Pandemia na pandemia: a escalada de ataques cibernéticos pós COVID-19

Pandemic in pandemic: the climbing of post COVID-19 cyber attacks

DOI: 10.34117/bjdv8n4-375

Recebimento dos originais: 21/02/2022
Aceitação para publicação: 31/03/2022

Luiz Sergio Dutra Nagli
Doutorando em Administração
Instituição: Escola de Administração de Empresas de São Paulo da Fundação Getúlio Vargas (FGV - EAESP)
Endereço: Avenida Joaquim Porfírio Botelho, 603, Bairro Santo Antônio, CEP: 38182178, Araxá - MG
E-mail: luizn@terra.com.br

RESUMO
A identificação do vírus COVID-19 em dezembro de 2019 em Wuhan, Hubei, China e a decretação de pandemia pela Organização Mundial da Saúde em março de 2020 impactaram a sociedade em escala global. A pandemia forçou uma mudança de comportamento na dinâmica dos relacionamentos interpessoais ao promover medidas de distanciamento social. Neste contexto, muitos trabalhadores foram apresentando ao Home Office, trabalhando longe da segurança das redes corporativas e expostos continuamente ao ambiente virtual. Esta exposição sem proteção adequada criou as condições para a pandemia na pandemia, ou seja, a escalada de ataques cibernéticos verificadas pós COVID-19. Para fazer frente a este quadro, fica a necessidade da Higiene Digital e de uma postura mais empática por parte das empresas, ajudando seus colaboradores neste momento de transição e investindo na mais eficaz das medidas: A educação digital.

Palavras-chave: pandemia, covid-19, ataques cibernéticos, hackers, segurança digital.

ABSTRACT
The identification of the COVID-19 virus in December 2019 in Wuhan, Hubei, China, and the World Health Organization's pandemic decree in March 2020 impacted society on a global scale. The pandemic forced a change in behavior in the dynamics of interpersonal relationships by promoting measures of social distance. In this context, many workers were introduced to the Home Office, working away from the security of corporate networks, and continuously exposed to the virtual environment. This exposure without adequate protection created the conditions for the pandemic in the pandemic, that is, the escalation of cyber-attacks verified after COVID-19. To face this situation, there is the need for Digital Hygiene and a more empathic attitude on the part of companies, helping their employees in this moment of transition and investing in the most effective of measures: Digital education.

Keywords: pandemic, covid-19, cyber attacks, hackers, digital security.

1 INTRODUÇÃO

A identificação do vírus COVID-19 em dezembro de 2019 em Wuhan, Hubei, China e a decretação de pandemia pela Organização Mundial da Saúde em março de 2020 impactaram a sociedade em escala global. A pandemia forçou uma mudança de comportamento, principalmente no que se refere ao trabalho e a como as pessoas se relacionam em um contexto de distanciamento social.

Neste contexto, muitos trabalhadores foram apresentados ao Home Office, trabalhando de casa com uma exposição crescente na internet. Neste cenário, com a dependência crescente de recursos de TI e de rede para o desenvolvimento de suas tarefas, começaram as notícias relacionadas à ataques cibernéticos.

Como o grande facilitador das reuniões virtuais no trabalho e na família, logo após o início da pandemia, o software Zoom foi um dos primeiros a ter ataques noticiados pela grande mídia. Na esteira de um crescimento extraordinário de sua base de usuários, a empresa passou por uma série de críticas a fatores relacionados à segurança digital e precisou de investir pesado em segurança para contornar esta situação. Esta crise culminou com o comunicado do FBI emitido em 30/03/2020, Setera (2020).

Neste artigo, defendemos que este contexto criou as condições para o surgimento de uma outra pandemia dentro na pandemia, neste caso criada pelos crescentes ataques cibernéticos, ataques estes impulsionados pelo grande número de usuários longe da proteção de suas redes corporativas, aumento exponencial do uso da internet e pela sempre presente exploração do medo e do psicológico abalado dos usuários pelos criminosos virtuais.

A Metodologia está baseada na revisão bibliográfica recente, principalmente de revistas, análises de consultorias e de instituições internacionais de combate ao crime virtual. Foram feitas também duas entrevistas com especialistas em segurança digital e finalmente temos a observação dos fatos pelo próprio autor que interage com esta área, segurança digital, por muitos anos.

Em Resultados procurou-se tipificar o crime virtual e enumerar as classes de ataques cibernéticos mais utilizadas neste período. Na Discussão, procurou-se relatar impactos e métodos de prevenção a serem utilizados na mitigação dos ataques sofridos por usuários em home office e suas empresas.

Como Conclusão, são enfatizadas as medidas recentemente denominadas Higiene Digital, e a necessidade de uma postura mais humana e empática por parte das empresas, ajudando seus colaboradores nesta transição e investindo na medida com indiscutível custo x benefício positivo: A educação.

2 METODOLOGIA

O objetivo deste artigo é o de descrever impactos e métodos de prevenção para o que aqui se denomina Pandemia na Pandemia, a escalada de ataques virtuais pós COVID-19, utilizando uma estratégia de pesquisa qualitativa. Segundo Creswell (2010), a pesquisa qualitativa é exploratória e conveniente quando o pesquisador não conhece as variáveis importantes a serem examinadas.

O método utilizado foi a pesquisa bibliográfica, Vergara (2016). Para a autora, este método é um estudo sistematizado com base em material publicado em livros, revistas, jornais e Internet. Pode ser usado para fornecer instrumental analítico para qualquer outro tipo de pesquisa, mas também pode esgotar-se em si mesmo. Para Snyder (2019), o volume da produção de conhecimentos verificadas atualmente, faz com que a revisão de literatura seja considerada um método de pesquisa mais relevante do que nunca. Para o autor, a revisão de literatura como método de pesquisa, cria uma fundação sólida para o avanço do conhecimento. Neste artigo, dado que trabalhamos com um evento em curso, com início meses atrás, temos as fontes baseadas em artigos de jornais e revistas, material de consultorias e entidades de combate ao crime.

A coleta de dados foi baseada em dados primários, obtidos por meio de entrevistas com especialistas em segurança da informação, dados secundários, por meio de artigos como os citados acima, e pela observação, visto que o autor trabalha na área e tem contatos com grandes empresas do mercado.

O assunto escolhido se justifica pela atualidade do tema. Dado o isolamento social, temos uma grande proporção da força de trabalho em modo Home Office, lidando dia a dia com situações novas e com uma exposição grande a internet e aos ataques cibernéticos estudados no artigo.

3 RESULTADOS

A escalada do COVID-19 forçou as empresas a alterar abruptamente a maneira com que conduziam suas operações. Estas mudanças têm como resultado imediato a alocação de um grande volume de trabalhadores no regime de Home Office, aumentando exponencialmente a exposição dos trabalhadores, e suas famílias, a internet. Esta exposição, por motivos de trabalho ou lazer criou uma grande oportunidade para a ação de criminosos digitais. Com os trabalhadores em casa, convivendo com toda à família, também em casa e disputando os recursos de Internet para trabalho, estudo e lazer, o tempo de exposição à rede se multiplicou. Vale dizer, que em muitos casos, o Home Office não contou com o reforço educacional e de segurança digital necessário, longe da segurança das redes corporativas, os trabalhadores se tornaram presa fácil para os criminosos.

Gordon e Ford (2006), separam o crime digital em duas categorias: a primeira, com o foco na tecnologia e a segunda com foco no fator humano. O crime digital relacionado a tecnologia; tem

seu antídoto na mesma tecnologia. Mais ferramentas de proteção em investimentos de hardware e software com o treinamento técnico necessário à sua implementação. Já o crime focado nos fatores humanos tem antidoto na educação. Como elo mais fraco, o fator humano deve ser fortalecido por treinamento contínuo e no caso da atual pandemia reforçado para as questões de adaptação do ambiente remoto e higiene digital.

Para Accenture (2019), três são os fatores de evolução dos crimes digitais. Primeiro com a diversificação dos alvos, antes focados em dados e atualmente com foco em infraestrutura industriais e até nacionais. Em segundo lugar, com o impacto. Os dados podem ser roubados, destruídos, falseados e até sequestrados. Finalmente, as técnicas, focando no elo mais fraco, o fator humano e em estruturas sofisticadas de ataques á países, classificadas atualmente como atos de guerra. A empresa define um ataque digital como uma atividade maliciosa conduzida contra uma organização e sua estrutura de TI através de redes internas e externas ou da internet.

Segundo Mouton e Coning (2020) vários fatores contribuíram para o aumento de ataques pós COVID-19, entre eles:

- Dependência crescente da sociedade na infraestrutura digital;
- Treinamento deficiente dos trabalhadores transferidos para home office;
- O lado psicológico do ser humano e a exploração de seus medos, principalmente em tempo de crise;
- Sociedade dependente no que se refere a consumo de serviços online;
- Falta de treinamento adequado para uma força de trabalho longe da proteção das redes corporativas.

Neste artigo, vamos seguir a seguinte sequência de fatos para guiar a posterior análise de impactos

- 12/2019 – Identificação do vírus COVID-19 (OMS). WHO (2020)
- 02/2020 – Malware Brasileiro usa corona vírus como isca (KARPESKY). Rodrigues (2020)
- 03/2020 – Decretação de pandemia (OMS). WHO (2020)
- 03/2020 – Alerta de Segurança ZOOM (FBI). Setera (2020)
- 03/2020 – Alerta de Segurança Volume de Ataques CISA (2020)
- 04/2020 – Alertas semanais Check Point (2020), TrendMicro (2020) e Kaspersky (2020)

Seguindo a cronologia acima podemos definir os principais impactos no cenário da segurança digital pós COVID-19.

PHISHING / SPEAR-PHISHING

Mouton e Coning (2020) consideram esta técnica como a mais usada para a distribuição de conteúdo malicioso e captura de informação. Phishing chega geralmente com um e-mail, muito bem escrito e formatado de maneira a confundir o usuário com uma comunicação oficial qualquer. Ao acessar um arquivo ou link contido no e-mail o usuário é desviado para um site ou programa malicioso. Geralmente é o vetor de infecção utilizado na distribuição de outros ataques. Enquanto o phishing é baseado em campanhas massivas de envios de e-mail o spear-phishing é mais inteligente e segmentado. Geralmente o spear-phishing é precedido por uma extensa pesquisa de informação. Informação esta que vai ser utilizada para criar uma aproximação com os alvos do ataque.

ENGENHARIA SOCIAL

Ataques que levam em consideração o fator humano. Usando de manipulação e trabalhando com os medos do usuário tentando obter informações que quase sempre serão utilizadas para ganhar acesso a mais informações ou como facilitadoras de novos ataques feitos em conjunto com outras técnicas.

DESINFORMAÇÃO

Para Europol (2020), o compartilhamento de Fake News e os processos de desinformação são pontos chave no cenário atual de ataques digitais. Com os usuários em casa, amedrontados pela pandemia do COVID-19 fica pavimentado o terreno para a manipulação de conceitos e preconceitos dos cidadãos.

WEBSITES MALICIOSOS

Interpol (2020) reportou a criação de sites web maliciosos com o objetivo de iludir usuários a abrir arquivos anexos infectados ou acessar links que carregam malware. Principal objetivo: roubo de identidade. Este ataque é feito em conjunto com técnicas de phishing onde e-mails são enviados, com assuntos relacionados ao COVID-19 redirecionando os usuários para sites com conteúdo malicioso. A Interpol também reportou a criação de domínios com as palavras “covid” ou “corona” que também são usados como isca para este tipo de site.

MALWARE

Softwares maliciosos distribuídos em conjunto com outras técnicas de ataque como o phishing e websites maliciosos. Segundo Interpol (2020), estes softwares na forma de malware, spyware e trojans estão sendo distribuídos largamente sendo associados a assuntos relacionados a pandemia.

DDOS

Em um momento de extrema dependência da internet, como meio de trabalho estudo e lazer, os ataques de negação serviço são utilizados para chantagear os sites atacados e que são levados a indispobilidade, bem como tentando quebrar o código da aplicação possibilitando uma tentativa de acesso privilegiado ao sistema.

MAN IN THE MIDLE

Tipo de ataque onde o agressor se coloca entre o usuário e o acesso desejado. Em época de pandemia e home office, uma das técnicas mais utilizadas é a de manipular o roteador caseiro do usuário, ou instalar um roteador do seu domínio, fazendo com que o usuário pense que está em seu próprio device. A partir do momento que o agressor se interpõe entre usuário e seu objetivo de acesso, todo fluxo de informação está comprometido e sob o domínio do agressor.

RANSOMWARE

Europol (2020) reporta utilização de Ransomware, tipo de software malicioso que sequestra arquivos ou devices através de criptografia pedindo por resgate. Geralmente, o pagamento do resgate deve ser feito via Bitcoin ou qualquer outra moeda virtual. Este tipo de ataque é oferecido na dark web como ataque-as-a-service. Nestes ataques, o acesso ao sistema da vítima é conquistado com técnicas de engenharia social ou phishing, quando a vítima acessa o arquivo ou link infectado, arquivos ou devices são criptografados dando o início ao processo de sequestro.

FALTA DE PROFISSIONAIS DE SEGURANÇA

De um momento para outro as empresas têm seus colaboradores antes concentrados em suas sedes e protegidos pela rede corporativa espalhados por todos os lugares, compartilhando seus links domésticos com toda a família. Se a atividade de segurança da informação já era uma tarefa difícil, agora está ainda mais complexa. Para piorar a situação vivemos uma falta crônica de talentos em TI principalmente aqueles focados na segurança da informação. Muda também o perfil deste

profissional, antes centralizados e baseados em padrões, passam agora a necessitar de mais habilidades de relacionamento e empatia para entender as questões originadas neste novo ambiente.

EDUCAÇÃO DIGITAL

O fator humano é sempre o elo mais fraco nos incidentes de segurança da informação. Neste cenário, a educação é fundamental, os usuários agora em Home Office devem ter treinamento reforçado explicitando as questões relativas ao ambiente doméstico. A palavra de ordem é a Higiene Digital, da mesma maneira que existem normas de higiene para lidar com a pandemia do COVID-19 devem existir normas de Higiene Digital para proteger os acessos digitais dos usuários, sejam eles do trabalho, família ou lazer. O treinamento deve também ser estendido aos profissionais da segurança da informação, pois neste novo ambiente, mudanças de perfil são necessárias para que este profissional possa ajudar este contingente de pessoas trabalhando em Home Office.

SEGURANÇA DO AMBIENTE REMOTO - DOMÉSTICO

Torna-se imperativo que as preocupações com a segurança digital sejam estendidas para a nova realidade do trabalho em Home Office. Não basta apenas liberar acessos VPN e acreditar que tudo vai correr bem. Tanto questões básicas como a ergonomia, iluminação e uma verificação do ambiente caseiro devem ser promovidos como um viabilizador de todo o processo. Roteadores com senha padrão, criptografia fraca e autenticação simples devem ser banidos deste ambiente de trabalho.

D0 – DARK WEB

Para Europol (2020), o impacto da pandemia do COVID-19 foi proveitoso parra a Dark Web. A venda de produtos ilícitos bem como pornografia e artigos falsificados cresceu fortemente. Mas os produtos com a maior demanda são os ataques-as-a-service. Atualmente é possível alugar Bots para ataques bem como alugar infraestrutura sofisticada pera os chamados ataques estruturados. Um dos mercados de maior crescimento é o de vulnerabilidades de softwares recém descobertas. No passado, existia um mercado de vulnerabilidades suportado pelas próprias desenvolvedoras do software onde a descoberta e o compartilhamento da informação eram remunerados em dinheiro. Com as forças invisíveis do mercado sempre promovendo oportunidades de ganhos, honestos ou não, foi criado um mercado na Dark Web onde as chamadas vulnerabilidades D0 são comercializadas livremente em troca de moedas virtuais.

4 DISCUSSÃO

Observando as empresas com as quais lido profissionalmente consigo ver claramente uma corrida para o digital com projetos relacionados à transformação digital sendo priorizados com urgência máxima. A pandemia e o isolamento social geraram um grande impacto sobre os canais de comunicação com os clientes, com a pressão por um relacionamento digital. Podemos confirmar este fenômeno, simplesmente acompanhando as empresas de E-Commerce, marketplaces e as de logística focadas nas entregas de última milha.

Toda a restruturação dos canais das empresas teve que ser implementada ao mesmo tempo da mudança massiva dos trabalhadores para o regime de Home Office. Vale dizer, que este é um recurso já amplamente usado, principalmente pelas empresas de tecnologia, que já funcionavam parcialmente neste regime. A tecnologia já era também dominada pelas grandes empresas, mas com uma utilização efetiva quase marginal.

No ponto de vista do autor, o que aconteceu é que na urgência do processo de transferência para o Home Office, priorizaram-se as condições mínimas de conexão, com algumas empresas até cuidando das condições de trabalho e ergonomia, mas deixando de lado as questões de segurança envolvidas no trabalho em um ambiente doméstico e sem a proteção das redes corporativas.

Um dos consultores entrevistados, chama a atenção para o volume de ataques de Phishing explorando o assunto COVID-19 e ressalta também a sofisticação destes ataques com as técnicas de spear-phishing, onde os ataques são precedidos por uma intensa pesquisa sobre o público a ser atingido. Outro ponto realçado pelo consultor é a falta de cuidados relacionados à segurança do ambiente doméstico, ressaltando a configuração dos acessos de VPN, configurados as pressas e à segurança mínima dos roteadores domésticos sendo que segundo pesquisa atual, a grande maioria deles ainda utiliza as senhas padrão do fabricante. Finalmente, o último ponto ressaltado, foi a escalada de ataques com a utilização de ransomware. Os ataques, baseados em pesquisas prévias com o uso de phishing e engenharia social sequestraram arquivos e equipamentos por todo o mundo, cobrando um resgate em moeda virtual para a liberação.

Já nosso segundo entrevistado ressalta que pessoas e empresas foram forçadas ao isolamento diante de uma situação inusitada e repentina: COVID 19. Esse inimigo fez com que todos se trancassem em casa e utilizassem os recursos tecnológicos para continuarem suas atividades, funções e processos, que até então faziam no âmbito pessoal, na empresa/escritório. A vida do usuário na empresa de certa forma era “controlada” e protegida pelos vários dispositivos ou controles existentes dentro da rede corporativa da empresa. Assim sendo, se faz necessário aumentar os controles e/ou aplicar novas medidas de prevenção e proteção, no novo *modus operandi*.

Fora do ambiente controlado e protegido da rede corporativa, o usuário se torna um alvo mais suscetível a ataques. Mesmo com os meios e dispositivos de proteção presentes no computador, dependendo do modo como o usuário trabalha ou utiliza o recurso computacional, o atacante poderá atuar e agir para comprometer o sistema, utilizar o mesmo como sistema zumbi e ainda furtar informações relevantes dele mesmo usuário ou da empresa contidas ou acessadas no equipamento. Dentro do ambiente corporativo existem barreiras digitais que por sua vez fornecem uma proteção monitorada, diferentes das utilizadas ou existentes no mundo home office.

As instituições internacionais de combate ao crime obviamente tiveram e tem uma postura de investigação e confronto, mas atuaram também fortemente com medidas educacionais. Em FBI (2020) são reforçados os conceitos de proteção contra a pornografia infantil e medidas de proteção contra os crimes visando vantagens financeiras. Vale ressaltar os alertas diários, educativos e preventivos, FBI (2020) que de certa maneira ajudaram a mapear os crimes digitais, pós COVID-19 desde o mês de março. Outra importante atuação é a do CISA (2020), Cybersecurity and Infrastructure Security Agency, que com seus alertas e comunicados, neste caso de cunho mais técnico, ajudaram e ajudam a comunidade internacional de TI na prevenção e na mitigação dos resultados dos ataques.

A Interpol, com seus convênios com inúmeras consultorias de segurança também teve um grande esforço na educação digital dos usuários pelo mundo, reforçando de uma forma detalhada e didática os conceitos de higiene digital, Interpol (2020). Nos comunicados da Europol, já encontramos alertas focados em questões como Fake-News e a exploração da pornografia infantil. A instituição também expressa preocupação com os ataques mais sofisticados como os de DDOS e Ransomware, Europol (2020).

As consultorias por sua vez se manifestaram em termos de roteiros para a transição. Em Mckinsey (2020), são exploradas as medidas que devem ser tomadas em 3 áreas:

- Tecnologia:
  - Aumentar o ciclo de atualização de vulnerabilidades de softwares;
  - Implementação em larga escala de autenticação de dois fatores;
  - Preparar as aplicações internas para uso remoto;
  - Controle das aplicações shadow IT;
  - Virtualização de devices na NUVEM.
- Pessoas:
  - Investir na comunicação de forma criativa;
  - Foco no que fazer e não no negativo;
  - Cuidados com a engenharia social;

- Identificar e monitorar os grupos com grandes riscos.

- Processos:
  - Suporte remoto com foco em segurança;
  - Ajustes nos processos de resposta a incidentes, continuidade de negócios e restabelecimento de desastres;
  - Expandir a monitorização dos pontos de home office;
  - Estreitar relacionamentos com os terceiros;
  - Agilidade nas compras.

KPMG (2020) complementa o roteiro com preocupações relacionadas à capacidade da infraestrutura para suportar os acessos remotos e a questões de resiliência, onde procura se evitar pontos de falha com a implementação de redundâncias. A empresa ressalta também a capacidade de atendimento do Help Desk e seu preparo para lidar com a descentralização do ambiente de Home Office. Em BCG (2020) já são reforçados os conceitos de preparo prévio dos ambientes remotos de trabalho bem como a atualização dos procedimentos de suporte, contingência e restabelecimento de desastres.

5 CONCLUSÃO

Como conclusão, vale a transposição dos conceitos da epidemia do COVID-19 para a pandemia de ataques digitais. Os dois fenômenos devem ser tratados de forma similar. Atualizar os sistemas e devices do ambiente remoto são o mesmo que lavar as mãos. Não acessar links contidos em e-mails suspeitos é o mesmo que não levar as mãos no rosto. Manter firewall e antivírus atualizados é o mesmo que usar máscaras. A importância da higiene digital ficou evidenciada nesta crise.

Mudanças também devem acontecer nas empresas. As equipes de suporte e segurança devem ser dimensionadas e treinadas para o novo ambiente. Segurança antes, uma área centralizada deve se adaptar rapidamente à nova descentralização. Educação é a resposta principal, as empresas precisam investir no conhecimento de seus colaboradores reconhecendo o fato de que eles não estão mais protegidos pelas estruturas corporativas.

REFERÊNCIAS

Accenture. The Cost of Cybercrime. Acessado em 15/07/2020 de https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

BCG. Managing the Cyber Risks of Remote Work. Acessado em 15/07/2020 de https://www.bcg.com/pt-br/publications/2020/covid-remote-work-cyber-security

Creswell, J. W. Projetos de Pesquisa: Métodos Qualitativo, Quantitativo e Misto. 3. ed. Porto Alegre: Artmed, 2010.

Check Point. (2020) Secure Remote Workforce During Coronavirus. Acessado em 15/07/2020 de https://www.checkpoint.com/solutions/secure-remote-workforce-during-coronavirus/

Cybersecurity and Infrastructure Security Agency – CISA. (2020) Defending Against COVID-19 Cyber Scams. Acessado em 15/07/2020 de https://us-cert.cisa.gov/ncas/current-activity/2020/03/06/defending-against-covid-19-cyber-scams

Europol. (2020) Catching the virus: cybercrime, disinformation and the COVID-19 pandemic. Acessado em 15/07/2020 de https://www.europol.europa.eu/publications-documents/catching-virus-cybercrime-disinformation-and-covid-19-pandemic

FBI (2020) FBI urges Vigilance During COVID-19 Pandemic. Acessado em 15/07/2020 de https://www.fbi.gov/coronavirus

Gordon, S.; Ford, R. COVID-19: On the Definition and Classification of Cybercrime. Journal of Computing Virology, 2006.

Interpol. (2020) Global Landscape on COVID-19 cyberthreat. Acessado em 15/07/2020 de https://www.interpol.int/Crimes/Cybercrime/COVID-19-cyberthreats

Karpersky. (2020) COVID-19 Guia de sobrevivência para sua vida digital. Acessado em 15/07/2020 de https://www.kaspersky.com.br/blog/coronavirus-digital-survivor-guide/14799/

KPMG. Risk and security in the wake of COVID-19. Acessado em 15/07/2020 de https://assets.kpmg/content/dam/kpmg/xx/pdf/2020/04/risk-and-security-in-the-wake-of-covid-19-concern.pdf

Mckinsey. Cybersecurity tactics for the coronavirus pandemic. Acessado em 15/07/2020 de https://www.mckinsey.com/business-functions/risk/our-insights/cybersecurity-tactics-for-the-coronavirus-pandemic

Mouton, F.; Conning, A. COVID-19: Impact on the Cyber Security Threat Landscape. Researchgate, 2020.

Rodrigues, R. (2020) Malware Brasileiro usa Corona vírus como isca. Acessado 15/07/2020 em https://www.kaspersky.com.br/blog/malware-coronavirus-isca-brasil/14021/

Setera, K. (2020) FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic. Acessado 15/07/2020 em https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic

Snyder, H. Literature Review as a Research Methodology: An overview and Guidelines. Journal of Business Research, 2019.

TrendMicro. (2020) COVID-19 Threat Brief Summary. Acessado em 15/07/2020 de https://resources.trendmicro.com/rs/945-CXD-062/images/Trend-Micro-Research-COVID19-Threat-Brief-Summary-27Mar.pdf

Vergara, S. C. Projetos e Relatórios de Pesquisa em Administração. São Paulo: Atlas, 2016.

World Health Organization - WHO (2020) Timeline of WHO's response to COVID-19. Acessado em 15/07/2020 de https://www.who.int/news-room/detail/29-06-2020-covidtimeline