computadores e segurança 1 0 5 (2 0 2 1) 1 0 2 2 4 8

Disponível on-line emwww.sciencedirect.com

ScienceDirect

Página inicial do jornal:www.elsevier.com/locate/cose

Computers & Security

Segurança cibernética na era do COVID-19: uma linha do tempo e análise de crimes cibernéticos e ataques cibernéticos durante a pandemia

Harjinder Singh Lallie [uma,*], ***Lynsay A. Shepherd*** [b], ***Jason RC enfermeira*** [c], ***Arnau Erola*** [d], ***Gregório Epifânio*** [uma], ***Carsten Maple*** [uma], ***Xavier Bellekens*** [e]

uma *WMG, Universidade de Warwick, Coventry, Reino Unido*

b *Escola de Design e Informática, Abertay University, Dundee, Reino Unido*

c *Escola de Computação, Universidade de Kent, Canterbury, Reino Unido*

d *Departamento de Ciência da Computação, Universidade de Oxford, Oxford, Reino Unido*

e *Departamento de Engenharia Eletrônica e Elétrica, Universidade de Strathclyde, Glasgow, Reino Unido*

artigoinfo

Historia do artigo:

Recebido em 28 de junho de 2020 Revisado em 21 de novembro de 2020 Aceito em 22 de fevereiro de 2021 Disponível online em 3 de março de 2021

Palavras-chave:

Coronavírus

COVID-19

Cíber segurança

Ataque cibernético

Crime cibernético

Linha do tempo do ataque

Trabalho em casa

abstrato

A pandemia do COVID-19 foi um evento notável e sem precedentes que alterou a vida de bilhões de cidadãos em todo o mundo, resultando no que ficou conhecido como o*novo normal*em termos de normas sociais e a maneira como vivemos e trabalhamos. Além do impacto extraordinário na sociedade e nos negócios como um todo, a pandemia gerou um conjunto de circunstâncias únicas relacionadas ao crime cibernético que também afetaram a sociedade e os negócios. O aumento da ansiedade causada pela pandemia aumentou a probabilidade de sucesso dos ataques cibernéticos, correspondendo a um aumento no número e alcance dos ataques cibernéticos.

Este artigo analisa a pandemia do COVID-19 sob a perspectiva do crime cibernético e destaca a variedade de ataques cibernéticos experimentados globalmente durante a pandemia. Os ataques cibernéticos são analisados e considerados no contexto dos principais eventos globais para revelar o modus operandi das campanhas de ataques cibernéticos. A análise mostra como, seguindo o que pareciam ser grandes lacunas entre o surto inicial da pandemia na China e o primeiro ataque cibernético relacionado ao COVID-19, os ataques se tornaram muito mais prevalentes a ponto de, em alguns dias, três ou quatro ciberataques únicos -ataques estavam sendo relatados. A análise prossegue utilizando o Reino Unido como um estudo de caso para demonstrar como os cibercriminosos aproveitaram eventos importantes e anúncios governamentais para elaborar e executar cuidadosamente campanhas de cibercrime.

1. Introdução

O Coronavírus-2 da Síndrome Respiratória Aguda Grave (SARS-CoV-2) é uma nova cepa da doença do coronavírus detectada pela primeira vez em humanos em 2019. Em 11 de fevereiro de 2020, o mundo

A Organização Mundial da Saúde (OMS) anunciou que se referiria à doença como COVID-19. A pandemia que resultou da disseminação do COVID-19 rapidamente se tornou um evento de crise global, resultando na quarentena em massa de centenas de milhões de cidadãos em vários países ao redor do mundo. No momento da redação deste artigo, o Painel da Doença de Coronavírus da OMS (COVID-19) relatou mais de 7,5 milhões de casos confirmados e em excesso

*Autor correspondente.

*Endereço de e-mail:*HL@warwick.ac.uk (HS Lallie),lynsay.shepherd@abertay.ac.uk (LA Pastor),jrcnurse@kent.ac.uk (Enfermeira JRC), arnau.erola@cs.ox.ac.uk (A. Erola),gregory.epiphaniou@warwick.ac.uk (G. Epifânio),CM@warwick.ac.uk (C. Bordo), xavier.bellekens@strath.ac.uk (X. Bellekens). https://doi.org/10.1016/j.cose.2021.102248

0167-4048/

de 430.241 mortes (Organização Mundial da Saúde (OMS), 2020c) globalmente. À medida que o COVID-19 se espalhou pelo mundo, ele também levou a uma ameaça secundária significativa a uma sociedade impulsionada pela tecnologia; ou seja, uma série de ataques cibernéticos e campanhas de crimes cibernéticos indiscriminados e também direcionados. Desde o surto, houve relatos de golpes que se faziam passar por autoridades públicas (por exemplo, OMS) e organizações (por exemplo, supermercados, companhias aéreas) (MalwareBytes, 2020; The Times, 2020), visando plataformas de suporte (Krebs sobre Segurança, 2020; Smithers, 2020), conduzindo fraudes de equipamentos de proteção individual (EPI) (Europol, 2020) e oferecendo curas para a COVID-19 (Norton, 2020; O Guardião, 2020). Esses golpes têm como alvo o público em geral, bem como os milhões de indivíduos que trabalham em casa. Trabalhando em casa*em massa*percebeu um nível de preocupações e desafios de segurança cibernética nunca antes enfrentados pela indústria e pelos cidadãos. Os cibercriminosos aproveitaram esta oportunidade para expandir seus ataques, usando truques tradicionais (por exemplo, Enfermeira (2019)) que também reza pelo aumento do estresse, ansiedade e preocupação enfrentados pelos indivíduos. Além disso, as experiências de trabalho em casa revelaram o despreparo geral dos fornecedores de software, principalmente no que diz respeito à segurança de seus produtos.

Os ataques cibernéticos também têm como alvo infraestruturas nacionais críticas, como serviços de saúde (Com fio, 2020). Em resposta a isso, em 8 de abril de 2020, o Centro Nacional de Segurança Cibernética (NCSC) do Reino Unido e a Agência de Segurança Cibernética e Segurança de Infraestrutura (CISA) do Departamento de Segurança Interna (DHS) dos Estados Unidos publicaram um comunicado conjunto sobre como os criminosos cibernéticos e avançados grupos de ameaça persistente (APT) estavam explorando a atual pandemia de COVID-19 (Centro Nacional de Segurança Cibernética do Reino Unido (NCSC), 2020a). Este comunicado discutiu questões como phishing, malware e comprometimento da plataforma de comunicação (por exemplo, Zoom, Microsoft Teams). O que provavelmente falta aqui e na pesquisa, no entanto, é uma avaliação mais ampla da ampla gama de ataques relacionados à pandemia. O estado da arte atual é extremamente disperso, com ataques sendo relatados por governos, mídia, organizações de segurança e equipes de incidentes. Portanto, é extremamente desafiador para as organizações desenvolver medidas adequadas de proteção e resposta, dado o ambiente dinâmico.

Neste artigo, pretendemos apoiar a pesquisa em andamento, propondo uma nova linha do tempo de ataques relacionados à pandemia de COVID-19. Essa linha do tempo e a análise subsequente podem ajudar a entender esses ataques e como eles são elaborados e, como resultado, a se preparar melhor para enfrentá-los, caso sejam vistos novamente. Nossa linha do tempo mapeia os principais ataques cibernéticos em todo o mundo contra a propagação do vírus e também medidas como quando os bloqueios foram implementados. A linha do tempo revela um padrão que destaca ataques cibernéticos e campanhas que normalmente seguem eventos como anúncios de políticas. Isso nos permite rastrear a rapidez com que ataques cibernéticos e crimes foram testemunhados em comparação com quando os primeiros casos de pandemia foram relatados na área; ou, de fato, se os ataques anteciparam qualquer um desses eventos. Expandimos a linha do tempo para focar em como ataques específicos se desenrolaram, como eles foram elaborados e seu impacto no Reino Unido. Para complementar essas análises, refletimos mais amplamente sobre a variedade de ataques relatados, como eles impactaram a força de trabalho e como a força de trabalho ainda pode estar em risco. De muitas maneiras, essa análise da linha do tempo também constitui uma chave contribuição do nosso trabalho tanto em termos de sequenciamento cronológico de ataques quanto na representação de campanhas usando uma taxonomia de ataque aceita. Isso, portanto, fornece uma plataforma que se alinha com a literatura atual e também fornece a base sobre a qual outras pesquisas podem ser construídas facilmente.

Este artigo está estruturado da seguinte forma.Seção 2reflete sobre a literatura relevante sobre ataques cibernéticos e crimes cibernéticos e considera como ataques oportunistas surgiram no passado devido a crises/incidentes da vida real. Em seguida, apresentamos nossa linha do tempo de ataques cibernéticos relacionados ao COVID-19 emSeção 3 bem como um foco dedicado no Reino Unido como um estudo de caso da principal atividade cibercriminosa. Isso é seguido por uma reflexão mais ampla sobre os ataques (aqueles dentro e fora da linha do tempo). Dentro Seção 4discutimos o impacto dos ataques naqueles que trabalham em casa e o risco tecnológico mais amplo.Seção 5conclui o artigo e delineia direções para trabalhos futuros.

2. Revisão da literatura

Com a ampla adoção de tecnologias digitais, muitas facetas da sociedade passaram a ser online, desde compras e interações sociais até negócios, indústria e, infelizmente, também crimes. Os últimos relatórios estabelecem que o cibercrime está crescendo em frequência e gravidade (Hiscox, 2019), com previsão de atingir US$ 6 trilhões até 2021 (acima dos US$ 3 trilhões em 2015) (Empreendimentos de segurança cibernética, 2019) e até assumir o crime tradicional em número e custo (Anderson et al., 2019; CBS Holanda, 2020). Devido à sua natureza lucrativa (McGuire, 2018) e baixo nível de risco (já que os cibercriminosos podem lançar ataques de qualquer lugar do mundo), fica claro que o cibercrime veio para ficar.

O cibercrime, como crime tradicional, é frequentemente descrito pelo triângulo do crime (Cruz e Shinder, 2008), que especifica que para que um cibercrime ocorra, três fatores devem existir: uma vítima, um motivo e uma oportunidade. A vítima é o alvo do ataque, o motivo é o aspecto que leva o criminoso a cometer o ataque e a oportunidade é uma chance de o crime ser cometido (por exemplo, pode ser uma vulnerabilidade inata no sistema ou um dispositivo desprotegido). Outros modelos em criminologia, como a Teoria da Atividade Rotineira (RAT) (Ano, 2005) e o triângulo da fraude (Cressey, 1953) utilizam fatores semelhantes para descrever os crimes, alguns substituindo a vítima por meio do agressor, o que pode ser considerado de outra forma como parte da oportunidade.

Enquanto os ataques hoje se tornaram mais sofisticados e direcionados a vítimas específicas, dependendo da motivação do invasor, por exemplo, para ganho financeiro, espionagem, coerção ou vingança; ataques não direcionados oportunistas também são muito prevalentes. Definimos “ataques oportunistas” como ataques que selecionam as vítimas com base em sua susceptibilidade de serem atacadas (Dhanjani e outros, 2009). Os invasores oportunistas capturam vítimas com vulnerabilidades específicas ou usam ganchos, geralmente na forma de engenharia social, para criar essas vulnerabilidades. Assim, definimos como*gancho*qualquer mecanismo usado para induzir uma vítima a ser vítima de um ataque.

Esses ganchos aproveitam a distração, as restrições de tempo, o pânico e outros fatores humanos para fazê-los funcionar (Enfermeira, 2019; Stajano e Wilson, 2011). Quando as vítimas estão distraídas com o que chama sua atenção/interesse ou quando

eles estão em pânico, eles são mais suscetíveis a serem enganados. Da mesma forma, as restrições de tempo colocam as vítimas sob mais pressão, o que pode levar a erros e aumentar a probabilidade de serem vítimas de golpes e ataques. Outros exemplos incluem pressão de trabalho, mudança de situação pessoal, problemas médicos ou eventos que causam impacto profundo e traumático em toda a sociedade em geral, como fatalidades e catástrofes.

Os invasores oportunistas sempre buscam maximizar seu ganho e, portanto, aguardarão o melhor momento para lançar um ataque em que as condições se encaixem nas mencionadas acima. Um desastre natural, crise em andamento ou evento público significativo são casos perfeitos dessas condições (Tisíaco, 2018). No passado, foram observados vários ataques oportunistas que se aproveitaram de incidentes específicos; abaixo, fornecemos alguns exemplos:

- Desastres naturais: Em 2005, o furacão Katrina causou destruição maciça na cidade de Nova Orleans e arredores nos EUA (FBI, 2016). Não muito tempo depois, milhares de sites fraudulentos apareceram apelando para doações humanitárias, e os cidadãos locais receberam e-mails fraudulentos solicitando informações pessoais para receber possíveis pagamentos ou esforços de ajuda do governo. Golpes e ataques semelhantes foram testemunhados em inúmeros desastres naturais desde então, como os terremotos no Japão e no Equador em 2016FTC (2016), Furacão Harvey em 2017CNET (2017), ou os incêndios florestais na Austrália em 2020Elsworthy (2020).
- Incidentes ou eventos notáveis: Em 25 de junho de 2009, a trágica morte de Michael Jackson dominou as notícias em todo o mundo. Apenas 8 horas após sua morte, e-mails de spam alegando conhecer os detalhes do incidente estavam circulando online (Segurança Nua, 2009). Ondas de e-mails ilegítimos ecoando a fatalidade apareceram logo depois, contendo links prometendo acesso a vídeos e fotos não publicados ou mercadorias de Jackson, que na verdade estavam vinculados a sites maliciosos, ou e-mails com anexos infectados por malware (Hoffman, 2009). Eventos públicos notáveis também atraem uma série de atividades de crimes cibernéticos. Durante a Copa do Mundo da FIFA em 2018, por exemplo, houve várias tentativas de atrair indivíduos com ingressos gratuitos e brindes (ESET, 2018). Na verdade, eram golpes que levavam à fraude.

- Incidentes de segurança: em 2012, 164 milhões de endereços de e-mail e senhas foram expostos em uma violação de dados do LinkedIn (Jansson, 2018). Esses dados não foram divulgados até 4 anos depois, 2016, quando apareceram à venda no mercado negro. Logo depois disso, atacantes oportunistas começaram a lançar uma série de ataques. Muitos usuários sofreram golpes, como chantagem e phishing, e algumas contas comprometidas que não haviam alterado suas senhas desde a violação foram usadas para enviar links de phishing por mensagem privada e InMail (Seguro, 2017).

Considerando a variedade de golpes e ataques cibernéticos que ocorrem em torno dos eventos acima, não é surpreendente que ataques semelhantes tenham surgido durante a atual pandemia de COVID-19. O surto causou transtornos em massa em todo o mundo, com as pessoas tendo que adaptar suas rotinas diárias a uma nova realidade: trabalhar em casa, falta de interações sociais e atividade física e medo de não estar preparado (NHS, 2020; OMS, 2020). Essas situações podem sobrecarregar muitos e causar estresse e ansiedade que pode aumentar as chances de ser vítima de um ataque. Além disso, a mudança repentina de contextos de trabalho fez com que as empresas tivessem que improvisar novas estruturas de trabalho, potencialmente deixando os ativos corporativos menos protegidos do que antes por causa da interoperabilidade.

A maioria dos relatórios concorda que o número de golpes e ataques de malware aumentou significativamente desde o início da pandemia (Gallagher e Brandt, 2020). Houve um aumento relatado de 600% nos ataques de phishing em março de 2020Shi (2020). O Fórum Econômico Mundial (WEF) informou que a pandemia levou a um aumento de 50,1% em ataques cibernéticos e 30.000 ataques cibernéticos associados especificamente relacionados ao COVID-19 entre 31 de dezembro de 2019 e 14 de abril de 2020 (Fórum Econômico Mundial, 2020). A CGI relatou um aumento de 30.000% no número de ameaças cibernéticas especificamente devido ao COVID-19 (Exuberante, 2020). Nos quatro meses entre janeiro e abril de 2020, a Interpol detectou cerca de *"907.000 mensagens de spam, 737 incidentes relacionados a malware e 48.000 URLs maliciosos vinculados ao COVID-19"* e descobriu que o *"o pagamento médio de ransomware no segundo trimestre de 2020 foi de US$ 178.254, um aumento de 60% em relação ao primeiro trimestre"* (Davis, 2020). O aumento das demandas de pagamento de ransomware pode indicar que os cibercriminosos podem perceber uma maior probabilidade de pagamento devido às circunstâncias extraordinárias apresentadas pela pandemia. Para agravar esses fatos, durante abril de 2020, o Google supostamente bloqueou 18 milhões de e-mails de malware e phishing relacionados ao vírus diariamente (Kumaran e Lugani, 2020). Para aumentar a probabilidade de sucesso, esses ataques visam a venda de mercadorias em alta demanda (por exemplo, equipamentos de proteção individual (EPI) e kits e medicamentos para teste de coronavírus), investimentos potencialmente altamente lucrativos em ações relacionadas ao COVID-19 e falsificações de representantes de instituições públicas autoridades como a OMS e golpes de ajuda (Europol, 2020; O'Brien, 2020).

Grandes intervalos foram especificados em termos de aumento de ataques cibernéticos e, em particular, formas específicas de ataques cibernéticos, como phishing e/ou ransomware. De certa forma, não está claro que proporção desse aumento de ataques se deve especificamente à pandemia e como eles são distribuídos por tipo de ataque cibernético. Embora possamos esperar que o número de COVID*ganchos* em ataques cibernéticos aumentaria em meio à pandemia, é difícil avaliar o nível em termos quantitativos. Também é um desafio determinar até que ponto essas *ganchos* substituído ou complementado anterior *ganchos* tal como *Brexit*. Para ilustrar o problema, considere o seguinte. É difícil determinar qual proporção do aumento de 50,1% relatado pelo WEF compreendeu os 30.000 ataques inspirados no COVID-19, houve outros *ganchos* identificados, em caso afirmativo, qual a proporção? Os números relatados pelo CGI são de experiência própria e não há referência a números anteriores à pandemia.

Ataques de força bruta nos sistemas Microsoft Remote Desktop Protocol (RDP) também aumentaram (Galov, 2020), sinalizando ataques também à tecnologia, não apenas aos aspectos humanos. Fica claro, então, que os invasores estão tentando aproveitar ao máximo a interrupção causada pela pandemia, principalmente porque ela continua a persistir. Como consequência, várias diretrizes e recomendações também foram publicadas para proteção contra ataques (FTC, 2020; NCSC, 2020a; NIST, 2020). Essas diretrizes são imperativas para mitigar a ameaça crescente, mas para fortalecer sua base, primeiro é necessário haver um núcleo

compreensão dos ataques cibernéticos que estão sendo lançados. Este artigo procura abordar essa lacuna na pesquisa e na prática, definindo um cronograma de ataques cibernéticos e considerando como eles afetam os cidadãos e a força de trabalho.

3. Linha do tempo dos ataques cibernéticos relacionados ao COVID-19

Os incidentes de cibercrime decorrentes da pandemia de COVID-19 representam sérias ameaças à segurança e à economia global da população mundial, pelo que é essencial compreender os seus mecanismos, bem como a propagação e o alcance dessas ameaças. Inúmeras soluções foram propostas na literatura para analisar como tais eventos se desenrolam, variando de definições formais a abordagens sistêmicas que revisam a natureza das ameaças (Hindy et al., 2018; Kotenko e Chechulin, 2013; Tsakalidis e Vergidis, 2017). Embora essas abordagens permitam a categorização do ataque, elas geralmente carecem da capacidade de mapear eventos maiores e distribuídos, como os apresentados neste manuscrito, onde vários eventos decorrentes da pandemia não estão relacionados. Para tal, optámos pela visualização temporal, permitindo mapear os acontecimentos sem comprometer a narrativa (Kolomiyets et al., 2012). Além disso, esse tipo de visualização é usado em todo o domínio de segurança cibernética para representar ataques cibernéticos consequentes (Falliere et al., 2011; Horton e DeSimone, 2018; Van Heerden e outros, 2016).

3.1. Metodologia de criação de linha do tempo

Nesta seção, descrevemos a metodologia usada para criar a linha do tempo. Explicamos os termos de pesquisa usados para coletar dados relevantes sobre ataques cibernéticos COVID-19, as fontes de dados (mecanismos de pesquisa) utilizadas, as fontes de informação nas quais escolhemos focar e os tipos de ataque. Também reconhecemos as possíveis limitações do trabalho.

3.1.1. Nomenclatura

Exploramos uma série de ataques cibernéticos que ocorreram durante a pandemia de COVID-19. O novo coronavírus foi referido por vários termos diferentes no mundo de língua inglesa, incluindo Coronavírus, COVID19, COVID-19, 2019-nCoV e SARS-CoV-2. Usamos o termo COVID-19 para nos referir ao vírus, o que está de acordo com a terminologia usada peloOrganização Mundial da Saúde (OMS) (2020b).

3.1.2. Construção da linha do tempo

Para auxiliar na construção da linha do tempo, inicialmente realizamos uma série de buscas para identificar ataques cibernéticos intimamente ligados à pandemia. Esses ataques cibernéticos foram categorizados por tipo de ataque, método de entrega e foram ordenados por data. A informação recolhida foi recolhida e apresentada em Figura 2que serve de base para a construção da Tabela 1.

As informações apresentadas na linha do tempo incluem a data em que a China alertou a OMS sobre o vírus, a data em que a pandemia foi oficialmente declarada e os ataques cibernéticos relacionados especificamente a hospitais ou remédios. Além disso, foram identificados os principais países envolvidos na pandemia e, para eles, apresentamos o primeiro caso identificado, a data em que o bloqueio foi implementado e o primeiro ataque cibernético sofrido. A tabela procura examinar um subconjunto das informações da linha do tempo.

Além disso, optamos por incluir várias fontes que oferecem relatórios de ataques. As fontes são uma mistura de agências de notícias respeitáveis (como a Reuters e a BBC), artigos de blog, relatórios de empresas de segurança e postagens de mídia social. Embora os artigos de blog e postagens de mídia social não sejam considerados uma fonte acadêmica, no contexto desta pesquisa em que estamos examinando uma ameaça emergente, eles oferecem informações importantes sobre as tendências de ataques cibernéticos. Também é importante observar que os ataques cibernéticos podem ser apresentados primeiro nesses domínios, antes de serem destacados pelos principais meios de comunicação. No que diz respeito à inclusão de notícias na tabela de ataques e subsequente linha do tempo, deve-se reconhecer que esses ataques estão sendo apresentados através de lentes jornalísticas e, como tal, podem ser escritos na tentativa de ganhar manchetes. No entanto, esses ataques cibernéticos relatados ainda representam uma ameaça tangível para o público em geral durante a pandemia do COVID-19. A linha do tempo procura fornecer uma visão geral dos ataques que ocorreram.

A revisão dos relatórios foi realizada de meados de março a meados de maio de 2020. A linha do tempo limita os ataques cibernéticos aos ocorridos até 31 de março. Isso porque atingimos o que acreditávamos ser um ponto de saturação com um número suficiente de ataques cibernéticos para ser representativo. Após a conclusão da busca, o primeiro ataque relatado foi em 6 de janeiro de 2020 (Henderson e outros, 2020), enquanto o ataque listado mais recentemente na linha do tempo foi em 31 de março de 2020 (O'Donnell, 2020). O ataque listado mais recentemente na tabela foi em 13 de maio de 2020 (CNET, 2020). A tabela avança um pouco mais no período de tempo, pois pretende fornecer mais detalhes em relação aos ataques cibernéticos ocorridos durante esse período. As fontes foram coletadas de vários locais. Os critérios usados para localizar relatórios foram definidos abaixo e são apresentados de maneira semelhante às revisões existentes na literatura de segurança cibernética (Chockalingam et al., 2017; Pastor e Renaud, 2018). A estrutura da linha do tempo é descrita com mais detalhes em Seção 3.2.

*Motores de busca*Vários mecanismos de busca foram usados na criação da tabela e da linha do tempo. Estes foram- Google[1] (com sede nos EUA e domina a participação no mercado de mecanismos de busca), Baidu[2](Provedor de pesquisa baseado na China), Qwant[3] (Mecanismo de busca francês com foco em privacidade) e Duck-DuckGo[4] (Mecanismo de busca baseado nos EUA com foco em privacidade).

*Palavras-chave usadas*Uma variedade de palavras-chave foi usada ao coletar relatórios de ataques cibernéticos e crimes cibernéticos. Além dos relatórios em inglês, também buscamos resultados em chinês, japonês, francês, italiano e espanhol. Limitamos nosso escopo para focar nos países que relataram grandes grupos de casos de COVID-19 durante os estágios iniciais da pandemia.

Os termos não ingleses foram traduzidos usando o serviço Google Tradutor (Google, 2020) e fontes independentes adicionais foram usadas como meio de validar a tradução. Quando fo-

1 www.google.com
2 www.baidu.com
3 www.qwant.com
4 www.duckduckgo.com

Tabela 1 – Descrições de ataques cibernéticos relacionados ao COVID-19.

EU IRIA	Ref.	País	Ataque modelo	Descrição	Artigo encontro	Ataque encontro
1	Henderson e outros. (2020)	China	PM	Vietname acusado de lançar um *METAL JACK* campanha de phishing contra os escritórios do distrito de Wuhan	22/04	01/06
2	AON (2020)	Global	PM	Relatórios internacionais de que campanhas de phishing e smishing estão ocorrendo	19/01	-
3	Forbes (2020)	China, Mongólia	PM	Hackers chineses acusados de distribuir o *Panda Cruel* malware para a Mongólia através de e-mails supostamente vindos do ministério de negócios da Mongólia	12/03	20/01
4	F-Secure (2020)	Filipinas	PMF	*REMCOS* malware distribuído a cidadãos filipinos Campanha	13/03	23/01
5	Kaspersky (2020)	Cingapura	P	de phishing rouba credenciais de login de e-mail Medidas de	28/01	-
6	Valter (2020)	Japão	PMF	segurança distribuição de campanha de phishing *Emotet* malware	28/01	28/01
7	smzdm. com (2020)	China	PMF	E-mail de 'medida de segurança' de um 'especialista de Cingapura' distribui *Emotet* malware	06/02	29/01
8	Kaspersky (2020)	EUA	P	E-mail com suposta lista de casos de COVID-19 na cidade da vítima leva usuário a site que rouba credenciais DoS em	11/02	31/01
9	CSDN (2020)	China	H	unidades de prevenção de epidemias	02/09	02/02
10	CSDN (2020)	China	P	Campanha de phishing rouba credenciais de login de e-mail	02/09	02/02
11	TechRepublic (2020)	Mundo	PMF	Primeiros casos de *AZORult* um malware de roubo de dados	10/02	-
12	cqgbxa.com (2020)	China	PM	E-mail com medidas de segurança especializadas da OMS solicita download de malware	12/02	-
13	F-Secure (2020)	Vietnã	PM	*LOKIBOT* malware espalhado por e-mail alegando pagamento incorreto de fatura	13/03	03/02
14	Patranobis (2020)	China	P.Ph	Ataque de phishing a grupos médicos na China (da Índia)	06/02	06/02
15	freebuf. com (2020)	China	PME	Distribuição de *CXK-NMSL* ransomware através de e-mails com tema COVID-19	18/02	02/09
16	freebuf. com (2020)	China	PME	Distribuição de *Dharma/Crise* ransomware através de e-mails com tema COVID-19	18/02	13/02
17	F-Secure (2020)	Itália	PM	*Trickbot* malware distribuído por e-mail malware MBR	13/03	02/03
18	Stonefly (2020)	Global	PMF	wiper disfarçado como informações de rastreamento de contato	04/03	-
19	F-Secure (2020)	EUA	PM	*FORMBOOK* malware distribuído por e-mail com informações sobre remessa de encomendas	13/03	08/03
20	O Registro (2020)	EUA	M	Sistemas de saúde no Distrito de Saúde Pública de Champaign Urbana (Illinois) afetados pelo *internauta* ransomware	12/03	10/03
21	F-Secure (2020)	Espanha	PM	E-mail sugere remédio COVID-19 como discutido por cientistas israelenses com dias de antecedência	13/03	10/03
22	Millman (2020)	tcheco	H	Ataque cibernético no hospital tcheco Negação de	14/03	14/03
23	Stein e Jacobs (2020)	EUA	H	serviço na agência de saúde dos EUA	16/03	-
24	Rosso (2020)	Líbia	PM	Corona live 1.1 é o *SpyMax* malware que, neste caso, é um aplicativo trojanizado que exfiltra os dados do usuário A oferta	18/03	-
25	Desai (2020)	Mundo	PM	da máscara Corona instala o que parece ser um malware inofensivo que distribui um SMS para todos os contatos. Presumivelmente, uma atualização do aplicativo mobilizará o malware	19/03	-
26	FitzGerald (2020)	Global	EDUCAÇAO FISICA	Campanha de extorsão ameaça infectar o destinatário com COVID-19, a menos que um pagamento de $ 4.000 em bitcoin seja feito	17/04	20/03
27	Murica Hoje (2020)	Espanha	PM	*internauta* ataque de ransomware disfarçado de e-mail avisando sobre o uso do banheiro	24/03	-
28	Koenig (2020)	EUA	PM	SMS pede que o destinatário faça um teste obrigatório de 'preparação' para COVID-19 e aponta para um site que baixa malware	24/03	24/03
29	Glos Safe Cyber (2020)	Reino Unido	PM	SMS informa destinatário para ficar em casa com um link para mais informações. O link direciona o destinatário para um site cheio de malware	24/03	-

(*Continua na próxima página*)

Tabela 1 (*contínuo*)

30	Rodger (2020)	Reino Unido	P.Ph.F	Refeição escolar gratuita SMS direciona destinatário para site que rouba credenciais de pagamento	25/03	24-03
31	Muncaster (2020)	Mundo	MF	*Ginp*Trojan distribuído em um aplicativo Android. Cobranças de aplicativos€0,75 para informações sobre pessoas infectadas na região receptora. Na verdade, ele rouba as informações de pagamento	25/03	-
32	O'Donnell (2020)	Global	P	Credenciais do Skype roubadas por meio de uma campanha de phishing criada	23/04	31/03
33	Strawbridge (2020)	Mundo	P.Ph.MF	A oferta gratuita da Netflix direciona os usuários para um site cheio de malware	27/03	-
34	de Seguridad del Internauta (2020a)	Espanha	PF	SMS falso pedindo para introduzir dados bancários para obter o pagamento da licença	27/03	-
35	Chadwick (2020)	Reino Unido	M	Site falso do NHS reúne credenciais de usuário E-mail pretende	28/04	-
36	Revista (2020)	Reino Unido	PM	oferecer pagamento de retenção de emprego de acordo com o anúncio governamental do Reino Unido	30/04	19/04
37	Abrams (2020)	Global	M	*Coronalocker*bloqueia um computador e parece causar mais aborrecimento do que qualquer dano real Destinatários do	21/04	-
38	Leitura Sombria (2020)	Global	PM	Docusign direcionados para um site falso que oferece informações sobre o COVID-19	08/05	-
39	Smithers (2020)	Reino Unido	PM	Os destinatários são direcionados para um site falso de rastreamento e rastreamento que coleta as credenciais do usuário	13/05	-

chave: P:Phishing (ou smishing); Ph:Pharming; E: Extorsão; M:Malware; F:Fraude financeira; H: Hackeando.

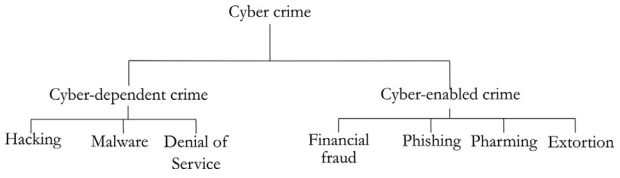

Fig. 1 – Crimes ciberdependentes e ciberativadosPSC (2019).

xingando o próprio vírus, foram usadas as seguintes palavras-chave: SARS-CoV-2, Covid, COVID19, Coronavirus, ---- (tradução chinesa para Coronavirus, confirmada peloOrganização Mundial da Saúde (OMS), 2020a), - - (Japonês tradução para o Coronavírus, confirmado porMinistério da Saúde, Trabalho e Bem-Estar, 2020).

Ao pesquisar por ataques cibernéticos, as seguintes frases-chave foram usadas: ---- (tradução chinesa significa ataque de redeWang e outros, 2009ou ataque cibernéticoOrganização Mundial da Saúde (OMS), 2020d), - - (japonês trans-lação para ataque cibernético ou ataque de hackingJisho, 2020), Attaque Informatique (tradução francesa para Computer Attack Le Parisien, 2020), Attacco Informatico (tradução italiana para Cyber Attacka República, 2020), Ataque Informático (tradução em espanhol para Computer AttackPais, 2020) ou Ciberataque (tradução em espanhol para Cyber Attackde Seguridad del Internauta, 2020b).

*intervalo de tempo*Tentamos encontrar o primeiro ataque cibernético relatado associado à pandemia de COVID-19. Para permitir o desenvolvimento do cronograma e a análise das descobertas, meados de maio de 2020 foi definido como ponto de corte, com a notícia mais recente datada de 13 de maio de 2020 (Smithers, 2020).

*Critério de exclusão*Embora tenhamos criado uma tabela e um cronograma abrangentes, vários resultados foram excluídos da pesquisa. Isso incluía resultados que (a) estavam protegidos por acesso pago, (b) exigiam a criação de uma conta antes da exibição do artigo completo, (c) eram duplicatas de reportagens existentes e d) não podiam ser traduzidos.

3.1.3. Tipos de ataques cibernéticos

Para orientar nossa análise e a criação de uma linha do tempo dos ataques cibernéticos relacionados ao COVID-19, decidimos definir os ataques com base em seus tipos. Isso nos permitiu examinar a proeminência em certos tipos de ataques. Embora existam inúmeras taxonomias relacionadas a ataques e crimes cibernéticos (por exemplo, Cebula e Young, 2010; Ciardhuáin, 2004; Enfermeira, 2019), não existe um modelo universalmente aceito (Hindy e outros, 2020). Neste trabalho, portanto, contamos com a categorização do crime cibernético do Crown Prosecution Service (CPS) do Reino Unido. Essa definição inclui segurança cibernética por padrão e inspirou muitas definições internacionais de crime cibernético.

As diretrizes do CPS categorizar crime cibernético em duas grandes categorias:*ciberdependente*e*cibernético* crimes (CPS, 2019). Um crime ciberdependente é uma ofensa, *"que só pode ser cometido usando um computador, redes de computadores ou outra forma de tecnologia de informação e comunicação (TIC)"*(McGuire e Dowling, 2013a). Os crimes cibernéticos são,*"crimes tradicionais, que podem ser aumentados em sua escala ou alcance pelo uso de computadores, redes de computadores ou outras formas de tecnologia de informação e comunicação (TIC)"*(McGuire e Dowling, 2013b). Essas categorias, bem como exemplos de suas subcategorias, podem ser vistas emFigura 1. Alguns dos elementos descritos pelo CPS são frequentemente interligados em um ataque cibernético. Por exemplo, um e-mail ou mensagem de texto de phishing (por exemplo, SMS ou WhatsApp) pode ser usado para atrair a vítima para um site fraudulento. O site pode coletar dados pessoais que são usados para cometer fraudes financeiras ou pode instalar malware (mais especificamente, ransomware) que é usado para cometer extorsão. Essa noção de sequências de ataques cibernéticos é explicada com mais detalhes em Seção 3.2.

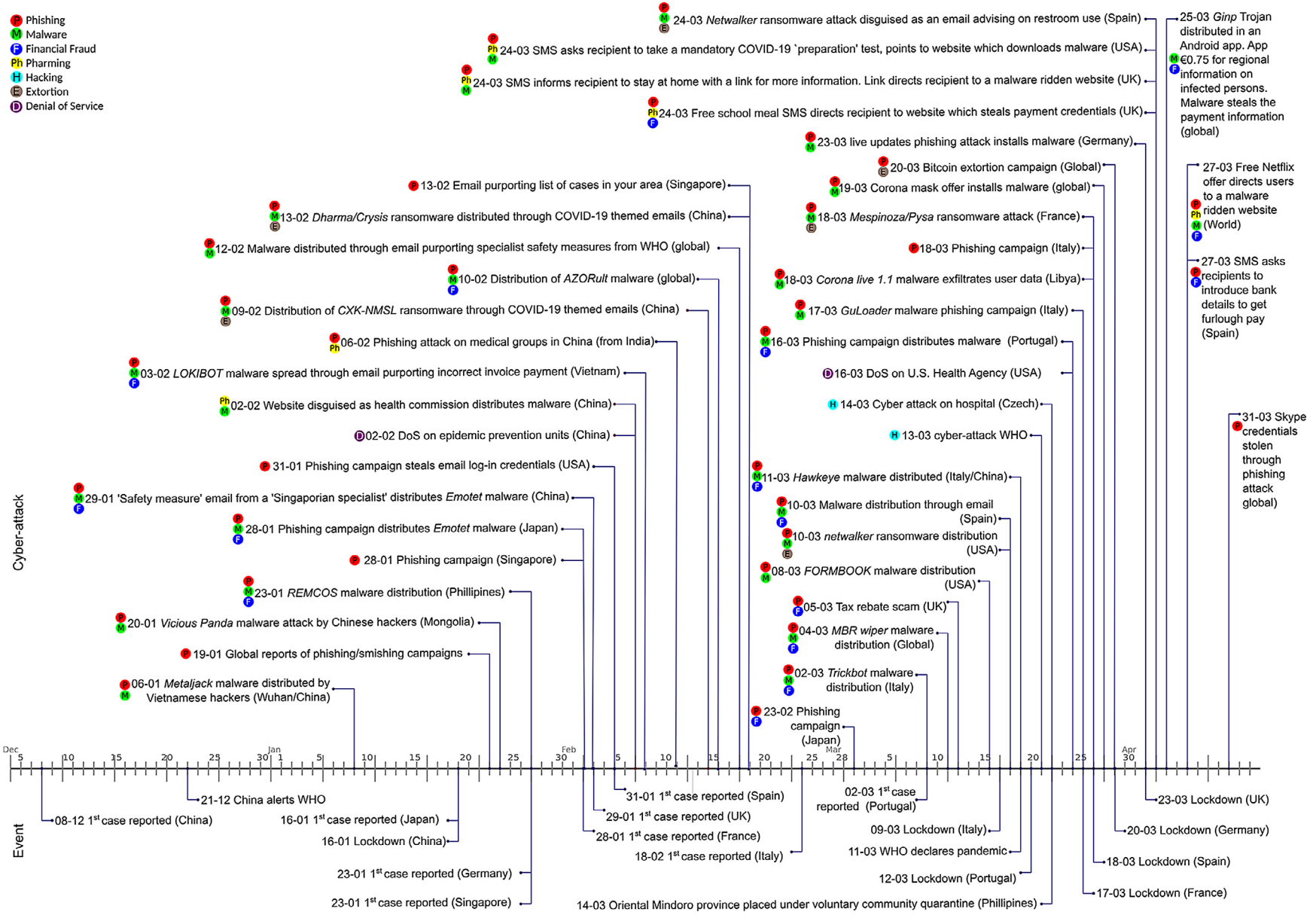

Fig. 2 – Linha do tempo dos principais eventos relacionados a ataques cibernéticos e à pandemia de COVID-19.

Da mesma forma, os ataques de negação de serviço (DoS) são cada vez mais usados por cibercriminosos para distrair (ou atuar como 'cortinas de fumaça' para) empresas durante tentativas de hacking (Bellekens et al., 2019; Kaspersky, 2016). A seguir, consideramos os tipos desses ataques e refletimos sobre como eles foram lançados, incluindo quaisquer fatores humanos ou aspectos técnicos (por exemplo, vulnerabilidades) que tentam explorar.

Phishing, ou Engenharia Social de forma mais ampla, inclui tentativas de partes ilegítimas de convencer indivíduos a realizar uma ação (por exemplo, compartilhar informações ou visitar um site) sob o pretexto de que estão se envolvendo com uma parte legítima. Muitas vezes, mensagens de e-mail são usadas, ocasionalmente mensagens SMS ou WhatsApp são usadas (conhecidas como smishing). O pharming é semelhante ao phishing, mas em vez de enganar os usuários para que visitem sites maliciosos, os invasores confiam em sistemas comprometidos (por exemplo, o dispositivo do usuário ou servidores DNS) para redirecionar os indivíduos para sites ilegítimos. Esse tipo de ataque é menos comum em geral, pois requer mais acesso ou recursos técnicos. A fraude financeira geralmente envolve enganar indivíduos ou organizações usando tecnologia para obter algum ganho financeiro para o invasor ou criminoso.

Ataques de hacking, malware e negação de serviço (DoS) são formas de crime geralmente preferidas por invasores mais técnicos. Hackear envolve comprometer a confidencialidade ou integridade de um sistema e requer uma quantidade razoável de habilidade; suas técnicas podem envolver a exploração de vulnerabilidades do sistema para invadir sistemas. Malware refere-se a software malicioso e pode ser usado para interromper serviços, extrair dados e uma série de outros ataques. Ransomware é um dos tipos mais comuns de malware atualmente (Fruhlinger, 2020; Malwarebytes, 2020) e combina malware com tentativas de extorsão. Os ataques DoS visam a disponibilidade do sistema e funcionam inundando os principais serviços com solicitações ilegítimas. O objetivo aqui é consumir a largura de banda usada para solicitações legítimas do servidor e, eventualmente, forçar o servidor a ficar offline.

Esses tipos de ataque fornecem a base para nossa análise na linha do tempo e como abordamos nossa discussão na parte posterior desta pesquisa.

3.1.4. Limitações da mesa

Dentro detabela 1, são fornecidas duas colunas referentes a datas. A primeira coluna “Data do artigo” refere-se à data em que a referência foi inicialmente publicada. Reconhecemos que, em alguns casos, as páginas da web vinculadas às referências continuaram a ser atualizadas com informações após sua inclusão no artigo. A tabela foi ordenada por “Data do artigo” para fornecer uma representação cronológica consistente dos eventos.

Também fornecemos uma segunda coluna, "Data do ataque". Ao examinar cada referência, se foi fornecida uma data específica de quando o ataque foi executado, ela foi incluída. O raciocínio por trás da inclusão da data do ataque e da data do relatório é que um ataque pode não surgir até vários dias após ter sido realizado.

3.1.5. Limitações da linha do tempo

Dois tipos de relatórios de ataques cibernéticos são considerados neste manuscrito, aqueles que descrevem ataques cibernéticos sem fornecer a data do ataque e aqueles que descrevem ataques cibernéticos. ataques e incluir a data da perpetração. Quando a data do ataque não é incluída, a data fornecida na linha do tempo refere-se à data da publicação. A lógica por trás da inclusão de ambos os tipos de relatórios é baseada em fornecer uma representação cronológica dos eventos. Além disso, embora a tabela forneça uma ampla visão geral do cenário de ameaças, não é de forma alguma uma lista exaustiva de todos os ataques realizados em relação à pandemia, pois a coleta de tais informações não seria possível neste contexto devido à falta e qualidade dos relatórios, o número de incidentes direcionados, o número de incidentes direcionados ao público em geral, a cobertura global da pandemia e o número de atores mal-intencionados realizando esses ataques.

No entanto, apesar dessas limitações, exploramos todos os recursos disponíveis para representar o cenário de ameaças com a maior precisão possível.

3.2. A linha do tempo

Nesta seção, examinamos os ataques cibernéticos com mais detalhes. Figura 2fornece uma representação temporal detalhada da cadeia dos principais ataques cibernéticos induzidos pela pandemia do COVID-19. A linha do tempo inclui os primeiros casos relatados na China, Japão, Alemanha, Cingapura, Espanha, Reino Unido, França, Itália e Portugal e, em seguida, os anúncios subsequentes de bloqueio. A linha do tempo apresenta 44 ataques cibernéticos categorizados usando a taxonomia CPS descrita emSeção 3.1.3e abreviado como:*P:phishing* (ou*smishing*), *M:malware. Ph:pharming, E:extorsão, H:hacking, D:negação de serviço*e *F:fraude financeira*.Os eventos relacionados à crise foram validados em relação ao cronograma de eventos da OMS para garantir uma reprodução temporal precisa.

tabela 1descreve uma série de ataques cibernéticos em mais detalhes. Dentro da tabela, os ataques cibernéticos foram organizados por data de ataque. Se a data de ataque não estiver disponível na referência, então a data do artigo foi usada. O país-alvo de cada ataque cibernético foi listado, juntamente com uma breve descrição dos métodos envolvidos. Finalmente, o tipo de ataque também foi classificado de acordo com a taxonomia CPS descrita anteriormente, onde foi mencionado na referência.

Tanto a figura quanto a tabela apresentam incidentes e ataques cibernéticos específicos e excluem: avisos gerais (por exemplo, de departamentos governamentais), discussões gerais e resumos de ataques e explicações detalhadas de técnicas e abordagens utilizadas pelos invasores.

3.3. Ataques cibernéticos COVID-19 no Reino Unido

A extensão dos problemas relacionados à segurança cibernética enfrentados no Reino Unido foi bastante excepcional e, nesta seção, usamos o Reino Unido como um estudo de caso para analisar o cibercrime relacionado ao COVID-19. A discussão aqui demonstra que, conforme esperado e descrito acima, havia uma correlação frouxa entre anúncios de políticas/notícias e campanhas de crimes cibernéticos associadas. A análise aqui apresentada se concentra apenas em eventos de crimes cibernéticos específicos do Reino Unido. Assim, por exemplo, embora muitos dos incidentes identificados na seção anterior e particularmente emMimecast (2020)são ataques cibernéticos globais, a discussão aqui os ignora. Consequentemente, numerosos anúncios supostamente vindos de reputados or-

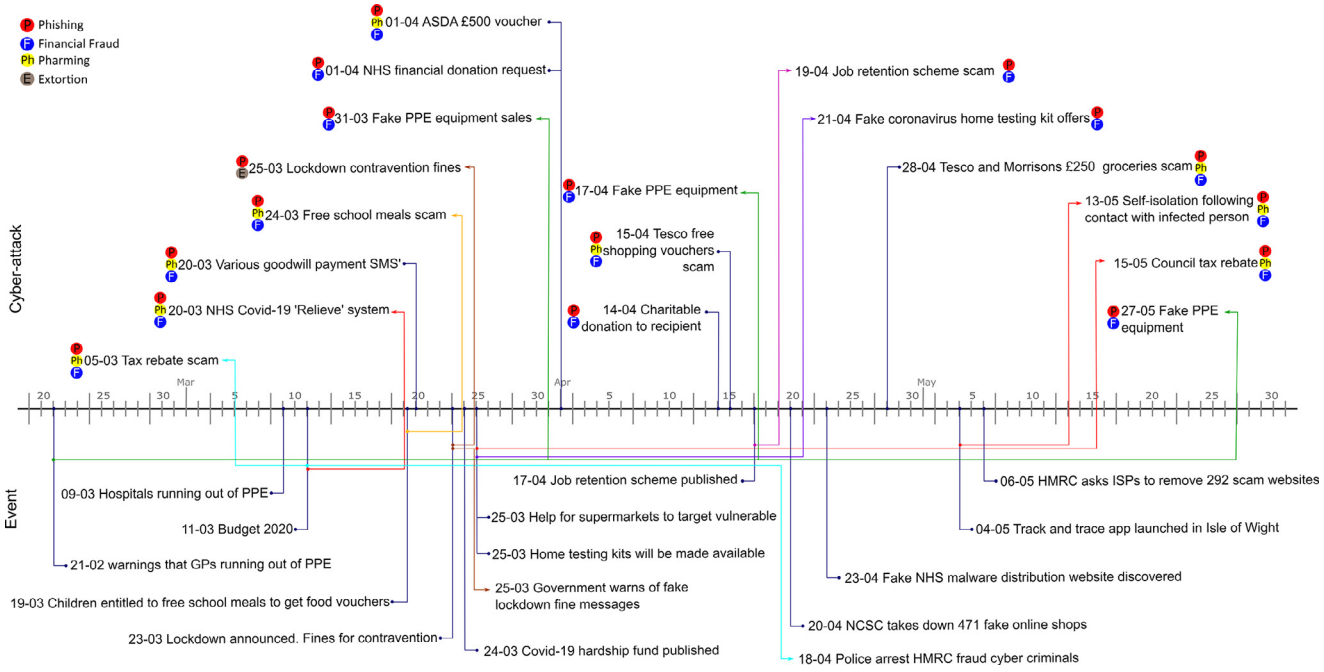

Fig. 3 – Linha do tempo do Reino Unido.

organizações como a OMS e uma infinidade de malware que atingiram os cidadãos do Reino Unido são ignorados, pois não eram problemas específicos do Reino Unido.

Indicações da extensão do problema de incidente de cibercrime no Reino Unido experimentado durante a pandemia são fornecidas pelo nível relatado de e-mails suspeitos e fraudes relatadas. Até o início de maio (07-05-20), mais de 160.000 e-mails 'suspeitos' haviam sido reportados aoNCSC (2020b)e até o final de maio (29-05-20), £ 4,6 milhões foram perdidos para golpes relacionados ao COVID-19 com cerca de 11.206 vítimas de campanhas de phishing e / ou smishing (Sky Notícias, 2020). Em resposta, o Centro Nacional de Segurança Cibernética (NCSC) derrubou 471 lojas online falsas (Arrumado, 2020) e HMRC (Her Majesty's Revenue and Customs) derrubaram 292 sites falsos (Colina, 2020).

A linha do tempo emFig. 3mostra uma série de eventos específicos do Reino Unido e incidentes de crimes cibernéticos. A linha do tempo indica uma correlação direta e inversa entre anúncios e incidentes.

*correlações diretas*são instâncias em que os perpetradores parecem seguir anúncios ou eventos, eles podem ter se aproveitado desses eventos e configurado cuidadosamente os ataques cibernéticos em torno do contexto da política. Estes são mostrados na figura com uma seta de conexão de cor sólida.

*correlações inversas*são casos em que um incidente não tem correlação clara com um evento ou anúncio. Embora as correlações inversas não pareçam ter uma correlação direta, elas podem existir porque vários eventos foram ativamente destacados na mídia. Por exemplo, a questão do equipamento de proteção individual (EPI) estava em discussão ativa bem antes de o governo do Reino Unido dar prioridade a essa consideração. Da mesma forma, a probabilidade de um esquema de redução de impostos estava sendo considerada ativamente no início de março, antes do anúncio do orçamento em 20/11/03. As primeiras campanhas de phishing de redução de impostos estavam em circulação antes do anúncio do orçamento. Em ambos os casos, devemos enfatizar que essas são correlações vagas.

ções e mais trabalho precisa ser feito em termos de se um modelo preditivo pode ser construído usando esses dados e dados em todo o mundo como exemplos.

Em 11 de março de 2020, o governo do Reino Unido fez vários anúncios orçamentários importantes (Governo, 2020) que incluía: um fundo de emergência de £ 5 bilhões para apoiar o NHS e outros serviços públicos na Inglaterra; um direito ao auxílio-doença estatutário para indivíduos aconselhados a se auto-isolar; um Subsídio de Apoio ao Emprego contributivo para trabalhadores independentes; um fundo de £ 500 milhões para os conselhos ajudarem os mais vulneráveis em suas áreas; um Esquema de Empréstimo para Interrupção de Negócios COVID-19 para pequenas empresas; e a abolição das tarifas comerciais para certas empresas.

Logo depois, o governo continuou a fazer anúncios para apoiar a cidadania e a economia. Estes anúncios incluíram: um esquema de apoio a crianças com direito a merenda escolar gratuita (19-03-20); um fundo de dificuldades (24-03-20); ajuda aos supermercados para atingir pessoas vulneráveis (25-03-20); a possível disponibilidade de kits de teste domiciliar (25-03-20); um esquema de retenção de empregos (17-04-20); e o lançamento do tão esperado*seguir e rastrear*aplicativo (04-05-20).

Eventos como esses aumentam a probabilidade de uma resposta positiva a uma campanha cibercriminosa e é muito provável que os perpetradores se apeguem a esses eventos. Embora pareça haver uma ligação entre alguns dos eventos e incidentes, vários golpes não podem ser facilmente atribuídos a um único evento ou anúncio. Exemplos disso incluem um*boa vontade*pagamento de £ 250 (21-03-20), um pedido de doação financeira do NHS (02-04-20), vouchers para supermercados do Reino Unido (02-04-20, 15-04-20, 28-04-20) e uma doação de caridade ao destinatário. Nenhum desses eventos tem anúncios governamentais associados ou mesmo especulação do público em geral.

Exemplos que apoiam nossa noção de correlação entre eventos e campanhas de segurança cibernética são fornecidos em

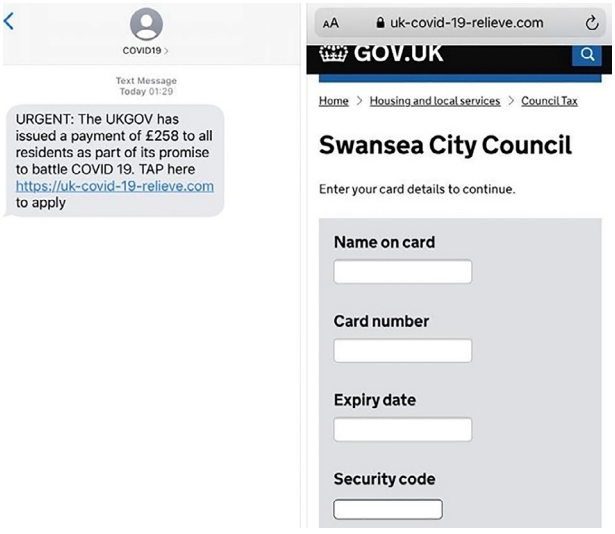

Fig. 4 – O esquema de alívio COVID-19 (Conselho de Swansea, 2020).

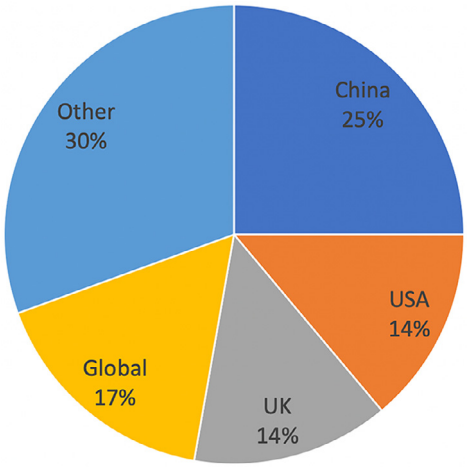

Fig. 5 – Distribuição dos ataques cibernéticos entre os países examinados.

mesa 2e ilustrado emFig. 3. Esses exemplos indicam uma fraca correlação entre eventos e campanhas cibercriminosas. Muitos dos casos descritos emmesa 2eFig. 3, eram muito simples. Vítimas em potencial receberam URLs por e-mail, SMS ou Whatsapp. Um exemplo disso é fornecido em Fig. 4. Nesse caso, a URL apontava para um site institucional falso que solicita dados de cartão de crédito/débito. Embora existam elementos desse processo que são obviamente suspeitos para um usuário de computador mais experiente, por exemplo, erros de ortografia (*aliviar*ao invés de*alívio* no esquema de alívio do COVID-19), endereços de e-mail de resposta suspeitos e URLs claramente incorretos, eles não são imediatamente óbvios para muitos usuários.

3.4. Análise de ataques cibernéticos e riscos associados

A linha do tempo mostrada emFigura 2e o estudo de caso do Reino Unido acima cria uma plataforma ideal para analisar os ataques cibernéticos que ocorreram à luz da pandemia. A partir do momento em que o primeiro caso foi anunciado na China (12-08-19), o primeiro ataque cibernético inspirado no COVID-19 relatado levou 30 dias. O próximo ataque cibernético relatado foi de 14 dias (19-01-20). Deste ponto em diante, fica claro que o intervalo de tempo entre eventos e ataques cibernéticos reduz drasticamente.

Os 43 ataques cibernéticos apresentados na linha do tempo podem ser categorizados da seguinte forma:

- 37 (86%) envolveram phishing e/ou smishing
- 2 (5%) envolveram hacking
- 2 (5%) envolveram negação de serviço
- 28 (65%) envolviam malware
- 15 (34%) envolveram fraude financeira
- 6 (13%) envolveram farmácia
- 6 (15%) envolviam extorsão

Embora essa análise seja útil, a sequência de eventos no ataque completo também pode fornecer informações importantes sobre o ataque. A linha do tempo revela essas sequências e mostra a campanha completa que compreende, por exemplo, a distribuição de mal-

porcelana (*m*) através de phishing (*p*) que rouba credenciais de pagamento usadas para fraudes financeiras (*f*). Podemos descrever essa sequência de ataque cibernético comop,m,f. Analisar ataques cibernéticos dessa maneira é importante porque indica vários pontos em um ataque cibernético onde as proteções podem ser aplicadas. A linha do tempo revela as seguintes sequências de ataques cibernéticos:

- PM:*n=8, 19%*
- p,m,f:*n=10, 23%*
- ph,m:*n=1, 2%*
- p,ph:*n=1, 2%*
- pme:*n=5, 12%*
- p,ph,m:*n=2, 5%*
- p, f, f:*n=1, 2%*
- educaçao Fisica:*n=1, 2%*
- p,ph,m,f:*n=1, 2%*

Esta análise não inclui a sequência de eventos ocorridos nos dois incidentes de hacking e nos dois incidentes de negação de serviço. Deve-se notar que, embora a fraude financeira seja o objetivo mais provável na maioria dos ataques cibernéticos descritos na linha do tempo, a fraude financeira foi registrada apenas na linha do tempo, onde os relatórios indicaram claramente que esse foi o resultado de um ataque cibernético. Na realidade, op,m,fep, f, fcasos provavelmente serão maiores.

Fig. 5fornece um resumo dos países que foram alvo dos primeiros ataques cibernéticos durante a pandemia, organizados por data de ataque. Conforme demonstrado, a China e os EUA respondem por 39% dos ataques relatados. Também fica claro a partirtabela 1que esses dois países foram o alvo principal desde o início da pandemia. Os ataques então se espalharam para o Reino Unido e mais outros países. Em março de 2020, no entanto, a grande maioria dos ataques é direcionada ao mundo inteiro, com um lembrete de ataques especificamente focados em eventos em um único país, como abatimentos de impostos devido ao COVID-19 ou mensagens de phishing de rastreamento de contatos.

É útil considerar isso no contexto de ataques cibernéticos específicos do Reino Unido. Este exame revela que o phishing era um componente de todos (*n=17*) os ciberataques analisados. Um em-

Tabela 2 – Correlações selecionadas entre eventos e campanhas cibercriminosas.

Evento encontro	Evento	Incidente data e tipo	Incidente
21-02-20,	Os médicos alertam que os GPs estão ficando sem EPI;	17-04-20 p, f, f	Ofertas falsas de EPI por e-mail. Link para URLs que capturam cartão de crédito e outros detalhes
09-03-20	Hospitais sem EPIs	27-05-20 p, f, f	
11-03-20	Governo anuncia um gama de pacotes de assistência financeira no orçamento	20-03-20 p, f, f	Campanha Smishing prometendo um pagamento de alívio financeiro COVID-19. Os entrevistados são direcionados para um falso*gov.uk* site que solicita detalhes do cartão de crédito/débito
19-03-20	Governo anuncia um esquema que dá direito às crianças que se qualificam para uma refeição escolar gratuita a um vale-alimentação ou alternativas, se não puderem para continuar frequentando a escola.	24-03-20 p, f, f	Uma campanha smishing que visava os pais com a promessa de ajuda com suas refeições escolares gratuitas em troca de dados bancários. Bancário detalhes são fraudados
23-03-20	Bloqueio anunciado. Multa de contravenção de £ 60, mais tarde (10-05-20) aumentada para £ 100	27-03-20educaçao Fisica	SMS de violação de bloqueio
24-03-20	Fundo de dificuldades COVID-19 permite que os conselhos reduzam as contas do imposto municipal em £ 150 para residentes em idade ativa e que tiveram sua conta reduzida por um prêmio de redução do imposto municipal	15-05-20 p, f, f	Golpe de desconto de imposto municipal
25-03-20	anúncio do governo intenção de disponibilizar kits de testes caseiros	31-03-20p, f, 17-04-20p, f, 27-05-20p, f	Campanhas de phishing na Inglaterra e na Escócia direcionam as vítimas para sites falsos que afirmam vender equipamentos de EPI
17-04-20	Governo anuncia esquema de retenção de empregos	19-04-20p, f	Campanha falsa de phishing de esquema de retenção de empregos.

envolviam a extorsão como objetivo final, os 16 restantes envolviam fraude financeira. Nove ataques cibernéticos compuseram a sequência: p, f, f, sete compunham a sequênciap, f, o restante composto por educaçao Fisica.

É notável que, embora um site de distribuição de malware do NHS tenha sido descoberto e removido em 23-04, nenhum dos ataques cibernéticos que analisamos parecia envolver malware da mesma forma que a análise global revela. Pode haver uma série de razões para isso. Lançar uma campanha conectada a malware requer mais sofisticação e tempo. Pode haver menos oportunidade de conectá-lo diretamente a um evento ou anúncio específico. O intervalo de tempo entre alguns dos anúncios e as campanhas associadas foi notavelmente curto. Por exemplo, o intervalo de tempo entre o anúncio do bloqueio (23-03-20) e a 'multa de contravenção do bloqueio' (25-03-20) foi de 2 dias, e o intervalo de tempo entre o anúncio do esquema de retenção de empregos (17-04- 20) e o golpe de retenção de emprego (19-04-20) também foi de dois dias.

Para refletir de forma mais geral sobre os ataques cibernéticos descobertos, podemos ver que o phishing (incluindo o smishing) foi, de longe, o mais comum com base em nossa análise. No total, esteve envolvido em 86% dos ataques globais. No entanto, isso não é surpreendente, pois as tentativas de phishing são de baixo custo e têm sucesso razoável cotações. No caso do COVID-19, isso incluiu tentativas de se passar por organizações governamentais, a OMS, o Serviço Nacional de Saúde do Reino Unido (NHS), companhias aéreas, supermercados e fornecedores de tecnologia de comunicação. O contexto específico dos ataques pode ser ligeiramente diferente, no entanto, as técnicas subjacentes e o objetivo final são idênticos.

Por exemplo, em um e-mail que se faz passar pela OMS, os invasores anexam um arquivo zip que afirmam conter um e-book que fornece: "*a pesquisa/origem completa do vírus corona e o guia recomendado a seguir para proteger a si e aos outros*"(Bellekens et al., 2016a; MalwareBytes, 2020). Além disso, afirmam: "*Você está recebendo este e-mail agora porque sua vida conta como a vida de todos*". Aqui, os invasores estão usando a marca da OMS, se passando por úteis (o restante do e-mail contém orientação legítima) e apelando para as emoções das pessoas ao elaborar seu e-mail de ataque (Iuga et al., 2016; Enfermeira, 2019). Técnicas semelhantes podem ser vistas em um site falso do NHS criado por criminosos detectados online, que possui marca idêntica, mas está repleto de malware (Correio diário, 2020) e um site malicioso contendo malware que também apresenta o painel COVID-19 legítimo da Johns Hopkins University (Krebs sobre segurança, 2020). É notável que o e-mail falso da OMS contém erros ortográficos/gramaticais. o dis-

discussão emSeção 3.3fornece mais exemplos específicos disso.

Para aumentar ainda mais o provável sucesso dos ataques de phishing, os cibercriminosos foram identificados registrando um grande número de domínios de sites contendo as palavras 'covid' e 'coronavírus' (Ponto de Verificação, 2020). Esses domínios provavelmente são críveis e, portanto, acessados, especialmente se combinados com palavras respeitáveis, como OMS ou Centros de Controle e Prevenção de Doenças (CDC) ou palavras-chave (por exemplo, Corona-virusapps.com, anticovid19-pharmacy.com, que foram destacados como em usoForbes, 2020)). Plataformas de comunicação, como Zoom, Microsoft e Google, também foram falsificadas, tanto por e-mails quanto por nomes de domínio (Ponto de Verificação, 2020). Isso é digno de nota devido ao fato de que essas são as principais tecnologias usadas por milhões em todo o mundo para se comunicar, tanto para trabalho quanto para lazer. Esses fatos, em combinação com e-mails convincentes de engenharia social, mensagens de texto e links, fornecem vários caminhos notáveis para os criminosos atacarem. Ataques de pharming foram muito menos comuns, mas ocorreram em 13% dos casos. Como pode ser vistotabela 1, geralmente ocorrem junto com outros ataques.

A fraude inspirada no COVID-19 alavancou anúncios governamentais/científicos para explorar as ansiedades dos usuários e buscar benefícios financeiros. De acordo com nossa análise, a fraude normalmente era cometida por meio de ataques de phishing e e-mail – também podemos ver isso em nosso sequenciamento acima. Em um caso, criminosos se fizeram passar pelo CDC em um e-mail e solicitaram educadamente doações para desenvolver uma vacina e também que quaisquer pagamentos fossem feitos em Bitcoin (Arrumado, 2020). Técnicas típicas de phishing foram usadas, mas nesta ocasião incluíram pedidos de dinheiro: "*O financiamento do projeto acima é um custo enorme e pedimos sua doação de boa vontade, nada é muito pequeno*". Um ponto notável sobre esse ataque em particular é que ele também pede aos destinatários que compartilhem a mensagem com o maior número possível de pessoas. Isso é preocupante, pois as pessoas têm maior probabilidade de confiar em e-mails que acreditam ter sido examinados por entes próximos (Enfermeira, 2019).

Houve uma série de outras tentativas de fraude, em grande parte baseadas em ameaças ou apelos. Por exemplo, nossa análise identificou ofertas de investimento em empresas que alegam prevenir, detectar ou curar o COVID-19 e investimento em esquemas/opções comerciais que permitem aos usuários aproveitar uma possível crise econômica causada pelo COVID-19 (Departamento de Justiça dos EUA (DOJ), 2020). Houve ofertas de curas, vacinas e conselhos sobre tratamentos eficazes para o vírus. A Food and Drugs Administration (FDA) emitiu 16 cartas de advertência entre 6 de março e 1º de abril de 2020 para empresas*"por vender produtos fraudulentos com alegações de prevenir, tratar, mitigar, diagnosticar ou curar"* COVID-19 (Bellekens et al., 2016b;Administração de Alimentos e Medicamentos (FDA), 2020). O Organismo Europeu Antifraude (OLAF) respondeu à inundação de produtos falsificados online abrindo um inquérito sobre as importações de produtos falsificados devido à pandemia de COVID-19 (Organismo Europeu de Luta Antifraude (OLAF), 2020), e no Reino Unido, a Agência Reguladora de Produtos Médicos e de Saúde (MHRA) começou a investigar dispositivos médicos falsos ou não licenciados atualmente sendo comercializados por meio de sites não autorizados e não regulamentados (Governo do Reino Unido, 2020).

Ataques de extorsão foram testemunhados em nossa análise, mas foram menos prevalentes (aparecendo em apenas 13% dos casos) em comparação com os outros acima. O caso mais proeminente deste ataque foi um e-mail de extorsão ameaçando infectar o destinatário e seus familiares com COVID-19, a menos que um pagamento em Bitcoin seja feito (Sophos, 2020). Para aumentar a credibilidade da mensagem, ela incluía o nome do indivíduo e uma de suas senhas (provavelmente coletada de uma violação de senha anterior). Após exigir o dinheiro, a mensagem segue afirmando: "*Se eu não receber o pagamento, vou infectar todos os membros da sua família com coronavírus*". Isso tenta usar o medo para motivar os indivíduos a pagar e usa senhas (ou seja, itens pessoais) para aumentar a confiança na mensagem do criminoso.

O malware relacionado ao COVID-19 ganhou destaque durante a pandemia e afetou indivíduos e organizações em todo o mundo. Como mostrado acima, foi o segundo maior tipo de ataque cibernético, aparecendo em 65% dos casos.*panda vicioso*e *Carregador MBR*foram os únicos novos malwares descobertos neste período. Os ataques de malware restantes eram variantes de malware existente e incluíam*Metaljack, REMCOS, Emotet, LOKI-BOT, CXK-NMSL, Dharma-Crysis, Netwalker, Mespinoza/Pysa, Spy-Max*(disfarçado de*corona ao vivo 1.1*aplicativo)*GuLoader, Hawkeye, FORMBOOK, Trickbot*e*Ginp*. O ransomware, em particular, era uma ameaça notável e um exemplo disso era o COVIDLock, um aplicativo Android disfarçado de mapa de calor que agia como ransomware; basicamente bloqueando a tela do usuário, a menos que um resgate seja pago (Ferramentas de domínio, 2020).

No nível organizacional, o ransomware teve um impacto significativo nos serviços de saúde — sem dúvida o componente mais frágil da infraestrutura nacional crítica de um país no momento. Ataques foram relatados nos Estados Unidos, França, Espanha e República Tcheca (Mídia Incisiva: Computação, 2020;Com fio, 2020) e usando ransomware como*internauta*. Esses ataques se encaixam em um modus operandi criminoso se presumirmos que agentes mal-intencionados terão como alvo áreas onde acreditam poder capitalizar seus ataques; ou seja, as organizações de saúde podem ser mais propensas a pagar resgates para evitar a perda de vidas de pacientes. Curiosamente, desde então, houve promessas das principais gangues de crimes cibernéticos de que não irão (ou pararão) de atacar os serviços de saúde. Em um relatório, os operadores por trás do CLOP Ransomware, DoppelPaymer Ransomware, Maze Ransomware e Nefilim Ransomware enfatizaram que não visavam (normalmente) hospitais ou que pausariam todas as atividades contra os serviços de saúde até que o vírus se estabilizasse (BleepingComputer, 2020).

Outros exemplos notáveis de malware durante a pandemia incluem:*Trickbot*, um trojan que normalmente é usado como uma plataforma para instalar outros malwares nos dispositivos das vítimas — de acordo com a Microsoft,*Trickbot*é a operação de malware mais prolífica que faz uso de iscas com o tema COVID-19 para seus ataques (InfoSegurança, 2020); um malware reescritor de Master Boot Record (MBR) que limpa os discos de um dispositivo e substitui o MBR para torná-los inutilizáveis (SonicWall, 2020); e *Corona Vivo 1.1*, um aplicativo que utilizou um rastreador COVID-19 legítimo lançado pela John Hopkins University e acessou fotos, vídeos, dados de localização e a câmera do dispositivo (CNET, 2020). À medida que a pandemia continua, é provável que haja mais variedades de malware, visando vários tipos de danos, por exemplo, físicos, financeiros, psicológicos, reputacionais (para empresas) e sociais (Agrafiotis et al., 2018).

Durante a pandemia de COVID-19, nossa análise identificou apenas uma quantidade muito pequena (5%) de ataques DoS, mas houve vários relatos de hackers. Esses relatórios sugeriram que o hacking

não foi indiscriminado, mas sim direcionado a instituições envolvidas em pesquisas sobre o coronavírus.

Em um relatório, o vice-diretor assistente do FBI declarou: "*Certamente vimos atividades de reconhecimento e algumas intrusões em algumas dessas instituições, especialmente aquelas que se identificaram publicamente como trabalhando em pesquisas relacionadas ao COVID.*"(Reuters, 2020). Isso foi ainda apoiado por um comunicado de segurança conjunto um mês depois do NCSC do Reino Unido e do CISA dos EUA (Centro Nacional de Segurança Cibernética do Reino Unido (NCSC), 2020b). Neste comunicado, grupos de Ameaça Persistente Avançada (APT) – alguns dos quais podem se alinhar com estados-nação – foram identificados como tendo como alvo empresas farmacêuticas, organizações de pesquisa médica e universidades envolvidas na resposta ao COVID-19. O objetivo não era necessariamente interromper suas atividades (como no caso do ransomware), mas sim roubar dados confidenciais de pesquisa ou propriedade intelectual (por exemplo, sobre vacinas, tratamentos).

Embora uma análise detalhada desses ataques ainda não tenha surgido, a pulverização de senha (um ataque de força bruta que aplica senhas comumente usadas na tentativa de fazer login em contas) e a exploração de vulnerabilidades na rede virtual privada (VPN) foram sinalizadas (Centro Nacional de Segurança Cibernética do Reino Unido (NCSC), 2020b). A atribuição é outra consideração importante durante esses ataques. Determinar a verdadeira origem dos ataques cibernéticos sempre foi difícil, no entanto, em resposta a essas ameaças relacionadas ao COVID-19, os EUA nomearam abertamente a República Popular da China (PRC) como perpetrador em um anúncio conjunto do FBI/CISA (Federal Bureau of Investigation (FBI), 2020).

4. Impacto na força de trabalho

Os efeitos da pandemia, a quarentena em massa de funcionários e as medidas implementadas para facilitar o trabalho remoto e a resiliência das infraestruturas cibernéticas existentes, contra os ataques e cronogramas descritos anteriormente, tiveram um efeito profundo na força de trabalho - as pessoas envolvidas ou disponível para o trabalho. A pandemia também afetou a resiliência da tecnologia, das estruturas socioeconômicas e ameaçou, até certo ponto, a maneira como as pessoas vivem e se comunicam.Fig. 6ilustra o impacto do COVID-19 na força de trabalho em oito categorias diferentes. Todas as categorias aparentemente se integram com ativos e ferramentas cibernéticas e diferentes categorias podem ser impactadas de forma diferente. A pandemia criou conflitos de risco, por exemplo, o cumprimento estrito de padrões de segurança que desencorajam o compartilhamento de dados, pode ser mais prejudicial do que o compartilhamento de dados. Portanto, embora possa haver requisitos estritos para que os dados do paciente não sejam acessados em casa pelos GPs (clínicos gerais), isso causa um dano maior durante a quarentena do que permitir que os GPs acessem os dados do paciente. Além disso, a forma como as informações confidenciais do paciente são processadas requer uma avaliação de impacto na proteção de dados (DPIA) para permitir mais suporte do NHS quando necessário. Isso pode ter um impacto em termos de entrega oportuna de intervenções médicas em resposta ao COVID-19.

Na classificação de risco tradicional, elementos como registro e avaliação de ativos, frequência de ameaças e probabilidade de vulnerabilidade apresentam maior risco de ameaça cibernética. Antecipamos, portanto, mudanças na forma como a força de trabalho acessa esses ativos de informação e como as tarefas estratégicas, táticas e operacionais são executadas para gerar resultados socioeconômicos. coloca. Essas mudanças podem ser capturadas pelo desenvolvimento e teste de captura de declarações de risco: (1) agentes de ameaças; (2) vulnerabilidades; (3) Violação de política/processo; e (4) exposição geral de ativos em todos os cenários de ameaças emergentes, conforme ilustrado em Fig. 6. Essas mudanças inevitavelmente acarretam mais mudanças nos cenários de ameaças associados às atividades remotas da força de trabalho e à crescente frequência de vetores de ataque armados relacionados à disseminação do coronavírus. Dado o clima atual, é difícil prever se essas mudanças terão um efeito duradouro na força de trabalho, mas sua importância já está registrada (Pipikaite e Davis, 2020). Assim, é cada vez mais importante que o controlo da informação (armazenamento, processamento, transmissão) tenha uma importância elevada dado o aumento dos ciberataques a infraestruturas importantes.

Governos, setores público e privado em toda a Europa atualmente consideram medidas para conter e mitigar o impacto do COVID-19 nas estruturas de dados e estruturas de governança de informações existentes (por exemplo,Comissão de Proteção de Dados, 2020). É dada particular ênfase às implicações da pandemia no tratamento de dados pessoais. O Regulamento Geral de Proteção de Dados da Europa (GDPR) determina que os dados pessoais devem ser processados apenas para os fins específicos e explícitos para os quais foram obtidos (Gabinete do Comissário de Informação, 2020). Além disso, os titulares dos dados devem sempre receber informações explícitas e transparentes sobre as atividades de processamento realizadas, incluindo características e natureza da atividade, período de retenção e finalidade do processamento. Existem desafios relacionados ao cenário de conformidade legal e regulamentar da governança em termos de conformidade versus acesso rápido e processamento de dados por diferentes entidades. Isso é bastante aparente nos casos em que as autoridades públicas buscam obter IPI para reduzir a propagação do COVID-19. Exemplos típicos também incluem aplicativos de rastreamento de contato e plataformas nas quais os dados são agregados online para pós-processamento (Downey, 2020b). Medidas legislativas específicas devem ser reimplantadas ou introduzidas para salvaguardar a segurança pública, mantendo a privacidade em escala, enquanto os princípios legais e regulatórios continuam a ser respeitados (Equipe NHSXIG, 2020).

Com o rápido aumento dos sintomas da COVID-19, os governos tiveram que elaborar um plano que lhes permitisse entender melhor os dados epidemiológicos e identificar intervenções positivas para conter e mitigar o impacto da pandemia. A pesquisa mostra uma alta correlação entre o uso de big data que inclui informações privadas identificáveis na eficácia dessas investigações epidemiológicas (Preço e Cohen, 2019). Isso significava que, na maioria dos casos, os cidadãos precisavam fornecer essas informações voluntariamente e isso rapidamente resultou em discussões e debates sobre as compensações entre segurança pública e privacidade pessoal (Ahn et al., 2020). As informações também foram obtidas por meio da tecnologia de comunicação pela internet. Equipamentos de exames médicos e testes de coronavírus em larga escala foram usados como instrumentos de coleta de dados na luta para reduzir as taxas de mortalidade. As estruturas de conformidade legal e regulamentar diferem entre os países; assim, o gerenciamento de informações pessoais estava sujeito a diferentes medidas de proteção à privacidade.

A desidentificação de informações pessoais foi outro componente que os governos tiveram que exercer para satisfazer os requisitos de privacidade pessoal e aumentar a confiança das pessoas

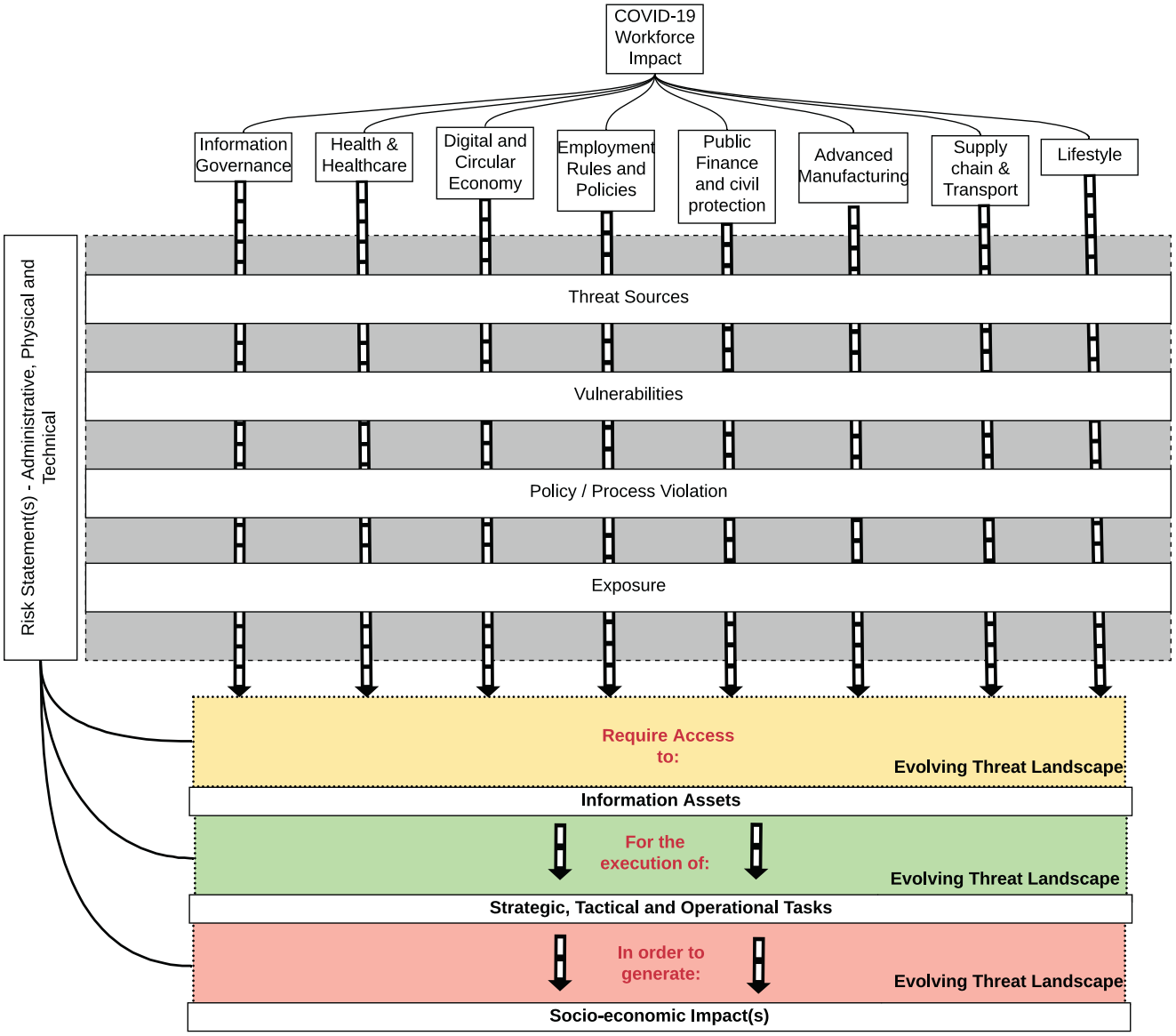

Fig. 6 – Impacto da COVID-19 na força de trabalho.

participantes durante as investigações epidemiológicas. O processo de coleta e processamento de informações pessoais por meio da aplicação de tecnologias de desidentificação levantou desafios técnicos em relação à precisão e consentimento, descarte de dados seguro e legalmente defensivo e robustez das políticas associadas de processamento e gerenciamento de dados para pesquisa epidemiológica. A urgência da situação e a rapidez com que os dados tiveram de ser adquiridos e tratados, criaram um sentimento de desconfiança nos cidadãos e colocaram em causa a eficácia dos processos existentes (Ahn et al., 2020). Os extensos períodos de bloqueio introduzidos em muitos países (descritos em Seção 3) também testaram sua capacidade de implantar estratégias de recuperação dos negócios após esses períodos. Essas estratégias tiveram que garantir uma recuperação suave e gradual dentro de uma pandemia em andamento, o que provou ser uma tarefa desafiadora. No entanto, há uma velocidade e escala sem precedentes nas atividades de P&D em resposta ao surto de COVID-19, forçando o cruzamento de colaborações organizacionais multilaterais (AstraZeneca, 2020; Downey, 2020a).

Atualmente, existe um desafio em toda a Europa para orquestrar o compartilhamento de informações de maneira oportuna e precisa, pois até mesmo as principais fontes da mídia parecem ter propagado informações falsas (Gagne, 2020). O aumento da frequência e do impacto desses ataques testará ainda mais nossos recursos existentes de monitoramento e auditoria, controles de acesso lógico e físico, esquemas de autenticação e verificação atualmente implantados. Além disso, como parte das abordagens atuais de gerenciamento de riscos corporativos, a maneira como as organizações limpam os relatórios de incidentes, o descarte de mídia e os processos de destruição e compartilhamento de dados também serão testados juntamente com os princípios tradicionais de defesa aprofundada atualmente estabelecidos como de fato. O setor financeiro também é afetado, pois a recessão financeira prevista alavancará a sofisticação e a escala dos ataques direcionados à medida que os agentes de ameaças aumentam suas capacidades (Cozinhar, 2020).

5. Conclusão e trabalho futuro

A pandemia do COVID-19 gerou circunstâncias sociais e econômicas notáveis e únicas, alavancadas por cibercriminosos. Nossa análise de eventos como anúncios e histórias da mídia mostrou o que parece ser uma correlação vaga entre o anúncio e uma campanha de ataque cibernético correspondente que utiliza o evento como um gancho, aumentando assim a probabilidade de sucesso.

A pandemia do COVID-19 e o aumento da taxa de ataques cibernéticos que ela invocou têm implicações mais amplas, que vão além dos alvos de tais ataques. Mudanças nas práticas de trabalho e socialização significam que as pessoas agora passam mais tempo online. Além disso, as taxas de desemprego também aumentaram, o que significa que mais pessoas estão sentadas em casa online - é provável que algumas dessas pessoas recorram ao crime cibernético para se sustentar. A combinação de níveis crescentes de ataques cibernéticos e crimes cibernéticos significa que pode haver implicações para o policiamento em todo o mundo - a aplicação da lei deve garantir a capacidade de lidar com o crime cibernético (Collier et al., 2020).

A análise apresentada neste artigo destacou um modus operandi comum de muitos ataques cibernéticos durante esse período. Muitos ataques cibernéticos começam com uma campanha de phishing que direciona as vítimas para baixar um arquivo ou acessar um URL. O arquivo ou a URL atuam como portadores de malware que, quando instalado, atua como veículo para fraudes financeiras. A análise também mostrou que, para aumentar a probabilidade de sucesso, a campanha de phishing utiliza anúncios da mídia e do governo.

Embora esta análise não seja necessariamente nova, acreditamos que esta é a primeira vez que ela é apoiada por um contexto de eventos reais ao vivo. Esta análise dá origem à recomendação de que os governos, os meios de comunicação e outras instituições devem estar cientes de que os anúncios e a publicação de histórias são susceptíveis de dar origem à perpetração de campanhas de ataques cibernéticos associados que alavancam esses eventos. Os eventos devem ser acompanhados de uma nota/disclaimer descrevendo como as informações relacionadas ao anúncio serão retransmitidas.

Nossa pesquisa apresenta oportunidade para trabalhos futuros. Este artigo mostrou o que pode ser melhor descrito como uma correlação direta e inversa frouxa entre eventos e ataques cibernéticos. Pesquisas futuras devem investigar esse fenômeno e definir se um modelo preditivo pode ser usado para confirmar essa relação. Há uma oferta abundante de estudos de caso de ataques cibernéticos relacionados a países ao redor do mundo e uma análise mais ampla do problema pode ajudar a afirmar esse fenômeno.

Declaração de Interesse Concorrente

Os autores declaram que não têm interesses financeiros concorrentes conhecidos ou relacionamentos pessoais que possam parecer influenciar o trabalho relatado neste artigo.

Declaração de contribuição de autoria do CRediT

Harjinder Singh Lallie: Redação - revisão e edição, Redação - projeto original.**Lynsay A. Shepherd:**Redação - revisão e edição, Redação - rascunho original.**Enfermeira Jason RC:**Redação - revisão e edição, Redação - rascunho original.**Arnau Erola:**Redação - revisão e edição, Redação - rascunho original.**Gregório Epifânio:** Redação - revisão e edição, Redação - rascunho original.**Carsten Bordo:** Redação - revisão e edição, Redação - rascunho original. **Xavier Bellekens:**Redação - revisão e edição, Redação - rascunho original.

REFERÊNCIAS

Abrams, L., 2020. Novo malware de bloqueio de tela de coronavírus é extremamente irritante. https://www.bleepingcomputer.com/news/security/ new-coronavirus-screenlocker-malware-is-extremely - chato/(Acessado em 30 de maio de 2020).

Ahn, N.-Y., Park, JE, Lee, DH, Hong, PC, 2020. Balanceamento privacidade pessoal e segurança pública no COVID-19: caso da Coréia e da França.

Agrafiotis I, Nurse JRC, Goldsmith M, Creese S, Upton D. A taxonomia dos danos cibernéticos: definindo os impactos dos ataques cibernéticos e entendendo como eles se propagam. J. Cybersecur. 2018;4(1):1–15.

Anderson R, Barton C, Bölme R, Clayton R, Ganán C, Grasso T, Levi M, Moore T, Vasek M. Em: Workshop sobre Economia da Segurança da Informação (WEIS). Medir o custo variável do cibercrime; 2019.

AON, 2020. Ataques de engenharia social e COVID-19. https://www.aon.com/cyber-solutions/thinking/ social-engineering-attacks-and-covid-19/(Acessado em 17 de junho de 2020).

AstraZeneca, 2020. A AstraZeneca avança na resposta ao global Desafio COVID-19 ao receber os primeiros compromissos para a nova vacina em potencial de Oxford. https://www.astrazeneca.com/media-centre/press-releases/ 2020/astrazeneca-advances-response-to-global-covid-19-challenge-as-it-receives-first-commitments-foroxfords-potential- new-vaccine.html (Acessado em 20 de junho de 2020).

Bellekens X, Hamilton A, Seeam P, Nieradzinska K, Franssen Q, Seeam A. Pervasive eHealth oferece uma pesquisa de conscientização sobre riscos de segurança e privacidade. In: Conferência Internacional de 2016 sobre consciência situacional cibernética, análise de dados e avaliação (CyberSA). IEEE; 2016. pág. 1–4.

Bellekens X, Jayasekara G, Hindy H, Bures M, Brosset D, Tachtatzis C, Atkinson R. Do engano da segurança cibernética à manipulação e gratificação por meio da gamificação. In: Conferência Internacional sobre Interação Humano-Computador. Springer; 2019. pág. 99–114.

Bellekens, XJ, Nieradzinska, K., Bellekens, A., Seeam, P., Hamilton, AW, Seeam, A., 2016b. Um estudo sobre a consciência situacional de segurança e privacidade de dispositivos vestíveis de monitoramento de saúde.

BleepingComputer, 2020. Gangues de ransomware devem parar de atacar Órgãos de Saúde Durante a Pandemia. https:// www.bleepingcomputer.com/news/security/ ransomware-gangs-to-stop-attacking-health-orgs-during - pandemia/(Acessado em 15 de junho de 2020).

CBS Holanda, 2020. Menos crime tradicional, mais cibercrime. https://www.cbs.nl/en-gb/news/2020/10/ less-traditional-crime-more-cybercrime(Acessado em 9 de maio de 2020).

Cebula JL, Jovem LR. In: Relatório Técnico. Uma taxonomia de Riscos operacionais de segurança cibernética. Universidade Carnegie Mellon, Instituto de Engenharia de Software; 2010.

Chadwick, J., 2020. Criminosos cibernéticos criam uma cópia falsa do nhs site no meio da pandemia de coronavírus para induzir os usuários a baixar um malware perigoso que pode roubar suas senhas e dados de cartão de crédito. https://www.dailymail.co.uk/sciencetech/article-8250737/ Kaspersky-detects-fake-NHS-site-steals-credit-card-data. html (Acessado em 30 de maio de 2020).

Check Point, 2020. Atualização sobre ataques cibernéticos de coronavírus: cuidado com o Phish.https://blog.checkpoint.com/2020/05/12/ coronavirus-cyber-attacks-update-beware-of-the-phish/ (Acessado em 17 de maio de 2020).

Chockalingam S, Pieters W, Teixeira A, van Gelder P. Bayesian modelos de rede em segurança cibernética: uma revisão sistemática. In: Conferência Nórdica sobre Sistemas de TI Seguros. Springer; 2017. pág. 105–22.

Ciardhuáin SÓ. Um modelo estendido de investigações de crimes cibernéticos. Int. J. Dígito. Evid. 2004;3(1):1–22.

CNET, 2017. Cuidado com os golpes de phishing do furacão Harvey. https://www.cnet.com/news/ hurricane-harvey-charity-donations-scam-phishing - ataque/(Acessado em 15 de junho de 2020).

CNET, 2020. Aplicativos falsos de rastreamento de coronavírus são realmente malware Isso Persegue Você.https://www.cnet.com/news/ fake-coronavirus-tracking-apps-are-really-malware-that - espreita-seus-usuários/(Acessado em 15 de junho de 2020).

Collier B, Horgan S, Jones R, Shepherd L. In: Research Evidence in Policiamento: Pandemias. As implicações da pandemia de COVID-19 para o policiamento de crimes cibernéticos na Escócia: uma rápida revisão das evidências e considerações futuras. Instituto Escocês de Pesquisa Policial; 2020. Número 1

Cook, A., 2020. COVID-19: Empresas e verticais em risco de ataques cibernéticos. https://www.digitalshadows.com/blog-and-research/ covid-19-companies-and-verticals-at-risk-for - ataques cibernéticos/(Acessado em 17 de junho de 2020).

CPS. In: Relatório Técnico. Cibercrime - Orientação de Acusação. O Crown Prosecution Service (CPS); 2019. https://www.cps.gov.uk/ legal-guidance/ cybercrime-prosecution-guidance(Acessado em 17 de junho de 2020) cqgbxa.com, 2020. Lutando contra a disseminação de coronavírus que enfrenta graves ameaças de segurança cibernética. www.cqgbxa.com/newshy/ 67936.html(Acessado em 30 de maio de 2020). Cressey, DR, 1953. Dinheiro de outras pessoas; um estudo da sociedade psicologia do desfalque..

Cruz M, Shinder DL. Cenário do cibercrime. Syngress Pub.; 2008.

CSDN, 2020. Aproveite o fogo! “a epidemia é uma isca” ataque cibernético.https: //blog.csdn.net/weixin_43634380/article/details/104237121 (Acessado em 30 de maio de 2020).

Cybersecurity Ventures, 2019. Cibercrime anual oficial de 2019 relatório.https://www.herjavecgroup.com/ the-2019-official-annual-cybercrime-report(Acessado em 17 de junho de 2020).

Daily Mail, 2020. Criminosos cibernéticos criam uma cópia falsa do NHS Site no meio da pandemia de coronavírus para induzir os usuários a baixar malware perigoso que pode roubar suas senhas e dados de cartão de crédito. https://www.dailymail.co.uk/sciencetech/article-8250737/ Kaspersky-detects-fake-NHS-site-steals-credit-card-data. html (Acessado em 15 de junho de 2020).

Dark Reading, 2020. Campanha de phishing da Docusign usa COVID-19 como isca.https://www.darkreading.com/attacks-breaches/ docusign-phishing-campaign-uses-covid-19-as-bait/d/d-id/ 1337776 (Acessado em 30 de maio de 2020).

Comissão de Proteção de Dados, 2020. Proteção de Dados e COVID-19.https://dataprotection.ie/en/news-media/blogs/ data-protection-and-covid-19(Acessado em 20 de junho de 2020).

Davis, J., 2020. Impacto do COVID-19 em ransomware, ameaças, Cibersegurança em Saúde.https://healthitsecurity.com/news/ covid-19-impact-on-ransomware-threats-healthcarecybersecurity (Acessado em 10 de novembro de 2020).

Desai, S., 2020. Novo aplicativo Android oferece máscara de segurança contra coronavírus mas oferece sms trojan. https://www.zscaler.com/blogs/research/ new-android-app-offers-coronavirus-safety-mask-delivers - sms-trojan(Acessado em 30 de maio de 2020).

de Seguridad del Internauta, O., 2020a. Detectada uma campanha Fraude de mensagens sms com asunto “erte”. https:// www.osi.es/es/actualidad/avisos/2020/03/ investigado-una-campana-fraudulenta-de-mensajes - sms-con-asunto-erte(Acessado em 20 de novembro de 2020).

de Seguridad del Internauta, O., 2020b. Guia de ciberataques. https://www.osi.es/es/guia-ciberataques(Acessado em 20 de novembro de 2020).

Dhanjani N, Rios B, Hardin B. Hacking: A Próxima Geração: A Próxima geração. O'Reilly Media, Inc.; 2009. Ferramentas de domínio, 2020. Atualização do Covidlock: análise mais profunda de ransomware android coronavírus. https://www.domaintools.com/ resources/blog/ covidlock-update-coronavirus-ransomware(Acessado em 15 de junho de 2020).

Downey, A., 2020a. COVID-19: A colaboração é o motor da Ciência global – especialmente para países em desenvolvimento. https://www.weforum.org/agenda/2020/05/ global-science-collaboration-open-source-covid-19/ (Acessado em 20 de junho de 2020).

Downey, A., 2020b. O aplicativo de rastreamento de contatos do NHS 'fica aquém dos dados lei de proteção'.https://www.digitalhealth.net/2020/05/ nhs-contact-tracing-app-falls-short-of-data-protection - lei/(Acessado em 20 de junho de 2020).

Elsworthy, E., 2020. Centenas de golpes de doação de incêndios florestais circulando.https://www.abc.net.au/news/2020-02-07/ australia-fires-sees-spike-in-fraudster-behaviour/11923174 (Acessado em 15 de junho de 2020).

ESET, 2018. Você NÃO Ganhou! Uma olhada no falso mundo da FIFA Loterias e brindes com tema de Copa. https:// www.welivesecurity.com/2018/06/06/ fake-fifa-world-cup-themed-lotteries-giveaways/(Acessado em 15 de junho de 2020).

Organismo Europeu de Luta Antifraude (OLAF), 2020. OLAF lança inquérito em produtos falsos relacionados ao COVID-19.https: //ec.europa.eu/ anti-fraud/media-corner/news/20-03-2020/ olaf-launches-enquiry-fake-covid-19-related-products_en (Acessado em 17 de maio de 2020).

Europol, 2020. Lucro pandêmico: como os criminosos exploram Crise COVID-19. https://www.europol.europa.eu/publications-documents/ pandemia-profiteering-how-criminals-exploitcovid-19-crisis (Acessado em 15 de junho de 2020).

F-Secure, 2020. Ataques de e-mail de coronavírus evoluindo como surto espalha.https://blog.f-secure.com/ coronavirus-email-attacks-evolving-as-outbreak - espalha/(Acessado em 30 de maio de 2020).

Falliere N, Murchu LO, Chien E. W32. Dossiê Stuxnet. Papel branco Symantec Corp. Segurança. Resposta 2011;5(6):29.

FBI, 2016. Fraude do furacão Katrina.https: //www.fbi.gov/history/famous-cases/hurricane-katrina-fraud (Acessado em 9 de maio de 2020).

FitzGerald, N., 2020. Golpes, mentiras e coronavírus.https://www. welivesecurity.com/2020/04/17/scams-lies-coronavirus/ (Acessado em 30 de maio de 2020).

Food and Drugs Administration (FDA), 2020. Fraudulento produtos da doença de coronavírus 2019 (COVID-19). https://www.fda.gov/consumers/health-fraud-scams/fraudulent-coronavirus-disease-2019-covid-19 - produtos(Acessado em 15 de junho de 2020).

Forbes, 2020. Hackers chineses 'armam' dados de coronavírus para novo ataque cibernético: Aqui está o que eles fizeram. https://www.forbes.com/sites/zakdoffman/2020/03/12/chinese-hackers-weaponized-coronavirus-data-to - lançar este novo ataque cibernético/#196851b03861(Acessado em 30 de maio de 2020).

Forbes, 2020. Existem agora mais de 40.000 'alto risco' Ameaças COVID-19 na Web. https://www.forbes.com/sites/thomasbrewster/2020/04/22/ there-are-now-more-than-40000-high-risk-covid-19- ameaças-on-the-web/(Acessado em 17 de maio de 2020). freebuf.com, 2020. Análises e sugestões sobre diversos tipos de ameaças de segurança de rede durante o período de prevenção e controle da epidemia. https://www.freebuf.com/company-information/227585.html (Acessado em 30 de maio de 2020).

Fruhlinger, J., 2020. Ataques recentes de ransomware definem o nova era do malware. https://www.csoonline.com/article/3212260/recent-ransomware-attacks-define-the-malwares-new-age. html(Acessado em 30 de maio de 2020).

FTC, 2016. Como ajudar as vítimas do terremoto no Equador e Japão.https://www.consumer.ftc.gov/blog/2016/04/how-help-earthquake-victims-ecuador-and-japan(Acessado em 15 de junho de 2020).

FTC, 2020. Dicas de segurança online para trabalhar em casa. https://www.consumer.ftc.gov/blog/2020/03/online-security-tips-working-home(Acessado em 9 de maio de 2020). Gagne, M., 2020. O perigo de infecções na mídia tradicional com informações virais e falsas.https://alibi.com/news/60740/ The-Danger-of-Mainstream-Media-Infections-with-Vir.html (Acessado em 18 de junho de 2020).

Gallagher, S., Brandt, A., 2020. Enfrentando as inúmeras ameaças vinculado ao COVID-19. https://news.sophos.com/en-us/2020/04/14/covidmalware (Acessado em 9 de maio de 2020).

Galov, D., 2020. Remote spring: the rise of rdp bruteforce attack. https://securelist.com/remote-spring-the-rise-of-rdp-bruteforce-attacks/96820 (Acessado em 9 de maio de 2020).

Glos Safe Cyber, 2020. Nosso @glospolice_fcr recebeu ligações perguntando se Textos COVID-19 como os abaixo são genuínos.https: //twitter.com/GlosSaferCyber/status/1242525105508532225 (Acessado em 30 de maio de 2020).

Google, 2020. Google Tradutor.https://translate.google.co.uk/ (Acessado em 30 de maio de 2020).

Governo, U., 2020. Orçamento 2020: o que você precisa saber. https://www.gov.uk/government/news/ budget-2020-what-you-need-to-know, (Acessado em 10 de junho de 2020).

Henderson, S., Roncone, G., Jones, S., Hultquist, J., Read, B., 2020. Agentes de ameaças vietnamitas apt32 visando o governo de Wuhan e o ministério chinês de gerenciamento de emergências no exemplo mais recente de espionagem relacionada ao COVID-19. https://www.fireeye.com/blog/threat-research/2020/04/ apt32-targeting-chinese-government-in-covid-19-relatedespionage.html (Acessado em 17 de junho de 2020).

Hill, M., 2020. HMRC encerra quase 300 phishing de COVID19 Sites fraudulentos.https://www.infosecurity-magazine.com/news/hmrc-covid19-phishing-scams/, (Acessado em 10 de junho de 2020). Hindy, H., Brosset, D., Bayne, E., Seeam, A., Tachtatzis, C., Atkinson, R., Bellekens, X., Uma taxonomia e pesquisa de técnicas de design de sistemas de detecção de intrusão, ameaças de rede e conjuntos de dados.arXiv pré-impressão arXiv:1806.03517

Hiscox, 2019. Relatório de prontidão cibernética hiscox 2019. https://www.hiscox.co.uk/cyberreadiness(Acessado em 9 de maio de 2020).

Hoffman, S., 2009. A morte de Michael Jackson estimula spam e malware campanhas.https: //www.crn.com/blogs-op-ed/the-channel-wire/218101623/ michael-jacksons-death-spurs-spam-malware-campaigns. htm (Acessado em 9 de maio de 2020).

Hindy H, Brosset D, Bayne E, Seeam A, Tachtatzis C, Atkinson R, Bellekens X. Uma taxonomia de ameaças de rede e o efeito dos conjuntos de dados atuais em sistemas de detecção de intrusão. Acesso IEEE 2020;8:104650–75.

Horton N, DeSimone A. Em: Relatório Técnico. Pesadelo da Sony Antes do Natal: O ataque cibernético norte-coreano de 2014 à Sony e lições para ações do governo dos EUA no ciberespaço. JHUAPL Laurel Estados Unidos; 2018.

Mídia incisiva: Computação, 2020. Hospitais espanhóis visados Com iscas de phishing com tema de coronavírus em ataques de ransomware Netwalker.https://www.computing.co.uk/news/ 4012969/hospitals-coronavirus-ransomware(Acessado em 15 de junho de 2020).

InfoSecurity, 2020. Trickbot nomeado o mais prolífico #COVID19 Malware.https://www.infosecurity-magazine.com/news/ trickbot-named-most-prolific/(Acessado em 15 de junho de 2020). Iuga C, Nurse JRC, Erola A. Isca do anzol: fatores que impactam suscetibilidade a ataques de phishing. Hum.-Centric Comput. Inf. ciência 2016;6(1):8.

Jansson, T., 2018. Chantagem e vazamentos de senhas. https://www.linkedin.com/pulse/ blackmailing-passwords-leaks-thomas-jansson(Acessado em 17 de junho de 2020).

Jisho, 2020. Ataque cibernético.https://jisho.org/search(Acesso 30 maio de 2020).

Kaspersky, 2016. Pesquisa revela táticas de hackers: cibercriminosos Use DDoS como cortina de fumaça para outros ataques aos negócios. https://www.kaspersky.com/about/press-releases/2016_research-reveals-hacker-tactics-cybercriminals-use - ddos-como-cortina-de-fumaça-para-outros-ataques-aos negócios(Acessado em 15 de junho de 2020). Kaspersky, 2020. Phishing de coronavírus.https: //www.kaspersky.com/blog/coronavirus-phishing/32395/ (Acessado em 30 de maio de 2020).

Koenig, B., 2020. Tentativa de phishing por SMS da Covid.https: //twitter.com/BigBenKoenig/status/1242503232527589376 (Acessado em 30 de maio de 2020).

Kolomiyets O, Bethard S, Moens MF. Extraindo narrativa linhas do tempo como estruturas de dependência temporal. Em: Anais da 50ª Reunião Anual da Associação de Linguística Computacional: Long Papers-Volume 1. Associação de Linguística Computacional; 2012. pág. 88–97. Kotenko I, Chechulin A. Modelagem e impacto de um ataque cibernético quadro de avaliação. In: 2013 5ª Conferência Internacional sobre Conflitos Cibernéticos (CYCON 2013). IEEE; 2013. pág. 1–24.

Krebs on Security, 2020. Mapa ao vivo do coronavírus usado para se espalhar Malware.https://krebsonsecurity.com/2020/03/ live-coronavirus-map-used-to-spread-malware/(Acessado em 15 de junho de 2020).

Kumaran, N., Lugani, S., 2020. Protegendo empresas contra cibersegurança ameaças durante a COVID-19 e além. https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid - 19 anos ou mais(Acessado em 17 de junho de 2020).

Le Parisien, 2020. Municipal: ataque informático “massivo” no Câmara Municipal de Marselha. http://www.leparisien.fr/elections/municipales/ municipales-attaque-informatique-massive-a-la-mairie - de-marseille-15-03-2020-8280114.php(Acessado em 30 de maio de 2020).

Lush, R., 2020. Ajudando na defesa contra um aumento de 30.000% em ataques de phishing relacionados a golpes de COVID-19. https://www.cgi-group.co.uk/en-gb/blog/cyber-security/help-defend-against-a-30000-increase-in-phishing - golpes relacionados a ataques de covid-19(Acessado em 10 de novembro de 2020).

Magazine, DCR, 2020. Hackers exploram trabalho de coronavírus hmrc esquema de retenção com esquema de e-mail de phishing. https://datacentrereview.com/news/ 1680-hackers-exploit-hmrc-coronavirus-job-retentionscheme-with-phishing-email-scam(Acessado em 30 de maio de 2020). Malwarebytes, 2020. Relatório do estado do malware em 2020. https://resources.malwarebytes.com/files/2020/02/ 2020_State-of-Malware-Report.pdf(Acessado em 30 de maio de 2020). MalwareBytes, 2020. Cibercriminosos se fazem passar por World Health Organização para distribuir e-book falso sobre coronavírus. https://blog.malwarebytes.com/social-engineering/2020/03/ cybercriminals-impersonate-world-health-organization-todistribute-fake-coronavirus-e-book/, (Acessado em 15 de junho de 2020). McGuire M. In: Compreendendo o crescimento do cibercrime Economia. Bromo. Na teia do lucro; 2018. McGuire M, Dowling S. Em: Relatório Técnico. Capítulo 1: Crimes Ciberdependentes; 2013. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246751/horr75-chap1.pdf(Acessado em 18 de junho de 2020)

McGuire M, Dowling S. Em: Relatório Técnico. Capítulo 2: Crimes Cibernéticos - Fraude e Roubo; 2013. https://assets.publishing.service.gov.uk/government/uploads/ system/uploads/attachment_data/file/248621/horr75-chap2. pdf(Acessado em 18 de junho de 2020)

Millman, R., 2020. Resultados do teste de coronavírus atrasados por ataque cibernético no hospital checo.https://www.scmagazineuk.com/ coronavirus-test-results-delayed-cyber-attack-czech-hospital/article/1677194(Acessado em 30 de maio de 2020).

Mimecast, 2020. Novo relatório de inteligência de ameaças: 100 dias de Coronavírus.https://www.mimecast.com/blog/2020/05/100-days-of-coronavirus/, (Acessado em 15 de junho de 2020).

Muncaster, P., 2020. O malware Android aceita pagamento por mapa 'localizador de coronavírus'.https://www.infosecurity-magazine.com/news/android-malware-payment/(Acessado em 30 de maio de 2020).

Murica Today, 2020. Ciberataque ameaça hospital espanhol sistemas de computador. https://murciatoday.com/cyber_attack_threatens_spanish_hospital_computer_systems_1367723-a.html(Acessado em 30 de maio de 2020).

Naked Security, 2009. A morte de Michael Jackson desencadeia spam. https://nakedsecurity.sophos.com/2009/06/26/ michael-jackson-harvesting-email-addresses(Acessado em 9 de maio de 2020).

NCSC, 2020a. Trabalho em casa: preparando sua organização e funcionários.https://www.ncsc.gov.uk/guidance/home-working (Acessado em 9 de maio de 2020).

NCSC, 2020b. NCSC ilumina os golpes que estão sendo frustrados por meio de Novo serviço de geração de relatórios pioneiro. https://www.actionfraud.police.uk/news/ cyber-experts-shine-light-on-online-scams-as-britishpublic-flag-over-160000-suspect-emails, (Acessado em 7 de maio de 2020).

NHS, 2020. 10 dicas para ajudar se você estiver preocupado com o coronavírus. https://www.nhs.uk/oneyou/every-mind-matters/ coronavirus-covid-19-anxiety-tips(Acessado em 9 de maio de 2020). NHSXIG Team, 2020. Conselho de governança de informações COVID-19 para profissionais de ig. https://www.nhsx.nhs.uk/covid-19-response/data-and-information-governance/information-governance/ covid-19-information-governance-advice-igprofessionals/(Acessado em 18 de junho de 2020).

NIST, 2020. Segurança para teletrabalho empresarial, acesso remoto e traga suas próprias soluções de dispositivo (byod). https://csrc.nist.gov/CSRC/media/Publications/Shared/documents/itl-bulletin/itlbul2020-03.pdf(Acessado em 9 de maio de 2020).

Norton, 2020. E-mails de phishing de coronavírus: como se proteger Contra golpes do COVID-19.https://us.norton.com/ internetsecurity-online-scams-coronavirus-phishing-scams. html(Acessado em 15 de junho de 2020).

Enfermeira JRC. In: O Manual Oxford de Ciberpsicologia. O cibercrime e você: como os criminosos atacam e os fatores humanos que procuram explorar. OUP; 2019.

O'Brien, TL, 2020. Golpes de ajuda Covid e negócios duvidosos podem ter sido evitado. https://www.bloomberg.com/opinion/articles/2020-05-01/coronavirus-trillions-in-aid-draws-scams-and-dodgydeals (Acessado em 9 de maio de 2020).

O'Donnell, L., 2020. O ataque de phishing do Skype tem como alvo remoto senhas dos trabalhadores.https://threatpost.com/ skype-phishing-attack-targets-remote-workers-passwords/ 155068/(Acessado em 30 de maio de 2020). Pais, E., 2020. Ataques informaticos. https://elpais.com/noticias/ataques-informaticos/(Acessado em 20 de novembro de 2020).

Patranobis, S., 2020. Hackers indianos visando médicos chineses Institutos em meio a surto de coronavírus, diz relatório. https://www.hindustantimes.com/world-news/indian-hackers-targetting-chinese-medical-institutesamid-coronavirus-outbreak-says-report/história-piDHQeY4UfTVy8BWa2GG3O.html, (Acessado em 12 de junho de 2020).

Pipikaite, A., Davis, N., 2020. Por que a cibersegurança é mais importante do que nunca durante a pandemia de coronavírus. https://www.weforum.org/agenda/2020/03/ coronavirus-pandemic-cybersecurity/(Acessado em 18 de junho de 2020).

Price W, Cohen I. Privacidade na era do big data médico. Nat. Med. 2019;25. doi:10.1038/s41591-018-0272-7 .

la Repubblica, 2020. Ataque cibernético à easyjet, comprometeu o dados de nove milhões de clientes. https://www.repubblica.it/tecnologia/sicurezza/2020/05/19/ news/attacco_informatico_a_easyjet_compromessi_i_dati_di_nove_milioni_di_clienti-257099879/(Acessado em 30 de maio de 2020). Reuters, 2020. Funcionário do FBI diz que hackers estrangeiros têm como alvo Pesquisa COVID-19. https://uk.reuters.com/article/us-health-coronavirus-cyber/strange-state-hackers-target-us-coronavirus-treatmentresearch-fbi-official-idUKKBN21Y3GL(Acessado em 15 de junho de 2020). Rodger, J., 2020. O golpe de texto de coronavírus das refeições escolares que poderia enganar os pais de milhares. https://www.birminghammail.co.uk/news/midlands-news/school-meals-coronavirus-text-scam-17975311(Acessado em 30 de maio de 2020).

Rosso, KD, 2020. Nova descoberta de ameaças mostra comercial os operadores de vigilância mais recentes a explorar o COVID-19. https://blog.lookout.com/ Commercial-surveillanceware-operators-latest-totake-advantage-of-covid-19(Acessado em 30 de maio de 2020). Segura, J., 2017. Contas vinculadas comprometidas usadas para enviar links de phishing via mensagem privada e e-mail. https://blog.malwarebytes.com/threat-analysis/2017/09/comprometido-linkedin-accounts-used-to-send-phishing - links-via-mensagem-privada-e-e-mail(Acessado em 9 de maio de 2020).

Shepherd L, Renaud K. Como projetar a segurança do navegador e alertas de privacidade. In: AISB 2018. Society for the Study of Artificial

Inteligência e Simulação para o Comportamento (AISB); 2018. pág. 21–8. Convenção AISB 2018: Simpósio sobre Intervenção Comportamental Digital para Segurança Cibernética

Shi, F., 2020. Ameaça em destaque: phishing relacionado ao coronavírus. https://blog.barracuda.com/2020/03/26/ ameaça-spotlight-coronavirus-related-phishing(Acessado em 9 de maio de 2020).

Sky News, 2020. Coronavírus: vítimas de fraudes perderam mais de £ 4,6 milhões para golpes relacionados a vírus.https://news.sky.com/story/ coronavirus-fraud-victims-have-lost-more-than-4-6mto-virus-related-scams-11996721, (Acessado em 10 de junho de 2020). Smithers, R., 2020. Fraudadores usam aplicativo falso de rastreamento de contatos nhs em golpe de phishing.https://www.theguardian.com/world/2020/may/13/fraudsters-use-bogus-nhs-contact-tracing-app - esquema de phishing(Acessado em 30 de maio de 2020).

smzdm.com, 2020. Os hackers estão usando o medo do "coronavírus" para phishing, preste atenção prevenção!https://post.smzdm.com/p/a07ol5x0/(Acessado em 30 de maio de 2020).

SonicWall, 2020. Trojan de coronavírus substituindo o MBR. https://securitynews.sonicwall.com/xmlpost/ coronavirus-trojan-overwriting-the-mbr/(Acessado em 15 de junho de 2020).

Sophos, 2020. E-mail de extorsão secreto e sujo ameaça dar seu coronavírus familiar. https://nakedsecurity.sophos.com/2020/03/19/ dirty-little-secret-extortion-email-threatens-to-give-your - família-coronavírus/(Acessado em 15 de junho de 2020).

Stajano F, Wilson P. Entendendo as vítimas de golpes: sete princípios de segurança de sistemas. Comum. ACM 2011;54(3):70–5.

Stein, S., Jacobs, J., 2020. Ataque cibernético atinge agência de saúde dos EUA em meio ao surto de COVID-19. https://www.bloomberg.com/news/articles/2020-03-16/ us-health-agency-suffers-cyber-attack-during-covid-19-response(Acessado em 30 de maio de 2020).

Stonefly, 2020. Infecção por coronavírus e ransomware - o que é a conexão?https://stonefly.com/blog/coronavirus-ransomware-infection-whatsthe-connection(Acessado em 12 de junho de 2020).

Strawbridge, G., 2020. Alerta sobre o golpe do coronavírus netflix. https://www.metacompliance.com/blog/ warning-over-coronavirus-netflix-scam/(Acessado em 30 de maio de 2020).

Conselho de Swansea, 2020. Golpes de coronavírus. https://www.swansea.gov.uk/coronavirusscam, (Acessado em 10 de junho de 2020).

TechRepublic, 2020. Indústria naval global atacada por malware com tema de coronavírus. https://www.techrepublic.com/article/ global-shipping-industry-attacked-by-coronavirus-themed -malware/(Acessado em 30 de maio de 2020).

Federal Bureau of Investigation (FBI), 2020. República Popular da China (PRC) Segmentação de organizações de pesquisa COVID-19. https://www.fbi.gov/news/pressrel/press-releases/peoples-republic-of-china-prc-targeting-of-covid-19 - organizações de pesquisa(Acessado em 15 de junho de 2020).

The Guardian, 2020. Autoridades dos EUA lutam contra o surto de coronavírus Golpes, de phishing a tratamentos falsos.https: //www.theguardian.com/world/2020/mar/19/coronavirus - golpes-phishing-tratamentos-falsos(Acessado em 15 de junho de 2020).

Gabinete do Comissário da Informação, 2020. Dados gerais regulamento de proteção (RGPD): Princípio (b): Limitação de finalidade. https://ico.org.uk/for-organizations/guide-to-data-protection/ guide-to-the-general-data-protection-regulation-gdpr/princípios/purpose-limitation/(Acessado em 19 de junho de 2020).

Ministério da Saúde, Trabalho e Bem-Estar, 2020. Últimas informações sobre a doença de coronavírus 2019 (COVID-19).https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000164708_00001.html(Acessado em 30 de maio de 2020). The Register, 2020. Nova miséria de vírus para Illinois: saúde pública agência derrubada por... web ransomware. ótimo momento, canalhas. https://www.theregister.co.uk/2020/03/12/ ransomware_illinois_health/ (Acessado em 30 de maio de 2020). The Times, 2020. Fraudadores se fazem passar por companhias aéreas e Tesco em golpes de coronavírus.https://www.thetimes.co.uk/article/ fraudsters-impersonate-airlines-and-tesco-in-coronavirusscams-5wdwhxq7p, (Acessado em 15 de junho de 2020).

Tidy, J., 2020. Coronavírus: Israel habilita poderes de espionagem de emergência. https://www.bbc.co.uk/news/technology-51930681(Acessado em 30 de maio de 2020).

Tsakalidis G, Vergidis K. Uma abordagem sistemática para descrição e classificação de incidentes de crimes cibernéticos. IEEE Trans. Sist. Homem Cibern. 2017;49(4):710–29.

Tysiac, K., 2018. Como os cibercriminosos atacam vítimas de violência natural desastres. https://www.journalofaccountancy.com/news/2018/sep/cyber-criminals-prey-on-natural-disaster-victims-201819720. html(Acessado em 9 de maio de 2020).

Governo do Reino Unido, 2020. Medicamentos e dispositivos médicos do Reino Unido Regulador investiga 14 casos de produtos médicos COVID-19 falsos ou não licenciados.https://www.gov.uk/government/news/uk-medicines-and-medical-devices-regulatorinvestigating-14-cases-of-fake-or-unlicensed-covid-19-medical-products(Acessado em 17 de maio de 2020).

Centro Nacional de Segurança Cibernética do Reino Unido (NCSC) e dos EUA Departamento de Segurança Interna (DHS) Agência de Segurança Cibernética e Infraestrutura (CISA), 2020b. Aconselhamento: os grupos APT visam cuidados de saúde e serviços essenciais. https://www.ncsc.gov.uk/news/apt-groups-target-healthcare-essential-services - consultivo(Acessado em 15 de junho de 2020).

Centro Nacional de Segurança Cibernética do Reino Unido (NCSC) e dos EUA Departamento de Segurança Interna (DHS) Agência de Segurança Cibernética e Infraestrutura (CISA), 2020a. Aviso: COVID-19 explorado por agentes cibernéticos maliciosos. https://www.ncsc.gov.uk/news/covid-19-exploited-by-cyber-actors-advisory(Acessado em 15 de junho de 2020).

Departamento de Justiça dos EUA (DOJ), 2020. Fraude COVID-19. https://www.justice.gov/usao-edky/covid-19-fraud-1 (Acessado em 15 de junho de 2020).

Van Heerden R, Von Soms S, Mooi R. Classificação do cyber ataques na África do sul. In: Conferência IST-Africa Week 2016. IEEE; 2016. pág. 1–16.

Walter, J., 2020. Ameaça Intel: Ataques Cibernéticos Aproveitando o Pandemia de COVID-19/CoronaVirus. https://labs.sentinelone.com/Threat-intel-update-cyber-attacks-leveraging-the-covid-19-coronavirus-pandemic/, (Acessado em 10 de junho de 2020). OMS, 2020. #healthyathome.https://www.who.int/news-room/campanhas/conectando-o-mundo-para-combater-o-coronavírus/healthathome(Acessado em 9 de maio de 2020).

Wired, 2020. Hackers estão mirando em hospitais prejudicados por Coronavírus.https://www.wired.co.uk/article/ coronavirus-hackers-cybercrime-phishing(Acessado em 15 de junho de 2020).

Fórum Econômico Mundial, 2020. Perspectivas de riscos da COVID-19: uma Mapeamento Preliminar e suas Implicações. https://www.weforum.org/reports/covid-19-risks-outlook-a-preliminary-mappingand-itsimplications(Acessado em 10 de novembro de 2020). Organização Mundial da Saúde (OMS), 2020a. Doença do coronavírus (Pandemia do covid19.https://www.who.int/zh/emergencies/disease/novel-coronavirus-2019(Acessado em 18 de junho de 2020).

Organização Mundial da Saúde (OMS), 2020b. Nomeando o doença de coronavírus (COVID-19) e o vírus que a causa. https://www.who.int/emergencies/diseases/ novel-coronavirus-2019/technical-guidance/ naming-the-coronavirus-disease-(covid-2019) - e-o-vírus-que-causa-isso(Acessado em 15 de junho de 2020).

Organização Mundial da Saúde (OMS), 2020c. OMS Coronavírus Painel de controle de doenças (COVID-19).https://covid19.who.int/, (Acessado em 15 de junho de 2020).

Organização Mundial da Saúde (OMS), 2020d. Quem relata cinco vezes aumento de ataques cibernéticos, pede vigilância. https://www.who.int/zh/news-room/detail/ 23-04-2020-who-reports-fivefold-increase-in-cyberattacks-urges-vigilance (Acessado em 18 de junho de 2020).

Wang Gy, Wang Hm, Chen Zj, Xian M. Pesquisa em computador modelagem de ataque de rede baseada em gráfico de ataque. J. Natl. Univ. Tecnologia de Defesa. 2009;4:816–19.

Yar M. A novidade do 'crime cibernético' uma avaliação à luz de teoria da atividade rotineira. EUR. J. Criminol. 2005;2(4):407–27.

Dr. Harjinder Singh Lallieé professor associado da University of Warwick e acadêmico visitante da University of Oxford. Harjinder possui um Ph.D. em segurança cibernética, um M.Phil, um M.Sc. e um BSc. Harjinder tem mais de vinte anos de experiência de ensino e atualmente lidera o grau M.Sc.Cyber Security and Management. A pesquisa de Harjinder se concentra na área de modelagem complexa de ataques cibernéticos, análise forense digital e uso de IA em análise forense digital. Ele publicou vários artigos de pesquisa nas principais revistas de segurança cibernética do mundo. Harjinder foi membro de vários comitês de conferências, atua como examinador externo e realizou várias revisões institucionais nacionais e internacionais. Recentemente, atuou como consultor da Agência Internacional de Energia Atômica (AIEA) nas Nações Unidas em Viena.

Dra Lynsay A. Shepherdé professor de segurança cibernética e interação humano-computador na Abertay University, Dundee, e trabalha na Escola de Design e Informática. Lynsay tem um Ph.D. em Segurança Utilizável, um M.Sc. em Computação na Internet e um B.Sc. (Hons) em Computação. Os interesses de pesquisa de Lynsay atualmente se concentram nos aspectos humanos da segurança cibernética, examinando o comportamento de segurança do usuário final e explorando métodos para melhorar a conscientização sobre segurança.

Dr Jason RC Enfermeiroé Professor Associado em Segurança Cibernética na Escola de Computação da Universidade de Kent, Reino Unido e no Instituto de Segurança Cibernética para a Sociedade (iCSS), Reino Unido. Ele também ocupa os cargos de Acadêmico Visitante na Universidade de Oxford, Membro Visitante em Defesa e Segurança na Universidade de Cranfield, Reino Unido e Membro Associado no Royal United Services Institute for Defense and Security Studies (RUSI). Seus interesses de pesquisa incluem gerenciamento de riscos de segurança, comunicações corporativas e segurança cibernética, Internet das Coisas segura e confiável, ameaças internas e crimes cibernéticos. Jason foi selecionado como uma estrela em ascensão por sua pesquisa em segurança cibernética, como parte da campanha de prêmios Recognizing Inspirational Scientists and Engineers (RISE) do Conselho de Pesquisa em Engenharia e Ciências Físicas do Reino Unido. A Dra. Nurse possui um Ph.D. em segurança cibernética, um M.Sc. em Computação na Internet e um B.Sc. em Ciência da Computação e Contabilidade. Ele publicou mais de 100 artigos revisados por pares em revistas e conferências de segurança reconhecidas internacionalmente.

Dr Arnau Erolaé Pesquisador Associado Sênior no Departamento de Ciência da Computação da Universidade de Oxford, trabalhando em seguros cibernéticos e compreendendo melhor o cenário de ameaças cibernéticas. Seus interesses de pesquisa incluem, mas não estão limitados a, segurança, sistemas de defesa e economia da cibersegurança. O Dr. Erola possui um Ph. D., M. Sc. e B.Sc. em Ciência da Computação pela Universitat Rovira i Virgili (Tarragona). Ele é autor de vários artigos em jornais internacionais sobre privacidade online, protocolos de anonimato e mecanismos de detecção de intrusão.

Dr. Gregory Epiphaniouatualmente ocupa o cargo de professor associado de engenharia de segurança na Universidade de Warwick. Sua função envolve suporte a licitações, pesquisa aplicada e publicações. Ele liderou e contribuiu para vários projetos de pesquisa financiados por EPSRC, IUK e autoridades locais, totalizando mais de 3M. Anteriormente, ele ocupou o cargo de leitor em segurança cibernética e atuou como vice-diretor do Wolverhampton Cybersecurity Research Institute (WCRI). Lecionou em diversas universidades, tanto a nível nacional como internacional, diversas áreas relacionadas com a defesa proativa de redes com mais de 80 publicações internacionais em revistas, atas de conferências e autor de vários livros e capítulos. Ele possui várias certificações do setor em segurança da informação e trabalhou com várias agências governamentais, incluindo o MoD do Reino Unido em projetos relacionados à segurança cibernética.

Professor Carsten Mapleé o pesquisador principal do Centro Acadêmico de Excelência NCSC-EPSRC em Pesquisa de Segurança Cibernética da Universidade e professor de Engenharia de Sistemas Cibernéticos na WMG. Ele também é coinvestigador do Centro Nacional de Excelência PETRAS para Segurança Cibernética de Sistemas IoT, onde lidera Transporte e Mobilidade. Carsten é membro do Alan Turing Institute, onde é o principal pesquisador do projeto Trustworthy Digital Infrastructure de US$ 5 milhões. Ele tem uma reputação internacional em pesquisa e ampla experiência no desenvolvimento de estratégias institucionais e na interação com agências externas. Ele publicou mais de 250 artigos revisados por pares e é coautor do Relatório de Investigações de Violação de Segurança do Reino Unido de 2010, apoiado pela Agência de Crime Organizado Grave e pela Unidade Central de Crimes Eletrônicos da Polícia. Carsten também é coautor de Cyberstalking in the UK, um relatório apoiado pelo Crown Prosecution Service and Network for Surviving Stalking. Sua pesquisa atraiu milhões de libras em financiamento e foi amplamente divulgada pela mídia. Ele deu provas a comitês governamentais sobre questões de anonimato e segurança infantil online. Além disso, ele aconselhou diretores executivos e não executivos de organizações do setor público e organizações privadas multibilionárias. O professor Maple é ex-presidente do Conselho de Professores e Chefes de Computação no Reino Unido, membro do Zenzic Strategic Advisory Board, membro do IoTSF Executive Steering Board, membro do comitê executivo da EPSRC RAS Network e membro do o UK Computing Research Committee, o grupo de especialistas ENISA CarSEC,

Doutor Xavier Bellekensé Professor Assistente do Chancellor's Fellow no Departamento de Engenharia Eletrônica e Elétrica da Universidade de Strathclyde e membro não residente do Scowcroft Center for Strategy and Security no Atlantic Council. Seus interesses de pesquisa atuais incluem proteção de infraestrutura crítica, defesa, bem como dissuasão e fraude cibernética. Xavier também é o presidente das conferências IEEE Cyber Science, o líder temático de segurança cibernética educacional, o presidente do Blockchain Group e o vice-presidente do grupo de segurança cibernética do IEEE Reino Unido e Irlanda. Ele frequentemente aparece na mídia para fornecer comentários à imprensa internacional – no rádio, TV e jornais sobre os principais eventos cibernéticos.