a2.b2.c2.d2) by mta1294.mail.mud.bob.com with SMTP; Tue, 30 Nov 2010 07:36:34 -0800*

13	***Received:***	*from MTBLAPTOP (unknown [a1.b1.c1.d1]) (Authenticatedsender: tariq@tariq.com) by mailbox-us-s-7b.tariq.com (Postfix) with ESMTPA id 8F0AE139002E for ; Tue, 30 Nov 2010 15:36:23 +0000 (GMT)*
14	***From:***	*"Allice" <Allice@a.com>*
15	***Subject:***	*A Sample Mail Message*
16	***To:***	*"Bob Jones" <bob@bob.com>*
17	***Content-Type:***	*multipart/alternative; charset="utf-8"; boundary="KnRl8MgwQQWMSCW6Q5=_HgI2hw Adah5NLY"*
18	***MIME-Version:***	*1.0*
19	***Content-Transfer-Encoding:***	*8bit*
20	***Content-Length:***	*511*
21	***Reply-To:***	*"Smith" <smith@smith.com*
22	***Organization:***	*AlicesOrganization*
23	***Date:***	*Tue, 28 Nov 2010 21:06:22 +0530*
24	***Return-Receipt-To:***	*smith@smith.com*
25	***Disposition-Notification-To:***	*jones@jones.com*
26	***Message-Id:***	*<20101130153623.8F0AE139002E@mailbox-us-s7b.tariq.com>*

Fonte: Banday, 2011.

Neste exemplo de mensagem de *e-mail* do Quadro 4, vários campos foram falsificados, o que pode ser detectado facilmente porque o primeiro campo *Received* (linha 12) mostra o endereço de remetente, que é diferente do remetente da mensagem.

Uma das formas de verificar se o conteúdo de um *e-mail* é proveniente de um remetente confiável, é verificar os dados detalhados da mensagem. O Gmail, servidor usado pela UFGD para fornecer *e-mails* institucionais para os alunos, possui uma ferramenta na qual é possível visualizar o conteúdo completo de uma mensagem de *e-mail*, que inclui todo o *header* e *body*. A Figura 9 mostra um *e-mail* institucional enviado pela Universidade.

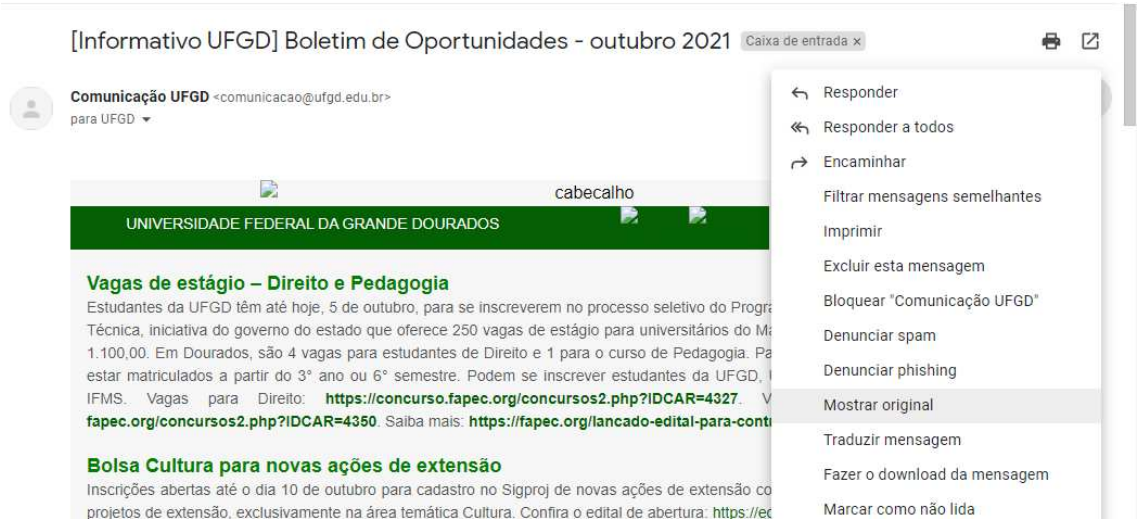


Figura 9: Menu que o Gmail disponibiliza para visualizar todo o conteúdo de um *e-mail*. Fonte: Imagem do autor.

Ao clicar no menu do *e-mail* (Figura 9), pode-se abrir a mensagem original, e são obtidos dados mais detalhados do cabeçalho, como mostrado no Quadro 5.

Quadro 5: Dados detalhados do cabeçalho.

1	ID da mensagem	<CAA8jojGtW7J2CSXZBc0ndjkxKbkd1hbH0sPDmefpbybntDmYmA@mail.gmail.com>
2	Criado em:	5 de outubro de 2021 15:07 (entregue após 48 segundos)
3	De:	Comunicação UFGD <comunicacao@ufgd.edu.br>
4	Para:	UFGD <ufgd@ufgd.edu.br>
5	Assunto:	[Informativo UFGD] Boletim de Oportunidades - outubro 2021
6	SPF:	PASS com o IP 209.85.220.69
7	DKIM:	'PASS' com o domínio ufgd-edu-br.20210112.gappssmtp.com
8	DMARC:	'PASS'

Fonte: Elaborado pelo autor.

Consultando o endereço IP mostrado na linha 6 no portal who.is (https://who.is/), um *site* que disponibiliza informações de domínio, propriedades de IPe verifica dezenas de outras estatísticas, confirmando que o endereço realmente pertence ao Google. A Figura 10 mostra a verificação retornada pelo *site*Whois, em que o Google é o responsável pelo serviço Gmail.

```
NetRange:       209.85.128.0 - 209.85.255.255
CIDR:           209.85.128.0/17
NetName:        GOOGLE
NetHandle:      NET-209-85-128-0-1
Parent:         NET209 (NET-209-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   Google LLC (GOGL)
RegDate:        2006-01-13
Updated:        2012-02-24
Ref:            https://rdap.arin.net/registry/ip/209.85.128.0
```

Figura 10: Verificação de IP realizada no *site* Who.is. Fonte: Imagem do autor.

3.3.2Medidas de proteção contra o *E-mail Spoofing.*

Quando se trata de proteção contra o *e-mail spoofing* nas organizações, existem duas preocupações principais: como proteger que meu domínio sofra um ataque e como evitar receber mensagens enganosas. Crane (2020) mostra quatro pontos que podem ajudar a mitigar o seu endereço de *e-mail* ou domínio de serem expostos. O primeiro é implementar padrões de segurança em *e-mails*: o *SenderPolicy Framework* (SPF) define endereços IP válidos que são aprovados para enviar *e-mails* para um domínio específico. O *Domain Keys Identified Mail* (DKIM) atualiza a entrada DNS de um domínio de *e-mail* para adicionar uma assinatura digital ao cabeçalho da mensagem e garantir que o *e-mail* permaneça inalterado desde o momento em que foi enviado. *Domain-basedMessageAuthenticationReportingandConformance* (DMARC) é um protocolo de autenticação, relatório e política de *e-mail* que usa SPF e DKIM para fornecer informações sobre o domínio de *e-mail* (alinhamento, conformidade, falhas etc.). Já o segundo ponto levantado por Crane (2020) é um certificado de assinatura de *e-mails* que confirma a identidade através do uso de assinaturas digitais e usa criptografia de chave pública para fornecer segurança, e criptografia ponta a ponta[16] para seus e-mails. Considerando que a maioria dos servidores de *e-mail* hoje em dia também usam criptografia SSL / TLS, isso significa que você pode usar os dois tipos de proteção de dados transportados. O terceiro ponto é o treinamento cujo tema, é tratado seção 2.1. E por fim, a checagem da *header* de um *e-mail*, como mostrado no Quadro 5 e na Figura 10.

3.4IP*Spoofing.*

IP Spoofing é uma técnica que consiste em mascarar um endereço para realizar um acesso, ou algo similar, indevidamente. Nesse sentido,busca aparentar que um acesso foi realizado por um determinado endereço IP, quando na verdade foi realizado por outro. Uma analogia que pode ser feita é quando um invasor deseja enviar um pacote para alguém com o remetente escrito de maneira enganosa (CLOUDFLARE, 2021). Essa abordagem pode ser usada para atrapalhar investigações forenses,pois o

[16] Criptografa os dados durante uma troca de mensagens, de forma a que o conteúdo só possa ser acessado pelos dois extremos da comunicação: o remetente e o destinatário.

endereço IP é uma informação necessária para investigação de crimes virtuais (MACIEL; VITERBO, 2020). Ao utilizar um endereço falso, registros de *sites* e servidoresarmazenam informações que não são úteis em investigações.Dessa forma, o trabalho da perícia forense é prejudicado.

A Figura 11 ilustra a interação entre um computador que solicita páginas usando um endereço IP falsificado e o servidor *web* que responde às solicitações. O computador A envia uma solicitação para o servidor usando um falso endereço de IP.Neste caso, o endereço real é 192.168.0.5, porém, o servidor recebe a solicitação de um IP identificado como 172.16.0.6. Dessa forma, o servidor tentará enviar a resposta para o endereço que ele acredita ser o real, ou seja, enviará informações para o verdadeiro endereço que pertence a máquina B. A máquina B simplesmente irá descartar as informações não solicitadas.

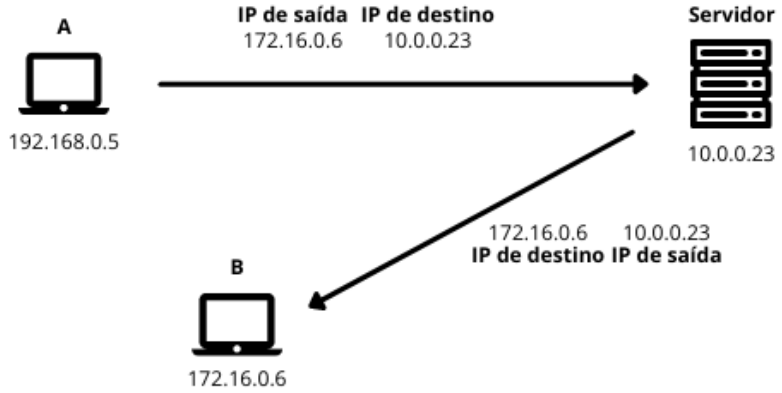


Figura 11: IP Spoofing. Fonte: Imagem do autor.

Para descrever como funciona o *IP Spoofing*, é necessário expor brevemente como funciona a transmissão de dados pela internet. Na internetcada bit de informação é enviado pelo que chamamos de pacote. Esse pacote contém o endereço da fonte e o de destino. Este último é usado para definir para onde o pacote será enviado através de roteamento. Roteador é o dispositivo responsável pelo encaminhamento de pacotes de comunicação em uma rede ou entre redes (ELIAS; LOBATO, 2013). Hoje, a Internet é construída com base no protocolo TCP/IP. Este protocolo é organizado em quatro camadas (Figura12): aplicação, transporte, rede e interface de rede. O *IP Spoofing* acontece na camada de rede.

Figura 12: Camadas do protocolo TCP/IP. Fonte: Elias e Lobato (2013, p. 62)

O roteamento de um pacote é ponto-a-ponto, ou seja, cada pacote é enviado para o próximo roteador conforme sua tabela de roteamento. Cada pacote de IP é enviado separadamente. A rota de um pacote IP é decidida por todos os roteadores pelos quais o pacote passa. A falsificação de endereço IP é possível porque os roteadores exigem apenas a inspeção do endereço IP de destino no pacote para tomar decisões de roteamento. O endereço IP de origem não é exigido pelos roteadores e um endereço IP de origem inválido não afetará a entrega de pacotes. Esse endereço só é usado pela máquina de destino quando ela responde de volta à origem (RAHMAN; ZHOU, 2015).

Por sua vez, Rashid e Pau (2013) levantam uma lista de ataques com a aplicação de *IP Spoofing*. Embora alguns sejam problemas de segurança já conhecidos, outros trazem discussões pertinentes aos dias atuais, são eles:

- *Non-Blind Spoofing*: ocorre quando o atacante está na mesma sub-rede da vítima. Por este motivo, o bloco de endereços IP é limitado, o que pode ajudar na detecção.
- *Blind Spoofing*: geralmente ocorre fora da sub-rede local, dessa forma, os endereços IP não são limitados. Por este fato, a verificação destes endereços não será possível.
- *HijackinganAuthorizedSession*: endereços falsos são usados afim de obter acessos não autorizados em um sistema.
- *Man in the Middle Attack*: acontece quando o criminoso intercepta o fluxo de informações que estão sendo transmitidas pela rede e passa a controlar quais pacotes serão enviados ou não. Ele também pode alterar as informações contidas em cada pacote.
- *DistributedDenialof Service Attack*: O *spoofing* de IP é usado principalmente em ataques distribuídos de negação de serviço (DDoS), nos quais os *hackers* estão preocupados em consumir largura de banda e recursos, são enviadas diversas requisições para a máquina que é o *host* de destino com o máximo de pacotes possíveis em um curto espaço de tempo. Para conduzir o ataque com eficácia, os hackers falsificam os endereços IP de origem para tornar o rastreamento e a interrupção do DDoS o mais difícil possível.

3.4.2 Proteção contra o IP*Spoofing*.

Quando se trata da proteção contra o *IP Spoofing*, deve-se entender que é uma técnica em que o usuário comum é praticamente incapaz de se proteger. Umas das poucas recomendações é procurar navegar em *sites* que usam protocolos de conexão criptografados, como o *HyperTextTransferProtocolSecure* (HTTPS) (KASPERSKY, 2021).

Hassan (2019) mostra como a proteção em baixo nível deve ser implementada para proteção das organizações. Recomenda-se:

- O uso de protocolos como o IPSec, que é um protocolo que protege os pacotes IP, encapsulando-os em outros pacotes IP para serem transportados.

- Usar listas de controle de acesso para filtrar endereços IP privados em sua interface. Implementar filtragem do tráfego de entrada e saída.
- Configurar roteadores e switches, para rejeitar pacotes originados de fora de sua rede local que afirmam ser originados de dentro.
- Habilitar criptografia nos roteadores para que *hosts* confiáveis que estão fora de sua rede possam se comunicar com segurança com seus *hosts* locais.

A próxima seção aborda o crime de *Ransomware,* explicando no que consiste, como é realizado e os mecanismos disponíveis para proteção.

4 *Ransomware*

Em maio de 2017, mais de 150 países foram afetados por um ataque mundial de *ransomware.* Mais de 100 mil empresas e grupos foram afetados (CBS NEWS, 2017). Estima-se que os prejuízos causados por este ataque são de aproximadamente 4 bilhões de dólares (JONATHAN BERR, 2017). Um dos maiores ataques cibernéticos da história foi causado pelo *ransomware*conhecido como *Wannacry*(IAN SHERR, 2017). Em abril de 2017, um grupo de *hackers* criminosos conhecidos como Shadow Brockers, se utilizou de uma ferramenta chamada The EternalBlue, que foi roubada da Agência Nacional de Segurança dos Estados Unidos (MOYER, 2019). Com essa ferramenta em mãos, foram exploradas vulnerabilidades em diferentes versões do Windows, como o Windows Vista, Windows 7, Windows Server 2008, Windows 8.1, entre outros. Depois que a vítima abre um arquivo malicioso (como um anexo de *e-mail*, por exemplo) contendo o código do *ransomware*, o *WannaCry* começará a se propagarem todas as LANs conectadas e a outros computadores na Internet, afetando todos computadores Windows que sofrem desta vulnerabilidade (HASSAN, 2019). Diversas empresas foram afetadas, como a FedEx e Nissan, empresas ferroviárias na Alemanha, na Rússia, empresas de telecomunicações como a Telefonica na Espanha (MOHURLE; PATIL, 2017). A transportadora multinacional FedEx, por exemplo, teve um prejuízo estimado em 300 milhões de dólares (LAWLER, 2017).

Ransomware é um termo utilizado para descrever uma classe de *malwares* que são usados pelos criminosos para extorquir digitalmente as vítimas para o pagamento de alguma taxa específica (LISKA; GALLO, 2017). Impede os usuários de acessar seus computadores e/ou dados pessoais usando vários métodos, pode-se considerar que, mediante o pagamento da extorsão, não pretende causar nenhum dano ao sistema de arquivos do computador, os deixa funcional para exibir a mensagem de resgate (HASSAN, 2019). Porém, sem o pagamento, os arquivos se tornam inúteis e o computador inacessível. A vítima, ao ser condicionada ao pagamento de alguma quantia em dinheiro, configura o crime de extorsão, previsto no art. 158 do Código Penal (MACIEL;VITERBO, 2020).

Liska e Gallo (2017) classificam o *Ransomware* em dois tipos: *LockerRansomware* e *CryptoRansomware*. O primeiro tipo consiste na negação de acesso do usuário aos seus recursos ou dados, por exemplo, bloqueando a área de trabalho ou impedindo o usuário de efetuar *login* na máquina. Já na segunda categoria o ataque é baseado na criptografia de todos os dados e arquivos da máquina de destino, que só são descriptografados mediante o pagamento de resgate. A Figura 13 mostra a classificação destes ataques.

Figura 13: Classificação de *ransomware*. Baseado em Liska e Gallo (2017).

Nesta seção será abordado o *modus operandi* dos dois tipos citados anteriormente, trazendo uma abordagem analítica do ponto de vista técnico.

A criptografia é uma ferramenta muito importante nos sistemas informáticos, pois permite que os dados sejam armazenados com um nível de segurança muito maior do que deixá-los armazenados sem esse método. Entretanto, a utilização dessa tecnologia pode ser aplicada em outro contexto, o de extorsão.

O *Cryptolocker* é um *trojan* que é categorizado no tipo *CryptoRansomware*, que será descrito com o objetivo de explicar de maneira geral o funcionamento desta categoria de ataque. O *Cryptolocker* é direcionado ao Microsoft Windows e circula desde o final de 2013. Geralmente, é propagado como uma extensão de uma aparentemente notificação por *e-mail* inofensiva (KONG, 2020). Assim que é executado ele imediatamente começa a escanear unidades de rede, renomeia todos os arquivos e pastas e os criptografa (SALVI; KERKAR, 2014). Aziz (2016) lista dois tipos de algoritmos de criptografia que são muito utilizados em ataques do tipo *CryptoLocker*, o *AdvancedEncryptionSymmetric* (AES) e o Rivest-Shamir-Adleman (RSA).

A Bleeping Computer (2013) levantou um guia descrevendo o funcionamento deste *trojan* no Windows. Quando for infectado pela primeira vez, o *trojan* fica armazenado com um nome aleatório no diretório *%AppData%* ou *%LocalAppData%*. Em seguida, são criados registros de inicialização automática para executar o *trojan* assim que o *login* no computador for realizado. O Quadro 6 mostra um exemplo dos registros criados. Os asteriscos no final dos valores de registro fazem com que o *CryptoLocker* seja iniciado no modo de segurança.

Quadro 6: Registros alterados pelo *CryptoLocker*.

Linha	Registo
1	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run "CryptoLocker"
2	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ru

	nOnce "* CryptoLocker"
3	KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run" CryptoLocker_ <version_number>"
4	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce "* CryptoLocker_ <version_number"

Fonte: Elaborado pelo autor.

Os arquivos com extensão ".exe" também são afetados, para que, quando o usuário iniciar um executável, sejam excluídas as cópias Shadow Volume que estão no computador afetado. Shadow Volume é uma ferramenta que permite criar cópias de segurança de arquivos na máquina do usuário, tornando possível voltar ao ponto anterior ou fazer uma restauração do sistema (AMAYA, 2017). Ele faz isso para impedir que o uso de cópias de Shadow Volumes seja usado para restaurar os arquivos criptografados. O comando que o *trojan* executa quando o usuário clica em um executável malicioso é:

"C:\Windows\SYsWOW64\cmd.exe" /C "C:\Windows\Sysnative\vssadmin.exe" Delete Shadows /All /Quiet

Os registros também são alterados, como mostrado no Quadro 7. Pode-se observar que os nomes são aleatórios. Após excluir as cópias Shadow Volume, os arquivos com extensão ".exe" são restaurados aos padrões do Windows.

Quadro 7: Registros alterados. Fonte: Elaborado pelo autor.

Linha	Registo
1	[HKEY_CLASSES_ROOT\.exe]@="Myjiaabodehhltdr""Content Type"="application/x-msdownload"
2	[HKEY_CLASSES_ROOT\.exe\PersistentHandler]@="{098f2470-bae0-11cd-b579-08002b30bfeb}"
3	[HKEY_CLASSES_ROOT\Myjiaabodehhltdr]
4	[HKEY_CLASSES_ROOT\Myjiaabodehhltdr\DefaultIcon] @="%1"
5	[HKEY_CLASSES_ROOT\Myjiaabodehhltdr\shell]
6	[HKEY_CLASSES_ROOT\Myjiaabodehhltdr\shell\open]
7	[HKEY_CLASSES_ROOT\Myjiaabodehhltdr\shell\open\command] @="\"C:\\Users\\User\\AppData\\Local\\Rlatviomorjzlefba.exe\" -\"%1\" %*"

Este ataque requer que alguma forma de comunicação seja estabelecida para garantir que este possa ocorrer (LISKA; GALLO, 2017). Dessa forma, será efetuada uma tentativa de conexão o que é chamado de "*Command andControl Server*" (C&C), que são sistemas de computador usados por invasores para enviar e receber comandos de máquinas que fazem parte de uma rede automatizada usadas neste tipo de ataque.

Desse modo,assim que um servidor C&C ativo for descoberto,será realizada uma conexão e será baixada uma chave de criptografia pública que será usada para criptografar seus arquivos de dados. Em seguida, essa chave será armazenada junto com outras informações nos valores da chave de registro no caminho "HKEY_CURRENT_USER \ Software \ CryptoLocker_0388". Na sequência, a chave privada usada para descriptografarosarquivos infectados é salva no servidor de comando e controle. Na continuidade, oCryptoLockerirá examinar todas as unidades de rede físicas ou mapeadas em seu computador em busca de arquivos com as seguintes extensões:

> * .odt, * .ods, * .odp, * .odm, * .odc, * .odb, * .doc, * .docx, * .docm, * .wps, * .xls, * .xlsx, * .xlsm, * .xlsb, * .xlk, * .ppt, * .pptx, * .pptm, * .mdb, *. accdb, * .pst, * .dwg, * .dxf, * .dxg, * .wpd, * .rtf, * .wb2, * .mdf, * .dbf, * .psd, * .pdd, * .pdf, * .eps, * .ai, * .indd, * .cdr, * .jpg, * .jpe, * .jpg, * .dng, * .3fr, * .arw, * .srf, * .sr2, *. bay, * .crw, * .cr2, * .dcr, * .kdc, * .erf, * .mef, * .mrw, * .nef, * .nrw, * .orf, * .raf, * .raw, * .rwl, * .rw2, * .r3d, * .ptx, * .pef, * .srw, * .x3f, * .der, * .cer, * .crt, * .pem, * .pfx, *. p12, * .p7b, * .p7c.

Ao encontrar arquivos que correspondam a um desses tipos, ele criptografará o arquivo usando a chave de criptografia pública e adicionará o caminho completo para o arquivo e o nome do arquivo como um valor na chave de registro "HKEY_CURRENT_USER \ Software \ CryptoLocker_0388 \ Files".

4.2 Medidas de proteção contra *CryptoLocker*.

Por sua vez, Richardson e North (2017) mostram que a proteção contra esse tipo de ataque é dividida entre proteção do usuário comum e de organização. Para a proteção do usuário comum, são recomendados quatro passos que buscam aumentar o nível de segurança, que são:

- *Backup*: possuir um sistema de *backup* dos arquivos, o mais atual possível, para evitar grandes perdas. Alguns *ransomwares* tentam criptografar sistemas de *backup* conectados na rede local, então, recomenda-se o uso de um *backup* em nuvem ou um sistema que só está conectado enquanto o *backup* está sendo feito, como um HD externo, por exemplo. Também é importante manter várias versões e cópias dos *backups*. Se o *backup* dos arquivos for feito com segurança, os usuários podem remover arquivos e software infectados de um computador e redefini-lo para o que é chamado de condição de fábrica (ROSENBERG, 2015).
- *E-mails*: ataques de *phishing* são a forma mais comum de se espalhar *ransomware*. Evitar clicar em *links* ou abrir anexos em e-*mails* desconhecidos ou suspeitos.
- *Patch andBlock*: o sistema operacional, navegadores e softwares de segurança devem sempre ser mantidos corrigidos e atualizados.
- *Drop-and-Roll*: ao primeiro sinal de infecção por *ransomware*, a máquina infectada deve ser imediatamente desligada e desconectada da rede, para minimizar os danos aos arquivos.

Segundo *Federal BurealofInvestigation* (FBI), quando se trata do *ransomware*nas organizações, o que acontece muitas vezes é que após ser vítima, a empresa acaba optando por pagar a taxa de extorsão e não recebe nenhuma chave para descriptografia(FBI, 2016). Por este motivo, este órgão, não recomenda o pagamento da extorsão. Para evitar que isso aconteça, algumas precauções podem ser tomadas. Richardson e North (2017) citam três pontos, que são: entender os riscos, desenvolver políticas de segurança e instituir melhores práticas para o usuário. Além disso, o FBI recomenda algumas ações para atingir esses objetivos de segurança.

- Certificar de que os *softwares* antivírus e *antimalware* sejam configurados para realizar atualizações automaticamente e realizar verificações regulares nos computadores e sistemas.
- Gerenciar o uso de contas com privilégios, pois nenhum usuário deve receber acesso administrativo, a menos que seja absolutamente necessário, e use contas de administrador apenas quando necessário.
- Configurar os controles de acesso, incluindo acesso a arquivos, diretórios e permissões de compartilhamento de rede de forma apropriada. Se os usuários precisam apenas ler informações específicas, eles não precisam ter acesso de gravação a esses arquivos ou diretórios. Desse modo, deve-se desativar os*scripts* de macro de arquivos de escritório transmitidos por *e-mail*.
- Implementar políticas de restrição de software ou outros controles para evitar que programas sejam executados em locais comuns de *ransomware* (por exemplo, pastas temporárias que oferecem suporte a navegadores de Internet populares, programas de compactação / descompactação)

No entanto, os riscos de ataques não se limitam ao *Cryptolocker*.Novas possibilidades de ataque são conduzidas pelo*LockerRansomware,* que é um *ransomware* que não criptografa os arquivos na máquina da vítima. Ele bloqueia a tela e não permite que mais nenhum tipo de ação até que o resgate seja pago (MOHANTA; HAHAD; VELMURUGAN, 2018). Esse tipo de abordagem também é chamado de *ScreenLockerRansomware*. Neste contexto,Mohanta, Hahad e Velmurugan (2018) listam os mais populares tipos de *ScreenLocker*, dentre eles está o Reveton. O Reveton se utiliza de engenharia social para exibir mensagens de aviso para vítimas alegando que seu computador foi bloqueado por alguma autoridade da lei (YOUNG, 2020). Como exemplo, na Figura 13 o autor do ataque envia uma mensagem para a vítima alegando que o computador foi bloqueado por *download* e distribuição de “material suspeito” (CIMPANU, 2018).

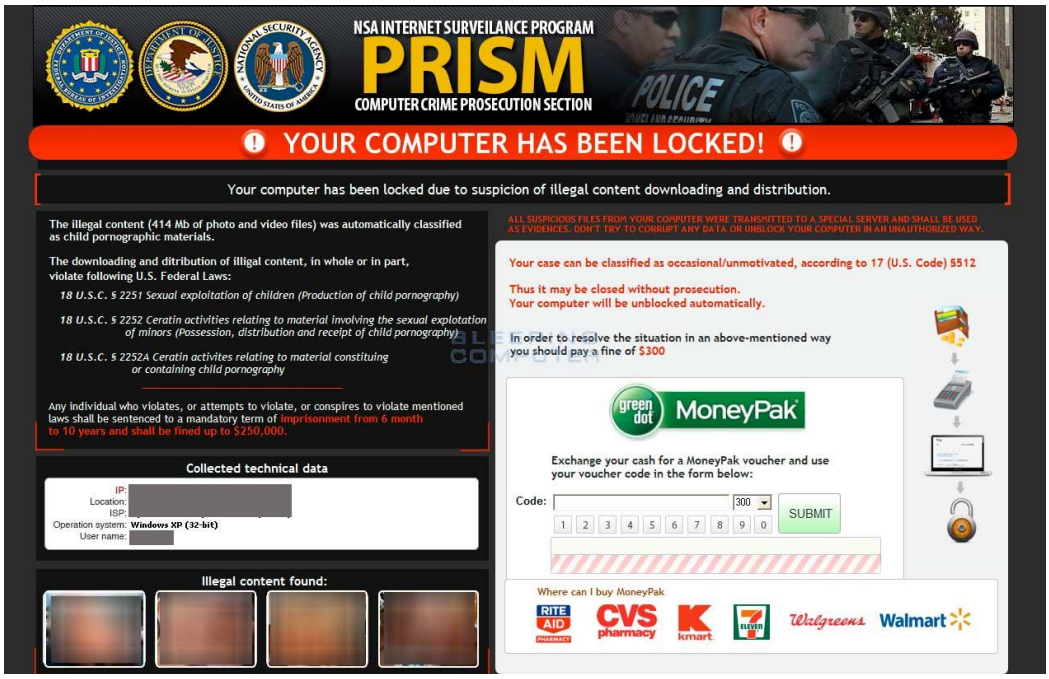


Figura 14: Exemplo de bloqueio por Reveton*ransomware*. Fonte: Cimpanu,2018.

Horejší (2012) faz uma análise do funcionamento desse ataque. Após o *ransomware* ser instalado, a área de trabalho do computador será bloqueada. Como mostrado na Figura 14, uma quantia em dinheiro é exigida para a liberação do computador. Esse pagamento é uma fraude. No exemplo da Figura 14, os criminosos disponibilizam a ferramenta de pagamentos MoneyPak, que é uma carteira digital muito popular nos EUA. Por ter um meio de pagamento prático, muitas vítimas assustadas acabam caindo na fraude.

O Reveton começa a após a inicialização do computador, portando, reiniciar não funciona. O malware é criado com o nome "*ctfmon.lnk*" na seguinte pasta:

"C: \ Documentsand Settings\<username>\Start Menu\Programs\Startup"

O arquivo carrega o seguinte comando que inicia o malware na inicialização:

"% systemroot% \ system32 \ rundll32.exe <path_to_malware>, FQ10"

O Reveton é um *ransomware* que possui uma maneira mais prática para sua remoção da máquina. Horejší (2012), em seu artigo, mostra um passo a passo para removê-lo computador. Primeiro, reiniciar o computador no modo de segurança. Em seguida, ir até o diretório mencionado acima e deletar o arquivo "*ctfmon.ink*". E, por fim, reiniciar o computador em modo normal.

As formas de proteção contra este tipo são as mesmas mencionadas por Richardson e North (2017).

5. Considerações finais

Neste artigo, foi realizada uma revisão bibliográfica com o objetivo de descrever três crimes virtuais que são muito comuns no ambiente online. Visando o comum ou organizações, sejam elas governamentais ou privadas.

Conforme a análise realizada, percebe-se que muitas vezes os criminosos acabam se utilizando de diversas técnicas com o mesmo objetivo: obter vantagens sobre terceiros.Ressalta-se que não é necessário um grande conhecimento técnico para aplicar e explorar os crimes virtuais.

Observa-se que as técnicas apresentadas são interligadas. O principal meio de transmissão do *ransomware* é via *phishing*, por exemplo. E o *e-mail spoofing*, é uma das formas de tornar o *phishing* o mais crível possível. A engenharia social como principal fator de sucesso dos criminosos é explicada por diversos especialistas. Conclui-se que, os criminosos podem combinar diversas técnicas e tecnologias para cometer o crime desejado.

Mesmo seguindo os protocolos de segurança, os usuários sempre podem ser potenciais vítimas de crimes virtuais. Caso isso aconteça, deve-se procurar os meios legais para que possa haver a devida investigação e que os responsáveis sejam punidos devidamente. Frederighi (2021) fez um levantamento dos passos que devem ser seguidos caso uma pessoa se torne vítima de um crime virtual. O primeiro passo é coletar o máximo de evidências possíveis. Considera-se evidência captura de telas (computadores, celulares, e etc.), trocas de mensagens, *e-mails*, documentos, fotos, registros de chamadas, nomes de usuários e etc. E por fim, procurar os órgãos competentes para registrar o crime. No Brasil pode ser procurar delegacias de polícia, e também o Ministério Público. Em casos de crimes que envolvam menores de idade, o Conselho Tutelar também pode ser procurado. Maciel e Viterbo (2019) mostram como o poder judiciário, mediante investigações, é capaz de encontrar e punir responsáveis por praticar crimes virtuais.

Como trabalhos futuros, pode-se realizar uma pesquisa estatística aplicada no contexto da UFGD (Universidade Federal da Grande Dourados), cujo objetivo é levantar dados de possíveis vulnerabilidades que os usuários inseridos no ambiente acadêmico estão propensos. A partir dos dados obtidos, a elaboração de um plano de ações para mitigar perdas futuras deve ser projetado com intenção de implementação pela universidade.

Referências

AL-JARRAH, Omar; KHATER, Ismail; AL-DUWAIRI, Basheer. **IdentifyingPotentiallyUsefulEmail Header Features for Email Spam Filtering**. In: INTERNATIONAL CONFERENCE ON DIGITAL SOCIETY, 6., 2012, Valencia. ICDS 2012, The SixthInternationalConferenceon Digital Society. Valencia: Icds, 2012. p. 140-145.

AKITA, Fabio. **RANT: Selo de Segurança é Marketing: Entendendo o Fator Humano.** 2020. Disponível em: https://www.akitaonrails.com/2020/12/08/akitando-

88-rant-selo-de-seguranca-e-marketing-entendendo-o-fator-humano. Acesso em: 03 out. 2021.

AMAYA, Camilo Gutiérrez. **Shadow Copies: a funcionalidade de backup do Windows**. 2017. Disponível em: https://www.welivesecurity.com/br/2017/10/18/shadow-copies-backup-do-windows/. Acesso em: 20 out. 2021.

ANTISPAM.BR. **Domain Keys Identified Mail**. 2006. Disponível em: https://www.antispam.br/admin/dkim/. Acesso em: 12 out. 2021.

AZIZ, Shallaw. M..**Ransomware in High-Risk Environments**. 2016. 38 f. – DepartmentOfComputingAndInformationSciences, Valparaiso University, United States OfAmerica, 2016.

BANDAY, M. Tariq. **Technology Corner: Analysing E-Mail Headers for ForensicInvestigation**. Journal Of Digital Forensics. Kashmir, p. 49-64. jan. 2011.

BISHOP, Matthew A..**Introductionto Computer Security**. Massachusetts: Addison-Wesley, 2003

BLEEPING COMPUTER. **CryptoLockerRansomwareInformationGuideand FAQ**. Disponível em: https://www.bleepingcomputer.com/virus-removal/cryptolocker-ransomware-information. Acessoem: 20 out. 2021.

CBS NEWS. **Cyberattack hit more than 100,000 groups in atleast 150 countries, Europolsays**. 2017. Disponível em: https://www.cbsnews.com/news/cyberattack-hit-more-than-100000-groups-in-at-least-150-countries-europol-says/. Acessoem: 04 out. 2021.

CIMPANU, Catalin. **Microsoft EngineerCharged in RevetonRansomware Case**. 2018. Disponível em: https://www.bleepingcomputer.com/news/security/microsoft-engineer-charged-in-reveton-ransomware-case/. Acesso em: 25 out. 2021.

CLOUDFLARE. **Whatis IP spoofing?** Disponível em: https://www.cloudflare.com/pt-br/learning/ddos/glossary/ip-spoofing. Acesso em: 12 out. 2021.

COMODO. **Computer Vulnerability: Definition**. 2018. Disponível em: https://enterprise.comodo.com/blog/computer-vulnerability-definition. Acesso em: 07 ago. 2019.

CORREIO DO POVO. **Inquérito dos hackers aponta crime contra a segurança nacional.** 2019. Disponível em: https://www.correiodopovo.com.br/not%C3%ADcias/pol%C3%ADcia/inqu%C3%A9rito-dos-hackers-aponta-crime-contra-a-seguran%C3%A7a-nacional-1.368807. Acesso em: 03 out. 2021.

CRANE, Casey. **EmailSpoofing 101: HowtoAvoidBecoming a Victim**. 2020. Disponível em: https://securityboulevard.com/2020/01/email-spoofing-101-how-to-avoid-becoming-a-victim/. Acessoem: 18 out. 2021.

DAEMEN, Joan; RIJMEN, Vincent. **AES Proposal**: Rijndael. Belgium: Independent, 1999. 45 p.

DIÁRIO DA AMAZÔNIA. **62 milhões de pessoas foram vítimas de crimes virtuais**. 2019. Disponível em: https://www.diariodaamazonia.com.br/62-milhoes-de-pessoas-foram-vitimas-de-crimes-virtuais/?dinamico. Acesso em: 19 ago. 2019.

DONOHUE, Brian. **O que é a autenticação de dois fatores e como usá-la?** 2014. Disponível em: https://www.kaspersky.com.br/blog/o-que-e-a-autenticacao-de-dois-fatores-e-como-usa-la/3226/. Acesso em: 12 mar. 2020.

ELIAS, Glêdson; LOBATO, Luiz Carlos. **Arquitetura e Protocolos de Rede TCP-IP**. Rio de Janeiro: Rnp, 2013.

ESET. **Falsa campanha de vacinação contra a Covid□19 propaga o trojan bancário Mekotio.** São Paulo: Eset Brasil, 2021. Disponível em: https://www.welivesecurity.com/br/2021/05/06/falsa-campanha-de-vacinacao-contra-a-covid-19-propaga-o-trojan-bancario-mekotio/. Acessoem: 26 set. 2021.

ESET. **Complete Antivirus Software for allofyour devices**. 2021. Disponível em: https://www.eset.com/gr-en/antivirus-software/. Acesso em: 12 out. 2021.

ESTADÃO. **Crimes virtuais afetam 42 milhões de brasileiros**. 2017. Disponível em: https://economia.estadao.com.br/noticias/releases-ae,crimes-virtuais-afetam-42-milhoes-de-brasileiros,70001644185. Acesso em: 10 ago. 2019.

ESTADÃO. **Após ataque hacker explorar brecha, Anatel proíbe ligação para o próprio número**. 2019. Disponível em: https://politica.estadao.com.br/blogs/fausto-macedo/apos-ataque-hacker-explorar-brecha-anatel-proibe-ligacao-para-o-proprio-numero. Acesso em: 12 mar. 2020.

FBI. **IncidentsofRansomwareontheRise**. 2016. Disponível em: https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise?__cf_chl_jschl_tk__=pmd_Nw.hgPM25xkIOLba71gQqVvNP3UmpsLsIFpsF.BxAOc-1635632666-0-gqNtZGzNApCjcnBszQjR. Acesso em: 30 out. 2016.

FREDERIGHI, Daniel. **Crimes virtuais: como se proteger e denunciar?** 2021. Disponível em: https://jus.com.br/artigos/93032/crimes-virtuais-como-se-proteger-e-denunciar. Acesso em: 26 out. 2021.

G1. **Celular de Sérgio Moro sofre tentativa de invasão, e Ministério da Justiça apura incidente**. 2019. Disponível em: https://g1.globo.com/politica/noticia/2019/06/05/celular-de-sergio-moro-sofre-tentativa-de-invasao-e-ministerio-da-justica-apura-incidente.ghtml. Acesso em: 03 out. 2021.

G1. **Polícia Federal prende quatro em operação que investiga invasão do celular de Sergio Moro**. 2019. Disponível em: https://g1.globo.com/politica/noticia/2019/07/23/pf-deflagra-operacao-em-busca-de-hacker-que-invadiu-celular-de-moro.ghtml. Acesso em: 03 out. 2021.

GUPTA, Surekha; PILLI, Emmanuel S.; MISHRA, Preeti; PUNDIR, Sumit; JOSHI, R. C..**Forensicanalysisof E-mail addressspoofing**. In: InternationalConference-Confluence The Next Generation Information Technology Summit, 5., 2014, Noida. 2014 5th InternationalConference - Confluence The Next Generation Information Technology Summit (Confluence). [S.L.]: Ieee, 2014. p. 309-314.

HASSAN, NihadA..**RansomwareRevealed: a beginnersguidetoprotectingandrecoveringfromransomwareattacks**. New York: Apress, 2019. 229 p.

HASSELL, Jonathan. **Whatis IP spoofing?**And 5 waystoprevent it. 2003. Disponívelem: https://www.csoonline.com/article/2115848/data-protection-ip-spoofing.html. Acessoem: 18 out. 2021.

HOřEJŁÍ, Jaromír. **United States Cyber Security RansomwareScam**. 2012. Disponível em: https://blog.avast.com/2012/09/05/united-states-cyber-security-ransomware-scam/. Acessoem: 22 out. 2021.

HU, Hang; WANG, Gang. **RevisitingEmailSpoofingAttacks**. ComputingResearchRepository. Estados Unidos, p. 1-16. 21 ago. 2018.

IAN SHERR. Cnet. **WannaCryransomware: Everythingyouneedtoknow**. 2017. Disponívelem: https://www.cnet.com/tech/services-and-software/wannacry-wannacrypt-uiwix-ransomware-everything-you-need-to-know/. Acesso em: 04 out. 2021.

IETF. **Simple Mail TransferProtocol**. Disponível em: https://datatracker.ietf.org/doc/html/rfc821. Acesso em: 19 ago. 2019.

IT.EAM. **Como proteger sua empresa de ataques de phishing?** 2021. Disponível em: https://it-eam.com/ataques-de-phishing/. Acessoem: 12 out. 2021.

ITU, TelecommunicationStandardization Sector Of. **IntroductionTo CCITTSignaling System N0o. 7.**Helsinki: Itu-T, 1994.

IYER, R. Padmavathi; ATREY, Pradeep K.; VARSHNEY, Gaurav; MISRA, Manoj. **EmailSpoofingDetectionUsingVolatileMemoryForensics**. In: 2017 IEEE CONFERENCE ON COMMUNICATIONS AND NETWORK SECURITY (CNS), 1., 2017, Las Vegas. 2017 IEEE Conferenceon Communications and Network Security (CNS). [S.L.]: Ieee, 2017. p. 619-625.

JONATHAN BERR. Cbs News (org.). **"WannaCry" ransomwareattacklossescouldreach $4 billion. 2017**. Disponívelem: https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/. Acessoem: 04 out. 2021.

KASPERSKY. **Scammers target jobseekerswithsophisticatedmoney-stealingscheme**. 2019. Disponívelem: https://www.kaspersky.com/about/press-releases/2019_scammers-target-job-seekers-with-sophisticated-money-stealing-scheme. Acesso em: 30 out. 2019.

KASPERSKY. **O que é um ataque spearphishing?** 2017. Disponível em: https://www.kaspersky.com.br/blog/what-is-spearphishing/9933/. Acesso em: 07 mar. 2020.

KASPERSKY. Whatis IP spoofing? Disponível em: https://www.kaspersky.com/resource-center/threats/ip-spoofing. Acessoem: 18 out. 2021.

KING, Lisa Hope. **Top 5 social media scamstoavoid**: **scammershavebeenwormingtheirwayintogiant social media networks to trick**

peopleintogiving over theirpersonaland financial information.2016. Disponível em: https://money.cnn.com/2016/04/22/technology/facebook-twitter-phishing-scams/. AcessoEm: 02 out. 2021.

KNOWBE4 (Estados Unidos). **PhishingbyIndustry 2020: benchmarking report**. Clearwater: Knowbe4, 2020. 23 p.

KONG, L.A..**RansomwareAttackandRemedial: A Survey.**InternationalJournalOfInnovativeResearch In Applied SciencesAndEngineering. Tamil Nadu, p. 490-497. jan. 2020.

LAWLER, Richard. **FedEx estimatesransomwareattackcost $300 million**. 2017. Disponívelem: https://www.engadget.com/2017-09-21-fedex-ransomware-notpetya.html. AcessoEm: 25 out. 2017.

LISKA, Allan; GALLO, Timothy. **Ransomware: defendingagainst digital extortion**. Sebastopol: O'reilly Media, 2017. 174 p.

MACIEL, Cristiano; VITERBO, José. **Computação e Sociedade**. Cuiabá: Ufmt, 2020. 269 p.

MASTER JURIS. **Principais crimes contra o patrimônio**. 2019. Disponível em: https://masterjuris.com.br/principais-crimes-contra-o-patrimonio/. Acesso em: 26 set. 2021.

MITNICK, Kevin D.; SIMON, William L..**A Arte de Enganar**. São Paulo: Pearson Education, 2003. 286 p.

MOHANTA, Abhijit; HAHAD, Mounir; VELMURUGAN, Kumaraguru. **PreventingRansomware: understand, prevent, andremediateransomwareattacks.** Birmingham: Packt, 2018.

MOHURLE, Savita; PATIL, Manisha**. A briefstudyofWannacryThreat: RansomwareAttack** 2017. InternationalJournalOfAdvancedResearch In Computer Science. Udaipur, p. 1938-1940. maio 2017.

MOYER, Edward. **Stolen NSA hacking tool nowvictimizing US cities, reportsays**. 2019. Disponível em: https://www.cnet.com/tech/services-and-software/stolen-nsa-hacking-tool-now-victimizing-us-cities-report-says/. Acessoem: 25 out. 2021.

MUSTAFA, Hossen; XU, Wenyuan; SADEGHI, Ahmad-Reza; SCHULZ, Steffen. YouCanCallButYouCan'tHide: **DetectingCaller ID SpoofingAttacks**. In: INTERNATIONAL CONFERENCE ON DEPENDABLE SYSTEMS AND NETWORKS, 44., 2014, Atlanta. 2014 44th Annual IEEE/IFIP InternationalConferenceonDependable Systems and Networks. Atlanta: Ieee, 2014. p. 1-12.

O'HAGAN, Louise. **AnglerPhishing: CriminalityonSocial Media**. In: EUROPEAN CONFERENCE ON SOCIAL MEDIA, 5., 2018, Limerick. Proceedingsofthe 5th EuropeanConferenceonSocial Media. Limerick: Acpi, 2018. p. 190-197

PANORAMA MOBILE TIME/OPINION BOX. São Paulo: Mobile Time, 2021. Disponível em: https://www.mobiletime.com.br/pesquisas/mensageria-no-brasil-agosto-de-2021/. Acesso em: 25 set. 2021.

PHISHING.ORG. **HistoryofPhishing**. 2019. Disponível em: https://www.phishing.org/history-of-phishing. Acesso em: 22 out. 2019.

PRESIDÊNCIA DA REPÚBLICA**. Lei Nº 12.737, de 30 de novembro de 2012**., 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 4, de setembro de 2019.

PSAFE. **Mais de 5 milhões de brasileiros foram vítimas do golpe de Clonagem de WhatsApp em 2020**.: especialistas alertam que as redes sociais têm sido os principais meios utilizados por cibercriminosos para atrair vítimas do golpe. 2021. Disponível em: https://www.psafe.com/blog/mais-de-5-milhoes-de-brasileiros-foram-vitimas-do-golpe-de-clonagem-de-whatsapp-em-2020/. Acessoem: 25 set. 2021.

THE TIMES OF INDIA (India). **PaintgiantlosesRs 28 lakh in case ofemailspoofing**. 2019. Disponível em: https://timeshttps://timesofindia.indiatimes.com/city/mumbai/paint-giant-loses-rs-28-lakh-in-case-of-email-spoofing/articleshow/67580796.cmsofindia.indiatimes.com/city/mumbai/paint-giant-loses-rs-28-lakh-in-case-of-email-spoofing/articleshow/67580796.cms. Acesso em: 14 out. 2021.

RAHMAN, Leila Fatmasari; ZHOU, Rui. **IpAddressSpoofing**. - Institute For Computer Science, Albert-Ludwigs-Universität Freiburg, Freiburg.

RAINS, Tim. **CybersecurityThreats, Malware Trends, andStrategies: mitigateexploits, malware, phishingandother social engineeringattacks.** Birmingham: PacktPublishing Ltd, 2020. 429 p.

RASHID, Sharmin; PAU, SubhraProsun. **ProposedMethodsof IP SpoofingDetection&Prevention.**InternationalJournalOf Science AndResearch. India, p. 438-444. jun. 2013.

RICHARDSON, Ronny; NORTH, Max M.. Ransomware: Evolution, MitigationandPrevention. International Management Review. Kennesaw, p. 10-21. jan. 2017. Disponívelem: https://digitalcommons.kennesaw.edu/facpubs/4276/. Acessoem: 25 out. 2021.

RISKIQ (comp.). **The Evil Internet Minute 2019**: every minute, $2,900,000 islosttocybercrime. Every Minute, $2,900,000 isLosttoCybercrime. 2019. Disponível em: https://www.riskiq.com/resources/infographic/evil-internet-minute-2019/. Acesso em: 22 set. 2021.

ROSENBERG, Joyce M..**Computer users face hard choice: Payransomorloseaccessto files**. 2015. Disponível em: https://www.spokesman.com/stories/2015/apr/12/computer-users-face-hard-choice-pay-ransom-or/. Acessoem: 26 out. 2021.

SALVI, Harshada U.; KERKAR, Ravindra V..**Ransomware: A Cyber Extortion**. AsianJournalOfConvergence In Technology. India, p. 1-6. out. 2014.

SOPHOS LTD (ReinoUnido). Phishing Insights 2021: a Sophoswhitepaper. Oxford: Sophos, 2021. 10 p.

STALLINGS, William. Criptografia e segurança de redes. São Paulo: Pearson, 2006.

STATISTA (Alemanha). **RegisteredusersofFortniteworldwidefrom August 2017 to May 2020**. 2020. Disponívelem: https://www.statista.com/statistics/746230/fortnite-players/. Acesso em: 17 set. 2021.

STATISTA. Global digital population as ofJanuary 2021. 2021. Disponível em: https://www.statista.com/statistics/617136/digital-population-worldwide/. Acessoem: 02 out. 2021.

UOL. Spoofing: entenda a técnica hacker usada para invadir o celular de Moro. 2019. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2019/07/24/spoofing-entenda-a-tecnica-hacker-usada-para-invadir-o-celular-de-moro.htm. Acesso em: 6 set. 2019.

UPGUARD TEAM (Austrália). **COBIT vs ITIL vs TOGAF: WhichIsBetter For Cybersecurity?**2021. Disponível em: https://www.upguard.com/blog/cobit-vs-itil-vs-itsm-which-is-better-for-cybersecurity-and-digital-resilience#toc-0. Acessoem: 03 out. 2021.

YOUNG, Cian. **ForensicInvestigationofRansomwareActivities**. Cyber And Digital ForensicInvestigations. New York City, p. 51-77. 2020