ATAQUES CIBERNÉTICOS: COVID-19 E OS RISCOS DO HOME OFFICE

CYBER ATTACKS: COVID-19 AND THE RISKS OF HOME OFFICE

Nathan Tomaz de Oliveira; Cássio Gonçalves Sena
nathan.tomaz01@gmail.com; cassiosena@gmail.com
Faculdade Presidente Antônio Carlos de Teófilo Otoni.

Resumo

As constantes evoluções tecnológicas dos sistemas de informação trouxeram grandes benefícios para a sociedade moderna, contudo, se tornou uma sociedade totalmente dependente e vulnerável. Assim, atores tanto estatais como não-estatais se aproveitaram dessas vulnerabilidades para realização de diversos crimes, genericamente conhecidos como ameaças cibernéticas ou ataques cibernéticos. Tudo se tornou mais grave com a pandemia de coronavírus, a dependência tecnológica aumentou repentinamente e não houve tempo de qualquer preparo das redes em relação a segurança da informação, nem qualquer ensino dos perigos e precauções que devem ser tomadas ao se trabalhar remotamente, levando a exploração criminosa dessa falta de informação dos usuários. Então, este trabalho de conclusão de curso busca através de uma revisão bibliográfica, analisar os impactos dos ataques cibernéticos em período de COVID-19 com o crescimento do trabalho home office assim como as principais técnicas utilizadas nesses ataques.

Palavras-chave: Ataque cibernético; ameaça cibernética; covid-19; coronavírus; home office;

Abstract

The constant technological evolutions of information systems have brought great benefits to modern society, however, it has become a totally dependent and vulnerable society. Thus, both state and non-state actors took advantage of these vulnerabilities to carry out several crimes, generically known as cyber threats or

cyber-attacks. Everything became more serious with the coronavirus pandemic, the technological dependence suddenly increased and there was no time for any preparation of the networks in relation to information security, nor any teaching of the dangers and precautions that must be taken when working remotely, leading to criminal exploitation of this lack of user information. So, this undergraduate final work seeks, through a bibliographic review, to analyze the impacts of cyber-attacks in the period of COVID-19 with the growth of home office work as well as the main techniques used in these attacks.

Keywords: Cyber-attack; cyber threat; covid-19; coronavirus; home office;

1. INTRODUÇÃO

Durante a revolução informacional da década de 90 que tecnologias e métodos novos para se comunicar surgiram, tornando a TI elemento central da sociedade moderna, mas ao mesmo tempo abriu-se todo um novo universo de vulnerabilidades a serem exploradas (MENDONÇA, 2014).

No entanto, as ameaças cibernéticas não são um fenômeno novo. Vírus e worms fazem parte do ruído de fundo do ciberespaço desde seus primeiros dias, sendo o uso das tecnologias de informação e comunicação (TIC) como ferramenta de ataque por uma ampla gama de atores malévolos, uma das grandes ameaças nos tempos modernos (CAVELTY, 2007).

Pouco mais de meio século depois do projeto da ARPANET, a sociedade está totalmente dependente da internet, comunicando-se com facilidade e rapidez como nunca antes, mas isso veio junto com uma série de vulnerabilidades até então desconhecidas (DE ALMEIDA ROSSATO, 2019). Tais vulnerabilidades seriam exploradas por pessoas mal intencionadas, que estão sempre buscando tirar alguma vantagem do aparente ambiente “anárquico” presente na web (MENDONÇA, 2014).

Nesse contexto, a COVID-19 veio para agravar essa situação pois, através de medidas drásticas como o distanciamento social, minando o desenvolvimento econômico e a existência diária, há uma crescente dependência da Internet (MOHSIN, 2020). Essa dependência cria vulnerabilidade no ciberespaço e é uma grande oportunidade para exploração não só das vulnerabilidades dos sistemas, mas também

do fator humano, que representa um dos maiores problemas dos sistemas de informação (MOHSIN, 2020; MENDONÇA, 2014).

Como uma forma de minimizar o impacto econômico e obedecer às medidas de distanciamento social, muitas empresas aderiram ao home office, que mesmo auxiliando-as a aumentar a produtividade e diminuir os custos trouxe consigo vários problemas relacionados à segurança da informação, levando a um aumento generalizado dos ataques cibernéticos (CARREIRAS et al., 2020).

Nosso objetivo é fazer uma revisão bibliográfica sobre os impactos dos ataques cibernéticos em tempos de COVID-19 com o crescimento do trabalho home office e determinar quais as técnicas mais utilizadas.

Os objetivos específicos são: entender os impactos dos ataques cibernéticos durante a pandemia do coronavírus; descobrir os tipos de ataque mais utilizados; identificar a influência do home office nesse contexto;

Para atingir tais objetivos, foi realizada uma revisão bibliográfica a partir de artigos acadêmicos, livros e relatórios de especialistas em segurança cibernética.

2. REVISÃO DA LITERATURA

2.1 História das Ameaças Cibernéticas

Após a criação da ARPANET, em 1980 começa a surgir o que conhecemos hoje como ameaças cibernéticas, essa demora pode ser atribuída à subestrutura tecnológica, que ainda não havia se popularizado o bastante para se tornar um fenômeno de massa, que só viria a acontecer quando as redes de computadores se tornassem um dos elementos fundamentais da sociedade moderna (ELLISON et al., 1997; CAVELTY, 2007).

Com a popularização dos computadores pessoais um fenômeno que era bastante restrito se expandia para o mundo. Devido ao desenvolvimento de uma infraestrutura de informação global e o avanço da tecnologia no setor civil, os 'hackers' como o famoso Kevin Mitnick que utilizava técnicas de engenharia social chamadas de “phreaking” (o hackeamento de linhas telefônicas) para obter informações confidenciais de amigos e professores (ULBRICH, 2004), agora com um computador, de sua casa era possível explorar vulnerabilidades em redes emergentes. Tais transformações afetariam a concepção da natureza dos conflitos e das estruturas,

doutrinas e estratégias militares, sendo considerado que: o cerne do problema de segurança na década de 1980 foi a disseminação das tecnologias da informação em muitos aspectos da vida e a dependência dessas tecnologias (CAVELTY, 2007).

Logo no seu início a ARPANET já teria suas vulnerabilidades exploradas, quando Robert Morris, um aluno da Universidade Cornell, fez uma ferramenta de ataque que se chamaria “MorrisWorm”, ela se infiltrava na rede e consumia todos os recursos dos computadores afetados, paralisando 10% dos computadores americanos conectados à ARPANET (CALVETY, 2007). O General Accounting Office (GAO) avaliou o dano financeiro entre US $ 10 e US $ 100 milhões (NEED, 1994).

Segundo Stoll (1989), outro incidente foi apelidado de Cuckoo's Egg, um hacker alemão que tentou realizar uma invasão às redes de computadores norte-americanas a serviço dos soviéticos, evidenciando que espiões estrangeiros poderiam se aproveitar de vulnerabilidades para conseguir informações altamente classificadas, preocupando autoridades sobre os riscos à segurança nacional (apud CALVETY, 2007), ao passo que, segundo Ronald Reagan (Presidente dos Estados Unidos 81-89):

> A tecnologia para explorar esses sistemas eletrônicos é difundida e amplamente utilizada por nações estrangeiras, podendo ser empregada também por grupos terroristas e elementos criminosos. Os sistemas governamentais, bem como aqueles que processam as informações privadas ou proprietárias de pessoas e empresas americanas, podem se tornar alvos de exploração estrangeira. (REAGAN, 1984, p.1, tradução nossa).

2.2 Ataques Cibernéticos

“Ataque cibernético é uma ação realizada por um indivíduo ou grupo individual com o intuito de provocar danos (físicos, financeiros ou morais), destruição ou vítimas sem que tenham o objetivo de obter uma vantagem estratégica” (MENDONÇA, 2014, p. 22). Esse conceito não pode ser confundido com o de guerra cibernética, pois pode ser praticado de forma independente por cibercriminosos e não depende de atores estatais (AGOSTINI, 2014).

3. AMEAÇAS CIBERNÉTICAS NA PANDEMIA DE COVID-19

A pandemia Covid-19 começou em 2019 e logo se tornou uma crise global que impôs várias restrições aos países afetados e expôs as fraquezas das sociedades modernas em enfrentar situações de crise ou emergência. “Esta situação sanitária atípica, veio também provar a elevada dependência das sociedades modernas relativamente às tecnologias da informação, à internet e ao ciberespaço” (CARREIRAS et al., 2020, p. 7). Tal dependência tecnológica evidenciou que as ameaças cibernéticas são significativamente perigosas e que ataques cibernéticos se tornaram comuns e são muitas vezes direcionados para situações especificas de crise como essa (LALLIE et al., 2020).

Atualmente as ameaças vem se tornando cada vez mais sofisticadas, segundo o relatório anual da Microsoft (Digital Defense Report) sobre segurança cibernética, várias são as técnicas usadas para explorar sistemas vulneráveis, sendo IoT um dos grandes focos nos últimos anos. E durante a pandemia de COVID-19, o número de malware se manteve constante, porém os cibercriminosos adaptaram o tipo de ataque, se aproveitando da situação e criando iscas de phishing, uma técnica de engenharia social para obtenção de informações e roubo de credenciais (MICROSOFT, 2020).

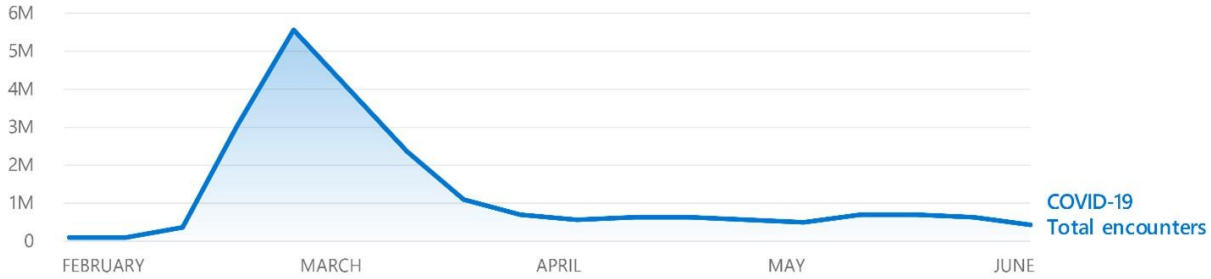

Figura 1: Ataques com o tema COVID-19 - Estados Unidos. Fonte: BURT (2020).

“Os autores destas campanhas de phishing aproveitaram o confinamento para simular serviços digitais com maior consumo e fidelização, como os serviços de homebanking, conteúdos digitais em streaming e lojas online” (CARREIRAS et al., 2020, p. 4).

3.1 Pishing

Phishing é uma das técnicas de engenharia social mais utilizadas para roubo de informações, significando “pescaria” (fishing) de vítimas ou “e-mail falso”, que através de e-mails manipulados, sites clonados, mensagens em redes sociais ou SMS (Short Message Service, que em português significa Serviço de Mensagens Curtas), leva o usuário a recebe-los como se fossem autênticos e a realizar as ações definidas pelos cibercriminosos (PIOVESAN et al., 2019; RAFAEL, 2013). Tem por objetivo, por link ou anexo te direcionar para um site, abrir um arquivo malicioso pré-definido pelo atacante ou instalar um vírus de computador para obter informações valiosas (MENDONÇA, 2014; CABRAL, 2020).

Os ataques cibernéticos só aumentaram com a pandemia, o tema COVID-19 está sendo usado por criminosos para criação de sites falsos, espalhar malwares e aplicar golpes (MOHSIN, 2020).

Ainda que o COVID-19 tenha se tornado uma crise na China em dezembro, phishing e outros golpes associados ao vírus só começaram em janeiro. E em março já existe um tráfego de spam considerável e em crescimento sobre o Coronavírus (GALLAGHER e BRANDT, 2020), como é mostrado na Figura 2.

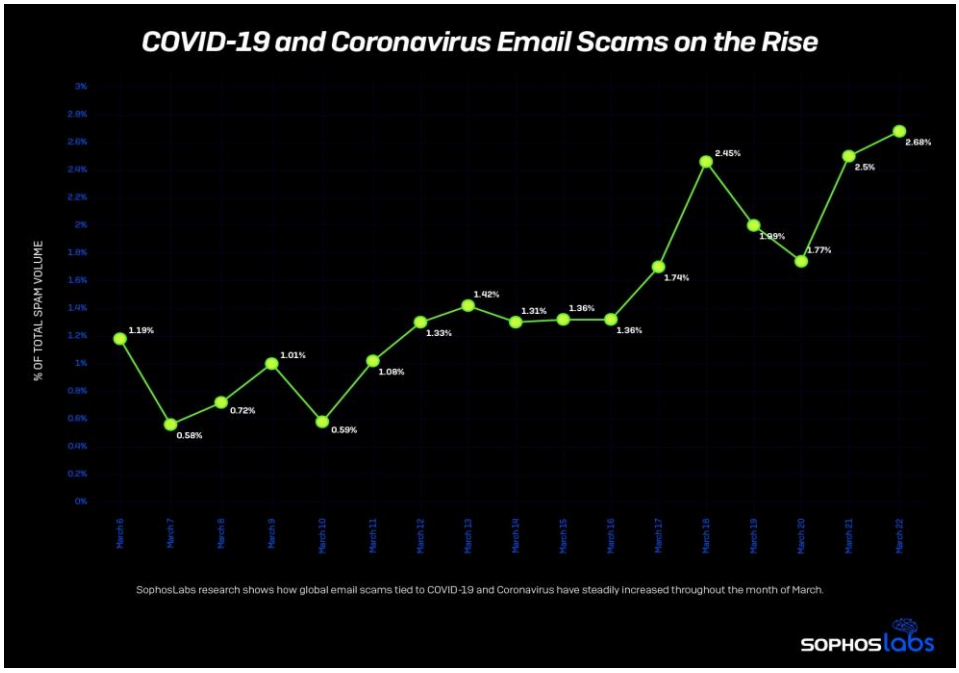

Figura 2: Golpes por e-mail em ascensão. Fonte: GALLAGHER e BRANDT (2020).

Os pesquisadores da Barracuda também têm visto um aumento constante no número de ataques de phishing relacionados ao coronavírus COVID-19 desde janeiro, mas observaram um aumento recente neste tipo de ataque, um aumento de 667% desde o final de fevereiro (SHI, 2020a).

Entre 1º de março e 23 de março, o Barracuda Sentinel detectou 467.825 ataques de e-mail de phishing, e 9.116 dessas detecções estavam relacionadas ao COVID-19, representando cerca de 2% dos ataques. Em comparação, um total de 1.188 ataques de phishing relacionados ao coronavírus foram detectados em fevereiro, e apenas 137 foram detectados em janeiro. Embora o número total desses ataques ainda seja baixo em comparação com outras ameaças, a ameaça está crescendo rapidamente (SHI, 2020a).

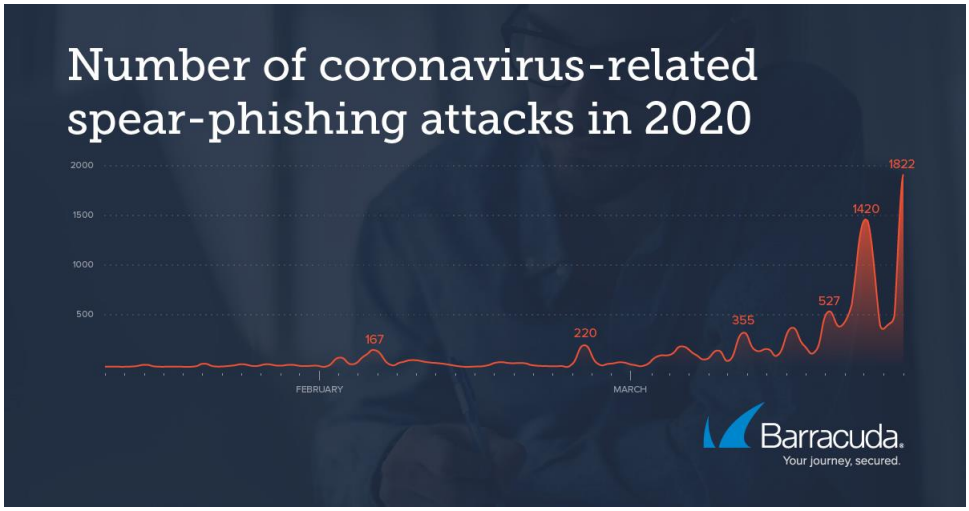

Figura 3: Ataques phishing relacionados ao coronavírus. Fonte: SHI (2020a).

Ao passo que, a Sophos, empresa desenvolvedora de softwares para cibersegurança, descobriu uma série de e-mails de phishing que se passavam por organizações de saúde com informações sobre o coronavírus para conseguir informações sigilosas dos usuários (PULIDO, 2020).

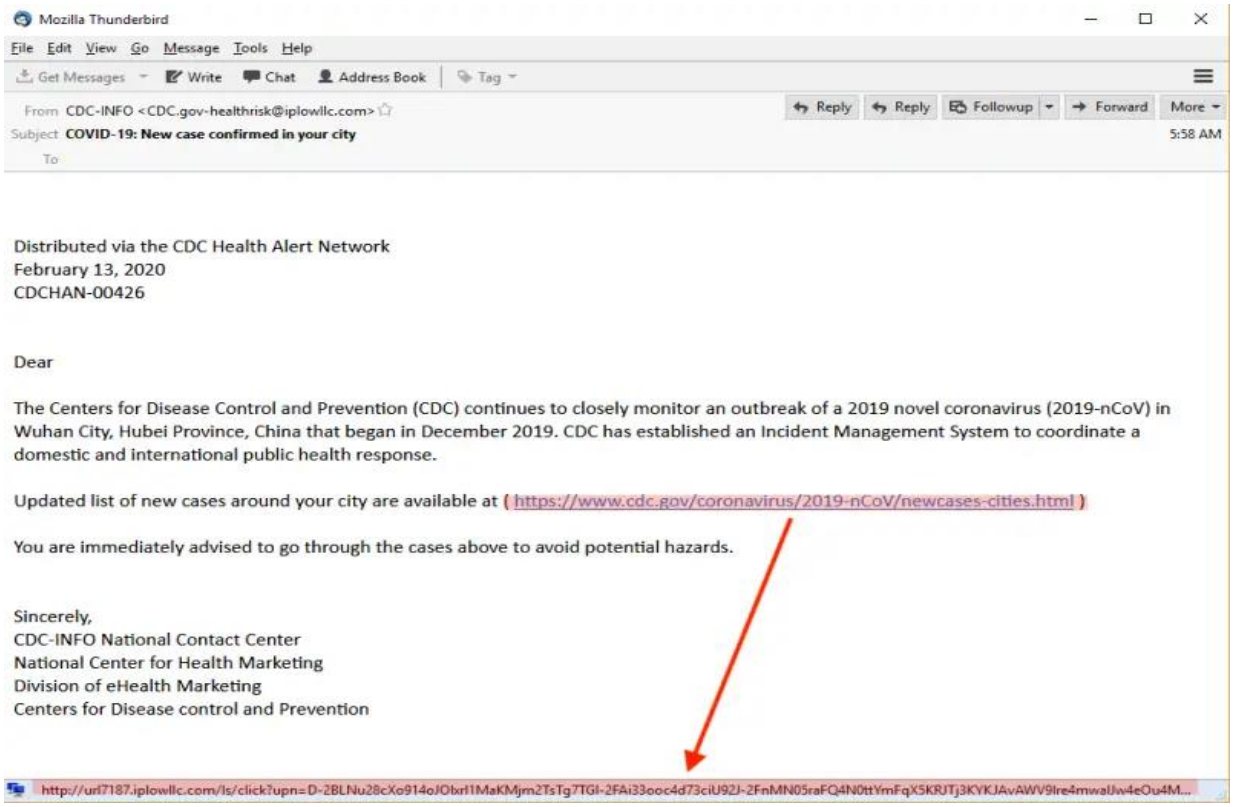

Figura 4: Link malicioso. Fonte: PACAG (2020).

> Na suposta mensagem enviada pelo CDC, indica que foi criado um sistema para controlar e coordenar as ações relacionadas ao tema Saúde Coletiva e Coronavírus dentro e fora do país, e incita os destinatários a entrarem em uma página adicional que fornecerá informações atualizadas sobre novos casos de infecção em sua cidade. Ao clicar no link o usuário é redirecionado para um site com interface idêntica ao Microsoft Outlook, embora o site não seja relacionado a esta empresa. Ele solicita intencionalmente credenciais de login e uma senha para que os criminosos possam roubar credenciais de um e-mail, enviando-lhes o nome de usuário e a senha para acessar posteriormente a conta de e-mail original do usuário e buscar informações úteis para cometer seus crimes (GUTIÉRREZ GARCÍA; BARRANTES CENTURION; SÁNCHEZ SILVA, 2020, p. 19, tradução nossa).

A Figura 5 é um exemplo de site falso para roubo de credenciais, interface semelhante ao site original, porém ao analisar o código fonte, é possível ver que suas credenciais serão enviadas para outra página hospedada no mesmo site, ‘send03.php’ (PACAG, 2020).

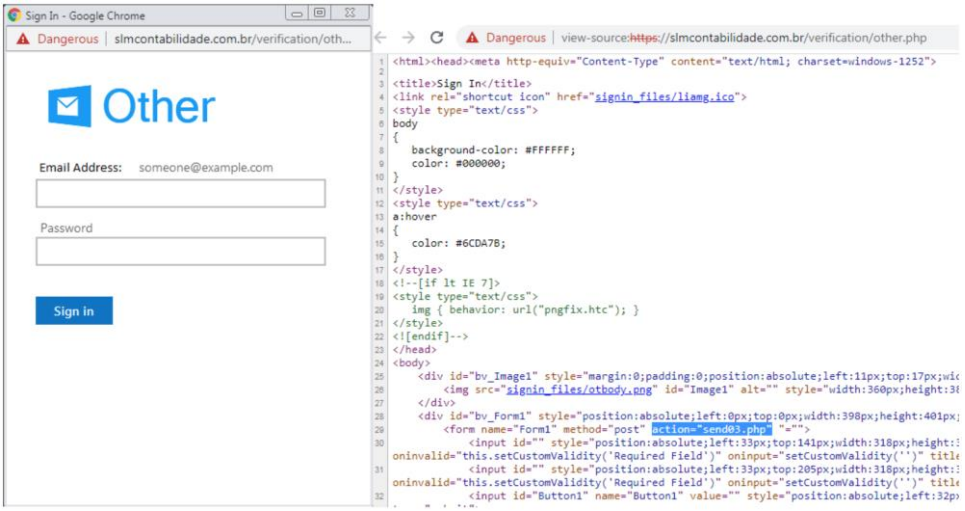

Figura 5: Site Falso. Fonte: PACAG (2020).

"É importante lembrar que ler atentamente o e-mail é a forma mais fácil de detectar sua falsidade. É possível notar que o site do link contido no e-mail é HTTP e não HTTPS, o que indica que o site não possui certificado de segurança" (GUTIÉRREZ GARCÍA; BARRANTES CENTURION; SÁNCHEZ SILVA, 2020, p. 20, tradução nossa).

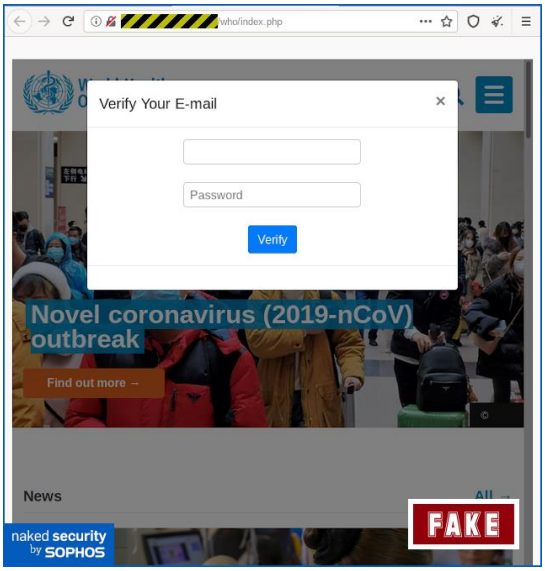

Figura 6: Site fake da OMS. Fonte: DUCKLIN (2020).

A Figura 6 mostra uma página visualmente idêntica à da Organização Mundial da Saúde (OMS), pois de fato é a página da OMS em segundo plano, ela é renderizada em um quadro do site. Porém diferente do original ele abre um formulário pop-up, que ao ser preenchido envia suas informações como e-mail e senha do

usuário para o criminoso e redireciona para a página inicial da OMS, como se fosse a página anterior sem o pop-up (DUCKLIN, 2020).

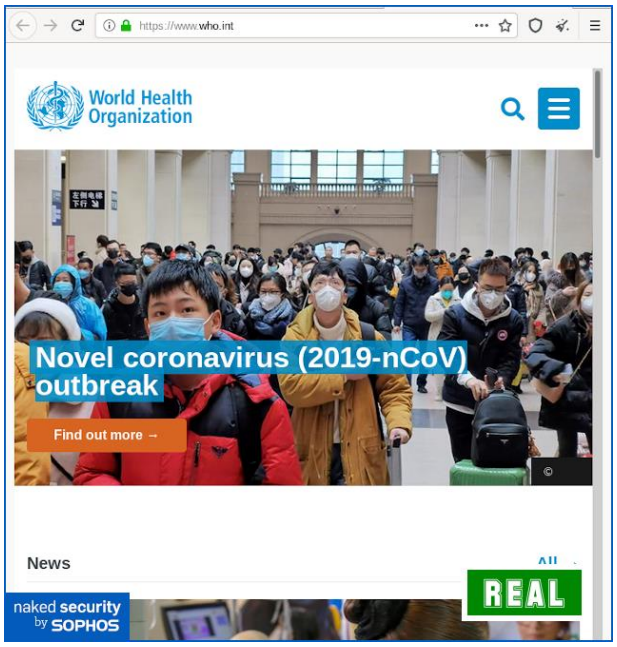

Figura 7: Site real da OMS. Fonte: DUCKLIN (2020).

No Brasil, já com rumores de um auxilio emergencial do governo federal, mensagens falsas diziam que o governo estava emitindo voucher de R$200,00 para trabalhadores autônomos e pessoas de baixa renda, com intuito de fazer a vítima entrar em um site que coletaria suas informações (CABRAL, 2020; REIS, 2020).

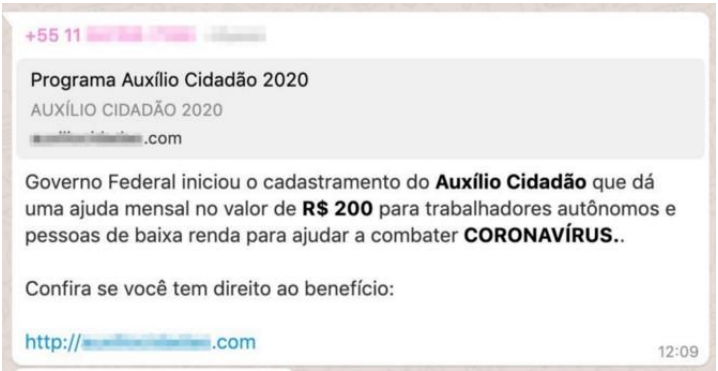

Figura 8: Mensagem falsa. Fonte: CABRAL (2020).

3.2 Ransomware

> Ransomware é um malware que impede o acesso do usuário vítima a um recurso valioso e extorque um pagamento de resgate para restabelecer o acesso. O ransomware vem em muitas formas e formatos. Isso inclui, por exemplo, bloqueios de tela maliciosos em dispositivos móveis ou ransomware baseado em criptografia que

> criptografa o arquivo da vítima com algoritmos criptográficos de última geração (KOLODENKER et al., 2017, p. 599, tradução nossa).

Esse tipo de malware já existe a mais de duas décadas, mas vem crescendo muito nos últimos anos (SHI, 2020b), o WannaCry de 2017 já havia feito instituições hospitalares de alvo, como o serviço nacional de saúde britânico, pois essas instituições em geral têm seus softwares mais desatualizados que o comum e muitas pessoas tem acesso a computadores e servidores sem um controle adequado, havendo pouca ou nenhuma política de segurança (CARREIRAS et al., 2020).

Os ataques envolvendo ransomware contra organizações de saúde, governamentais e de educação também aumentaram, se aproveitando da pandemia e do trabalho remoto para amplificar seus danos nessas organizações (SHI, 2020b).

Uma pesquisa feita pela Barracuda identificou que desde 2019 o foco dos ataques tem sido governos municipais, como escolas, bibliotecas, tribunais entre outros, porém esse ano houve um redirecionamento desses ataques para organizações de saúde e logística, setores fundamentais durante uma pandemia. A figura 9 mostra uma análise da preferência do tipo de organização que os ataques ransomware tiveram em 2019 comparando com 2020 (SHI, 2020b).

Figura 9: Ataques ransomware por tipo de organização. Fonte: SHI (2020b).

A equipe de pesquisa de segurança do DomainTools descobriu que vários dominios relacionado ao Coronavirus e o COVID-19 que estavam sendo usados para prática de golpes, um deles é o (coronavirusapp[.]site) (SALEH e ANDERSON, 2020). Nele a vítima é induzida a baixar um aplicativo chamado COVID-19 Tracker para que consiga ver o número de casos perto de onde ela mora ou trabalha, porém, se trata

de um ransomware que ao ser instalado exibe uma mensagem que o celular foi hackeado e solicita um pagamento para que o usuário volte a utilizar o celular normalmente (CABRAL, 2020; CARREIRAS et al., 2020).

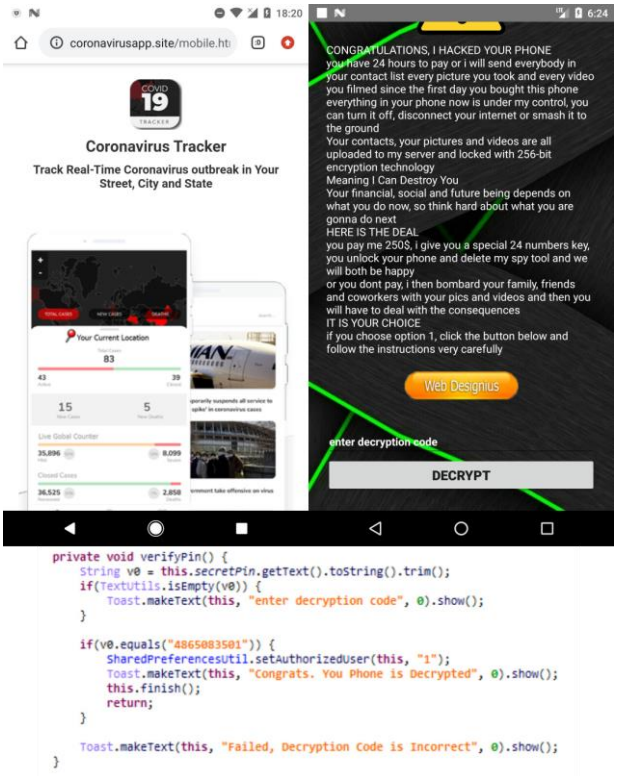

Figura 10: Ransomware em APP de monitoramento do coronavírus. Fonte: SALEH e ANDERSON (2020).

Uma análise do código fonte do Ransomware mostrou que não era um malware desenvolvido de forma muito sofisticada, é visível que utiliza a linguagem de programação Java e a função ‘verifyPin()’ foi programada para desbloquear simplesmente utilizando o código "4865083501" como mostrado na figura 10, porém ainda sim é um malware bastante eficiente (SALEH e ANDERSON, 2020).

4. HOME OFFICE

Há várias terminologias para designar o home office: trabalho à distância, trabalho em casa, trabalho virtual, escritório virtual ou teletrabalho (GASPAR et al., 2011; HAUBRICH e FROEHLICH, 2020). Ao passo que, “Teletrabalho” tem origem no termo *telecommuting,* criado por Jack Nilles nos anos 70, que define o objetivo dessa nova modalidade de trabalho como: “levar o trabalho aos trabalhadores, em vez de

levar estes ao trabalho; atividade periódica fora do escritório central, um ou mais dias por semana, seja em casa ou em um centro de telesserviço" (NILLES, 1997, p. 14 apud SAKUDA, 2001, p. 37).

Porém há estudos apontando seu surgimento na França de 1791, pois é com a criação do telegrafo ótico para comunicação a longas distâncias que se tem um prelúdio do que viria a ser o home office. Originalmente criado para fins militares, esses primeiros telégrafos já demonstravam que era possível uma relação de trabalho a distância tendo uma tecnologia como mediadora, porém foram abandonados com a chegada dos telégrafos elétricos antes da popularização do seu uso em empresas (FINCATO, 2016; HISTEL, 2006).

Portanto, essa nova modalidade de trabalho só iria se popularizar com o surgimento das tecnologias de informação e comunicação (TICs), liberando os trabalhadores de locais físicos, permitindo que as mesmas tarefas fossem realizadas remotamente (LEUNG e ZHANG, 2017).

Mesmo não havendo um consenso, "uma certeza há: o surgimento do teletrabalho está intimamente relacionado à evolução das tecnologias de comunicação e à possibilidade de, via mensagens que por estas trafegavam, enviar o trabalho ao trabalhador" (FINCATO, 2016, p. 372).

De acordo com a CIO (2016), 80% das empresas que adotaram o home office são do setor de serviços e da indústria de transformação, são: tecnologia da informação e telecomunicações (24%); químico, petroquímico e agroquímico (12%); serviços de suporte e provimento (9%); bens de consumo (8%); e máquinas/equipamentos e automação (8%), com a maioria, 67% sendo empresas multinacionais.

4.1 Home office durante e pandemia

O Covid-19 acelerou uma tendência do trabalho home office já crescente a alguns anos (MICROSOFT, 2020), alterando o ambiente de trabalho, onde a presença física era o *modus operandi*, e agora é o ciberespaço (CARREIRAS et al., 2020).

Atualmente o trabalho remoto se tornou um assunto muito discutido, pois sua adoção está sendo essencial para a continuidade do funcionamento das empresas durante o Covid-19, um estudo feito pelo Gartner Group aponta que antes da

pandemia 30% dos trabalhadores iriam realizar suas funções remotamente pelo menos algumas vezes, após o início da pandemia esse número aumentou para 48% (CARVALHO, 2020).

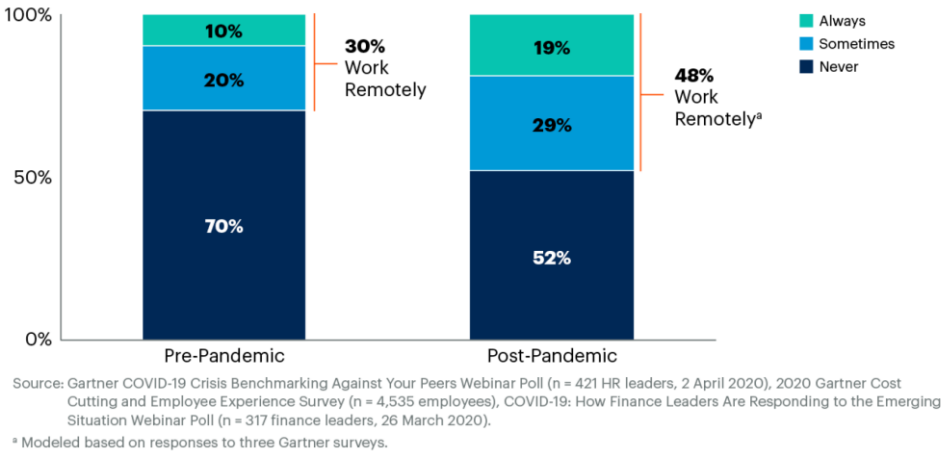

Figura 11: Trabalho Remoto antes e pós pandemia. Fonte: CARVALHO (2020).

Segundo uma pesquisa feita pela Fundação Instituto de Administração (FIA), 46% das empresas brasileiras adotaram o trabalho em casa durante a pandemia. A adoção foi maior nos setores hospitalares (53%) e na indústria (47%) (MELLO, 2020).

Com milhões de pessoas passando a usar as redes e servidores das suas empresas e organizações a partir de casa e através de redes com níveis de segurança inferiores, não é surpreendente que tenha havido um aumento generalizado de ataques cibernéticos, com o FBI relatando um crescimento de 300% no número de incidentes referentes a ataques cibernéticos. A mesma situação é verificada em todo o mundo (CARREIRAS et al., 2020).

Pesquisas sobre cibersegurança encontraram vários malwares referentes ao coronavírus, como cavalos de tróia e ransomware. Devido ao grande número de pessoas dependente de meios de comunicação online para trabalhar, os malwares podem se espalhar rapidamente entre os sistemas internos das empresas através de VPNs (redes virtuais privadas) (BANACH, 2020).

5. CONSIDERAÇÕES FINAIS:

No decorrer das leituras e pesquisas, percebemos que com a sociedade cada vez mais dependente da tecnologia, desde compras e interações sociais até negócios, indústria, tudo está online, inclusive o crime (LALLIE et al., 2020), por isso do grande

aumento de ataques cibernéticos nos últimos anos, o que levou muitos países a investirem em defesa cibernética, mesmo assim, como mostramos no estudo, o ciberespaço ainda é profundamente vulnerável e as ameaças cibernéticas vem se tornando cada vez mais sofisticadas (MICROSOFT, 2020).

Com a pandemia COVID-19 os problemas relacionados a cibersegurança se agravaram exponencialmente, mesmo que não se tenha detectado nenhum ataque de grandes proporções, houve um volume crescente de ataques cibernéticos registrados nesse período, evidenciando a necessidade de defesas e estratégias para alguns tipos de ataques mais sofisticados, como phishing e o ransomware. Apesar de não terem sido assinalados ataques de grande capacidade disruptiva e/ou destrutiva (CARREIRAS et al., 2020), a pandemia serviu como um grande impulsionador desses ataques (LALLIE et al., 2020).

Ficou evidente que a tecnologia poderia amenizar algumas consequências negativas da quarentena, o trabalho remoto se tornou uma solução para as empresas, mesmo que temporária para não ter suas operações todas interrompidas. Porém, o aumento de ataques durante a pandemia deixou claro que tanto os sistemas como as pessoas não estavam preparadas para esse tipo de mudança tão rapidamente, a camada social se tornou o vetor mais vulnerável devido as técnicas de engenharia social, que mesmo que antigas, foram adaptadas ao cenário e continuam eficientes para obter informações importantes de usuários desatentos ou pouco familiarizados com os sistemas (CARREIRAS et al., 2020).

Os estudos e relatórios analisados nessa revisão bibliográfica foram feitos durante a pandemia, de janeiro até dezembro de 2020, assim sendo todos os ataques estudados estão limitados a esse período e depende que outros estudos sejam feitos no pós pandemia para ampla compreensão dos impactos causados pelas mudanças feitas durante a pandemia, se realmente o trabalho remoto permanecerá e a infraestrutura tecnológica se adaptará a nova realidade, ou se foi apenas uma solução temporária em um momento de crise.

Referências

AGOSTINI, Marcos Tocchetto et al. **A CIBERNÉTICA SOB A ÓTICA DO FENÔMENO DA GUERRA E DA AGENDA DE SEGURANÇA**. 2014. Disponível em: < https://repositorio.ufsc.br/bitstream/handle/123456789/124695/Monografia%20do%2

0Marcos%20Tocchetto%20Agostini.pdf?sequence=1&isAllowed=y >. Acesso em: 23 de novembro de 2020.

BANACH, Zbigniew. **Cybersecurity During the COVID-19 Pandemic**. 2020. Disponível em: <https://www.netsparker.com/blog/web-security/covid-19-crisis-cyberattacks/>. Acesso em: 13 de novembro de 2020.

BURT, Tom. **Microsoft report shows increasing sophistication of cyber threats**. 2020. Disponível em: < https://blogs.microsoft.com/on-the-issues/2020/09/29/microsoft-digital-defense-report-cyber-threats/ >. Acesso em: 22 de novembro de 2020.

CABRAL, Carlos. **As estratégias por trás dos ataques com o tema do novo coronavírus**. 2020. Disponível em: < https://medium.com/sidechannel-br/as-estrat%C3%A9gias-por-tr%C3%A1s-dos-ataques-com-o-tema-do-novo-coronav%C3%ADrus-c5438c92dd3b >. Acesso em: 25 de novembro de 2020.

CARREIRAS, Helena et al. **Cibersegurança e ciberdefesa em tempos de pandemia**. IDN Brief, 2020. Disponível em: <https://www.jstor.org/stable/pdf/resrep25591.pdf>. Acesso em: 23 de novembro de 2020.

CARVALHO, Carlos Eduardo. **Análise sobre os importantes impactos do trabalho remoto para as organizações**. Bridge & Co, 2020. Disponível em: < https://bridgeconsulting.com.br/insights/analise-sobre-os-importantes-impactos-do-trabalho-remoto-para-as-organizacoes/ >. Acesso em: 30 de novembro de 2020.

CAVELTY, Myriam Dunn. **Cyber-security and threat politics: US efforts to secure the information age**. Routledge, 2007. Disponível em: <https://www.researchgate.net/publication/277714726_Cyber-Security_and_Threat_Politics_US_Efforts_to_Secure_the_Information_Age>. Acesso em: 23 de novembro de 2020.

CIO. **Home office e teletrabalho são cada vez mais comuns no Brasil**. 2016. Disponível em: < https://cio.com.br/gestao/home-office-e-teletrabalho-sao-cada-vez-mais-comuns-no-brasil/ >. Acesso em: 29 de novembro de 2020.

DE ALMEIDA ROSSATO, Isaac et al. **A Importância do Desenvolvimento Cibernético para a Defesa Nacional no Entorno Estratégico**. 2019. Disponível em: < https://www.gov.br/defesa/pt-br/arquivos/ensino_e_pesquisa/defesa_academia/cadn/artigos/xvi_cadn/aa_importa

nciaa_doa_desenvolvimentoa_ciberneticoa_paraa_aa_defesaa_nacionala_noa_entornoa_estrategico.pdf>. Acesso em: 13 de novembro de 2020.

DUCKLIN, Paul. **Coronavirus "safety measures" email is a phishing scam**, 2020. Disponível em: < https://nakedsecurity.sophos.com/2020/02/05/coronavirus-safety-measures-email-is-a-phishing-scam/>. Acesso em: 22 de novembro de 2020.

ELLISON, Robert J. et al. **Survivable network systems: An emerging discipline**. Carnegie-mellon Univ Pittsburgh PA Software Engineering Inst, 1997. Disponível em: < https://resources.sei.cmu.edu/asset_files/TechnicalReport/1998_005_001_16598.pdf >. Acesso em: 01 de dezembro de 2020.

FINCATO, Denise Pires. **A regulamentação do teletrabalho no Brasil: indicações para uma contratação minimamente segura**. Revista Jurídica Luso-brasileira, 2016. Disponível em: < https://repositorio.pucrs.br/dspace/bitstream/10923/11404/2/A_regulamentacao_do_teletrabalho_no_Brasil_indicacoes_para_uma_contratacao_minimamente_segura.pdf >. Acesso em: 27 de novembro de 2020.

GALLAGHER, Sean; BRANDT, Andrew. **Facing down the myriad threats tied to COVID-19**. Sophos News, 2020. Disponível em: < https://news.sophos.com/en-us/2020/04/14/covidmalware/ >. Acesso em: 02 de dezembro de 2020.

GASPAR, Marcos Antonio et al. **Teletrabalho no desenvolvimento de sistemas: um estudo sobre o perfil dos teletrabalhadores do conhecimento**. Revista Ciências Administrativas, v. 17, n. 3, p. 1029-1052, 2011. Disponível em: < https://periodicos.unifor.br/rca/article/view/3301/pdf >. Acesso em: 27 de novembro de 2020.

GORE JR, Albert. **National high-performance computer technology act of 1989**. 1990. Disponível em: < https://books.google.com.br/books?id=mgT75xrFGksC&dq=Computer%20Security%20Virus%20High&hl=pt-BR&pg=PA374#v=onepage&q=100&f=false >. Acesso em: 13 de novembro de 2020.

GUTIÉRREZ GARCÍA, Sonia; BARRANTES CENTURION, Jaime; SÁNCHEZ SILVA, Jenny. **Seguridad de la información: Phishing y coronavirus**. 2020. Disponível em: <https://repositorio.ins.gob.pe/xmlui/bitstream/handle/INS/1180/SEGURIDAD%20DE%20LA%20INFO.pdf>. Acesso em: 12 de novembro de 2020.

HAUBRICH, Deise Bitencourt; FROEHLICH, Cristiane. **Benefícios e desafios do home office em empresas de tecnologia da informação**. Revista Gestão & Conexões, v. 9, n. 1, p. 167-184, 2020. DOI: 10.13071/regec.2317-5087.2020.9.1.27901.167-184. Disponível em: https://www.periodicos.ufes.br/ppgadm/article/view/27901. Acesso em: 27 de novembro de 2020.

HISTEL. **HISTORIA DE LAS TELECOMUNICACIONES**. 2006. Disponível em: <http://histel.com/z_histel/biografias.php?id_nombre=34>. Acesso em: 29 de novembro de 2020.

KOLODENKER, Eugene et al. **Paybreak: Defense against cryptographic ransomware**. In: Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security. 2017. p. 599-611. Disponível em: < https://dl.acm.org/doi/pdf/10.1145/3052973.3053035 >. Acesso em: 27 de novembro de 2020.

LALLIE, Harjinder Singh et al. **Cyber security in the age of COVID-19: a timeline and analysis of cyber-crime and cyber-attacks during the pandemic**. arXiv preprint arXiv:2006.11929, 2020. Disponível em: < https://arxiv.org/pdf/2006.11929.pdf >. Acesso em: 02 de dezembro de 2020.

LEUNG, Louis; ZHANG, Renwen. **Mapping ICT use at home and telecommuting practices: A perspective from work/family border theory**. Telematics Informatics, 34, 385-396, 2017. Disponível em: <http://www.com.cuhk.edu.hk/ccpos/en/pdf/ICT%20Use%20at%20Home%20&%20Telecommuting.pdf>. Acesso em: 29 de novembro de 2020.

MELLO, Daniel. **Home office foi adotado por 46% das empresas durante a pandemia**. Agência Brasil, 2020. Disponível em: < https://agenciabrasil.ebc.com.br/economia/noticia/2020-07/home-office-foi-adotado-por-46-das-empresas-durante-pandemia >. Acesso em: 29 de novembro de 2020.

MENDONÇA, Cláudia da Silva. **Guerra cibernética: desafios de uma nova fronteira**. 2014. Disponível em: < https://pantheon.ufrj.br/bitstream/11422/3340/1/CMendon%C3%A7a.pdf>. Acesso em: 23 de novembro de 2020.

MICROSOFT. **Microsoft Digital Defense Report**. 2020. Disponível em: < https://download.microsoft.com/download/f/8/1/f816b8b6-bee3-41e5-b6cc-e925a5688f61/Microsoft_Digital_Defense_Report_2020_September.pdf >. Acesso em: 12 de novembro de 2020.

MOHSIN, Kamshad. **Cybersecurity in Corona Virus (COVID-19) Age**. 2020. Disponível em: < encurtador.com.br/lxzGX >. Acesso em: 12 de novembro de 2020.

NEED, **Virus Highlights**. United States General Accounting Office. Washington, DC, 1994. Disponível em: <http://ftp.cerias.purdue.edu/pub/doc/morris_worm/GAO-rpt.txt>. Acesso em: 13 de novembro de 2020.

PACAG, Homer. **Multiple Phishing Attacks Discovered Using the Coronavirus Theme**, 2020. Disponível em: <https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/multiple-phishing-attacks-discovered-using-the-coronavirus-theme/>. Acesso em: 12 de novembro de 2020.

PIOVESAN, Leonardo Gubert et al. **ENGENHARIA SOCIAL: Uma abordagem sobre Phishing**. REVISTA CIENTÍFICA UNIBALSAS, v. 10, n. 1, p. 45-59, 2019. Disponível em:<http://www.unibalsas.edu.br/revista/index.php/unibalsas/article/view/94/87>. Acesso em: 22 de novembro de 2020.

PULIDO, Pepe. **Detectan campaña de phishing en alerta sobre coronavirus**, 2020. Disponível em:<https://codigoespagueti.com/noticias/internet/detectan-campana-de-phishing-en-alerta-sobre-coronavirus/>. Acesso em: 22 de novembro de 2020.

RAFAEL, Gustavo de Castro. **Engenharia Social: as técnicas de ataques mais utilizadas**, 2013. Profissionais TI. Disponível em:< http://www. profissionaisti. com. br/2013/10/engenharia-social-astecnicas-de-ataques-mais-utilizadas/>. Acesso em: 22 de novembro de 2020.

REAGAN, Ronald. **National Policy on Telecommunications and Automated Information Systems Security**. National Security Decision Directive NSDD, v. 145, p. 17, 1984. Disponível em: < https://fas.org/irp/offdocs/nsdd/nsdd-145.pdf >. Acesso em: 01 de dezembro de 2020.

REIS, Emanuel. **Golpes sobre Covid-19 no WhatsApp têm 11 milhões de acessos e envios**. 2020. Disponível em: < https://www.techtudo.com.br/noticias/2020/05/golpes-sobre-covid-19-no-whatsapp-tem-11-milhoes-de-acessos-e-envios.ghtml >. Acesso em: 25 de novembro de 2020.

SALEH, Tarik, ANDERSON, Chad. **CovidLock Update: Deeper Analysis of Coronavirus Android Ransomware**. DomainTools, 2020. Disponível em: < https://www.domaintools.com/resources/blog/covidlock-update-coronavirus-ransomware >. Acesso em: 02 de dezembro de 2020.

SAKUDA, Luiz Ojima. **Teletrabalho: desafios e perspectivas**. FGV - Fundação Getúlio Vargas, São Paulo, 2001. Disponível em: < https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/4832/1200101410.pdf >. Acesso em: 27 de novembro de 2020.

SHI, Fleming. **Threat Spotlight: Coronavirus-Related Phishing**. Barracuda, 2020a. Disponível em: < https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing/ >. Acesso em: 02 de dezembro de 2020.

SHI, Fleming. **Threat Spotlight: Ransomware**. Barracuda, 2020b. Disponível em: < https://blog.barracuda.com/2020/08/27/threat-spotlight-ransomware/ >. Acesso em: 03 de dezembro de 2020.

ULBRICH, Henrique César. **Universidade H4ck3r**. Edição 4. Universo dos Livros Editora, 2004. Disponível em: < https://tsilvestre.files.wordpress.com/2012/06/universidade-hacker.pdf >. Acesso em: 02 de dezembro de 2020.